Secure polarization-independent subcarrier quantum key distribution in optical fiber channel using BB84 protocol with a strong reference

A. V. Gleim,[1,3,4] V. I. Egorov,[1,5] Yu. V. Nazarov,[1] S. V. Smirnov,[1] V. V. Chistyakov,[1] O. I. Bannik,[1] A. A. Anisimov,[1] S. M. Kynev,[1] A. E. Ivanova,[1] R. J. Collins,[2] S. A. Kozlov,[1] and G. S. Buller[2]

[1]*ITMO University, Department of Photonics and Optical Information Technology, 199034 Kadetskaya Line 3b, Saint Petersburg, Russia*

[2]*Heriot-Watt University, Institute of Photonics and Quantum Sciences, School of Engineering and Physical Sciences, Edinburgh, EH14 4AS, UK*

[3]*Kazan National Research Technical University KAI, 420111, Karl Marx str. 10, Kazan, Russia*

[4]*agleim@corp.ifmo.ru*

[5]*viegorov@corp.ifmo.ru*

Abstract: A quantum key distribution system based on the subcarrier wave modulation method has been demonstrated which employs the BB84 protocol with a strong reference to generate secure bits at a rate of 16.5 kbit/s with an error of 0.5% over an optical channel of 10 dB loss, and 18 bits/s with an error of 0.75% over 25 dB of channel loss. To the best of our knowledge, these results represent the highest channel loss reported for secure quantum key distribution using the subcarrier wave approach. A passive unidirectional scheme has been used to compensate for the polarization dependence of the phase modulators in the receiver module, which resulted in a high visibility of 98.8%. The system is thus fully insensitive to polarization fluctuations and robust to environmental changes, making the approach promising for use in optical telecommunication networks. Further improvements in secure key rate and transmission distance can be achieved by implementing the decoy states protocol or by optimizing the mean photon number used in line with experimental parameters.

OCIS codes: (270.5568) Quantum cryptography; (270.5565) Quantum communications.

References and Links

1. C. Bennett and G. Brassard, "Quantum cryptography: public key distribution and coin tossing," in *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, (IEEE, 1984), pp 175–179.
2. W. K. Wootters and W. H. Zurek, "A single quantum cannot be cloned," Nature **299**(5886), 802–803 (1982).
3. V. Fernandez, R. J. Collins, K. J. Gordon, P. D. Townsend, and G. S. Buller, "Passive optical network approach to gigahertz-clocked multiuser quantum key distribution," IEEE J. Quantum Electron. **43**(2), 130–138 (2007).
4. K. A. Patel, J. F. Dynes, I. Choi, A. W. Sharpe, A. R. Dixon, Z. L. Yuan, R. V. Penty, and A. J. Shields, "Coexistence of high-bit-rate quantum key distribution and data on optical fiber," Phys. Rev. X **2**(4), 041010 (2012).
5. M. Peev, C. Pacher, R. Alléaume, C. Barreiro, J. Bouda, W. Boxleitner, T. Debuisschert, E. Diamanti, M. Dianati, J. F. Dynes, S. Fasel, S. Fossier, M. Fürst, J.-D. Gautier, O. Gay, N. Gisin, P. Grangier, A. Happe, Y. Hasani, M. Hentschel, H. Hübel, G. Humer, T. Länger, M. Legré, R. Lieger, J. Lodewyck, T. Lorünser, N. Lütkenhaus, A. Marhold, T. Matyus, O. Maurhart, L. Monat, S. Nauerth, J.-B. Page, A. Poppe, E. Querasser, G. Ribordy, S. Robyr, L. Salvail, A. W. Sharpe, A. J. Shields, D. Stucki, M. Suda, C. Tamas, T. Themel, R. T. Thew, Y. Thoma, A. Treiber, P. Trinkler, R. Tualle-Brouri, F. Vannel, N. Walenta, H. Weier, H. Weinfurter, I. Wimberger, Z. L. Yuan, H. Zbinden, and A. Zeilinger, "The SECOQC quantum key distribution network in Vienna," New J. Phys. **11**(7), 075001 (2009).

#254859 Received 3 Dec 2015; revised 27 Jan 2016; accepted 27 Jan 2016; published 2 Feb 2016

