Eur. Phys. J. D **30**, 143–148 (2004)
DOI: 10.1140/epjd/e2004-00080-8

THE EUROPEAN PHYSICAL JOURNAL D

Quantum key distribution over 30 km of standard fiber using energy-time entangled photon pairs: a comparison of two chromatic dispersion reduction methods

S. Fasel, N. Gisin[a], G. Ribordy, and H. Zbinden

University of Geneva, Group of Applied Physics, 20 rue de l'École-de-Médecine, 1211 Geneva 4, Switzerland

Received 22 March 2004
Published online 22 June 2004 –

Abstract. We present a full implementation of a quantum key distribution system using energy-time entangled photon pairs over a 30 km standard telecom fiber quantum channel. Two bases of two orthogonal states are implemented and the set-up is shown to be robust to environmental constraints such as temperature variation. Two different ways to manage chromatic dispersion in the quantum channel are discussed.

PACS. 03.67.Dd Quantum cryptography – 03.67.Hk Quantum communication

Since the birth of quantum key distribution (QKD) [1–3], a lot of research and discoveries have been made [4–7] leading today to demonstrated long distance QKD [8–11] and even to commercially available quantum cryptography devices. However, these systems rely on faint laser pulses containing around 0.1 photon per pulse to guarantee absolutely secure keys. Therefore, only a fraction of the pulses will lead to effective bit transmission. Another consequence is that more than one photon are present per pulse with non-zero probability. True single photon sources [12,13] seem to be a promising solution, but existing devices are not yet usable for out-of-the-lab systems. The most serious alternatives are systems based on entangled photon pairs [14–17], but no real-world long distance QKD using this approach has been reported yet, mainly for two reasons. First, the set-up itself is relatively complex. Second, the spectral characteristics of the photon pairs sources imply that chromatic and polarization dispersion effects are not negligible and increase the error rate. Consequently, one has to find solutions if the aim is to deploy systems over fibre telecom networks.

The goal of the present article is to demonstrate solutions to the chromatic dispersion issue for an energy-time entanglement based QKD system using a standard fiber quantum channel. We have improved a set-up previously presented by our group [17] by using dispersion compensation or spectral filtering and thus extending the transmission range.

Our set-up is based on a Franson arrangement [18] of interferometers. A parametric down conversion photon pair source is located between Alice and Bob. They both have an unbalanced Mach-Zender interferometer with photon-counting detectors connected at all outputs. When considering a given photon pair, four different events can be detected by both Alice and Bob. First, the photons can both propagate through the short arms of the interferometers. Alternatively, one can take the long arm at Alice while the other takes the short one at Bob. The opposite is also possible. Finally, both photon can propagate through the long arms. When the path differences of the interferometers are matched within a fraction of the coherence length of the down-converted photons, the short-short and the long-long processes are indistinguishable and thus yield two-photon interferences, provided that the coherence length of the pump photons is longer than the path-length difference. If one records events as a function of time difference between detections at Alice and at Bob, 3 peaks appear (Fig. 1). The central one corresponds to the interfering short-short and long-long events. It can be distinguished from the others with a time window discriminator, and is used to isolate nonlocal quantum correlation between Alice's and Bob's detections. In Figure 1 we see that to allow the window discriminator to take the maximum of the central peak into account (to have an optimal detection rate) but at the same time avoid the side peaks (non-correlated side peaks detections introduce errors), the separation between the peaks ΔT must be significantly bigger than $\Delta\tau$. $\Delta\tau$ is the RMS of all the temporal spreading contributions: photon's coherence time, electronic and detection jitter and, for dispersive medium between the source and the interferometers, the spreading of the wave packet due to chromatic dispersion. This condition reads:

$$\Delta\tau < \Delta T < t_c^{pump}$$

where t_c^{pump} is the coherence time of the pump laser.

