A fast and versatile quantum key distribution system with hardware key distillation and wavelength multiplexing

Journal Article

Author(s):
Walenta, Nino; Burg, Andreas P.; Caselunghe, Dario; Constantin, Jeremy; Gisin, Nicolas; Guinnard, Olivier; Houlmann, Raphaël; Junod, Pascal; Korzh, Boris; Kulesza, Natalia; Legré, Matthieu; Lim, C.W.; Lunghi, Tommaso; Monat, Laurent; Portmann, Christopher; Soucarros, Mathilde; Thew, Robert T.; Trinkler, Patrick; Trolliet, Gregory; Vannel, Fabien; Zbinden, Hugo

Publication date:
2014-01

Permanent link:
https://doi.org/10.3929/ethz-b-000080907

Originally published in:
New Journal of Physics 16, https://doi.org/10.1088/1367-2630/16/1/013047

New Journal of Physics
The open access journal at the forefront of physics

Deutsche Physikalische Gesellschaft DPG IOP Institute of Physics

PAPER • OPEN ACCESS

A fast and versatile quantum key distribution system with hardware key distillation and wavelength multiplexing

To cite this article: N Walenta *et al* 2014 *New J. Phys.* **16** 013047

New Journal of Physics
The open access journal at the forefront of physics
Deutsche Physikalische Gesellschaft DPG | IOP Institute of Physics

A fast and versatile quantum key distribution system with hardware key distillation and wavelength multiplexing

N Walenta[1,7], A Burg[2], D Caselunghe[3], J Constantin[2], N Gisin[1], O Guinnard[1], R Houlmann[1], P Junod[4], B Korzh[1], N Kulesza[3], M Legré[3], C W Lim[1], T Lunghi[1], L Monat[3], C Portmann[1,5], M Soucarros[3], R T Thew[1], P Trinkler[3], G Trolliet[6], F Vannel[6] and H Zbinden[1,7]

[1] Group of Applied Physics-Optique, University of Geneva, Chemin de Pinchat 22, CH-1211 Geneva, Switzerland
[2] Telecommunications Circuits Laboratory, EPFL, CH-1015 Lausanne, Switzerland
[3] idQuantique SA, Chemin de la Marbrerie 3, CH-1227 Geneva, Switzerland
[4] University of Applied Sciences Western Switzerland in Yverdon-les-Bains (HEIG-VD), Route de Cheseaux 1, CH-1401 Yverdon, Switzerland
[5] Institute for Theoretical Physics, ETH Zurich, Gloriastrasse 35, D-8093 Zurich, Switzerland
[6] University of Applied Sciences Western Switzerland in Geneva (Hepia), Rue de la Prairie 4, CH-1202 Geneva, Switzerland
E-mail: nino.walenta@unige.ch and hugo.zbinden@unige.ch

Received 10 September 2013, revised 13 December 2013
Accepted for publication 19 December 2013
Published 23 January 2014

New Journal of Physics **16** (2014) 013047

doi:10.1088/1367-2630/16/1/013047

Abstract

We present a compactly integrated, 625 MHz clocked coherent one-way quantum key distribution system which continuously distributes secret keys over an optical fibre link. To support high secret key rates, we implemented a fast hardware key distillation engine which allows for key distillation rates up to 4 Mbps in real time. The system employs wavelength multiplexing in order to run over only a single optical fibre. Using fast gated InGaAs single photon detectors, we reliably distribute secret keys with a rate above 21 kbps over 25 km of optical fibre. We optimized the system considering a security analysis that respects finite-key-size effects, authentication costs and system errors for a security parameter of $\varepsilon_{\mathrm{QKD}} = 4 \times 10^{-9}$.

[7] Authors to whom any correspondence should be addressed.

1. Introduction

Today's society relies heavily on confidential and authenticated communication. Encryption and authentication can be realized with provable information-theoretic security, derived from Shannon's theory [1]. This means that even an adversary who has unlimited computing powers can decipher an encrypted message or forge an authenticated message only with arbitrarily small probabilities. To date, the only message encryption scheme that has been proven information-theoretically secure [1] is the Vernam one-time pad cipher [2]. Secure message authentication has been demonstrated for schemes utilizing universal hash functions [3, 4]. The fundamental resources of these schemes are random and secret strings of bits, shared between the two distant parties commonly known as Alice and Bob. Hence, information-theoretically secure communication necessitates continuous distribution of random secret keys with provable security. Classically, the generation of two identical key streams of truly random bits at two distinct locations relies on the assumption of a secure channel or public-key cryptography. However, their security is based on certain assumptions, such as the difficulty to factorize large composite integers, or to compute discrete logarithms in certain finite groups.

A completely different approach is quantum key distribution (QKD), introduced in 1984 by Bennett and Brassard [5] (see [6] for a review). The idea is to send random bits encoded in non-orthogonal states of single photons. The security is based on the laws of quantum mechanics, in particular the no-cloning theorem which forbids the creation of identical copies of unknown quantum states and the fact that a measurement of an unknown quantum state inevitably disturbs it. Subsequent authenticated communication between Alice and Bob enables a measure of the information an eavesdropper potentially possesses, and hence, its reduction. Seen in this light, QKD is essentially a key expansion scheme, that is, a short initial authentication key is sufficient to continuously generate new information-theoretically secure keys [6]. Most importantly, the secret keys generated by QKD are universally composable, which allows one to partially reuse them for authenticating the distillation processes of subsequent QKD rounds. Remaining bits are then available for message encryption and authentication. QKD may also be used to enhance security of cryptography schemes based on computational complexity, e.g. advanced encryption standard (AES) can benefit from regularly refreshed encryption keys.

Since the mid 1990s, QKD has progressed rapidly in several aspects. Starting from the early demonstration of feasibility experiments [7, 8], faster and faster (with bit rates on the order of Mbps [9, 10]) and long reaching systems (up to 250 km [11, 12]) have been developed. With the aim of reducing the number of required fibre links between two QKD systems, dense-wavelength division multiplexing (DWDM) of quantum and classical channels over one single fibre has been investigated, e.g. in [13–16]. However, most of the early experiments focused only on the physical layer: photon generation, manipulation, transmission and detection. Even up to today, systems which include all necessary components for secure and fast QKD are rare. Indeed, those components are numerous and need multidisciplinary competence (see figure 4). Important and often forgotten parts include random number generation, real-time error correction and privacy amplification, secure authentication and finite-key security analysis. Recently, the need for faster systems has stimulated the development of dedicated hardware engines for quantum key distillation, e.g. [17–19].

In this paper, we present the results of a project (www.nano-tera.ch/nanoterawiki/qcrypt) whose ambition was to implement a complete and practical fibre based QKD prototype in collaboration between six research teams in Switzerland. In particular we put emphasis on

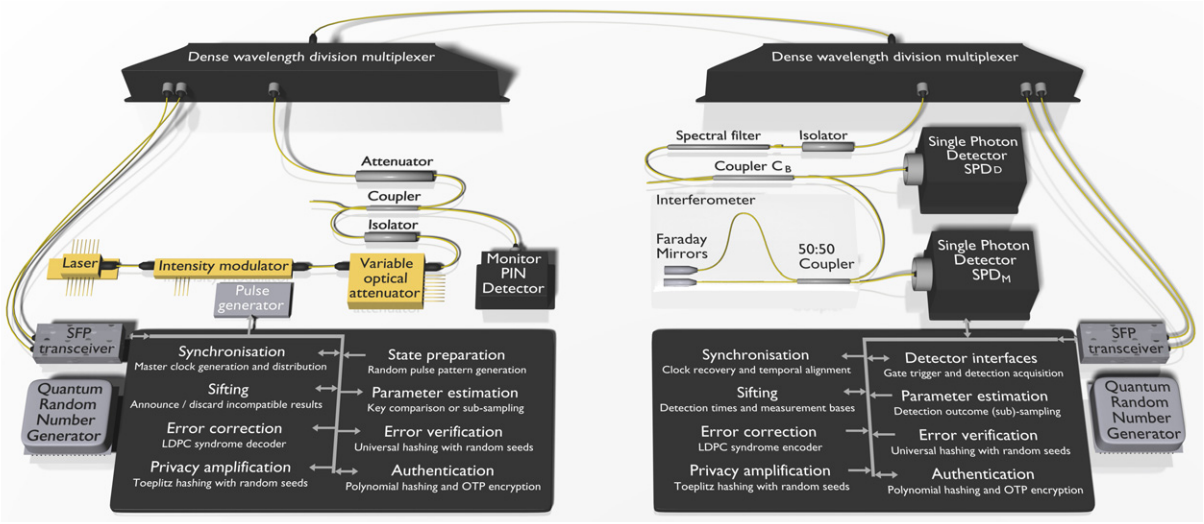

Figure 1. Schematic representation of our optical implementation for the COW QKD protocol and the key distillation procedures implemented in the fast FPGA hardware.

continuous operation with a wavelength multiplexed service channel for synchronization and distillation, efficient hardware real-time distillation, finite-key security analysis and frugal authentication. In section 2, we present the heart of any QKD prototype, the field programmable gate array (FPGA) based engine controlling all the hardware as well as the complete key distillation and authentication process. This QKD engine can be adapted to many QKD protocols. In section 4, we briefly present the employed 'coherent one-way' (COW) protocol and its specific opto-electronic realization. Section 4 presents the experimental results and a discussion.

