



universität  
wien

## DISSERTATION / DOCTORAL THESIS

Titel der Dissertation / Title of the Doctoral Thesis

„Strategies for optimal realization and operation of  
entanglement-based quantum communication along fiber links“

verfasst von / submitted by

Sebastian Philipp Neumann, BSc BA MSc MA

angestrebter akademischer Grad / in partial fulfilment of the requirements for the degree of

Doktor der Naturwissenschaften  
(Dr. rer. nat.)

Wien, 2022 / Vienna, 2022

Studienkennzahl lt. Studienblatt /  
degree programme code as it appears on  
the student record sheet:

UA 796 605 411

Dissertationsgebiet lt. Studienblatt /  
field of study as it appears on  
the student record sheet:

Physik

Betreut von / Supervisor:

Mag. Dr. Marcus Huber, Privatdoz.



This thesis is, in loving memory, dedicated to  
my father Gerald Neumann  
and my grandfather Horst Neumann.



# Acknowledgments

This thesis wouldn't have been possible without the continuing support of many people, to whom I owe heartfelt gratitude. The order of the following acknowledgments is meaningless, since all of you have helped, influenced and, very importantly, entertained me during the time of my employment at IQOQI, and it is impossible to rank the impact you've had on me.

However, before I start, I still want to point out three people who (more than just) deserve my special appreciation: My mother Karin Neumann, who has supported me and my sometimes very fuzzily outlined goals for the future with all the warmth of her heart, which is a *lot*. My significant other Sonia Friedmann, who never ceased to motivate me, supplied me with the admiration that I dearly need, and distracted me from my work whenever necessary. And Dr. Rupert Ursin, the leader of my research group — a generous sender and appreciative receiver of insults, who decided to hire me on three separate occasions, although deep regret about these decisions hit him every single time even before the ink of our signatures had dried.

I want to thank my brother Laurenz Neumann and my stepfather Hannes Bauer for their emotional and physical support and many beautiful experiences together. Thank you to my oldest and closest friends Viktoria Nowak, Axel Innerebner, Tamara Mijatovic, Johannes Bruckbauer, Max Potzel and Helene Muhr. Sebastian Ecker of course also prominently belongs to this enumeration, but he is cross-listed with my colleagues at IQOQI — thanks for years and years of sharing a ridiculously overstaffed office, for an abundance of hilarious distractions given and received and for many rounds of backgammon.

Colleagues I also want to thank and who I dare say have become friends during our IQOQI time together are Martin Bohmann and the Lukases, Bulla and Achatz. Thank you Martin for all the German beer, thank you Bulla for making me risk my own and my nanowire's life for nothing and thank you Achatz for your constant inferiority in backgammon. Besides the already mentioned Dr. Rupert Ursin, I would like to thank Dr. Thomas Scheidl, Dr. Fabian Steinlechner, Dr. Matthias Fink and Dr. Sören Wengerowsky for their seemingly inexhaustible patience with all my questions and for the kind of knowledge transfer that anybody could only wish for. I will also not forget the efforts of IQOQI's administrative staff to divert as much bureaucracy away from us students as possible: thank you Lukas Edengruber, Benjamin Skarabela and Manuela Csapo. Special thanks go to Roland Blach, whose unbelievable skills in anything remotely related to handiwork have made most of my experiments possible in the first place. I would also like to thank my master students for their acceptance of my improvised on-the-go lecturing and their intelligent questions, which have helped me a lot in understanding what I was actually talking about: Ulrich Galander, Domenico Ribezzo, Mirela Selimovic and Alexander Buchner, in order of appearance.

Furthermore, I would like to thank all my "classmates" of the CoQuS PhD school, who I discovered to be very enjoyable and open-minded people — all the best to your scientific careers!

Naturally, over the course of the seven and a half years I have spent at IQOQI, more people than I can list here have had an impact on me and my work. Therefore, I apologize to all those colleagues, friends and acquaintances whom I cannot mention here, and extend my gratefulness to them.

Last, but definitely not least, I want to thank Marcus Huber, who spontaneously jumped in as my thesis advisor and successfully tried to make my last months as a doctoral candidate as pleasant as possible.

Thank you all!



# Abstract

Quantum key distribution is one of the most mature applications of quantum mechanics. It promises unconditionally secure communication between distant partners based on the laws of physics rather than assumptions about computational hardness, as is the case in currently used asymmetric encryption protocols. The long-distance transmission of single quanta, which is a precondition for feasible quantum key distribution, is most efficiently achieved using single photons. While there are many different protocols for quantum key distribution, entanglement-based applications such as the BBM92 protocol have the advantage of being immune to certain potential attacks, and they require comparably little electronical engineering overhead. In BBM92, the communication partners Alice and Bob each receive one entangled photon of a pair and measure the degree of freedom they are entangled in, e.g. polarization. By randomly switching between two mutually unbiased polarization bases for each of these measurements and comparing parts of the results, Alice and Bob can find out whether a potential eavesdropper has tried to hack their communication by extracting information from the photon states. If Alice and Bob conclude that this hasn't been the case, they and only they are in possession of the same quantum-random bit string, which they can use as a symmetric encryption key via any classical, unsecured channel.

In this work, I show a continuously working long-distance polarization-based BBM92 protocol over 248 km of deployed telecommunication fiber, as well as the necessary pre-studies. While free-space quantum connections via satellite have the advantage of substantially lower loss, fiber-based applications do not require an obstruction-free line of sight. This means that they can be operated continuously, without limitations by time of day, weather, or satellite position. This can in certain configurations compensate for the substantially lower transmission rates.

There are several specific challenges to be overcome in fiber-based BBM92, the most important ones being strong attenuation, chromatic dispersion and polarization drift. In this work, I present altogether four publications: The first paper is concerned with the establishment of a correct mathematical model that not only allows to design the experimental set-up of any BBM92 realization, but also to calculate the optimal operation parameters once it is deployed. In the second paper, a high-brightness, high-fidelity source of polarization-entangled photon pairs is presented. Firstly, this source can be used for long-distance fiber links. Secondly, we show how it could provide as much as 1 Gbit/s secure key rate over shorter links, and identify today's single-photon detector performance as the bottleneck in present-day quantum key distribution. The third publication deals with the problem of chromatic dispersion, which is unique to fiber connections and smears out the single photon's temporal distribution. This in turn decreases the measurement fidelity. By exploiting the frequency-correlations of the entangled photon pairs, we manage to re-establish tight temporal correlations, making use of nonlocal dispersion compensation. Finally, the fourth publication combines all these findings to establish a two-channel link for polarization-entangled photon pairs crossing the Austrian-Slovakian border, thereby bridging 248 km of fiber and altogether 79 dB of loss. We operate this link for an exemplary time of 110 hours with a duty cycle of nearly 75%, where the other 25% are required for automatized nonlocal polarization drift compensation. During the on-time, we observe stable pair rates of  $9\text{ s}^{-1}$  and an average quantum bit error rate of 7%, resulting in a quantum secure key of altogether 403 kbit, created with a rate of 1.4 bits/s.





# Kurzfassung

Quantenschlüsselverteilung ist eine der ausgereiftesten Anwendungen der Quantenmechanik. Sie ermöglicht prinzipiell unknackbar verschlüsselte Kommunikation zwischen weit entfernten Partnern. Ihre Sicherheit basiert auf den Gesetzen der Physik und nicht auf unbewiesenen Vermutungen über das Ausmaß des Rechenaufwands für die Umkehrung gewisser mathematischer Probleme, wie es in derzeit verwendeten asymmetrischen Verschlüsselungsprotokollen der Fall ist. Eine notwendige Voraussetzung für die Realisierung von Quantenschlüsselverteilung ist das Versenden einzelner Quanten über große Distanzen. Diese wird am effizientesten durch die Verwendung von Einzelphotonen erreicht. Es gibt verschiedene Quantenschlüsselverteilungsprotokolle; verschränkungsbasierte Anwendungen wie das BBM92-Protokoll jedoch haben den Vorteil, dass sie gegen gewisse Attacken von vornherein immun sind. Für BBM92 erhalten die Kommunikationspartner Alice und Bob jeweils ein Photon eines verschränkten Photonenpaares und messen es in dem Freiheitsgrad, in dem es mit dem anderen verschränkt ist, z.B. in Polarisation. Durch den randomisierten Wechsel zwischen zwei voneinander unabhängigen Messbasen und das Vergleichen eines Teils der Messergebnisse können Alice und Bob feststellen, ob ein Lauschangriff durchgeführt wurde, der Information aus dem verschränkten Zustand extrahiert hätte. War dies nicht der Fall, sind einzig und allein die beiden im Besitz eines quantenzufälligen Bit-Strings, mit dem sie über jeden beliebigen Kanal völlig abhörsicher mittels symmetrischer Verschlüsselung kommunizieren können.

In dieser Dissertation zeige ich ein stabiles polarisationsbasiertes BBM92-Protokoll über 248 km verlegte Glasfaserkabel und die dazugehörigen Vorstudien. Auch wenn Freistrah-Quantenverbindungen via Satellit substantiell geringeren Transmissionsverlust aufweisen, haben Faserverbindungen doch den Vorteil, dass sie unabhängig von einer obstruktionsfreien Sichtverbindung operieren können. Das bedeutet, dass sie unterbrechungsfrei betrieben werden können, ohne durch Tageszeit, Wetter oder Satellitenposition eingeschränkt zu sein, was den erhöhten Verlust ausgleichen kann.

Es gibt etliche faserspezifische Herausforderungen bei BBM92, wobei starker Verlust, chromatische Dispersion und Polarisationsdrift die herausragendsten darstellen. In dieser Arbeit präsentiere ich insgesamt vier Publikationen: Die erste beschäftigt sich mit der Entwicklung eines mathematischen Modells, das es nicht nur erlaubt, jedwede BBM92-Realisierung zu planen, sondern auch deren optimale Betriebsparameter, sobald diese einsatzfähig ist. In der zweiten Publikation wird eine helle und zuverlässige Quelle polarisationsverschränkter Photonenpaare vorgestellt. Diese Quelle kann einerseits für Faserkanäle über lange Distanzen eingesetzt werden. Andererseits zeigen wir auch, wie sie über kürzere Faserstrecken bis zu 1 Gbit/s Schlüsselrate herstellen könnte, und identifizieren die Leistung heutiger Einzelphotonendetektoren als limitierenden Faktor für die Performance moderner Quantenschlüsselverteilung. In der dritten Publikation wird chromatische Dispersion behandelt, die einzig Faserverbindungen betrifft und das Ausschmieren der Photonen-Zeitverteilung bewirkt. Dies wiederum sorgt für verringerte Messqualität. Indem wir die Frequenzkorrelationen der verschränkten Photonen ausnutzen, stellen wir wieder scharfe Zeitverteilungen her und bedienen uns dabei nichtlokaler Dispersionskompensation. Die vierte Publikation schließlich behandelt die Herstellung einer Zweikanalverbindung für polarisationsverschränkte Photonenpaare, die die österreichisch-slowakische Grenze überquert und dabei insgesamt 248 km Faser und 79 dB Abschwächung überbrückt. Diese Verbindung betreiben wir für eine exemplarische Zeit von 110 Stunden mit fast 75% aktiver Einschaltzeit, wobei die restlichen 25% dazu verwendet werden, Polarisationsdrifts automatisiert und nichtlokal auszugleichen. Während der aktiven Zeit registrieren wir stabile Raten von 9 Photonenpaaren pro Sekunde mit einer durchschnittlichen Quantenbiterrate von 7%, was in einer Schlüsselrate von 1.4 bits/s und einem Gesamtschlüssel von 403 kbit resultiert.



# List of publications

## 1 Peer-reviewed

- **Sebastian Philipp Neumann**, Siddarth Koduru Joshi, Matthias Fink, Thomas Scheidl, Roland Blach, Carsten Scharlemann, Sameh Abouagaga, Daanish Bambery, Erik Kerstel, Mathieu Barthelemy and Rupert Ursin  
*Q<sup>3</sup>Sat: quantum communications uplink to a 3U CubeSat — feasibility & design*  
EPJ Quantum Technology 5, 4 (2018)
- **Sebastian Philipp Neumann**, Domenico Ribezzo, Martin Bohmann and Rupert Ursin  
*Experimentally optimizing QKD rates via nonlocal dispersion compensation*  
Quantum Science and Technology 6, 025017 (2021)  
(Section 3.3)
- Siddarth Koduru Joshi, Djeylan Aktas, Sören Wengerowsky, Martin Lončarić, **Sebastian Philipp Neumann**, Bo Liu, Thomas Scheidl, Guillermo Currás Lorenzo, Željko Samec, Laurent Kling, Alex Qiu, Mohsen Razavi, Mario Stipčević, John G. Rarity, Rupert Ursin  
*A trusted node-free eight-user metropolitan quantum communication network*  
Science Advances, Vol. 6, No. 36 (2020)
- **Sebastian Philipp Neumann**, Thomas Scheidl, Mirela Selimovic, Matej Pivoluska, Bo Liu, Martin Bohmann and Rupert Ursin  
*Model for optimizing quantum key distribution with continuous-wave pumped entangled-photon sources*  
Physical Review A 104, 022406 (2021)  
(Section 3.1)
- Elena Anisimova, Dmitri Nikulov, Simeng Simone Hu, Mark Bourgon, **Sebastian Philipp Neumann**, Rupert Ursin, Thomas Jennewein and Vadim Makarov  
*A low-noise single-photon detector for long-distance free-space quantum communication*  
EPJ Quantum Technology 8, 23 (2021)
- Zixin Huang, Siddarth Koduru Joshi, Djeylan Aktas, Cosmo Lupo, Armanda O. Quintavalle, Natarajan Venkatachalam, Sören Wengerowsky, Martin Lončarić, **Sebastian Philipp Neumann**, Bo Liu, Željko Samec, Laurent Kling, Mario Stipčević, Rupert Ursin and John G. Rarity  
*Experimental implementation of secure anonymous protocols on an eight-user quantum key distribution network*  
npj Quantum Information 8, 25 (2022)

## 2 Under peer-review

- Naomi R. Solomons, Alasdair I. Fletcher, Djeylan Aktas, Natarajan Venkatachalam, Sören Wengerowsky, Martin Lončarić, **Sebastian Philipp Neumann**, Bo Liu, Željko Samec, Mario Stipčević, Rupert Ursin, Stefano Pirandola, John G. Rarity, Siddarth Koduru Joshi  
*Scalable authentication and optimal flooding in a quantum network*  
arXiv:quant-ph 2101.12225  
Submitted April 4th 2021
- **Sebastian Philipp Neumann**, Mirela Selimovic, Martin Bohmann and Rupert Ursin  
*Experimental entanglement generation for quantum key distribution beyond 1 Gbit/s*  
arXiv:quant-ph 2107.07756v2 (2021)  
Submitted January 4th 2022  
(Section 3.2)
- Yoann Pelet, Ittoop Verghese Puthoor, Natarajan Venkatachalam, Sören Wengerowsky, Martin Lončarić, **Sebastian Philipp Neumann**, Bo Liu, Željko Samec, Mario Stipčević, Rupert Ursin, Erika Andersson, John G. Rarity, Djeylan Aktas, Siddarth Koduru Joshi  
*Unconditionally secure digital signatures implemented in an 8-user quantum network*  
arXiv:quant-ph 2202.04641v2  
Submitted 3rd April 2022
- Lukas Bulla, Matej Pivoluska, Kristian Hjorth, Oskar Kohut, Jan Lang, Sebastian Ecker, **Sebastian Philipp Neumann**, Julius Bittermann, Robert Kindler, Marcus Huber, Martin Bohmann and Rupert Ursin  
*Non-local temporal interferometry for robust and flexible quantum communication using high-dimensional entanglement over a 10 km free-space link*  
Submitted March 16th 2022
- **Sebastian Philipp Neumann**, Alexander Buchner, Lukas Bulla, Martin Bohmann and Rupert Ursin  
*Continuous entanglement distribution over a transnational 248 km fiber link*  
arXiv:quant-ph 2203.12417  
Submitted March 30th 2022  
(Section 3.4)

## 3 In preparation

- Julius Bittermann, Lukas Bulla, **Sebastian Philipp Neumann**, Sebastian Ecker, Martin Bohmann, Marcus Huber and Rupert Ursin  
*Photonic entanglement exposed to micro- and hypergravity during a zero-g flight*

# Contents

|  |            |
|--|------------|
| <b>Acknowledgments</b>   | <b>iii</b> |
| <b>Abstract</b>  | <b>v</b>   |
| <b>Kurzfassung</b>   | <b>vii</b> |
| <b>List of publications</b>  | <b>ix</b>  |
| 1 Peer-reviewed . . . . .  | ix         |
| 2 Under peer-review . . . . .  | x          |
| 3 In preparation . . . . .   | x          |
| <b>1 Introduction</b>  | <b>1</b>   |
| 1.1 One-time pad (OTP) . . . . .   | 1          |
| 1.2 Quantum entanglement . . . . .   | 2          |
| 1.3 Entanglement-based QKD: the BBM92 protocol . . . . .   | 4          |
| <b>2 Experimental entanglement-based QKD via deployed fiber</b>  | <b>7</b>   |
| 2.1 Past and present BBM92 implementations . . . . .   | 7          |
| 2.2 Advantages and challenges of this work's fiber-based BBM92 implementation . . . . .                          | 8          |
| 2.2.1 Fiber attenuation . . . . .  | 8          |
| 2.2.2 Chromatic dispersion . . . . .   | 8          |
| 2.2.3 Polarization drift . . . . .   | 9          |
| 2.2.4 Optimal operation parameters . . . . .   | 9          |
| <b>3 Publications</b>  | <b>11</b>  |
| 3.1 Model for optimizing quantum key distribution with continuous-wave pumped entangled-photon sources . . . . . | 12         |
| 3.2 Experimental entanglement generation for quantum key distribution beyond 1 Gbit/s . . . . .                  | 24         |
| 3.3 Experimentally optimizing QKD rates via nonlocal dispersion compensation . . . . .                           | 33         |
| 3.4 Continuous entanglement distribution over a transnational 248 km fiber link . . . . .                        | 44         |
| <b>Bibliography</b>  | <b>69</b>  |



# 1 Introduction

This introduction is meant to give a short overview of the fundamental techniques and principles the papers of this cumulative thesis are based on. It is meant to serve as an aid to contextualize these publications and, by introducing references to the most important literature in the field of entanglement-based quantum key distribution, embed the thesis in today’s science landscape. Due to the extensiveness of the ever growing field of experimental quantum optics, I will strictly limit myself to the concepts that my publications directly refer to. In Chapter 2, I will then go into more detail, describing the technical and experimental aspects of the thesis. There, I will highlight the interconnections and co-dependencies of my publications and outline the contributions of each paper to the main goal of this experimental thesis, namely the establishment of a real-world, long-distance, transnational and ultra-stable entanglement-based QKD connection over deployed fiber. Then, the scientific publications are printed in original in Chapter 3.

Quantum key distribution (QKD) is one of the most mature applications of quantum mechanics, exploiting quantum properties of single quanta to generate random, secret and therefore information-theoretically secure cryptographic keys. This is done by exploiting quantum effects to create so-called one-time pads, which I explain in the following section (1.1). Afterwards, I introduce the concept of quantum “entanglement”, along with two phenomena QKD relies on, namely the “no-cloning theorem” and “monogamy of entanglement” (section 1.2). Proceeding from these considerations, I lay out the BBM92 protocol, which was the basis of the experimental work this thesis presents (section 1.3).

## 1.1 One-time pad (OTP)

The promise of “information-theoretical security” means that there exist security proofs for QKD rather than assumptions about computational complexity, as is the case with currently used asymmetric encryption schemes, such as RSA. These schemes essentially rely on the *assumed* hardness of integer factorization [1]. Quantum cryptography, however, utilizes a symmetric encryption scheme called one-time pad (OTP), which is, in itself, completely classical. The idea behind OTP-based encryption has been patented nearly a hundred years ago [2] and is provably information-theoretically secure [3]. The scheme works as follows, assuming messages in binary code: Both receiver and sender (most commonly called Alice and Bob) own an identical secret, random and unique key of the same length as the message they want to transmit securely. Alice performs an XOR gate between this key and the message (see Table 1.1) and sends it to Bob, who performs the same operation with the encrypted message, thus recovering the original one.

|                    |   |          |   |   |     |
|--------------------|---|----------|---|---|-----|
|                    |   | Alice    |   |   | Bob |
| Clear-text message |   | $\oplus$ | { | 1 | 1   |
| Key                |   |          |   | 1 | 1   |
| Encrypted message  | = |          | } | 0 | 0   |
|                    |   |          |   | 0 | 0   |
|                    |   |          |   | 1 | 1   |
|                    |   |          |   | 1 | 1   |
|                    |   |          |   | 0 | 0   |
|                    |   |          |   | 0 | 0   |
|                    |   |          |   | 1 | 1   |
|                    |   |          |   | 0 | 0   |
|                    |   |          |   | 0 | 0   |
|                    |   |          |   | 1 | 1   |
|                    |   |          |   | 0 | 0   |
|                    |   |          |   | 0 | 0   |
|                    |   |          |   | 1 | 1   |
|                    |   |          |   | 0 | 0   |
|                    |   |          |   | 0 | 0   |
|                    |   |          |   | 1 | 1   |
|                    |   |          |   | 0 | 0   |
|                    |   |          |   | 0 | 0   |
|                    |   |          |   | 1 | 1   |
|                    |   |          |   | 0 | 0   |
|                    |   |          |   | 0 | 0   |
|                    |   |          |   | 1 | 1   |
|                    |   |          |   | 0 | 0   |
|                    |   |          |   | 0 | 0   |
|                    |   |          |   | 1 | 1   |
|                    |   |          |   | 0 | 0   |
|                    |   |          |   | 0 | 0   |
|                    |   |          |   | 1 | 1   |
|                    |   |          |   | 0 | 0   |
|                    |   |          |   | 0 | 0   |
|                    |   |          |   | 1 | 1   |
|                    |   |          |   | 0 | 0   |
|                    |   |          |   | 0 | 0   |
|                    |   |          |   | 1 | 1   |
|                    |   |          |   | 0 | 0   |
|                    |   |          |   | 0 | 0   |
|                    |   |          |   | 1 | 1   |
|                    |   |          |   | 0 | 0   |
|                    |   |          |   | 0 | 0   |
|                    |   |          |   | 1 | 1   |
|                    |   |          |   | 0 | 0   |
|                    |   |          |   | 0 | 0   |
|                    |   |          |   | 1 | 1   |
|                    |   |          |   | 0 | 0   |
|                    |   |          |   | 0 | 0   |
|                    |   |          |   | 1 | 1   |
|                    |   |          |   | 0 | 0   |
|                    |   |          |   | 0 | 0   |
|                    |   |          |   | 1 | 1   |
|                    |   |          |   | 0 | 0   |
|                    |   |          |   | 0 | 0   |
|                    |   |          |   | 1 | 1   |
|                    |   |          |   | 0 | 0   |
|                    |   |          |   | 0 | 0   |
|                    |   |          |   | 1 | 1   |
|                    |   |          |   | 0 | 0   |
|                    |   |          |   | 0 | 0   |
|                    |   |          |   | 1 | 1   |
|                    |   |          |   | 0 | 0   |
|                    |   |          |   | 0 | 0   |
|                    |   |          |   | 1 | 1   |
|                    |   |          |   | 0 | 0   |
|                    |   |          |   | 0 | 0   |
|                    |   |          |   | 1 | 1   |
|                    |   |          |   | 0 | 0   |
|                    |   |          |   | 0 | 0   |
|                    |   |          |   | 1 | 1   |
|                    |   |          |   | 0 | 0   |
|                    |   |          |   | 0 | 0   |
|                    |   |          |   | 1 | 1   |
|                    |   |          |   | 0 | 0   |
|                    |   |          |   | 0 | 0   |
|                    |   |          |   | 1 | 1   |
|                    |   |          |   | 0 | 0   |
|                    |   |          |   | 0 | 0   |
|                    |   |          |   | 1 | 1   |
|                    |   |          |   | 0 | 0   |
|                    |   |          |   | 0 | 0   |
|                    |   |          |   | 1 | 1   |
|                    |   |          |   | 0 | 0   |
|                    |   |          |   | 0 | 0   |
|                    |   |          |   | 1 | 1   |
|                    |   |          |   | 0 | 0   |
|                    |   |          |   | 0 | 0   |
|                    |   |          |   | 1 | 1   |
|                    |   |          |   | 0 | 0   |
|                    |   |          |   | 0 | 0   |
|                    |   |          |   | 1 | 1   |
|                    |   |          |   | 0 | 0   |
|                    |   |          |   | 0 | 0   |
|                    |   |          |   | 1 | 1   |
|                    |   |          |   |   |     |

## 1 Introduction

The encrypted message can be sent along arbitrary channels, even broadcast, since due to the key's randomness, there is no information about the initial message left in the encrypted one. This is, however, only true, if the following conditions are met:

1. The key must be *secret*, i.e. there should exist exactly two copies of it, one at Alice and one at Bob.
2. Its *length* must be the same as the message's.
3. The key must be truly *random*.
4. It is only to be *used once*.

Up until the invention of QKD, the only way to meet these conditions with certainty was to create a random key (e.g. via electrical noise), copy it and immediately hand it over to the two communicating partners, who could then, in the future, use it to exchange secure messages. Asymmetric encryption protocols on the other hand do not require the communication partners to ever meet, since the encrypting key can be broadcast publicly, while the decrypting key is owned by the receiver alone. This scheme is, despite its inferior security claim, much more practical than physically meeting to exchange an OTP, especially considering modern information and telecommunication technology.

QKD can, however, *remotely* establish keys usable as OTP, thus featuring *provable* security (which asymmetric protocols lack) between *distant* communication partners (which all early OTP realizations lack). Since the basic idea for QKD first appeared in the ground-breaking publication by Charles H. Bennett and Gilles Brassard in 1984 [4], there have been numerous different realizations of how to create such a quantum-secure key [5, 6, 7, 8, 9, 10, 11, 12, 13]. In the following, I will however restrict myself to the entanglement-based BBM92 protocol [14], which was the basis of the experiments conducted in the course of this thesis. To this end, I will first briefly introduce the concept of “entanglement”, together with the “no-cloning theorem” and “monogamy of entanglement”.

## 1.2 Quantum entanglement

Entanglement is a non-classical property of quantum states which was first described in 1935 in a gedankenexperiment by Albert Einstein, Boris Podolsky and Nathan Rosen [15]. There, they consider (w.l.o.g.) two particles whose spin directions are correlated by angular momentum conservation, i.e. their total spin should be 0. The particles' individual spins are, however, still undefined due to Heisenberg's uncertainty relation [16]. If one now measures the spin of one particle, the other particle has to instantaneously “know” the measurement outcome and itself take the correlated individual state, since it cannot violate momentum conservation. Assuming that this information has to be sent from one particle to the other instantaneously, no matter how far they are separated, this would violate the assumption that no physical system can travel faster than light. Einstein found these implications so bewildering that he famously called entanglement “spooky action at a distance” (“spukhafte Fernwirkung” [17]). He believed that quantum mechanics was correct, but incomplete, i.e., that there existed some yet to be discovered physical quantity (“hidden variables”) that in fact predetermined the measurement outcome and was an attribute of both particles, such that no information had to be exchanged between them when they were separated and measured. Nearly thirty years passed before John Stewart Bell proposed an experiment in 1964 that would allow to test whether such hidden variables did in fact exist [18]. To this end, he introduced the so-called “Bell inequality”, a violation of which proves that quantum correlations can be stronger than hidden variable theories would allow. This proposal, together with a variation of Bell's inequality more suitable for experiments [19], kicked off numerous experimental efforts to observe such “Bell violations”. From the first experiment in 1972 [20] on, every single test favored the quantum mechanical description. The experimental realizations became ever more stringent [21, 22, 23, 24, 25, 26, 27, 28], leaving less



and less so-called experimental “loopholes” for hidden-variable theories, until the first loophole-free Bell tests were realized in 2015 [29, 30, 31].

Note, however, that these results do not imply that superluminal communication is possible [32]. Simply speaking, this is because measurements on entangled particles do not allow to transmit any information: Since the measurement outcome is random, no “encoding” is possible and therefore, no information travels from one particle to the other.

All these experimental verifications imply that entanglement in fact allows for the distribution of particles which carry information about their *joint* state, but not about their *individual* ones. Mathematically speaking, this means that an entangled quantum state is not separable, i.e. it cannot be written as a product state of the individual particles; the simplest maximally entangled states are the so-called Bell states:

$$\begin{aligned}
 |\phi^+\rangle &= \frac{1}{\sqrt{2}} \left( |0\rangle_a |0\rangle_b + |1\rangle_a |1\rangle_b \right) \\
 |\phi^-\rangle &= \frac{1}{\sqrt{2}} \left( |0\rangle_a |0\rangle_b - |1\rangle_a |1\rangle_b \right) \\
 |\psi^+\rangle &= \frac{1}{\sqrt{2}} \left( |0\rangle_a |1\rangle_b + |1\rangle_a |0\rangle_b \right) \\
 |\psi^-\rangle &= \frac{1}{\sqrt{2}} \left( |0\rangle_a |1\rangle_b - |1\rangle_a |0\rangle_b \right),
 \end{aligned} \tag{1.1}$$

where  $|0\rangle$  and  $|1\rangle$  denote two orthogonal basis states spanning a Hilbert space with dimension 2, and  $a$  and  $b$  two (distinct) modes, in our case spatial modes referring to Alice and Bob. For a detailed discussion of the so-called “Bra-ket notation” used here, I refer the reader to introductory textbooks such as Ref. [33].

Since the entangled particles’ individual states are undefined due to the superpositions of Eq. 1.1, the outcome of a measurement of this state is completely *random* — but still *correlated* with the outcome of the other particle.

It follows that “shared randomness” between distant users is possible with the use of entanglement, i.e. condition 3 of the previous chapter can be met. Assuming that conditions 2 and 4 can be fulfilled trivially, there is only condition 1 left: The *secrecy* of the measurement outcomes.

In fact, there exist two quantum mechanical phenomena which can guarantee that the measurement outcomes at Alice and Bob aren’t only random, but cannot be known to anybody else in principle. The first one, the “no-cloning theorem”, is true for any single quantum state [34], entangled or not: A single quantum cannot be copied. An intuitive understanding of this effect can be given by using Heisenberg’s uncertainty relation: If one knows the quantum mechanical quantity of a state with sufficient precision — a necessary condition for copying —, this means that this quantity’s conjugate variable is undefined (to a certain degree). If one wants to copy the quantity *and* its conjugate and, in order to do so, determines it with sufficient precision, the first quantity becomes undefined again. Therefore, a single quantum can never be copied with full information (with the exception of eigenstates — however, with a single measurement, one cannot know with certainty whether a particle was in an eigenstate of the measurement basis). It follows that an eavesdropper (traditionally called “Eve”) cannot, in principle, intercept any particle sent between Alice and Bob, copy it to keep it for herself and forward a particle carrying identical information to the original receiver. In classical communications, this is perfectly possible, e.g. by tapping a wire.

The second quantum property needed to guarantee secrecy is called “monogamy of entanglement” [35]. It means that if two particles  $A$  and  $B$  are entangled, there exists a strict bound on the entanglement of these two particles with another particle  $C$  — in fact, if  $A$  and  $B$  are maximally entangled in a certain degree of freedom (e.g. polarization), they can share no entanglement in this degree of freedom with  $C$ . This means that if Alice and Bob each receive one particle of an entangled pair, they can be certain that there does not exist a third particle somewhere which could still

contain some information about the correlations they will observe when measuring their particles. This is, again, a fundamental difference to classical communication, where one can never know with certainty that there doesn't exist a third copy of the OTP in use.

The implications of above considerations for an OTP protocol are obvious: If randomness can secretly be shared between two distant communication partners, they can use it to create two random, but correlated and therefore identical bit strings which cannot be known by anybody else and use them as OTPs to transmit messages between them with unbreakable security. The following chapter is concerned with the actual implementation of such a QKD protocol.

### 1.3 Entanglement-based QKD: the BBM92 protocol

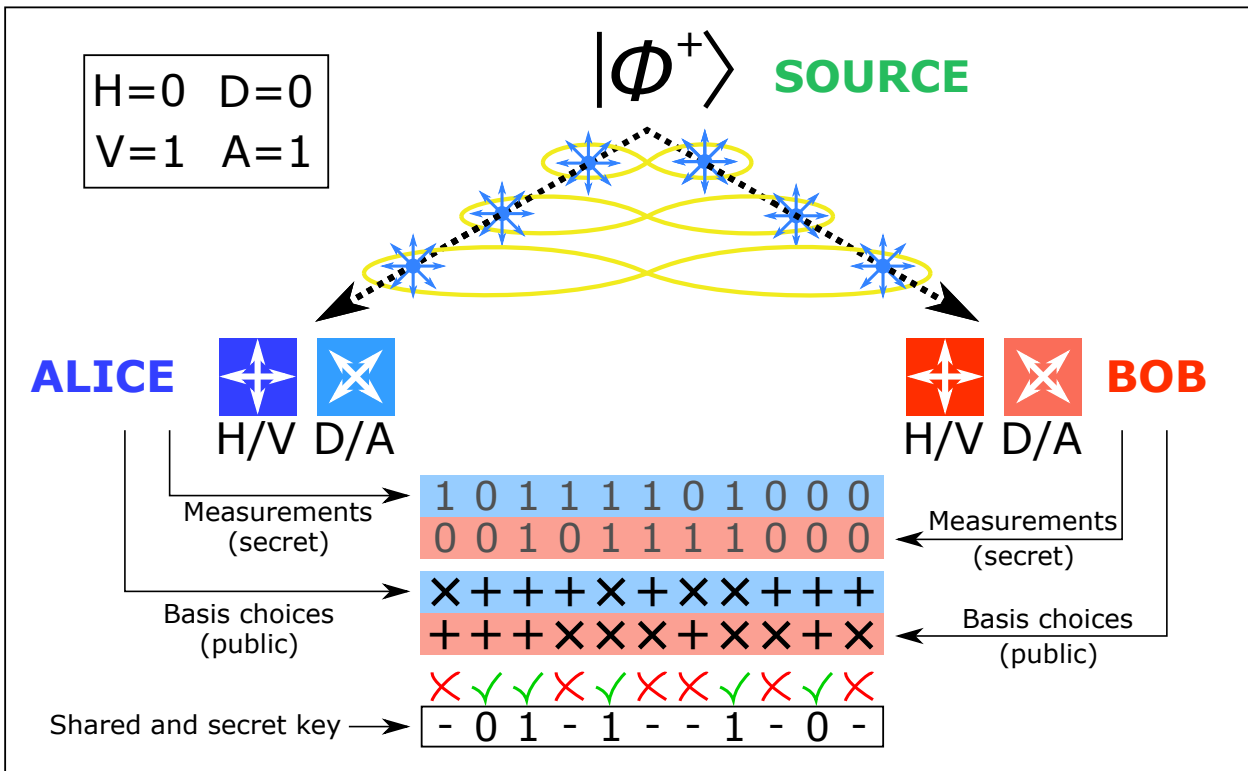


Figure 1.1: Working principle of the idealized BBM92 protocol. The source creates polarization-entangled photon pairs and sends them to Alice and Bob, respectively. They randomly choose one of two mutually unbiased bases per photon measurement (e.g.  $H/V$  or  $D/A$ ) and record both this choice and the measurement outcome. Afterwards, they publicly communicate their basis choices only. Since only those photon pairs measured in matching bases show a correlation, they discard all of their measurements performed in different bases and keep the others. The bits collected in identical bases can now be considered a quantum secure key.