6. K. Yoshino, M. Fujiwara, A. Tanaka, S. Takahashi, Y. Nambu, A. Tomita, S. Miki, T. Yamashita, Z. Wang, M. Sasaki, and A. Tajima, "High-speed wavelength-division multiplexing quantum key distribution system," Opt. Lett. **37**(2), 223–225 (2012).
7. M. Sasaki, M. Fujiwara, H. Ishizuka, W. Klaus, K. Wakui, M. Takeoka, S. Miki, T. Yamashita, Z. Wang, A. Tanaka, K. Yoshino, Y. Nambu, S. Takahashi, A. Tajima, A. Tomita, T. Domeki, T. Hasegawa, Y. Sakai, H. Kobayashi, T. Asai, K. Shimizu, T. Tokura, T. Tsurumaru, M. Matsui, T. Honjo, K. Tamaki, H. Takesue, Y. Tokura, J. F. Dynes, A. R. Dixon, A. W. Sharpe, Z. L. Yuan, A. J. Shields, S. Uchikoga, M. Legré, S. Robyr, P. Trinkler, L. Monat, J.-B. Page, G. Ribordy, A. Poppe, A. Allacher, O. Maurhart, T. Länger, M. Peev, and A. Zeilinger, "Field test of quantum key distribution in the Tokyo QKD Network," Opt. Express **19**(11), 10387–10409 (2011).
8. J.-M. Mérolla, Y. Mazurenko, J.-P. Goedgebuer, H. Porte, and W. T. Rhodes, "Phase-modulation transmission system for quantum cryptography," Opt. Lett. **24**(2), 104–106 (1999).
9. J.-M. Merolla, Y. Mazurenko, J.-P. Goedgebuer, and W. T. Rhodes, "Single-photon interference in sidebands of phase-modulated light for quantum cryptography," Phys. Rev. Lett. **82**(8), 1656–1659 (1999).
10. L. Duraffourg, J.-M. Merolla, J.-P. Goedgebuer, Y. Mazurenko, and W. T. Rhodes, "Compact transmission system using single-sideband modulation of light for quantum cryptography," Opt. Lett. **26**(18), 1427–1429 (2001).
11. O. Guerreau, J.-M. Mérolla, A. Soujaeff, F. Patois, J. P. Goedgebuer, and F. J. Malassenet, "Long distance QKD transmission using single sideband detection scheme with WDM synchronization," IEEE J. Sel. Top. Quantum Electron. **9**(6), 1533–1540 (2003).
12. A. Ortigosa-Blanch and J. Capmany, "Subcarrier multiplexing optical quantum key distribution," Phys. Rev. A **73**(2), 024305 (2006).
13. J. Mora, A. Ruiz-Alba, W. Amaya, A. Martínez, V. García-Muñoz, D. Calvo, and J. Capmany, "Experimental demonstration of subcarrier multiplexed quantum key distribution system," Opt. Lett. **37**(11), 2031–2033 (2012).
14. J. Mora, W. Amaya, A. Ruiz-Alba, A. Martinez, D. Calvo, V. García Muñoz, and J. Capmany, "Simultaneous transmission of 20x2 WDM/SCM QKD and 4 bidirectional classical channels over a PON," Opt. Express **20**(15), 16358 (2012).
15. A. V. Gleim, A. A. Anisimov, L. N. Asnis, Yu. B. Vaktkhtomin, A. V. Divochii, V. I. Egorov, V. V. Kovaluk, A. A. Korneev, S. M. Kynev, Yu. V. Nazarov, R. V. Ozhegov, A. V. Rupasov, K. V. Smirnov, M. A. Smirnov, G. N. Gol'tsman, and S. A. Kozlov, "Quantum key distribution in an optical fiber at distances of up to 200 km and a bit rate of 180 bit/s," Bull. Russ. Acad. Sci., Physics **78**(3), 171–175 (2014).
16. G. N. Gol'tsman, O. Okunev, G. Chulkova, A. Lipatov, A. Semenov, K. Smirnov, B. Voronov, A. Dzardanov, C. Williams, and R. Sobolewski, "Picosecond superconducting single-photon optical detector," Appl. Phys. Lett. **79**(6), 705–707 (2001).
17. E. A. Dauler, M. E. Grein, A. J. Kerman, F. Marsili, S. Miki, S. W. Nam, M. D. Shaw, H. Terai, V. B. Verma, and T. Yamashita, "Review of superconducting nanowire single-photon detector system design options and demonstrated performance," Opt. Eng. **53**(8), 081907 (2014).
18. V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, "The security of practical quantum key distribution," Rev. Mod. Phys. **81**(3), 1301–1350 (2009).
19. "Corning SMF-28e+ optical fiber product information," http://www.corning.com/media/worldwide/coc/documents/PI1463_07-14_English.pdf.
20. H. K. Lo, X. Ma, and K. Chen, "Decoy state quantum key distribution," Phys. Rev. Lett. **94**(23), 230504 (2005).
21. M. Koashi, "Unconditional security of coherent-state quantum key distribution with a strong phase-reference pulse," Phys. Rev. Lett. **93**(12), 120501 (2004).
22. O. Guerreau, F. J. Malassenet, S. W. McLaughlin, and J.-M. Merolla, "Quantum key distribution without a single photon source using a strong reference," IEEE Photonics Technol. Lett. **17**(8), 1755–1757 (2005).
23. S. Wang, W. Chen, J. F. Guo, Z. Q. Yin, H. W. Li, Z. Zhou, G. C. Guo, and Z. F. Han, "2 GHz clock quantum key distribution over 260 km of standard telecom fiber," Opt. Lett. **37**(6), 1008–1010 (2012).
24. J. Capmany and C. R. Fernandez-Pousa, "Impact of third-order intermodulation on the performance of subcarrier multiplexed quantum key distribution," J. Lightwave Technol. **29**(20), 3061–3069 (2011).
25. C.-C. Chen, H. Porte, A. Carenco, J.-P. Goedgebuer, and V. Armbruster, "Phase correction by laser ablation of a polarization independent LiNbO3 Mach–Zehnder modulator," IEEE Photonics Technol. Lett. **9**(10), 1361–1363 (1997).
26. G. S. Buller and R. J. Collins, "Single-photon detectors for infrared wavelengths in the range 1–1.7 μm," in *Springer Series on Fluorescence: Methods and Applications: Advanced Photon Counting*, P. Kapusta, M. Wahl, and R. Erdmann, eds. (Springer, 2014), pp 43–69.
27. B. Korzh, N. Walenta, T. Lunghi, N. Gisin, and H. Zbinden, "Free-running InGaAs single photon detector with 1 dark count per second at 10% efficiency," Appl. Phys. Lett. **104**(8), 081108 (2014).
28. B. Korzh, C. C. W. Lim, R. Houlmann, N. Gisin, M. J. Li, D. Nolan, B. Sanguinetti, R. Thew, and H. Zbinden, "Provably secure and practical quantum key distribution over 307 km of optical fibre," Nat. Photonics **9**(3), 163–168 (2015).
29. D. M. Rowe, ed., *Thermoelectrics Handbook: Macro to Nano*, (CRC, 2005).
30. J. Capmany, "Photon nonlinear mixing in subcarrier multiplexed quantum key distribution systems," Opt. Express **17**(8), 6457–6464 (2009).
31. M. Fox, *Quantum Optics: An Introduction* (Oxford University, 2006).

#254859 Received 3 Dec 2015; revised 27 Jan 2016; accepted 27 Jan 2016; published 2 Feb 2016

32. J. Martinez-Mateo, C. Pacher, M. Peev, A. Ciurana, and V. Martin, "Demystifying the information reconciliation protocol Cascade," Quantum Inf. Comput. **15**, 453–477 (2015).
33. X. Ma, B. Qi, Y. Zhao, and H.-K. Lo, "Practical decoy state for quantum key distribution," Phys. Rev. A **72**(1), 012326 (2005).
34. S. Bhattacharya and P. Kumar, "Decoy-state method for subcarrier-multiplexed frequency-coded quantum key distribution," J. Opt. Soc. Am. B **30**(4), 782–787 (2013).
35. R. Y. Q. Cai and V. Scarani, "Finite-key analysis for practical implementations of quantum key distribution," New J. Phys. **11**(4), 045024 (2009).
36. F. Xu, B. Qi, Z. Liao, and H.-K. Lo, "Long distance measurement-device-independent quantum key distribution with entangled photon sources," Appl. Phys. Lett. **103**(6), 061101 (2013).
37. P. A. Hiskett, D. Rosenberg, C. G. Peterson, R. J. Hughes, S. Nam, A. E. Lita, A. J. Miller, and J. E. Nordholt, "Long-distance quantum key distribution in optical fiber," New J. Phys. **8**(9), 193 (2006).
38. A. R. Dixon, Z. L. Yuan, J. F. Dynes, A. W. Sharpe, and A. J. Shields, "Continuous operation of high bit rate quantum key distribution," Appl. Phys. Lett. **96**(16), 161102 (2010).
39. K. A. Patel, J. F. Dynes, M. Lucamarini, I. Choi, A. W. Sharpe, Z. L. Yuan, R. V. Penty, and A. J. Shields, "Quantum key distribution for 10 Gb/s dense wavelength division multiplexing networks," Appl. Phys. Lett. **104**(5), 051123 (2014).
40. R. Amiri, P. Wallden, A. Kent, and E. Andersson, "Secure quantum signatures using insecure quantum channels," arXiv:1507.02975 [quant-ph] (2015).
41. R. J. Collins, R. J. Donaldson, V. Dunjko, P. Wallden, P. J. Clarke, E. Andersson, J. Jeffers, and G. S. Buller, "Realization of quantum digital signatures without the requirement of quantum memory," Phys. Rev. Lett. **113**(4), 040502 (2014).

1. Introduction

Quantum key distribution (QKD) systems allow the creation of a shared secure symmetric key between two users by transmitting a stream of single photons encoded in non-orthogonal basis sets [1]. According to the laws of quantum physics, it is impossible for a third party to measure these states without disturbing the system and introducing errors, so that legitimate users of such systems can detect the potential eavesdropping of the secure channel [2]. In recent years, there has been increasing research work in integrating these systems into the installed optical fiber telecommunication network infrastructure [3]. This work has included simultaneous key distribution and data transfer in a single fiber [4], quantum network architectures [5] and multiplexed multichannel QKD systems [6]. In practice, the environmental robustness of QKD systems devices under varying external conditions remains an important criterion for deployment in optical telecommunication networks [7].