[a] e-mail: Nicolas.Gisin@physics.unige.ch

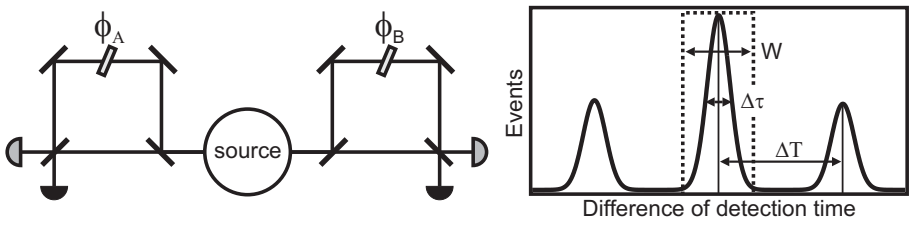

Fig. 1. Schematic diagram of a Franson-type interferometer-source arrangement and the corresponding event frequency plotted as a function of the difference of detection time at Alice and at Bob. The resulting peaks can be approximated by Gaussians with FWHM $\Delta\tau$ and are separated by a time ΔT corresponding to the path length difference. A temporal window discriminator of width W is placed around the central peak. The two phases ϕ_A and ϕ_B modulate the correlations.

Dispersive media introduce chromatic dispersion of $D = \delta\tau/\delta\lambda$ per unit length. For standard telecom fibers and light around 1550 nm this value is $D \cong 17\ \mathrm{ps\,nm^{-1}\,km^{-1}}$. The Gaussian uncertainty in time due to chromatic dispersion only is then given by $\Delta\tau_{\mathrm{disp}} = D\,\Delta\lambda\,L$ (where $\Delta\lambda$ is the photon's spectral width and L the length of the fiber). Consequently, the inequality

$$D\,\Delta\lambda\,L < \Delta T$$

has to be fulfilled to perform QKD with negligible errors due to chromatic dispersion. To match this condition for a given length of fiber, one can use large ΔT, reduce the dispersion D, or use photons with fine spectral width. We do not have to deal with similar problems caused by polarization mode dispersion, as information is not encoded in polarization.

Theoretically, ΔT could be as large as needed by increasing the path length difference of the interferometers. For example, a difference larger than 3 m is needed for 30 km of standard fiber with our source. However, interferometers of this size are hard to stabilize. Moreover, fiber interferometers suffer from a chromatic dispersion difference between the 2 arms that reduces the visibility. Another point is that even if there is no overlap between the peaks, dispersion broadens them. Consequently, wider coincidence windows are required, increasing the error contribution of the detectors' noise. For these reasons we did not implement this solution.

In order to reduce D it is possible to use dispersion shifted fiber for the quantum channel as in [17]. This solution is not relevant because the resulting set-up would not be deployable in a real-world telecom network, as there are only few installed lines using this kind of fiber.

Another possibility is to use dispersion compensation [19], with the only drawback of the added loss on the quantum channel (which lowers the signal over noise ratio). This solution is the first that we investigate in this article.

Alternatively, we reduce the $\Delta\lambda$ of the 1550 nm photons (for 30 km the above necessary condition implies $\Delta\lambda < 5.5$ nm) by inserting a bandpass filter on Alice's side. As the central wavelength and the spectral width of the 2 down converted photons are related by energy conservation, filtering on one side reduces the spectral width of the twin photons detected on the other side. Bob's detectors are gated upon Alice's detections, thus, even if the key rate is reduced, the signal over noise ratio remains constant.

To implement the full BB84 protocol, two different measurement bases are needed. This can be done by using 2 interferometers or a fast switch inside a single interferometer. Here we use a birefringent interferometer where the phase applied on the photons depends on the polarization. Thanks to this, we implement the full energy-time entangled BB84 protocol [2,3] with only 2 interferometers instead of 4. More details can be found in [17]. Pairs of 810−1550 nm photons are produced from a type I configuration of $KNbO_3$ crystal pumped by a 532 nm continuous laser. The 810 nm photons are collected in a single mode fiber and sent to Alice's interferometer which is made of bulk optical components. It has 4 outputs, each of them consisting of a single mode fiber coupling system followed by a passively quenched silicon photon counter (EG&G). The 1550 nm photons are collected in a single mode fiber and launched into the quantum channel which is a spool of several kilometers of standard fiber. It can be optionally followed by our dispersion compensation device, i.e. a spool of negative dispersion fiber. Bob's interferometer is connected at the other side of the quantum channel, together with a polarization beam-splitter and Faraday mirror system that are part of the BB84 implementation. Two gated-mode InGaAs detectors (idQuantique) are connected at the interferometer's outputs. The path difference of both interferometers correspond to 1 m optical length, and consequently $\Delta T \cong 3.3$ ns.