Bennett, Brassard and N. David Mermin proposed an entanglement-based QKD protocol in 1992 [14] (in short: BBM92), which elaborated on the work by Artur Ekert from the previous year [5].

For the sake of comprehensibility, I will lay out the protocol in terms of photon pairs entangled in their polarization degree of freedom, as was the case for the experimental implementations in the course of this thesis.

The protocol works as follows (see also Fig. 1.1):

1. An EPR-source successively creates polarization-entangled photon pairs, e.g. in the state

$$\begin{aligned} |\phi^+\rangle &= \frac{1}{\sqrt{2}} \left( |H\rangle_a |H\rangle_b + |V\rangle_a |V\rangle_b \right) \\ &= \frac{1}{\sqrt{2}} \left( |D\rangle_a |D\rangle_b + |A\rangle_a |A\rangle_b \right) \end{aligned} \quad (1.2)$$

where  $H$  ( $V$ ,  $D$ ,  $A$ ) refers to horizontal (vertical, diagonal, antidiagonal) polarization and the subscripts  $a$  and  $b$  denote the recipients of the photons, Alice and Bob.

2. Alice and Bob measure the polarization state of the photons they receive. For each photon, they randomly choose one of two predefined, mutually unbiased measurement bases to measure in, e.g.,  $H/V$  and  $D/A$ .
3. Alice and Bob assign predefined bit values to each measurement outcome, e.g.  $H, D = 0$  and  $V, A = 1$ . They record these bit values and another bit for the measurement basis for each photon that reaches them and store these bit strings locally and secretly.
4. Once they have accumulated a certain amount of measurements (called the “raw key”), they publicly announce the measurement basis of each of their registered photons. Alice and Bob discard of all those measurements where they measured in different bases, which leaves them with the so-called “sifted key”.
5. They now compare the actual measurement values of a randomly chosen subset of their sifted key in order to assess the quantum bit error rate (QBER)  $E$ , i.e. the portion of correlations not in accordance with Eq. (1.2).
6. If  $E$  is above 11 %, Alice and Bob abort the protocol, since security cannot be guaranteed. If it is below this value, a secure key can be created, further using classical post-processing [36].
7. Post-processing consists of *a*) classical error correction [37] in order to arrive at perfectly identical keys, and *b*) privacy amplification to minimize any potentially leaked information to Eve [38]. Essentially, these two steps require low-density parity checks to correct erroneous bits, and large matrix multiplications to introduce “new” randomness to those bit values which might be in possession of Eve [39].
8. Once Alice and Bob have carried out above steps, they each possess identical, random and secret bit strings that they can use to encrypt messages of equal length with physical security.

The idea behind this protocol is the following: If Alice and Bob each receive one photon of an entangled pair, they will arrive at perfect correlations between their measurement outcomes if they choose to measure in the same basis. This can immediately be seen from Eq. (1.2): If the  $H/V$  basis is chosen, the first line of the equation has to be applied — a 50:50 chance to measure either  $HH$  or  $VV$ , but zero chance to measure  $HV$  or  $VH$ . The same is true for  $D/A$  (second line). If Alice and Bob however measure in different bases, their outcomes are maximally uncorrelated, since

$$\begin{aligned} |H\rangle &= \frac{1}{\sqrt{2}} \left( |D\rangle + |A\rangle \right), \\ |V\rangle &= \frac{1}{\sqrt{2}} \left( |D\rangle - |A\rangle \right), \\ |D\rangle &= \frac{1}{\sqrt{2}} \left( |H\rangle + |V\rangle \right), \\ |A\rangle &= \frac{1}{\sqrt{2}} \left( |H\rangle - |V\rangle \right). \end{aligned} \quad (1.3)$$

## 1 Introduction

Thus, assuming Alice's measurement yields  $H$ , one should expect Bob to measure  $H$  as well — but only if he measures in the  $H/V$  basis too. If  $D/A$  is chosen, however, there is an equal probability of measuring  $D$  and  $A$ . These uncorrelated measurements in the protocol is to force a possible eavesdropper, Eve, to reveal herself. This works as follows:

As we have already established in the previous section, Eve cannot create perfect copies of a photon she intercepts, and she also cannot entangle any other system with the pair shared between Alice and Bob. Let us now consider an attack Eve could carry out with perfect efficiency without being caught in a classical communication protocol: the so-called “intercept and resend” attack, where she reads out each bit value sent between Alice and Bob, writes it down, and sends on a copy of the same bit value. In BBM92 however, if Eve wants to listen in on the key exchange without Alice and Bob noticing, she has to decide for each single photon in which polarization basis she wants to measure it. Since she cannot know which basis the other recipient will choose, she must hope that she guessed the basis right and then sends a photon of the polarization she just measured (which is the best guess available to her) to its original recipient. (Note that for the following considerations, the cases where Alice and Bob choose different bases are irrelevant since they will never contribute to the key due to step 4 of the protocol.) Let us, without loss of generality, assume that Eve intercepts a photon traveling to Bob and that she measures it to be  $D$  polarized. In this case, she would write down the bit value 0 and send a  $D$  photon on to Bob. Now there are two scenarios: In the one favorable for Eve, Alice and Bob choose  $D/A$  too, they both get  $D$  as a result, Eve gains 1 bit of information and Alice and Bob will never know about it. In the other scenario however, Alice and Bob actually measure in  $H/V$ . Therefore, the  $D$  polarized photon Eve sends on to Bob will not be correlated with Alice's measurement any more. Still, in half of all cases, Bob's measurement outcome will be the same as Alice's just by chance, and no error is introduced. In the other half however, Bob will get a result uncorrelated with that of Alice, although they have measured in the same basis. This means that over many rounds, Eve will introduce an error of 25% in the correlations. Therefore, when Alice and Bob perform step 5, they will notice the high QBER and abort the protocol because they cannot exclude the existence of an eavesdropper in that case.

From above attack, it also becomes apparent why the basis choice at Alice and Bob has to be random: If there would be any preexisting or leaked information about the basis they will measure in, Eve could use this information to measure in the same basis as them, thus being able to completely recreate their correlations without being caught. Other attacks mostly focus on the actual experimental implementation [40, 41, 42, 43, 44].

Note that even if Eve *owns* the source of polarization-entangled photons, she will not be able to learn anything about the key: This is because no information stays behind at the source due to monogamy of entanglement. If Eve tries to avoid that by sending states that are not entangled, e.g. just  $HH$ , Alice and Bob will again notice that their correlations don't look as expected in both bases.

As a final remark, entanglement-based QKD implementations have an intrinsic advantage over prepare-and-measure protocols using faint light pulses. This is because the latter have a non-vanishing probability of producing more than one photon per pulse. Therefore, Eve can carry out a so-called photon number splitting (PNS) attack, where she keeps some photons of a pulse and forwards the others, thus in part avoiding the restrictions imposed on her by the no-cloning theorem. There is a scheme to avoid this problem, called decoy-state protocol [11], which, however, requires technically elaborate randomized attenuation of the faint pulses. Entanglement however intrinsically occurs in pairs of single photons, therefore PNS is fundamentally impossible for BBM92 [45].

Now that the basic concepts of QKD using entanglement have been introduced, the next chapter will be concerned with the actual experimental implementation of these concepts, the difficulties that have to be overcome and the contribution of my publications to this scientific problem.

## 2 Experimental entanglement-based QKD via deployed fiber

Since the first proof-of-principle QKD experiment over 30 cm in 1989 [46], there has been a plethora of experimental realizations and also protocols pushing the limits of QKD further; I will continue to focus on BBM92 for the sake of simplicity. In Section 2.1, I will give a short overview of history and status quo of experimental BBM92. Then, I will outline the concrete challenges of a long-distance fiber-based BBM92 implementation such as the one this thesis is concerned with, and how my publications have helped overcome them (Section 2.2). The subsequent Chapter 3 will then show my publications in the original.

### 2.1 Past and present BBM92 implementations

The experimental evolution of entanglement-based QKD such as BBM92 is naturally closely connected to that of entanglement distribution. The majority of early proof-of-principle papers focused on violating Bell inequalities rather than implementing a full BBM92 protocol, although the changes to the experiment would have been small (predominantly simply adapting the alignment of the measurement bases). Also, the entangled state's fidelity required for BBM92 is higher than the one needed to prove entanglement only. The minimum entanglement visibility  $V$  for BBM92 (relating to the QBER as  $V = 100\% - 2E$ ) is 78% [36], while a Bell violation is possible with  $V=71\%$  already [19]. However, most experiments, even when only concerned with proving entanglement, achieve visibilities  $> 80\%$ .

Entanglement was first proven to exist over distances now considered negligible [23]. The first efforts used free-space propagation of the photons due to the comparably low losses. In 1998, Weihs et al. showed such a link sending one photon of a pair over 400 m [47], and Aspelmeyer et al. were the first ones to implement a two-channel experiment of altogether 650 m length [48]. The single-channel distances were increased to 7.8 km [49] in 2005 and even 144 km [26] in 2007. The next huge step in free-space entanglement distribution was taken with the launch of the Chinese quantum satellite Micius in 2016, which established entanglement via a dual downlink over a distance of 1200 km in 2017 [50] and created a quantum-secure key with BBM92 over 1120 km in 2020 [51].

Efforts to implement fiber-based entanglement distribution started later because of the higher losses, chromatic dispersion and more difficult polarization control in fibers due to their inherent birefringence [52]. The latter was also the reason why the first in-fiber realizations mostly relied on time-bin entanglement, which is less influenced by temperature drifts and environmental circumstances: The first long-distance experiment in fiber was carried out by Tittel et al. in 1998 over altogether 17.4 km of deployed fiber in a two-channel configuration [24]. Since fiber spools can easily contain hundreds of kilometers of fiber, many proof-of-principle “long-distance” experiments used such coiled fibers inside the laboratory, e.g. over 100 km [53, 54] and 300 km [55]. Up to now, the longest fiber-based in-field entanglement distribution was carried out by Wengerowsky et al. over 96 km of deployed submarine fiber [56]. Additionally, they showed a 192 km link in a round-trip configuration where source and detectors were all located in close vicinity [57]. The latter two publications already focused on polarization-based BBM92, since it promises a higher key rate than time-bin QKD: In polarization, every time-bin can carry *two* bits (since each photon detection, i.e. each time-bin, carries a polarization bit rather than having to encode the bit values in (at least two) time bins themselves).

## 2.2 Advantages and challenges of this work’s fiber-based BBM92 implementation

Although losses in fibers are much higher than for free-space links, one main advantage of fiber-based QKD implementations is the fact that they can in principle run interruption-free. Free-space connections can so far only be operated at nighttime due to the absence of stray sunlight, and only if there’s neither rain nor fog. Efforts to increase the noise resistance of such connections, such as the ones shown in Ref.s [58, 59, 60] and the yet to be published work of Bulla et al. (cf. chapter ), are only now beginning to yield promising results, and in any case the key rates are substantially decreased in the presence of (sunlight) noise. Additionally, free-space satellite connections can only operate on time scales of less than 7 minutes every 1.5 hours [50], at least as long as the satellites are deployed in a low-earth orbit — higher orbits with longer overfly times or even geostationary satellites [61] however exhibit higher losses.

Fiber links do not suffer from above fundamental limitations. Nevertheless, they require several stabilization and compensation mechanisms and the mitigation of high losses. In the following, I will shortly outline the challenges one faces when trying to establish a long-distance polarization-based BBM92 experiment in fiber, and highlight how my publications have helped to study and overcome them.

### 2.2.1 Fiber attenuation

Firstly, as already mentioned, losses are much greater in fibers than via free-space connections. This is because especially in satellite configurations, the photons mainly travel in absorption- and scattering-free vacuum. Even when the photons hit the atmosphere, the absorption there is much lower than inside a glass fiber [62], at least when a suitable wavelength is chosen (e.g. in the near infrared). Therefore, the losses in free-space links mainly originate from beam divergence [63], which can in principle be mitigated by using larger telescopes. Even ultra-low-loss fibers however have an attenuation coefficient of at least 0.16 dB/km [64], and the most common G.652 fiber standard allows up to 0.35 dB/km of loss [65, 66]. A typical real-world attenuation coefficient is about 0.2 dB/km [67]. Therefore, it is essential to produce entangled photon pairs with high rates in order to arrive at non-negligible pair rates, i.e., a *high-brightness source* (developed in **publication 3.2**) is necessary. This, in turn, also requires detectors capable of temporally resolving photons potentially arriving in close succession, i.e., *low-jitter single-photon detectors* (which have been used in **publication 3.4**).

### 2.2.2 Chromatic dispersion

Chromatic dispersion (CD) along the fiber results in an effect very similar to that of a detector with high jitter. CD smears out the temporal distribution of the photon wave packets, depending on their spectral width. This means that the size of the time-bins needs to be increased, effectively making the “alphabet” shorter, i.e. less information can be gained in the same time span. This is obviously detrimental for the bit rate of time-bin protocols, but also for polarization-based BBM92, since also there, time bins are needed to identify photons of the same pair. This means that less photons can be sent per second when the bin size is enlarged. There is, however, a quantum mechanical method of compensating for CD called “nonlocal dispersion compensation” [68], which we deployed in our link implementation (**publication 3.4**) using a single *dispersion compensation module (DCM)* to compensate for CD in both fiber links. Additionally, as a pre-study to the actual link experiment, we analyzed the impact of different magnitudes of CD on the secure key rate in **publication 3.3**.

### 2.2.3 Polarization drift

Naturally occurring shifts in the fiber birefringence have a detrimental effect on the fidelity of polarization-entangled photon states [69]. One way to understand this is that any birefringence drift can be considered as a rotation of the measurement bases. If such a rotation happens, Alice’s and Bob’s bases do not match any more, and the strong quantum correlations of their measurements get lost. For time scales in the order of a few hours, this effect can be mitigated manually, e.g. by fiber polarization control paddles [56]. However, if stable and human-intervention-free operation of the link is required, one needs to deploy *automatized polarization-control* adjusting for polarization drift. There have been several efforts in this direction. One approach is to multiplex the quantum signal with a classical laser. This laser is then used to read out the change of the polarization state along the fiber and compensate for drifts accordingly [70, 71]. Another approach uses the QBER, i.e. the decrease in fidelity of the polarization state transmission, directly and corrects from there [72, 73]; note that in this case, the bits used for this QBER analysis cannot be used for key creation any more, since both bit *and* basis values have to be communicated via a classical channel. In **publication 3.4**, we show how such a QBER-based compensation scheme achieved an unprecedented stable operation time of more than 100 hours over a high-loss link.

Additionally, besides fiber drifts, any real-world source of entangled photon pairs exhibits intrinsic error, i.e. it produces a mixed rather than a pure entangled state. Since the QBER limit for key creation is 11%, it is of utmost importance that the pair creation device is not only a high-brightness, but also a *high-fidelity source* of entangled photons, which is presented in **publication 3.2**.

As a side remark, polarization-mode dispersion (PMD) did not pose a limiting factor in our experimental implementation. PMD is an effect in randomly birefringent media such as fibers, which causes polarization modes to travel with different speeds [74]. This can potentially harm the entangled state’s polarization fidelity [75, 76]. However, in our experiment (**publication 3.4**), PMD along the fibers is substantially smaller than the coherence time of our entangled photon pairs, and thus has no observable effect on their fidelity.

### 2.2.4 Optimal operation parameters

As already mentioned, the production rate of the source of entangled photon pairs has to be adjusted to the timing resolution of the single-photon detectors. This is because on one hand, the emission of two or more photon pairs within the timing resolution can lead to errors, since Alice and Bob might measure different pairs but have to assume that they are correlated, which they are not. Therefore, pair creation rates must be kept low to keep the temporal measurement fidelity high. On the other hand, it is obvious that pair creation rates that are too low will lead to less throughput and therefore less secure key. In order to obtain the optimal operation parameters for our experiment, we developed a mathematical model which includes link loss, detection efficiency, detector noise, timing jitter, CD and entangled-state fidelity to calculate the photon pair creation rate (or “brightness”) and the time-bin size (or “coincidence window”) yielding the maximum secure key rate. In **publication 3.1**, we present this model and data confirming the high accuracy of its predictions. We also show that Ref. [77], which was the only work modeling BBM92-based QKD up until then, is not applicable to photon sources with continuous-wave pump lasers such as the ones we used. Our model therefore was essential to design the final experiment presented in **publication 3.4**. Note that we had not yet developed the model when writing **publication 3.3**, where we use much more simple calculations to fit our data.





## 3 Publications

In the following, I present four of my publications contributing to the overarching research question of establishing a long-distance fiber-based quantum key distribution link with polarization-entangled photon pairs.






The order in which the publications are presented is not chronological with respect to their publication respectively submission. Instead, I start with “Model for optimizing quantum key distribution with continuous-wave pumped entangled-photon sources” (Section 3.1), since this paper explains the basic idea of entanglement-based quantum key distribution and develops a mathematical model to describe all necessary design and operation parameters for such an experiment. It is followed by a paper describing the sending apparatus of the BBM92 protocol, the source of polarization-entangled photon pairs, in detail and evaluating its performance (“Experimental entanglement generation for quantum key distribution beyond 1 Gbit/s”, Section 3.2). In the next paper, “Experimentally optimizing QKD rates via nonlocal dispersion compensation” (Section 3.3), one of the main problems in fiber-based quantum key distribution is assessed: chromatic dispersion. The publication shows the impact of chromatic dispersion on quantum secure key rates and offers nonlocal dispersion compensation as a solution, which is also quantified in terms of effectiveness. Finally, the main publication concludes this thesis: the paper “Continuous entanglement distribution over a transnational 248 km fibre link” (Section 3.4) reports on the establishment of a real-world BBM92 implementation running for 110 hours and crossing the border between Austria and Slovakia.

### **3.1 Model for optimizing quantum key distribution with continuous-wave pumped entangled-photon sources**

This publication explains how to operate and design a BBM92-implementation over long distances and produces the necessary mathematical tools for doing so. It was also used in publications 3.2 and 3.4 to assess the possible secure key rates for both link configurations. In publication 3.3, which was written earlier, we still use another, simplified model.

I contributed to the publication by developing the mathematical model with Thomas Scheidl and Bo Liu, by coding and plotting all simulations, by designing and constructing the source that was used to test the model experimentally, and by writing the publication with the help of Matej Pivoluska and Martin Bohmann.

## Model for optimizing quantum key distribution with continuous-wave pumped entangled-photon sources

Sebastian Philipp Neumann <sup>1,2,\*</sup> Thomas Scheidl<sup>1,2</sup> Mirela Selimovic <sup>1,2</sup> Matej Pivoluska <sup>1,3,4</sup> Bo Liu,<sup>5</sup>  
Martin Bohmann <sup>1,2</sup> and Rupert Ursin <sup>1,2,†</sup>

<sup>1</sup>*Institute for Quantum Optics and Quantum Information Vienna, Boltzmanngasse 3, 1090 Vienna, Austria*

<sup>2</sup>*Vienna Center for Quantum Science and Technology, Boltzmanngasse 5, 1090 Vienna, Austria*

<sup>3</sup>*Institute of Computer Science, Masaryk University, 602 00 Brno, Czech Republic*

<sup>4</sup>*Institute of Physics, Slovak Academy of Sciences, 845 11 Bratislava, Slovakia*

<sup>5</sup>*College of Advanced Interdisciplinary Studies, NUDT, Changsha 410073, People's Republic of China*



(Received 1 April 2021; accepted 14 July 2021; published 5 August 2021)

Quantum key distribution (QKD) allows unconditionally secure communication based on the laws of quantum mechanics rather than assumptions about computational hardness. Optimizing the operation parameters of a given QKD implementation is indispensable in order to achieve high secure key rates. So far, there exists no model that accurately describes entanglement-based QKD with continuous-wave pump lasers. We analyze the underlying mechanisms for QKD with temporally uniform pair-creation probabilities and develop a simple but accurate model to calculate optimal tradeoffs for maximal secure key rates. In particular, we find an optimization strategy of the source brightness for given losses and detection-time resolution. All experimental parameters utilized by the model can be inferred directly in standard QKD implementations, and no additional assessment of device performance is required. Comparison with experimental data shows the validity of our model. Our results yield a tool to determine optimal operation parameters for already existing QKD systems, to plan a full QKD implementation from scratch, and to determine fundamental key rate and distance limits of given connections.

DOI: [10.1103/PhysRevA.104.022406](https://doi.org/10.1103/PhysRevA.104.022406)

### I. INTRODUCTION

Quantum key distribution (QKD) is a method of creating a secret and random one-time pad for two remote users usable for unconditionally secure encryption of messages [1,2]. Since its first proposal in 1984 [3], intense research has pushed QKD ever closer to real-life realizations. It has been shown via free-space links on ground [4–6] and from space [7] as well as for long-distance fiber links [8] and in network configurations [9,10]. Many different schemes have been proposed in recent decades, such as entanglement-based protocols (E91 [11] and BBM92 [12]), and twin-field [13] and decoy-state prepare-and-send implementations [14]. Unlike prepare-and-measure protocols, entanglement-based applications have the advantage of being able to create their quantum states in a single coherent process based, for example, on spontaneous parametric down-conversion. Therefore, no quantum random number generators or other electronic inputs are required. Thus, provably no information about the individual photon state exists before the actual measurement. In

this sense, entanglement-based protocols exploit the quantum nature of the correlations necessary for QKD on the most fundamental level and can be extended to device-independent QKD [15]. QKD with entangled photons also allows quantum network configurations with many users using one and the same sending apparatus, an entangled-photon source (henceforth simply referred to as “source”) [10]. There are two fundamentally different ways to operate such a source: by creating the photon pairs with a continuous-wave (CW) or a pulsed pump laser. Up to now, no in-depth model exists for the prediction of key rates and the calculation of optimal source brightness for CW sources. A model describing sources pumped with a pulsed laser was published in 2007 [16] and has been the state of the art ever since. In such pulsed schemes, all photon pairs are found in discrete and evenly spaced time modes depending on the laser’s repetition rate. This rate can be tuned independently of the pulse intensity, allowing one to individually address photon creation rate and multipair emission. Due to the broad frequency spectra in a pulsed-pump scheme, dispersion effects in the optics have to be accounted for, especially in the nonlinear crystals where the entangled photons are created.

This model of pulsed operation can be applied to CW pumped sources with limited accuracy only, as will be shown below. CW pumping has several advantages compared to pulsed-pump schemes, especially in the context of fiber-based QKD: first, the spectrum of the down-converted photons is narrower, thus reducing dispersion effects in both source and transmission channels [17]. Second, additional high-precision

\*sebastian.neumann@oeaw.ac.at

†rupert.ursin@oeaw.ac.at

*Published by the American Physical Society under the terms of the Creative Commons Attribution 4.0 International license. Further distribution of this work must maintain attribution to the author(s) and the published article’s title, journal citation, and DOI.*

time synchronization is not needed as the temporal correlation peak can be precisely determined using a delay histogram. And third, damage to the source optics due to high-intensity pulses can be avoided.

In this paper, we present a model that accurately describes CW-pumped entanglement-based QKD systems. Importantly, all necessary inputs to the model can be read directly from experimentally available data, without the need of any additional assumptions. Our approach allows one to calculate optimal brightness values and coincidence window lengths as well as the resulting final key rate. Hence, the present results are of particular importance for state-of-the-art entanglement-based QKD applications. Comparison with experimental data demonstrates the validity of our model. Although we are focusing here on polarization-encoded BBM92 implementations, our approach can be extended to other degrees of freedom, which is, however, outside of the scope of this paper.

The paper is structured as follows: in Sec. II, we explain the basic working principle of polarization-encoded BBM92. We then develop our model in Sec. III by first introducing parameters for an idealized model (Sec. III A), modifying them to account for experimental imperfections (Sec. III B) and then combining them into the final model to calculate the expected secure key rates (Sec. III C). We optimize the key rate with regard to pair creation rate and temporal detection tolerance and compare our model with experimental data (Sec. IV). Concluding, in Sec. V we discuss our findings and present optimal parameters to maximize key rates.

## II. WORKING PRINCIPLE OF ENTANGLEMENT-BASED QKD

Entanglement-based QKD protocols such as BBM92 [12] rely on entanglement between distant physical systems, in our case specifically in the polarization degree of freedom of a photon pair. In an idealized scenario, one can create maximally entangled photon pairs which form a so-called Bell state, e.g.,

$$|\phi^+\rangle = \frac{1}{\sqrt{2}}(|H\rangle_A \otimes |H\rangle_B + |V\rangle_A \otimes |V\rangle_B), \quad (1)$$

where  $H$  ( $V$ ) denotes horizontal (vertical) polarization and the subscripts signify the recipient of the single photon traditionally called Alice (A) and Bob (B). We choose this state because of the fact that it is correlated in the mutually unbiased linear polarization bases  $HV$  and  $DA$  (diagonal and antidiagonal), where  $|D\rangle = \frac{1}{\sqrt{2}}(|H\rangle + |V\rangle)$  and  $|A\rangle = \frac{1}{\sqrt{2}}(|H\rangle - |V\rangle)$ . The following model can however be used for any Bell state, if the correlations are adapted accordingly.

Alice and Bob measure their photons randomly and independently from each other either in the  $HV$  or the  $DA$  basis. The basis choice can in practice be realized actively or passively. Actively means that Alice and Bob switch their measurement bases depending on the outputs of a quantum random number generator. A QKD implementation with passive basis choice uses probabilistic beamsplitters to direct the photons to either a  $HV$  or a  $DA$  measurement, both of which are realized simultaneously. In the course of the paper, we will assume active basis choice unless noted otherwise. In

any case, Alice and Bob record outcome ( $H$ ,  $D = 0$  and  $V$ ,  $A = 1$ ) and measurement basis for each event. By communicating about their measurement bases only, Alice and Bob can discard those recorded events where they measured in different bases and therefore see no correlation between their bit outcome (“sifting”). For the other events, they can expect perfect correlation, and thus use their sifted bit strings for key creation. By checking a randomly chosen subset of their sifted measurement outcomes to make sure that correlations have not degraded, Alice and Bob can rule out the existence of an eavesdropper.

In a real experiment, however, perfect Bell states such as in Eq. (1) do not exist. The polarization correlations are degraded through optical imperfections of the source and the detectors, which result in bit and/or phase flips. Also, in practice it is not possible to distinguish each and every consecutively emitted entangled pair from one another due to imperfections in temporal detection, as discussed below. We call such temporally irresolvable emissions “multipairs.”<sup>1</sup> Multipairs degrade the quantum correlations necessary to create a secure key, since detection of a multipair photon at Alice does not unambiguously herald the detection of its entangled—and therefore perfectly correlated—partner photon at Bob (and vice versa). Instead, with a certain probability, the photon is wrongly identified as being correlated with a photon from another pair, which leads to errors. Based on these considerations, in what follows, we will define the parameters necessary to calculate the performance of a CW-QKD system. All of these parameters can easily be obtained from experimental detection results, thus making our model ideally suited for direct implementation in real-world applications.

## III. MODELING QKD WITH CW-PUMPED SOURCES

For developing the model, we will start out with an idealized polarization-encoded CW-QKD protocol introducing the basic parameters (Sec. III A). In Sec. III B, we will extend this consideration by taking into account noise counts and multipair effects. We then use the experimental quantities defined in this way to calculate error rate and secure key rate (Sec. III C).

### A. Idealized CW-QKD system

The most general CW-pumped source setup uses a photon source creating an average number of entangled photon pairs per time unit. This quantity is called brightness  $B$ , for which we use the unit counts per second (cps) instead of hertz to emphasize the random nature of the emission process. We assume the probability of photon-pair creation to be uniformly distributed in time, as is justified in the case of CW pumping [18,19].

The entangled photons are spatially separated and sent to communication partners Alice and Bob, where they are detected with overall channel probabilities  $\eta_A$  and  $\eta_B$ , respectively. Although these probabilities are composed of the

<sup>1</sup>Unlike in pulsed-source BBM92 [16], coherent emission of  $n$ -pair states is negligible in the case of sources using CW pump lasers due to the photons’ temporal multimode character [18].

source's intrinsic heralding efficiency [20], the channel and coupling losses, the detection optics' transmission, and the detectors' dead times and efficiencies, we will consider each  $\eta_i$  as one single entity in the following calculations, sometimes referred to as system efficiency. This is because isolating individual loss effects is difficult in a real experiment and not required for our model.

As a result of these definitions, the average local photon detection rate of Alice and Bob, the so-called single counts, can be written, respectively, as

$$S_A^t = B\eta_A \text{ and } S_B^t = B\eta_B, \quad (2)$$

where we ignore noise counts for now. Note also that dead-time-induced losses, unlike other effects contributing to the  $\eta_i$ , are a function of detector count rates  $S_i^t$  and therefore of the brightness  $B$ , which has to be taken into account for low-loss scenarios (see Appendix B 1).

Naturally, two photons of a pair must be detected in order to observe their polarization correlation, i.e., use them for generating a cryptographic key. The rate of such two-photon events, which we call "true coincident counts" or "true coincidences,"<sup>2</sup> is given as

$$CC^t = B\eta_A\eta_B, \quad (3)$$

where we again preliminarily ignore noise counts. Using Eqs. (2) and (3), the  $\eta_i$  can be calculated as [20]

$$\eta_A = \frac{CC^t}{S_B^t} \text{ and } \eta_B = \frac{CC^t}{S_A^t}. \quad (4)$$

The  $\eta_i$  are sometimes also called "heralding efficiency," since they give the probability that the detection of one photon in one arm announces, or "heralds," the detection of a photon in the other arm. One can also define a total heralding efficiency  $\eta = \sqrt{\eta_A\eta_B}$ .

Imperfections of source, polarization compensation, and optical detection system lead to erroneous polarization measurement outcomes, i.e., two-photon events which do not comply with the expected Bell state. We call the probability of such an erroneous measurement  $e^{\text{pol}}$ . It consists of contributions of the individual polarization error probabilities  $e_A^{\text{pol}}$  and  $e_B^{\text{pol}}$  of Alice and Bob, respectively:

$$e^{\text{pol}} = e_A^{\text{pol}}(1 - e_B^{\text{pol}}) + e_B^{\text{pol}}(1 - e_A^{\text{pol}}). \quad (5)$$

It should be noted that measuring the wrong bit value at Alice *and* Bob still counts as a valid measurement, since it is impossible in principle for the experimenter to distinguish such an event from a correctly measured true coincidence. In most practical implementations, it is more convenient to read

$e^{\text{pol}}$  directly from the experimental data instead of quantifying the  $e_i$  individually (see Appendix A).

## B. Noise-afflicted CW-QKD system

In a real-world entanglement-based QKD implementation, the crucial source of error is not  $e^{\text{pol}}$ , which can be kept below 1% in modern applications [21], but the unavoidable registration of uncorrelated multipair photons which have lost their partner, and/or noise counts as coincidences. Such erroneous coincidences are called "accidental coincidence counts." To calculate the accidental coincidence rate for BBM92 with a CW pump, first one needs to modify Eq. (2) to account for dark counts  $DC_i$  in the detectors:

$$S_A^m = S_A^t + DC_A \text{ and } S_B^m = S_B^t + DC_B \quad (6)$$

where  $S_i^m$  are the actually measured count rates. Note that stray light, residual pump laser light, intrinsic detector dark counts, or any other clicks which do not originate from source photons all have the same effect for our purposes. Therefore, we include all such clicks in the  $DC_i$ . In a real experiment, Alice and Bob require at least two detectors each to be capable of distinguishing orthogonal quantum states. In Eq. (6), we assume that Alice and Bob each own identical detectors the photon and dark count rates of which can simply be added; for the case of nonidentical detectors and polarization dependent detection efficiency, see Appendix B 3.

Alice and Bob identify coincidences by looking for simultaneous detection times (accounting for a certain constant delay  $t_D$  caused by different photon travel times and electronic delays). There are three main effects that can degrade the fidelity of this identification: the detection system's finite timing precision, the coherence length of the photons, and chromatic dispersion effects in fiber, which delay photons of different wavelengths with respect to each other [17]. These effects cause a spread of the photons' temporal correlation function, the full width at half maximum (FWHM) of which we call  $t_\Delta$ . Because in any real experiment  $t_\Delta > 0$ , Alice and Bob need to define a so-called coincidence window  $t_{CC}$ . It can be understood as the temporal tolerance allowed for the difference in detection time of two correlated photons.

It follows that there is a possibility of confusing uncorrelated detector clicks with true coincidences. This possibility can be calculated, since it depends on  $t_{CC}$  and the  $S_i^m$ . Assuming independent Poissonian photon statistics at Alice and Bob, one can define the mean number of clicks at Alice and Bob, respectively, per coincidence window as

$$\mu_A^S = S_A^m t_{CC} \text{ and } \mu_B^S = S_B^m t_{CC}. \quad (7)$$

Most single-photon detectors used today are not photon-number resolving. Therefore, the chance of an accidental coincidence being registered can be approximated by the probability of *at least* one detection event taking place at each of them:

$$P^{\text{acc}} = (1 - e^{-\mu_A^S})(1 - e^{-\mu_B^S}), \quad (8)$$

where we use the fact that the click probability is given by  $(1 - e^{-\mu_i^S})$ ; see Refs. [22,23]. This expression for  $P^{\text{acc}}$  provides a good estimate for the accidental coincident-count probabilities in high-loss regimes. For low-loss scenarios it

<sup>2</sup>Please note that *true coincidences* are not a measurable quantity, since the experimenter cannot distinguish between a true or an accidental coincidence in principle. Even if an accidental coincidence does not conform to the expected correlations, it cannot be unambiguously identified as "accidental," since "true" coincidences can also be measured erroneously [see Eq. (5)]. Therefore, the notion of true pairs is solely a useful concept for our model, describing the photons that actually provide the nonclassical correlations necessary for QKD.

