OPEN ACCESS

Quantum key distribution and 1 Gbps data encryption over a single fibre

New Journal of Physics
The open-access journal for physics

Quantum key distribution and 1 Gbps data encryption over a single fibre

P Eraerds[1,3], N Walenta[1,3], M Legré[2], N Gisin[1] and H Zbinden[1]

[1] Group of Applied Physics-Optique, University of Geneva,
Rue de l'École-de-Médecine 20, 1205 Geneva, Switzerland
[2] idQuantique SA, Chemin de la Marbrerie 3, 1227, Geneva, Switzerland
E-mail: patrick.eraerds@unige.ch and nino.walenta@unige.ch

New Journal of Physics **12** (2010) 063027 (15pp)
Received 8 December 2009
Published 15 June 2010
Online at http://www.njp.org/
doi:10.1088/1367-2630/12/6/063027

Abstract. We perform quantum key distribution (QKD) over a single fibre in the presence of four classical channels in a C-band dense wavelength division multiplexing (DWDM) configuration using a commercial QKD system. The classical channels are used for key distillation and 1 Gbps encrypted communication, rendering the entire system independent of any other communication channel than a single dedicated fibre. We successfully distil secret keys over fibre spans of up to 50 km. The separation between the quantum channel at 1551.72 nm and the nearest classical channel is only 200 GHz, while the classical channels are all separated by 100 GHz. In addition to that, we discuss possible improvements and alternative configurations, e.g. whether it is advantageous to choose the quantum channel at 1310 nm or to opt for a pure C-band (1530–1565 nm) configuration.

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

Contents

1. Introduction

Since the initial proposal of quantum key distribution (QKD) in 1984 [1] and its first experimental demonstration [2], major progress in long-distance, fibre-based point-to-point QKD has been achieved (for an overview of current state-of-the-art implementations, see [3]).

The next consequential step towards larger availability of QKD links is to look at the compatibility of QKD with existing fibre infrastructures. Common public dense wavelength division multiplexing (DWDM) telecom networks multiplex up to 50 different wavelength channels in a single fibre. If the quantum channel is launched into a fibre accompanied by other classical signals, several effects, such as channel crosstalk, Raman scattering, four-wave mixing (FWM) or amplified spontaneous emission (in the case of amplification of the classical channels), can severely degrade the QKD system operation, or worse, can prevent it completely.

This is why until recently, one of the specifics of QKD systems was the need for a dedicated dark optical fibre, exclusively reserved for the quantum channel (single-photon level). Signals of classical strength, used to perform key distillation and encrypted communication between the end users, were sent through a second fibre to avoid compromising the weak quantum signal.

First investigations in this direction were conducted by Townsend in the late 1990s [4]. The impact of a single classical C-band channel, wavelength multiplexed with a quantum channel at 1310 nm, was analysed. Later, in 2005, Lee and Wellbrock demonstrated QKD, placing both the quantum channel and one classical channel into the C-band with a separation of down to 400 GHz equivalent to 3.2 nm [5]. We note that the classical channel was neither linked to the QKD system operation nor used for encrypted communication. More recent works [6, 7] investigate different impairment sources on a more general level, including effects that occur when more than one classical channel is present, e.g. FWM.

Apart from the long-term goal of QKD operation on public DWDM networks, investigated in [8], another frequently encountered network topology could push forward QKD availability in the short-term. In order to accommodate future growth, telecom companies have spent the

last few years installing point-to-point dedicated fibres [9]. These fibres can also be used in the standard configuration of QKD using a dark fibre for the quantum channel and another for the encrypted communication. However, for reasons of availability and fibre leasing costs, the operation on only one fibre is highly desirable. This objective thus necessitates wavelength multiplexing of all relevant system channels, i.e. key distillation and encrypted communication channels as well as the quantum channel on a single fibre. In contrast to a public DWDM network approach, such a configuration offers the advantage of having perfect information on the classical channels. Therefore a reliable performance characterization of the entire system is achievable. Finally, QKD systems that require a classical clock signal to synchronize their separate devices would benefit from greater robustness against relative fibre length drifts, present between the two fibres in the conventional dedicated dark fibre setup.

In this paper, we investigate exactly this situation where, in total, only one dedicated fibre is available and an encrypted link, based on QKD, should be established between its endpoints. In our experiment, we use a standard eight-channel C-band DWDM with 100 GHz (corresponding to 0.8 nm) spacing. We simultaneously multiplex four classical channels (one bidirectional channel for distillation and encrypted 1 Gbit per second (Gbps) communication, respectively) with a quantum channel, separated from the nearest classical channel by only 200 GHz.

This paper is organized as follows. In section 2, we discuss the different impairment sources relevant to our implementation. Section 3 describes the QKD setup and presents the experimental results, followed by a discussion and outlook in section 4. Section 5 contains our conclusions.

2. Impairment sources

2.1. Raman scattering

Due to photon–phonon interaction, photons can change their wavelength and thus compromise other channels. Depending on whether a phonon gets excited or de-exited, photons at wavelengths above (Stokes) and below (anti-Stokes) the initial wavelength are generated. Scattering off acoustic phonons (Brillouin scattering) is not critical, since the maximal frequency shift of the scattered photons is small (10 GHz, in the backward direction) and therefore cannot reach adjacent channels on a 100 GHz grid. By contrast, scattering off optical phonons (Raman scattering) can lead to significant frequency shifts covering the entire C-band[4], having an intensity maximum at a shift of about 13 THz (corresponding to a wavelength shift of 100 nm at 1550 nm). Unlike acoustic phonons, the more or less flat dispersion relation of optical phonons causes frequency shifts independent of the scatter direction. This means that in the co-propagating direction as well as in the counter-propagating direction (with respect to the exciting signal), a broad spectrum of photons is generated.

In order to evaluate the amount of Raman scatter, we scan the wavelength of a tunable laser (NetTest) connected to a 50 km standard single mode fibre via a circulator. The lower port of the circulator is connected to a fixed 0.8 nm wide spectral passband filter, transmitting the Raman backscatter that corresponds to the difference between the laser and filter centre wavelengths. From this we extract an effective Raman scattering cross-section $\rho(\lambda)$, shown in figure 1. It is normalized with respect to filter spectral bandwidth and fibre length, and it accounts for the

[4] Assuming the initial pump frequency to lie somewhere in the C-band.

