Physical layer secret key generation for fiber-optical networks

Konstantin Kravtsov,[1,*] **Zhenxing Wang,**[2] **Wade Trappe,**[3] **and Paul R. Prucnal**[4]

[1]*A. M. Prokhorov General Physics Institute, Russian Academy of Sciences, Moscow, Russia*
[2]*Finisar Corporation, 200 Precision Road, Horsham PA, 19044 USA*
[3]*WINLAB, Rutgers University, North Brunswick NJ, 08902 USA*
[4]*Department of Electrical Engineering, Princeton University, Princeton NJ, 08544 USA*
[*] *kravtsov@kapella.gpi.ru*

Abstract: We propose and experimentally demonstrate a method for generating and sharing a secret key using phase fluctuations in fiber optical links. The obtained key can be readily used to support secure communication between the parties. The security of our approach is based on a fundamental asymmetry associated with the optical physical layer: the sophistication of tools needed by an eavesdropping adversary to subvert the key establishment is significantly greater and more costly than the complexity needed by the legitimate parties to implement the scheme. In this sense, the method is similar to the classical asymmetric algorithms (Diffie-Hellman, RSA, etc.)

OCIS codes: (060.4785) Optical security and encryption; (060.2330) Fiber optics communications; (060.4510) Optical communications.

References and links

1. S. Mathur, R. Miller, A. Varshavsky, W. Trappe, and N. Mandayam, "ProxiMate: proximity-based secure pairing using ambient wireless signals," in "MobiSys '11 Proceedings of the 9th international conference on Mobile systems, applications, and services," (2011), pp. 211–224.
2. K. Ren, H. Su, and Q. Wang, "Secret key generation exploiting channel characteristics in wireless communications," IEEE Wireless Communications **18**, 6–12 (2011).
3. W. Wells, R. Stone, and E. Miles, "Secure communications by optical homodyne," IEEE J. Sel. Areas Commun. **11**, 770–777 (1993).
4. J. Menders, C. Diamond, and E. Miles, "Interferometric generation of random binary keys for secure optical communication," Proc. SPIE **4471**, 208–213 (2001).
5. W. Wells, J. Menders, E. Miles, B. Loginov, and H. Hodara, "Another alternative to quantum cryptography," Quant. Inform. Processing **1**, 91–106 (2002).
6. H. Hodara, E. Miles, J. Menders, and W. Wells, "Secure fiberoptic communications," Fiber and Integrated Optics **22**, 47–61 (2003).
7. M. P. Fok, Z. Wang, Y. Deng, and P. R. Prucnal, "Optical layer security in fiber-optic networks," IEEE Trans. Inf. Forensics Security **6**, 725–736 (2011).
8. B. B. Wu and E. E. Narimanov, "A method for secure communications over a public fiber-optical network," Opt. Express **14**, 3738–3751 (2006).
9. K. Kravtsov, B. Wu, I. Glesk, P. R. Prucnal, and E. Narimanov, "Stealth transmission over a WDM network with detection based on an all-optical thresholder," in "Proc. of LEOS 2007," (Lake Buena Vista, FL USA, 2007).
10. S. Goldberg, R. Menendez, and P. Prucnal, "Towards a cryptanalysis of spectral-phase encoded optical CDMA with phase-scrambling," in "Proc. of OFC/NFOEC 2007 OThJ7," (Anaheim, CA USA, 2007), pp. 1–3.
11. O. Hirota, K. Katob, M. Shomac, and T. S. Usuda, "Quantum key distribution with unconditional security for all optical fiber network," Proc. SPIE **5161**, 320–331 (2004).
12. E. Corndorf, C. Liang, G. S. Kanter, P. Kumar, and H. P. Yuen, "Quantum-noise randomized data encryption for wavelength-division-multiplexed fiber-optic networks," Phys. Rev. A **71**, 062326 (2005).