One of the practical approaches to the implementation of QKD, with particular potential for optical network implementation, is based on subcarrier wave generation (SCW) [8–15]. Its main feature lies in a method of single photon generation in which the signal photons are not emitted directly by a source but are generated on subcarrier frequencies, or sidebands, as a result of phase [8] or amplitude [13] modulation of a classical field on the central frequency, or carrier wave. Advantages of this type of QKD system include an absence of complicated distributed interferometry schemes and the simplification of phase shift matching in the transmitter (Alice) and receiver (Bob) modules. Perhaps one of the most valuable features of SCW QKD systems is the exceptionally efficient use of the quantum channel bandwidth and the ready capability of signal multiplexing of added subcarriers on the same carrier source. This could give the subcarrier approach a significant advantage in fiber networking applications. For example, recent work [12,13] has investigated the use of the subcarrier method for simultaneous distribution of several keys on different sidebands of a single carrier wave. This technique can also be combined with traditional wavelength division multiplexing (WDM) [14], which potentially allows significantly increased quantum channel bandwidth use in optical fibers (up to 40% compared to 2-4% in other QKD systems for 1 Gbit Ethernet, as discussed in [13]), therefore making SCW QKD systems perfect candidates for building blocks in quantum networks.

Until recently, experimentally demonstrated transmission distances in SCW QKD systems have been relatively short-range, typically over fiber spans of less than 50 km [11,13]. This is mostly due to the technical challenges of maintaining polarization stability in

#254859 Received 3 Dec 2015; revised 27 Jan 2016; accepted 27 Jan 2016; published 2 Feb 2016

telecommunications optical fiber and efficient separation of signal and carrier in receiver modules. Previously, secure SCW QKD operation could only be implemented for systems with relatively low channel loss of around 2.5 dB (corresponding to a range of 12 km for photons at a wavelength of 1550 nm) [14]. More recently [15], our group demonstrated a subcarrier wave QKD system that generated sifted bits at a rate of 180 bit/s over a distance of 200 km (corresponding to a loss of 34 dB). This result was achieved using a clock frequency of 100 MHz as well as a superconducting nanowire single photon detector (SNSPD) [16,17] with a single-photon detection efficiency of 16% and dark count rate of 10 counts per second. However, the setup in [15] used a two-state phase protocol that was insecure at long distances [18]. It is also important to note that the setups developed in [13,14] require special optical fibers with shifted dispersion, as well as active polarization controllers (also used in [15] for long distances). These issues restrict the compatibility of these systems with the existing optical fiber network infrastructure.

In this paper a SCW QKD system is described, in which a sifted bit rate of 800 bit/s was demonstrated in a quantum channel with 30 dB loss. This loss corresponded to, for example, a 150 km link of single mode fiber with 0.2 dB/km loss at a wavelength of 1550 nm [19]. The system demonstrated in this paper is characterized by several major improvements compared to our previous work [15], providing unconditionally secure key exchange and improved robustness to environmental changes. First, the four-state BB84 protocol was implemented using a strong reference instead of the two-state protocol employed previously in [15]. The strong reference method, usually deployed as an alternative to the widely-used decoy states approach [20], was initially proposed in [21] and studied for SCW systems in [22]. Secondly, a passive unidirectional subsystem was introduced in order to compensate for the polarization dependence of the phase modulators in the Bob module. This removed the requirement for active polarization compensators or polarization preserving fibers in the communication channel between Alice and Bob. In comparison to the active approach implemented previously [15], the passive method highlighted in this paper improved the interference signal visibility in the receiver module to 98.9%, from 97.8% achieved previously and consequently decreased the quantum bit error rate (QBER) contribution related to imperfections in the passive optical system by 0.55%. This approach also made the QKD scheme almost entirely insensitive to polarization changes and robust against environmental fluctuations in the quantum channel. This advantage of the SCW QKD approach comes from the method of quantum state generation where information is encoded using a strong optical carrier and a weak pulse on sidebands rather than a pair of successive weak pulses. Thirdly, an improved detector was used with single-photon detection efficiency of 20% compared to the 16% used previously (the dark count rate of the detector remained at 10 counts per second). In addition, our SCW QKD system was improved by introducing an optical synchronization subsystem that replaced the electrical cable used in [15], significantly improving the practicality of future integration into the installed optical fiber infrastructure. Notably, the results were achieved despite a relatively low phase change frequency of 100 MHz (see e.g [23].), and suggest the potential of higher clock rates with the corresponding prospect of further increases in key distribution rate in SCW QKD systems in the future.

2. Principles of operation

Figure 1 shows a block diagram of our SCW QKD system. It consisted of Alice and Bob modules connected by the quantum channel and the synchronization channel, both of which were composed of Corning SMF-28e + optical fiber [19]. In addition, the quantum channel also had an optical attenuator to allow longer transmission lengths to be simulated. An open classical channel was used for basis set reconciliation connecting the two control computers (this is not shown in the Fig. 1). All optical connections inside the Alice and Bob modules were implemented using 8.2 μm core diameter panda-eye polarization-maintaining fibers. A semiconductor laser in Alice (Diode Laser 1 in Fig. 1) was used as a photon source for the

#254859 Received 3 Dec 2015; revised 27 Jan 2016; accepted 27 Jan 2016; published 2 Feb 2016

quantum channel. The emitted photons from the laser passed through an optical isolator and entered a lithium niobate ($LiNbO_3$) electro-optical travelling wave phase modulator (PM), where their phase was modulated by a radio frequency signal. The system reference (clock) frequency was set in the Alice system by the voltage controlled oscillator (VCO) that acted as a clock source. In order to generate the subcarrier a signal from the VCO was routed to an external phase-locked loop device, where it was transformed by frequency multiplication in order to generate an output electrical signal with frequency Ω (modulation frequency). The clock signal from the VCO also controls operation of a field-programmable gated-array (FPGA) logic module. The electrical signal with frequency Ω was used as the input to an electrical modulator (EPM) where a phase shift φ_A was induced into the electrical signal at a rate governed by the phase change frequency *f*, defined by the FPGA. The phase shift control was performed by an FPGA logic module that contains an algorithmic random number generator used to select the phase shift φ_A from several possible states according to the QKD protocol employed. In this demonstration we used four possible phase-states, namely 0, π/2, π and 3π/2, as in the BB84 protocol. An electrical signal modulated in the EPM was used as a driving signal for the PM. Therefore, a phase shift introduced into the optical signal in the PM is equivalent to the phase shift φ_A introduced into the electrical signal in the EPM. The PM on Alice's side also contained a linear polarizer aligned with the electro-optical crystal axis.

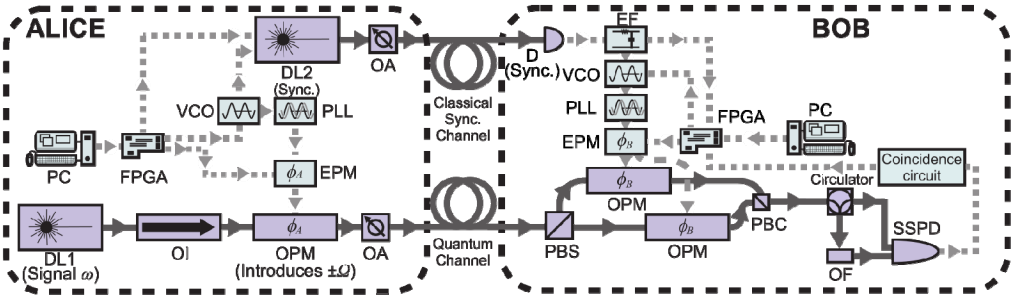

Fig. 1. Schematic of the polarization-independent subcarrier wave quantum key distribution system employing a standard telecommunication optical fiber quantum channel. DL1 and DL2 - Diode Laser 1 and 2, OI - Optical Isolator, OPM - Optical Phase Modulator, OA - Optical Attenuator, FPGA denotes a Field-Programmable Gated-Array and these serve (in conjunction with the control computers) as the control apparatus of this system, VCO - Voltage Control Oscillator, PLL - Phase Looked Loop, EPM - Electrical Phase Modulator, PBS and PBC are Polarization Beam Splitter and Combiner, OF – Optical Filter, SSPD – Superconducting Single Photon Detector, D - Photodiode. Φ denotes an optical phase modulator. In the current configuration, the system uses separate synchronization and signal channels to avoid additional noise in the quantum channel originating from Raman scattering and other unwanted optical contributions. The different quantum channel transmission distances were either composed of fiber or a combination of fiber and additional optical attenuation. Parameters ω and Ω are carrier and modulation frequencies (respectively), as detailed in Fig. 2 and utilized in (1) and (2).