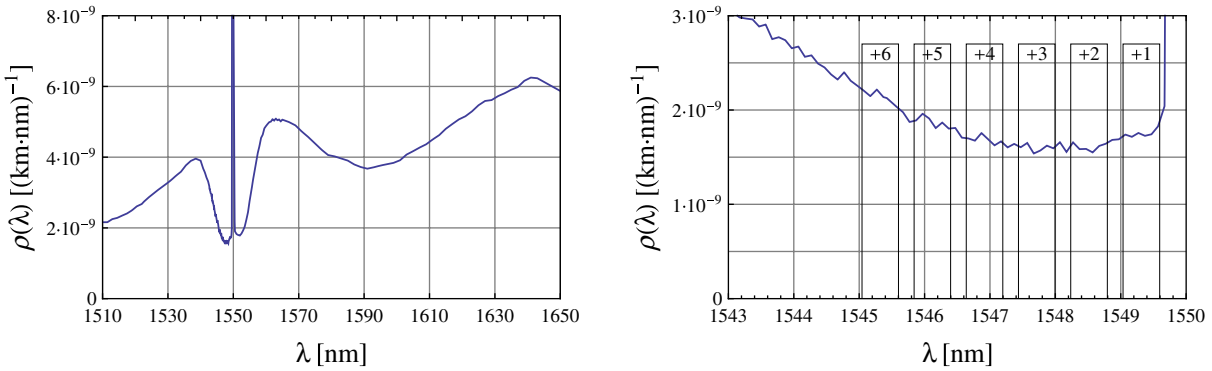

Figure 1. Left: measured effective Raman cross-section $\rho(\lambda)$ (per km fibre length and nm bandwidth) for a pump laser wavelength centred at 1550 nm in a standard single mode fibre at room temperature. Right: zoom on anti-Stokes dip of the Raman spectrum. In channels +2 and +3 the minimal amount of Raman scatter is found.

fibre caption ratio of the scattered light (see also appendix A). In return, by means of $\rho(\lambda)$ and allowing for fibre attenuation, we can calculate the Raman scatter power emerging from the input $P_{\mathrm{ram,b}}$ (backward Raman scattering) and the output $P_{\mathrm{ram,f}}$ (forward Raman scattering) of a fibre of arbitrary length L. Assuming a certain filter passband $[\lambda, \lambda + \Delta\lambda]$ and approximating the spectral integration via

$$\int_{\lambda}^{\lambda+\Delta\lambda} \rho(\lambda')\,\mathrm{d}\lambda' \approx \rho(\lambda)\cdot\Delta\lambda, \tag{1}$$

we obtain (see appendix A)

$$P_{\mathrm{ram,f}} = P_{\mathrm{out}}\cdot L\cdot\rho(\lambda)\cdot\Delta\lambda \tag{2}$$

$$P_{\mathrm{ram,b}} = P_{\mathrm{out}}\cdot\frac{\sinh(\alpha\, L)}{\alpha}\cdot\rho(\lambda)\cdot\Delta\lambda, \tag{3}$$

where P_{out} is the power of the exciting laser at the fibre output (W), α the fibre attenuation coefficient (km^{-1}) and L the fibre length (km). P_{out} can be written in terms of the input power via $P_{\mathrm{out}} = P_{\mathrm{in}}\,\mathrm{e}^{-\alpha L}$, if desired. The impact of each of the Raman contributions, represented by the detection probability per ns detector gate, is depicted in figure 2.

Note that we assume equal attenuation for initial and scattered wavelengths, which is reasonable for our total wavelength span of 4 nm (see section 3).

2.2. *Channel crosstalk*

The relative strength of the classical channels with respect to the quantum channel requires a large DWDM isolation between them. To calculate an adequate isolation, we need to consider the receiver sensitivity of the transceiver modules used for the classical communication (see section 3), since it determines the required input power.

Our particular modules (Finisar FWLF-1631-xx) require an optical power of at least −28 dBm (transceiver sensitivity) in order to guarantee a bit error rate (BER) $< 10^{-12}$. This

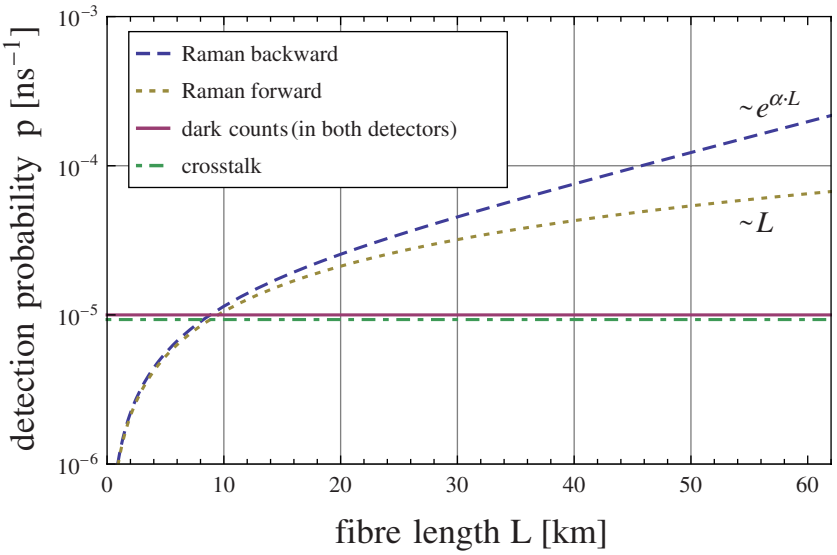

Figure 2. Different contributions to the total noise count probability per ns gate in both detectors assuming our system parameters ($\eta = 0.07$, DWDM channel isolation $= 82$ dB, fibre loss $\alpha_{\mathrm{dB}} = 0.21$ dB km^{-1}, four classical channels each with a power of -28 dBm at the receiver and internal components loss $=2.65$ dB; hence $P_{\mathrm{out}} = -25.35$ dBm).

power corresponds to approximately 1.2×10^4 photons per ns. With an isolation of about 82 dB, this photon number is attenuated such that the detection probability per ns gate is of the order of the dark count probability of a single detector (5×10^{-6} ns^{-1}). Here we assume a detector efficiency of $\eta = 0.07$.