2. Quantum key distribution (QKD) engine

The QKD system described in the following was designed to have the flexibility to adapt to different QKD implementations and protocols. A schematic representation of our implementation is shown in figure 1. It is built around FPGAs (Xilinx Virtex 6), which manage the fast interfaces for the optical components, the classical communication channels, all the sub-protocols that accompany QKD as well as the distribution of the generated secret keys. The choice of various parameters as well as all the algorithms used for key distillation and authentication processes have been carefully chosen by taking into account various trade-offs between engineering and cost constraints. Importantly, we have taken special care to analyse and optimize all tasks with respect to reducing the requirements and resources such that only one single FPGA is needed in each device. In general, compromises had to be found between the post-processing key size ($\geqslant 10^5$ bits), as required in finite-key scenarios analysed in appendix, and limits imposed by the hardware in terms of memory size and throughput. A personal computer (PC) is connected to each FPGA via PCI Express to access the configuration, status and monitoring registers. The final secret key can be transferred from the key manager to this PC and further distributed to external applications. Two communication links are established, a one-way quantum channel and a bidirectional classical service channel. All channels can be

wavelength-multiplexed on a single fibre using DWDM. In the following, we describe in more detail the functionality of each module of our QKD engine. For a more complete (and technical) description of the code architecture and the used algorithms, please refer to [20].

2.1. Quantum channel interface module

Two digital 1.25 Gbps full-duplex serial interfaces at each FPGA (for Alice and Bob) allow synchronized interconnection with the optical hardware of the quantum channel. At Alice, they output up to two parallel streams of digital on-off pulses with adjustable amplitude and width, which are used to drive an electro-optical modulator for quantum state preparation. For the implementation of the COW protocol as presented later, the output of one interface is needed to drive an intensity modulator. Using the output of the second interface as well, one can control a dual-drive modulator and prepare all quantum states required by BB84 or the differential phase-shift (DPS) protocol, as we have shown in [21]. At Bob's device, both digital full-duplex serial interfaces are used, each connected to one single photon detector (SPD), SPD_D and SPD_M, respectively. They provide the detector gate trigger if needed, and receive the detection signals from the corresponding SPD. Digital delays with 10 ps resolution allow temporal alignment of the detector gates with respect to the quantum signals, and temporal alignment of the detection signals with respect to Bob's FPGA clock.

2.2. Service channel interface module

Two optical 2.5 Gbps small form-factor pluggable (SFP) transceivers (Finisar) on each side establish a bidirectional (full-duplex) classical communication link between Alice and Bob. All tasks which are needed to continuously generate secret keys or to further use these keys, share this link employing time-division multiplexing. These tasks requiring classical communication comprise, in particular, synchronization, alignment, sifting, parameter estimation, error correction and verification, privacy amplification, authentication, key management, encryption, administration and logging. Some of them strictly require authentication, some of them encryption or even both as discussed later. The priority of each task, as well as the allocated communication bandwidth, can be adjusted individually. We employ DWDM to transmit all classical communication channels together with the quantum channel simultaneously over a single fibre. The FPGA system clock of Bob is synchronized and phase stabilized with 10 ps precision with the master clock of Alice. All other necessary frequencies are derived from this clock, most importantly Alice's quantum state modulation frequency and Bob's detector gate frequency.

2.3. Sifting and sampling module

This module realizes sifting of incompatible detections and optionally parameter estimation. Sifting essentially comprises three steps. Firstly, since a large fraction of photons is lost in the fibre link or is not detected, Bob discloses which of the qubits he detected, without revealing the detected bit value. Secondly, Bob announces for each detection his randomly chosen measurement basis. Finally, Alice responds for each detection whether or not to discard it due to incompatible preparation and measurement basis. The first two sifting steps have to be performed as fast as possible in order to allow Alice to sift out undetected and incompatible

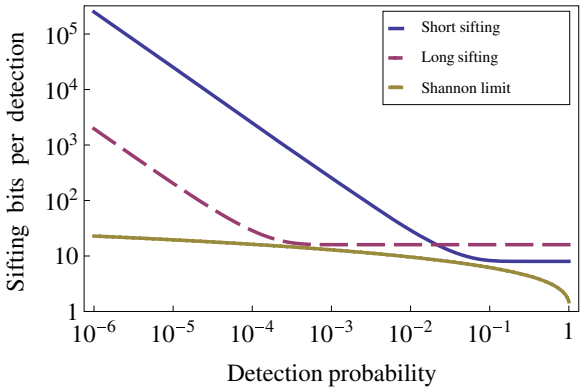

Figure 2. Number of bits per detection which have to be sent from Bob to Alice for detection times and base sifting. Blue corresponds to short sifting blocks optimized for detection probabilities >0.021, red uses longer sifting blocks optimized for lower detection probabilities. For comparison, the minimum amount given by the Shannon limit is shown in yellow (dashed).

bits from her memory before exceeding the available buffer size. In each sifting block, Bob encodes the detection time index of a detection relative to the index of the previous detection. Additionally, he attaches to each sifting block two control bits, which are used to indicate either the measurement basis for each detection, or empty blocks when no detection occurred during the maximum time that can be encoded in a single sifting block.

The number of bits exchanged during sifting has to be kept as small as possible, since this communication has to be authenticated at the cost of secret bits. The longer the fibre, the more bits are needed to indicate the time (number of clock cycles) passed between two succeeding detections. We switch to 14 bits instead of 6, for detection probabilities smaller than 2×10^{-2} per gate. As shown in figure 2, our way to encode the time information is very efficient (less than twice the Shannon limit) for detection probabilities between 10^{-1}–10^{-4} per gate.

Some QKD protocols, e.g. COW, use only one basis to obtain the raw key. All detection outcomes in the second basis are publicly revealed in order to estimate the *phase error* of the received quantum states. Bob reveals these measurement outcomes in the two control bits, too. If parameter estimation based on randomly revealing a fraction of detection outcomes is required for the quantum bit error rate (QBER) in the raw key, optionally a third control bit can be sent per detection. However, for the results we present here, we omit such sampling in favour of a more efficient solution as described below.

If double detections occur in both detectors at the same time, we only keep the result from one detector, e.g. for COW the data detector $\mathrm{SPD_D}$. If double detections occur in both time-bins of the same qubit, we assign a randomly chosen value. A logical deadtime between 8 ns and 10 μs can be applied after detection, during which all detections are discarded to reduce errors due to detector afterpulsing.

2.4. Error correction and verification module

Due to practical limitations in the preparation of the quantum states, and due to detector noise and jitter, Bob's sifted key differs from Alice's original key even in the absence of eavesdropping. Therefore, a forward error correction (FEC) code is implemented in the FPGA

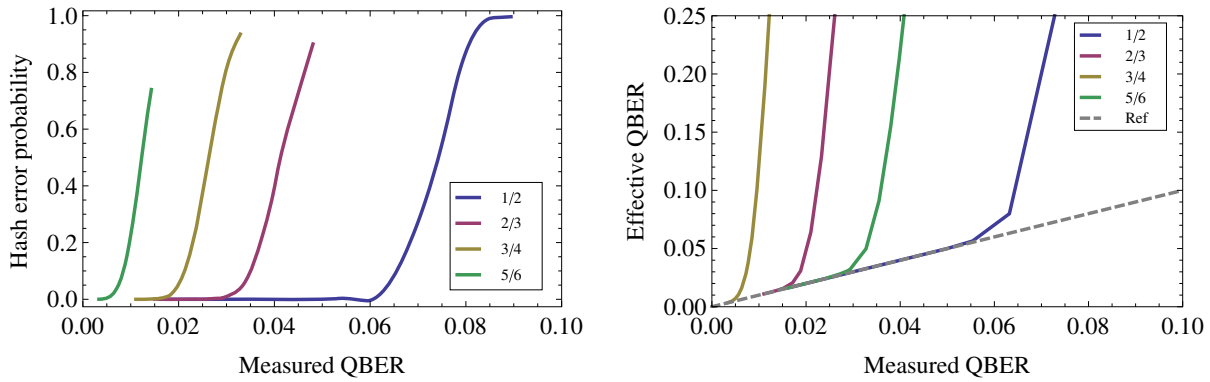

Figure 3. (left) Measurement results for different code rates showing the probability that the comparison between Alice and Bob's verification hash tags indicates at least one remaining error per 2048 bit block of error corrected keys. (right) Effective QBER under the conservative assumption that during each block with verification hash failure the eavesdropping attacks induced an error rate of 1/2.