Modulation in Alice's PM resulted in an optical path change, described by an additional exponential term in the field equation [8] given as:

$$E = A' e^{i\omega t} + \frac{iAa}{2} \cdot \left(e^{i((\omega+\Omega)t+\varphi_A)} + e^{i((\omega-\Omega)t-\varphi_A)} \right) \tag{1}$$

where A is the initial source amplitude and A' the modulated signal amplitude at the carrier wave (with a minor fraction of light energy moved to the subcarriers). It can be seen from (1) that two sidebands, separated from the ω frequency carrier wave by the value of modulation frequency Ω, appear in the optical spectrum, as shown in Fig. 2(a). The amplitude ratio between the central and subcarrier frequencies is defined by modulation index a. The spacing from the carrier to the subcarrier depends on the modulation frequency, thus limiting the

#254859 Received 3 Dec 2015; revised 27 Jan 2016; accepted 27 Jan 2016; published 2 Feb 2016

possible values of modulation frequency Ω which exhibit a distinguishable spectrum. After modulation the signal was attenuated and routed to the optical transmission medium. The attenuation introduced at Alice was chosen to ensure that the the total mean photon number μ of both the two sidebands combined met the security requirements for the quantum channel in the system. As discussed in [22,24], for subcarrier wave QKD systems the optimal value is μ = 1. This choice was made in order to implement an unconditionally secure BB84 protocol with strong reference [21], briefly described in the next section.

The polarization independence of the QKD system results from the use of a polarizing beam splitter (PBS) in the Bob module that splits the incoming signal into two orthogonal polarization modes, each one of which is aligned to the electro-optical crystal axis of the PM at each output. Each of the two orthogonally polarized beams passes through an independent PM where an equal phase shift φ_B is introduced into both polarization components, giving for any small a [8]:

$$E = A' \cdot 10^{-\frac{\alpha L+\beta}{10}} e^{i\omega t} + iaA \cdot 10^{-\frac{\alpha L+\beta}{10}} \cdot \cos\left(\frac{\varphi_A - \varphi_B}{2}\right) \cdot \left(e^{i((\omega+\Omega)t+\frac{\varphi_A+\varphi_B}{2})} + e^{i((\omega-\Omega)t-\frac{\varphi_A+\varphi_B}{2})} \right) \quad (2)$$

where β are the losses in the Bob module, α is the optical fiber attenuation coefficient at the central wavelength of the photon source, L is the optical fiber length.

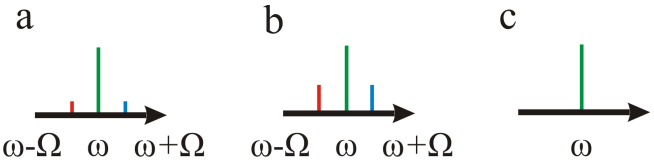

Fig. 2. Optical frequency spectra in the subcarrier wave quantum cryptography system after (a), Alice modulation; Bob modulation in case of (b) constructive; and (c) destructive interference. In each subfigure the green line represents the carrier while red and blue indicates the sub carriers.

Electro-optic modulators typically exhibit strong polarization dependence, hence in the Bob module we used a commercially available polarizing beamsplitter coupled with polarization-maintaining fibers in both output arms to route the light to each modulator. The orientation of the fibers at the two PBS outputs was rotated to match the linear polarization of the light in the fiber to the input of the electro-optic phase modulator. This step was required due to the polarization dependence of the phase shift introduced by electro-optical modulator. The approach outlined here is an alternative to that suggested earlier in [8], which employed $LiNbO_3$ Mach-Zehnder amplitude modulators with the effective thickness in one of the arms modified by laser ablation to produce polarization insensitivity [25]. An advantage of this approach is that it introduces the possibility of using conventional off-the-shelf phase modulators in the SCW QKD system. The modulators in Bob operate the same way as those in Alice: both are driven by radio frequency signals with equal amplitude, frequency and phase. The frequency and amplitude of the driving signal are selected so that the responses of Bob's modulators were equal to that of Alice's modulator. No thermal stabilization of the optical components used in this polarization compensation scheme was required, since phase information is equal in both arms (defined by φ_A and φ_B), and the signals must simply arrive at the detector at the same time interval defined by clock frequency (~10 ns).

The optical signals from modulators were then combined in a polarizing beam combiner (PBC). Afterwards, they were transmitted through a circulator to an optical spectral filter that separates the carrier from the subcarriers and transmits a component with frequency $\omega + \Omega$ or $\omega - \Omega$ that is detected by a single-photon detector which, in this case, was an SNSPD. The reflected carrier followed another arm of the circulator and was then directed to the second optical channel of the same SNSPD. In this manner, the carrier and subcarriers were time-

#254859 Received 3 Dec 2015; revised 27 Jan 2016; accepted 27 Jan 2016; published 2 Feb 2016

division multiplexed and could be identified and de-multiplexed in the electrical signal from the SNSPD by examining certain time windows. Monitoring the light at the central frequency is critical to the security analysis and will be explained and analyzed in the next section. The SNSPD was used because of its low dark count rate of only several counts per second [16] at detection efficiencies in the region of 10-20%. This detector performance levels permit long-distance QKD even at relatively low clock rates, such as the one used in our system. In addition, SNSPDs are characterized by low dead time (~30 ns) and jitter (~100 ps) [26], features which can be exploited in high-bandwidth multiplexed QKD networks, where a single SNSPD combined with time multiplexing techniques can be efficiently used instead of an array of detectors. However, SNSPDs must be operated at low temperatures (~2.7 K), typically in relatively complex closed cycle cooler systems [16]. Future systems may deploy InGaAs/InP single-photon avalanche diode (SPAD) detectors which have recently been used in high performance QKD systems [27,28]. These detectors have the potential to operate at higher temperatures (~150 K) [27,28], offering the prospect of operation with the next generation of thermoelectric coolers [29].

The resulting power of the subcarrier wave depends on the values of φ_A and φ_B. In the case that Alice and Bob introduced equal phase shifts ($\varphi_A - \varphi_B = 0$), constructive interference was observed in the side frequency optical signal, and the optical signal power differed from zero at the sidebands, as shown in Fig. 2(b). On the contrary, when the difference in phase shifts is a multiple of π, destructive interference (Fig. 2(c)) was observed, and the detected counts of the subcarrier waves corresponded predominantly to dark noise in the detector. Secure key generation can be therefore performed using two or four state phase protocols as discussed in [8,11]. In this system both Alice and Bob control their systems by using FPGA devices. Alice and Bob independently record information corresponding to the phase shifts introduced at each time instance, regulated by a signal from the clock synchronization. Bob also registers the SNSPD signals at each time interval as well as their relative arrival times on the coincidence circuit, indicating the reception or absence of photon interference and the signal at central frequency. As can be seen from Fig. 3, high signal levels on the SNSPD correspond to a matching phase of modulating electrical signals $\varphi_A - \varphi_B = 0$, the case shown in Fig. 2(b).