Our standard eight-channel DWDM provides an isolation of just 82 dB between non-adjacent channels. Figure 2 depicts the calculated noise count probability from crosstalk for our actual setup described in section 3, accounting for two detectors and two co-propagating classical channels. We note that here the DWDM insertion loss of 1.95 dB requires a higher classical power and, hence, increases the crosstalk by the same amount, whereas the internal components loss of 2.65 dB on the receiver side equally attenuates all light impinging on the detector (see section 3). Thus, this isolation attenuates crosstalk below the dark count contribution. In the case of insufficient isolation, additional filters can further improve the isolation but at the expense of additional insertion loss in the quantum channel. In particular, considering Raman scattering we find that crosstalk is not a limiting factor for long fibre lengths.

Finally, we note that a sufficient isolation between the co-propagating quantum and classical channels entails that crosstalk from Rayleigh backscatter in a counter-propagating configuration can be neglected.

2.3. Four-wave mixing (FWM)

FWM is mediated by the third order susceptibility $\chi^{(3)}$ and describes the generation of additional photon frequencies, different from those present in the initial fields. In contrast to Raman scattering, no energy is transferred to or taken from the fibre, i.e. no phonon excitation or de-excitation takes place. Most harmful for our setup would be the degenerate case where two

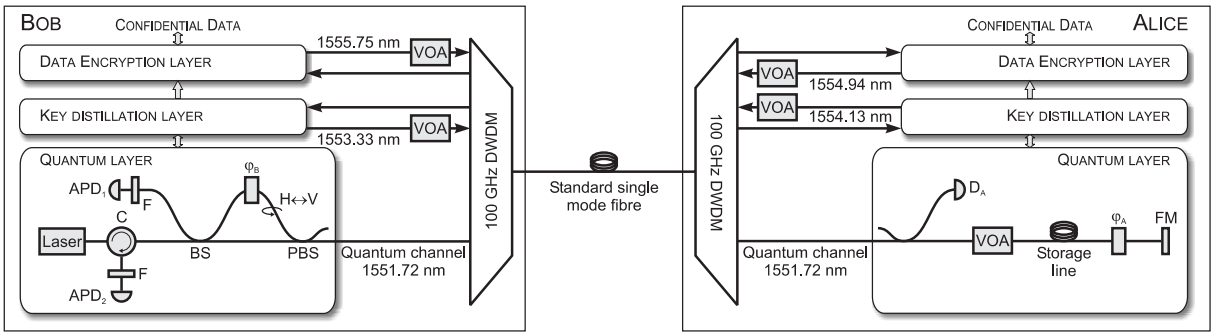

Figure 3. The setup scheme. APD, avalanche photo diode; BS, beam splitter; C, circulator; D, photo diode; F, spectral filter (optional); FM, Faraday mirror; PBS, Polarizing beam splitter; VOA, variable optical attenuator; ϕ, phase modulator.

exciting frequencies f_1, f_2 (assuming $f_1 > f_2$) generate side band frequencies $f_+ = f_1 + (f_1 - f_2)$ and $f_- = f_2 - (f_1 - f_2)$. If the channel separation is not properly chosen, $f_{+/-}$ may coincide with the quantum channel passband. The generation efficiency depends on the phase-matching condition, as well as on the relative polarization and propagation direction of the involved field frequency components. Phase matching is particularly easy to fulfil around the zero dispersion wavelength, where generated sidebands can corrupt even classical communication [10]. In section 3, we present a channel configuration that prevents efficient FWM generation in the quantum channel passband in standard single-mode fibres, dispersion shifted fibres and nonzero dispersion shifted fibres.

In addition to the stimulated case described before, it is also important to assess the noise contribution from spontaneous FWM. Spontaneous FWM allows the creation of signal and idler frequencies f_s, f_i from each pump frequency f_p, satisfying energy conservation via $2f_p = f_s + f_i$. The efficient generation again depends on the phase-matching condition. Around the zero dispersion wavelength the generated spectrum can be rather broad, superposing the spectrum generated by Raman scattering [11]. Following [11] we calculate the $\gamma P_0 L$ product, which is a measure for the generated spontaneous FWM under phase-matching conditions. Here, γ is the nonlinear fibre parameter, P_0 the laser power and L the fibre length. Even in our most demanding configuration we obtain a very small value, i.e. 0.002. For considerable contributions at least $\gamma P_0 L$ of about 0.1 is needed. This indicates that, even when we were operating around the zero dispersion wavelength, spontaneous FWM can be neglected with respect to Raman scattering.

3. Experiment

3.1. Setup

For the experiments we adopt a commercial QKD system (Cerberis from idQuantique [12]). As outlined in figure 3, this solution combines a QKD server for secure point-to-point key distribution and Layer 2 encryption units to encode and decode messages, with the key provided by the QKD server for complete secure bidirectional communication between two distant partners, Alice and Bob.

The QKD layer is based on a 'plug and play' phase encoding QKD system where all optical and mechanical fluctuations are automatically and passively compensated [13].

Bob generates a sequence of optical pulses with a frequency of $f_{\mathrm{rep}} = 5\,\mathrm{MHz}$. It propagates through his unbalanced Mach–Zehnder interferometer such that each pulse is split into two orthogonally polarized pulses that are separated by the interferometer imbalance. The sequence length is chosen to match twice the length of the storage line of $L_{\mathrm{s}} \approx 10\,\mathrm{km}$ at Alice's in order to avoid compromising Rayleigh backscatter. At Alice's, the major proportion of photons per pulse is used to trigger the classical detector D_{A} in order to synchronize her device with Bob's. The remaining proportion is reflected at the FM, phase modulated by ϕ_{A} in accordance with Alice's choice of bit value and encoding base, attenuated by the VOA to μ photons per pulse and returned to Bob through the same fibre link. Due to the Faraday rotation, each pulse propagates along the contrary interferometer arm as before and interferes at the BS in accordance with the phase difference between ϕ_{A} and Bob's base choice ϕ_{B}. All internal losses of Bob's optical components sum up to $t_{\mathrm{B}} = 2.65\,\mathrm{dB}$ (excluding DWDMs and optional filters).