as described in [22], which uses the quasi-cyclic low-density parity-check (LDPC) code defined in [23]. Error correction based on LDPC codes uses syndrome encoding with the advantage that only non-iterative one-way communication is required. Moreover, its efficiency in terms of revealed information can in principle approach the Shannon limit. Our FPGA implementation for LDPC performs FEC on blocks of 1944 bit length and provides rates up to 235 Mbps at 62.5 MHz clock frequency with ten decoding iterations. The LDPC code rate, i.e. the fraction of unpublished information, can be set to $f_{\mathrm{EC}}(Q) \in \{1/2, 2/3, 3/4, 5/6\}$ to adapt to the expected error rates. Bob calculates all syndromes for a constant expected error rate, and forwards them to Alice through an authenticated channel. Alice performs syndrome decoding and checks the parity. If an error occurred, the corresponding block is discarded. However, there is still a certain probability that uncorrected errors remain after error correction, especially for error rates larger than 6% (see figure 3, left). To detect remaining errors, we implement a subsequent verification step, where Bob transmits a 48-bit hash checksum per LDPC code block to Alice. The checksums are generated using polynomial hashing [3, 4], with a new random 48-bit seed for each checksum. The universal hash function is randomly chosen, and the collision probability on at least one of 512 subsequent blocks (corresponding to 995 328 bit input length for privacy amplification) is upper-bounded by $\varepsilon_{\mathrm{VER}} \leqslant 7.7 \times 10^{-11}$. For each block, the hash, as well as the random choice of hash function, is sent to Alice. If a checksum mismatch occurs, the associated block is discarded. Figure 3 (left) shows for all implemented code rates the probability that a verification fails as a function of the measured raw QBER.

2.5. Bit error estimation module

In every QKD protocol the number of errors of the received quantum states has to be estimated in order to determine an upper bound on the fraction of information which could have leaked to an eavesdropper. The standard procedure consists in random sampling of a subset of the sifted key, comparing the bit values over an authenticated channel and calculating the error rate in each basis. While straightforward, this method reduces the final secret key rate as all revealed outcomes have to be discarded. Most importantly, it has a substantial impact on

finite-key analysis, since a small sample gives only an imprecise estimate of the true error rate in the remaining, unrevealed detections.

To overcome these impairments, we perform parameter estimation exploiting our knowledge about the correctness of the key after verification. Once we obtain 512 blocks of 1944 error corrected and verified bits, Alice compares them with her original random bit sequence [24]. By counting the total number of mismatches, an exact number for the true bit errors is obtained. Additionally, we take into account blocks which were dropped due to checksum mismatches during error verification. We conservatively assume for each block with verification hash failure a maximum error rate of $1/2$ induced by eavesdropping attacks. In figure 3 (right) we show the resulting, effective QBER for different code rates as a function of the measured QBER. The failure probability for parameter estimation is then equal to the failure probability of error verification, i.e. $\varepsilon_{\mathrm{PE}} \leqslant 7.7 \times 10^{-11}$.

2.6. Privacy amplification module

Our FPGA implementation of privacy amplification uses Toeplitz hashing [3, 4], a construction for families of universal hash functions, in combination with linear-feedback shift register (LFSR) based hashing as proposed in [25, 26]. This approach is very efficient in terms of communication bandwidth needed to convey the chosen hash function, and allows parallelized computation and efficient, scalable implementation on the FPGA hardware.

The privacy amplification compression is the ratio between the length of the output and input keys, i.e. the ratio between the number of rows and columns of the Toeplitz matrix. In order to obtain high secret key rates based on finite-key analysis, we choose a fixed input length of 995 328 bits. As a consequence of this large block size, the size of the resulting matrix is such that it has to be stored in an external memory outside the FPGA. Our hardware implementation for privacy amplification has been shown to treat up to 48 Mbps input rate. Changing the output block length, the compression ratio can be adjusted over the full range between 0–100% in steps of 0.05%. We optimize and fix the compression ratio once in advance for a given scenario. Then, we verify for each key that the parameter estimates are indeed within the limits which guarantee security with the chosen compression ratio.

2.7. Authentication module

The classical communication channel is authenticated in order to prevent an eavesdropper from forging messages, which would open the door for man-in-the-middle attacks. For information-theoretically secure authentication, we use a combination [27] of $\varepsilon_{\mathrm{AUT}}$-almost strongly universal hash functions in combination with a strongly universal family of hash functions named polynomial hashing [3, 4], which is very efficient with respect to consumed secret bits as well as required operations. Bob randomly and secretly selects a hash function from this family to calculate a hash tag for each transmitted message, and sends the hash tags together with the messages to Alice. To verify that the transmission has not been forged, Alice has to know which hash functions Bob has chosen to be able to verify the hash tags for the received messages. Only when her calculated and the received tag for a message match, is it considered valid. We send a new 127-bit authentication tag for every 2^{20} bits of classical communication to obtain a collision probability of $\varepsilon_{\mathrm{AUT}} \leqslant 10^{-33}$. This approach would require 383 secret bits to select a new hash function for every tag. However, recently it has been shown that the same hash function can be reused for multiple authentication rounds if the tags attached to the messages [28] are one-time

pad encrypted. This authentication scheme is proven ε-universal-composable-secure if ε-almost strongly universal$_2$ hash functions are used and provides a bound for its information leakage. This strategy reduces the secret key consumption to one third, since only 127 bit secret keys are needed to encrypt each tag instead of 383 secret bits to select a new hash function.

2.8. Random number generation module

Random numbers are extensively needed during preparation for selecting the quantum states, as well as during key distillation, e.g. to generate the privacy amplification matrices. These random bits must be provided by true quantum random number generators (QRNGs), ideally QRNGs where up to 2 GHz output rates have been demonstrated [29] to date. However for the time being, we use a commercial QRNG (www.idquantique.com/random-number-generators/products.html) (certified by Swiss Federal Office of Metrology). Since its bit rate of 4 Mbps is by far not sufficient, we implement the NIST SP800-90 recommended AES (counter mode) cryptographically secure pseudo-random number generator that uses seeds of 256 bits provided by the QRNG to generate up to 1.1 Gbps random bits. We note that, due to AES, the random number expansion protocol is the only key distillation step for which we cannot provide an information-theoretic security statement.

2.9. Key manager

A fraction of the privacy amplified, secret keys is transferred by the key manager to the authentication module. Once their authenticity has been verified, the key manager distributes the remaining keys to an internal one-time pad encryption application, or via a PCI Express link to a PC and further to external consumers, e.g. network encryptors.

3. Coherent one-way protocol and implementation

The presented QKD system provides the flexibility to drive different QKD protocols [21]. In the following, we present the implementation of the COW protocol [30].

The COW protocol belongs to the class of distributed phase reference protocols and seeks to enable long fibre distance QKD while maintaining a simple and convenient setup. The advantages of the COW protocol are that it allows implementation of a completely passive receiver, without any active element for the choice of basis, requiring only two SPDs. Its implementation is robust against birefringence fluctuations, fibre transmission losses and photon number splitting attacks. A schematic of the setup is sketched in figure 1.

Following the COW protocol, Alice encodes each bit value by the choice of sending a weak coherent pulse in one out of two possible time-bins, while the other time-bin contains the vacuum state. Formally, these quantum states can be written as $|\beta_0\rangle_n = |\alpha\rangle_{2n}\,|\mathrm{vac}\rangle_{2n-1}$ and $|\beta_1\rangle_n = |\mathrm{vac}\rangle_{2n}\,|\alpha\rangle_{2n-1}$, where α is the complex coherent state amplitude with an average photon number per time bin $\mu = |\alpha|^2 < 1$, and n labels the qubit index. These states can be discriminated optimally by a simple time-of-arrival measurement. In addition, a third state called decoy sequence with both time-bins containing weak coherent pulses is randomly prepared, i.e. $|\beta_d\rangle_n = |\alpha\rangle_{2n}\,|\alpha\rangle_{2n-1}$.

As for distributed-phase-reference QKD, the integrity of the quantum channel is monitored using an unbalanced interferometer (IF). It measures the coherence between pulses in two successive, non-empty time-bins, either within a bit when a decoy sequence was prepared, or

across bit separation whenever corresponding sequences are prepared. The latter measurement across bit separation renders photon number splitting attacks on individual states less powerful as the adversary reduces the interference visibility if trying to discriminate individual states. As a consequence, the optimal average number of photons which can be sent per qubit becomes independent of the fibre transmission, but dependent on QBER and visibility. Security against zero error attacks and restricted collective attacks was proven, including imperfections of the state preparation [31]. Note that a general security proof was obtained for a modified COW protocol [32], which, however, involves more intricate hardware.