An electronic system is used to trigger Bob's detectors whenever a photon is detected by any of Alice's detectors. These electronics can also be used to characterize the system in real-time: the information about which of Alice's detectors registered a count can optionally be coded and sent to Bob's through a synchronized classical channel (consisting of another spool of standard fiber) using a 1550 nm laser. Upon detection at Bob's side, this information can be used for sifting and to verify the bits. These electronics thus enables one to have immediate information about the sifted raw key creation rate and the error rate.

The most relevant experimental parameters are the following: spectral FWHM of the down converted photons: 6.9 nm at 1550 nm, 2 nm at 810 nm; probability of having a photon coupled into the quantum channel whenever the 810 nm silicium detector fires: 0.5; losses of Bob's

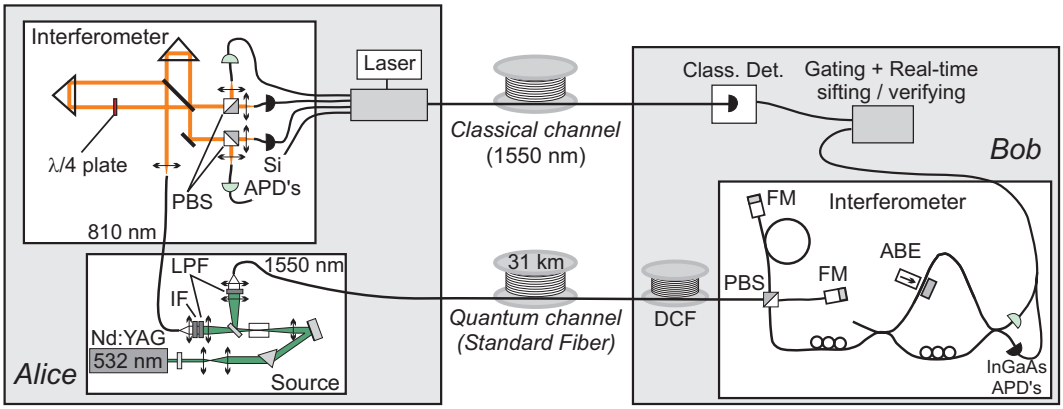

Fig. 2. Schematic diagram of the experimental set-up (PBS: polarizing beam splitter; LPF: low-pass pump filters; IF: optional 2 nm bandpass filter; DCF: optional dispersion compensating fiber; FM: Faraday mirrors; ABE: adjustable birefringent element used as fibre $\lambda/4$ plate).

apparatus: 5.4 dB; quantum efficiency of Bob's detectors: 10%; detection gate width $W = 1.1$ ns; false counts per gate due to the average noise of both detectors at Bob: $\sim 1.13 \times 10^{-5}$; false counts per gate due to noise on Alice's side: negligible.

The whole set-up requires very careful tuning. The most difficult part is the alignment of Alice's bulk interferometer. In particular, we have to pay attention that the probabilities for the short-short and long-long events are equals for all combination of detections at Alice and at Bob [20]. Bob's apparatus must also be aligned to ensure that the polarization transformations in both arms of the interferometer are identical.

We used a quantum channel consisting of a spool of 31 km of standard fiber, inducing losses of 8.3 dB. Two different configurations were implemented to limit the effect of chromatic dispersion.

In the first one, the dispersion compensating spool (OFS) was connected in between the quantum channel and Bob's apparatus. This device compensates a dispersion of $D_{comp} \cong 506\ \mathrm{ps\,nm^{-1}}$, which corresponds to about 30 km of standard fiber. It induces losses of 2.9 dB, and a delay corresponding to 4 km of standard fiber. A 31+4 km spool of standard fiber was consequently used for the classical channel. In this case we implemented the full two bases BB84 protocol using 4 detectors on Alice's side. The total count rate at Alice was about 79 kHz. The visibility of the interferences was about 89%.

In the second configuration, an interferometric bandpass filter was placed in the source apparatus just before the collection lenses of the 810 nm output port (see IF in Fig. 2). We used a filter of 2 nm FWHM centered at 814 nm (as this has been determined to be optimal for production/collection) and consequently the central wavelength of the co-detected photons was 1536 nm. As the Gaussian 2 nm filter acts on an approximately 2 nm wide Gaussian spectrum, we obtained a width of about 1.45 nm FWHM at 814 nm, and 5.2 nm at 1536 nm. The number of 810 nm photons detected was reduced by a factor of about 3. To facilitate the alignment and measurement in this second configuration, we increased the coincidences count rate by using only one of the two BB84 bases. The total count rate at Alice was about 36 kHz and the visibility of the interference was about 92% in this case.