The signals are detected by InGaAs APDs operated in Geiger mode. The APDs are temperature stabilized at 220 K, gated using 1.5 ns long gates with a dead time of $\tau_{\mathrm{dead}} = 10\,\mu\mathrm{s}$ applied after each detection to reduce the afterpulse probability to $\leqslant 0.8\%$ of the total detection probability. The detection efficiencies are $\eta \approx 0.07$ at a dark count probability of approximately $5 \times 10^{-6}\,\mathrm{ns}^{-1}$. After key sifting, optionally via the sifting protocols BB84 or SARG [14], followed by fully implemented error correction using the CASCADE algorithm [15] and privacy amplification using hashing functions based on Toeplitz matrices [16], Alice and Bob remain with shared secret keys. During this post-processing the key distribution is automatically interrupted. The integrity of the public distillation communication is ensured by a Wegman–Carter-type authentication scheme based on universal hashing functions [17].

The pair of Ethernet encryptors is periodically updated with the secret keys to establish a permanent AES-256 encrypted 1 Gbps data link between Alice and Bob. The data to be encrypted are continuously provided by two 1 Gbps streams of random bits from a network test system (EXFO PacketBlazer FTB-8510). We note that typically the key refresh rate is once per minute, which requires a secret key rate of at least 8.6 Gbps. In order to guarantee continuous operation, the key refresh rate is temporarily reduced if the secret key rate drops below that limit.

All in all, to completely operate the Cerberis system, four classical communication channels have to be set up between Alice and Bob in addition to the quantum channel. The bidirectional communication for distillation, i.e. key sifting, error correction and privacy amplification, demands two authenticated channels, one from Alice to Bob and one from Bob to Alice. Similarly, two channels are required for the bidirectional encrypted data transmission between the encryptors. All classical communication channels are implemented using standard optical 2.67 Gbps DWDM SFP transceivers (Finisar FWLF-1631-xx). For the fibre link, we use standard single-mode fibre spools of different lengths with an average attenuation $\alpha_{\mathrm{dB}} \approx 0.21\,\mathrm{dB\,km}^{-1}$.

We multiplex the quantum channel along with the four classical channels using off-the-shelf 100 GHz DWDM modules (OptiWorks). The modules possess an insertion loss of 1.95 dB and an isolation of 59 dB (82 dB) for adjacent (non-adjacent) channels. The implemented channel configuration is shown in figure 3. For the quantum channel we choose a wavelength of 1551.72 nm on the ITU C-band grid. We take advantage of 10% less Raman noise on the anti-Stokes side of the Raman spectrum at ambient temperature (see figure 1) by placing all classical channels at higher wavelengths. To benefit from both the considerably higher DWDM channel isolation for non-adjacent channels and lower Raman noise, we omit the adjacent channel and

set up the quantum channel 200 GHz (1.6 nm) apart from the nearest classical channel. We minimize the direct impairment due to FWM by choosing the frequency difference between two co-propagating channels, such that no FWM frequency product is generated within the quantum channel passband (see section 2.3).

The discussion on impairment sources has shown that, in general, the amount of noise impinging on the detectors increases with the total power present in the fibre. Hence, we reduce the power of the classical channels to the overall transmission losses using VOAs, such that the corresponding power at the receiver's end just matches the receiver sensitivity of −28 dBm. This corresponds to $P_{\text{out}} = -26.05$ dBm in (2) and (3) due to the insertion losses of our DWDM modules.

With the aim to further minimize the amount of Raman noise, we optionally add phase-shifted fibre Bragg grating filters (F) (from AOS [18]) centred on the quantum channel wavelength in front of each APD. Their spectral bandwidth of 45 pm (FWHM) and extinction ratio of 14 dB entails an 85 % rejection of noise photons, outweighing the additional attenuation of 2 dB due to insertion loss. The filters are actively and independently temperature stabilized using standard temperature controllers, mainly to permit fine adjustment of their transmission bandwidth. A straightforward configuration with only one filter inserted between the PBS and the DWDM was abandoned because of backreflections of the quantum channel laser, which completely saturated the APDs.

3.2. Results

We characterize the system performance for different lengths of standard single mode fibre by measuring the quantum bit error rate (QBER) and the secret key rate R_{sec}. The QBER, i.e. the number of erroneous detections over the total number of detections, can be approximated by

$$\text{QBER} = \text{QBER}_{\text{opt}} + \text{QBER}_{\text{det}} + \text{QBER}_{\text{wdm}} \tag{4}$$

(for more details see appendix B). The optical share QBER_{opt} is determined by the interference visibility entailed by the quality of the optical components and their alignment. Its typical value was 0.3% (0.6%) using BB84 (SARG). QBER_{det} depends on the characteristics of Bob's single photon detectors and includes errors due to detector dark counts in both detectors of around 1×10^{-5} per ns as well as afterpulses. QBER_{wdm} summarizes all additional errors from noise due to wavelength-division multiplexing with classical channels, i.e. channel crosstalk and Raman scatter (see figure 2).

The secret key rate, i.e. the net rate of secret key bits provided to the encryptors to cipher data communication between Alice and Bob, is given by [19]

$$R_{\text{sec}} = R_{\text{sift}}\,(1 - r_{\text{ec}})\,(1 - r_{\text{pa}}). \tag{5}$$

Here, R_{sift} is the detection rate after sifting (B.2), and r_{ec} and r_{pa} are the fractions of bits used for error correction and privacy amplification. Both r_{ec} and r_{pa} increase non-linearly with the QBER. As explained in more detail in appendix B, the amount of information attributed to an eavesdropper and, hence, the fraction r_{pa} discarded during privacy amplification are calculated assuming incoherent attacks [20, 21].

Our performance results in terms of QBER (estimated by the CASCADE error correction protocol) and net rate of secret keys are plotted in figure 4 (dots) and listed in table 1. The solid lines indicate our calculations that make use of the formulae given in appendix B. We note that, in contrast to the measured secret key rates, our theoretical estimates do not take into account

Table 1. The secret key rate R_{sec} and QBER values from figure 4, which we obtain experimentally using BB84 and SARG, without and with the spectral filters (F).