#191857 - $15.00 USD Received 14 Jun 2013; revised 15 Sep 2013; accepted 17 Sep 2013; published 30 Sep 2013

13. I. Glesk, Y.-K. Huang, C. S. Brès, and P. R. Prucnal, "Design and demonstration of a novel optical CDMA platform for use in avionics applications," Opt. Commun. **271**, 65–70 (2007).
14. K.-I. Kitayama, M. Sasaki, S. Araki, M. Tsubokawa, A. Tomita, K. Inoue, K. Harasawa, Y. Nagasako, and A. Takada, "Security in photonic networks: Threats and security enhancement," J. Lightwav. Technol. **29**, 3210–3222 (2011).
15. P.-L. Liu, "A key agreement protocol using band-limited random signals and feedback," J. Lightwav. Technol. **27**, 5230–5234 (2009).
16. P.-L. Liu, "Key exchange using random signals and feedback-statistical analysis," J. Lightwav. Technol. **28**, 65–70 (2010).
17. L. L. Kish, B. Zhang, and L. B. Kish, "Cracking the Liu key exchange protocol in its most secure state with lorentzian spectra," Fluct. and noise lett. **9**, 37–45 (2010).
18. J. Scheuer and A. Yariv, "Giant fiber lasers: A new paradigm for secure key distribution," Phys. Rev. Lett. **97**, 140502 (2006).
19. A. Zadok, J. Scheuer, J. Sendowski, and A. Yariv, "Secure key generation using an ultra-long fiber laser: transient analysis and experiment," Opt. Express **16**, 16680–16690 (2008).
20. D. Bar-Lev and J. Scheuer, "Enhanced key-establishing rates and efficiencies in fiber laser key distribution systems," Phys. Lett. A **373**, 4287–4296 (2009).
21. P. LeCong, "Secure communication system," U.S. Patent (Mar. 2, 1993).
22. E. Udd, "Secure fiber optic communication system based on the Sagnac interferometer," Proc. SPIE **2837**, 172–176 (1996).
23. G. Grosche, O. Terra, K. Predehl, R. Holzwarth, B. Lipphardt, F. Vogt, U. Sterr, and H. Schnatz, "Optical frequency transfer via 146 km fiber link with 10^{-19} relative accuracy," Opt. Lett. **34**, 2270–2272 (2009).
24. M. Amemiya, M. Imae, Y. Fujii, T. Suzuyama, F.-L. Hong, and M. Takamoto, "Precise frequency comparison system using bidirectional optical amplifiers," IEEE Trans. Instr. Meas. **59**, 631–640 (2010).
25. L.-S. Ma, P. Jungner, J. Ye, and J. L. Hall, "Delivering the same optical frequency at two places: accurate cancellation of phase noise introduced by an optical fiber or other time-varying path," Opt. Lett. **19**, 1777–1779 (1994).
26. S. M. Foreman, A. D. Ludlow, M. H. G. de Miranda, J. E. Stalnaker, S. A. Diddams, and J. Ye, "Coherent optical phase transfer over a 32-km fiber with 1 s instability at 10^{-17}," Phys. Rev. Lett. **99**, 153601 (2007).
27. P. A. Williams, W. C. Swann, and N. R. Newbury, "High-stability transfer of an optical frequency over long fiber-optic links," J. Opt. Soc. Am. B **25**, 1284–1293 (2008).
28. S.-B. Cho and T.-G. Noh, "Stabilization of a long-armed fiber-optic single-photon interferometer," Opt. Express **17**, 19027–19032 (2009).
29. G. B. Xavier and J. P. von der Weid, "Stable single-photon interference in a 1 km fiber-optic Mach-Zehnder interferometer with continuous phase adjustment," Opt. Lett. **36**, 1764–1766 (2011).
30. G. Xavier, T. da Silva, G. Tempora, and J. von der Weid, "Polarisation drift compensation in 8 km-long Mach-Zehnder fibre-optical interferometer for quantum communication," Electron. Lett **47**, 608–609 (2011).
31. J. Minář, H. de Riedmatten, C. Simon, H. Zbinden, and N. Gisin, "Phase-noise measurements in long-fiber interferometers for quantum-repeater applications," Phys. Rev. A **77**, 052325 (2008).
32. A.-S. Babak, K. Aggelos, M. Alejandra, and Y. Bulent, "Robust key generation from signal envelopes in wireless networks," in "CCS '07 Proceedings of the 14th ACM conference on Computer and communications security," (2007), pp. 401–410.
33. I. Coddington, W. C. Swann, L. Lorini, J. C. Bergquist, Y. L. Coq, C. W. Oates, Q. Quraishi, K. S. Feder, J. W. Nicholson, P. S. Westbrook, S. A. Diddams, and N. R. Newbury, "Coherent optical link over hundreds of metres and hundreds of terahertz with subfemtosecond timing jitter," Nature Photon. **1**, 283 – 287 (2007).
34. S. M. Foreman, K. W. Holman, D. D. Hudson, D. J. Jones, and J. Ye, "Remote transfer of ultrastable frequency references via fiber networks," Rev. Sci. Instrum. **78**, 021101 (2007).
35. C.-H. F. Fung, B. Qi, K. Tamaki, and H.-K. Lo, "Phase-remapping attack in practical quantum-key-distribution systems," Phys. Rev. A **75**, 032314 (2007).
36. Y. Zhao, C.-H. F. Fung, B. Qi, C. Chen, and H.-K. Lo, "Quantum hacking: Experimental demonstration of time-shift attack against practical quantum-key-distribution systems," Phys. Rev. A **78**, 042333 (2008).
37. F. Xu, B. Qi, and H.-K. Lo, "Experimental demonstration of phase-remapping attack in a practical quantum key distribution system," New J. Phys. **12**, 113026 (2010).
38. L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, "Hacking commercial quantum cryptography systems by tailored bright illumination," Nature Photon. **4**, 686–689 (2010).
39. N. Patwari, J. Croft, S. Jana, and S. K. Kasera, "High-rate uncorrelated bit extraction for shared secret key generation from channel measurements," IEEE Trans. Mobile Computing **9**, 17–30 (2010).
40. C. Ye, S. Mathur, A. Reznik, Y. Shah, W. Trappe, and N. B. Mandayam, "Information-theoretically secret key generation for fading wireless channels," IEEE Trans. Inf. Forensics Security **5**, 240–254 (2010).
41. G. Brassard and L. Salvail, "Secret-key reconciliation by public discussion," in "EUROCRYPT '93: Workshop on the theory and application of cryptographic techniques on Advances in cryptology," (Secaucus, NJ, USA, 1994), pp. 410–423.