Figure 3 shows the resulting temporal distributions of the events obtained for 4 set-ups. Using the first plot, we obtained the total electronic/detection jitter of value 0.7 ns, the FWHM of the (central) peak; we also use this plot to verify that $\Delta T = 3.3$ ns. The second plot clearly shows that a dispersion reduction method is necessary. Indeed, in the absence of any dispersion reduction, the two side peaks overlap to a large extent within the detection window. We determined that in this case, the error rate due, only to the contribution of uncorrelated events counted inside the detection windows, is already about 10% of the total count rate. Moreover, the peaks are more than 3 time larger than the detection windows, lowering the detection rate. The effect of the dispersion reduction is clearly visible on the third and fourth plots, corresponding to the two configurations described above. Note that the available filter of 2 nm does not completely remove the effect of chromatic dispersion. However, a narrower filter would further decrease the total count rate.

We achieved key distribution for both these solutions. Because of phase instabilities in the interferometers the duration of a key exchange was limited to about 40−50 minutes, but this issue could be addressed by using actively stabilized interferometers [21]. During this period the quantum bit error rate (QBER), the ratio of the error rate over the total rate after sifting, was about 10% on average. Table 1 summarizes the performance obtained in terms of the different sources of errors. The total QBER is the sum of several contributions:

(i) Opt: the optical error rate due to the imperfect contrast of the interferences;

(ii) Acc: the accidental coincidences due to the non-zero probability of creating two pairs during the detection gate time-interval: the photons from two different pairs are not entangled and thus have a 50% probability of producing incorrect bits;