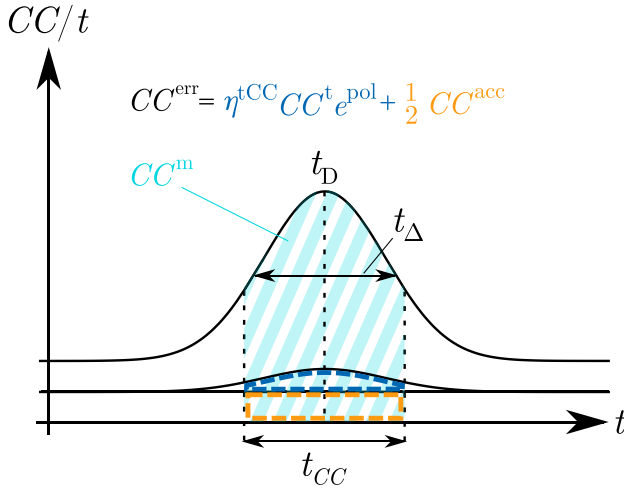


FIG. 1. Number of coincidences per time unit for different relative measurement times.  $t_D$  is the delay between Alice and Bob and  $t_\Delta$  is the FWHM of the temporal distribution, both of which are constant. The magnitude of the freely selectable coincidence window  $t_{CC}$  not only determines the number of total coincidences  $CC^m$ , but also the QBER  $E$ , i.e., the ratio of erroneous ( $\eta^{t_{CC}} CC^t e^{\text{pol}}$ ) plus half of all accidental ( $\frac{1}{2} CC^{\text{acc}}$ ) coincidence counts to  $CC^m$ .

needs to be adapted as it overestimates the probability of accidental coincidence counts by also counting true coincidences as accidental (see Appendix B 2). For  $\mu_i^S \ll 1$ , Eq. (8) can be simplified to

$$P^{\text{acc}} \approx \mu_A^S \mu_B^S. \quad (9)$$

The rate of accidental coincidences per second is therefore

$$CC^{\text{acc}} = \frac{P^{\text{acc}}}{t_{CC}} \approx \frac{\mu_A^S \mu_B^S}{t_{CC}} = S_A^m S_B^m t_{CC}. \quad (10)$$

Note that, since we assume *at least* one detector click per receiver for an accidental count to happen, we take into account the fact that in a real experiment with several detectors there can be more than one click per coincidence window (see Appendix B 2). In that case, a random bit value has to be assigned [24,25], which has the same error probability as an accidental count and can therefore be seen as a part of Eq. (10). Also note that  $CC^{\text{acc}}$  depends quadratically on  $B$ , but  $CC^t$  linearly. Thus, noise increases faster than the desired signal when increasing  $B$ , which gives an intuitive understanding why simply pumping the source with higher power can only enhance the key rate up to a certain degree (see Sec. IV).

It is not only accidental coincidences which depend on the choice of  $t_{CC}$ . If it is chosen in the order of the timing imprecision  $t_\Delta$ , true coincidences will be cut off and lost due to the Gaussian shape of the  $g^{(2)}$  intensity correlation with FWHM  $t_\Delta$  between Alice's and Bob's detectors (see Fig. 1).

This  $g^{(2)}$  function can be modeled as a normal distribution

$$j(t, t_\Delta, t_D) = \frac{2}{t_\Delta} \sqrt{\frac{\ln(2)}{\pi}} \exp\left[-\frac{4 \ln(2)}{t_\Delta^2} (t - t_D)^2\right] \quad (11)$$

with delay  $t_D$ .  $t_\Delta$  is the resulting timing imprecision between Alice's and Bob's measurements, i.e., it is the convolution of

detector jitter, chromatic dispersion, and coherence time of the photons at both Alice and Bob. To arrive at the loss which true coincidences suffer due to the coincidence window, one can carry out the integration

$$\eta^{t_{CC}} = \int_{-t_{CC}/2}^{t_{CC}/2} j(t, t_\Delta, t_D = 0) dt \quad (12)$$

$$= \text{erf}\left[\sqrt{\ln(2)} \frac{t_{CC}}{t_\Delta}\right]. \quad (13)$$

Here,  $\eta^{t_{CC}}$  is the proportion of true coincidences which fall into the chosen coincidence window  $t_{CC}$  and are thus identified as coincidences in the experiment. In this sense,  $\eta^{t_{CC}}$  can be interpreted as coincidence-window dependent detection efficiency. Now we can define the actually measured coincidences as

$$CC^m = \eta^{t_{CC}} CC^t + CC^{\text{acc}}. \quad (14)$$

This is the total number of detector events per second that Alice and Bob use to create their key. But obviously, a subset of these events occurring with rate  $CC^{\text{err}}$  actually does not show correlations in accordance with Eq. (1)—first, all those correlated photons which are measured erroneously; and second, on average half of all accidental coincidence counts:

$$CC^{\text{err}} = \eta^{t_{CC}} CC^t e^{\text{pol}} + \frac{1}{2} CC^{\text{acc}}. \quad (15)$$

### C. Error rate and secure key rate

From the quantities defined above, one can now calculate the quantum bit error rate (QBER  $E$ ), i.e., the ratio of erroneous coincidences to total coincidences:

$$E = \frac{CC^{\text{err}}}{CC^m} = \frac{\eta^{t_{CC}} CC^t e^{\text{pol}} + \frac{1}{2} CC^{\text{acc}}}{\eta^{t_{CC}} CC^t + CC^{\text{acc}}}. \quad (16)$$

As a side remark, the commonly used parameter “visibility”  $V$  relates to  $E$  as  $V = 1 - 2E$  [1]. Figure 1 shows a geometrical interpretation of Eq. (16). Coincidences correspond to different areas under the graphs, which are restricted by the chosen coincidence window. On one hand, it is desirable to increase the ratio of the light blue area to the combined dark blue and orange ones, which is equivalent to decreasing  $E$ . This can be done by decreasing  $t_{CC}$ , since the Gaussian-shaped  $CC^m$  (dark blue curve) scales more favorable in this case than the uniformly distributed accidental coincidence counts  $CC^{\text{acc}}$ . On the other hand, reducing  $t_{CC}$  means that  $\eta^{t_{CC}}$  reduces the total number of coincidences which can be used for key creation.

In order to evaluate the tradeoff between these two effects, we will analyze the secret key rate in the limit of infinitely many rounds—the so-called asymptotic key rate.<sup>3</sup> Alice and Bob choose randomly between measurement settings in the  $HV$  and  $DA$  bases. Let us denote the probability that Alice and Bob measure in the same basis as  $q$ . Only in this case, the polarization measurement outcomes at Alice and Bob are

<sup>3</sup>Where finite-key effects are of interest, one will have to take into account the total number of coincidences per block size and modify Eq. (17) accordingly. This might lead to different optimal experimental parameters satisfying Eq. (20). Nevertheless, the experimental parameter definitions of Sec. III B will be applicable also in this case.

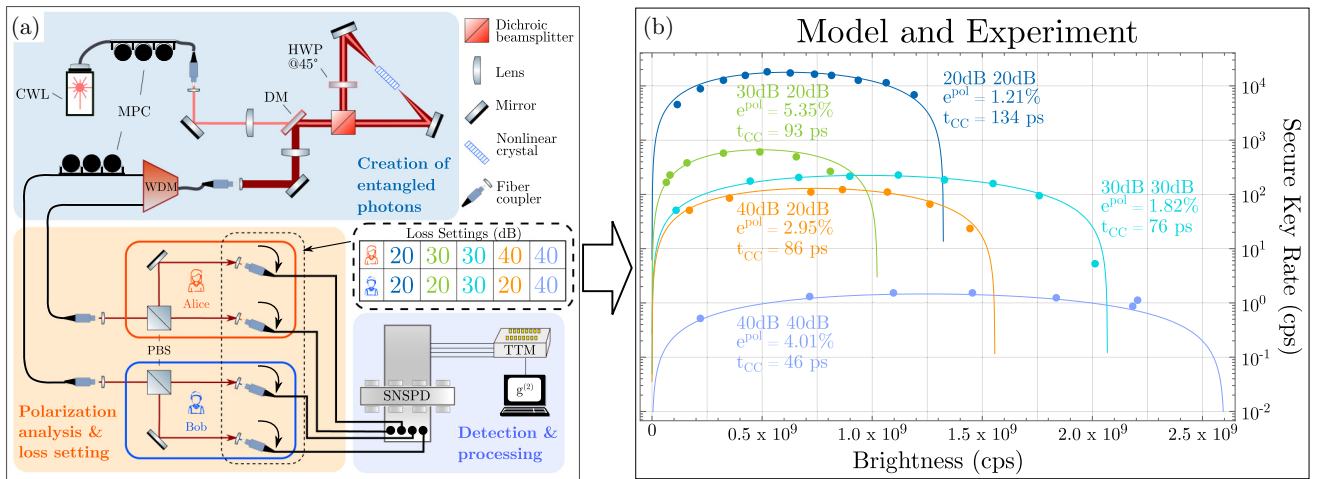


FIG. 2. (a) Setup used to create and detect polarization-entangled photon pairs for quantum key distribution. Top: A periodically poled lithium niobate nonlinear crystal is placed inside a Sagnac-type interferometer loop and pumped bidirectionally with a 775-nm continuous-wave laser (CWL). Via spontaneous parametric down-conversion (SPDC), it produces  $H$ -polarized photon pairs. The polarization of the counterclockwise pair is rotated to  $V$  via a half-wave plate (HWP) set to  $45^\circ$ . It interferes with the clockwise pair at the beamsplitter and is directed to a single-mode-fiber (SMF) coupler by use of a dichroic mirror (DM). An off-the-shelf wavelength division demultiplexer (WDM) separates the two photons and directs them to two polarization analyzing modules (bottom left). The manual polarization controller (MPC) in the pump fiber is used to set the photon pairs' Bell state of Eq. (1). The MPC in Alice's arm compensates for the random polarization rotation in Bob's arm in order to arrive at the desired correlations. Alice and Bob perform an orthogonal polarization state measurement on their photon using polarizing beamsplitters (PBS) the output modes of which are coupled into SMF and directed to superconducting nanowire single-photon detectors (SNSPD). Different loss scenarios are set by purposeful misalignment of the fiber couplers. Detection events of the SNSPD channels are recorded using a time-tagging module (TTM). From these tags, the  $g^{(2)}$  correlation function can be determined from delay histograms between the channels, and secure key rates can be calculated. (b) Comparison of our model (solid lines) and experimentally obtained data points (dots) for different loss settings and polarization measurement errors  $e^{\text{pol}}$ . SNSPD jitter values vary with count rate, which we account for in the model calculations by making  $t_{\Delta}$  a linear function of  $B$ . The data show that our model correctly predicts secure key rates over a wide range of losses, polarization errors, and brightness values.

correlated. All other coincidences have to be discarded. Therefore, the rate of coincidence rounds left for postprocessing is equal to  $qCC^m$ . Subsequently, Alice and Bob reveal a small fraction of measurement outcomes in both bases to estimate the error. Now we can finally evaluate the amount of achievable key per second as [16]

$$R^s = qCC^m[1 - f(E_{\text{bit}})H_2(E_{\text{bit}}) - H_2(E_{\text{ph}})], \quad (17)$$

where  $H_2$  is the binary entropy function defined as

$$H_2(x) = -x\log_2(x) - (1-x)\log_2(1-x). \quad (18)$$

$E_{\text{bit}}$  and  $E_{\text{ph}}$  are the bit and phase error rates, which are measurement-basis-dependent rates of measurement outcomes incompatible with the maximally entangled state described in Eq. (1).  $f(E_{\text{bit}})$  is the bidirectional error correction efficiency which takes into account how much of the key has to be sacrificed due to the fact that postprocessing is performed in finite blocks. In order to assess the validity of our model against an actual experiment, both the sifting rate  $q$  and efficiency  $f(E_{\text{bit}})$  need to be defined. We assume that the measurement settings of Alice and Bob are chosen uniformly, and thus  $q = 1/2$ . Further, we choose a realistic value of  $f(E_{\text{bit}}) = 1.1$  [26]. Finally, since in our model the noise parameters are independent of measurement settings, we can set  $E_{\text{bit}} = E_{\text{ph}} = E$ . With these choices, the key rate

formula becomes

$$R^s = \frac{1}{2}CC^m[1 - 2.1H_2(E)]. \quad (19)$$

From Eq. (19) follows immediately that there is a fundamental limit  $E_{\text{max}} \approx 0.102$ , above which no key creation is possible. In the following section we maximize  $R^s$  depending on the parameters discussed up to now. Importantly, all parameters used in this optimization can be directly determined in real-life experiments, which is explained in detail in Appendix A. Finally, note that the key rate formula can be adjusted using Eq. (17) to take into account measurement setting dependent losses as well; see Appendix B 4 for details.

#### IV. COMPARISON TO EXPERIMENTAL DATA

For realistic applications, the  $\eta_i$ , the optical error  $e^{\text{pol}}$ , the dark counts  $DC_i$ , and the temporal imprecision  $t_{\Delta}$  cannot be modified freely. Two important parameters however can be chosen by the experimenter: brightness  $B$  and coincidence window  $t_{\text{CC}}$ . The experimenter can vary  $B$  up to a certain level by changing the laser pump power in the source. With laser powers of many hundreds of milliwatts, brightness values of up to  $10^{10}$  cps are feasible with current state-of-the-art sources [21]. The coincidence window  $t_{\text{CC}}$  can in principle be chosen at will. It follows that for each QKD scenario there is an optimal choice of  $B$  and  $t_{\text{CC}}$  which maximizes  $R^s$  of Eq. (19). Figure 2 shows a comparison of our model and

experimental values, where  $t_{CC}$  has been numerically optimized for each curve with regard to the highest obtainable key rate and is then kept constant for every curve.

The data were collected using a Sagnac-type source of polarization-entangled photons in the telecom C band. For a detailed description of such a source's working principle, we refer the reader to Ref. [21]. After passing wavelength division multiplexing (WDM) filters of 18.4-nm FWHM centered about 1531 and 1571 nm, the photons impinge on single-photon superconducting nanowire detectors (SNSPDs) of the Single Quantum Eos series with detection efficiencies of 80% and dead times as low as 40 ns according to the manufacturer. The detectors were connected to the time tagging module (TTM) Ultra 8 by Swabian Instruments. To keep the analysis of the model simple, we measured only in one superposition basis. Losses were introduced by controlled misalignment of the single-mode-fiber (SMF) couplers. All experimental parameters were determined by using count rates, coincidence rates, and temporal histograms of the single-photon detections only, with no need of additional "external" characterization (see Appendix A). Since the timing jitter of nanowire detectors strongly depends on the count rates they measure, linear fits of the jitter change depending on brightness have been included in the model.

The data show excellent agreement with our model's predictions. The losses introduced in the measurements range from 40 to 80 dB in total, with different distributions along the channels. Note that the two loss scenarios with equal total loss of 60 dB (orange and turquoise curve) perform very differently. Assuming  $DC_A = DC_B$ ,<sup>4</sup> symmetric loss is preferable to asymmetric loss because the probability of a partnerless photon matching with a dark count is reduced in this case. In Fig. 2, this effect on the two 60-dB curves is, however, exaggerated due to different polarization errors  $e^{pol}$ , which we set via a manual polarization controller (MPC) to show the model's validity for different parameter regions. The total losses are equivalent to in-fiber distances between 200 and 400 km. Nevertheless, our model can be applied to all kinds of quantum channels, including, e.g., free-space satellite connections, where variation of the channel attenuation [27,28] can be integrated in our model in a straightforward manner.

We want to emphasize that in any case our optimization strategy works exclusively with experimentally measurable quantities that can be inferred directly from the actual QKD implementation (see Appendix A). Furthermore, the presented model can be used during the planning phase of an experiment to devise optimal working parameters based on specification sheets. While several calculations are approximated in our model, it shows excellent agreement with the experimental data. This is proof of its usefulness in a wide range of experimental parameters. For a more extensive treatment of phenomena that might become necessary in certain parameter

<sup>4</sup>If  $DC_A$  and  $DC_B$  differ strongly, loss asymmetry can actually be beneficial. In a simplified view, this is because higher dark count rates matter less when occurring at detectors with higher single count rates. However, since in most scenarios neither loss nor dark counts can be chosen freely, we omit an in-depth discussion of this effect.

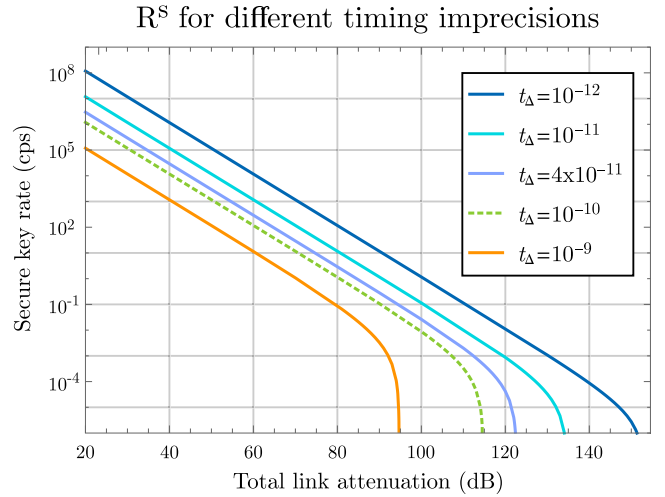


FIG. 3. Key rate  $R^s$  vs total symmetric link loss  $\eta_A\eta_B$  for different timing imprecision values  $t_\Delta$ . Brightness  $B$  and coincidence window  $t_{CC}$  have been optimized for every point of every curve. Dark counts  $DC_A = DC_B = 250$  cps are kept constant for each of the four detectors per communication partner. Also polarization error  $e^{pol} = 1\%$  is constant for all curves. Lower  $t_\Delta$  allows both for higher key rates and longer maximum distance, since  $CC^{acc}$ , the main source of errors, is directly proportional to  $t_\Delta$ . Note that the dotted green curve ( $t_\Delta = 10^{-10}$  ps) is the same curve as the equally colored one in Fig. 4.

regimes, such as dead-time effects, low-loss channels, and nonidentical detectors, we refer the reader to Appendix B.

## V. OPTIMIZATION OF QKD WITH A CW-PUMPED SOURCE

Now that we have shown the validity of our model in different parameter scenarios, we want to use it to illustrate the limits and potential of CW-QKD. Therefore, we numerically maximize both  $B$  and  $t_{CC}$  for every point on the curves in Figs. 3 and 4, i.e.,

$$\frac{\partial}{\partial B} \frac{\partial}{\partial t_{CC}} R^s(B, t_{CC}; \eta_i, e^{pol}, DC_i, t_\Delta) = 0 \quad (20)$$

is fulfilled continuously. Figure 3 shows the maximum obtainable key rate assuming symmetric loss for different jitter values. Lower jitter allows for a smaller coincidence window, which in turn allows for higher brightness values and thus key rates. Note that no matter the jitter value there is an abrupt drop to zero key after a certain amount of loss. This is because dark counts will inevitably induce a minimum accidental coincidence count value  $CC_{min}^{acc} = DC_A DC_B t_{CC}$ . In a regime of high loss, this constant value can mask true coincidences if  $\eta^{t_{CC}} CC^t \lesssim 10 CC_{min}^{acc}$ . In this case, key creation is frustrated. Figure 4 now shows how  $CC_{min}^{acc}$  is reduced with lower dark count values. For the hypothetical case of  $DC_i = 0$ , the accidental coincidences  $CC^{acc}$  can be decreased to arbitrarily low values by reducing the brightness  $B$ . Although this also decreases maximum key rates beyond the point of usefulness, they never drop to zero, as indicated by the dark blue curve. When comparing Figs. 3 and 4, it becomes apparent that in a real-world scenario reducing the timing imprecision  $t_\Delta$  is



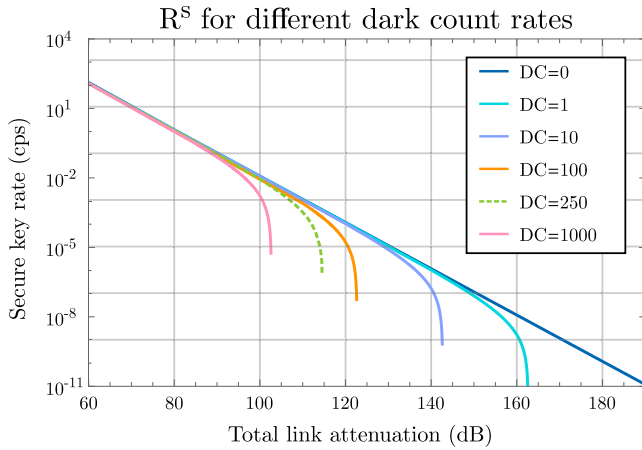


FIG. 4. Key rate  $R^s$  vs total symmetric link loss  $\eta_A\eta_B$  for different dark count rates DC per detector and four detectors per communication partner. The timing imprecision  $t_\Delta$  is kept constant at 100 ps and the polarization error at  $e^{\text{pol}} = 1\%$ . As can clearly be seen, reducing detector noise counts effectively only increases the maximum achievable distance. In the case of no dark counts (dark blue curve), there exists no distance limit, since  $t_{\text{CC}}$  can in principle be set arbitrarily small, thus keeping the error rate below  $E_{\text{max}}$  for any loss. Note that the dotted green curve (DC = 250) is the same curve as the equally colored one in Fig. 3.

more important than reducing the dark counts. This is because lower  $\text{DC}_i$  can only increase the maximum distance in high-loss regimes, where key rates are extremely low already. To increase the key rate for a given loss, it is more favorable to lower  $t_\Delta$  in most cases.

We would also like to emphasize that when wrongly using the model for pulsed-source BBM92 by Ma *et al.* [16] to estimate key rates for a CW-pumped implementation one arrives at erroneous results, even when trying to adapt it. One could try to do so by replacing the mean photon number per pulse  $2\lambda$  with the average photon number per coincidence window

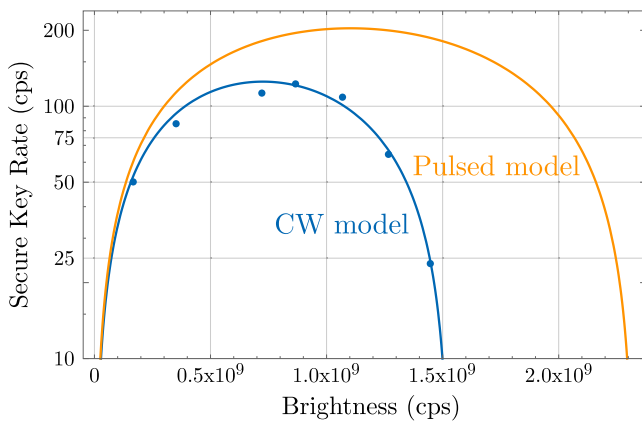


FIG. 5. Comparison of 40- and 20-dB experimental data with the secure key predicted by our model (blue line) vs an adapted version of the pulsed-source model from Ref. [16] (orange line). Since temporal detection imprecision does not enter the pulsed-source model, it overestimates both the maximum key rate and the optimal brightness value.

$\mu = Bt_{\text{CC}}$  and changing the multipair probability of Eq. (5) in Ref. [16] to a Poissonian distribution. Since doing so ignores any effects of temporal uncertainty, the results differ strongly, as can be seen in Fig. 5.

## VI. CONCLUSION

In this paper, we have presented a comprehensive and accurate model of continuous-wave entanglement-based quantum key distribution. Our model allows one to estimate and optimize the performance of any given CW-QKD system by extracting experimental parameters from the recorded detections only, without the need to perform any additional characterization of the experiment. It also allows one to compare different devices and find the optimal solution for a given quantum link. For a given QKD setup, the model can accurately estimate the optimal settings of brightness and coincidence window to extract the maximal possible key and thus enhance the performance of the implementation. Furthermore, the presented approach is readily extendable to BBM92 based on entanglement in other degrees of freedom. We are confident that our easy-to-implement model will be used as an important design and optimization tool for CW-QKD links.

## ACKNOWLEDGMENTS

We acknowledge European Union's Horizon 2020 program Grant No. 857156 (OpenQKD) and the Austrian Academy of Sciences. M.P. additionally acknowledges the support of VEGA Project No. 2/0136/19 and GAMU Project No. MUNI/G/1596/2019. B.L. acknowledges support of the National Natural Science Foundation of China under Grant No. 61972410 and the Research Plan of National University of Defense Technology under Grant No. ZK19-13.

## APPENDIX A: PARAMETER ESTIMATION

There are numerous ways to estimate the parameters discussed in this paper. When planning a QKD link from scratch, one has to rely on data sheets and fiber loss measurements. However, one can also estimate all parameters with the same QKD equipment used for the experiment, if already available.

Directly accessible parameters for the experimenter are  $t_{\text{CC}}$  (since it is a free variable to be chosen by the experimenter),  $S_i^m$ , and  $\text{CC}^m$ . The delay  $t_D$  between Alice's and Bob's detection times can be found out by calculating a delay histogram of single counts at Alice and Bob and determining the location of the histogram peak (see Fig. 6). From the same histogram, the (total) timing imprecision  $t_\Delta$  can be read from the peak's FWHM (less  $\text{CC}^{\text{acc}}$ ). It should be mentioned that SNSPD jitter depends on both the detector's bias current and its count rate, and exhibits the lowest specified values for high current and low count rates only. This dependency has been included in the model of Fig. 2 by using a linear fit of  $t_\Delta$  vs  $B$  rather than a constant jitter value.

The dark counts  $\text{DC}_i$  can be determined by blocking the source of photons and observing the  $S_i^m$ , which are equal to the  $\text{DC}_i$  for  $B = 0$  [see Eqs. (2) and (6)]. Note however that stray light from the pump beam cannot be observed with this method. To do so, one either needs filters that block just

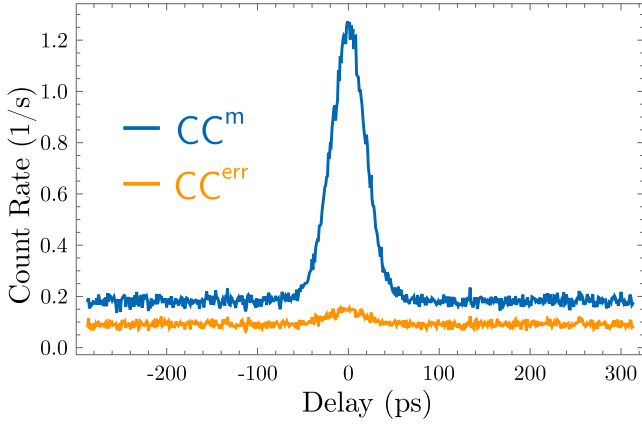


FIG. 6. Measured  $g^{(2)}$  correlation histogram for the 40- and 40-dB loss setting.  $CC^m$  contains all measured counts for all possible channel combinations, where all histograms have been shifted by their respective delays  $t_D$ .  $CC^{err}$  only shows undesired correlations, i.e., between polarization measurements not in accordance with Eq. (1). The orange curve's small peak around zero corresponds to erroneous polarization measurements, while the noise floor is equivalent to accidental coincidence counts  $CC^{acc}$  (see Fig. 1).

the SPDC wavelength, or the possibility to frustrate SPDC without blocking or misdirecting the laser, e.g., by changing the crystal temperature. Especially for long-distance single-mode-fiber links designed for the SPDC wavelength, it is safe to assume that pump light is sufficiently suppressed at the detectors.

For the following calculations, it is necessary to determine  $CC^t$  (for a certain brightness). Especially in the case of low loss and low jitter, this can be done experimentally by lowering the brightness to a value where  $CC^{acc} \rightarrow 0$  and therefore  $CC^m \rightarrow CC^t$ . Alternatively,  $CC^{acc}$  can be subtracted from  $CC^m$ : either by calculation using Eq. (10) or experimentally by changing  $t_D$  to a value far from the actual coincidence peak, while keeping  $t_{CC}$  constant. In absence of  $CC^t$ , the measured  $CC^m$  become equal to  $CC^{acc}$ . For all these approaches, it is important to choose  $t_{CC}$  large enough such that  $\eta^{t_{CC}} \rightarrow 1$ ; as a rule of thumb,  $t_{CC} = 3t_\Delta$  is sufficient.

Now to determine the optical error  $e^{pol}$ , one can use the methods just described to eliminate  $CC^{acc}$  in Eq. (16) such that  $E \approx e^{pol}$ .

The heralding efficiencies or transmission factors  $\eta_i$  can be calculated using Eq. (4), where again  $CC^t$  and  $S_i^t$  have to be determined in advance by subtracting  $CC^{acc}$  and  $DC_i$ .

Finally, also the brightness  $B$  can be calculated using  $CC^t$  and  $S_i^t$  via

$$B = \frac{S_A^t S_B^t}{CC^t}. \quad (A1)$$

Note that for this calculation of the  $\eta_i$  and  $B$ , dead-time effects have not been taken into account. Thus, even if the  $CC^{acc}$  are simply measured and subtracted, one should take care to operate the source at sufficiently low pump power (see Appendix B 1).

If it should be necessary to incorporate dead-time effects, the most efficient way to determine  $t_\dagger$  is to calculate an auto-correlation histogram in time of each detector channel while

subjecting it to photons with Poissonian emission statistics. The temporal stretch for which no correlations are found is the detector channel's dead time.

## APPENDIX B: ADDITIONAL CORRECTIONS

### 1. Dead-time loss

In scenarios with high detector count rates, an additional loss factor might be considered to account for the detectors' dead time  $t_\dagger$  [29]:

$$\eta_i^{t_\dagger} = \frac{1}{1 + B\eta_i t_\dagger / d}. \quad (B1)$$

Here  $d$  is the number of (identical, see Appendix B 3) detectors deployed per communication partner. This effective loss cannot simply be considered as a constant contribution to  $\eta_i$ , since it is a function of  $S_i^m$  and therefore  $B$ . For  $B\eta_i t_\dagger / d < 0.02$ ,  $\eta_i^{t_\dagger} \approx 1$  holds. Note that the estimation of  $B$  can be compromised if this assumption is not justified due to low loss, high brightness, and/or long detector dead time.

Another result of dead-time loss is that the definition of the  $\mu_i^S$  in Eq. (7) needs to be modified, since photons arriving at the detectors during the dead time do not contribute to  $S_i^m$ . One therefore needs to modify the  $CC^{acc}$  in Eq. (10) to

$$CC_{t_\dagger}^{acc} \approx \frac{S_A^m S_B^m t_{CC}}{\eta_A \eta_B} \quad (B2)$$

where we assume  $DC_i \ll S_i^t \eta_i$ , which is reasonable in the high single-count regimes where dead-time effects become important.

### 2. Accidental coincidence probability

Equation (8) slightly overestimates the probability of accidental coincidence counts. Since it assumes completely independent photon statistics at Alice and Bob, *any* photon contributes to  $CC^{acc}$ , regardless of whether it has lost its partner or not. Thus, here we want to give a more extensive description  $P_{ext}^{acc}$ , which is well approximated by  $P^{acc}$  in Eq. (9) for  $\eta_i \ll 1$ . We start by defining the probability of a coincidence happening per coincidence window,  $P^{CC'}$ :

$$\begin{aligned} P^{CC'} &= \sum_{n=1}^{\infty} e^{-\mu} \frac{\mu^n}{n!} \sum_{i=1}^n \left[ [(1 - \eta_A)^{i-1} (1 - \eta_B)^{i-1} \eta_A \eta_B] \right. \\ &\quad \times \left(1 - \frac{\eta_A}{2}\right)^{n-i} \left(1 - \frac{\eta_B}{2}\right)^{n-i} \\ &\quad \left. \times \left(1 - \frac{P_A^{DC}}{2}\right) \left(1 - \frac{P_B^{DC}}{2}\right) \right] \end{aligned} \quad (B3)$$

where  $\mu = Bt_{CC}$  is the average number of photon pairs created per coincidence window before any loss, and  $P_i^{DC} = DC_i t_{CC}$  are the probabilities of a noise count happening at Alice and Bob, respectively, per coincidence window. This formula takes into account the Poissonian emission and dark count statistics. Multipair emissions can still yield a valid measurement if photons get lost in a way that two correlated photons end up at the detectors before all others (first factor inside the square brackets). However, if photons emitted after the

true pair, but inside the coincidence window, are detected as well, they can in some cases eliminate a true coincidence (second line). The divisions by 2 come from the fact that if the later photon detection occurs in the same detector as the true photon detections this case cannot be distinguished from a true coincidence. If it clicks in the other detector, a random bit value has to be assigned, i.e., only this case has to be counted as an accidental. Dark counts can also occur in the presence

$$P_{\text{cor}}^{\text{acc}} = 1 - e^{-\mu} [1 - P_A^{\text{DC}} P_B^{\text{DC}}] - P^{\text{CC}'} - \sum_{n=1}^{\infty} e^{-\mu} \frac{\mu^n}{n!} [(1 - \eta_A)^n + (1 - \eta_B)^n - (1 - \eta_A)^n (1 - \eta_B)^n - (1 - \eta_A)^n [1 - (1 - \eta_B)^n] P_A^{\text{DC}} - [1 - (1 - \eta_A)^n] (1 - \eta_B)^n P_B^{\text{DC}} - (1 - \eta_A)^n (1 - \eta_B)^n P_A^{\text{DC}} P_B^{\text{DC}}]. \quad (\text{B4})$$

The formula can be understood as follows: The accidental coincidence probability  $P_{\text{cor}}^{\text{acc}}$  can be seen as all those two-click events that did not originate from a true pair. We proceed by subtracting from probability 1 all events which are no accidental coincidences.

Thus, in the first line, we subtract the probability of no photon pair being emitted, corrected by the case of two dark counts producing a coincidence. We also subtract all correct coincidences according to Eq. (B3). Then we subtract the sum over all remaining pair emission probabilities which are not the vacuum state, not a true coincidence, and not an accidental count. In the second line, we count those cases where no accidental coincidence happens since in at least one arm no click occurs. Since the possibility of both detectors not clicking is included in both  $(1 - \eta_A)^n$  and  $(1 - \eta_B)^n$ , it has to be subtracted. This subtraction avoids mistakenly counting the case of all photons lost twice.

In lines 3 and 4 of Eq. (B4), we have to re-add the cases where dark counts cause an accidental coincidence by “replacing” a photon. All other dark count cases are already included in the first line of the equation—either as part of  $P^{\text{CC}'}$  or in 1, since a dark count happening when an accidental coincidence would have occurred anyway does not change their statistics.

For  $\eta_i \ll 1$ , one can approximate  $P_{\text{cor}}^{\text{acc}}$  with  $P^{\text{acc}}$  from Eq. (9), which actually constitutes an upper bound for Eq. (8).