#191857 - $15.00 USD Received 14 Jun 2013; revised 15 Sep 2013; accepted 17 Sep 2013; published 30 Sep 2013

42. A. M. Fraser and H. L. Swinney, "Independent coordinates or strange attractors from mutual information," Phys. Rev. A **33**, 1134–1140 (1986).
43. A. Kraskov, H. Stögbauer, and P. Grassberger, "Estimating mutual information," Phys. Rev. E **69**, 066138 (2004).
44. M. Sasaki, M. Fujiwara, H. Ishizuka, *at al.*, "Field test of quantum key distribution in the Tokyo QKD Network," Opt. Express **19**, 10387 (2011).

1. Introduction

Secret key distribution has always been a challenging problem in secure communications. Today the most adopted key distribution methods are based on asymmetric, or public-key, cryptography. Key establishment schemes, such as Diffie-Hellman, and public key algorithms like RSA, are only as secure as the supposed intractability of their underlying algorithms, and recent advancements in quantum computing algorithms, such as Shor's algorithm, threaten to undermine the future utility of public key schemes. The only solid alternative known today is quantum cryptography, which provides unconditional security. However, in most cases it is a very expensive solution suitable only for the most critical applications and thus the development of simple, cheap and efficient methods of key distribution is a high priority.

One promising approach for secret key establishment is to exploit the properties of the underlying physical layer communications to arrive at secret keys. Physical layer secret key establishment has been successfully demonstrated in the wireless domain [1, 2], where the channel reciprocity properties of the wireless fading channel provide the basis for key establishment. These approaches are not applicable to large metro and long-haul networks, where the transmission medium is necessarily an optical fiber. The physical layer underlying optical communications is dramatically different than in wireless communications, and thus devising physical layer secret key establishment for optical networks requires a different approach.

The history of secure fiber-optic communications is quite rich. There are dozens of papers addressing the subject using different approaches. However, most of them, as will be discussed later, use naive assumptions that an adversary does not know a secret parameter or a code, used by the legitimate users; or even the assumption that Eve cannot implement a "complicated" method of data extraction used in the system. Further, these methods do not exploit any asymmetries associated with the physical layer itself.

We present a secret key establishment scheme for optical communications that utilizes the properties of the optical physical layer. Specifically, our approach is based on monitoring phase fluctuations within the fiber optical medium and works under the assumption that the adversary knows all possible information about the system even while it is working. The approach is 'asymmetric', which means that an implementation of an eavesdropping system (which is discussed later in the paper) is significantly more complicated and costly than building the system itself. Having these two properties combined in the same system makes it advantageous with respect to previous approaches and efficient in terms of amount of work that legitimate parties must use in order to impose serious complications for an eavesdropping adversary.