3.1. Alice's optical QKD module

The coherent light source is a continuous-wave distributed feedback laser diode (Agilecom) with a sufficiently long coherence time of >300 ns. It is compatible with the 100 GHz DWDM telecom standard, and its central wavelength regulated by a thermo-electric controller to $\lambda = 1551.72$ nm (ITU channel 32)[8].

An integrated $LiNbO_3$ intensity modulator (IM, Photline MX-LN 20) prepares the COW states. It tailors the continuous optical signal in a coherent train of short pulses, according to the states selected by the random number generator. The corresponding digital on–off signals are provided through the high-speed serial interfaces of the FPGA, reshaped to clean pulses of 50–400 ps duration and amplified to appropriate voltage levels for the IM input. The bias voltage is adjusted to maximize the optical pulse extinction ratio. Indeed, the extinction ratio of the IM limits the minimum QBER since spurious light in a supposedly empty time bin causes erroneous detections. Therefore, we use the QBER as feedback to re-adjust the IM bias voltage continuously. More than 25 dB extinction is achieved for 130 ps long pulses at a frequency of 625 MHz, limiting the expected QBER to 0.3%. Decoy sequences are prepared with a probability of 15.5%, close to the optimum, which allows for a sifted key rate as high as 73% of the raw key rate.

A micromirror based variable optical attenuator (Sercalo) attenuates the quantum signal down to the optimal photon level at Alice's output. Its value is optimized with respect to the QBER, visibility and other parameters as discussed later. The optical isolator prevents Trojan horse attacks (based on sending bright light from the outside). A 90:10 imbalanced fibre coupler and tap monitor diode allow continuous monitoring of Alice's output power and providing feedback to the variable optical attenuator to adjust the average number of photons per bit. Moreover, an unexpected increase of power in the monitor diode would indicate malfunction or a Trojan horse attack. Finally, a fixed, calibrated optical attenuator just before Alice's output reduces the average photon number per pulse to the optimal value.

3.2. Bob's optical QKD module

At Bob's quantum channel input, an optical isolator prevents information leakage due to detector backfiring or back-reflection of potential Trojan horse attacks. A 45 pm spectral fibre Bragg grating (aos) filter with 1.4 dB insertion loss and 14 dB isolation reduces incoming Raman noise. Subsequently, a fibre coupler C_B realizes the passive, random base choice and splits the quantum signals towards data and monitoring line. Its splitting ratio of 80:20 is close to optimal for the experimental settings used in the following.

[8] 2013 ITU-T Recommendation G.694.1 Spectral grids for WDM applications: DWDM frequency grid, 02.

Two SPDs are installed: SPD_D measures the photon arrival time in the data line to obtain the raw key, SPD_M detects the output of the unbalanced IF in the monitoring line. For the results presented in section 4, SPD_D is a sine gated InGaAs avalanche photo diode (APD) with a frequency of 1.25 GHz as described in [33]. Its gate width (full-width at half-maximum (FWHM)) is 130 ps, which proves to be a good trade-off between sufficiently low afterpulsing while maintaining good detection efficiency. The efficiency is varied in the range 6–10%, maximizing the final secret key rate. For the considered fibre distances, the dark counts are not the limiting factor and the highest key rate was indeed obtained at room temperature (20 °C). At this temperature, the dark count probability is about 10^{-6} per gate at 10% efficiency.

As the monitoring detection rate is much smaller, SPD_M is a free-running negative feedback InGaAs APD [34]. Applying 20 μs deadtime, its dark count rate was typically 800 Hz at 20% detection efficiency. Importantly, its timing jitter is only 200 ps (FWHM), sufficiently low to discriminate time-bins at 1.25 GHz. The gate times for both detectors are derived from the clock signal distributed over the service channel, and are digitally delayed to compensate for any temporal delay between quantum and service channels.

The Michelson type IF as sketched in figure 1 is made up of a fibre coupler with two Faraday mirrors terminating the two arms. The arms are cut such that the length difference corresponds to half the separation between consecutive time bins. The measured free-spectral range of 1.247 GHz matches very well the target frequency of 1.25 GHz. The IF has 1.3 dB insertion loss and a maximum visibility >0.998. It is thermally well isolated and actively temperature stabilized. The relative phase, however, is adjusted by tuning Alice's laser wavelength such that two succeeding pulses interfere destructively and do not generate detector clicks. In contrast, non-interfering pulse sequences are distributed randomly between the two output ports of the IF. Using detections due to both interfering and non-interfering sequences, we compute the visibility as described at the end of appendix. Note that the second output port could be monitored via an additional circulator at the cost of increased insertion loss and the need of a third detector. This would slightly increase the secret key fraction, as Eve's information could be estimated more precisely.

3.3. Mechanical housing and DWDM modules

Each QKD device is integrated in a 19 inch 2U housing as shown in figure 4. It provides a power input, a single mode fibre connector (APC) for the quantum channel, a PCI-Express link to the control PC and two SFP slots for the service channel and an optional external encryptor. Importantly, despite these connectors the mechanical housing is perfectly encapsulated from the environment to prevent any physical attack point other than through the optical fibre. In particular, the arrangement of all components has been carefully chosen to maintain efficient heat release and to guarantee maximum stability, while the cooling air only flows around the outside of the devices without entering.

During all key exchanges presented here, we used one single optical fibre and DWDM of quantum and all classical channels. We implemented external DWDM modules for Alice and Bob in separate 19-inch 1U cases, comprising a 100 GHz multiplexer (OptiWorks) and a variable optical attenuator (OptoLink) to minimize the power of the transmitted classical channels. The multiplexers have an isolation of 80 dB and an insertion loss of 1.8 dB.

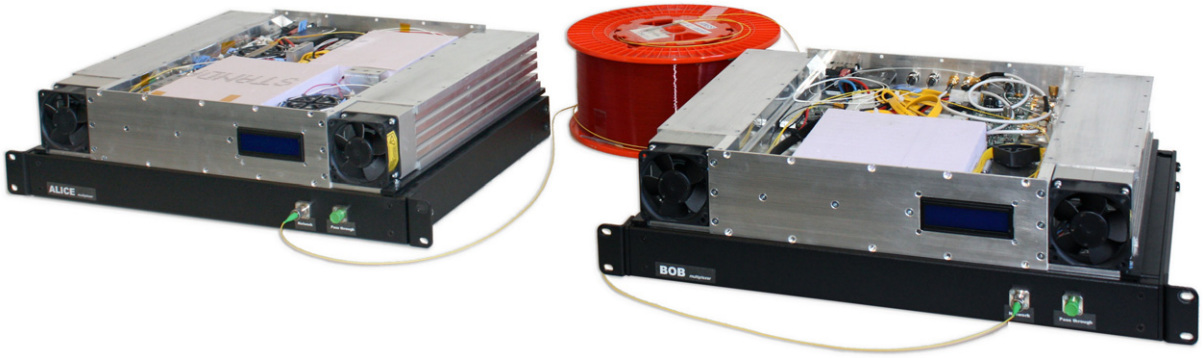

Figure 4. Photo of the opened QKD devices. Each system is compatible with 19-inch 2U industrial cases and houses all the electronics, optics and interfaces to distribute quantum keys, using the QKD keys for Ethernet authentication and one-time pad encryption, and to additionally supply them to external consumer devices. In consideration of security aspects, their interior is completely mechanically encapsulated, while thermal stabilization is provided by two external fans. Using external 19 inch 1U DWDM modules (bottom), both devices were connected by only one single telecom fibre and have demonstrated stable QKD functionality with a security guarantee of $\varepsilon_{\mathrm{QKD}} = 4 \times 10^{-9}$ over more than 25 km distance.

3.4. Practical security considerations

While security proofs for QKD assume ideal, well implemented devices, practical hacking against imperfections of experimental systems has been demonstrated. We designed our system considering known attacks: Alice's device is protected against Trojan horse attacks by an optical isolator in combination with the attenuators and tap monitor as shown in figure 1. At Bob's device, the isolator and spectral filter protect against information leakage due to reflected photons or detector backfiring. Attacks which exploit detector efficiency mismatches [35], e.g. time-shift attacks, can be ruled out since only one detector is used to discriminate the bit values. Similarly, information leakage due to optical side channels of the source is prevented by using only one laser and the same modulator to prepare all quantum states.

Another powerful attack is the so-called detector blinding attack [36, 37]. However, due to the large imbalance of Bob's fibre coupler for passive random base choice (C_B in figure 1) this attack is unlikely to work if two similar photo diodes are used [38]. Moreover, this attack would significantly increase the photo current [39], which we continuously monitor for both detectors independently. In order to prevent attacks exploiting the dead time of the monitor detector, a conservative approach is to disregard detections in the data detector during this time. However, this is not necessary if the eavesdropper does not know when the monitor detector clicks. This is the case if the detections are announced only after a certain delay, and the detector is not saturated. Extensive testing of the practical security is the subject of future work.