### 3. Nonidentical detectors

In our model, we assume Alice and Bob, respectively, to use identical detectors for their orthogonal polarization measurements. It has recently been shown [30] that vast differences in detector performance do not necessarily degrade the security of a QKD protocol. However, different detection efficiencies lead to asymmetric single-count rates and therefore different accidental coincidence rates for different polarization correlations. On top of this, different detector jitters lead to different  $\eta^{\text{tcc}}$  for each correlation. These asymmetries and differences of used detectors can lead to a deviation from the reported model.

To account for such imbalances one has to define two heralding efficiencies per communication partner, which we denote by  $\eta_{Aj}$  and  $\eta_{Bk}$ , where  $j$  and  $k$  indicate the detectors. Following Eq. (3), one can now differentiate true coincidence

of a true pair, eliminating a valid coincidence in the same way as photons arriving later, which gives rise to the factors in the third line. As a side remark, in the case of passive basis choice using beamsplitters, there are four instead of two detectors deployed; accordingly, the factor 1/2 has to be replaced by 3/4.

Using  $P^{\text{CC}'}$ , the actual probability of detecting an accidental coincidence per coincidence window reads

values:

$$\text{CC}_{jk}^{\text{t}} = B\eta_{Aj}\eta_{Bk}, \quad (\text{B5})$$

for which

$$\sum_{j,k=1}^2 \text{CC}_{jk}^{\text{t}} = \text{CC}^{\text{t}} \quad (\text{B6})$$

holds. Additionally, one has to subdivide the  $S_i^{\text{m}}$  while accounting for different dark count rates

$$S_{Aj}^{\text{m}} = B\eta_{Aj} + \text{DC}_{Aj}, \quad (\text{B7})$$

$$S_{Bk}^{\text{m}} = B\eta_{Bk} + \text{DC}_{Bk} \quad (\text{B8})$$

where similarly

$$S_A^{\text{m}} = \sum_{j=1}^2 S_{Aj}^{\text{m}} \quad \text{and} \quad S_B^{\text{m}} = \sum_{k=1}^2 S_{Bk}^{\text{m}} \quad (\text{B9})$$

and assign different accidental coincidence rates to different detector combinations:

$$\text{CC}^{\text{acc}} = \sum_{j,k=1}^2 \text{CC}_{jk}^{\text{acc}} = \sum_{j,k=1}^2 S_{Aj}^{\text{m}} S_{Bk}^{\text{m}} t_{\text{CC}}. \quad (\text{B10})$$

To take into account different detector jitters, one arrives at different values of  $t_{\Delta,jk}$ , which require an adaptation of the coincidence window loss of Eq. (13):

$$\eta_{jk}^{\text{tcc}} = \text{erf} \left[ \sqrt{\ln(2)} \frac{t_{\text{CC}}}{t_{\Delta,jk}} \right]. \quad (\text{B11})$$

In this case, Eq. (14) becomes

$$\text{CC}^{\text{m}} = \sum_{j,k=1}^2 [\eta_{jk}^{\text{tcc}} \text{CC}_{jk}^{\text{t}} + \text{CC}_{jk}^{\text{acc}}], \quad (\text{B12})$$

and similarly Eq. (15) can be written as

$$\text{CC}^{\text{err}} = \sum_{j \neq k}^2 [\eta_{jk}^{\text{tcc}} \text{CC}_{jk}^{\text{t}} e^{\text{pol}} + \text{CC}_{jk}^{\text{acc}}]. \quad (\text{B13})$$

Here we assume a correlated Bell state ( $\phi^{+/-}$ ) in the respective basis. For anticorrelated ones ( $\psi^{+/-}$ ), the indices to be summed over have to be replaced by  $j = k$ .

#### 4. Key-rate-formula adjustments

Following from the above considerations, in a realistic experiment, one might additionally expect that one of the polarization measurement settings used in the BBM92 protocol is more prone to errors than the other one. Let us assume that this is due to different optical errors  $e^{\text{pol}}$  which can depend on the measurement basis. As an example, the  $HV$  basis often shows higher fidelity than the superposition bases as a result of the source design, which relies on polarizing beamsplitters defining  $H$  and  $V$  with high extinction (1 : 1000 or better). Because of this, we obtain two values of QBER [see Eq. (16)], one for each measurement setting. Let us denote these with  $E_{HV}$  and  $E_{DA}$ . If coincidences obtained in the  $HV$  basis are used to derive the key, then in Eq. (17) we can set  $E_{\text{bit}} = E_{HV}$  and  $E_{\text{ph}} = E_{DA}$ . Similarly, for a key derived from coincidences in the  $DA$  basis we set  $E_{\text{bit}} = E_{DA}$  and  $E_{\text{ph}} = E_{HV}$ . If both Alice and Bob choose the  $HV$  setting with probability  $p$  and the  $DA$  setting with probability  $(1 - p)$ , they would obtain two key rates, each in one basis:

$$R_{HV}^s = p^2 CC^m [1 - H_2(E_{DA}) - f(E_{HV})H_2(E_{HV})], \quad (\text{B14})$$

$$R_{DA}^s = (1 - p)^2 CC^m [1 - H_2(E_{HV}) - f(E_{DA})H_2(E_{DA})]. \quad (\text{B15})$$

The total key rate is then the sum of these two key rates, and the total compatible basis choice probability from Eq. (17) is  $q = p^2 + (1 - p)^2$ .

Another common technique is to use predominantly one of the basis settings and use the other only with very low probability to obtain the estimate on  $E_{\text{ph}}$ . This is often referred to as the “efficient BB84 protocol” [31]. In the asymptotic setting, one can therefore assume that the probability  $p$  to choose the  $HV$  basis approaches unity, and the final key rate is

$$R_{\text{efficient}}^s = CC^m [1 - H_2(E_{DA}) - f(E_{HV})H_2(E_{HV})]. \quad (\text{B16})$$

Additionally, in some works the authors assume that in the asymptotic setting the block length is also approaching infinity and therefore  $f(E_{\text{bit}})$  approaches unity [32,33]. Last but not least, even in the case of different error rates, one can in practice use the average error  $E = (E_{HV} + E_{DA})/2$  with Eq. (19) to obtain a lower bound on the secret key rate [10,34], since

$$2H_2\left(\frac{E_1 + E_2}{2}\right) \geq H_2(E_1) + H_2(E_2) \quad \forall E_i \in [0, 0.5]. \quad (\text{B17})$$

- 
- [1] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, *Rev. Mod. Phys.* **74**, 145 (2002).
- [2] F. Xu, X. Ma, Q. Zhang, H.-K. Lo, and J.-W. Pan, *Rev. Mod. Phys.* **92**, 025002 (2020).
- [3] C. H. Bennett and G. Brassard, *Theoretical Computer Science* **560**, 7 (2014).
- [4] R. Ursin, F. Tiefenbacher, T. Schmitt-Manderbach, H. Weier, T. Scheidl, M. Lindenthal, B. Blauensteiner, T. Jennewein, J. Perdigues, P. Trojek, B. Ömer, M. Fürst, M. Meyenburg, J. Rarity, Z. Sodnik, C. Barbieri, H. Weinfurter, and A. Zeilinger, *Nature Phys.* **3**, 481 (2007).
- [5] J. Yin, J.-G. Ren, H. Lu, Y. Cao, H.-L. Yong, Y.-P. Wu, C. Liu, S.-K. Liao, F. Zhou, Y. Jiang, X.-D. Cai, P. Xu, G.-S. Pan, J.-J. Jia, Y.-M. Huang, H. Yin, J.-Y. Wang, Y.-A. Chen, C.-Z. Peng, and J.-W. Pan, *Nature (London)* **488**, 185 (2012).
- [6] S. Ecker, B. Liu, J. Handsteiner, M. Fink, D. Rauch, F. Steinlechner, T. Scheidl, A. Zeilinger, and R. Ursin, *npj Quantum Inf.* **7**, 5 (2021).
- [7] J. Yin, Y.-H. Li, S.-K. Liao, M. Yang, Y. Cao, L. Zhang, J.-G. Ren, W.-Q. Cai, W.-Y. Liu, S.-L. Li, R. Shu, Y.-M. Huang, L. Deng, L. Li, Q. Zhang, N.-L. Liu, Y.-A. Chen, C.-Y. Lu, X.-B. Wang, F. Xu, J.-Y. Wang, C.-Z. Peng, A. K. Ekert, and J.-W. Pan, *Nature (London)* **582**, 501 (2020).
- [8] S. Wengerowsky, S. K. Joshi, F. Steinlechner, J. R. Zichi, S. M. Dobrovolskiy, R. van der Molen, J. W. N. Los, V. Zwiller, M. A. M. Versteegh, A. Mura, D. Calonico, M. Inguscio, H. Hübel, L. Bo, T. Scheidl, A. Zeilinger, A. Xuereb, and R. Ursin, *Proc. Natl. Acad. Sci. USA* **116**, 6684 (2019).
- [9] S. Wengerowsky, S. K. Joshi, F. Steinlechner, H. Hübel, and R. Ursin, *Nature (London)* **564**, 225 (2018).
- [10] S. K. Joshi, D. Aktas, S. Wengerowsky, M. Lončarić, S. P. Neumann, B. Liu, T. Scheidl, Ž. Samec, L. Kling, A. Qiu, M. Stipčević, J. G. Rarity, and R. Ursin, *Sci. Adv.* **6**, eaba0959 (2020).
- [11] A. K. Ekert, *Phys. Rev. Lett.* **67**, 661 (1991).
- [12] C. H. Bennett, G. Brassard, and N. D. Mermin, *Phys. Rev. Lett.* **68**, 557 (1992).
- [13] J.-P. Chen, C. Zhang, Y. Liu, C. Jiang, W.-J. Zhang, Z.-Y. Han, S.-Z. Ma, X.-L. Hu, Y.-H. Li, H. Liu, F. Zhou, H.-F. Jiang, T.-Y. Chen, H. Li, L.-X. You, Z. Wang, X.-B. Wang, Q. Zhang, and J.-W. Pan, *Nat. Photon.* **15**, 570 (2021).
- [14] H.-K. Lo, X. Ma, and K. Chen, *Phys. Rev. Lett.* **94**, 230504 (2005).
- [15] A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani, *Phys. Rev. Lett.* **98**, 230501 (2007).
- [16] X. Ma, C. H. F. Fung, and H. K. Lo, *Phys. Rev. A* **76**, 012307 (2007).
- [17] S. P. Neumann, D. Ribezzo, M. Bohmann, and R. Ursin, *Quantum Sci. Technol.* **6**, 025017 (2021).
- [18] H. Takesue and K. Shimizu, *Opt. Commun.* **283**, 276 (2010).
- [19] R. Hošák, I. Straka, A. Predojević, R. Filip, and M. Ježek, *Phys. Rev. A* **103**, 042411 (2021).
- [20] D. N. Klyshko, *Sov. J. Quantum Electron.* **10**, 1112 (1980).
- [21] A. Anwar, C. Perumangatt, F. Steinlechner, T. Jennewein, and A. Ling, *Rev. Sci. Instrum.* **92**, 041101 (2021).
- [22] M. Bohmann, R. Kruse, J. Sperling, C. Silberhorn, and W. Vogel, *Phys. Rev. A* **95**, 033806 (2017).
- [23] M. Bohmann, L. Qi, W. Vogel, and M. Chekhova, *Phys. Rev. Research* **1**, 033178 (2019).
- [24] N. Lütkenhaus, *Phys. Rev. A* **59**, 3301 (1999).

- [25] T. Moroder, O. Gühne, N. Beaudry, M. Piani, and N. Lütkenhaus, *Phys. Rev. A* **81**, 052342 (2010).
- [26] D. Elkouss, J. Martínez-Mateo, and V. Martín, *Quantum Inf. Comput.* **11**, 226 (2011).
- [27] D. Vasylyev, A. A. Semenov, and W. Vogel, *Phys. Rev. Lett.* **117**, 090501 (2016).
- [28] M. Bohmann, R. Kruse, J. Sperling, C. Silberhorn, and W. Vogel, *Phys. Rev. A* **95**, 063801 (2017).
- [29] V. Bécaries and J. Blázquez, *Sci. Technol. Nucl. Install.* **2012**, 240693 (2012).
- [30] Y. Zhang, P. J. Coles, A. Winick, J. Lin, and N. Lütkenhaus, *Phys. Rev. Research* **3**, 013076 (2021).
- [31] H.-K. Lo, H. F. Chau, and M. Ardehali, *J. Cryptology* **18**, 133 (2005).
- [32] M. Koashi and J. Preskill, *Phys. Rev. Lett.* **90**, 057902 (2003).
- [33] M. Koashi, *New J. Phys.* **11**, 045018 (2009).
- [34] C. H. F. Fung, X. Ma, and H. F. Chau, *Phys. Rev. A* **81**, 012318 (2010).

## 3.2 Experimental entanglement generation for quantum key distribution beyond 1 Gbit/s

This paper describes the source of polarization-entangled photon pairs in detail and assesses its performance parameters. This source was used for all other papers as well: We tested the model of publication 3.1 with it and it also supplied the photon pairs needed for publications 3.3 and 3.4.

I contributed to the paper by planning the experiment with Rupert Ursin and Martin Bohmann, by designing and constructing the source of polarization-entangled photon pairs, by measuring all of its performance parameters except for the spectrum, by coding and plotting all simulations and by writing the paper.

# Experimental entanglement generation for quantum key distribution beyond 1 Gbit/s

Sebastian Philipp Neumann,\* Mirela Selimovic, Martin Bohmann, and Rupert Ursin†  
*Institute for Quantum Optics and Quantum Information Vienna,  
 Austrian Academy of Sciences, Boltzmannngasse 3, 1090 Vienna, Austria  
 Vienna Center for Quantum Science and Technology, Boltzmannngasse 5, 1090 Vienna, Austria*  
 (Dated: January 4, 2022)

Top-performance sources of photonic entanglement are an indispensable resource for many applications in quantum communication, most notably quantum key distribution. However, up to now, no source has been shown to simultaneously exhibit the high pair-creation rate, broad bandwidth, excellent state fidelity, and low intrinsic loss necessary for gigabit secure key rates. In this work, we present for the first time a source of polarization-entangled photon pairs at telecommunication wavelengths that covers all these needs of real-world quantum-cryptographic applications, thus enabling unprecedented quantum-secure key rates of more than 1 Gbit/s. Our source is designed to optimally exploit state-of-the-art telecommunication equipment and detection systems. Any technological improvement of the latter would result in an even higher rate without modification of the source. We discuss the used wavelength-multiplexing approach, including its potential for multi-user quantum networks and its fundamental limitations. Our source paves the way for high-speed quantum encryption approaching present-day internet bandwidth.

## I. INTRODUCTION

Entanglement-based quantum key distribution (QKD) requires sources of photonic entanglement that exhibit high overall pair creation rates, high spectral brightness, low intrinsic loss, high fidelity to maximally entangled states and low maintenance. These points are getting ever more important for achieving non-vanishing key rates over fiber and free-space quantum links which are governed by unavoidable strong losses. In order to achieve this, different source designs have achieved remarkable individual figures of merit: Atzeni et al. [1] achieved  $2.2 \times 10^9$  cps/mW overall brightness and Sun et al. [2]  $1.2 \times 10^9$  cps/mW/nm spectral brightness, both in waveguide configurations. Liu et al. [3] reported an average collection efficiency of 84.1%, Kaiser et al. [4] as well as Joshi [5] showed 99.8% polarization visibility, and the source of Tang et al. [6] even survived a rocket explosion. For a recent comprehensive overview and a detailed discussion of the parameters in use, see Ref.s [7, 8].

While all of the reported sources show excellent merits regarding one or even two of these fundamental parameters, none of them exhibit outstanding overall performance necessary for first-grade real-world QKD applications. In such applications, high *overall brightness* is necessary to create high key rates required in telecommunication infrastructures today. It is defined as the number of entangled photon pairs created in the source before all losses. High *spectral brightness*, i.e. the rate of photon pairs created per wavelength, enables efficient wavelength division multiplexing (WDM) of signals [9, 10], diminishes dispersion effects [11] and will be necessary to couple to quantum memories in the future [12]. *Collection efficiency* is the probability of a photon created in the

source being detected. High source-intrinsic collection efficiency allows to tolerate more (unavoidable) channel loss. High *visibility* of the entangled state allows the experimenter to efficiently perform error correction and privacy amplification in post-processing, which means that a larger fraction of the raw key can be utilized; additionally it can partly compensate for noise, detector jitter and channel loss.

The highest experimentally generated key rates as of today were acquired under laboratory conditions, without deployment of real-life links. The record values are 10 Mbit/s [13] in a decoy-state configuration, 26.2 Mbit/s [14] using time-bin qudits and 7.0 Mbit/s [15] in an implementation with high-dimensional entanglement.

In this work, we present a source of polarization-entangled photon pairs performing competitively in all of the above-mentioned parameters, enabling unprecedented key rates beyond 1 Gbit/s by exploiting polarization entanglement only. The source was built in a bulk Sagnac-loop configuration deploying type-0 spontaneous parametric down-conversion (SPDC) inside a nonlinear crystal producing polarization-entangled photon pairs at telecom wavelength. Using bulk polarization measurement modules and a tunable blazed-grating filter, respectively, we quantified brightness, collection efficiency, spectral bandwidth and polarization visibility for different WDM channels as well as the full spectrum. We find that using 66 channel pairs of off-the-shelf WDM devices, the source could supply a total of 1.2 Gbit/s secure key in a point-to-point configuration. Even higher values of up to 3.6 Gbit/s are conceivable when using narrow ultra-dense WDM channels and pumping with high laser power. Additionally, we show that by using the full 106 nm-bandwidth spectrum of our source, a fully connected local quantum network with up to 33 users could be created. Our results provide an essential contribution towards high-key-rate quantum communication

\* sebastian.neumann@oeaw.ac.at

† rupert.ursin@oeaw.ac.at

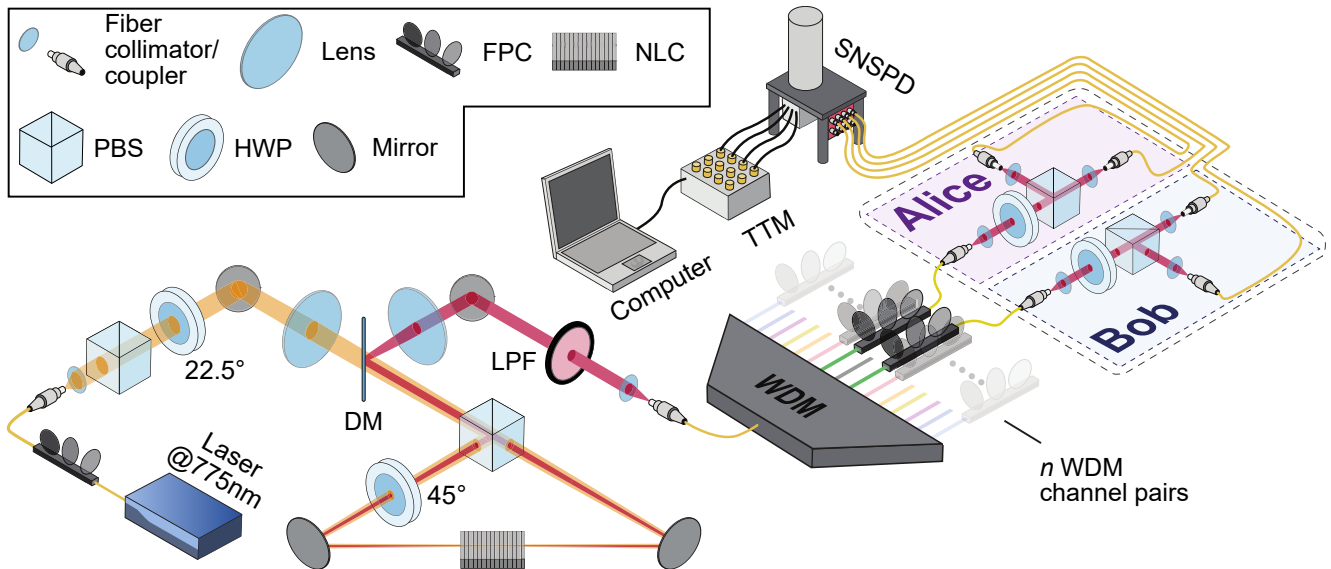


FIG. 1. Sketch of the setup. The continuous-wave pump laser at 775.06 nm is coupled into a single-mode fiber (SMF) and directed towards the bulk optics setup. After beam collimation, a polarizing beam splitter (PBS) and a half-wave plate (HWP) set the pump laser's polarization to 45°. A pump lens bidirectionally focuses the pump into the nonlinear crystal (NLC) placed inside a Sagnac loop. The loop consists of a dichroic PBS splitting the pump by transmitting (reflecting) the horizontally (vertically) polarized part. The reflected part passes a HWP at 45°. Thus, all pump photons are horizontally polarized when entering the NLC, where photon pairs are created via type-0 spontaneous parametric down-conversion (SPDC). They travel back to the PBS, where both propagation direction modes interfere and the SPDC photons' polarization states become entangled. Successively, a dichroic mirror (DM) separates the SPDC beam from the pump. The SPDC traverses a longpass filter (LPF) blocking residual pump light before being collected by a SMF. The broad total photon spectrum is subdivided by use of a WDM. For visibility measurements, polarization rotations in the fiber have to be compensated using fiber polarization controllers (FPC) in order to acquire the desired correlations. Measurements in mutually unbiased bases are realized by setting both receiver's HWP to either 0° or 22.5°. The PBS output modes are coupled into SMF and directed to four channels of superconducting nanowire single-photon detectors (SNSPD), whose detection times are registered using a time-tagging module (TTM) and post-processed with a computer. For measurements of brightness and collection efficiency, the WDMs are directly connected to the SNSPDs. For the measurement of the total spectrum, the WDM was replaced by a 50:50 beam splitter, one arm of which was connected to a tunable filter (not depicted) before detection.

necessary for future quantum infrastructures.

## II. RESULTS

### A. Source design

To arrive at key rates above 1 Gbit/s, we need to determine the outstanding values of the source's spectral bandwidth, collection efficiency, brightness and visibility values, which we will set forth in the following. The experimental set-up is depicted in Fig. 1. The source was built in a bulk Sagnac configuration with the loop containing a type-0 nonlinear crystal (NLC). It was bidirectionally pumped using a 775.06 nm continuous-wave laser with its focusing parameters optimized for high-brightness SPDC. It produces telecom-wavelength entangled photon pairs with their spectrum centered around 1550.12 nm. Carefully chosen collimation and coupling optics allow for the SPDC's low-loss insertion into a single-mode fiber. For a more detailed description of

the source's working principle, see the caption of Fig. 1 and the Methods section. The photons were detected by use of two fiber-coupled superconducting nanowire single-photon detector (SNSPD) channels connected to a time-tagging module (TTM). From its time stamps, our computer software calculated  $g^{(2)}$  correlations between the channels, from which we identified the entangled photon pairs.

### B. Evaluation of source performance parameters

Figure 2 shows the source's collection efficiency over the full SPDC spectrum. The graph was acquired by probabilistically separating the entangled pairs with a 50:50 in-fiber beam splitter before detection and using a free-space grating-based tunable wavelength filter in one of its arms. The spectrally resolved collection efficiency is required to quantify the portion of the spectrum usable in QKD. The source spectrum can be optimally exploited for QKD by deterministically separating entangled pho-



ton pairs using WDM channels. Due to energy conservation during the SPDC process, entangled photons are found in channel pairs equidistant from the spectrum’s central wavelength. Such pairs are depicted in the same colors in Fig. 2. Each of the  $n$  channel pairs can be considered an independent carrier of photonic entanglement [16].

To precisely determine collection efficiencies and brightness values, matching WDM channel pairs were connected directly to the SNSPDs. To ensure straightforward comparability with other source designs, we did not subject the photon pairs to long-distance link attenuation. The single-mode fibers in use added up to no more than 10 m length. All of the following collection efficiencies include coupling and transmission losses of WDMs and fibers as well as SNSPD detection efficiencies. We define the collection efficiency  $\eta$ , sometimes called “heralding” or “Klyshko” [17] efficiency, as  $\eta = CC/\sqrt{S_A \cdot S_B}$ , where  $CC$  are the coincident counts between the communicating partners’ detectors with single count rates  $S_A$  and  $S_B$ . Figure 3 shows collection efficiency values for different standard WDM channels of 100 and 200 GHz (dense WDM) and 2500 GHz (coarse WDM, CWDM). Collection efficiencies stay above 20% on average in a 56.3 nm range around the central SPDC wavelength. As a comparison, averaging over the full spectral range, the value decreases to 12.9%. This value was acquired using a 50:50 in-fiber beam splitter and is in accordance with Fig. 2, since coupling into the tunable filter’s collecting single-mode fiber is less efficient far from the central wavelength due to chromatic aberration of the coupling

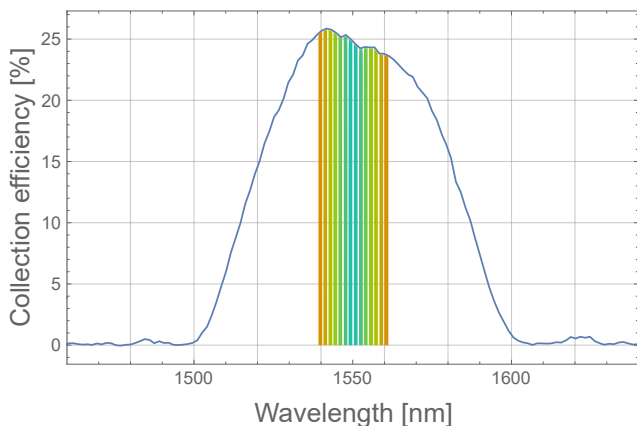


FIG. 2. Measured collection efficiency of the source per wavelength. The measurement was carried out using a tunable wavelength filter based on a rotatable blaze grating, which one photon of a pair passed. The graph was obtained by determining the ratio of coincidence counts vs. singles of the lossy filter arm and normalizing to the highest collection efficiency obtained in the WDM measurements (see Fig. 3). WDM channel pairs carrying entangled photon pairs are shown as slices of the same color. The slight asymmetry of the spectrum can be explained by varying coupling efficiencies of the tunable filter and the single-photon detectors.

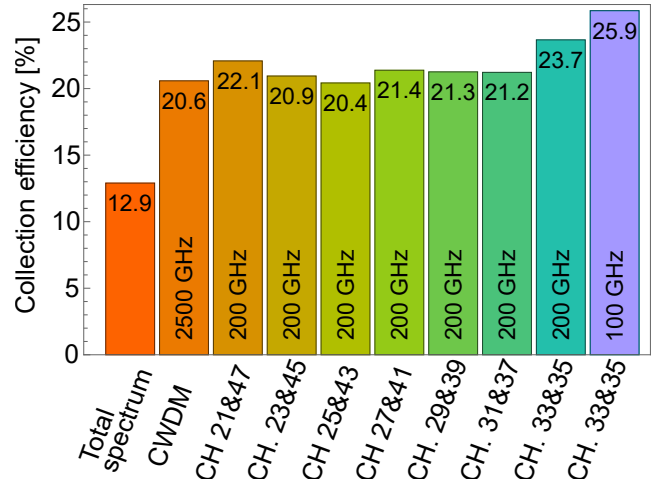


FIG. 3. Average measured collection efficiencies per wavelength-channel pair obtained by determining the ratio between coincident and single detector counts. Note that the lower values for the full spectrum originate in part from the fact that a probabilistic beam splitter was used to separate the photons, and in part from the fact that far from the central wavelength, the source intrinsically shows lower collection efficiencies due to its focusing parameters [18].

optics and wavelength-dependent mode structures.

Figure 4 shows spectral brightness values, i.e., the number of photon pairs per pump power, wavelength and time, for the same WDM channels as used for Fig. 3. Solid lines refer to *detected* pair rates, while faint lines are calculated pair creation rates in the crystal before any loss. This parameter is called spectral brightness  $B$ . The latter depends on measured pair rates and collection efficiencies as  $B = CC/\eta^2$ . The highest spectral brightness value of  $B_{31+37} = 4.17 \times 10^6$  cps/mW/nm was found in the 200 GHz WDM channel pair 31+37.

Figure 5 demonstrates our source’s exceptional fidelity to a maximally entangled state with measured polarization visibilities  $V$  of up to 99.4% in two mutually unbiased bases. To arrive at these values, bulk polarizing beam splitters with single-mode coupled output ports were implemented between WDMs and SNSPDs (cf. Fig. 1).  $V$  stayed above 99.2% for all observed 100 and 200 GHz channels. Since polarization rotations in fiber are wavelength dependent, no full polarization compensation using fiber polarization controllers (FPC) can be achieved for broad spectra. However, even for the broader CWDM channels and the full spectrum, the quantum bit error rate (QBER)  $E = (100\% - V)/2$  stays above the 11% limit necessary for secure key creation [19].

As a final figure of merit, we want to point out our source’s stability: All of the above data was taken more than 6 months after source alignment, with no certifiable performance degradation during this period. The only active stabilization necessary was carried out by an electronically controlled oven restricting crystal temperature fluctuations to  $< 0.01^\circ \text{C}$ , while no performance degra-

dation could be observed for changes  $< 0.1^\circ \text{C}$ .

### C. Secure key rate analysis

From this experimental data, maximum secure key rates can be inferred according to the model in Ref. [8]. This model considers the probabilistic multi-photon-pair statistics of a continuous-wave-pumped entangled-photon source. An in-depth analysis of these statistics is necessary, since simply increasing the pump power can be detrimental to the key rate. This is because multi-photon pairs lead to so-called accidental coincidences and thus an increased QBER, making it necessary to use a larger portion of the key for classical post-processing. Therefore, there exists an optimal pump power. This optimum additionally depends on the wavelength-channel width, leading to a trade-off between the rate of detected photon pairs and the accidental detection probability per wavelength-channel pair. The source can be operated as is, by optimizing the laser power inside the crystal. Using the collection efficiency, brightness, and visibility values experimentally achieved in our experiment, we simulate QKD implementations with different WDM scenarios in Fig. 6. Here, each WDM-channel pair can provide a secure key rate  $R_k^s$  depending on its individual collection efficiency and entanglement quality. In this work, we are concerned with the total key rate  $R^s = \sum_{k=1}^n R_k^s$  achievable with  $n$  channel pairs from our source. Our calculations, depicted in Fig. 6, show that already with standard off-the-shelf 100 GHz WDM channels, 1.2 Gbit/s secure key rate could be achieved at 400 mW pump power when deploying suitable high-end detectors. With 132 channels of 50 GHz width,  $R^s = 2.0$  Gbit/s can be achieved with 660 mW pump power. 25 GHz channels would even

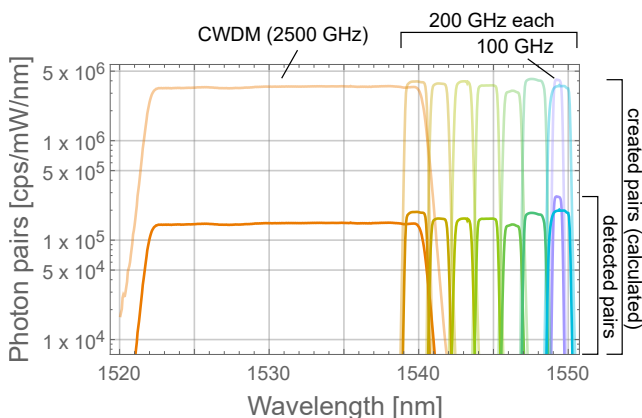


FIG. 4. Source brightness per wavelength. Brightness values (transparent) and measured coincidences (solid) of the source for measured WDM channel pairs per mW. The central wavelength is 1550.12 nm, and only the channels with the lower wavelength of each channel pair are depicted for simplicity. Brightness values were calculated from measured coincidences and collection efficiencies.

allow for 3.0 Gbit/s at 900 mW, and reducing the spacing further to 529 channel pairs of 12.5 GHz, the same key rate value could be reached already with 800 mW pump power. When pumping with 1000 mW in the latter WDM configuration, a maximum value of 3.6 Gbit/s is possible.

## III. DISCUSSION

We have presented a stable source of polarization-entangled photon pairs with high total and spectral brightness, high collection/heralding efficiency and extremely high state fidelity. Calculating the quantum secure key rates that our source could sustain when operating with sufficiently performing single-photon detectors, we arrive at key rates above 1 Gbit/s with off-the-shelf wavelength-division-multiplexing devices and laser powers below the crystal's damage threshold. When relaxing the latter requirements, key rates of more than 3 Gbit/s are conceivable with our state-of-the-art source:

Firstly, stronger pump laser power could increase the effective spectral and overall brightness. To mitigate the risk of damage to our setup, we restricted ourselves to powers of no more than 400 mW, for which we could still certify undiminished source performance. However, if one were to install laminar airflow boxes to keep dust away from the optical surfaces, specifications by the crystal manufacturer suggest that powers of 1000 mW and beyond are feasible [20]. Secondly, using narrower WDM spacings and therefore higher channel pair numbers  $n$  reduces the number of undesired accidental correlation measurements and therefore enhances the

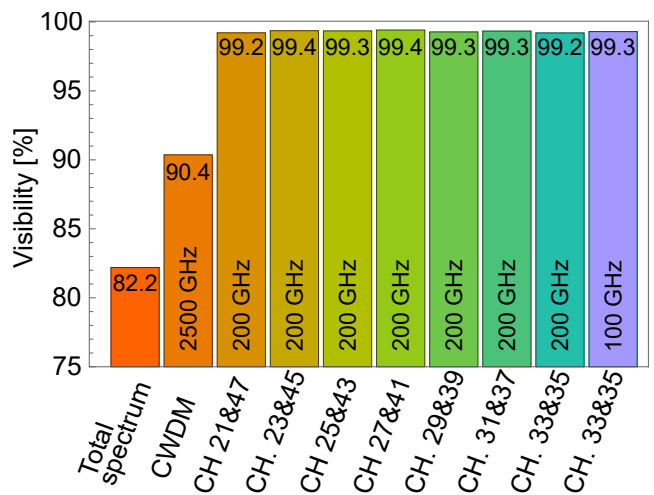


FIG. 5. Visibility per wavelength-channel pair. Average values of visibility  $V$  obtained by measuring correlations in polarization in two mutually unbiased bases. We measured  $V > 99.2\%$  for all WDM spectral widths used for key calculations. We attribute lower visibility values for the 2500 GHz coarse WDM (CWDM) and the full spectrum to wavelength-dependent polarization rotations in the fibers, which can be compensated individually if subdividing in narrow spectra.