After the detection process, the information from the detector is sent to Alice though an Ethernet connection, which the two parties use as the open classical channel for post-processing. The bits corresponding to these selected time instances are uploaded to the operators' computers from the FPGA, while the rest are discarded. All subsequent operations with the key, including sifting, privacy amplification and message encoding are performed by using the computers with software that is external to the FPGA.

Synchronization of the Alice and Bob modules is implemented in a separate optical fiber to prevent the relatively intense classical synchronization signal introducing noise photons to the quantum signal due to Raman scattering and other effects [4]. Even though efforts can be made to reduce the effects for moderate distances [4], previous work [23,28] has shown that at high optical channel losses, such as those experienced in this experiment, optical synchronization in the same channel as the quantum transmission is not practical due to increased errors caused by Raman scattering effects and the increased complexity of the system. Moreover, increasing the spectral spacing between the quantum and synchronization channels in a single fiber would require employing a shorter wavelength for the quantum signal in order to minimize the nonlinear effects [4,30] and such an approach would therefore greatly reduce the maximum key distribution distance due to higher per unit distance losses [19]. The optical pulse at the central frequency was not used as a reference since it must be maintained at a low energy level for effective filtration in the current setup, as discussed in section 4.

#254859 Received 3 Dec 2015; revised 27 Jan 2016; accepted 27 Jan 2016; published 2 Feb 2016

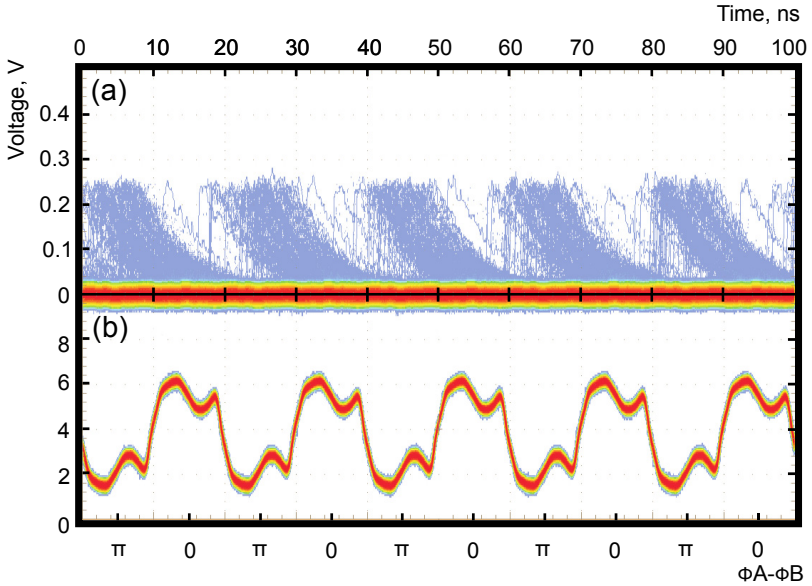

Fig. 3. Oscillogram of registered change of SNSPD response (a) based on relative phase introduced by Alice and Bob (b). An increase in number of optical counts per time interval due to constructive interference on sidebands corresponds to additive summation of electrical driving signals. It can be seen by comparing (a) and (b) that time periods with a high number of returns in (a) correspond to a low voltage in (b).

A second laser in Alice (Laser Diode 2) generated a sinusoidal signal with frequency defined by the VCO generator (10 MHz). The optical signal was also modulated by a signal from a FPGA to form a reference peak every 60 ms. In the Bob module the optical signal is detected on a photodetector. The output electrical signal is then filtered: the sinusoidal component is directed to the input of the VCO and used for clock generator frequency adjustments to ensure phase locking between Alice and Bob, while the modulated peak component introduced by the FPGA is interpreted by Bob's electronics as "start" and "refresh" commands. The latter commands periodically reset the lookup tables that establish relations between the electrical driving signal parameters in Bob's modulator and the respective induced phase shifts φ_B. This calibration procedure is performed in order to compensate the internal temporal phase drift of modulator driving signals and to ensure phase locking at Bob of the synchronization and secure channels, which propagate in separate fibers and are therefore subject to different environmentally induced changes in parameters.

3. Experimental results

The quantum channel photon source was a distributed feedback (DFB) laser with 1550.12 nm central wavelength and frequency linewidth 5 kHz full-width at half-maximum, which was operated in continuous wave mode. A stable laser with a narrow linewidth was used due to availability; in practice the requirements for the source are less strict in terms of modulation frequency and filter bandwidth. The average optical power at Alice's modulator input was 10 mW. The experiments were performed with a clock rate of 10 MHz, phase change frequency f = 100 MHz, and modulation frequency Ω = 4.2 GHz. The modulation frequency was chosen as the maximum possible in order to comply with the optical filter rejection bandwidth of 7.5 GHz. The modulation index a was chosen to be 0.01. The total optical power at the output of Alice was 257 pW, corresponding to μ = 1 photons in both sidebands in total in the quantum channel.

The PBS situated in the Bob module input introduced a loss of 0.55 dB. Travelling wave $LiNbO_3$ modulators were employed, which had 3 dB loss for signal modulation in both arms.

#254859 Received 3 Dec 2015; revised 27 Jan 2016; accepted 27 Jan 2016; published 2 Feb 2016

The modulated signal components were then transmitted through a fiber optic beam combiner based on fused bi-conical tapers (0.55 dB loss) to a spectral filter based on a fiber Bragg grating with passive thermal stabilization, which had a reflection coefficient of 99.99% in a 7.5 GHz band and introduced 1 dB losses. Optical connections in the Bob module introduced an additional 1.3 dB loss. The circulator introduced 0.5 dB losses in each arm. Overall, the total losses in Bob were 6.9 dB for the sideband signals and 7.4 dB for the carrier wave. The filtered signal of the sideband was incident on a single photon detector operating in asynchronous mode. A NbN meander nanowire superconductor single photon detector was used in these experiments, and was cooled to ~2.7 K by liquid helium in a closed cycle unit [16]. At a wavelength of 1550 nm, the single-photon detection efficiency was 20% with a dark count rate of less than 10 counts per second. The quantum channel was composed of 50, 100, 125 or 150 km of Corning SMF-28e + optical fiber with loss 0.2 dB/km at the central wavelength [19]. Additional measurements were performed in a channel with variable attenuation comprised of 50 km of Corning SMF-28e + fiber (corresponding to a measured loss of 10 dB) with additional calibrated loss provided via an optical attenuator. The parallel optical synchronization channel was configured to exhibit the same loss as the quantum channel, to simulate the same transmission distance for both channels. The electronic control units in the transmitter and receiver modules were synchronized by a sinusoidal waveform signal at 10 MHz (clock) frequency. Raw key generation and basis set sifting was performed experimentally using the BB84 protocol. A phase shift introduced into the modulating signal was chosen by Alice from four possible phase-states contained in two conjugate bases each comprising two states ({0, π} and {π/2, 3π/2}) to represent the binary 0 (phases 0, π/2) and binary 1 (π, 3π/2) levels. The selection of which of the two phase states represented a given binary level was made randomly. Bob randomly and independently selected one of the two conjugate bases to perform a measurement in. An exchange of information required for post-processing was performed through the open classical channel. During sifting, half of the bit sequence was discarded due to the wrong basis choice and then a further half of the remainder for a probability of photons returning to the carrier due to phase modulation with phase difference $\varphi_A - \varphi_B = \pi$ (Fig. 2(c)). The results are presented in Fig. 6. Calculation of secure key rate will be explained in the next section.