4. Experimental results

We tested the system over fibre lengths between 1–50 km using rapid sine gated SPDs [33] as well as free-running SPDs (id220, IDQ). All classical and quantum communication channels

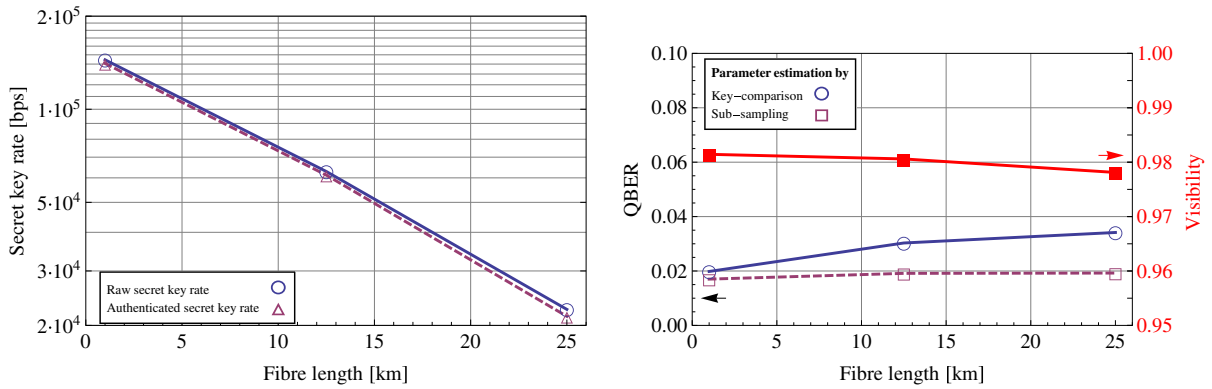

Figure 5. (left) Secret key rates after privacy amplification (blue circles) and authenticated secret key rate (purple triangles) which accounts for secret key consumption for authenticating the classical communication channel. We considered a security analysis that respects finite-key-size effects, authentication costs and system errors with a security parameter of $\varepsilon_{\mathrm{QKD}} = 4 \times 10^{-9}$. (right) QBER and raw visibility results before removing dark counts.

were multiplexed onto a common fibre. Using different configurations of the distillation engine we optimized the key rates for a security parameter of 4×10^{-9}, while respecting a security analysis for finite-key-size effects, authentication costs and system errors.

For the measurements which we discuss in the following, we obtained the highest secret key rate using an LDPC error correction code rate of 3/4, parameter estimation based on key comparison and longer sifting blocks to encode the detection times in 14 bits. The secret key rate, which is provided by the FPGA distillation engine after privacy amplification, is shown in figure 5 (left, circle). Multiplexing quantum and classical channels over a single 1 km fibre, secret keys were distributed at a rate of 144.5 kbps. Over a single 25 km long fibre, after privacy amplification, we obtained a secret key rate of 22.5 kbps. The useful rate of secret bits available for applications, e.g. internal one-time-pad encryption or external encryptors is shown as red triangles in figure 5 and accounts for secret bit consumption to encode the authentication tags.

4.1. Parameter optimization

For each setting we optimized several parameters to maximize the final authenticated secret key rate. These are summarized in table 1. For longer fibres, the average photon number was increased and the detection efficiency decreased in order to compensate for increasing DWDM noise (Raman scattering and crosstalk) and dark counts. As such, the QBER was maintained close to the maximum QBER, which could be efficiently corrected with the chosen LDPC code rate (see figure 3). For the different fibre lengths we obtained a QBER (before subtracting dark counts) as shown in figure 5 (right). The QBER increases for longer fibres and is considerably larger than the error rate, which we estimated using sub-sampling instead. This additional contribution stems from blocks of error corrected bits, which have not passed the subsequent hash tag verification. For these blocks we conservatively attribute *a priori* an error rate of 1/2 to the eavesdropper. Thus, with a verification failure probability of 3.1% for a 25 km fibre, the QBER that we take into account increases above 3.4%. Nevertheless, we verified that in the presented configurations the final secret key rate was still higher compared to configurations

Table 1. Parameters and measurement results summarizing the performance of the QKD prototype for information theoretic secure key distribution with a security parameter of 4×10^{-9}.

Fibre length (km)	1 km	12.5 km	25 km
Pulse amplitude μ	0.089	0.084	0.105
Detection efficiency (%)	9.6	7.3	6.9
Compression factor (%)	11.5	12.0	6.5
LDPC code rate	3/4	3/4	3/4
QBER (%) (raw/verified)	$1.70 \pm 0.01/1.98$	$1.87 \pm 0.02/3.03$	$1.91 \pm 0.03/3.42$
Dark count contribution	0.41	0.76	0.85
DWDM noise contribution	0.05	0.11	0.19
Raw visibility (%)	98.14 ± 0.14	98.06 ± 0.13	97.81 ± 0.13
Sifted key rate (bps)	$(1.26 \pm 0.006) \times 10^6$	$(5.38 \pm 0.032) \times 10^5$	$(3.59 \pm 0.042) \times 10^5$
Secret key rate (bps)	1.45×10^5	6.29×10^4	2.25×10^4
Authenticated key rate (bps)	1.41×10^5	6.12×10^4	2.14×10^4

with parameter estimation based on sub-sampling, since the impairment due to verification failures is overcompensated by the advantage that no bits have to be revealed and discarded. Similarly, we found that smaller error correction code rates did not result in higher key rates.

The raw visibility (before subtracting dark counts) in figure 5 (right, red) remains almost constant for all fibre lengths. It drops slightly, below 97%, for long fibres due to increasing DWDM noise and dark count detections. Mainly determined by the visibility and photon number, and with slight dependence on the QBER, we applied privacy amplification with a compression factor of 11.5% for a fibre of 1 km length, which dropped to 6.5% for 25 km.

4.2. Stability

In figure 6 we show the stability in terms of key rates, QBER and visibility for an autonomous QKD run over a period of more than 11 hours using a single 12.5 km DWDM fibre link. The results clearly reflect the good stability of all system components including synchronization and alignment, Alice's state preparation, Bob's IF and SPDs, and the whole distillation engine. The average raw QBER as measured by comparing Alice's error corrected key with her original key was 1.91% over the whole measurement period (figure 6, right). The raw visibility before subtracting dark counts had an average of 98.1%, and was constantly above 97.0%. Considering finite-key security with $\epsilon_{\mathrm{QKD}} = 4 \times 10^{-9}$, we applied a compression factor of 0.12, and accounting for the fraction of blocks which were discarded due to verification failures, the resulting secret key rate was 62.9 kbps.

During two live presentations at conferences[9], we have demonstrated the robustness, stability and reliability of our QKD system. Over periods of 2 and 5 days, the system ran continuously and provided, at a rate of more than 30 times per second, new secret 128 bit keys to network encryptors, which used the keys for AES encryption of user data and video streams.

[9] Nano-Tera 2013, Annual Plenary Meeting (30–31 May 2013, Bern, Switzerland) and QCrypt 2013, 3rd International Conference on Quantum Cryptography (5–9 August 2013, Waterloo, Canada).

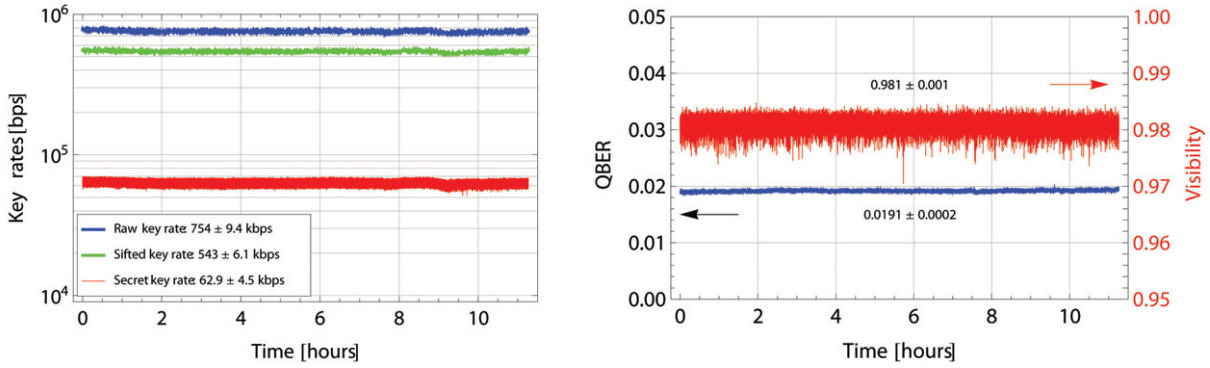

Figure 6. Key rates (left), QBER and visibility (right) demonstrating the stability of an autonomous QKD run for a period of more than 11 hours. Alice's and Bob's devices were connected by a single 12.5 km fibre. The secret key rate (left, red) accounts for finite-key effects, the authenticated key rate (left, purple) for the consumption of secret keys to encrypt the authentication tags.