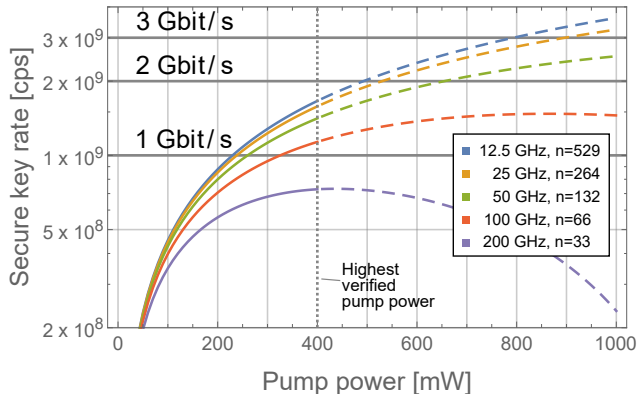


FIG. 6. Quantum-secure key rates per pump power. Expected key rates per pump power at 775.06 nm for different wavelength demultiplexing scenarios after sifting and error correction, taking into account multipair statistics. The WDM channels under consideration follow standards defined by the International Telecommunication Union and we indicate the number of used channel pairs  $n$ . Already for 100 GHz channels, our source could provide key rates above 1 Gbit/s. While we experimentally verified source operation without performance decrease up until 400 mW pump power, it is reasonable to assume that 1000 mW are still feasible [20]. This could allow for more than 2.0 Gbit/s in a 50 GHz demultiplexing scheme, while 25 GHz and 12.5 GHz enable more than 3.0 Gbit/s. The relative increase in key rate for ever narrower channels becomes smaller due to the accompanying increase of the entangled photons' coherence time.

key rate [10]. Deploying WDMs narrower than 100 GHz might require customization, but is possible in principle and also covered by ITU standards [21]. However, going below 6.25 GHz is hardly beneficial anymore. This is because the entangled photons' coherence time is in the order of tens of picoseconds in this case, which deteriorates the timing precision necessary for photon pair correlation. Ultimately, even assuming perfect temporal photon detection, this time-bandwidth product effect represents the physical limit of increasing the rate of polarization and time-bin based QKD protocols. As a side remark, further narrowing the channel width might nevertheless be beneficial in order to address quantum memories for future quantum computing or quantum repeater schemes [22].

In a real-world QKD implementation, where many channels including their respective detection system can terminate at one and the same communication partner,  $n$  channel pairs can connect between 2 and  $2n$  users individually. However, due to its broad spectrum, our source is also ideally suited for fully connected multi-user quantum network configurations [16]. With the 66 channel pairs available when using 100 GHz spacing, our source could fully connect 12 users in a trusted-node-free network design without any probabilistic multiplexing [23]. Deploying 529 channel pairs of 12.5 GHz width, this number increases to 33 fully connected users.

Although our source is ideally suited for a large variety of applications, its practical deployment is limited by current single-photon detector performance. For calculating the overall key rate, we assume our detector's quantum efficiency, specified to be 80% by the manufacturer, to stay constant for all wavelength channels and count rates. We assume 38 ps jitter of the full detection system including time-tagging electronics, which was the lowest value we observed during our experiment. Most importantly, we have simultaneously assumed maximum detector count rates of 200 MHz. While such count rates can be achieved in state-of-the-art experiments [24], so far there exists no detection system simultaneously exhibiting high detection efficiency as well as low jitter. We note, however, that in (high-loss) long-distant communication scenarios, maximum count-rate limitations do not pose any practical problems for QKD implementations due to the reduced number of registered photons. But even in these cases, low jitter is crucial to avoid accidental two-fold clicks of uncorrelated photons. Thus, it becomes apparent that although recent research shows promising approaches [24–26], detector technology has yet to catch up with high-end entangled-photon-pair sources such as the one presented in this work.

We want to stress that for the claims presented in this work, no problems or challenges of the source design were shifted to the detection devices. There is no conceivable enhancement to the source that could lead to a QKD performance increase without a significant advance in detector technology first. As of today, detectors are the limiting factor for achieving high key rates: temporal jitter as well as dead time of SNSPDs (and, even more so, of semiconductor-based single-photon detectors) can neither resolve nor register the extraordinarily high pair creation rates of our high-end source.

#### IV. CONCLUSION

We have described a source capable of providing more than 1 Gbit/s secure key rate using off-the-shelf components. To the best of our knowledge, this is the brightest source with simultaneously optimized collection efficiency and visibility up to date. Exceptional visibility of the source's polarization-entangled photon pairs enables quantum bit error rates below 0.4%. Measured collection efficiencies of up to 25.9% provide high photon yield. Damage threshold measurements by the crystal manufacturer [20] suggest that the crystal could be pumped with up to 1 W, which would create more than  $10^{11}$  photon pairs per second over the full spectrum. These exceptional entangled photon pair creation rates cannot be resolved by single-photon detection systems as of today. Thus, we have identified the most pressing problem in current QKD technology as the trade-off between maximum count rate and timing jitter of modern detection systems, which limits the performance of state-of-the-art source technology as presented in this work.

## V. METHODS

### A. Source design and working principle

The source is a bulk optics telecom-wavelength source making use of SPDC inside a nonlinear periodically poled 5% magnesium-doped congruent lithium niobate crystal with type-0 phase-matching [27]. The crystal is placed inside a Sagnac loop to enable coherent superposition of orthogonally polarized SPDC modes. The loop was built as small as possible to allow for strong focusing of the pump laser, which has to be carried out by a single lens outside the loop in order to be able to separately optimize pump focusing and SPDC collimation. Additionally, using one pump lens benefits indistinguishability of the beam profile in both of the loop's propagation direction modes. The focusing parameter  $\xi$  was chosen carefully according to efficiency considerations in Ref. [18]. We put emphasis on obtaining a large ratio of crystal length to Rayleigh length of the pump beam in order to obtain high pair creation rates. Concretely, this corresponded to a focus length  $f = 254$  mm for the pump lens and  $f = 200$  mm for the SPDC collection lens. To ensure good fidelity of the pump beam to a  $TE_{00}$  mode, an aspheric lens with  $f = 18.4$  mm was used to couple out of the single-mode fiber. The comparably strong pump focusing required for this goal can lead to divergence-induced degradation of the PBS extinction ratio, which negatively influences the brightness. We therefore regularly checked the PBS's performance during source construction with lasers at both pump and SPDC wavelength. The loop length is restricted on one hand by the focal length of the lenses, since tighter focusing corresponds to higher brightness. On the other hand, it is limited by the length of the crystal including its temperature control, which has to fit in the long side of the loop. Additionally, the pump and SPDC beams must not be clipped when entering and leaving the crystal, therefore again limiting beam divergence. To account for these different trade-offs, we chose a loop length of  $\approx 35$  cm to house a nonlinear crystal of 50 mm length for enabling the SPDC process. In combination with the pump beam's calculated Gaussian profile, this resulted in  $\xi = 1.99$ . The SPDC beam's focus parameters were matched to the same value as the pump's, which required different collimation and collection parameters due to their different wavelengths. The entangled photons were coupled into an SMF with a 1550 nm anti-reflection coating via an aspheric lens. After passing a longpass filter, all SPDC photons were coupled into one standard SMF-28 single-mode fiber. For a detailed description of the source's working principle, we additionally refer the reader to Fig. 1.

To ensure outstanding performance of our source, not only the correct choice of parameters, but also an elaborate alignment procedure was essential. To this end, we measured the power of light being reflected back to the pump laser's isolator to ensure perfect alignment of the loop. This also allows for perfect collimation of the pump

beam, which can be guaranteed by maximizing the back-coupling. Additionally, one alignment step was to couple an amplified and polarization-controlled 1550.12 nm laser out of the SPDC collection fiber to make use of up-conversion for reversing the beam paths and aligning the full set-up with strong laser light.

Separation of the entangled photon pairs was carried out using standard dense wavelength-division multiplexing (DWDM) modules with a channel spacing of 200 as well as 100 GHz according to the ITU grid. We want to emphasize that we deployed off-the-shelf telecommunication devices for this task. Their spectrum's full width at half maximum (FWHM) amounts to only about 75% of the channel spacing. Deploying custom-made DWDM channels with steeper edges, thus allowing broader FWHM, could therefore increase the usable part of the spectrum by up to 25%. The WDM channels carrying the respective entangled photons of a pair were connected to two channels of a SNSPD system with 80% detection efficiency according to the manufacturer. Detection events were assigned a time stamp with 1 ps bin width by use of a time-tagging module. From two-fold coincident counts between the two detector channels, we calculated a  $g^{(2)}$  correlation function for each channel pair. The FWHM of the correlation peak amounted to 38 ps, which is equivalent to the total timing jitter of both detection systems.

### B. Benchmarking source performance

To determine the source brightness, i.e. the number of entangled pairs produced inside the crystal via SPDC before any losses per second, the WDM channels were connected to the SNSPDs directly. From their collection efficiencies [17], one can infer the total channel losses and thus the pair production rates (see Fig. 4 and the related discussion). Measurements were carried out for pump powers of 50  $\mu$ W to keep the ratio of accidental coincidence counts to pair counts low. This is important in order to neither overestimate the heralding efficiency nor underestimate brightness due to uncorrelated accidental counts mistakenly registered as coincidences. Only in then case, it is admissible to calculate the brightness as  $B = CC/\eta^2 = S_A S_B/CC$ , where noise counts have been subtracted from single count rates. Additionally, to check for crystal damages and overall source performance in high-power regimes, we exemplarily checked  $B_{33+35}^{100 \text{ GHz}}$ , the brightness for the 100 GHz channel pair 33 + 35, for a pump power of 400 mW over high-loss fiber links with  $\approx 40$  dB attenuation each. We confirmed  $B_{33+35}^{100 \text{ GHz}} = 4.10 \times 10^6$  cps/mW/nm for both 50  $\mu$ W and 400 mW, therefore verifying that for powers up to 400 mW, as required for our claim of 1.2 Gbit/s secure key rate, no gray-tracking, crystal damages or any other decreases of source performance occur. However, we chose not to increase the power even further in order not to risk compromising other experiments the source is needed for, although we are confident that even higher power levels

are feasible [20].

To determine the source’s collection efficiency per wavelength over its full spectral range, the WDMs were replaced by a 50:50 fiber beam splitter (FBS). One FBS output port was connected to a SNSPD channel directly, while the other one was directed to a free-space rotatable blazed grating reflecting the incoming signal with 1.46 nm/mrad angular dispersion towards an SMF. A 1.25 nm (FWHM) wide portion of the signal was coupled into the SMF, which effectively acted as a wavelength filter. The SMF was connected to a second SNSPD channel. We determined the ratio between coincident counts of both channels and the single counts of the filter channel for different angle settings of the channel. All measurements were obtained using the same detectors and thus include the SNSPD’s wavelength dependency. To account for excess loss due to inefficient coupling and dead-time loss in the first SNSPDs, we normalized for the collection efficiency achieved with the 100 GHz WDMs and thus arrived at Fig. 2.

The entangled photons’ state fidelity was measured using two polarization-detection modules with two detector channels each (see Fig. 1). This way, erroneous counts could be quantified directly. The error was determined in two mutually unbiased bases which were set using half-wave plates (HWP). Fidelity measurements were carried out for 7 channel pairs with 200 GHz width and resulted in  $> 99.2\%$  visibility, i.e.  $< 0.4\%$  QBER for all channel pairs. These values were determined with pump powers low enough to ignore noise-induced coincidence counts, which occurred with probabilities of less than  $10^{-4}$  per registered photon pair. Deploying broader wavelength channels generally leads to lower visibilities, since in-fiber polarization rotations along the WDMs and SMFs leading to the detectors are wavelength-dependent. Thus, compensation using FPC cannot be carried out equally well for the full channel spectrum. Therefore, for the 18.4 nm coarse WDM, the average visibility only reached 90.4%. This problem can easily be mitigated by deploying more WDM channels with denser spacing and individual polarization compensation.

To arrive at the final key rates depicted in Fig. 6, we made use of the model presented in Ref. [8], which was verified with the very same source as the one presented in this work. We used the following input parameters: *Collection efficiencies* were calculated by integrating the function depicted in Fig. 2 over wavelength intervals corresponding to the channel spacings in question. These efficiencies include coupling losses of the source, attenuation in the WDM devices and fibers leading to the SNSPDs, and detection efficiencies of the latter. The *polarization visibility* of at least 99.2% translates to a QBER of 0.4%. For the sake of consistency, we used the *spectral brightness* value  $B_{33+35}^{100\text{ GHz}} = 4.10 \times 10^6$  cps/mW/nm of the same 100 GHz channel pair that was used both to normalize for the collection efficiency in Fig. 2 and to check source performance for high laser powers. The *temporal measurement precision* was assumed to be a convolution of the 38 ps overall detection system jitter with the photons’ coherence time, which we approximated from the respective WDM width in use. Additionally, we assumed a maximum of 2% deadtime-induced loss at 200 MHz *detector count rate*. In our calculation, we assume a large raw key and asymmetric random basis choice [28], which are fair assumptions for our high key-rate scenario. This allows us to calculate key rates under conditions of perfect error correction and privacy amplification. [8].

## ACKNOWLEDGMENTS

We acknowledge European Union’s Horizon 2020 programme grant agreement No. 857156 (OpenQKD) and the Austrian Academy of Sciences in cooperation with the FhG ICON-Programm “Integrated Photonic Solutions for Quantum Technologies (InteQuant)”. We also gratefully acknowledge financial support from the Austrian Research Promotion Agency (FFG) Agentur für Luft- und Raumfahrt (FFG-ALR contract 844360 and 854022).

- 
- [1] S. Atzeni, A. S. Rab, G. Corrielli, E. Polino, M. Valeri, P. Mataloni, N. Spagnolo, A. Crespi, F. Sciarrino, and R. Osellame, Integrated sources of entangled photons at the telecom wavelength in femtosecond-laser-written circuits, *Optica* **5**, 311 (2018).
  - [2] C.-W. Sun, S.-H. Wu, J.-C. Duan, J.-W. Zhou, J.-L. Xia, P. Xu, Z. Xie, Y.-X. Gong, and S.-N. Zhu, Compact polarization-entangled photon-pair source based on a dual-periodically-poled ti:linbo3 waveguide, *Opt. Lett.* **44**, 5598 (2019).
  - [3] W.-Z. Liu, M.-H. Li, S. Ragy, S.-R. Zhao, B. Bai, Y. Liu, P. J. Brown, J. Zhang, R. Colbeck, J. Fan, Q. Zhang, and J.-W. Pan, Device-independent randomness expansion against quantum side information, *Nature Physics* **17**, 448 (2021).
  - [4] F. Kaiser, L. Ngah, A. Issautier, T. Delord, D. Aktas, V. D’Auria, M. De Micheli, A. Kastberg, L. Labonte, O. Alibert, A. Martin, and S. Tanzilli, Polarization entangled photon-pair source based on quantum nonlinear photonics and interferometry, *Optics Communications* **327**, 7 (2014), special Issue on Nonlinear Quantum Photonics.
  - [5] S. K. Joshi, *Entangled Photon Pairs: Efficient Generation and Detection, and Bit Commitment*, Ph.D. thesis, Phd Thesis at Centre for Quantum Technologies, National University of Singapore (2014).
  - [6] Z. Tang, R. Chandrasekara, Y. C. Tan, C. Cheng, K. Durak, and A. Ling, The photon pair source that survived a rocket explosion, *Scientific Reports* **6**, 25603 (2016).
  - [7] A. Anwar, C. Perumangatt, F. Steinlechner, T. Jennewein, and A. Ling, Entangled photon-pair sources

- based on three-wave mixing in bulk crystals, *Review of Scientific Instruments* **92**, 041101 (2021).
- [8] S. P. Neumann, T. Scheidl, M. Selimovic, M. Pivoluska, B. Liu, M. Bohmann, and R. Ursin, Model for optimizing quantum key distribution with continuous-wave pumped entangled-photon sources (2021), in print at *Physical Review A*, arXiv:2103.14639 [quant-ph].
- [9] D. Aktas, B. Fedrici, F. Kaiser, T. Lunghi, L. Labonte, and S. Tanzilli, Entanglement distribution over 150 km in wavelength division multiplexed channels for quantum cryptography, *Laser & Photonics Reviews* **10**, 451 (2016).
- [10] J. Pseiner, L. Achatz, L. Bulla, M. Bohmann, and R. Ursin, *Quantum Science and Technology* **6**, 035013 (2021).
- [11] S. P. Neumann, D. Ribezzo, M. Bohmann, and R. Ursin, Experimentally optimizing QKD rates via nonlocal dispersion compensation, *Quantum Science and Technology* **6**, 025017 (2021).
- [12] K. Heshami, D. G. England, P. C. Humphreys, P. J. Bustard, V. M. Acosta, J. Nunn, and B. J. Sussman, Quantum memories: emerging applications and recent advances, *Journal of Modern Optics* **63**, 2005 (2016), PMID: 27695198.
- [13] Z. Yuan, A. Plews, R. Takahashi, K. Doi, W. Tam, A. W. Sharpe, A. R. Dixon, E. Lavelle, J. F. Dynes, A. Murakami, M. Kujiraoka, M. Lucamarini, Y. Tanizawa, H. Sato, and A. J. Shields, 10-mb/s quantum key distribution, *Journal of Lightwave Technology* **36**, 3427 (2018).
- [14] 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**, 10.1126/sciadv.1701491 (2017).
- [15] 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, S. W. Nam, F. Marsili, M. D. Shaw, Z. Zhang, L. Wang, D. Englund, G. W. Wornell, J. H. Shapiro, and F. N. C. Wong, Photon-efficient quantum key distribution using time-energy entanglement with high-dimensional encoding, *New Journal of Physics* **17**, 022002 (2015).
- [16] S. Wengerowsky, S. K. Joshi, F. Steinlechner, H. Hübel, and R. Ursin, An entanglement-based wavelength-multiplexed quantum communication network, *Nature* **564**, 225 (2018).
- [17] D. N. Klyshko, Use of two-photon light for absolute calibration of photoelectric detectors, *Soviet Journal of Quantum Electronics* **10**, 1112 (1980).
- [18] R. S. Bennink, Optimal collinear gaussian beams for spontaneous parametric down-conversion, *Physical Review A* **81**, 053805 (2010).
- [19] P. W. Shor and J. Preskill, Simple proof of security of the bb84 quantum key distribution protocol, *Phys. Rev. Lett.* **85**, 441 (2000).
- [20] HC Photonics, “GRIIRA and Laser damage”, <https://drive.google.com/file/d/1qW05mq6-btPuY5uJjaCQ0qEJRAyIHH5P/view>.
- [21] Recommendation ITU-T G.694.1 (2020), “Spectral grids for WDM applications: DWDM frequency grid”.
- [22] Despite efforts to create quantum memories at terahertz bandwidths [29], most current quantum memories exhibit bandwidths of 5 GHz and below [12].
- [23] S. K. Joshi, D. Aktas, S. Wengerowsky, M. Lončarić, S. P. Neumann, B. Liu, T. Scheidl, G. C. Lorenzo, Ž. Samec, L. Kling, A. Qiu, M. Razavi, M. Stipčević, J. G. Rarity, and R. Ursin, A trusted node-free eight-user metropolitan quantum communication network, *Science Advances* **6**, 10.1126/sciadv.aba0959 (2020).
- [24] M. Perrenoud, M. Caloz, E. Amri, C. Autebert, C. Schoenenberger, H. Zbinden, and F. Bussières, Operation of parallel snspd at high detection rate, *Superconductor Science and Technology* (2020).
- [25] T. M. Rambo, A. R. Conover, and A. J. Miller, 16-element superconducting nanowire single-photon detector for gigahertz counting at 1550-nm (2021), arXiv:2103.14086 [quant-ph].
- [26] 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, G. M. Crouch, A. E. Dane, T. Gerrits, A. E. Lita, F. Marsili, G. Moody, C. Peña, E. Ramirez, J. D. Rezac, N. Sinclair, M. J. Stevens, A. E. Velasco, V. B. Verma, E. E. Wollman, S. Xie, D. Zhu, P. D. Hale, M. Spiropulu, K. L. Silverman, R. P. Mirin, S. W. Nam, A. G. Kozorezov, M. D. Shaw, and K. K. Berggren, Demonstration of sub-3 ps temporal resolution with a superconducting nanowire single-photon detector, *Nature Photonics* **14**, 250 (2020).
- [27] M. Fejer, G. Magel, D. Jundt, and R. Byer, Quasi-phase-matched second harmonic generation: Tuning and tolerances, *IEEE Journal of Quantum Electronics* **28**, 2631 (1992).
- [28] H.-K. Lo, H. F. Chau, and M. Ardehali, Efficient quantum key distribution scheme and a proof of its unconditional security, *Journal of Cryptology* **18**, 133 (2005).
- [29] D. G. England, P. J. Bustard, J. Nunn, R. Lausten, and B. J. Sussman, From photons to phonons and back: A thz optical memory in diamond, *Phys. Rev. Lett.* **111**, 243601 (2013).

### 3.3 Experimentally optimizing QKD rates via nonlocal dispersion compensation

This publication analyzes secure key rates of entanglement-based BBM92 protocols in fiber, depending on the chromatic dispersion the photons experience. We tune the total dispersion by making use of nonlocal dispersion compensation and observe the joint temporal distribution of the photon pairs, thus varying the possible secure key rate over a range from about 6 to 228 bits/s. These findings were essential to the dispersion compensation scheme of publication 3.4 and helped emphasize the fact that temporal detection precision is the most important parameter in present-day quantum key distribution, as can also be inquired from publication 3.1.

I contributed to the publication by designing the experiment together with Rupert Ursin, by designing and constructing the source producing the entangled photon pairs, by analyzing and plotting the data, by performing all additional calculations and trade-off predictions and by writing the paper with the help of Martin Bohmann.

# Quantum Science and Technology



PAPER

## Experimentally optimizing QKD rates via nonlocal dispersion compensation

OPEN ACCESS

RECEIVED

5 November 2020

REVISED

1 February 2021

ACCEPTED FOR PUBLICATION

12 February 2021

PUBLISHED

5 March 2021

Sebastian Philipp Neumann<sup>1,2,\*</sup> , Domenico Ribezzo<sup>1,2</sup>, Martin Bohmann<sup>1,2</sup>  and Rupert Ursin<sup>1,2,\*</sup> 

<sup>1</sup> Institute for Quantum Optics and Quantum Information Vienna, Austrian Academy of Sciences, Boltzmanngasse 3, 1090 Vienna, Austria

<sup>2</sup> Vienna Center for Quantum Science and Technology, Boltzmanngasse 5, 1090 Vienna, Austria

\* Author to whom any correspondence should be addressed.

† Current address: Istituto Nazionale di Ottica, Largo Enrico Fermi 6, 50125 Florence

E-mail: [sebastian.neumann@oeaw.ac.at](mailto:sebastian.neumann@oeaw.ac.at) and [rupert.ursin@oeaw.ac.at](mailto:rupert.ursin@oeaw.ac.at)

**Keywords:** quantum cryptography, quantum key distribution, quantum communication, nonlocal dispersion compensation, fiber telecommunication, chromatic dispersion, photonic entanglement

Original content from this work may be used under the terms of the [Creative Commons Attribution 4.0 licence](https://creativecommons.org/licenses/by/4.0/).

Any further distribution of this work must maintain attribution to the author(s) and the title of the work, journal citation and DOI.



### Abstract

Quantum key distribution (QKD) enables unconditionally secure communication guaranteed by the laws of physics. The last decades have seen tremendous efforts in making this technology feasible under real-life conditions, with implementations bridging ever longer distances and creating ever higher secure key rates. Readily deployed glass fiber connections are a natural choice for distributing the single photons necessary for QKD both in intra- and intercity links. Any fiber-based implementation however experiences chromatic dispersion which deteriorates temporal detection precision. This ultimately limits maximum distance and achievable key rate of such QKD systems. In this work, we address this limitation to both maximum distance and key rate and present an effective and easy-to-implement method to overcome chromatic dispersion effects. By exploiting entangled photons' frequency correlations, we make use of nonlocal dispersion compensation to improve the photons' temporal correlations. Our experiment is the first implementation utilizing the inherently quantum-mechanical effect of nonlocal dispersion compensation for QKD in this way. We experimentally show an increase in key rate from 6.1 to 228.3 bits/s over 6.46 km of telecom fiber. Our approach is extendable to arbitrary fiber lengths and dispersion values, resulting in substantially increased key rates and even enabling QKD in the first place where strong dispersion would otherwise frustrate key extraction at all.

### 1. Introduction

Quantum key distribution (QKD) enables communication partners to exchange messages with unconditional cryptographic security based on the laws of quantum physics rather than assumptions about computational hardness. This decisive advantage of QKD over classical encryption techniques has stimulated intensive research since its first proposal in 1984 [1]. The key challenge in state-of-the-art QKD research is the development of feasible strategies enabling the faithful distribution of quantum states of light over long distances and at high rates [2]. Glass fibers are an obvious choice for quantum communication, since existing telecommunication infrastructure can be used and links can be operated 24/7 independent of weather conditions, in contrast to satellite connections [3]. Fiber links are versatile. They can be deployed in network configurations for intra-city links over tens of kilometers [4–6] and have also been used for long-distance communication under laboratory conditions [7–9]. Only recently, in-field QKD using commercially deployed fibers has been shown over a 96 km submarine link [10]. Another in-field connection over 66 km withstood noise from classical traffic in another wavelength channel of the same fiber [11].

The performance of a QKD system is quantified by its secure key rate. Naturally, this rate can be enhanced by sending more photons per time unit, but such an increase in photon creation rate is only



beneficial as long as successively sent photons can still be unambiguously identified in time by both communication partners. If identification cannot be guaranteed with sufficient fidelity, the existence of an eavesdropper in the quantum channel cannot be ruled out anymore and no secure key is created. Chromatic dispersion in fiber however induces substantial temporal overlaps of single photons. This is because it causes photons at different parts of the photon source's wavelength spectrum to travel at different speeds in the fiber. Dispersion therefore forces experimenters to dim their single photon source to levels far below what would be technically possible [12, 13] in order to tell consecutively sent photons apart. This poses a substantial limit on the secure key rate of any fiber-based QKD protocol.

Assuming state-of-the-art detectors, this effect comes into play already for 10 km fiber links conforming to the International Telecommunication Union's most popular fiber and multiplexing standards [14–16], which we will use for all further calculations if not noted otherwise. For longer distances, the effect becomes ever more extensive, until key production is completely prevented at around 460 km fiber length, assuming entangled photons with 100 GHz spectral width (see appendix A.3). Importantly, dispersion negatively affects any QKD protocol, no matter which degree of freedom is carrying the quantum information and which particular protocol is used. This is also true for high-dimensional quantum information protocols [17] where more than one qubit per photon is transmitted. Therefore, dispersion poses a key challenge in fiber-based quantum communication, and has to be addressed by any future implementation.

Entanglement-based QKD protocols such as BBM92 [18] or device-independent protocols [19] offer a unique method of overcoming dispersion-induced performance degradation. An entangled photon pair's correlations in time and energy allow for so-called nonlocal dispersion compensation [20]. Such a compensation scheme uses the photons' (anti-)correlations in wavelength as a resource to tighten temporal correlations which have been dissolved by chromatic dispersion. Correlations in polarization, which are used for key creation in this work, are left intact in this process.

In this work, we experimentally overcome the detrimental effect of chromatic dispersion on QKD rates for the first time. In particular, we integrate a nonlocal dispersion compensation scheme into a full-fledged polarization-based BBM92 protocol over 6.46 km of telecom fiber. Canceling dispersion in this way, we enable polarization-state measurements with low error rate, thus significantly increasing the implementation's performance. In a realistic scenario of high loss, we report an increase of the secure key rate from 6.1 to 228.3 bits/s, i.e. by a factor of 37, with the method described.

## 2. Methods

### 2.1. Mitigating dispersion effects

The total timing uncertainty a QKD protocol is subjected to can be written as

$$\Delta T = \sqrt{\sigma_C^2 + \sigma_J^2 + \sigma_D^2}. \quad (1)$$

Here,  $\sigma_C$  is the photons' coherence time, which is a fundamental property related to their finite spectral width [21].  $\sigma_J$  signifies timing jitter due to imperfect detection electronics, and  $\sigma_D$  is the temporal spread due to chromatic dispersion. We assume independent normal distributions for each effect.

For photons of 100 GHz ( $\approx 0.8$  nm) spectral width at 1550 nm, the coherence time  $\sigma_C$  is less than 5 ps. This is negligible for current BBM92 applications. Regarding timing jitter  $\sigma_J$ , superconducting single-photon nanowire detectors (SSPD) are the state of the art. The lowest SSPD jitter values reported today are in the order of 5 ps for telecom wavelengths [22], while commercial devices including time-tagging electronics typically exhibit jitters of 40 ps [23–25]. The steady advancements in nanowire technology, however impressive they may be, can nonetheless only be put to use in entanglement-based QKD if chromatic dispersion effects of the links can be mitigated. Without such mitigation, any reduction of  $\sigma_J$  is masked by chromatic dispersion effects. This becomes apparent when calculating  $\sigma_D$  for a fiber of length  $L$ , using the formula [21]

$$\sigma_D = \sigma_\lambda D_\lambda L, \quad (2)$$

where  $\sigma_\lambda$  is the spectral width in wavelength of the propagating signal (typically 100 GHz) and  $D_\lambda$  is the wavelength-dependent dispersion coefficient.  $D_\lambda$  takes positive (negative) values for anomalous (normal) dispersion, i.e. higher-energy photons traveling faster (slower). Glass fibers and e.g. chirped fiber Bragg gratings can be manufactured to exhibit both positive and negative dispersion coefficients [26]. For a typical  $D_\lambda = +18$  ps nm<sup>-1</sup> km<sup>-1</sup> at 1550 nm, the dispersion amounts to  $\sigma_D \approx 1400$  ps for a 100 km inter-city link. But even a comparably short 10 km link in an intra-city network such as in [4, 5] exhibits about 140 ps of dispersion spread, which already poses a problem for high-end entanglement-based QKD implementations. It is therefore of utmost importance for state-of-the-art QKD implementations to overcome dispersion effects.

Local dispersion compensation has been shown for prepare-and-send [9] as well as entanglement-based [27, 28] QKD protocols by compensating right before or after the dispersive fiber channel. For entanglement-based protocols however, there is a unique method of dispersion compensation developed by Franson [20, 29]. He proposed to carry out so-called nonlocal dispersion compensation for entangled photon pairs by changing the dispersion in the transmission channel of one photon only. In this way, we can exploit their wavelength correlations to restore temporal correlations which have been degraded due to chromatic dispersion effects. In case of wavelength anti-correlation between entangled photons produced by spontaneous parametric down-conversion (SPDC), the total  $\sigma_D$  between Alice (A) and Bob (B) is equal to the sum of the channels' individual dispersion values:

$$\sigma_D = \sigma_D^A + \sigma_D^B \quad (3)$$

$$= \sigma_\lambda (D_\lambda^A L^A + D_\lambda^B L^B). \quad (4)$$

Here,  $\sigma_\lambda$  is the photons' effective spectral width in wavelength, which is determined by the SPDC source and the filters in use. Therefore,  $\sigma_D = 0$  is possible for zero total dispersion ( $D_\lambda^A L^A = -D_\lambda^B L^B$ ), reducing  $\Delta T$  to contributions by  $\sigma_C$  and  $\sigma_J$  alone.

It is important to stress that the possibility of nonlocal dispersion compensation is a unique feature of entangled photon pairs. The continuous cancellation of dispersion by acting on one photon only has no classical counterpart and can be considered a quantum advantage. Also, it is an example of the versatility of entanglement-based QKD schemes. The correlations of entangled photons, which naturally occur in SPDC in many different degrees of freedom, can be exploited in order to enhance secure key rates without compromising the degree of freedom used for actual key creation. Entanglement can therefore be seen as a resource to further improve QKD protocols which are, in their basic form, concerned with one degree of freedom only. In our case, this allows us to use just one device to compensate for dispersion in two different single-mode fibers (SMFs) carrying the entangled photons. Thus, loss and additional complexity caused by the compensation device are the same as they would be in a single-channel experiment.

The principal feasibility of nonlocal dispersion compensation has been shown using a broad SPDC spectrum centered around the zero-dispersion wavelength of two similar fibers [30]. Also, it was used to implement one measurement basis [31] and to significantly violate Bell's inequality [32] in measurements on time-energy entangled photon pairs. In this work, we develop the scheme further to demonstrate for the first time that nonlocal dispersion compensation can in fact be used for improving secure key rates in QKD applications. We implement a full-fledged BBM92 QKD scheme based on polarization-entangled photon pairs sent along standard telecom fibers and show experimentally that by introducing negative dispersion in one channel only, tight timing correlations can be restored and key rates can be increased substantially.