Figure 4 shows experimental measurements of QBER as a function of channel loss by measuring error rates in distributed sifted keys. In order to compare these with theoretical predictions, the following formula was used to predict the QBER in the system:

$$QBER = \frac{1-V}{2} + \frac{p}{4\mu\eta \cdot 10^{\frac{-\alpha L-\beta}{10}}} \tag{3}$$

where V is interference pattern visibility, β the losses in the Bob module, p is the dark count probability per bit, α is the optical fiber attenuation coefficient at the central wavelength of the photon source, L is the optical fiber length and η is the detection efficiency. The first term depends on the quality of optical phase matching in the Alice and Bob modules and is responsible for incorrect photon registration due to imperfect interference or depolarization. The second term characterizes the dark count as a fraction of all the registered counts. This increases with distance, since the number of photons reaching the detector decreases as transmission loss grows, whilst the dark count rate remains unchanged. The factor of four is introduced because the photons have a probability of one half of being in the correct basis and a probability of one half of returning from sidebands to the carrier (Fig. 2(c)).

#254859 Received 3 Dec 2015; revised 27 Jan 2016; accepted 27 Jan 2016; published 2 Feb 2016

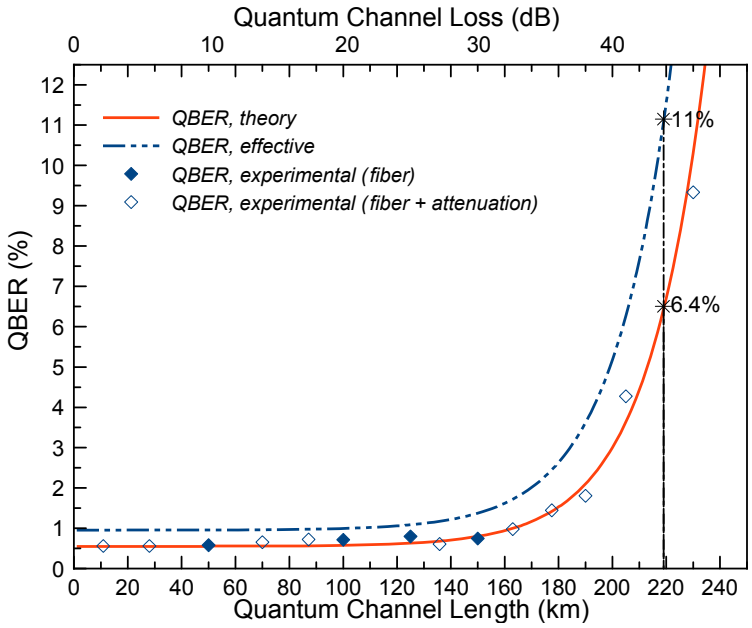

Fig. 4. QBER versus quantum channel length for experimental results and model. Measurements in optical fiber shown with filled markers, and unfilled markers denote those conducted using the combination of optical fiber and additional calibrated attenuation. "QBER, effective" denotes the BB84 protocol with strong reference.

The temporal stability of QBER was investigated experimentally during normal system operation. This was achieved due to a high visibility ($V > 98.9\%$), conditioned by the precise control of relative phase shifts, a high phase change frequency (due to the unidirectionality of Bob's apparatus) and low dark count rate of the detector. Figure 5 shows the QBER recorded every 650 ms over a 50 minute period with a channel loss of 5 dB. The slight fluctuations observed are related to spontaneous changes in signal visibility caused by minor inequalities in phase matching of transmitter and receiver modulating signals. For this visibility and channel loss the theory, which does not take into account these fluctuations, predicts a constant QBER of 0.55% while the results shown in Fig. 5 have a mean QBER of 0.67% and a standard deviation of 0.089.

Figure 6 shows the experimentally measured raw and sifted key rates against channel loss. As shown in Fig. 6, at the maximum measured loss of 42 dB (corresponding to 210 km fiber) the sifted key rate is around 60 bit/s with QBER value less than 5% (see Fig. 4), which would normally allow for generation of secure keys in QKD systems using the BB84 protocol [18]. However, in our current setup the distribution distance is also limited by detection of the strong reference in order to maintain the security against photon number splitting (PNS) attack, as discussed below. Therefore, in this experimental demonstration, usable secure operation is limited to less than 150 km (as indicated by the "Low intensity reference" line on Fig. 7). Operation at ranges greater than 150 km will be discussed in the next section.

#254859 Received 3 Dec 2015; revised 27 Jan 2016; accepted 27 Jan 2016; published 2 Feb 2016

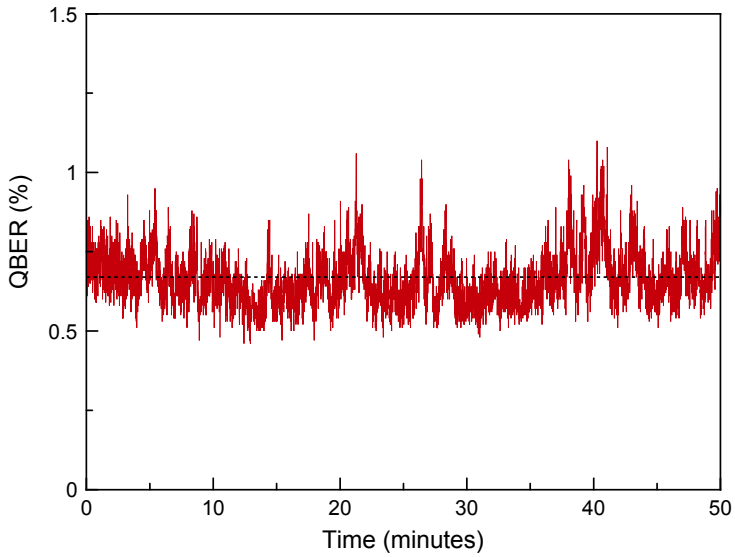

Fig. 5. The temporal fluctuations of the QBER in time monitored every 650 ms with a channel loss of 5 dB in the course of normal system operation. The dashed line indicates the mean value of the QBER for the illustrated period.

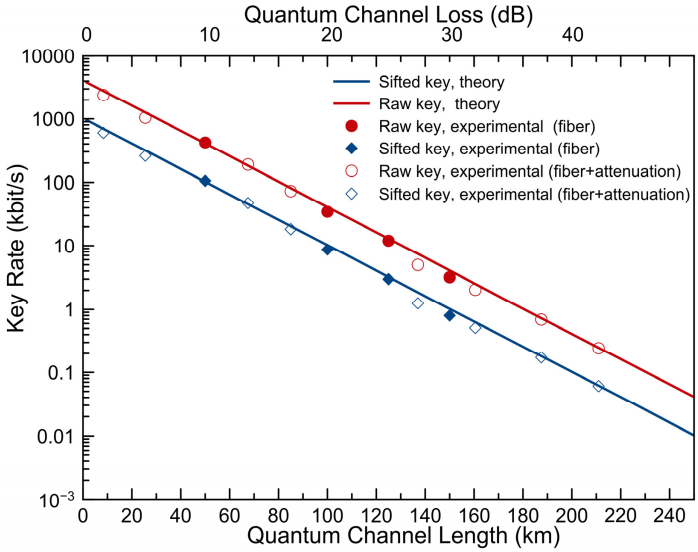

Fig. 6. Raw and sifted key rate values in SCW QKD system. Measurements in optical fiber shown with filled markers while unfilled markers denote those conducted using the combination of optical fiber and additional attenuation.