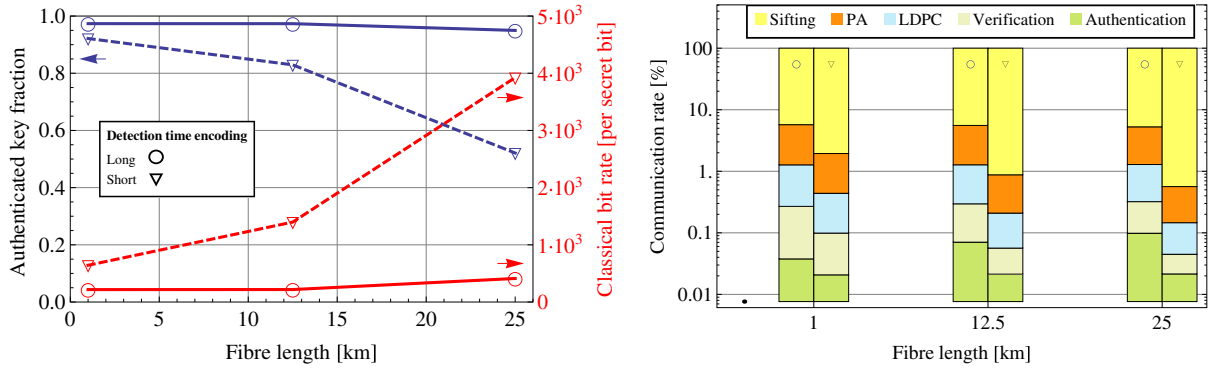

Figure 7. Amount of classical information accompanying QKD. (left) Total communication rates per secret bit and fraction of secret bits remaining after authenticating the classical communication channels. At least 2.7% of secret bits are consumed for authentication, i.e. to encrypt the authentication tags of 127 bits per 10^6 bits of classical communication. (right) Communication rates broken down by individual sub-protocols for the considered fibre lengths. The rates are dominated by the amount of sifting information sent from Bob to Alice, which adds up to 94–99%, depending on the specific configuration.

4.3. Authentication costs

The secret key rates usually presented are the key rates after privacy amplification, i.e. they do not account for secret bit consumption to encode the authentication tags. Therefore, figure 7 shows the amount of classical communication accompanying key distillation as well as the fraction of secret bits which are consumed to encrypt authentication tags of 127 bit per 10^6 bits of classical communication. The left side of figure 7 shows the amount of classical information which has to be communicated normalized per secret bit, as well as in terms of authenticated fraction of secret bits left after authentication. It reveals that, for all considered fibre lengths, the least fraction of secret bits consumed for authentication is obtained if we use long sifting blocks and parameter estimation based on key comparison (circles). For a fibre of 1 km length,

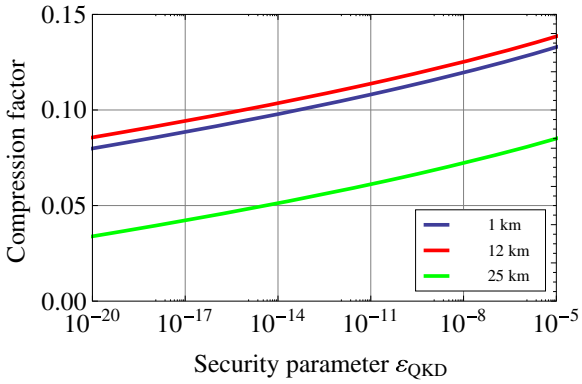

Figure 8. Projected compression factors as a function of the security parameter $\varepsilon_{\mathrm{QKD}}$ for fibre lengths of 1 km (blue), 12.5 km (red) and 25 km (green). All other parameters are taken from table 1.

217 classical bits have to be communicated per secret bit. Correspondingly, a fraction of 2.7% of secret bits is needed for authenticating this communication, i.e. the authenticated key rate amounts to 97.3%. It increases up to 412 bits of classical communication per secret bit for a 25 km fibre, where 5.0% of secret bits are needed for authentication, corresponding to an authenticated key rate of 95.0%. Much more classical information has to be sent and authenticated, if short sifting blocks with only 6 bits instead of 14 bits are used to encode the detection times, and nearly 20% of all secret bits are consumed for authentication (triangles in figure 7).

The origin of the different authentication losses is illustrated in figure 7 (right), where we compare the communication rates broken down by each individual sub-protocol. With more than 94% the largest amount of information is sent for sifting. More than one order of magnitude less, up to 4.5%, for communicating the randomly chosen Toeplitz matrices for privacy amplification. At most 1.2% of all classical communication is attributed to error correction including communication of the verification hash function and value, and less than 0.1% for authentication. Using shorter sifting blocks (triangles in figure 7), the relative amount of sifting information becomes even larger, giving rise to larger authentication loss. However, we expect that the shorter blocks used to encode the detection times become advantageous as soon as higher detection rates are obtained. This would be the case when detectors with higher detection efficiency are used, e.g. superconducting SPDs, or two fibre links instead of one, which would eliminate optical losses in multiplexers and spectral filters. When we used parameter estimation based on sub-sampling instead of key comparison, the amount of classical communication was 12.6% larger for all fibre lengths, corresponding to the fraction of bits which were revealed and discarded.

5. Conclusions and outlook

To conclude, we have presented a fully integrated versatile QKD platform that comprises a hardware key distillation engine, DWDM of quantum and all classical communication channels, and fast sine gating detectors. We demonstrated its stable performance for the COW protocol, and rigorously took into account all aspects which guarantee security in finite key scenarios with a security parameter of 4×10^{-9}. Our QKD platform has the flexibility to not only support the

COW protocol, but additionally provides all the means to run the DPS QKD protocol, as well as phase-time qubit BB84. The system is compactly mounted in standard industrial 19 inch 2U housings.

The particular choice of the security parameter value $\varepsilon_{\mathrm{QKD}}$ can to some extent be adapted to specific user requirements. In our current implementation the total security parameter is mainly limited to 7×10^{-11} by the failure probability of the error verification process. A simple increase of the error verification hash tag size from 48 bit to 72 bit would reduce this limit to approximately 10^{-20}. The security parameter can be improved by only reducing the privacy amplification compression factor, however, at the cost of the secret key rate. In figure 8 we show the projected compression factors as a function of $\varepsilon_{\mathrm{QKD}}$, using the same parameters and results of table 1. It can be seen that an adaptation of the compression factor to a security parameter of $\varepsilon_{\mathrm{QKD}} = 10^{-20}$ would reduce the secret key rate to 50–70%, depending on the fibre length.

All results were obtained using a one-fibre DWDM configuration with all quantum and classical communication channels multiplexed in one common fibre and taking into account finite key security for a block size of 10^6 bits. However, we want to stress that depending on the specific usage scenario and security requirements, the maximum secret key rate as well as the maximum fibre length can easily be increased. As an example, we performed the same set of measurements while neglecting finite-key effects, and obtained after authentication an asymptotic key rate of 293 kbps and 1.3 kbps for fibre lengths of 1 and 50 km, respectively. A further increase by more than a factor of two in both key rate and distance can be expected if instead of multiplexing all channels over one single fibre, two fibres are available, one dark fibre for the quantum channel and a second fibre for the classical communication channels.

Acknowledgments

We gratefully acknowledge the valuable discussions with Renato Renner, Marcos Curty, Christoph Pacher, Jesús Martínez Mateo and David Elkouss. Furthermore, we thank Hervé Gouraud from Photline for his kind support. This research project was financially supported by the Swiss Nano-Tera project QCRYPT and the National Center of Competence in Research QSIT.