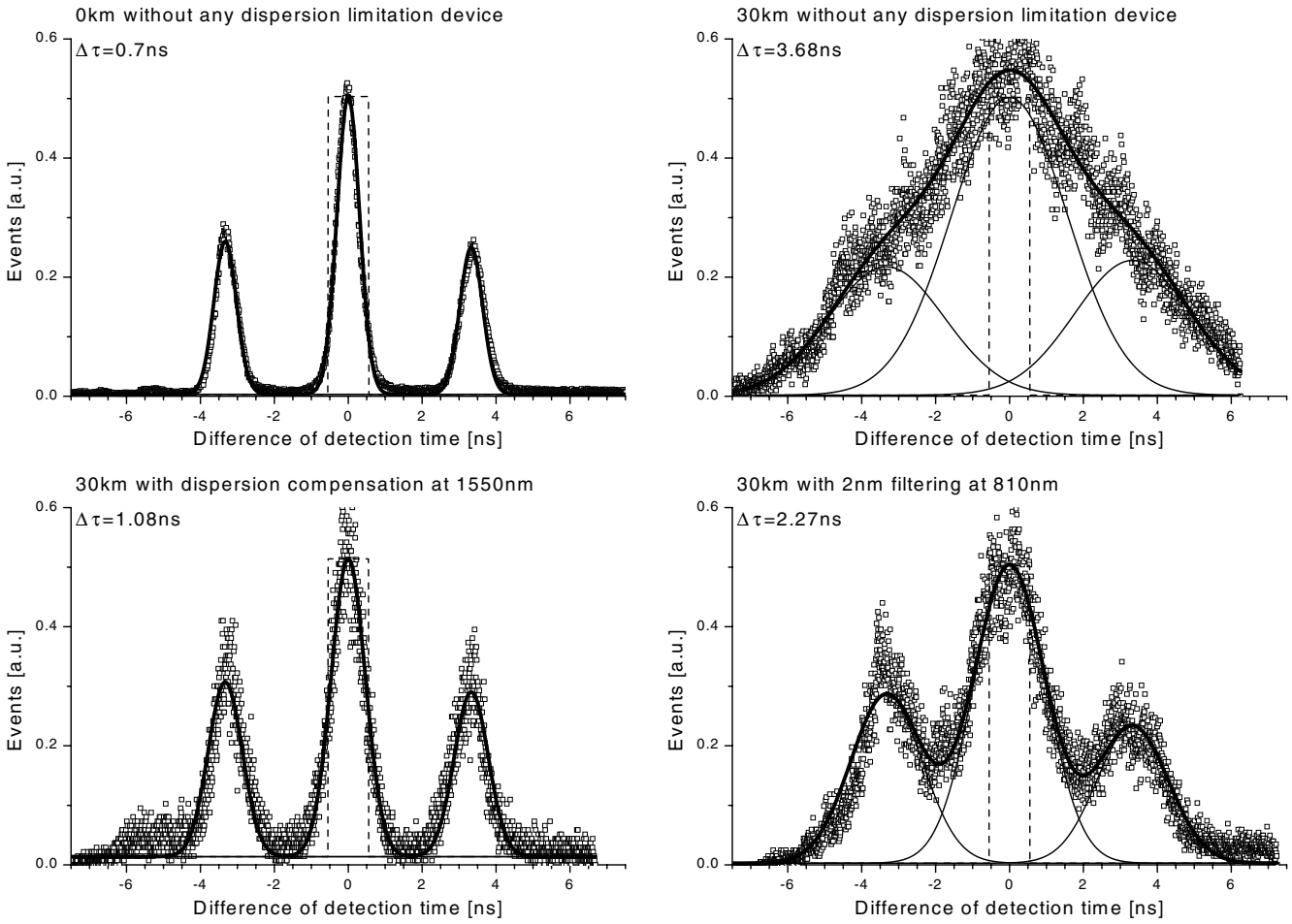

Fig. 3. Distribution of coincidence detection times for different set-ups. The squares show the experimental data. The plain curves show the individual Gaussian peak; the heavy curve shows the sum of the 3 peak's contributions which are fitted to the experimental data to extract the FWHM $\Delta\tau$ of the peaks; the dashed lines show the position and width of the detection gate.

Table 1. QKD performances for both implementations.

Configuration	Sifted key rate	Opt. QBER	Acc. QBER	Detect. QBER	Disp. QBER	Tot. QBER
compensation	23 Hz	5.5%	1%	4%	≅0%	10.5%
filtering	12 Hz	4%	1%	1.7%	0.5%	7.2%

(iii) Detect: the detectors' noise, which is independent of distance. As the detection count decrease with the losses in the line this detector QBER contribution increases with the distance and is generally the main contribution for large distances;

(iv) Disp: the dispersion which makes some non-correlated events to be registered inside the detection gate, as explained above.

To estimate this QBER contribution we used the measurement presented in Figure 3. Using the fitted $\Delta\tau$ of the peaks, it is possible to numerically integrate the 3 Gaussian curves inside the discriminator window to obtain the part of detections which comes from the side peaks. This is the error rate arising from the chromatic dispersion effect. Note that, for given ΔT and W, this integral value grows rapidly with $\Delta\tau$ when this variable reaches about one third of ΔT. The chromatic dispersion QBER is thus very sensitive to spectral width and fiber length.

The detector QBER is more important in the compensation configuration mainly because the compensating device add losses on the quantum channel, reducing the signal over noise ratio by a factor 2. However, one of Bob's detectors was about 5 times less noisy than the other. With two such detectors, the detection QBER for the compensating solution would drop below 1%.

The numerical integration of the event peaks was also used to calculate the fraction of the incoming photons which accounted for bits of the key. If all the photons that are part of the short-short/long-long events were inside the detection gate this number would be 0.5. In our case

Table 2. Factors leading to sifted key rates.

Configuration	Singles rate	μ	T_L (dB)	T_B (dB)	T_C (dB)	η_d	η_g	q_s	Sifted key rate
compensation	79 kHz	0.5	8.3	5.4	2.9	0.1	0.38	0.7	23 Hz
filtering	36 kHz	0.5	8.3	5.4	0	0.1	0.22	0.7	12 Hz