Fibre length	1 km	5 km	10 km	25 km	35 km	41 km	50 km
Without filters							
R_{sec} (bps) BB84/SARG	2829/–	2047/–	1524/–	134/511	4.3/72	–/2.0	
QBER (%) BB84/SARG	0.57/–	0.72/–	1.18/–	4.53/2.12	8.60/4.77	–/7.48	
With filters							
R_{sec} (bps) BB84/SARG				251/347	25/128	7.5/43	0/11
QBER (%) BB84/SARG				1.6/1.7	3.6/2.5	6.7/3.7	34.5/5.4

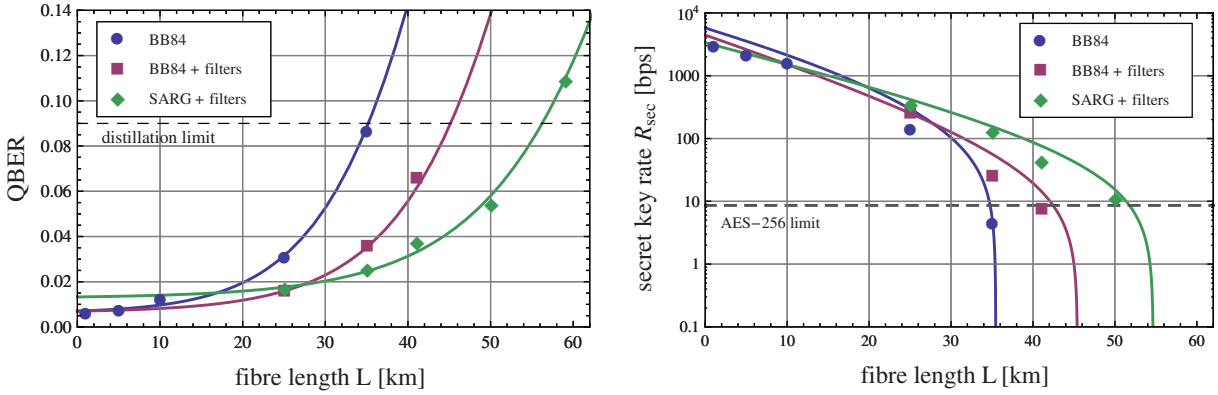

Figure 4. Performance of the QKD-based encryption system in terms of QBER (left) and secret key rate provided to the encryptors (right) in dependence of the fibre length. Symbols denote our experimental results and solid lines our calculations. Additional filtering increases the maximum fibre length to 41 km using BB84 key sifting and to 50 km using SARG.

interruptions of the key exchange during key distillation and fibre length measurements. Since this influence becomes more significant the higher the key rates, we overestimate the secret key rate in our calculations, especially for short fibre lengths. The dashed line in the left graph of figure 4 indicates the maximum QBER of 9% below which the CASCADE error correction algorithm is able to distil secret bits. This limit is lower than the theoretical limits given by 12.4% (10.95%) for BB84 (SARG) [21], since CASCADE cannot reach the theoretical Shannon limit and since a certain fraction of distilled secret bits is consumed for authenication. The dashed line in the right graph of figure 4 indicates the minimum secret key rate of 8.6 bit s^{-1} required for AES encryption with 256 bit keys, that are updated once a minute, respectively.

Without the optional spectral filters (F), we obtain a secret key rate that remains well above 1000 bit s^{-1} up to a fibre length of 10 km using BB84 key sifting. Inserting the optional spectral filters in front of the APDs does not only increase the secret key rate from 4.3 to 25 bit s^{-1} for a fibre length of 35 km but also increases the maximal distance to 41 km, at which we obtain 7.5 bit s^{-1}. We achieve a further increase in the secret key rate and maximum distance if we use the SARG key sifting protocol instead. Here, the average secret key rate is 128 bit s^{-1} for

35 km and 11 bit s^{-1} for 50 km fibre length. We emphasize that the SARG protocol equally guarantees the security of the key material under the assumption of incoherent attacks [21]. Whereas for BB84 the optimum mean photon number μ of the quantum pulses depends on the fibre transmission t according to $\mu_{BB84} = t$, the SARG protocol allows us to benefit from a higher mean photon number $\mu_{SARG} = 2\sqrt{t}$ [21].

Concerning the stability of the setup, we verify constant detection and secret key rates over a period as long as 5 days in the configuration without the additional filters (F). Having added the filters, we still observe constant detection rates at the beginning of our experiments, which confirms that a sufficient stabilization of the filter transmission spectra can be achieved using standard temperature control. However, after a few weeks of experiments, the detection rate in one detector tends to decrease within a few hours after the filter temperature has been adjusted. This impairment is caused by a drift of the transmission spectra of the corresponding filter, most likely due to a fabrication flaw in that particular filter.

4. Discussion and outlook

In figure 4 (left), we compare the QBER values obtained experimentally with theoretical calculations that take all discussed noise sources into account. It reproduces very well the measurement results, giving us confidence that we have successfully identified the dominant impairment sources present in our implementation. Based on this we discuss some alternative configurations in the following paragraphs.

Firstly, we address the question whether or not it might be advantageous to place the quantum channel in the O-band around 1310 nm while keeping the classical communication channels in the C-band around 1550 nm (for an O-band implementation see [22]). The maximal reach of the 1550 nm solution is ultimately limited by the Raman noise (see figure 2). Calculating the mean phonon occupation numbers, we find that the Raman noise at 1310 nm (anti-Stokes band) is about 4000 times weaker than at 1550 nm. For comparison we simulate two scenarios: firstly, we take the dark count probability of the detectors used in our experiment ($p_{dc} = 5 \times 10^{-6}$ ns^{-1}, $\eta = 0.07$) and, secondly, we assume a very small detector dark count probability for prospective InGaAs APDs ($p_{dc} = 5 \times 10^{-8}$ ns^{-1}, $\eta = 0.07$). In addition to that, we suppose a better channel isolation in the 1310 nm case of 100 dB, while it is at 82 dB in the 1550 nm case (like in our experiment). The results are shown in figure 5. For all curves we neglected the influence of detector dead time, the system-specific duty cycle and the reduced efficiency of the error correction protocol (see appendix B). As expected, we find that a lower dark count rate dramatically improves the 1310 nm curve, whereas it has a rather minor impact on 1550 nm. However, we see that if high key rates are desired, the 1310 nm solution cannot keep up with the 1550 nm one due to the higher fibre attenuation. Only in an extreme case where lower key rates are acceptable, the 1310 nm solution can reach a larger distance, provided detectors with very low dark count probability are used.