Appendix. COW finite-key rates

We consider a COW transmitter at Alice as depicted in figure 1 which prepares time-bin qubits with a frequency f_{Q}. In general, the prepared quantum state after a time $t_{\mathcal{N}} = \mathcal{N}/f_{\mathrm{Q}}$ can be written in the form of a product state

$$|\Psi\rangle_{\mathcal{N}} = \otimes_{n=1}^{\mathcal{N}} |\psi\,(b_n, v_n)\rangle_n \tag{A.1}$$

$$|\psi\,(b_n, v_n)\rangle_n = \otimes_{i=0}^{n_{\mathrm{bit}}-1} |\alpha\,(b_n, v_n, i)\rangle_{n\cdot n_{\mathrm{bit}}-i} \tag{A.2}$$

of coherent quantum states $|\alpha\rangle_\tau$. Their complex amplitudes α in temporal mode τ depend on Alice's random choice of basis $b_n \in \{0, 1\}$ and bit value $v_n \in \{0, 1\}$. We have introduced a parameter $n_{\mathrm{bit}} = f_{\mathrm{gate}}/f_{\mathrm{Q}}$ that accounts for the implementations where n_{bit} successive temporal modes are used to distinguish the states. It is $n_{\mathrm{bit}} = 2$ for COW and BB84 phase-time

qubits, while for DPS $n_{\mathrm{bit}} = 1$. Whenever Alice chooses $b_n = 0$, she prepares a quantum state corresponding to a bit value

$$|\psi\ (0,0)\rangle_n = \left|\sqrt{\frac{\mu}{(1+\eta_{\mathrm{IM}})}}\right\rangle_{2n} \otimes \left|\sqrt{\frac{\eta_{\mathrm{IM}}\cdot\mu}{(1+\eta_{\mathrm{IM}})}}\right\rangle_{2n-1},$$
$$|\psi\ (0,1)\rangle_n = \left|\sqrt{\frac{\eta_{\mathrm{IM}}\cdot\mu}{(1+\eta_{\mathrm{IM}})}}\right\rangle_{2n} \otimes \left|\sqrt{\frac{\mu}{(1+\eta_{\mathrm{IM}})}}\right\rangle_{2n-1}. \tag{A.3}$$

Here, $\mu = |\alpha^2|$ is the mean value of the Poissonian distributed number of photons per coherent state, and $0 \leqslant \eta_{\mathrm{IM}} \leqslant 1$ accounts for a limited extinction ratio of the intensity modulator. In the ideal case it is $\eta_{\mathrm{IM}} = 0$ and equation (A.3) becomes $|\sqrt{\mu}\rangle \otimes |0\rangle$ and $|0\rangle \otimes |\sqrt{\mu}\rangle$. Whenever Alice chooses $b_n = 1$ with probability p_{Decoy} a decoy sequence, irrespective of the bit value she prepares

$$|\psi(1,0)\rangle_n = |\psi\ (1,1)\rangle_n = |\sqrt{\mu}\rangle_{2n} \otimes |\sqrt{\mu}\rangle_{2n-1}. \tag{A.4}$$

The goal of Alice and Bob is to maximize the COW secret key rate (per prepared state) r_{sec}, which can be distilled from the transmitted and detected states

$$r_{\mathrm{sec}} = r_{\mathrm{det}} \cdot \beta_{\mathrm{sift}} \cdot \beta_{\mathrm{est}} \cdot f_{\mathrm{sec}} \cdot \beta_{\mathrm{auth}} \tag{A.5}$$
$$= r_{\mathrm{sift}} \cdot (1-\eta_{\mathrm{PE}}) \cdot f_{\mathrm{sec}} \cdot (1-\eta_{\mathrm{MAC}}), \tag{A.6}$$

where r_{det} is the detection rate (per prepared bit) in Bob's detector $\mathrm{SPD_D}$. Further, β_{sift}, β_{est}, f_{sec} and β_{aut} signify the key size reductions during sifting, parameter estimation, privacy amplification and authentication, respectively. In the considered COW implementation, a fraction $\beta_{\mathrm{sift}} = \left(1 - p_{\mathrm{Decoy}}\right) / \left(1 + p_{\mathrm{Decoy}}\right)$ of all detections in $\mathrm{SPD_D}$ is discarded during sifting. Furthermore, $\beta_{\mathrm{est}} = 0.875$ if we perform parameter estimation based on sub-sampling, and $\beta_{\mathrm{est}} = 1$ if we estimate the QBER by key comparison.

Including finite-key-size effects, the secret key fraction f_{sec} under the assumption of a restricted collective attack [31] is given for a QBER Q by the Devetak–Winter bound

$$f_{\mathrm{sec}} = 1 - \mathrm{leak_{EC}} - \mathrm{leak_{VER}}(Q+\delta Q) - (1-Q-\delta Q)\cdot h\left[\frac{1+\Delta}{2}\right] - \beta_{\mathrm{smooth}} - \beta_{\mathrm{EC}} - \beta_{\mathrm{PA}}. \tag{A.7}$$

The leakage of the error correction scheme $\mathrm{leak_{EC}}$ is in the ideal case the binary entropy $h\,[Q]$, while in the implementation at present, $\mathrm{leak_{EC}} = 1 - f_{\mathrm{EC}}$, with the chosen LDPC code rate $f_{\mathrm{EC}} \in \{5/6, 3/4, 2/3, 1/2\}$. The leakage from the verification step after error correction amounts to $\mathrm{leak_{VER}} = l/b = 0.023$ with $l = 48$ bits the length of each verification hash tag and $b = 2048$ bits the block length per verification. The overlap $\Delta = |\langle\psi_1|\psi_0\rangle|$ between the two bit states is for an observed visibility V

$$\Delta = (2\ (V-\delta V) - 1)\ \mathrm{e}^{-\mu} - 2\sqrt{1-\mathrm{e}^{-2\mu}}\ \sqrt{(V-\delta V)\cdot(1-(V-\delta V))}. \tag{A.8}$$

Due to the finite post-processing size we include statistical fluctuations of expected QBER and visibility values, given by analysis based on interval estimation. For parameter estimation based on sub-sampling, it is [40, 41]

$$\delta Q = \sqrt{\frac{1+\eta_{\mathrm{PE}}\,(n_{\mathrm{PP}}-1)}{(\eta_{\mathrm{PE}}\ n_{\mathrm{PP}})^2}\log\left[\frac{1}{\epsilon_{\mathrm{PE}}}\right]} \tag{A.9}$$

In contrast, for parameter estimation based on key comparison, no uncertainty from statistical fluctuations impairs the QBER, i.e.

$$\delta Q = 0. \tag{A.10}$$

However, in both cases the deducible visibility is limited by an uncertainty δV due to the finite-key-size as

$$\delta V = \sqrt{\frac{1}{2}\left(\log\left[\frac{1}{\epsilon_{\mathrm{PE}}^{V}}\right] + 2\log\left[n_V + 1\right]\right)/n_V}. \tag{A.11}$$

n_V is the number of useful detections in the monitor detector from which the visibility is calculated. In the trusted detector scenario the secret key rate is optimized using QBER and visibility values that are corrected for detector errors, which cannot be exploited or manipulated by an eavesdropper, e.g. dark counts. For the leakage term in equation (A.7), the uncorrected QBER value must be considered.

Furthermore, we account in equation (A.7) for the reduction β_{smooth} due to uncertainty induced by smoothing the min-entropy, and the failure probabilities β_{EC} and β_{PA} of the error correction and privacy amplification protocols [41]

$$\beta_{\mathrm{smooth}} = 7\sqrt{\log_2\left[\frac{2}{\varepsilon_{\mathrm{Smooth}}}\right]/n_{\mathrm{PP}}}, \tag{A.12}$$

$$\beta_{\mathrm{EC}} = \log_2\left[\frac{2}{\varepsilon_{\mathrm{EC}}}\right]/n_{\mathrm{PP}}, \tag{A.13}$$

$$\beta_{\mathrm{PA}} = 2\log_2\left[\frac{1}{\varepsilon_{\mathrm{PA}}}\right]/n_{\mathrm{PP}}, \tag{A.14}$$

where the respective ε-parameters specify the confidence interval. For the presented implementation, the key length after parameter estimation $n_{\mathrm{PP}} = \beta_{\mathrm{est}}\, n_{\mathrm{SIFT}}$ equals the sifted key rate as no bit values are revealed for estimating Q. Instead, the errors are measured by comparing the original bit string with the corrected one, which limits $\varepsilon_{\mathrm{EC}}$ to the confidence interval of subsequent error verification ($\varepsilon_{\mathrm{EC}} = \varepsilon_{\mathrm{VER}} = 8 \times 10^{-11}$). The total security parameter of the system is then fixed by the sum

$$\varepsilon_{\mathrm{QKD}} = \varepsilon_{\mathrm{sec}} = \varepsilon_{\mathrm{VIS}} + \varepsilon_{\mathrm{Smooth}} + \varepsilon_{\mathrm{PA}} + 2\,\varepsilon_{\mathrm{VER}} + \varepsilon_{\mathrm{MAC}} = 4 \times 10^{-9}. \tag{A.15}$$

Note the factor of two for $\varepsilon_{\mathrm{VER}}$ to account for failures in the QBER measure as well as the verification step.

As a first input parameter we fix the number of bits n_{SIFT} after sifting entering the further distillation post-processing, which in our system is limited by the allocated hardware memory to $n_{\mathrm{SIFT}} = 995\,328$ bits. The number of useful detections in the monitoring detector n_V (which is used to estimate the visibility) is

$$n_V = n_{\mathrm{SIFT}}\,\frac{p_{\mathrm{Decoy}} + \frac{(1+p_{\mathrm{Decoy}})^2}{4}}{1 - p_{\mathrm{Decoy}}}\,\frac{(1 - t_{\mathrm{B}})}{t_{\mathrm{B}}}. \tag{A.16}$$

Here, the first factor is the normalization since we use all useful monitor detections, the second factor specifies the number of useful events due to decoy sequences and combinations across bit

separations, and the third factor accounts for the beam splitting ratio. Any additional losses or differences in the detection efficiencies between data and monitor detector can be incorporated by a respective choice of the beam splitting ratio t_B and detection efficiency η_D.