1.1. Method overview

The proposed method of key distribution is built on the idea of a large-scale interferometer that detects phase fluctuations in the fiber links between the communicating parties. The simplest realization of the method is shown in Fig. 1, where Alice and Bob are the terminals of a large Mach-Zehnder interferometer. The observed output signal is the result of interference of the two optical fields $\frac{1}{2}E_0e^{i(\omega t+\varphi_1)}$ and $\frac{1}{2}E_0e^{i(\omega t+\varphi_2)}$ coming from the interferometer arms, where E_0 is the launched optical field amplitude, ω — angular light frequency, and $\varphi_{1,2}$ — total phase

#191857 - $15.00 USD Received 14 Jun 2013; revised 15 Sep 2013; accepted 17 Sep 2013; published 30 Sep 2013

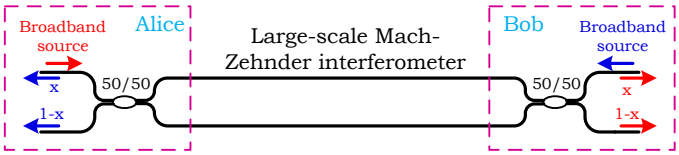

Fig. 1. Scheme of the proposed key sharing method.

shifts in the two arms of the interferometer. The effective splitting coefficient x is given by

$$x = \frac{\left|\frac{1}{2}E_0 e^{i\varphi_1} + \frac{1}{2}E_0 e^{i\varphi_2}\right|^2}{E_0^2} = \frac{1+\cos(\varphi_1-\varphi_2)}{2} = \frac{1+\cos\Delta\varphi}{2}.$$

It only depends on the relative phase shift $\Delta\varphi$ between the arms, and is the same for both directions of propagation. Since the phase in a long interferometer constantly fluctuates, the coefficient x is a function of time. Thus measuring the same function $x(t)$, Alice and Bob have shared *common randomness* that can be used to generate identical secret keys.

The interferometer is fed with a broadband light source from both sides to prevent direct phase tracking in both arms by the adversary Eve. Moreover, since phase fluctuations are spread across the full length of both fibers, Eve cannot substitute a part of the interferometer with her own setup. Instead, to conduct an attack she would require knowing the full characterization of the entire interferometer. The use of such a vast chaotic system as a fiber link places many restrictions on the potential strategies that Eve can use to eavesdrop, and we discuss this in detail in the security analysis section below.

1.2. Previous approaches to securing classical optical communications

In spite of popular belief, even in the early days of optical communications it was clear that an optical fiber did not provide physical protection from eavesdropping. Although tapping a fiber optic cable is a more complicated task that tapping an electrical wire [3], several methods of doing this were discovered, including the leaking of light when the fiber is bent, making a directional coupler by fusing with another fiber, the etching of silica cladding to expose the core, etc. Consequently, a standard assumption for all optical communication security models has been that the adversary has access to the transmitted signals, and thus the transmission should be secured by means other than relying on the physical sanctity of the medium.

Initially, several efforts to make transmissions more protected involved avoiding on-off keying modulation, where all data is clearly visible. The use of phase modulation, carrier-hopping or other techniques, where the intensity of the carrier remains constant also does not provide additional protection, since the same type of demodulator and detector used by the receiver can also be used by the adversary. This led to a substantial interest in making detectors parametrized by a secret code/feature, for which is it not possible to recover data without that code.

One of the first implementations of this technique [3–6] used a phase modulated broadband signal with homodyne detection. Without knowing the path difference in the imbalanced interferometer used, it is impossible to recover the data. Later approaches used more sophisticated modulators/demodulators, including the use of a secret optical CDMA code ([7] and references therein). A combination of this "secret parameter" approach with stealth signal transmission in the background of a conventional data stream, resulted in a number of steganographic methods used for improving data privacy at the physical layer [8,9]. Some methods involve a secret channel scrambler [10] or code scrambler [7] that makes the transmission virtually undetectable unless the same de-scrambler is used.

#191857 - $15.00 USD Received 14 Jun 2013; revised 15 Sep 2013; accepted 17 Sep 2013; published 30 Sep 2013

An interesting approach was proposed in 2000, where it is claimed that if Bob and Eve have statistically independent noise in their measurements, then there exist a secure key expansion protocol [11]. Realization of this protocol, usually called Y-00, can deliver very high data encryption rates up to Gb/s range [12]. It, however, also requires a pre-shared secret key, which is later expanded via pseudorandom bit generation. Therefore this method belongs to the class of "secret code" techniques, which are applicable only under special circumstances where pre-shared secrets exist.