Secondly, we want to estimate the implications of higher transmission rates in the encrypted channels. As described before, we minimize the total power present in the fibre by adapting the laser power of the SFP modules to their receiver sensitivity of −28 dBm. Modules designated for higher transmission rates currently have lower sensitivity. For example, the 10 Gbps transceiver module Finisar FTRX-1811-3 is specified with a receiver sensitivity of −23 dBm. Using two of these modules for the encrypted link instead of the 1 Gbps modules that we used would consequently increase the total classical power by 3.2 dB, and hence the detected noise. Taking

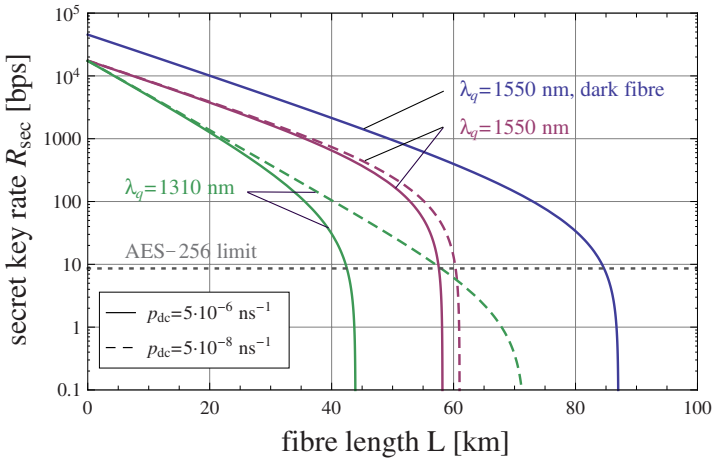

Figure 5. Comparison between 1550 and 1310 nm quantum channel wavelength (SARG, with filters). p_{dc} denotes detector dark count probability. The assumed fibre attenuation is $\alpha_{1550} = 0.21\,\mathrm{dB\,km^{-1}}$ and $\alpha_{1310} = 0.35\,\mathrm{dB\,km^{-1}}$. The calculations for a dark fibre configuration (without DWDMs and filters) are also shown for comparison.

this into account but keeping all other parameters unchanged, we estimate for distances up to 40 km no significant degradation of the secret key rate. However, the maximum distance at which a key rate of 8.6 bps can be achieved decreases by 4–5 km, depending on the sifting protocol.

Next, we take a look at possible measures that could improve the performance of the current setup. One possibility is the reduction of the total classical channel power. This could be achieved by amplification of the classical signals in front of the receivers or by prospective SFP modules with better receiver sensitivity. While a solution with amplifiers is cost-intensive, an improvement in the receiver sensitivity of more than 3 dB is unlikely in the near future. One could also assume that narrower spectral or temporal filtering of the quantum channel could further reduce the impact of Raman noise. However, we think that there is not much room for improvements here. On the one hand, the transmission width of 45 pm (corresponding to 5.6 GHz) of our additional filter is already the limit for the spectral width of our sub-nanosecond quantum signals. On the other hand, we cannot further reduce the detector gate width (temporal filtering) without clipping the pulses and, hence, introducing additional losses. Since the pulse duration of the quantum signals is related to the inverse of its spectral bandwidth, further narrower temporal filtering would entail broader spectral filtering and vice versa.

Finally, we would like to give an outlook on prospective DWDM implementations with next-generation QKD systems based on the differential-phase shift protocol [23] or the coherent-one-way protocol (COW; [24]). These systems largely benefit from high-speed electronics and a better key generation efficiency due to their improved tolerance to photon number splitting attacks. As an illustration, we take a look at the COW prototype as presented in [25], which uses a QKD encoding frequency of 312.5 MHz and a mean photon number of $\mu_{COW} = 0.5$ photons per pulse. Assuming the same parameters as used for the calculations with the additional filters in figure 4, we find an increase in the maximum link distance to 70 km and a secret key rate of $>10\,000\,\mathrm{bit\,s^{-1}}$ for fibre lengths up to 43 km.

5. Conclusions

We demonstrate that a QKD-based encryption system can be efficiently operated over a single dedicated fibre of up to 50 km length. All four classical channels necessary to establish the encrypted link can be multiplexed along with the quantum signal in a 100 GHz C-band DWDM configuration, rendering the system independent of any additional network connection. With respect to the conventional dark fibre configuration, requiring two independent fibres, comparable secret key rates can be obtained; for example, up to 25 km the decrease of the secret key rate is less than 50%. We find that in practice a pure C-band configuration shows superior performance compared to a combination of a quantum channel at 1310 nm and classical channels at 1550 nm. We conclude that with only moderate additional efforts a commercial QKD system can be upgraded to network topologies where only one dedicated fibre is available.

Acknowledgments

We acknowledge Patrick Trinkler from idQuantique for helpful support. This project was financially supported by the Swiss NCCR 'Quantum Photonics' and the ERC-AG QORE.

Appendix A. Derivation of Raman scatter power formulae

The Raman scatter power $\mathrm{d}P_{\mathrm{ram}}$ at wavelength λ from a fibre element of length $\mathrm{d}x$ at position x when a power P_{in} is launched into a fibre is

$$\mathrm{d}P_{\mathrm{ram}}(\lambda, x) = P_{\mathrm{in}} \cdot \mathrm{e}^{-\alpha x} \cdot \rho(\lambda) \cdot \Delta\lambda \cdot \mathrm{d}x, \tag{A.1}$$

where $\rho(\lambda)$ is the effective Raman cross section introduced in section 2.1. It accounts already for the fibre caption ratio and we used the same approximation for the spectral integral as in (1). The scatter from a single fibre element $\mathrm{d}x$ is almost isotropic. Now we have to account for the attenuation of the fibre (length L) when the scatter propagates to the fibre output (forward scatter) or back to the fibre input (backward scatter):