4. Security discussion

The optical emission from a faint laser source, such as the one used in this work, differs from a perfect single photon source [31], and will follow Poisson statistics. This means there is always a finite probability that multiphoton signal pulses are generated in the quantum channel. For such systems, the photon number splitting (PNS) attack is known to be the most effective eavesdropping strategy [18]. Under a PNS attack Eve identifies and blocks single-photon pulses from reaching Bob while extracting information from multiphoton signal

#254859 Received 3 Dec 2015; revised 27 Jan 2016; accepted 27 Jan 2016; published 2 Feb 2016

pulses, then resends the remaining fraction of the multiphoton signal pulse to Bob via a lossless channel. A combination of these strategies allows Eve to determine a significant fraction of the key and stay undetected at the same time, because Bob cannot distinguish between signal loss caused by high attenuation in the quantum channel and loss introduced by Eve blocking pulses. Eve must carefully match the fraction of the total number of pulses blocked to ensure she emulates the loss expected from the original attenuated quantum channel and furthermore ensure that the overall photon number distribution is not altered in a detectable manner.

The SCW method of generating the quantum channel is flexible in terms of quantum state preparation and allows one to utilize different QKD protocols that are secure against PNS attack, depending on chosen modulation parameters. One option is to use the BB84 protocol with a strong reference [21,22,24]. As shown in [22], Eve can be prevented from blocking pulses while exploiting a PNS if a strong reference is included in the transmission on the quantum channel and monitored by Bob. This condition is naturally satisfied in SCW systems, since the bright multiphoton signal at the central frequency is mixed with the lower intensity sidebands on the quantum channel and can be therefore used as a reference. One eavesdropping attack is for Eve could try to interrogate the spectrally separated carrier and quantum channels and modify each individually, however this approach would not compromise the security of the protocol. Indeed, if Eve tries to substitute Alice's information with her own photons on the subcarriers and recombine them with the original central wave, she would inevitably introduce 25% of phase errors, similar to the case of the Intercept-Resend attack [18]. On the other hand, if she suppresses the signal on the sidebands while forwarding the carrier to Bob, it will still increase the QBER, because the detection statistics of photons generated by modulation in the receiver module differ from the original. It can be shown that it is also not possible for Eve to generate her own reference signal without introducing this residual error [22], because in this case she must ensure that all initial signals with exactly one photon are removed during sifting, which is impossible, because Bob's choice of measurement phase is not known to her *a priori*.

Even though under these conditions Eve can no longer block pulses without being discovered, the information in multiphoton pulses is still available to her. Therefore, a privacy amplification procedure must be performed on the raw detector click events to extract the secret fraction attributable to pulses containing only one photon. The fraction of information that Eve can extract from multiphoton pulses is given by:

$$I_E = \frac{1-(1+\mu)e^{-\mu}}{1-e^{-\mu}} \tag{4}$$

This leads to a parameter $\Delta = 1 - I_E$, which describes the key fraction not known to Eve. As noted above, the PNS attack does not have to be considered and so the channel loss is not included in this analysis. It can be shown that I_E is minimized for $\mu = 1$, when $\Delta = 58\%$ (assuming no loss and errors). Such a high mean photon number was recently reported in several experimental implementations of SCW with the strong reference protocol [13,14]. The possibility of Eve's attack on the remaining bits utilizing the non-zero QBER to mask operations must be considered. In the worst case she can selectively attack only single photon pulses and perform PNS on multiphoton ones, effectively increasing the QBER by Δ^{-1} [22,24]. This leads to the conclusion that the maximum QBER for key distribution secure against both PNS and collective attacks has a value of 6.4% for the chosen protocol, as seen in Fig. 4. Therefore, for a given QBER value Q and sifted key rate F, the upper limit for secure key rate F_s after error correction and privacy amplification can be obtained by [14,24]:

$$F_s = F \cdot (\Delta \cdot (1 - h(Q/\Delta)) - h(Q)) \tag{5}$$

where $h(x)$ is the binary entropy function:

#254859 Received 3 Dec 2015; revised 27 Jan 2016; accepted 27 Jan 2016; published 2 Feb 2016

$$h(x) = -x \cdot \log_2(x) - (1-x) \cdot \log_2(1-x) \quad (6)$$

In practice a scaling factor for h must be taken into consideration due to the necessity of classical error correction [18]. The value of the scaling factor varies with the error correction protocol employed but is typically taken as 1.08 for the Cascade protocol which closely approaches the ideal unity value for the Shannon limit [32].

The main issue one has to address when using the strong reference approach is that one must always detect the carrier wave to satisfy the protocol conditions – the carrier wave fulfils the role of strong classical reference pulse. Another detector must be added to the setup in order to collect the light reflected from the optical filter (see Fig. 1) and the power of the carrier signal must remain sufficient to be detected at the Bob module without amplification. Another possibility is to register the presence of the strong reference by a using a single photon detector. Once again, two options are available: the parties can either add bits to the key only at instances when both the signal on sidebands and the carrier are detected, or monitor the joint probability of detection between the reference and the side signals to ensure it remains independent. In order to perform a model experiment, the light reflected from the filter was directed through a circulator to the second optical port of the SNSPD. The coincidence circuit connected to both electrical outputs of the SNSPD recorded the time instances when counts were received from each of the detector channels, and analyzed their time correlations. The efficiency of such method can be estimated as follows. For a μ value of 1 and modulation index 0.01 the power on the central wavelength at Alice corresponds to mean photon number at the carrier $n \sim 100$ photons. It is reasonable to calculate the carrier detection efficiency for any small value of n as $\eta_n = 1-(1-\eta)^n$. After considering the carrier photon number decay due to losses, the effective secure key rate can be estimated by multiplying the secure key rate from (5) by η_n. This results in experimentally measured secure key rates of 16.5 kbit/s at 50 km, 195 bit/s at 100 km and 1.5 bit/s at 150 km, limiting the maximum channel loss for secure generation to 30 dB. The experimental data received by processing the obtained sifted key rates (Fig. 6) using formula (5) and $n = 100$, confirms these conclusions ("Low intensity reference" on Fig. 7). Therefore, in our system, the high channel loss places challenging limitations on the secure operation at distances over 150 km. However, for medium distances (e.g. 50 km) the bitrate is sufficient for establishing a communication link without any change in architecture.

It can be seen from Fig. 7 that the probability of carrier detection quickly decays with distance and acts as the major limiting factor for SCW QKD performance. A straightforward way of overcoming this obstacle for long-distance secure communication is to increase the photon number n (i.e. optical power) on the carrier and proportionally lower the modulation index in order to keep μ constant. Assuming $\eta_n \sim 1$, then for a 42 dB (210 km) channel the initial carrier power at Alice should be about 10 μW. Since the power on the subcarriers should still remain at the single photon level, this raises the requirements for the optical filter, which must now have about 85 dB channel separation, instead of 40 dB as used in this work, to ensure low QBER. Even though such a filtration system was unavailable during the course of the experiments reported here, it can in principle be implemented in the future. Therefore, the secure key rate would reach the theoretical limit for the strong reference protocol: according to computation results, in this case the secret key rate at the maximum distance of 214 km is 1.3 bit/s (indicated by the "Strong reference" line on Fig. 7).