it is 0.38 for the compensation solution and 0.22 for the filtering solution as the events are more widely distributed in the second case (see Fig. 3). These values are taken into account as a small added loss for the filtering solution with respect to the compensating one. Table 2 summarizes the different factors leading to the registered sifted key rates, starting from the singles rate at Alice. These factors are: μ: probability of having a photon coupled into the quantum channel whenever the 810 nm silicon detector fires; T_L: loss over the quantum channel; T_B: loss in Bob's apparatus; T_C: loss in the dispersion compensating fiber spool; η_d: quantum efficiency of Bob's detectors; η_g: fraction of the incoming photons which are counted as bits; q_s: proportion of the bits that remain after sifting. This number should be 0.5 for a perfectly balanced two bases system. In the compensation case the value 0.7 is explained by two reasons. First, the bases choice at Alice is biased by the differences between the four bulk-to-fiber coupling and detector efficiencies. Secondly, the passive choice of bases at Bob depends on the polarization of the incoming photons. These photons are only partially depolarized by 30 km of fiber, and the remaining polarization fluctuates inside the quantum channel during the key exchange. In the filtering case, as we use only one base at Alice, we could achieve a value of 1 by tuning the passive choice at Bob if the incoming photons where perfectly polarized, but this is not the case. Moreover, as in the compensation case, the polarization fluctuates inside the quantum channel. Note that a $q_s \neq 0.5$ does not impair on the security of the scheme [22].

From theses results, we see that the choice of the best suitable dispersion reduction method is a matter of tradeoff between QBER and key rate values, and is different for each particular set-up. In our case, numerical estimations show that an optimized compensation solution is better in term of key rate beyond 15 km, for a given QBER. However, the amount of negative dispersion introduced must be calculated specifically for a given length of the quantum channel fiber. The main practical advantage of the filtering solution is thus that the system can be uniquely designed to be usable over a wide range of distances. The resulting key rate decrease can be compensated by pumping the source with a more powerful laser, or by using a more efficient photon pair source such as periodically poled lithium niobate waveguide [23]. When this is possible, filtering is more useful for real application. The only problem resulting from a configuration using a heavily pumped source filtered at Alice is the increase of accidental uncorrelated coincidence counts. This issue can be solved by filtering the photons at Bob with a corresponding filter. As both wavelengths are correlated, the only drawback is the non unity peak transmission of the filter.

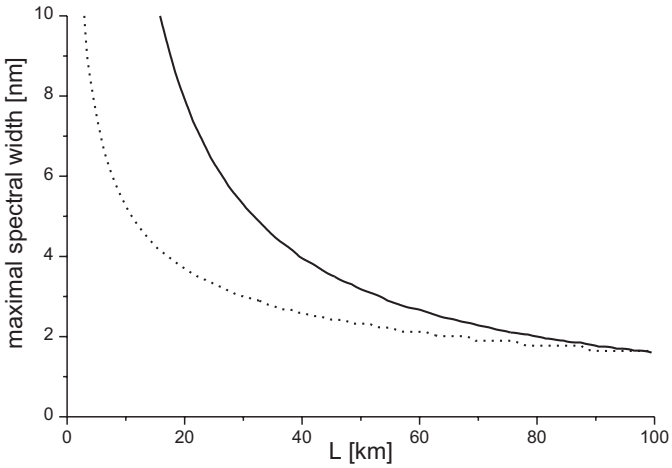

Fig. 4. Maximal spectral width that keeps chromatic and polarization dispersion induced QBER below 1% as function of the quantum channel length. Plain curve: this energy-time entanglement implementation, with $\Delta T = 3.3$ ns; dotted curve: possible optimal polarization entanglement implementation with PMD values of 0.1 ps km$^{-\frac{1}{2}}$.

The spectral width of the photons is also a limiting factor for polarization entanglement based QKD. QBER increasing in the case of polarization QKD is due to polarization mode dispersion (PMD) that depolarizes low coherent photons. Figure 4 shows the calculated maximal spectral width of 1550 nm photons that keeps the chromatic/polarization dispersion induced QBER below 1%. The curve for energy-time entangled photons is calculated using our particular experimental parameters, while the one for polarization is calculated using $QBER = 0.5 \times (1 - \overline{DOP})$ where $\overline{DOP}$ is the average degree of polarization computed numerically from formulas developed in [24], using the standard PMD value of 0.1 ps km$^{-\frac{1}{2}}$. We see that for distances up to about 100 km, the energy-time solution is more robust to large spectral width. For longer ranges both solutions become similar with a slight advantage for the one using polarization, because of the square root dependence of the PMD with distance. However, these curves strictly apply to dispersion QBER and do not take into account technical difficulties related to the necessary active polarization state control.