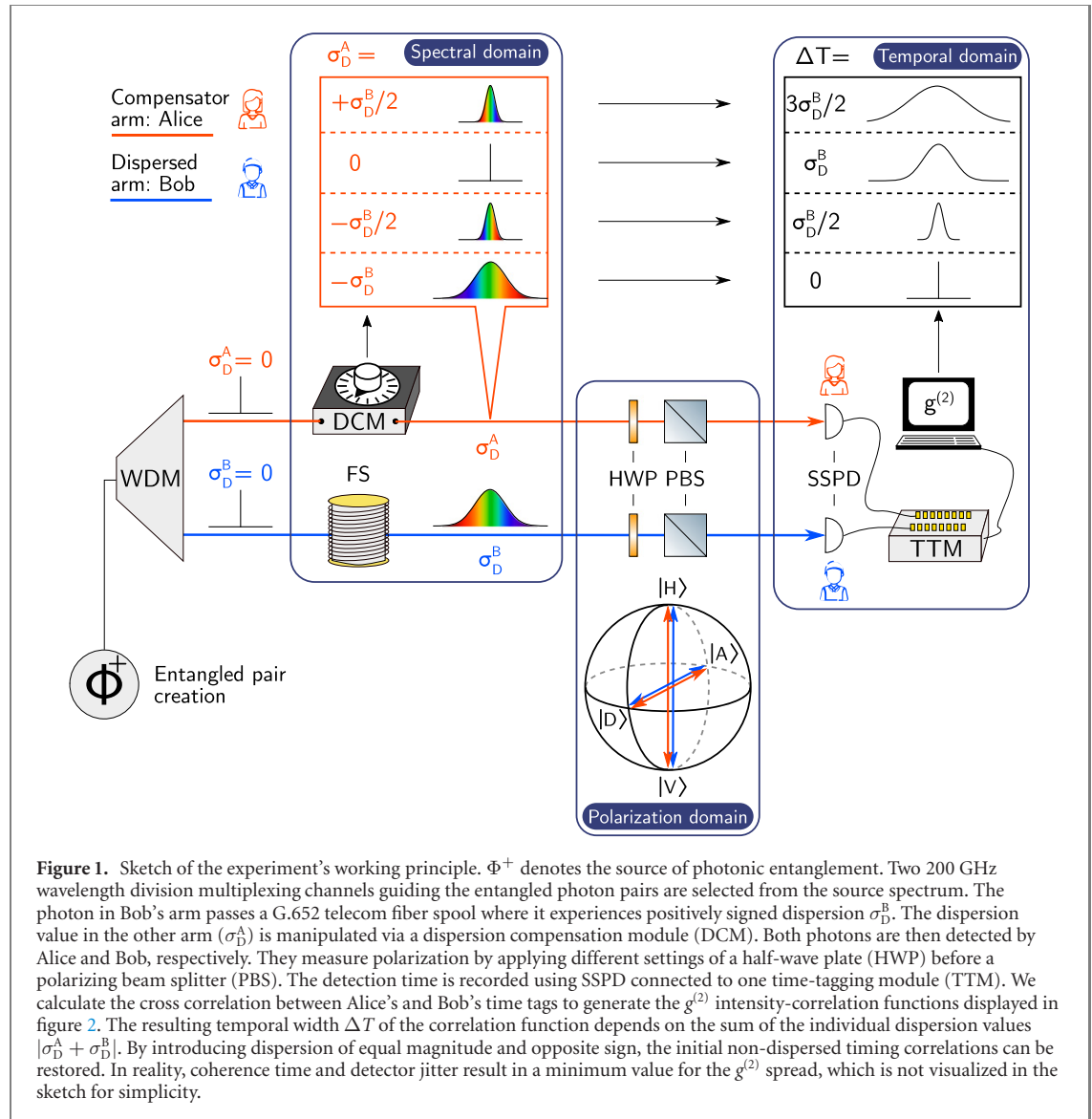
## 2.2. Experimental setup

The working principle of our experimental setup is shown in figure 1. We use a Sagnac-type source of polarization-entangled photons with a type-0 phase-matched nonlinear crystal [33]. It is pumped with a continuous-wave laser at wavelength  $\lambda_p = 775$  nm, producing photon pairs with their spectrum centered at approximately 1550 nm via SPDC. The down-converted photons are coupled into a SMF. Obeying energy conservation,  $\lambda_p \approx (\lambda_s + \lambda_i)/4$  holds for individual entangled photon-pairs, where *s* (*i*) denotes signal (idler) photons. This relation can be used to select entangled signal and idler photons from the full spectrum. To this end, we use dense wavelength division multiplexing (DWDM) top-hat filters with 200 GHz broad spectral transmission [15, 34]. With two such filters, we realize wavelength channels centered at 1549.32 and 1550.92 nm, respectively, each carrying one of the entangled photons. We align the source such that the photons in these respective color channels are maximally entangled in their polarization degree of freedom, forming the Bell state

$$\begin{aligned} |\phi^+\rangle_{\text{pol}} &= 1/\sqrt{2}(|H_s, H_i\rangle + |V_s, V_i\rangle) \\ &= 1/\sqrt{2}(|D_s, D_i\rangle + |A_s, A_i\rangle), \end{aligned} \quad (5)$$

where *H* (*V*, *D*, *A*) denotes horizontal (vertical, diagonal, antidiagonal) polarization.

The signal photons are injected into a 6.46 km long G.652 telecom fiber with  $D_\lambda = +16.7 \pm 1.0$  ps  $\text{nm}^{-1} \text{ km}^{-1}$  as specified by the manufacturer [35, 36], resulting in a calculated total dispersion of  $\sigma_D^B/\sigma_\lambda = +107.9 \pm 6.5$  ps  $\text{nm}^{-1}$ . In order to nonlocally compensate for this dispersion in Bob's arm, Alice's channel carrying the idler photons is connected to a Teraxion Clearspectrum T2506 DCM. According to the display's reading, it can introduce dispersion values  $\sigma_D^A/\sigma_\lambda$  ranging from  $-170$  to  $+170$  ps  $\text{nm}^{-1}$  in 10 ps  $\text{nm}^{-1}$  steps [37].



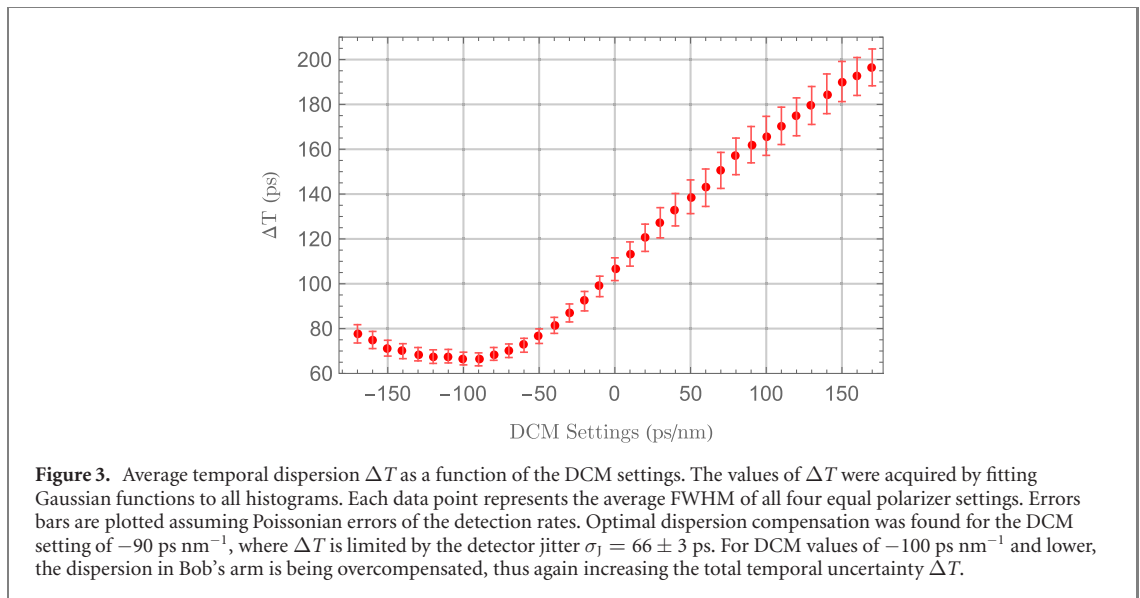
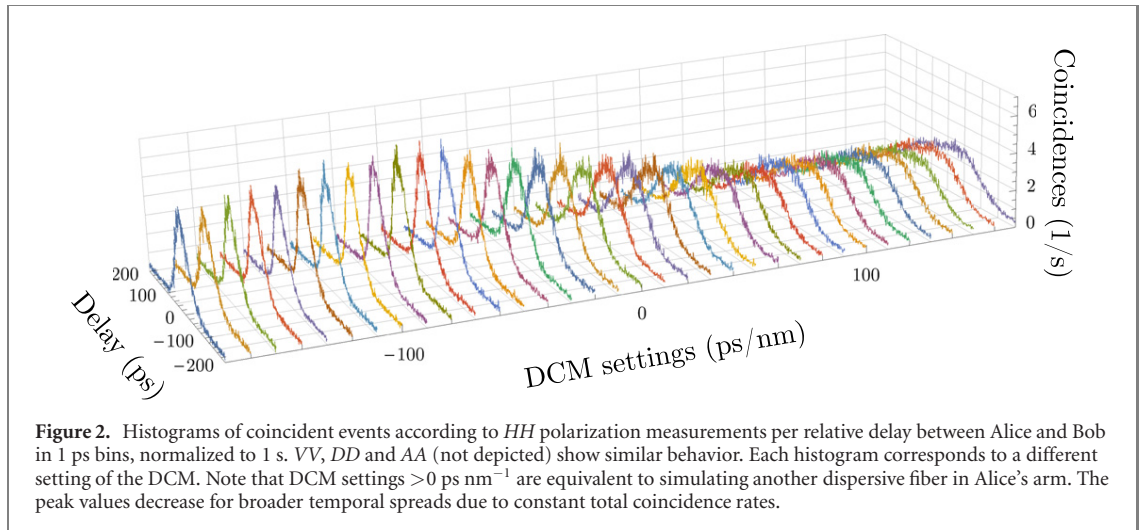
We simulate a long-distance scenario of 300 km distance in terms of loss by introducing attenuation of about 30 dB in each channel. This is done by decreasing the SMF coupling efficiency at the detectors. We calculate the loss via the Klyshko or heralding efficiency, i.e. by determining the ratio between correlated photons and all detector clicks (less noise counts) [38].

Alice and Bob determine the polarization state of their respective photons using polarization analysis modules, consisting of a HWP and a PBS, and detect the photons via SSPD of the Single Quantum Eos series connected to the same TTM Ultra 8 by Swabian Instruments. We report a constant background noise level of 160 kcps (Alice) and 175 kcps (Bob).

### 3. Results

In order to quantify the QKD protocol's performance, Alice and Bob record a time tag and the HWP's angle setting for each of their measurement events. The HWP settings correspond to different polarization measurements ( $0^\circ = H$ ,  $22.5^\circ = D$ ,  $45^\circ = V$ ,  $67.5^\circ = A$ ), where equal (orthogonal) settings at Alice and Bob correspond to correct (erroneous) results, owing to the desired Bell state described in equation (5). These measurements are carried out for different settings of the DCM.

$\Delta T$  can then be determined for each DCM setting by plotting a histogram showing the number of time tags at Alice and Bob per temporal delay between them (for  $HH$  see figure 2). The full width at half-maximum (FWHM) of these histograms corresponds to  $\Delta T$ . We clearly observe dispersion-induced changes of  $\Delta T$  when tuning the DCM settings over their full range of  $-170$  to  $+170$  ps nm $^{-1}$ . The positively signed temporal dispersion  $\sigma_D^B$  of the fiber can be counteracted by introducing negative dispersion



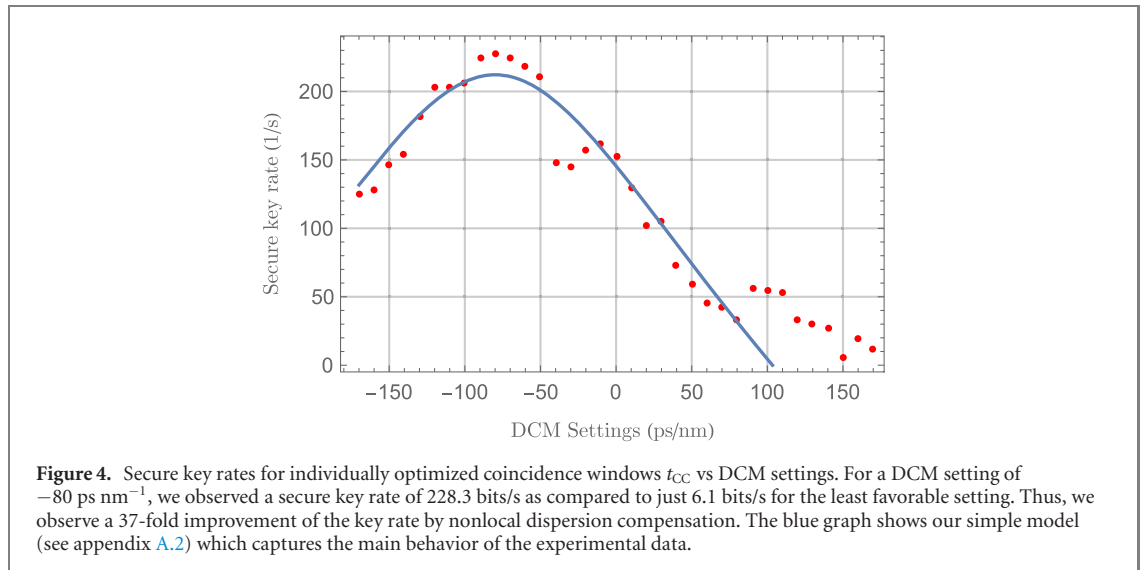
coefficients in the DCM, reducing  $\Delta T$  to contributions from detector jitter and coherence time only. Setting the DCM to positive dispersion values however simulates a long-distance fiber link in Alice's channel, thus further increasing  $\Delta T$ .

Figure 3 shows the average FWHMs of all correct correlations for each of these DCM settings, which we extracted from Gaussian fits to the experimental data. The minimal value of  $\Delta T = 66 \pm 3$  ps was found for a DCM display reading of  $-90$  ps nm $^{-1}$ . The mismatch with the calculated location of the minimal value at  $-107.9$  ps nm $^{-1}$ , which amounts to a 5% deviation in the considered range, can be explained by DCM imperfections and/or deviations of the fiber's dispersion specification.

Summarizing, we were able to tune  $\Delta T$  from 66 to 197 ps with our method, inducing both normal and anomalous dispersion in Alice's arm. Such dispersion manipulation of entangled photon pairs must be understood as a nonlocal process [29]. This is because the dispersion we introduced in Bob's arm was compensated for by changing solely the dispersion in Alice's arm, while Bob's dispersion value stayed constant.

#### 4. Discussion

We will now investigate the secure key rate implications of these dispersion-induced changes to  $\Delta T$ . For the above histograms, only correct polarization correlations were used to determine  $\Delta T$ , since the erroneous ones mainly consist of the noise floor due to high fidelity of our entangled state. For carrying out the actual QKD protocol however, all correlations have to be used, since Alice and Bob must not publicly communicate their polarization measurement outcomes, but only their time tags and basis choices. Once



they have done so, they have to agree on a delay including a tolerance interval, the so-called ‘coincidence window’  $t_{CC}$ , to define those events that are used for key creation (‘coincidences’). Naturally, the optimal choice of  $t_{CC}$  in terms of secure key rate strongly depends on  $\Delta T$  of the acquired histograms: if the histogram is flattened due to dispersion, one is forced to use a larger  $t_{CC}$  in order to collect as many coincidences as possible. The number of erroneous detection events however increases proportionally to  $t_{CC}$ , therefore inflating the quantum bit error rate. This explains the behavior of the secure key rate as shown in figure 4. Here, we calculated the maximal secure key rate for every setting of the DCM module as the average of horizontal-vertical and diagonal-antidiagonal basis settings. We numerically optimized  $t_{CC}$  to acquire the highest possible secure key rate for each DCM setting individually (see appendix A.1). The overall maximal secure key rate of 228.3 bits/s is found for the DCM setting at  $-80 \text{ ps nm}^{-1}$ . Compared to the lowest acquired value of 6.1 bits/s, our nonlocal dispersion compensation scheme therefore resulted in a 37-fold increase in secure key rate.

This demonstrates the detrimental effect of dispersion and its overcoming by nonlocal dispersion compensation. The dispersion-induced degradation of our QKD system’s error rate could be annihilated with our method. Furthermore, the observed overall behavior is in good agreement with our theoretical model as can be seen in figure 4. Also note that conventional compensation of dispersion in both channels would require the use of *two* lossy DCM modules. Assuming a hypothetical second module with the same attenuation of 4.56 dB, calculations using our model show that the maximum obtainable key rate would only have been 38.9 bits/s in such a *local* dispersion compensation case. Details on the model are provided in appendix A.2.

We have shown that chromatic dispersion acting on an entangled photon pair can be compensated in a nonlocal manner by manipulating only the dispersion experienced by one of the two entangled photons. Doing so, the tight original timing correlations of the entangled source’s emission process can be retrieved by exploiting their non-degraded wavelength anticorrelations. To the best of our knowledge, this is the first experimental demonstration of improving secure key rates in QKD via nonlocal dispersion compensation.

## 5. Conclusion

We have devised a QKD implementation over a 6.46 km fiber link and successfully managed to increase the resulting secure key rates by compensating for chromatic dispersion in a nonlocal manner. Utilizing wavelength anticorrelations of polarization-entangled photons to counteract temporal broadening, we have shown a 37-fold gain of key rates compared to the least favorable dispersion configuration. For this nonlocal compensation scheme, a ready-to-use off-the-shelf DCM and patch fibers were deployed, with no need for further alignment of sensitive components. Additionally, our experiment was designed to match real-life loss scenarios. Since one device is enough to compensate a two-channel QKD scheme, the DCM insertion loss is the same as it would be in a single-channel experiment. The scheme is therefore ideally suited for real-world applications.

Our findings can easily be generalized to substantially longer fiber links, where control of dispersion is a prerequisite for obtaining high key rates or even any key at all. Taking a 400 km link as an example, the

secure key rate can be increased by a factor of 400 to about 10 bits/s with our method. This estimate is ignoring noise counts, e.g., from parallel classical traffic, which would increase the necessity of tight timing correlations even further. Since excellent timing precision is obligatory for state-of-the-art QKD, our scheme can help to enhance any in-fiber entanglement-based QKD system. It is straightforward to adapt it to high-dimensional entanglement or other degrees of freedom, e.g. time-energy entanglement. Concluding, we are convinced that the nonlocal dispersion compensation scheme presented in this work will be an essential component for future implementations of fiber-based QKD networks.

### Author contributions

SN and RU devised the experiment. SN and DR built the measurement setup. DR collected measurement data. SN, DR and MB analyzed the data. RU supervised the work. SN, MB and RU contributed to write the paper.

### Conflict of interests

The authors declare no conflict of interests.

### Acknowledgments

We acknowledge European Union's Horizon 2020 Programme Grant agreement No. 857156 (OpenQKD) and the Austrian Academy of Sciences. We also want to thank Josef Vojtech of CESNET (Prague) for providing us with dispersion compensation equipment, Siddarth Koduru Joshi of NSQI (Bristol) for lending us a DWDM device and Sören Wengerowsky of IQOQI (Vienna) for fruitful discussions.

### Data availability statement

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

## Appendix A

### A.1. Secure key rate calculation

To quantify the improvements achieved by our dispersion compensation scheme, we calculated the secure key rate in the asymptotic limit of infinite key size for each DCM setting. In order to do so, one first needs to calculate the quantum bit error rate (QBER,  $E$ ) [2], which is defined as the ratio of erroneous coincidences to total coincidences. It can be written as

$$E = \frac{CC_{\text{err}}}{CC_{\text{corr}} + CC_{\text{err}}}, \quad (\text{A.1})$$

where  $CC_{\text{err}}$  ( $CC_{\text{corr}}$ ) is the number of erroneous (correct) coincidences per second. Using  $E$ , one can calculate the lower bound for the secure key rate  $R_s$  in the infinite-key limit is using the formula [39]

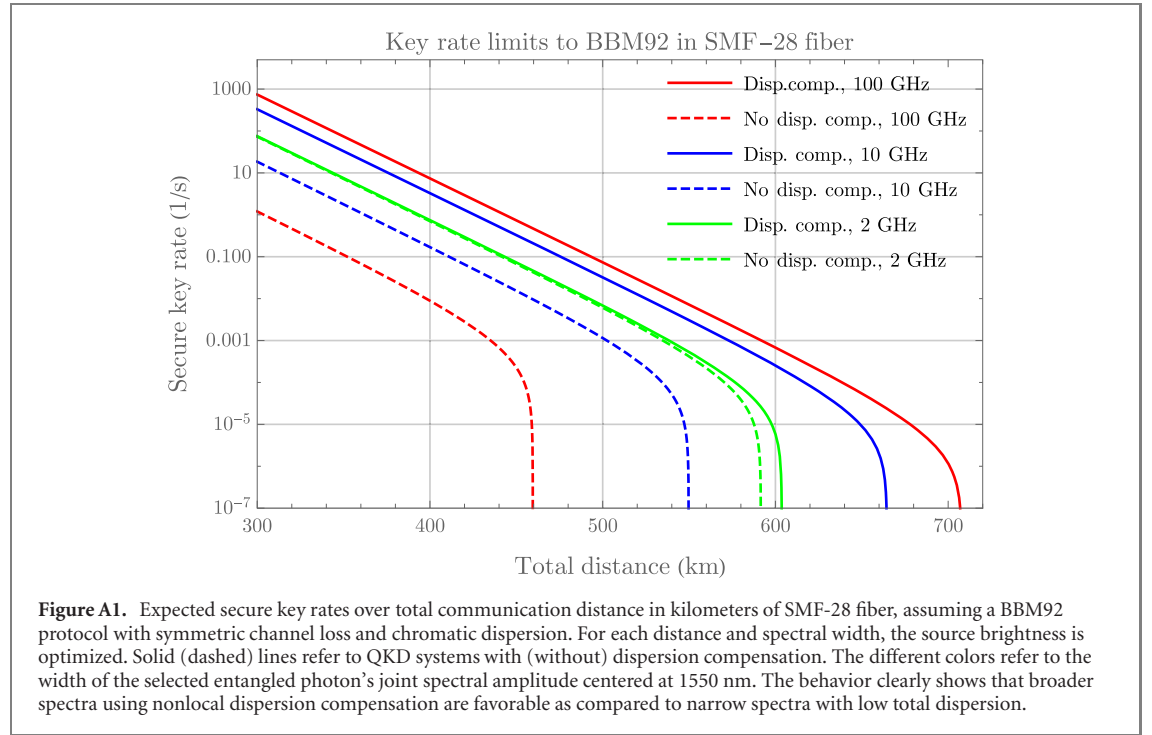
$$R_s = CC_{\text{tot}} \cdot (1 - (1 + f)H_2(E)). \quad (\text{A.2})$$

Here,  $CC_{\text{tot}} = CC_{\text{corr}} + CC_{\text{err}}$  is the total number of coincidences per second,  $f = 1.1$  [40] is the bi-directional error correction efficiency and  $H_2(x)$  is the binary entropy function [39].  $CC_{\text{corr}}$  and  $CC_{\text{err}}$  both depend on the chosen coincidence window  $t_{\text{CC}}$ , which has been determined numerically to optimize  $R_s$  for each DCM setting.

### A.2. Fitting model

The blue curve in figure 4 represents our model of the secure key rate behavior depending on the DCM settings. For this model,  $CC_{\text{tot}}$  in equation (A.2) is calculated using the source brightness  $B$ , channel losses  $\eta_i$ , and a correction factor  $s$  (ignoring noise counts):

$$CC_{\text{tot}} = sB\eta_A\eta_B. \quad (\text{A.3})$$



The QBER  $E$  in equations (A.1) and (A.2) is modeled as

$$E = \frac{sB\eta_A\eta_B e_o + \xi/2}{sB\eta_A\eta_B + \xi}, \quad (\text{A.4})$$

where  $e_o$  is the probability of erroneous detection due to optical imperfections of source and polarization analyzers,  $DC_i$  are the noise counts per detector and

$$\xi = (B\eta_A + 2DC_A)(B\eta_B + 2DC_B)\sqrt{\sigma_C^2 + \sigma_J^2 + \sigma_D^2} \quad (\text{A.5})$$

is the rate of coincident counts which arise by chance due to the finite coincidence window  $t_{CC}$  and not due to an actual photon pair.  $\xi$  is divided by 2 in the numerator of equation (A.4) because only half of these 'accidental' clicks contribute to erroneous coincidences with orthogonal polarizer settings and the other half is registered as correct. For simplicity, we do not account for the numerical optimization of the coincidence window in our model, but set  $t_{CC} = \Delta T$ . The factor  $s = \text{erf}[\sqrt{\ln(2)}] = 0.76$  in equations (A.3) and (A.4) accounts for the fact that true coincidence clicks originating from photon pairs follow a Gaussian distribution with FWHM  $\Delta T$ , i.e. clicks outside the coincidence window at the 'tails' of the distribution are lost.

Figure 4 shows this key rate model for the following parameters in use:  $B = 5.75 \times 10^8$  cps,  $\eta_1 = 29.05$  dB,  $\eta_2 = 29.31$  dB,  $DC_1 = 1.4 \times 10^5$  cps,  $DC_2 = 1.75 \times 10^5$  cps,  $e_o = 0.01$ ,  $\sigma_J = 66$  ps,  $\sigma_C = 0$  ps. All modeling parameters were estimated from experimental data. The model was offset by  $-80$  ps in order to fit the data, although we expected optimal compensation to take place at  $-90$  ps. This discrepancy is most likely due to statistical fluctuations in the measured count rates and will be subject of future studies. Further deviations between our model and the observed  $R_s$  can be explained by the fact that our simple model does not capture the numerically obtained optimal coincidence windows, which is especially important for low key rates, and that all underlying distributions were assumed to be perfectly Gaussian for simplicity. Nevertheless, we observe that our model correctly captures the main features of the experimentally obtained key rates and thus explains the functional dependence of secure key rate on nonlocal dispersion compensation.

### A.3. Improvements using non-local dispersion compensation over long distances

Using the model introduced above, we estimate the maximum achievable distance and key rate for a fiber-based BBM92 system along standard SMF-28 fiber. Figure A1 shows calculations for identical fiber channels from source to Alice and Bob, with attenuation of  $0.2$  dB  $\text{km}^{-1}$  and  $+18$  ps  $\text{km}^{-1}$   $\text{nm}^{-1}$  chromatic dispersion. We assume state-of-the-art parameters for all curves: dark counts  $DC = 100$  cps per detector, 1% optical error  $e_o$  and 20 ps detector jitter  $\sigma_J$ . Brightness values  $B$  are optimized for each curve

individually, with values ranging from  $6.6 \times 10^6$  to  $2.5 \times 10^9$  cps. Different spectral widths of the photons lead to different efficiencies of our non-local dispersion compensation scheme. If the photons are narrowly filtered, dispersion contributes much less to  $\Delta T$  than coherence time (see equation (1)). Thus, in the case of an optimal time-bandwidth product at 2 GHz, dispersion compensation can only marginally increase key rate and maximal communication distance. The broader the spectrum however, the more key rate and maximum distance can be gained with our scheme, and the 2 GHz case can be outperformed: for 10 GHz (100 GHz), the maximum distance is increased by 115 km (250 km). Also key rates can be increased substantially. Optimizing for 300 km distance, dispersion compensation allows for a gain in key rate from 5 to 1036 bits/s in the 100 GHz case and from 49 to 438 bits/s with 10 GHz. Broader photon spectra allow for a higher maximum key rate when using dispersion compensation, since one is not limited by long coherence times. In addition to enhanced performance, using broad spectra also has the advantage of substantially less complex source designs. This is because sources of photonic entanglement that exhibit both narrow photon spectra and high brightness require the use of cavities and/or waveguides [41].

## ORCID iDs

Sebastian Philipp Neumann  <https://orcid.org/0000-0002-5968-5492>

Martin Bohmann  <https://orcid.org/0000-0003-3857-4555>

Rupert Ursin  <https://orcid.org/0000-0002-9403-269X>

## References

- [1] Bennett C H and Brassard G 1984 Quantum cryptography: public key distribution and coin tossing *Int. Conf. on Computers, Systems and Signal Processing* (Bangalore, India December 1984) pp175–9
- [2] Xu F, Ma X, Zhang Q, Lo H-K and Pan J-W 2020 Secure quantum key distribution with realistic devices *Rev. Mod. Phys.* **92** 025002
- [3] Yin J et al 2020 Entanglement-based secure quantum cryptography over 1,120 kilometres *Nature* **582** 501–5
- [4] Joshi S K et al 2019 A trusted-node-free eight-user metropolitan quantum communication network (arXiv:1907.08229)
- [5] Dynes J F et al 2019 Cambridge quantum network *npj Quantum Inf.* **5** 101
- [6] Bacco D et al 2019 Field trial of a three-state quantum key distribution scheme in the florence metropolitan area *EPJ Quantum Technol.* **6** 5
- [7] Korzh B, Lim C C W, Houlmann R, Gisin N, Li M J, Nolan D, Sanguinetti B, Thew R and Zbinden H 2015 Provably secure and practical quantum key distribution over 307 km of optical fibre *Nat. Photon.* **9** 163–8
- [8] Yin H-L et al 2016 Measurement-device-independent quantum key distribution over a 404 km optical fiber *Phys. Rev. Lett.* **117** 190501
- [9] Boaron A et al 2018 Secure quantum key distribution over 421 km of optical fiber *Phys. Rev. Lett.* **121** 190502
- [10] Wengerowsky S et al 2019 Entanglement distribution over a 96-km-long submarine optical fiber *Proc. Natl Acad. Sci. USA* **116** 6684–8
- [11] Mao Y et al 2018 Integrating quantum key distribution with classical communications in backbone fiber network *Opt. Express* **26** 6010–20
- [12] Steinlechner F, Ramelow S, Jofre M, Gilaberte M, Jennewein T, Torres J P, Mitchell M W and Pruneri V 2013 Phase-stable source of polarization-entangled photons in a linear double-pass configuration *Opt. Express* **21** 11943–51
- [13] Meyer-Scott E, Prasanna N, Eigner C, Quiring V, Donohue J M, Barkhofen S and Silberhorn C 2018 High-performance source of spectrally pure, polarization entangled photon pairs based on hybrid integrated-bulk optics *Opt. Express* **26** 32475–90
- [14] International Telecommunication Union recommendation G.652 (11/16) 2017 <https://www.itu.int/rec/T-REC-G.652-201611-1/en>
- [15] International Telecommunication Union recommendation G.694.1 (12/2003) 2012 <https://www.itu.int/rec/T-REC-G.694.1-201202-1/en>
- [16] Warier S 2018 *Engineering Optical Networks* (Boston, MA: Artech House Publishers)
- [17] Cozzolino D, Da Lio B, Bacco D and Oxenløwe L K 2019 High-dimensional quantum communication: benefits, progress, and future challenges *Adv. Quantum Technol.* **2** 1900038
- [18] Bennett C H, Brassard G and Mermin N D 1992 Quantum cryptography without Bell's theorem *Phys. Rev. Lett.* **68** 557
- [19] Acín A, Brunner N, Gisin N, Massar S, Pironio S and Scarani V 2007 Device-independent security of quantum cryptography against collective attacks *Phys. Rev. Lett.* **98** 230501
- [20] Franson J D 1992 Nonlocal cancellation of dispersion *Phys. Rev. A* **45** 3126
- [21] Teich M C and Saleh B E A 2007 *Fundamentals of Photonics* 2nd edn (New York: Wiley)
- [22] Korzh B et al 2020 Demonstration of sub-3 ps temporal resolution with a superconducting nanowire single-photon detector *Nat. Photon.* **14** 250–5
- [23] Single Quantum 2020 Single Quantum Eos SNSPD closed-cycle system data sheet <https://singlequantum.com/wp-content/uploads/2019/05/Single-Quantum-Eos.pdf>.
- [24] ID Quantique 2020 ID Quantique ID281 superconducting nanowire system data sheet [https://marketing.idquantique.com/acton/attachment/11868/f-023b/1/-/-/-/ID281\\_Brochure.pdf](https://marketing.idquantique.com/acton/attachment/11868/f-023b/1/-/-/-/ID281_Brochure.pdf).
- [25] Swabian Instruments 2020 Swabian Instruments time tagger series <https://swabianinstruments.com/static/downloads/TimeTagger.pdf>.
- [26] Ramachandran S 2007 *Fiber Based Dispersion Compensation (Optical and Fiber Communications Reports)* (Berlin: Springer)
- [27] Fasel S, Gisin N, Ribordy G and Zbinden H 2004 Quantum key distribution over 30 km of standard fiber using energy-time entangled photon pairs: a comparison of two chromatic dispersion reduction methods *Eur. Phys. J. D* **30** 143–8



- [28] Aktas D, Fedrici B, Kaiser F, Lunghi T, Labonté L and Tanzilli S 2016 Entanglement distribution over 150 km in wavelength division multiplexed channels for quantum cryptography *Laser Photon. Rev.* **10** 451–7
- [29] Franson J D 2009 Nonclassical nature of dispersion cancellation and nonlocal interferometry *Phys. Rev. A* **80** 032119
- [30] Grieve J A, Shi Y, Poh H S, Kurtsiefer C and Ling A 2019 Characterizing nonlocal dispersion compensation in deployed telecommunications fiber *Appl. Phys. Lett.* **114** 131106
- [31] Lee C *et al* 2014 Entanglement-based quantum communication secured by nonlocal dispersion cancellation *Phys. Rev. A* **90** 062331
- [32] Zhong T and Wong F N C 2013 Nonlocal cancellation of dispersion in Franson interferometry *Phys. Rev. A* **88** 020103
- [33] Gayer O, Sacks Z, Galun E and Arie A 2008 Temperature and wavelength dependent refractive index equations for MgO-doped congruent and stoichiometric LiNb<sub>3</sub> *Appl. Phys. B* **91** 343–8
- [34] Grobe K 2008 *Wavelength Division Multiplexing (A Practical Engineering Guide. Wiley Series in Pure and Applied Optics)* 1st edn (New York: Wiley)
- [35] Fionec GmbH Personal Communication with Dr.-Ing. Frank Depiereux. 2020
- [36] Single Quantum 2020 Corning SMF 28 ultra optical fiber product information <https://singlequantum.com/wp-content/uploads/2019/05/Single-Quantum-Eos.pdf>.
- [37] Unfortunately, we cannot give more detailed information about the device, since production is discontinued by the manufacturer and neither data sheet nor manual are available to us.
- [38] Klyshko D N 1980 Use of two-photon light for absolute calibration of photoelectric detectors *Sov. J. Quantum Electron.* **10** 1112–7
- [39] Ma X, Fung C-H F and Lo H-K 2007 Quantum key distribution with entangled photon sources *Phys. Rev. A* **76** 012307
- [40] Elkouss D, Leverrier A, Alléaume R and Boutros J J 2009 Efficient reconciliation protocol for discrete-variable quantum key distribution *IEEE Int. Symp. on Information Theory, ISIT 2009* (IEEE) pp 1879–83
- [41] Anwar A, Perumangatt C, Steinlechner F, Jennewein T and Ling A 2020 Entangled photon-pair sources based on three-wave mixing in bulk crystals (arXiv:2007.15364)

### **3.4 Continuous entanglement distribution over a transnational 248 km fiber link**

This paper can be considered the main work of this thesis, since all other publications essentially helped in designing and operating this final experiment. In it, we report on a long-distance fiber connection carrying polarization-entangled photon pairs, thereby overcoming high loss, chromatic dispersion and polarization drifts. The mathematical model developed in publication 3.1 can be considered the foundation of this experiment, since it was used to assess its final design and operation parameters. At the heart of this work lies the high-brightness source of polarization-entangled photon pairs, which is described in detail in paper 3.2. Publication 3.3 reports on our findings and observations when carefully analyzing the effect of chromatic dispersion, which the long-distance fiber connection of this publications suffers from, and developing strategies to overcome it.

I contributed to the paper by designing the experiment with Rupert Ursin, Lukas Bulla and Martin Bohmann, by helping Rupert Ursin to acquire the necessary fiber connections, by designing and constructing the source of entangled photon pairs, the detection modules, and the chromatic dispersion stage, by operating the link together with Alexander Buchner, by taking and analyzing the data with Lukas Bulla, by plotting all graphs and by writing the paper.