(a) Forward:

$$\mathrm{d}P_{\mathrm{ram,f}} = \mathrm{d}P_{\mathrm{ram}}(\lambda, x) \cdot \mathrm{e}^{-\alpha (L-x)} \tag{A.2}$$

integrating over the whole fibre

$$\Rightarrow P_{\mathrm{ram,f}} = P_{\mathrm{in}} \cdot L \cdot \mathrm{e}^{-\alpha L} \cdot \rho(\lambda) \cdot \Delta\lambda. \tag{A.3}$$

(b) Backward:

$$\mathrm{d}P_{\mathrm{ram,b}} = \mathrm{d}P_{\mathrm{ram}}(\lambda, x) \cdot \mathrm{e}^{-\alpha x} \tag{A.4}$$

integrating over the whole fibre

$$\Rightarrow P_{\mathrm{ram,b}} = P_{\mathrm{in}} \cdot \mathrm{e}^{-\alpha L} \frac{\sinh(\alpha L)}{\alpha} \cdot \rho(\lambda) \cdot \Delta\lambda. \tag{A.5}$$

In order to obtain the detection probabilities per gate ($p_{\mathrm{ram,f}}$ and $p_{\mathrm{ram,b}}$, respectively), used for the QBER calculation (see appendix B), we calculate (in low-power approximation)

$$p_{\mathrm{ram,f}} = \frac{P_{\mathrm{ram,f}} \cdot \lambda}{hc} \cdot \eta \cdot \Delta t_{\mathrm{gate}}, \tag{A.6}$$

where Δt_{gate} is the gate duration and η the detector efficiency. By replacing $P_{\mathrm{ram,f}}$ with $P_{\mathrm{ram,b}}$, one obtains $p_{\mathrm{ram,b}}$ in the same manner.

Appendix B. Explicit QBER and key rate formulae

To calculate the QBER and secret key rate R_{sec} of the system, we have to consider the raw detection rate R_{raw} delivered by the detectors due to quantum signals, detector dark counts, afterpulses and additional noise, i.e.

$$R_{\mathrm{raw}} = (p_\mu + 2p_{\mathrm{dc}} + p_{\mathrm{AP}} + p_{\mathrm{ram}} + p_{\mathrm{ct}})\, f_{\mathrm{rep}}\, \eta_{\mathrm{duty}}\, \eta_{\mathrm{dead}}. \tag{B.1}$$

Here, f_{rep} is the pulse repetition frequency of the system and the quantities p_x signify detection probabilities per detector gate. In particular, p_μ = signal detection, p_{dc} = darkcount, p_{AP} = afterpulse, $p_{\mathrm{ram}} = p_{\mathrm{ram,f}} + p_{\mathrm{ram,b}}$ = Raman photon detection (see (A.6)), and p_{ct} = crosstalk photon detection. The signal detection probability p_μ is a product of the average number of photons per pulse μ, fibre transmission t, detector efficiency η and t_{B} the loss of Bob's internal components. The optimal μ also depends on the sifting protocol, i.e. $\mu_{\mathrm{BB84}} = t$ and $\mu_{\mathrm{SARG}} = 2\sqrt{t}$ [21].

The probability p_{AP} of detecting an afterpulse is a function of the total detection probability and the average time between two detections. Here, we approximate it by $p_{\mathrm{AP}} = 0.008\,(p_\mu + 2p_{\mathrm{dc}} + p_{\mathrm{ram}} + p_{\mathrm{ct}})$. This is an upper bound since the probability that after a detection an afterpulse is generated is less than 0.8% for our system. The coefficients η_{duty} and η_{dead} are introduced to account for the reduced detection rate due to the duty cycle of our 'plug and play' based system and due to a detector dead time τ_{dead} applied after each detection, respectively. They amount to $\eta_{\mathrm{duty}} = L_{\mathrm{S}}/(L + 2L_{\mathrm{S}})$, with L being the fibre length and L_{S} the length of Alice's storage line, and $\eta_{\mathrm{dead}} = (1 + \tau_{\mathrm{dead}}\, f_{\mathrm{rep}}(p_\mu + 2p_{\mathrm{dc}} + p_{\mathrm{AP}} + p_{\mathrm{ram}} + p_{\mathrm{ct}}))^{-1}$. We note that the rate estimates presented in this chapter do not account for double detections and Poissonian photon number statistics.

During sifting, a certain fraction of R_{raw} is discarded. Depending on the specific QKD protocol, the key rate after sifting is

$$R_{\mathrm{sift}} = \tfrac{1}{2}(\beta\, p_\mu + 2p_{\mathrm{dc}} + p_{\mathrm{AP}} + p_{\mathrm{ram}} + p_{\mathrm{ct}})\, f_{\mathrm{rep}}\, \eta_{\mathrm{duty}}\, \eta_{\mathrm{dead}}. \tag{B.2}$$

For simplicity we introduce a parameter β that is $\beta_{\mathrm{BB84}} = 1$ for BB84 and $\beta_{\mathrm{SARG}} = (2 - V)/2$ for SARG, with V being the interference visibility. Using (B.2) we estimate the secret key rate after error correction and privacy amplification by

$$R_{\mathrm{sec}} = R_{\mathrm{sift}}\,(I_{\mathrm{AB}} - I_{\mathrm{AE}})\,. \tag{B.3}$$

I_{AB} and I_{AE} are the mutual information per bit between Alice and Bob, and between Alice and a potential eavesdropper, respectively. Due to quantum bit errors, I_{AB} is smaller than 1 and amounts to

$$I_{\mathrm{AB}} = 1 - \eta_{\mathrm{ec}} H\,(\mathrm{QBER})\,, \tag{B.4}$$

with the binary entropy function $H(p) = -p \log_2 p - (1 - p)\log_2(1 - p)$. In the ideal case, the amount of bits discarded during error correction is given by the Shannon limit, i.e. $\eta_{\mathrm{ec}} = 1$. In practice, however, we observe that the implemented algorithm for CASCADE error correction consumes about 20% more bits than given by the Shannon limit. Hence, we correct (B.4) by choosing $\eta_{\mathrm{ec}}^{\mathrm{Cascade}} = \frac{6}{5}$.