However, all these "secret parameter" or "secret code" methods should be used with caution since a powerful adversary can learn the required settings of the decoder and use them for eavesdropping. The problem is particularly serious since, if the "secret code" is fixed, it eventually can be guessed or deduced by the adversary, and there has been an abundance of approaches developed to infer such secret codes. However, if the codes change with time, then the question arises as to how to secretly distribute the codes between the parties. The ultimate solution here, one-time pad encryption (see e.g. [13]), involves encrypting every bit with its own key stream bit, but this only turns the initial problem into another classical security problem– that of key distribution. In short, in order to achieve security one must assume a prior security problem has been solved. More information about some methods mentioned can be found in comprehensive reviews [7, 14].

In virtually all of the methods above their authors utilized increasingly complex terminal equipment, trying to prevent data detection by the adversary. Unfortunately, in all of the systems described, a copy of Alice's or Bob's setup would also work for Eve, making the system completely insecure.

Recently there were attempts to use conceptually different ideas based on extensive statistical analysis and noise-like transmission with a feedback [15, 16], however they proved to be insecure due to errors in the security analysis [17].

An interesting classical key distribution system was proposed by Scheuer and Yariv [18], where a communication line becomes a giant fiber laser, and choosing different terminal mirrors allows one to obtain anti-correlated sequences of data at the line ends. This method has been further advanced in order to produce higher key generation rates [19,20], however, there is still a lack of proof that the system is secure under an attack where the adversary directly measures the reflectance spectrum of the mirror used. On the contrary, it is clear that such a simple attack or a modification thereof may ruin the proposed expensive and technologically-advanced system.

The last method we would like to stress upon is a Sagnac interferometer-based communication system, proposed in [21] and also in [22]. It is a large Sagnac loop with an off-center transmitting phase modulator and a centered modulator generating phase noise. This is the only system that provides asymmetry in eavesdropping. For Alice and Bob it is a simple data transmission system, where, due to the interferometer used, Bob sees plain intensity-modulated data sent by Alice. However, for Eve it is relatively difficult to recover this data. A possible strategy (which became feasible much later than the method was proposed) is in precise measurement of phase shifts of Alice's entire setup in both directions. Doing simple math with the two obtained functions allows one to reconstruct the data, but as we already mentioned, this is an example of a strongly asymmetric method.

To the best of our knowledge, this completes the current list of classical security methods applicable to fiber-optic communications. Of course there is a large body of quantum cryptographic methods, including the famous BB84 and B92 protocols, but they are out of the scope of the present paper. To summarize the related work, there are only a few methods that can be used without any prior shared secrets, and these methods are vulnerable to certain types of (simple) attacks. Other methods, which require a pre-shared "code", are also important, but require an initial sharing of a secret, which would require solving the equivalent security problem

#191857 - $15.00 USD Received 14 Jun 2013; revised 15 Sep 2013; accepted 17 Sep 2013; published 30 Sep 2013

of key distribution (e.g. using quantum key distribution) before they could be used, and thus are quite limiting. Hence, a practical optical-based secret key distribution technique that does not rely on prior security contexts is highly desirable, especially if it ensures that the complexity of potential eavesdropping is significantly more than required of legitimate parties.

1.3. Potential applications

The proposed method allows for the generation of identical (random) secret keys at the two ends of the interferometer. As the method does not use any artificial phase scramblers or noise generators, which can be actively read out by Eve and instead uses random phase fluctuations in the whole length of the fiber link, it provides natural protection from eavesdropping. Moreover, it does not require any pre-existing "secret" between Alice and Bob.

As we already pointed out, our approach cannot guarantee absolute key protection. It only creates very serious technical challenges for the potential adversary. Thus, the use of the method by itself might not be sufficient for critical applications. However, we note that it may be used in conjunction with other security methods. For example, it is natural to envision our key establishment method being used to establish a key for AES encryption, and then further encrypt such data using public key cryptography. The net result would be that Eve would require not only computing power much superior to Alice/Bob's, but also much more advanced optical technologies!