## **Continuous entanglement distribution over a transnational 248 km fibre link**

Sebastian Philipp Neumann<sup>1,2 \*</sup>, Alexander Buchner<sup>1,2</sup>, Lukas Bulla<sup>1,2</sup>, Martin Bohmann<sup>1,2</sup> & Rupert Ursin<sup>1,2 \*</sup>

<sup>1</sup> *Institute for Quantum Optics and Quantum Information Vienna, Boltzmannngasse 3, 1090 Vienna*

<sup>2</sup> *Vienna Center for Quantum Science and Technology, Boltzmannngasse 5, 1090 Vienna, Austria*

\* Corresponding authors: [sebastian.neumann@oeaw.ac.at](mailto:sebastian.neumann@oeaw.ac.at), [rupert.ursin@oeaw.ac.at](mailto:rupert.ursin@oeaw.ac.at)

**Entanglement is the basis of many quantum applications [1–8]. The technically most mature of them, quantum key distribution [9–11], harnesses quantum correlations of entangled photons to produce cryptographic keys of provably unbreakable security [12, 13]. A key challenge in this context is the establishment of continuously working, reliable long-distance distributions of entanglement. However, connections via satellites [14, 15] don't allow for interruption-free operation, and deployed fibre implementations have so far been limited to less than 100 km by losses [16], a few hours of duty time [17, 18], or use trusted nodes [19]. Here, we present a continuously working international link between Austria and Slovakia, directly distributing polarization-entangled photon pairs via 248 km of deployed telecommunication fibre. Despite 79 dB loss, we measure stable pair rates of  $9 \text{ s}^{-1}$  over an exemplary operation time of 110 hours. We mitigate multi-pair detections with strict temporal filtering, enabled by nonlocal compensation of chromatic dispersion. Fully automatized active polarization stabilization keeps the entangled state's visibility at 86% for altogether 82 hours, producing 403 kbit of quantum-secure key at a rate of 1.4 bits/s. Our work paves the way for low-maintenance, ultra-stable quantum communication over long distances, independent of cloud coverage and time of day, thus constituting an important step towards the quantum internet.**

Fibre-based QKD systems offer stable operation, independence from meteorological conditions, substantially reduced maintenance effort and the use of already deployed telecommunication infrastructure. These advantages can compensate for their higher losses [20] compared to satellite connections. Therefore, while intercontinental quantum connections will most likely be operated using satellites, shorter distances of several hundred kilometres can be covered by fibre links [19, 21]. Metropolitan fibre networks deploying entanglement-based QKD additionally have the advantage of allowing to fully connect many users in a straightforward fashion [17, 22], potentially on fibres used for internet traffic, wavelength-multiplexed with the classical signal [23]. Nevertheless, losses in the fibres, imperfect preparation of entangled states, chromatic dispersion, polarization mode dispersion, and timing precision in the detection of single photons hinder stable operation over long distances.

Up until today, the longest distance for entanglement distribution in deployed fibre was along a single 96 km fibre between Malta and Sicily [16]; additionally, the same submarine cable was used for a round-trip connection of altogether 192 km [24]. The longest uninterrupted operation of entanglement distribution, using active stabilization, has been demonstrated to work for 6 hours along a deployed 10-km-link [18].

In this work, we combine state-of-the-art equipment and optimal exploitation of our polarization-entangled photons' quantum properties to demonstrate continuously operated entanglement distribution along a record distance of 248 km of deployed telecom fibre, connecting Bratislava in Slovakia and St. Pölten via Vienna in Austria. Additionally, we show, for the first time, ground-based entanglement distribution for QKD in a real-life two-channel configuration, while one channel crosses the international border between Austria and Slovakia without any intermediary trusted nodes. Despite unprecedented total loss of 79 dB, we achieve entangled pair rates of

9 s<sup>-1</sup> and secure key rates of 1.4 bits/s on average. We continuously operate the link for a record of 110 hours by actively stabilizing the polarization in a highly efficient, nonlocal way, achieving a duty cycle of 75% and a total key of 403 kbit.

## Sender and receiver infrastructure

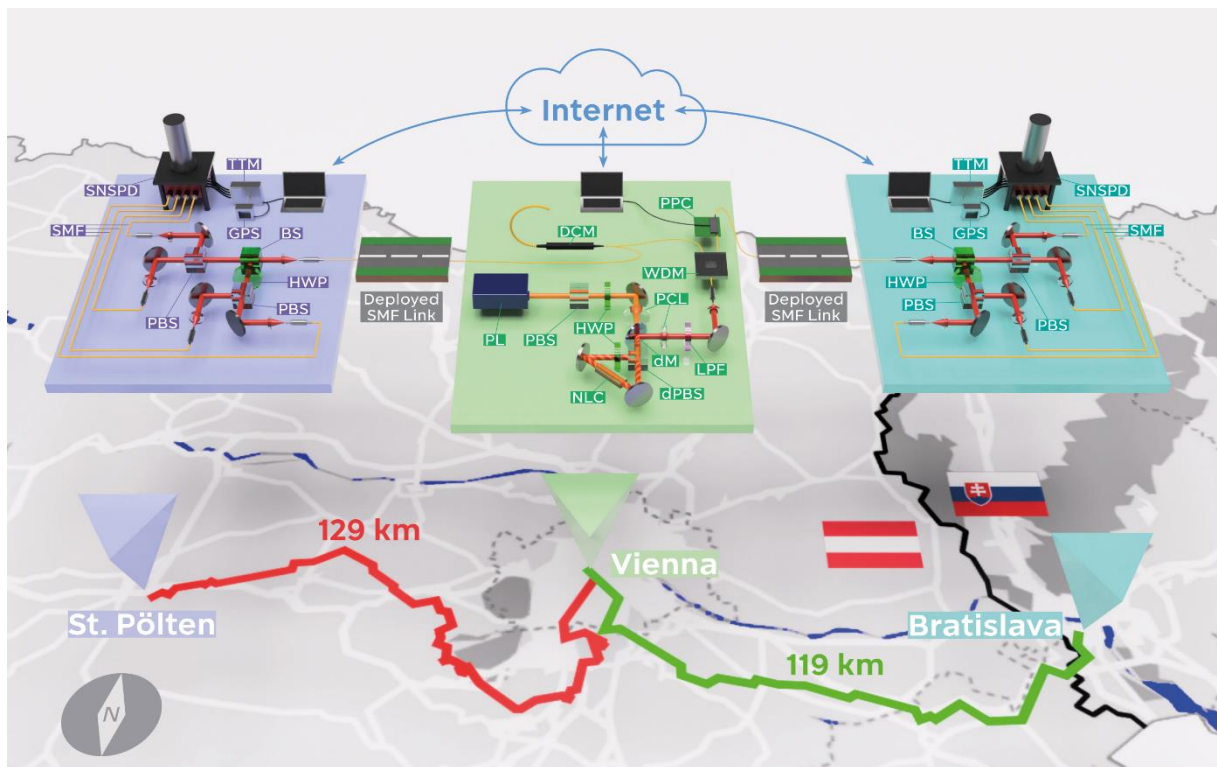


Figure 1. Sketch of the Setup. The source of entangled photon pairs is situated in Vienna. We create polarization-entangled photon pairs at two distinct telecommunication wavelengths by pumping a non-linear crystal (NLC) in a Sagnac configuration with a 775 nm laser (PL) and collecting the down-converted photons with single-mode fibres (SMF) connected to a wavelength division (de-)multiplexer (WDM). The idler photon passes a dispersion compensation module (DCM) which nonlocally recovers the entangled state's tight temporal correlations broadened by chromatic dispersion along the link. The idler is then directed along 129 km of fibre to a polarization measurement module (PMM) in St. Pölten in Lower Austria. The signal photon passes an automatized in-fibre piezo-based polarization controller (PPC) which nonlocally realigns the phase of the entangled state, should its quality decrease. Afterwards, it travels to a PMM in Bratislava of the same design as the one in Austria. In these PMMs, the photons are randomly directed to orthogonal measurements in two mutually unbiased linear polarization bases. They photons impinge on superconducting nanowire single-photon detectors (SNSPD), and a GPS-clock-disciplined time-tagging module (TTM) records detection time, measurement basis and outcome. Via classical internet connections, the two measurement stations' detection events are compared and coincidences calculated. If their quantum bit error rate increases, Vienna starts the polarization alignment. PBS: polarizing beamsplitter, HWP: half-wave plate, PL: planoconvex lens, dPBS: dichroic PBS, DM: dichroic mirror, LPF: longpass filter, BS: 50:50 beamsplitter

We implement a symmetric two-channel QKD system in a “source in the middle” configuration, following the BBM92 protocol [10] for polarization entanglement (see Fig. 1 and the Methods section). The source of entangled photon pairs is situated in Vienna, utilizing continuous-wave-pumped spontaneous parametric down-conversion

(SPDC) in a Sagnac configuration [25] and wavelength division demultiplexing (WDM) to create entangled photons of 100 GHz spectral width around 1550.12 nm with > 99% fidelity to the Bell state

$$\begin{aligned}
 |\phi^+\rangle &= 1/\sqrt{2} ( |H\rangle_{SP}|H\rangle_B + |V\rangle_{SP}|V\rangle_B ) \\
 &= 1/\sqrt{2} ( |D\rangle_{SP}|D\rangle_B + |A\rangle_{SP}|A\rangle_B ),
 \end{aligned} \tag{1}$$

where H (V, D, A) refers to horizontal (vertical, diagonal, antidiagonal) polarization.

The subscripts denote the receiver stations of the respective photon: St. Pölten in Lower Austria (SP) and the campus of the Slovakian Academy of Sciences in

Bratislava (B). The connections are realized via deployed telecom fibres of 129 and 119 km length, respectively. The receivers measure each photon's polarization state using a bulk polarization measurement module in two mutually unbiased, randomly chosen linear polarization bases (H/V or, with equal probability, D/A).

Superconducting nanowire single-photon detectors (SNSPD) connected to a time-tagging module (TTM) register each detection event. By comparing the detection times, SP and B identify the entangled photon pairs. The total transmission of each link was determined to be -40.2 dB (-38.4 dB) for the link to SP (B), including all losses and detection efficiencies. From this, it follows that an average of 8.9 pairs were detected per second between the receiver stations. We can only harness the quantum correlations of those pairwise (or "coincident") events measured in the same polarization basis. The rate of these photon pairs is called "sifted" key rate and amounted to  $4.4 \text{ s}^{-1}$  on average in our case due to our passively implemented, balanced and random basis choice. Strict temporal filtering with a width of  $t_{cc}=114 \text{ ps}$ , also called the "coincidence window", further reduces this value to  $3.8 \text{ s}^{-1}$ . Of this rate, on average 0.46 coincidences originate from accidental counts,

contributing 4.4 percent points to the quantum bit error rate (QBER), which is well below the 11.0% limit necessary to arrive at a non-zero key [26].

### **Nonlocal dispersion compensation**

To reach such a low level of accidental coincidences over our high-loss link, sufficiently high temporal detection precision is necessary, allowing for strict temporal filtering [27]. The greatest effect detrimental to timing precision in our experiment is chromatic dispersion (CD) along the fibres. CD causes photons with finite spectral distribution to disperse in time, thus spreading the entangled photons' temporal intensity correlation function  $g^{(2)}$ . In our case, optical time-domain reflectometer measurements of the link yielded a CD of 16.8 (6.0) ps/nm/km at 1550 nm for the link to St. Pölten (Bratislava). Thus, our 100-GHz-bandwidth photons would suffer from a total CD of about 1.8 ns over the full fibre stretch, which is 50 times larger than the SNSPD and TTM jitters combined. To prohibit this, we deployed a single passive dispersion compensation module (DCM) with equal and opposite CD of  $-1.8$  ns acting on the photon traveling to St. Pölten only. Such nonlocal dispersion compensation [28–30] harnesses the intrinsic quantum properties of entangled photon pairs to narrow their  $g^{(2)}$  distribution by acting on one photon of a pair only. The residual CD-induced temporal spread after compensation was masked by SNSPD jitter, TTM jitter and GPS clock drift, which we identify as the remaining contributions to the overall timing uncertainty (see Methods section).

### **Active polarization stabilization**

Besides accidental coincidence counts, erroneous polarization measurements of (correctly identified) photon pairs contribute to the QBER. While such errors can be kept below 0.4% under laboratory conditions and for short time scales [31], the nature of our experiment required active polarization stabilization of the altogether 248 km of

deployed fibres, which were subject to polarization drift [32]. Without stabilization, this drift randomly changes the phase of the Bell state in Eq. (1), such that the quantum correlations between the photons at SP and B can no longer be observed with sufficient fidelity. To guarantee long-term operation of our link despite this effect, we implemented an automatized algorithm for a piezo-based polarization controller (PPC) working on the fibre channel to Bratislava. It switched on whenever the QBER increased above 9% (see Fig. 2) and used the QBER value (calculated by B) directly as input, thus requiring no reference laser. Due to the nonlocal nature of the entangled quantum state, manipulation of just the photon in the B mode allows to arrive at the correlations of Eq. (1).

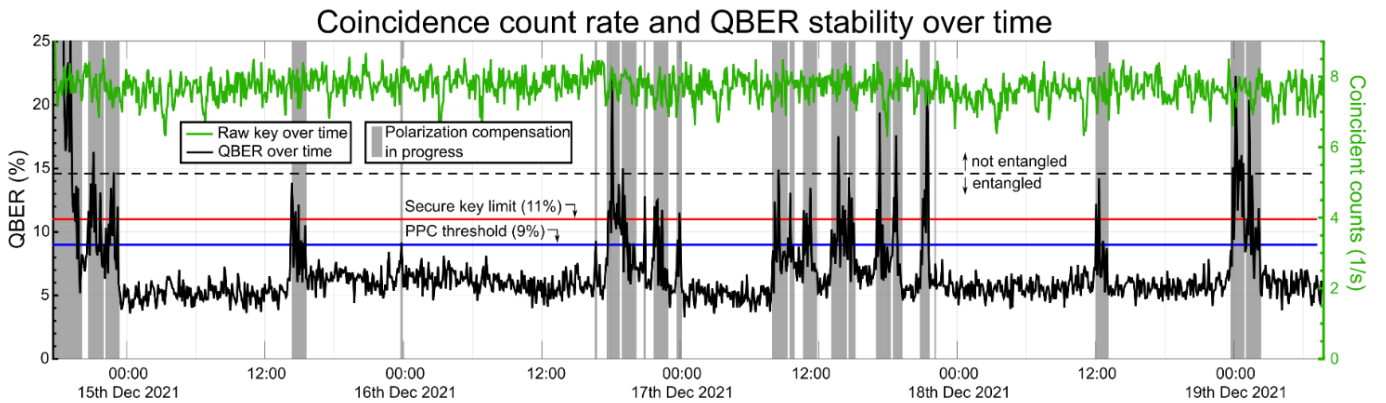


Figure 2. Quantum bit error rate (QBER) and coincident counts over time with a coincidence window of  $t_{CC} = 114$  ps. When polarization drifts along the overland fibre link increase the QBER above 9%, the piezo-based polarization controller (PPC) starts an iterative alignment procedure to reduce the QBER below 7%. The limits were chosen such that alignment is started well before the 11% limit of no key. Alignment takes between 8:10 minutes and 1:22 hours, and 57 minutes on average. We assume that the longer alignment phases are caused by polarization drift during alignment. The longest uninterrupted stable operation time amounted to 16:36 hours. The coincidence counts stay at a constant value of around  $7.7 \text{ s}^{-1}$  over the full 110 hours for  $t_{CC} = 114$  ps.

The PPC iteratively scanned the voltage for each of the four fibre-squeezing piezoelectric crystals, thus optimizing the QBER via a hill-climb algorithm. Due to the low coincidence rates, it took the algorithm 2:32 minutes on average to determine the QBER value with a precision of  $\pm 0.2\%$ . Therefore, the mean length of the alignment procedure amounted to 57 minutes along the link, rather than sub-seconds in the laboratory, where coincidence rates were in the order of  $10^4 \text{ s}^{-1}$ . While the PPC is in



operation, no key can be created, since both bit and basis information are sent via a classical internet connection. In our case, the PPC was active for altogether 27:57 of 109:55 hours, i.e., 25.4% of the time. This is equivalent to a duty cycle of 74.6% for the whole QKD scheme, with the longest uninterrupted operation time being 16 hours 37 minutes. During this duty cycle, the QBER was kept at an average of 7.0%, where we attribute 2.6% to polarization measurement errors and 4.4% to accidental coincidences (see Methods section).

### Secure key rate analysis

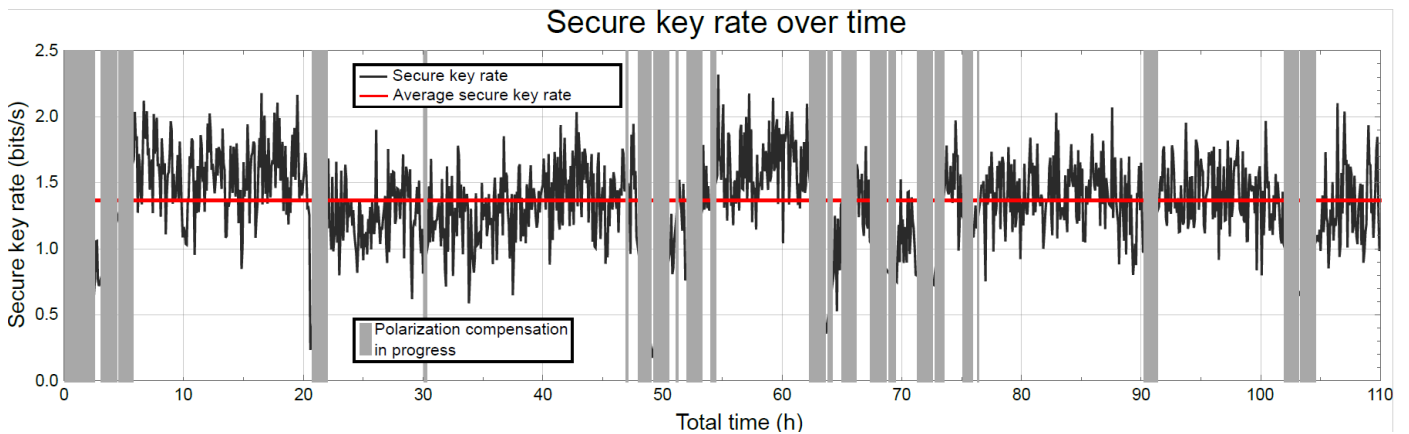


Figure 3. Secure key rate over time. As long as the quantum bit error rate (QBER) stays below 11 %, a quantum secure key can be created in principle (see Fig. 2). Our polarization alignment procedure allows to keep the QBER in the key creation regime for altogether 82 out of 110 hours of total link operation. The red line gives the average secret key rate (1.4 bits/s) calculated from all coincidences over these 82 hours. Thus, the total secure key amounts to 403 kbit, calculated with the overall, i.e. average, QBER. In black we show the secure key rate based on data acquired over 300 second time windows. Its fluctuations in the order of  $\pm 0.3$  bits/s originate from Poissonian photon statistics and polarization drifts.

To analyse the performance in a QKD setting, one has to consider the number of coincident clicks as well as their QBER. For calculation of the final key rates, we follow the formula outlined in Ref.s [26, 33] (for details see the Methods section).

Temporal filtering is of crucial importance for the final key size. Our optimal coincidence window  $t_{CC}$  amounted to 114 ps. It maximizes the total key accumulated over 110 hours of link operation: 3.1 Mbit of raw key with a QBER of 7.0% yield 403 kbit of quantum secure key, equivalent to a rate of 1.4 bits/s during the active

time of 82 hours (see Fig. 3). The obtainable maximum key rate will, due to finite-key effects, also depend on the actual running time of the link and might actually be lower if the link is operated for a short time only. To the best of our knowledge, the running time is only limited by the SNSPD maintenance cycle of about 10,000 hours.

## **Discussion and conclusion**

We have shown an ultra-stable in-fibre polarization-based entanglement distribution scheme capable of creating quantum secure keys over a length of 248 km and a time span of 110 hours, overcoming a total 79 dB of loss along two nearly symmetric fibre links. To this end, we deploy a high-brightness, high-fidelity source of entangled photon pairs at telecommunication wavelengths together with high-end SNSPD systems. We operate the link at the current limit of the state-of-the-art, which mainly originates from the precision of timing synchronization. We manage to lower it to 114 ps by non-locally compensating for the dispersion of our 100 GHz WDM channels and by the use of SNSPDs. We find coincidence rates in the order of  $7.7 \text{ s}^{-1}$  to be optimal to, on one hand, overcome loss and allow for live compensation of polarization drifts, and on the other hand to keep accidental coincidence rates sufficiently low.

Possible enhancements of our experiment could be realized by the use of several multiplexed wavelength channels, which could potentially increase the total key rates further [34]. Secondly, detection systems with lower detector jitter could allow for even stricter temporal filtering, which in turn enables higher pair production rates while keeping accidental coincidences low [27]. Thirdly, the PPC algorithm could be accelerated by automatically increasing the pump power during polarization alignment, which would yield better statistics for the QBER assessment. It might also allow for more stringent optimization, lowering the polarization-induced QBER below 1%. Fourthly, detailed trade-off calculations balancing the length of the polarization

alignment with the quality of entanglement it establishes have to be carried out to determine optimal operation parameters. Fifthly, our entanglement distribution system could be integrated in wavelength-multiplexed quantum networks [16], e.g. by implementing additional short fibre links to several users in Vienna. Sixthly, our analysis has mainly focused on QKD. The performance regarding other implementations, e.g. quantum computation or blind computing, still have to be evaluated and might have far-reaching implications.

Summarizing, our work paves the way for all kinds of continuously operated applications of quantum entanglement distributed over long fibre-distances, most notably, but not limited to, quantum key distribution.

## References

- [1] Bennett, C. H. and Wiesner, S. J., Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states, *Phys. Rev. Lett.* **69**, 2881 (1992).
- [2] Bouwmeester, D. et al., Experimental quantum teleportation, *Nature* **390**, 575 (1997).
- [3] Ma, X.-S. et al., Quantum teleportation over 143 kilometres using active feed-forward, *Nature* **489**, 269 (2012).
- [4] O'Brien, J. L., Pryde, G. J., White, A. G., Ralph, T.C. & Branning, D., Demonstration of an all-optical quantum controlled-not gate, *Nature* **426**, 264 (2003).
- [5] Jozsa, R. & Linden, N., On the role of entanglement in quantum-computational speed-up, *P. Roy. Soc. A-Math. Phys.* **459**, 2011 (2003).
- [6] Broadbent, A., Fitzsimons, J., & Kashefi, E., Universal blind quantum computation, *Ann. IEEE Symp. Found.* 517-526 (2009).
- [7] Bennett, C.H. et al., Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels, *Phys. Rev. Lett.* **70**, 1895 (1993).
- [8] Briegel, H.-J., Dür, W., Cirac, J., & Zoller, P., Quantum repeaters: The role of imperfect local operations in quantum communication, *Phys. Rev. Lett.* **81**, 5932 (1998).
- [9] Ekert, A. K., Quantum cryptography based on Bell's theorem, *Phys. Rev. Lett.* **67**, 661 (1991).
- [10] Bennett, C. H., Brassard, G., and Mermin, N. D., Quantum cryptography without Bell's theorem, *Phys. Rev. Lett.* **68**, 557 (1992).
- [11] Xu, F., Ma, X., Zhang, Q., Lo, H.-K., & Pan, J.-W., Secure quantum key distribution with realistic devices, *Rev. Mod. Phys.* **92**, 025002 (2020).
- [12] Waks, E., Zeevi, A., & Yamamoto, Y., Security of quantum key distribution with entangled photons against individual attacks, *Phys. Rev. A* **65**, 052310 (2002).
- [13] Tsurumaru, T. & Tamaki, K., Security proof for quantum-key-distribution systems with threshold detectors, *Phys. Rev. A* **78**, 032302 (2008).
- [14] Yin, J. et al., Satellite-based entanglement distribution over 1200 kilometres, *Science* **356**, 1140 (2017).
- [15] Yin, J. et al., Entanglement-based secure quantum cryptography over 1,120 kilometres, *Nature* **582**, 501 (2020).
- [16] Wengerowsky, S. et al., Entanglement distribution over a 96-km-long submarine optical fibre, *P. Natl. Acad. Sci. USA* **116**, 6684 (2019).
- [17] Joshi, S. K. et al., A trusted node-free eight-user metropolitan quantum communication network, *Sci. Adv.* **6**, 10.1126/sciadv.aba0959 (2020).
- [18] Shi, Y. et al., Stable polarization entanglement based quantum key distribution over a deployed metropolitan fibre, *Appl. Phys. Lett.* **117**, 124002 (2020).

- [19] Chen, Y.-A. et al., An integrated space-to-ground quantum communication network over 4,600 kilometres, *Nature* **589**, 214 (2021).
- [20] Liao, S.-K. et al., Satellite-to-ground quantum key distribution, *Nature* **549**, 43 (2017).
- [21] Chen, J.-P. et al., Twin-field quantum key distribution over a 511 km optical fibre linking two distant metropolitan areas, *Nat. Photonics* **15**, 570 (2021).
- [22] Wengerowsky, S., Joshi, S. K., Steinlechner, F., Hübel, H., and Ursin, R., An entanglement-based wavelength-multiplexed quantum communication network, *Nature* **564**, 225 (2018).
- [23] Dynes, J. F. et al., Cambridge quantum network, *NPJ Quantum Inf.* **5**, 101 (2019).
- [24] Wengerowsky, S. et al., Passively stable distribution of polarisation entanglement over 192 km of deployed optical fibre, *NPJ Quantum Inf.* **6**, 5 (2020).
- [25] Kim, T., Fiorentino, M. & Wong, F. N., Phase-stable source of polarization-entangled photons using a polarization Sagnac interferometer, *Phys. Rev. A* **73**, 012316 (2006).
- [26] Koashi, M. & Preskill, J., Secure quantum key distribution with an uncharacterized source, *Phys. Rev. Lett.* **90**, 057902 (2003).
- [27] Neumann, S. P. et al., Model for optimizing quantum key distribution with continuous-wave pumped entangled-photon sources, *Phys. Rev. A* **104**, 022406 (2021).
- [28] Franson, J., Nonlocal cancellation of dispersion, *Phys. Rev. A* **45**, 3126 (1992).
- [29] Grieve, J. A., Shi, Y., Poh, H. S., Kurtsiefer, C. & Ling, A., Characterizing nonlocal dispersion compensation in deployed telecommunications fibre, *App. Phys. Lett.* **114**, 131106 (2019).
- [30] Neumann, S. P., Ribezzo, D., Bohmann, M., and Ursin, R., Experimentally optimizing QKD rates via nonlocal dispersion compensation, *Quantum Sci. Technol.* **6**, 025017 (2021).
- [31] Neumann, S. P., Selimovic, M., Bohmann, M., & Ursin, R., Experimental entanglement generation for quantum key distribution beyond 1 Gbit/s (2022), *arXiv pre-print* 2107.07756 [quant-ph].
- [32] Czegledi, C. B., Karlsson, M., Agrell, E., and Johannisson, P., Polarization drift channel model for coherent fibre-optic systems, *Sci. Rep.-UK* **6**, 21217 (2016).
- [33] Ma, X., Fung, C.-H. F., and Lo H.-K., Quantum key distribution with entangled photon sources, *Phys. Rev. A* **76**, 012307 (2007).
- [34] Pseiner, J., Achatz, L., Bulla, L., Bohmann, M., & Ursin, R., Experimental wavelength-multiplexed entanglement-based quantum cryptography, *Quantum Sci. Technol.* **6**, 035013 (2021).

## **METHODS**

### **Source of entangled photon pairs**

The strong attenuation along both fibre links requires a high-brightness source of polarization-entangled photon pairs in order to achieve significant coincidence rates between the receivers. To this end, we deploy a Sagnac-type source based on spontaneous parametric down-conversion (SPDC) inside a bulk nonlinear ppLN crystal of type-0 phasematching pumped with a 775.06 nm continuous-wave Toptica laser. We choose a strong focusing parameter [31, 35] of  $\xi = 1.99$  in order to arrive at pair production rates of  $2.5 \times 10^6 \text{ s}^{-1}/\text{nm}/\text{mW}$  (before all losses). The spatially degenerate entangled photon pairs are separated from the pump via a dichroic mirror and a longpass filter and coupled into one single-mode fibre. From the source's 100 nm broad spectrum centred around 1550.12 nm, we select two 100 GHz wavelength division multiplexing (WDM) channels, using in-fibre add-drop multiplexers. The channel to SP (B) is centered at 1550.92 nm (1549.32 nm). Photons in one channel are entangled with their partner in the other channel due to energy conservation in the SPDC process [22]. The source was operated at 422 mW pump power, producing  $6.4 \times 10^8$  photon pairs per second. The source's intrinsic QBER due to erroneous polarization measurements was determined to be less than 0.4% in a laboratory environment.

### **Single-photon polarization measurement**

Two fibre links connect the source of entangled photons, located in the basement of the University of Vienna's physics institute, to two measurement stations: A Türk Telekom repeater station in Getzersdorf, part of District St. Pölten in Lower Austria (SP), and Bob at the Research Center for Quantum Information on the campus of the Slovakian Academy of Sciences in Bratislava (B). The measurement apparatuses at

SP and B are identical in construction (see Fig. 1). They each consist of a bulk polarization measurement module (PMM), a 4-channel superconducting nanowire single-photon detector (SNSPD) and time-tagging electronics (TTM). Local measurements in the laboratory without long-distance link but including all losses in source, PMM and SNSPD, have shown heralding efficiencies of about 20% on average, equivalent to  $-7.0$  dB. All additional loss in our experiment can be attributed to the fibre links and compensation stages.

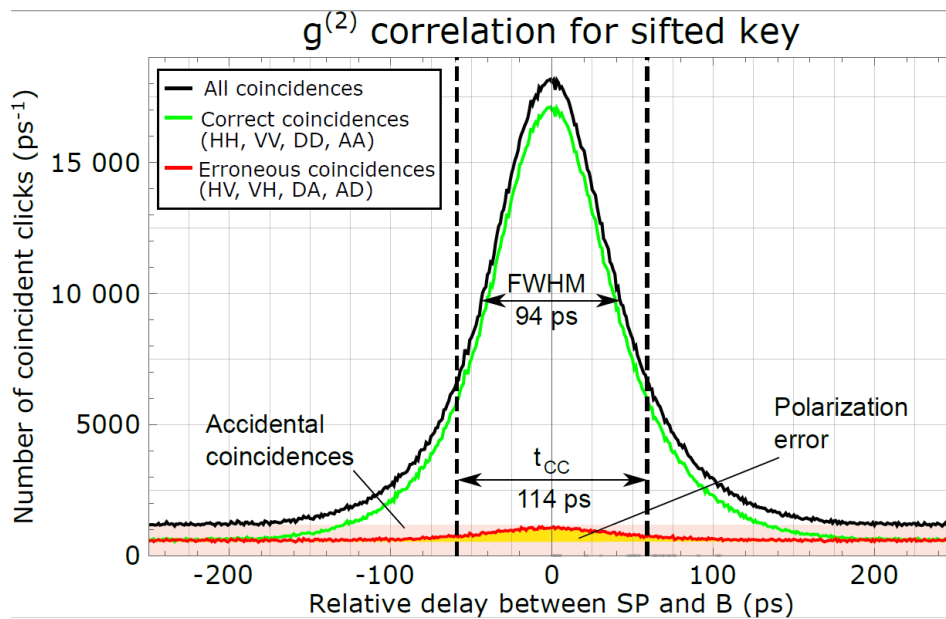


Figure 4.  $g^{(2)}$  intensity correlation of all coincidences used in key creation over the 82 hours of stable QBER. The dotted line shows the width of the coincidence window,  $t_{cc} = 114$  ps, yielding the highest total key of 403 kbit. The ratio of the areas below the red and below the black curve within  $t_{cc}$  corresponds to the overall QBER of 7.0%. The yellow area depicts the number of erroneous measurements due to imperfect polarization alignment, amounting to about 2.6%. The remaining 4.4% of QBER can be attributed to accidental coincidences. We have subtracted the overall delay of approximately  $44.8 \mu\text{s}$  from all relative delay values.

In the PMM, the photons are coupled out of the long-distance fibre and impinge on a 50:50 beamsplitter randomly directing them to two mutually unbiased linear polarization basis measurements. The first basis is realized by a PBS transmitting (reflecting) the horizontal (vertical) polarization mode, which is then coupled into one single-mode fibre each. The other basis, measuring the diagonal/antidiagonal basis, works alike except for an HWP set to  $22.5^\circ$  before the PBS, effectively rotating the

polarization modes by  $45^\circ$ . The four PMM single-mode fibres are connected to the SNSPD, which detects photons with a probability of  $\approx 80\%$  according to the manufacturer Single Quantum. All detection events are recorded using a TTM by Swabian Instruments with 1 ps resolution. The combined jitter of SNSPD and TTM on both sides amounts to  $\approx 38$  ps full-width at half maximum (FWHM). In order to identify detector clicks at SP and B originating from the same photon pair, each TTM is disciplined to a GPS clock. The relative drift of these clocks, on average 13 ps/s, limits the maximum integration time over which detection events at both receivers can be acquired and compared. As can be seen in Fig. 4, the polarization measurement error along the link (2.6 %) is higher than in laboratory measurements (0.2 %) mainly due to our efforts to keep the PPC alignment time low, which did not allow us to set the entangled state perfectly for every alignment.

### **Fibre link**

Measurements with an optical time domain reflectometer (OTDR) of the fibre to St. Pölten (Bratislava) yielded a fibre length  $L$  of 129.0 km (119.2 km) and losses of  $-31.9$  dB ( $-32.6$  dB). Additional to loss, there are two dispersion effects detrimental to QKD imposed by long-distance fibres: chromatic dispersion (CD) and polarization mode dispersion (PMD).