In this article, we presented two practical means of dealing with chromatic dispersion induced problems in long-range QKD using entangled photon-pairs: dispersion compensation and reduction of the photons' spectral width at Alice. Optimal parameters where investigated and these solutions were demonstrated by implementing a partial and complete BB84-like protocol with a set-up

featuring characteristics that could lead to real-world telecom applications. A secret key was distributed over 30 km of standard fiber at a sifted bit rate of more than 20 Hz and with an average QBER below the 11% limit for absolute security as stated in [25]. Higher key rates are possible using more efficient sources. However, for a practical implementation, actively stabilized interferometers are needed.

The authors would like to thank Claudio Barreiro and Jean-Daniel Gautier for technical support. Financial support by the Swiss NCCR Quantum Photonics is acknowledged.

References

1. C. Bennett, G. Brassard, in *Proceedings of the IEEE International Conference onf Computers, Systems and Signal Processing, Bangalore* (IEEE, New York, 1984), p. 175
2. A. Ekert, Phys. Rev. Lett. **67**, 661 (1991)
3. A. Ekert, J. Rarity, P. Tapster, M. Palma, Phys. Rev. Lett. **69**, 1293 (1992)
4. P. Townsend, Opt. Fiber Technol.: Mater., Devices Syst. **4**, 345 (1998)
5. J.-M. Mérolla, Y. Mazurenko, J.-P. Goedgebuer, W. Rhodes, Phys. Rev. Lett. **82**, 1656 (1999)
6. G. Ribordy, J.-D. Gautier, N. Gisin, O. Guinnard, H. Zbinden, J. Mod. Opt. **47**, 517 (2000)
7. A. Acín, N. Gisin, V. Scarani, Phys. Rev. A **69**, 012309 (2004); V. Scarani, A. Acín, G. Ribordy, N. Gisin, Phys. Rev. Lett. **92**, 057901 (2004)
8. R. Hughes, G. Morgan, C. Peterson, J. Mod. Opt. **47**, 533 (2000)
9. D. Stucki, N. Gisin, O. Guinnard, G. Ribordy, H. Zbinden, New J. Phys. **4**, 41 (2002)
10. H. Kosaka, A. Tomita, Y. Nambu, T. Kimura, K. Nakamura, Elec. Lett. **39**, 1199 (2003)
11. A. Shields et al., presented at CLEO/QELS2003, QThPDB8 (2003)
12. A. Beveratos, R. Brouri, T. Gacoin, A. Villing, J.-P. Poizat, P. Grangier, Phys. Rev. Lett. **89**, 187901 (2002)
13. M. Pelton, C. Santori, G.S. Solomon, O. Benson, Y. Yamamoto, Eur. Phys. J. D **18**, 179 (2002)
14. T. Jennewein, C. Simon, G. Weihs, H. Weinfurter, A. Zeilinger, Phys. Rev. Lett. **84**, 4729 (2000)
15. D.S. Naik, C.G. Peterson, A.G. White, A.J. Berglund, P.G. Kwiat, Phys. Rev. Lett. **84**, 4733 (2000)
16. W. Tittel, J. Brendel, H. Zbinden, N. Gisin, Phys. Rev. Lett. **84**, 4737 (2000)
17. G. Ribordy, J. Brendel, J.-D. Gautier, N. Gisin, H. Zbdinden, Phys. Rev. A **63**, 012309 (2000)
18. J.D. Franson, Phys. Rev. Lett. **62**, 2205 (1989)
19. IEEE J. Lightwave Technol. **12**, 1705 (1994); special issue, edited by D. Hall
20. This simple procedure can be interpreted as entanglement concentration. See A. Vaziri, J.-W. Pan, T. Jennewein, G. Weihs, A. Zeilinger, Phys. Rev. Lett. **91**, 22 (2003)
21. I. Marcikic, H. de Riedmatten, W. Tittel, H. Zbinden, M. Legré, N. Gisin, e-print `arXiv:quant-ph/0404124` (2004), submitted
22. M. Ardehali, H.F. Chau, H.-K. Lo, e-print `arXiv:quant-ph/9803007` (1998)
23. S. Tanzilli, W. Tittel, H. De Riedmatten, H. Zbinden, P. Baldi, M. De Micheli, D.B. Ostrowsky, N. Gisin, Eur. Phys. J. D **18**, 155 (2002)
24. N. Gisin, J. Mod. Opt. **48**, 1397 (2001)
25. P.W. Shor, J. Preskill, Phys. Rev. Lett. **85**, 441 (2000)