Another way of establishing unconditional security in the SCW system is the implementation of decoy-states [20,33]. Following the analysis of Ma *et al.* [33], one can estimate the optimal mean photon number for signal states in a decoy state variant of this SCW QKD system as being $\mu = 0.82$ and it is this value we will use for our subsequent theoretical analysis of the decoy state approach. This relatively large value for the optimal μ is explained by the high visibility of our system and a low contribution from imprecise phase matching to QBER (only around 0.75%, see Fig. 5). This is due to the SCW architecture,

#254859 Received 3 Dec 2015; revised 27 Jan 2016; accepted 27 Jan 2016; published 2 Feb 2016

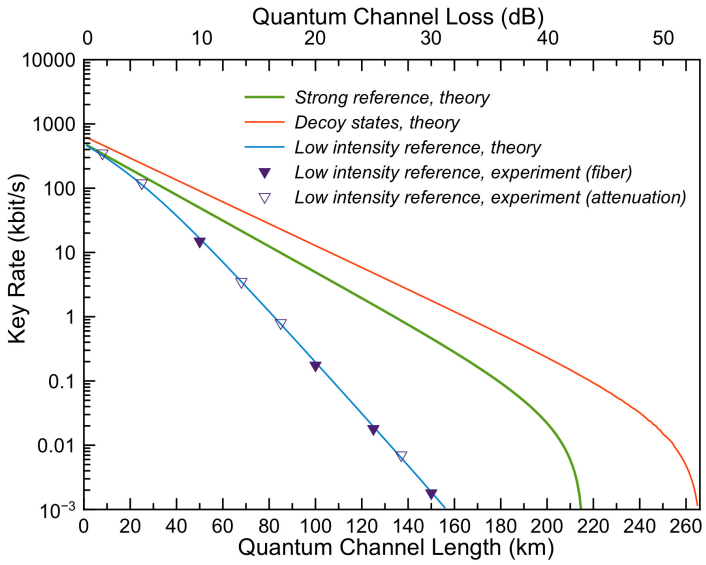

Fig. 7. Secure key exchange rates in SCW QKD system with different protocols

where phase control is simplified because it is performed for electrical signals, which have much lower frequencies than the optical ones. Theoretical results based on the parameters used in our system (see Table 1) are shown in Fig. 7. As can be seen, the decoy states method would offer higher bit rates over all transmission distances to an extended maximum transmission distance of 265 km (45 dB). However, implementation of decoy-states cannot be readily undertaken by varying the modulation index in our SCW system as this leads to a corresponding variation in the photon number of the central carrier wavelength which can be detected by the eavesdropper. An optimization technique to overcome this problem in a two-state SCW phase protocol has been suggested by Bhattacharya and Kumar [34] but no similar solution has yet been proposed for the four state BB84 protocol. The secure key rates presented on Fig. 7 do not consider any finite-key effects. According to the analysis from [35], in our implementation based on weak coherent pulses we can expect these results to be accurate when the raw key strings contain at least $N > 10^7$ bits.

Table 1. Parameters used in SCW QKD with decoy states simulation [33]

Parameter	Notation	Value
Signal single photon number	μ	0.82
Decoy state photon numbers	v1; v2	0.041; 0
Quantum efficiency, %	η	20
Dark count probability	Y0	10^{-7}
Detection error probability	e_{detector}	0.075
Fiber loss, dB/km	α	0.17
Clock frequency, Hz	F	10^8

5. Conclusions

In this work an experimental subcarrier wave modulation quantum key distribution (SCW QKD) with optical synchronization is presented. Secure quantum key distribution was demonstrated at a final secure key bit rate of 1.5 bit/s in an optical channel with 30 dB losses using the BB84 protocol with a strong reference. At the maximum loss, the quantum bit error rate did not exceed 0.8%. In comparison, 16.5 kbit/s secure key rate was possible with an error of 0.5% over an optical channel of 10 dB loss, and 18 bits/s with an error of 0.75% over 25 dB of channel loss. At short distances, the secure key rate reached 450 kbit/s with QBER

#254859 Received 3 Dec 2015; revised 27 Jan 2016; accepted 27 Jan 2016; published 2 Feb 2016

less than 0.6%. To the best of our knowledge, these results show the highest channel loss for secure subcarrier wave quantum cryptography systems. The secure fraction of the key is defined by the joint probability of detection of the quantum signal and the central frequency, which is monitored as a reference. Further improvement in secure bit rate can be achieved by raising the photon number at the carrier (which would require a more advanced optical filtration system) or implementing the decoy states technique. Indeed, as can be seen from Fig. 7 the theoretically predicted secure key rate in a 100 km link is around 20 kbit/s, the same order of magnitude as demonstrated in the presently longest reported quantum channel demonstrated in QKD [28]. These calculations show that a future improvement of the SCW QKD protocol performance would allow secure key distribution to distances beyond 200 km even without increasing the phase change frequency which governs quantum states preparation (e.g. in [28] it was set to 625 MHz compared to 100 MHz used in this work). The importance of these results is significant for several reasons. Firstly, SCW QKD systems with an unconditionally secure protocol are for the first time demonstrated to operate at high channel losses, in this case 30 dB in the optical line and 6.9 dB in the Bob module. This was achieved at a relatively low phase change frequency of 100 MHz, thus significantly simplifying the electronic subsystem and leaving significant potential for further bitrate improvement. Furthermore, even higher maximum losses can be achieved in the future by introducing the additional parties and organizing multi node "chain" quantum networks or integrating the SCW technology into measurement-device-independent QKD [36], which require some additional analysis. Secondly, the intrinsic properties of the SCW protocol as well as a one-pass polarization compensation scheme introduced in this work have made the system almost entirely insensitive to polarization changes in the quantum channel. This approach is an alternative to installing active polarization control elements [37] which require manual tuning and therefore are impractical for a deployed system.

SCW QKD systems possess great potential for signal multiplexing. Indeed, the approach is compatible with the method of generating multiple independent keys using the sidebands around a single carrier [12–14]. Combining these technologies with the results described in this paper could lead to a reliable and effective QKD system, especially in terms of efficiency of use of optical bandwidth, which can be increased for key distribution by more than an order of magnitude. For instance, today the most advanced QKD systems in terms of bitrate allow creation of keys at 1-2 Mbit/s for a link distance of 50 km [38,39]. Merging several such channels in one fiber by dense WDM with 100 GHz channel separation would result in only 2-4% spectral efficiency, as previously discussed in [13]. On the other hand, introducing broadband optical modulators (~50 GHz) into SCW systems can potentially improve the spectral efficiency up to some 50% of the optical bandwidth by using a large number of subcarriers with channel spacing of 1-2 GHz [13]. Overall, combining the results of this work with advances in SCW multiplexing techniques could make the subcarrier method an efficient and ultra-high bandwidth approach to quantum key distribution compatible with existing optical fiber infrastructure. It is entirely possible that such a system may also be applicable to adapted versions of recent protocols for quantum digital signatures [40,41] offering the prospect of multiplexed implementations of that emerging technology.

Acknowledgment

This work was financially supported by Government of Russian Federation, Grant 074-U01 and by the Ministry of Education and Science of Russian Federation (project Nº 14.578.21.0112).

#254859 Received 3 Dec 2015; revised 27 Jan 2016; accepted 27 Jan 2016; published 2 Feb 2016