CD is proportional to  $L$  and to the signal's spectral width. It induces different travel times along the fibre for different parts of the light spectrum. This can effectively be seen as a decrease in temporal measurement precision, which smears out the correlation function between Alice and Bob, thus increasing the QBER and rendering live tracking impossible in our high-loss setting. In our experiment, we benefit from the fact that entanglement-based QKD allows for non-local dispersion compensation [28-30]. This means that the total CD effect of both fibre links can be reduced to zero by



use of just one dispersion compensation module (DCM). It introduces additional attenuation of about  $-7$  dB. OTDR measurements yielded a CD of  $2073$  ps/nm ( $617$  ps/nm) to Alice (Bob). These values are so different because the fibre link to Bob partially conforms to the G.655 ITU standard, which allows less dispersion ( $6.0$  ps/nm) than the more commonly used G.652 standard that was used for the link to Alice ( $16.8$  ps/nm) [36]. Since about  $24$  km of fibre had not yet been connected to the link at the time the CD measurements were taken, we estimated the final overall CD to be  $3.0$  ns/nm, equivalent to  $1.8$  ns for our  $100$  GHz WDM spectra (with a FWHM of about  $75$  GHz  $\approx 0.6$  nm), and chose the DCM accordingly. The total FWHM of the correlation peaks amounts to  $94$  ps on average (see Fig. 4). We consider it a convolution of independent timing uncertainty effects:  $38$  ps originate from SNSPD and TTM jitter, as confirmed in the laboratory without link. The remaining  $86$  ps can be attributed either to the mean relative GPS clock drift accumulated over the post-processing integration time of  $7$  s [37], or to residual uncompensated CD, or to both. In our realization, we had no means to differentiate between the two effects.

PMD causes different travel speeds for different polarization states inside the fibre. This is due to varying birefringence over the full stretch of the connection, which is in turn induced by random fibre imperfections. This effect scales with  $\sqrt{L}$  since the accumulated imperfections can not only add up, but also cancel each other [38]. If PMD induces a temporal delay between two orthogonal polarization states which is larger than an unpolarized photon's coherence time, it becomes polarized. In our case, this is equivalent to a polarization measurement and would therefore inhibit distribution of polarization entanglement [39]. OTDR measurements of the fibre to SP (B) have shown the PMD to be  $0.63$  ps ( $0.24$  ps), which is substantially lower than our photons' estimated coherence time of  $\approx 10$  ps. Accordingly, we could not observe PMD-induced loss of polarization fidelity along our fibre link.

## Data acquisition

Data was taken over the course of 109:55 hours, starting on December 14th, 2021 at 17:38 and ending on December 19th, 7:05. The average count rates of all four detectors combined in SP (B) amounted to  $62,500 \text{ s}^{-1}$  ( $94, \text{ s}^{-1}$ ), where  $1,200 \text{ s}^{-1}$  each originate from detector-intrinsic dark counts. Of these detector clicks, about  $4.4 \text{ s}^{-1}$  were coincident in the same measurement bases (“sifted key”) and can be used for key creation after error correction and privacy amplification. This number depends on the chosen coincidence window  $t_{cc}$ : For live operation, we chose  $t_{cc} = 300 \text{ ps}$  and an integration time of  $9,600 \text{ ms}$  in order to register as many coincidences as possible. Note that these are the parameters used for polarization alignment and not those used for key creation, since for live operation, loss of tracking has to be prevented at all cost in order to ensure polarization stabilization. Such stable live operation of the system however relies on automatic temporal tracking of the coincidence peak, which is moving in time due to the GPS clocks’ relative temporal drift. If insufficient statistics, i.e. too few coincidences for the chosen integration time, cause the peak to be unrecognizable to the tracking algorithm, it can move out of the  $1 \text{ ns}$  monitoring window and be lost. This results in failure of the protocol. On the other hand, if the integration time is too long, the clock drift can already start to smear out the coincidence peak, and no additional precision can be gained by integrating further. We chose above parameters because they proved to work sufficiently well to not lose the tracking over the full measurement period, while still providing sufficient contrast for alignment. Thoroughly calculating the discussed trade-offs and optimizing the algorithm with regard to speed and effectiveness will be the subject of future studies. For key creation, which is done in post-processing,  $t_{cc} = 114 \text{ ps}$  and an integration time of  $7 \text{ seconds}$  – resulting in a sifted key rate of  $3.8 \text{ s}^{-1}$  and an average QBER of  $7.0 \%$  – was shown to

yield the largest key. For a detailed analysis of the choice of the optimal coincidence window, we refer the reader to the section “Key rate calculation” and Ref. [27].

### **Active polarization stabilization**

Polarization drift along the deployed fibres due to stress, vibrations and temperature changes constitutes a challenge we overcome with the use of non-local polarization control. There have been approaches to automatize polarization drift compensation in both entanglement-based [40] and prepare-and-send [41, 42] implementations, which however operated in regimes of substantially less loss and on shorter timescales. Our scheme was implemented in the B fibre, right after the source, via one piezoelectric-crystal-based polarization controller module (PPC). We align with respect to the QBER directly. No additional equipment such as a time- or wavelength-multiplexed reference laser have to be used in this scheme, which greatly reduces the engineering overhead of the experiment. Polarization drifts in both fibre links could be compensated with just one PPC due to the non-local nature of our entangled state. The algorithm in use optimized the visibility of the entangled state by iterative scanning of the voltages applied to the PPC’s four fibre-squeezing piezo-electric crystals. Since the coincidence rates used for live-tracking were only in the order of  $5.3 \text{ s}^{-1}$ , the most time-consuming part of polarization optimization is accumulating enough statistics to determine the current visibility value with sufficient precision, which we chose to be  $\pm 0.2$  QBER percent points, assuming Poissonian statistics. As can be seen in Fig. 2, the initial alignment takes much longer than the later corrections (more than 2:30 hours). Subsequent alignments on the other hand can take as few as 8 minutes, and 57 minutes on average. We assume this is because the phase of the entangled state is completely random in the beginning. Polarization drifts, however, do not suddenly

randomize the entangled state's relative phase but only cause gradual changes which can be compensated faster.

We managed to compensate for only 25.4% of the total time, which is important since the coincidence data used for polarization alignment can naturally not be used for key creation. This also means that continuous monitoring of the QBER value, which we did for illustrative purposes in this publication, is not possible. Therefore, one can check the QBER values at certain points in time only, e.g. every hour. This would mean that the actual duty cycle of the system is reduced by another 3.1 percent points, if one assumes the determination of the QBER to take about 2:30 minutes. Additionally, if the QBER is found to be above the PPC limit, it might be beneficial to discard all data collected since the last QBER measurement in order to not dilute the overall raw key. This however depends on an estimate of how fast the QBER actually changes, and on how great the violation of the PPC limit was. Such detailed trade-offs will be the subject of future studies.

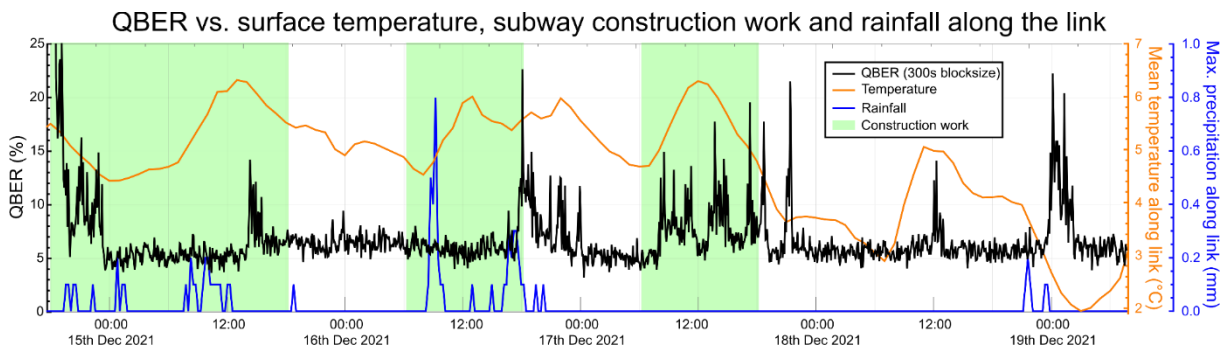


Figure 5. Depiction of QBER over time along with weather and construction site data. There was little variation in mean air temperature along the link and only short stretches of light rain. The construction site, whose operation times are depicted in green, was located close to the deployed fibre connecting the source with the overland fibre links. It involved subterranean drilling for the construction of a new subway line. We can find no convincing evidence for influences from weather and construction work on the polarization stability along the link. However, we cannot exclude destabilizing effects of possible additional construction sites along our 248 km link, since we had no data about them available. Also, harsher weather conditions might still result in polarization drift.

We also performed a preliminary investigation of possible environmental effects on the polarization stability (see Fig. 5). We compared QBER drifts with weather data by the Austrian Central Institution for Meteorology and Geodynamics (ZAMG) as well as with

the working times at drilling sites for the future Viennese subway line U5, which we were supplied with by the Viennese public transport organization Wiener Linien. We find no convincing evidence for a correlation of any of above effects and polarization drift.

### **Key rate calculation**

The key rate depends on several experimental factors. Parameters like pump power, link loss, chromatic dispersion, fidelity and stability of the quantum state, coupling efficiency of the source, and the coincidence window have been carefully analysed resp. chosen, following the methods outlined in Ref. [27]. For our calculation, we follow the key rate formula [33]

$$R^s = R^{\text{sift}}[1 - 2H_2(E)] \quad (2)$$

where  $R^s$  is the final secure key rate,  $R^{\text{sift}}$  is the sifted key rate, i.e. the rate of coincidences measured in compatible bases, and  $H_2(x)$  is the binary Shannon Entropy. Since both  $R^{\text{sift}}$  and  $E$  depend on  $t_{\text{cc}}$ , one has to choose a coincidence window that neither excludes too many entangled pairs nor includes too many accidental counts (see Fig. 4).

The trade-off behind this calculation can be understood as follows: On one hand, if  $t_{\text{cc}}$  is too big, we unnecessarily include uncorrelated accidental counts in our valid coincidences, thus increasing the QBER and losing key to error correction and privacy amplification. On the other hand, if  $t_{\text{cc}}$  is chosen too small, too many valid coincidences get lost, and the size of our raw key decreases. This trade-off with regard to  $t_{\text{cc}}$  further depends on the block size and the assumed error correction efficiency  $f$ . The latter we set to 1 in Eq. (2), since we assume an arbitrarily long key in our ultra-stable, actively compensated QKD scheme. If one however wants to divide the raw key into smaller

blocks,  $f$  will increase [43], which would in turn also lead to a different optimal value of  $t_{cc}$ .

Such smaller block sizes might be desirable due to the fact that in a real-life implementation, the QBER unavoidably fluctuates in time. In this case, it is beneficial to split a block of QBER  $E$  into  $n$  sub-blocks with  $E_1, \dots, E_n$  where  $E = (\sum_{i=1}^n E_i)/n$  and calculate  $R^s$  as the sum of all  $R^{s_i}(E_i)$ , since  $H_2(x)$  is a concave function. On the other hand, smaller block sizes lead to less precise QBER estimates, effectively increasing the QBER, because one has to assume the worst  $E$  possible to guarantee a quantum secure key. Such trade-offs however are outside of the scope of this paper; we just present one final key size of 403 kbit for a single block containing the complete raw key, i.e. not exploiting above considerations for shorter blocks.

## References

- [35] Bennink, R. S., Optimal collinear gaussian beams for spontaneous parametric down-conversion, *Phys. Rev. A* **81**, 053805 (2010).
- [36] Recommendation ITU-T G.694.1, "Spectral grids for WDM applications: DWDM frequency grid" (2020).
- [37] Specification sheet and manual of the FS740 GPS Time and Frequency System, <https://www.thinksrs.com/downloads/pdfs/catalog/FS740c.pdf> (accessed March 2022).
- [38] Poole, C. D., Measurement of polarization-mode dispersion in single-mode fibres with random mode coupling, *Opt. Lett.* **14**, 523 (1989).
- [39] Antonelli, C., Shtaif, M., and Brodsky, M., Sudden death of entanglement induced by polarization mode dispersion, *Phys. Rev. Lett.* **106**, 080404 (2011).
- [40] Shi, Y., Poh H. S., Ling, A., and Kurtsiefer, C., Fibre polarisation state compensation in entanglement-based quantum key distribution, *Opt. Express* **29**, 37075 (2021).
- [41] Xavier, G. B. et al., Experimental polarization encoded quantum key distribution over optical fibres with real-time continuous birefringence compensation, *New J. Phys.* **11**, 045015 (2009).
- [42] Ramos, M. F., Silva, N. A., Muga, N. J., & Pinto, A. N., Full polarization random drift compensation method for quantum communication, *Opt. Express* **30**, 6907 (2022).
- [43] Elkouss, D., Martínez-Mateo, J., & Martin V., Information reconciliation for QKD, *Quantum Inf. Comput.* **11**, 226 (2011)

## **Contributions**

SPN, MB and RU designed the experiment. SPN and RU acquired the link infrastructure. SPN built the source of entangled photon pairs, the detection modules and the passive compensation stages. SPN and AB conducted the experiment. LB established the timing synchronization and wrote and operated the coincidence, data collection and data analysis software. AB wrote and operated the PPC algorithm. LB and AB built the PPC stage. SPN and MB wrote the paper.

## **Data availability**

The time-tag files collected in the course of the experiment are in the order of Terabyte and available from the corresponding authors upon reasonable request.

## **Code availability**

The code used for the polarization alignment procedure is available from the corresponding authors upon reasonable request.

## **Competing interests**

The authors declare no competing interests.

## **Acknowledgements**

We acknowledge European Union's Horizon 2020 programme grant agreement No.857156 (OpenQKD) and the Austrian Academy of Sciences in cooperation with the FhG ICON-Program "Integrated Photonic Solutions for Quantum Technologies (InteQuant)". We thank Peter Rapčan, Djeylan Aktas, Mário Ziman, and Vladimír Bužek of Bratislava for their help. We thank Ewald Martinelli, Harald Zeitlhofer and Giuseppe Antonelli of Türk Telekom for their help and discussions regarding the deployed fibre link. We thank Thomas Scheidl and Sören Wengerowsky for fruitful



discussions and calculations, and Matej Pivluska for advice regarding key rate estimates. We thank Ulrich Galander for prototyping parts of the experiment. We thank the Austrian Central Institution for Meteorology and Geodynamics (ZAMG) for the weather data and the Viennese public transport institution Wiener Linien for disclosing their construction site schedules.



# Bibliography

- [1] J. P. Buhler, H. W. Lenstra, and Carl Pomerance. Factoring integers with the number field sieve. In Arjen K. Lenstra and Hendrik W. Lenstra, editors, *The development of the number field sieve*, pages 50–94, Berlin, Heidelberg, 1993. Springer Berlin Heidelberg.
- [2] G. S. Vernam. Cipher printing telegraph systems for secret wire and radio telegraphic communications. *Transactions of the American Institute of Electrical Engineers*, XLV:295–301, 1926.
- [3] C. E. Shannon. Communication theory of secrecy systems. *The Bell System Technical Journal*, 28(4):656–715, 1949.
- [4] H Bennett Ch and G Brassard. Quantum cryptography: public key distribution and coin tossing int. In *Conf. on Computers, Systems and Signal Processing (Bangalore, India, Dec. 1984)*, pages 175–9, 1984.
- [5] Artur K Ekert. Quantum cryptography based on bell’s theorem. *Physical review letters*, 67(6):661, 1991.
- [6] Charles H Bennett. Quantum cryptography using any two nonorthogonal states. *Physical review letters*, 68(21):3121, 1992.
- [7] H. Bechmann-Pasquinucci and N. Gisin. Incoherent and coherent eavesdropping in the six-state protocol of quantum cryptography. *Phys. Rev. A*, 59:4238–4248, Jun 1999.
- [8] H. Bechmann-Pasquinucci and W. Tittel. Quantum cryptography using larger alphabets. *Phys. Rev. A*, 61:062308, May 2000.
- [9] Valerio Scarani, Antonio Acín, Grégoire Ribordy, and Nicolas Gisin. Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations. *Phys. Rev. Lett.*, 92:057901, Feb 2004.
- [10] Hoi-Kwong Lo, H. F. Chau, and M. Ardehali. Efficient quantum key distribution scheme and a proof of its unconditional security. *Journal of Cryptology*, 18(2):133–165, Apr 2005.
- [11] Hoi-Kwong Lo, Xiongfeng Ma, and Kai Chen. Decoy state quantum key distribution. *Phys. Rev. Lett.*, 94:230504, Jun 2005.
- [12] Muhammad Mubashir Khan, Michael Murphy, and Almut Beige. High error-rate quantum key distribution for long-distance communication. *New Journal of Physics*, 11(6):063043, jun 2009.
- [13] 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(7705):400–403, May 2018.
- [14] Charles H Bennett, Gilles Brassard, and N David Mermin. Quantum cryptography without bell’s theorem. *Physical Review Letters*, 68(5):557, 1992.
- [15] A. Einstein, B. Podolsky, and N. Rosen. Can quantum-mechanical description of physical reality be considered complete? *Physical Review*, 47:777–780, 1935.

## Bibliography

- [16] W. Heisenberg. Über den anschaulichen inhalt der quantentheoretischen kinematik und mechanik. *Zeitschrift für Physik*, 43(3):172–198, Mar 1927.
- [17] Albert Einstein and Max Born. *Briefwechsel : 1916 - 1955*. Langen Müller, München, 3. aufl.. edition, 2005.
- [18] J. Bell. On the einstein podolsky rosen paradox. *Physics*, 1(3):195–200, 1964.
- [19] John F. Clauser, Michael A. Horne, Abner Shimony, and Richard A. Holt. Proposed experiment to test local hidden-variable theories. *Phys. Rev. Lett.*, 23:880–884, Oct 1969.
- [20] Stuart J. Freedman and John F. Clauser. Experimental test of local hidden-variable theories. *Phys. Rev. Lett.*, 28:938–941, Apr 1972.
- [21] Alain Aspect, Philippe Grangier, and Gérard Roger. Experimental tests of realistic local theories via bell’s theorem. *Phys. Rev. Lett.*, 47:460–463, Aug 1981.
- [22] A. Aspect, J. Dalibard, and G. Roger. Experimental test of bell’s inequalities using time-varying analyzers. *Physical Review Letters*, 49(25):1804–1807, 1982.
- [23] Alain Aspect, Philippe Grangier, and Gérard Roger. Experimental realization of einstein-podolsky-rosen-bohm gedankenexperiment: a new violation of bell’s inequalities. *Physical review letters*, 49(2):91, 1982.
- [24] W. Tittel, J. Brendel, H. Zbinden, and N. Gisin. Violation of bell inequalities by photons more than 10 km apart. *Phys. Rev. Lett.*, 81:3563–3566, Oct 1998.
- [25] M. A. Rowe, D. Kielpinski, V. Meyer, C. A. Sackett, W. M. Itano, C. Monroe, and D. J. Wineland. Experimental violation of a bell’s inequality with efficient detection. *Nature*, 409(6822):791–794, Feb 2001.
- [26] Rupert Ursin, F Tiefenbacher, T Schmitt-Manderbach, H Weier, Thomas Scheidl, M Lindenthal, B Blauensteiner, T Jennewein, J Perdigues, P Trojek, et al. Entanglement-based quantum communication over 144 km. *Nature physics*, 3(7), 2007.
- [27] D. Salart, A. Baas, J. A. W. van Houwelingen, N. Gisin, and H. Zbinden. Spacelike separation in a bell test assuming gravitationally induced collapses. *Phys. Rev. Lett.*, 100:220404, Jun 2008.
- [28] Thomas Scheidl, Rupert Ursin, Johannes Kofler, Sven Ramelow, Xiao-Song Ma, Thomas Herbst, Lothar Ratschbacher, Alessandro Fedrizzi, Nathan K. Langford, Thomas Jennewein, and Anton Zeilinger. Violation of local realism with freedom of choice. *Proceedings of the National Academy of Sciences*, 107(46):19708–19713, 2010.
- [29] B. Hensen, H. Bernien, A. E. Dréau, A. Reiserer, N. Kalb, M. S. Blok, J. Ruitenbergh, R. F. L. Vermeulen, R. N. Schouten, C. Abellán, W. Amaya, V. Pruneri, M. W. Mitchell, M. Markham, D. J. Twitchen, D. Elkouss, S. Wehner, T. H. Taminiiau, and R. Hanson. Loophole-free bell inequality violation using electron spins separated by 1.3 kilometres. *Nature*, 526(7575):682–686, Oct 2015.
- [30] Marissa Giustina, Marijn A. M. Versteegh, Sören Wengerowsky, Johannes Handsteiner, Armin Hochrainer, Kevin Phelan, Fabian Steinlechner, Johannes Kofler, Jan-Åke Larsson, Carlos Abellán, Waldimar Amaya, Valerio Pruneri, Morgan W. Mitchell, Jörn Beyer, Thomas Gerrits, Adriana E. Lita, Lynden K. Shalm, Sae Woo Nam, Thomas Scheidl, Rupert Ursin, Bernhard Wittmann, and Anton Zeilinger. Significant-loophole-free test of bell’s theorem with entangled photons. *Phys. Rev. Lett.*, 115:250401, Dec 2015.

- [31] Lynden K Shalm, Evan Meyer-Scott, Bradley G Christensen, Peter Bierhorst, Michael A Wayne, Martin J Stevens, Thomas Gerrits, Scott Glancy, Deny R Hamel, Michael S Allman, et al. Strong loophole-free test of local realism. *Physical review letters*, 115(25):250402, 2015.
- [32] G. C. Ghirardi, A. Rimini, and T. Weber. A general argument against superluminal transmission through the quantum mechanical measurement process. *Lettere al Nuovo Cimento (1971-1985)*, 27(10):293–298, Mar 1980.
- [33] Jean Dalibard Jean-Louis Basdevant. Quantum mechanics. In *Introductory Quantum Physics and Relativity*, pages 27–42. IMPERIAL COLLEGE PRESS, October 2010.
- [34] W. K. Wootters and W. H. Zurek. A single quantum cannot be cloned. *Nature*, 299(5886):802–803, Oct 1982.
- [35] Valerie Coffman, Joydip Kundu, and William K. Wootters. Distributed entanglement. *Phys. Rev. A*, 61:052306, Apr 2000.
- [36] Masato Koashi and John Preskill. Secure quantum key distribution with an uncharacterized source. *Phys. Rev. Lett.*, 90:057902, Feb 2003.
- [37] A. R. Dixon and H. Sato. High speed and adaptable error correction for megabit/s rate quantum key distribution. *Scientific Reports*, 4(1):7275, Dec 2014.
- [38] Gilles van Assche. *Quantum Cryptography and Secret-Key Distillation*. Cambridge University Press, Cambridge, England, June 2006.
- [39] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden. Quantum cryptography. *Review of Modern Physics*, 74(1):145–195, 2002.
- [40] Z. L. Yuan, J. F. Dynes, and A. J. Shields. Avoiding the blinding attack in qkd. *Nature Photonics*, 4(12):800–801, Dec 2010.
- [41] Guillaume Adenier, Masanori Ohya, Noboru Watanabe, Irina Basieva, and Andrei Yu. Khrennikov. Double blinding-attack on entanglement-based quantum key distribution protocols. *AIP Conference Proceedings*, 1424(1):9–16, 2012.
- [42] Michael G. Tanner, Vadim Makarov, and Robert H. Hadfield. Optimised quantum hacking of superconducting nanowire single-photon detectors. *Opt. Express*, 22(6):6734–6748, Mar 2014.
- [43] Juan Carlos Garcia-Escartin, Shihan Sajeed, and Vadim Makarov. Attacking quantum key distribution by light injection via ventilation openings. *PLOS ONE*, 15(8):1–21, 08 2020.
- [44] Rupesh Kumar, Francesco Mazzoncini, Hao Qin, and Romain Alléaume. Experimental vulnerability analysis of qkd based on attack ratings. *Scientific Reports*, 11(1):9564, May 2021.
- [45] Edo Waks, Assaf Zeevi, and Yoshihisa Yamamoto. Security of quantum key distribution with entangled photons against individual attacks. *Phys. Rev. A*, 65:052310, Apr 2002.
- [46] C. H. Bennett and G. Brassard. Experimental quantum cryptography: The dawn of a new era for quantum cryptography: The experimental prototype is working]. *SIGACT News*, 20(4):78–80, nov 1989.
- [47] Gregor Weihs, Thomas Jennewein, Christoph Simon, Harald Weinfurter, and Anton Zeilinger. Violation of bell’s inequality under strict einstein locality conditions. *Phys. Rev. Lett.*, 81:5039–5043, Dec 1998.

## Bibliography

- [48] Markus Aspelmeyer, Hannes R. Böhm, Tsewang Gyatso, Thomas Jennewein, Rainer Kaltenbaek, Michael Lindenthal, Gabriel Molina-Terriza, Andreas Poppe, Kevin Resch, Michael Taraba, Rupert Ursin, Philip Walther, and Anton Zeilinger. Long-distance free-space distribution of quantum entanglement. *Science*, 301(5633):621–623, 2003.
- [49] K.J. Resch, M. Lindenthal, B. Blauensteiner, H.R. Böhm, A. Fedrizzi, C. Kurtsiefer, A. Poppe, T. Schmitt-Manderbach, M. Taraba, R. Ursin, P. Walther, H. Weier, H. Weinfurter, and A. Zeilinger. Distributing entanglement and single photons through an intra-city, free-space quantum channel. *Opt. Express*, 13(1):202–209, Jan 2005.
- [50] Juan Yin, Yuan Cao, Yu-Huai Li, Sheng-Kai Liao, Liang Zhang, Ji-Gang Ren, Wen-Qi Cai, Wei-Yue Liu, Bo Li, Hui Dai, et al. Satellite-based entanglement distribution over 1200 kilometers. *Science*, 356(6343):1140–1144, 2017.
- [51] Juan Yin, Yu-Huai Li, Sheng-Kai Liao, Meng Yang, Yuan Cao, Liang Zhang, Ji-Gang Ren, Wen-Qi Cai, Wei-Yue Liu, Shuang-Lin Li, Rong Shu, Yong-Mei Huang, Lei Deng, Li Li, Qiang Zhang, Nai-Le Liu, Yu-Ao Chen, Chao-Yang Lu, Xiang-Bin Wang, Feihu Xu, Jian-Yu Wang, Cheng-Zhi Peng, Artur K. Ekert, and Jian-Wei Pan. Entanglement-based secure quantum cryptography over 1,120 kilometres. *Nature*, 582(7813):501–505, Jun 2020.
- [52] Gordon Day. Birefringence measurements in single mode optical fiber. Number 425. Proc. Intl. Soc. for Optical Engineering (SPIE), 1983-01-01 1983.
- [53] T. Honjo, H. Takesue, H. Kamada, Y. Nishida, O. Tadanaga, M. Asobe, and K. Inoue. Long-distance distribution of time-bin entangled photon pairs over 100 km using frequency up-conversion detectors. *Opt. Express*, 15(21):13957–13964, Oct 2007.
- [54] Hannes Hübel, Michael R. Vanner, Thomas Lederer, Bibiane Blauensteiner, Thomas Lorünser, Andreas Poppe, and Anton Zeilinger. High-fidelity transmission of polarization encoded qubits from an entangled source over 100 km of fiber. *Opt. Express*, 15(12):7853–7862, Jun 2007.
- [55] Takahiro Inagaki, Nobuyuki Matsuda, Osamu Tadanaga, Masaki Asobe, and Hiroki Takesue. Entanglement distribution over 300 km of fiber. *Opt. Express*, 21(20):23241–23249, Oct 2013.
- [56] Sören Wengerowsky, Siddarth Koduru Joshi, Fabian Steinlechner, Julien R. Zichi, Sergiy M. Dobrovolskiy, René van der Molen, Johannes W. N. Los, Val Zwiller, Marijn A. M. Versteegh, Alberto Mura, Davide Calonico, Massimo Inguscio, Hannes Hübel, Liu Bo, Thomas Scheidl, Anton Zeilinger, André Xuereb, and Rupert Ursin. Entanglement distribution over a 96-km-long submarine optical fiber. *Proceedings of the National Academy of Sciences*, 116(14):6684–6688, 2019.
- [57] Sören Wengerowsky, Siddarth Koduru Joshi, Fabian Steinlechner, Julien R. Zichi, Bo Liu, Thomas Scheidl, Sergiy M. Dobrovolskiy, René van der Molen, Johannes W. N. Los, Val Zwiller, Marijn A. M. Versteegh, Alberto Mura, Davide Calonico, Massimo Inguscio, Anton Zeilinger, André Xuereb, and Rupert Ursin. Passively stable distribution of polarisation entanglement over 192 km of deployed optical fibre. *npj Quantum Information*, 6(1):5, Jan 2020.
- [58] Sheng-Kai Liao, Hai-Lin Yong, Chang Liu, Guo-Liang Shentu, Dong-Dong Li, Jin Lin, Hui Dai, Shuang-Qiang Zhao, Bo Li, Jian-Yu Guan, et al. Long-distance free-space quantum key distribution in daylight towards inter-satellite communication. *Nature Photonics*, 11(8):509–513, 2017.
- [59] Yun-Hong Gong, Kui-Xing Yang, Hai-Lin Yong, Jian-Yu Guan, Guo-Liang Shentu, Chang Liu, Feng-Zhi Li, Yuan Cao, Juan Yin, Sheng-Kai Liao, Ji-Gang Ren, Qiang Zhang, Cheng-Zhi

- Peng, and Jian-Wei Pan. Free-space quantum key distribution in urban daylight with the spgd algorithm control of a deformable mirror. *Opt. Express*, 26(15):18897–18905, Jul 2018.
- [60] M. Avesani, L. Calderaro, M. Schiavon, A. Stanco, C. Agnesi, A. Santamato, M. Zahidy, A. Scriminich, G. Foletto, G. Contestabile, M. Chiesa, D. Rotta, M. Artiglia, A. Montanaro, M. Romagnoli, V. Sorianello, F. Vedovato, G. Vallone, and P. Villoresi. Full daylight quantum-key-distribution at 1550 nm enabled by integrated silicon photonics. *npj Quantum Information*, 7(1):93, Jun 2021.
- [61] Bob Dirks, Ivan Ferrario, Alessandro Le Pera, Daniele Vito Finocchiaro, Marine Desmons, Dorus de Lange, Harry de Man, Arjan J. H. Meskers, Jaco Morits, Niels M. M. Neumann, Rudolf Saathof, and Gert Witvoet. GEOQKD: quantum key distribution from a geostationary satellite. In Bruno Cugny, Zoran Sodnik, and Nikos Karafolas, editors, *International Conference on Space Optics — ICSSO 2020*, volume 11852, pages 222 – 236. International Society for Optics and Photonics, SPIE, 2021.
- [62] L. Elterman. *UV, Visible, and IR Attenuation for Altitudes to 50 Km, 1968*. Environmental research papers. United States Air Force, Office of Aerospace Research, Air Force Cambridge Research Laboratories, Optical Physics Laboratory, 1968.
- [63] Shlomi Arnon, Stanley R. Rotman, and Norman S. Kopeika. Optimum transmitter optics aperture for free space satellite optical communication as a function of tracking system performance. *Proc. SPIE*, 2811:252–263, 1996.
- [64] Corning, <https://www.corning.com/media/worldwide/coc/documents/Fiber/product-information-sheets/PI-1470-AEN.pdf>. *Corning SMF-28 ULL optical fiber*, 2021.
- [65] S. Warier. *Engineering optical networks*. Artech House, Norwood, MA :, 2018.
- [66] International telecommunication union recommendation G.652 (11/16), May 2017.
- [67] Corning, <https://www.corning.com/media/worldwide/coc/documents/Fiber/PI-1463-AEN.pdf>. *Corning SMF-28e+ optical fiber product information*, 2021.
- [68] JD Franson. Nonlocal cancellation of dispersion. *Physical Review A*, 45(5):3126, 1992.
- [69] Yu-Yang Ding, Hua Chen, Shuang Wang, De-Yong He, Zhen-Qiang Yin, Wei Chen, Zheng Zhou, Guang-Can Guo, and Zheng-Fu Han. Polarization variations in installed fibers and their influence on quantum key distribution systems. *Opt. Express*, 25(22):27923–27936, Oct 2017.
- [70] G B Xavier, N Walenta, G Vilela de Faria, G P Temporão, N Gisin, H Zbinden, and J P von der Weid. Experimental polarization encoded quantum key distribution over optical fibres with real-time continuous birefringence compensation. *New Journal of Physics*, 11(4):045015, apr 2009.
- [71] Dong-Dong Li, Song Gao, Guo-Chun Li, Lu Xue, Li-Wei Wang, Chang-Bin Lu, Yao Xiang, Zi-Yan Zhao, Long-Chuan Yan, Zhi-Yu Chen, Gang Yu, and Jian-Hong Liu. Field implementation of long-distance quantum key distribution over aerial fiber with fast polarization feedback. *Opt. Express*, 26(18):22793–22800, Sep 2018.
- [72] Yicheng Shi, Soe Moe Thar, Hou Shun Poh, James A. Grieve, Christian Kurtsiefer, and Alexander Ling. Stable polarization entanglement based quantum key distribution over a deployed metropolitan fiber. *Applied Physics Letters*, 117(12):124002, 2020.

## Bibliography

- [73] Mariana F. Ramos, Nuno A. Silva, Nelson J. Muga, and Armando N. Pinto. Full polarization random drift compensation method for quantum communication. *Opt. Express*, 30(5):6907–6920, Feb 2022.
- [74] C. D. Poole. Measurement of polarization-mode dispersion in single-mode fibers with random mode coupling. *Opt. Lett.*, 14(10):523–525, May 1989.
- [75] Misha Brodsky, Elizabeth C. George, Cristian Antonelli, and Mark Shtaif. Loss of polarization entanglement in a fiber-optic system with polarization mode dispersion in one optical path. *Opt. Lett.*, 36(1):43–45, Jan 2011.
- [76] Cristian Antonelli, Mark Shtaif, and Misha Brodsky. Sudden death of entanglement induced by polarization mode dispersion. *Physical review letters*, 106(8):080404, 2011.
- [77] Xiongfeng Ma, Chi-Hang Fred Fung, and Hoi-Kwong Lo. Quantum key distribution with entangled photon sources. *Physical Review A*, 76(1):012307, 2007.



**Curriculum Vitae of Sebastian Philipp Neumann, MSc MA**

born 28. December 1988 in Wels, Austria

- May 2022 - present: Senior Scientist at Quantum Technology Laboratories, Vienna
- Oct 2016 - Apr 2022: Doctoral candidate at IQOQI Vienna, Austrian Academy of Sciences
- Oct 2015 - Jun 2016: Acting School “Schauspielschule Krauss”, left after first year
- Oct 2012 - Oct 2019: Master’s degree in German Philology at University of Vienna, graduation with distinction
- Oct 2012 - Mar 2016: Master’s degree in Physics at University of Vienna, graduation with distinction
- Oct 2008 - Oct 2012: Bachelor’s degree in Physics
- Oct 2008 - Oct 2012: Bachelor’s degree in German Philology
- Sep 1999 - Jun 2007: High school “BRG Wels Wallererstraße”, graduation with distinction