Some challenges in real applications of our method will be connected with a limited key generation rate. As will be shown later, key generation rate under typical conditions is of the order of 250 bits/s, which is much lower, than typical data rates in optical networks. However, this is not much different from the situation with conventional public key cryptography, where the asymmetric protocol itself is used for generation of session keys, which are then used for a much faster symmetric encryption. The generated key can as well become a seed "code" required by some other fiber optic security schemes, which allow encryption at the line rate [7]

Another challenge is in extension of the potential key distribution range. Without any modifications the method works up to the length, limited by the fiber loss. Using sensitive low-speed photodetectors and relatively high input power one can easily cope with a 40 dB attenuation, which translates to some 200 km in the ideal case and around 100+ km in practice. Going beyond this will require the use of optical amplifiers. As both fibers used in the setup carry a bi-directional stream of light, bi-directional Erbium-doped fiber amplifiers (EDFAs) will be required. Examples of their use have been successfully demonstrated in [23, 24], which provides some optimism for the future expansion of the method.

In the next section we provide details related to phase fluctuations in fiber optical links, which serve as the basis for the proposed method. Next we discuss security-related questions and formulate several necessary modifications, which make the system protected from eavesdropping. Section 4 provides details about the experimental demonstration and main results obtained in the experiments. We also analyze the achievable key generation rate and provide a simple algorithm of key extraction. In conclusion, we give a brief summary of the obtained results and a short discussion about future work towards practical realization of this secret key distribution method.

2. Phase fluctuations in fiber optical networks

Until very recently, phase fluctuations in fiber optical networks were largely ignored since all conventional forms of optical communication were immune to these line imperfections. Even with the migration to coherent optical transmission, phase fluctuations have a negligible impact since they are orders of magnitude slower than the data rate, so bit-to-bit phase fluctuations can always be ignored. A much more critical issue for coherent optical links is fluctuation of a

#191857 - $15.00 USD Received 14 Jun 2013; revised 15 Sep 2013; accepted 17 Sep 2013; published 30 Sep 2013

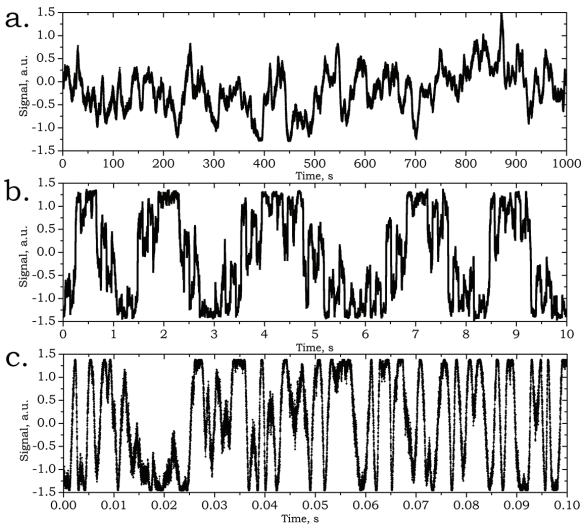

Fig. 2. Interference waveforms due to phase fluctuations in the Mach-Zehnder interferometer for different lengths of its arms: a. 2 m; b. 100 m; c. 26 km. The waveforms are normalized such that the in-phase ($\Delta\varphi = 0$) interference corresponds to 1.4 and the out-of-phase ($\Delta\varphi = \pi$) to -1.4.

polarization state, which is partially connected with phase fluctuations as it is related to optical phase between the two orthogonal polarization states. Polarization fluctuations are typically orders of magnitude slower than phase fluctuations because under normal conditions phase changes of the two polarizations are almost identical.

Phase fluctuations become a limiting factor when one considers the precise transfer of optical frequencies over large distances, e.g. for optical clock synchronization [25, 26]. As pointed out in a series of publications [25,27], most of the phase noise falls into kilohertz spectral range and leads to spectral broadening of ultrastable laser clock signals. Other critical applications sensitive to phase jitter include large-scale quantum coherence experiments [28, 29] and quantum communications [30].

Unlike the above mentioned applications, our key generation approach takes advantage of phase fluctuations and uses them as a source of randomness. In order to better understand underlying physics we collected some information about phase fluctuations. One interesting study of phase fluctuations was published in [31], where commercially installed optical fibers were used. For comparison with this work and validation of our experimental demonstration, we performed a series of experimental measurements in our laboratory environment.