To calculate the information per bit I_{AE} between Alice and an eavesdropper, we assume that an eavesdropper has full control over the quantum channel (i.e. the visibility and fibre transmission). In contrast, he cannot modify the characteristics of Bob's detectors. Additionally, we suppose that he performs an optimal incoherent attack [26] on pulses containing one photon,

and a PNS attack [27] if more than one photon is present in a pulse (without affecting the total detection rate at Bob). For BB84 with weak laser pulses, one then obtains [20]

$$I_{\mathrm{AE,BB84}} = \frac{\left(1-\frac{\mu}{2t}\right)(1-H(P))+\frac{\mu}{2t}}{1+\frac{2p_{\mathrm{dc}}}{\mu t\eta}}, \tag{B.5}$$

with $P = \frac{1}{2}+\sqrt{D(1-D)}$, $D = (1-V)/(2-\mu/t)$. Based on the same assumptions, we use the results in [21] to estimate for the SARG protocol

$$I_{\mathrm{AE,SARG}} = I_{\mathrm{pns}}(1)+\frac{1}{12}\frac{\mu^2}{t}\mathrm{e}^{-\mu}(1-I_{\mathrm{pns}}(1)), \tag{B.6}$$

where $I_{\mathrm{pns}}(k) = 1-H(\frac{1}{2}+\frac{1}{2}\sqrt{1-1/2^k})$ is the potential information gain of an eavesdropper due to PNS attacks on multi-photon pulses when k photons are split and stored.

To be able to estimate the QBER and hence (B.3), we start from the general definition of QBER as the ratio between the number of false detections and total detections (right + false),

$$\mathrm{QBER} = \frac{\mathrm{false}}{\mathrm{right}+\mathrm{false}}. \tag{B.7}$$

Using the same notation as before, in particular p_x for the detection probabilities, V for the visibility and β to account for both QKD protocols, we obtain

$$\mathrm{QBER} = \frac{1}{2}\frac{p_\mu(1-V)+2p_{\mathrm{dc}}+p_{\mathrm{AP}}+p_{\mathrm{ram}}+p_{\mathrm{ct}}}{\beta\, p_\mu+2p_{\mathrm{dc}}+p_{\mathrm{AP}}+p_{\mathrm{ram}}+p_{\mathrm{ct}}}. \tag{B.8}$$

Without additional noise it reduces to the well-known formulae $\mathrm{QBER}_{\mathrm{BB84}} = (1-V)/2$ for BB84 and $\mathrm{QBER}_{\mathrm{SARG}} = (1-V)/(2-V)$ for SARG [21].

References

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

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

[3] Lütkenhaus N and Shields A J 2009 Focus on quantum cryptography: theory and practice *New J. Phys.* **11** 045005

[4] Townsend P D 1997 Simultaneous quantum cryptographic key distribution and conventional data transmission over installed fibre using wavelength-division multiplexing *Electron. Lett.* **33** 188–190

[5] Xia T J, Chen D Z, Wellbrock G A, Zavriyev A, Beal A C and Lee K M 2005 In-band quantum key distribution (QKD) on fiber populated by high-speed classical data channels *Optical Fiber Communication Conf.* (*OFC*) (*Anaheim, CA, 5 March 2006*)

[6] Peters N A *et al* 2009 Dense wavelength multiplexing of 1550 nm QKD with strong classical channels in reconfigurable networking environments *New J. Phys.* **11** 045012

[7] Runser R J *et al* 2007 Progress toward quantum communications networks: opportunities and challenges *Optoelectronic Integrated Circuits IX* vol 6476 (Bellingham, WA: SPIE) p 6476OI

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

[9] Graham-Rowe D 2009 Quantum cryptography for the masses *Technol. Rev.* **8**

[10] Tkach R W, Chraplyvy A R, Forghieri F, Gnauck A H and Derosier R M 1995 Four-photon mixing and high-speed WDM systems *J. Lightwave Technol.* **13** 841–9

[11] Lin Q, Yaman F and Agrawal G P 2007 Photon-pair generation in optical fibers through four-wave mixing: role of Raman scattering and pump polarization *Phys. Rev.* A **75** 023803
[12] www.idQuantique.com
[13] Stucki D, Gisin N, Guinnard O, Ribordy G and Zbinden H 2002 Quantum key distribution over 67 km with a plug&play system *New J. Phys.* **4** 41
[14] Scarani V, Acín A, Ribordy G and Gisin N 2004 Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations *Phys. Rev. Lett.* **92** 057901
[15] Brassard G and Salvail L 1994 *Secret-Key Reconciliation by Public Discussion* (*Lecture Notes in Computer Science* vol 765) (Berlin: Springer) pp 410–23
[16] Wegman M N and Carter J L 1981 New hash functions and their use in authentication and set equality *J. Comput. Syst. Sci.* **22** 265–79
[17] Carter J L and Wegman M N 1979 Universal classes of hash functions *J. Comput. Syst. Sci.* **18** 143–54
[18] www.aos-fiber.com
[19] Ribordy G, Gautier J D, Gisin N, Guinnard O and Zbinden H 2000 Fast and user-friendly quantum key distribution *J. Mod. Opt.* **47** 517–31
[20] Niederberger A, Scarani V and Gisin N 2005 Photon-number-splitting versus cloning attacks in practical implementations of the Bennett-Brassard 1984 protocol for quantum cryptography *Phys. Rev.* A **71** 042316
[21] Branciard C, Gisin N, Kraus B and Scarani V 2005 Security of two quantum cryptography protocols using the same four qubit states *Phys. Rev.* A **72** 032301
[22] Tang X, Ma L, Mink A, Chang T, Xu H, Slattery O, Nakassis A, Hershman B, Su D and Boisvert R F 2008 High-speed quantum key distribution systems for optical fiber networks in campus and metro areas *Quantum Communications and Quantum Imaging VI. Proc. of SPIE* vol 7092 p 70920I
[23] Inoue K, Waks E and Yamamoto Y 2002 Differential phase shift quantum key distribution *Phys. Rev. Lett.* **89** 037902
[24] 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
[25] 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
[26] Fuchs C A, Gisin N, Griffiths R B, Niu C-S and Peres A 1997 Optimal eavesdropping in quantum cryptography. I. Information bound and optimal strategy *Phys. Rev.* A **56** 1163–72
[27] Brassard G, Lütkenhaus N, Mor T and Sanders B C 2000 Limitations on practical quantum cryptography *Phys. Rev. Lett.* **85** 1330–3