Note that an additional detector at the bright IF port is not necessary. Instead, we count the number of detections N_{int} due to sequences which should destructively interfere and not be detected in the dark port, and the number of detections N_{non} due to non-interfering sequences. Then, the visibility V is obtained by calculating

$$V = 1 - \frac{N_{int}}{N_{non}} \frac{p_{non}}{p_{int}}, \tag{A.17}$$

where p_{non}/p_{int} is the ratio between the number of interfering and non-interfering sequences sent.

References

[1] Shannon C E 1948 A mathematical theory of communication *Bell Syst. Tech. J.* **27** 379–423 and 623–56

[2] Vernam G S 1926 Cipher printing telegraph systems for secret wire and radio telegraphic communications *J. Am. Instrum. Electron. Eng.* **45** 295–301

[3] Lawrence Carter J and Wegman M N 1979 Universal classes of hash functions *J. Comput. Syst. Sci.* **18** 143–54

[4] Wegman M N and Lawrence Carter J 1981 New hash functions and their use in authentication and set equality *J. Comput. Syst. Sci.* **22** 265–79

[5] Bennett C H and Brassard G 1984 Quantum cryptography: public key distribution and coin tossing *Proc. Int. Conf. on Computers, Systems and Signal Processing* (Piscataway, NJ: IEEE) pp 175–9

[6] Gisin N, Ribordy G, Tittel W and Zbinden H 2002 Quantum cryptography *Rev. Mod. Phys.* **74** 145–95

[7] Bennett C, Bessette F, Brassard G, Salvail L and Smolin J 1992 Experimental quantum cryptography *J. Cryptol.* **5** 3–28

[8] Muller A, Herzog T, Huttner B, Tittel W, Zbinden H and Gisin N 1997 'Plug and play' systems for quantum cryptography *Appl. Phys. Lett.* **70** 793–5

[9] Dixon A R, Yuan Z L, Dynes J F, Sharpe A W and Shields A J 2010 Continuous operation of high bit rate quantum key distribution *Appl. Phys. Lett.* **96** 161102

[10] Tanaka A *et al* 2012 High-speed quantum key distribution system for 1-Mbps real-time key generation *IEEE J. Quantum Electron.* **48** 542–50

[11] Stucki D, Walenta N, Vannel F, Thew R T, Gisin N, Zbinden H, Gray S, Towery C R and Ten S 2009 High rate, long-distance quantum key distribution over 250 km of ultra low loss fibres *New J. Phys.* **11** 075003

[12] Wang S, Chen W, Guo J-F, Yin Z-Q, Li H-W, Zhou Z, Guo G-C and Han Z-F 2012 2 GHz clock quantum key distribution over 260 km of standard telecom fiber *Opt. Lett.* **37** 1008–10

[13] Chapuran T E *et al* 2009 Optical networking for quantum key distribution and quantum communications *New J. Phys.* **11** 105001

[14] Eraerds P, Walenta N, Legre M, Gisin N and Zbinden H 2010 Quantum key distribution and 1 Gbps data encryption over a single fibre *New J. Phys.* **12** 063027

[15] Xavier G B, Vilela de Faria G, Ferreira da Silva T, Temporão G P and von der Weid J P 2011 Active polarization control for quantum communication in long-distance optical fibers with shared telecom traffic *Microw. Opt. Technol. Lett.* **53** 2661–5

[16] Patel K A, Dynes J F, Choi I, Sharpe A W, Dixon A R, Yuan Z L, Penty R V and Shields A J 2012 Coexistence of high-bit-rate quantum key distribution and data on optical fiber *Phys. Rev.* X **2** 041010

[17] Mink A, Bienfang J C, Carpenter R, Ma L, Hershman B, Restelli A and Tang X 2009 Programmable instrumentation and gigahertz signaling for single-photon quantum communication systems *New J. Phys.* **11** 045016

[18] Jouguet P, Kunz-Jacques S, Leverrier A, Grangier P and Diamanti E 2013 Experimental demonstration of long-distance continuous-variable quantum key distribution *Nature Photon.* **3** 378–81
[19] Martinez-Mateo J, Elkouss D and Martin V 2013 Key reconciliation for high performance quantum key distribution *Sci. Rep.* **3** 1–6
[20] Constantin J, Houlmann R, Preyss N, Walenta N, Zbinden H and Burg A 2013 An FPGA-based secret key distillation engine for quantum key distribution systems (in preparation)
[21] Korzh B, Walenta N, Houlmann R and Zbinden H 2013 A high-speed multi-protocol quantum key distribution transmitter based on a dual-drive modulator arXiv:1306.5940
[22] Roth C, Meinerzhagen P, Studer C and Burg A 2010 A 15.8 pJ/bit/iter quasi-cyclic LDPC decoder for IEEE 802.11n in 90 nm CMOS *IEEE Asian Solid State Circuits Conf. (A-SSCC) (Beijing, Republic of China, November 2010)* (Piscataway, NJ: IEEE) pp 1–4
[23] IEEE 2009 Standard for IEEE information technology—telecommunications and information exchange between systems—local and metropolitan area networks—specific requirements: 11. Wireless medium LAN access control (MAC) and physical layer (PHY) specifications amendment: 5. Enhancements for higher throughput *IEEE Std 802.11n-2009* (Piscataway, NJ: IEEE) pp c1–565 10
[24] Pacher C, Lechner G, Portmann C, Maurhart O and Peev M 2012 Efficient QKD postprocessing algorithms *2nd Annu. Conf. on Quantum Cryptography (QCrypt 2012) (Singapore)* Poster presentation
[25] Mansour Y, Nisan N and Tiwari P 1993 The computational complexity of universal hashing *Theor. Comput. Sci.* **107** 121–33
[26] Krawczyk H 1994 *LFSR-Based Hashing and Authentication, Proc. 14th Annu. Int. Conf. on Advances in Cryptology* (Berlin: Springer) pp 129–39
[27] Stinson D R 1994 Universal hashing and authentication codes *Designs, Codes and Cryptography* **4** 369–80
[28] Portmann C 2012 Key recycling in authentication arXiv:1202.1229 [cs.IT]
[29] Symul T, Assad S M and Lam P K 2011 Real time demonstration of high bitrate quantum random number generation with coherent laser light *Appl. Phys. Lett.* **98** 231103
[30] Stucki D, Brunner N, Gisin N, Scarani V and Zbinden H 2005 Fast and simple one-way quantum key distribution *Appl. Phys. Lett.* **87** 194108
[31] Branciard C, Gisin N and Scarani V 2008 Upper bounds for the security of two distributed-phase reference protocols of quantum cryptography *New J. Phys.* **10** 013031
[32] Moroder T, Curty M, Ci Wen, Lim C, Thinh L P, Zbinden H and Gisin N 2012 Security of distributed-phase-reference quantum key distribution *Phys. Rev. Lett.* **109** 260501
[33] Walenta N, Lunghi T, Guinnard O, Houlmann R, Zbinden H and Gisin N 2012 Sine gating detector with simple filtering for low-noise infra-red single photon detection at room temperature *J. Appl. Phys.* **112** 063106
[34] Lunghi T, Barreiro C, Guinnard O, Houlmann R, Jiang X, Itzler M A and Zbinden H 2012 Free-running single-photon detection based on a negative feedback InGaAs APD *J. Mod. Opt.* **59** 1481–8
[35] Makarov V, Anisimov A and Skaar J 2006 Effects of detector efficiency mismatch on security of quantum cryptosystems *Phys. Rev.* A **74** 022313
[36] Makarov V 2009 Controlling passively quenched single photon detectors by bright light *New J. Phys.* **11** 065003
[37] Sauge S, Lydersen L, Anisimov A, Skaar J and Makarov V 2011 Controlling an actively-quenched single photon detector with bright light *Opt. Express* **19** 23590–600
[38] Lydersen L, Skaar J and Makarov V 2011 Tailored bright illumination attack on distributed-phase-reference protocols *J. Mod. Opt.* **58** 680–5
[39] Yuan Z L, Dynes J F and Shields A J 2011 Resilience of gated avalanche photodiodes against bright illumination attacks in quantum cryptography *Appl. Phys. Lett.* **98** 231104
[40] Sano Y, Matsumoto R and Uyematsu T 2010 Secure key rate of the BB84 protocol using finite sample bits *J. Phys. A: Math. Theor.* **43** 495302
[41] Tomamichel M, Ci Wen, Lim C, Gisin N and Renner R 2012 Tight finite-key analysis for quantum cryptography *Nature Commun.* **3** 634