Clearly, phase fluctuations depend on the length of the fiber and the environment where the fiber is located. In our study we measured phase fluctuations using a Mach-Zehnder interferometer similar to the one used in [31]. Three different lengths of the interferometer arms were chosen to explore phase jitter. In all experiments we measured optical intensity in one of the interferometer outputs, which is proportional to $1+\cos\Delta\varphi(t)$, where $\Delta\varphi(t)$ is the relative phase between the two arms. Figures 2 and 3 show samples of measured waveforms and their spectra calculated via Fourier transform of a long measurement series.

As expected, the time scale of measured fluctuations is directly related to the length of the interferometer arms. For the shortest interferometer with 2 m long arms the phase changes noticeably over periods of roughly 10 seconds and the amplitude of phase changes is such that the phase shift never exceeds π in the 1000 second long series. A Fourier transform of the wave-

#191857 - $15.00 USD Received 14 Jun 2013; revised 15 Sep 2013; accepted 17 Sep 2013; published 30 Sep 2013

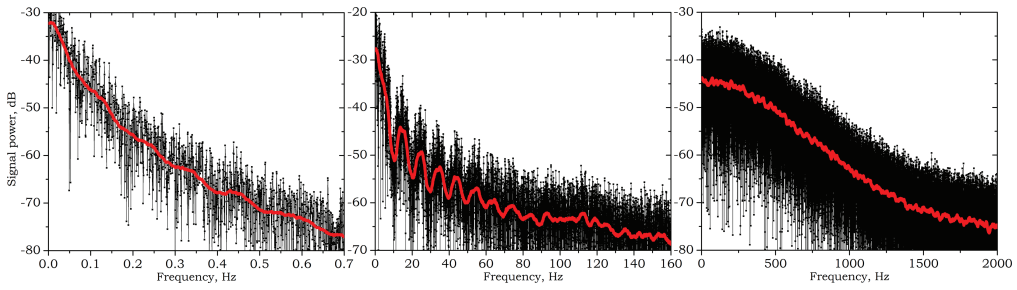

Fig. 3. FFT spectra of phase fluctuations in the Mach-Zehnder interferometer: a. 2 m long arms; b. 100 m long arms; c. 26 km long arms.

form shows that the most of power lies below 0.4 Hz. The intermediate length interferometer (100 m) shows much faster oscillations with a typical change time of 0.1 s, while most of oscillations are still relatively small, reaching a π value only several times in 10 s. The power spectrum lies below 60 Hz. The longest interferometer with 26 km arms exhibits qualitatively different behavior. Most phase changes are substantially larger than π thus most of the time the waveform goes directly from the maximum to the minimum and back. The time scale of such changes is in the millisecond range, while the power spectrum is around 1 kHz wide.

Our study demonstrated that measured phase fluctuations, especially in the long interferometer, are mainly due to the presence of acoustic noise in the lab environment: such an interferometer is extremely sensitive to sounds and even slightest vibrations. Slower effects such as a temperature change also contribute to fluctuations: intentional temperature change of the interferometer arm leads to a strong phase drift and thus to fast, nearly periodic intensity oscillations.

Our obtained results are in agreement with the experiment performed in a real telecom network [31], which allows us to generalize our further laboratory experiments to the case of real communication lines.

3. Security discussions

Realization of most security algorithms is often connected with an operation or a function that is able to be performed only under some very specific conditions accessible by the legitimate users. In quantum cryptography, meaningful measurement of a quantum state can be made only if there were no previous attempts of measuring it. In conventional asymmetric cryptography, factorization of a large number is possible only provided that one factor is known. Secret key generation in wireless systems [32] is possible because fading channel characteristics are unique for a pair of antennae, and cannot be measured by a third party. In the optical world, there is also an operation which can be performed only if some very rigorous conditions are satisfied — this is a measurement of an optical phase.

The difficulty of phase measurement is directly connected with the incredibly high rate of the phase change. At optical frequencies phase rotates with the speed of 10^{15} rad/s, which is not trackable, even by complex and powerful tools. The only known and potentially achievable method of phase measurement is via interference of two optical fields. In this way a relative phase or a difference between two optical phases can be accessed.

Another strong limitation is bandwidth: in most situations (usually called incoherent addition of light) even the difference of two optical phases falls far beyond potentially measurable bandwidth, which is limited by hundreds of gigahertz. Thus, a meaningful phase estimation can

#191857 - $15.00 USD Received 14 Jun 2013; revised 15 Sep 2013; accepted 17 Sep 2013; published 30 Sep 2013

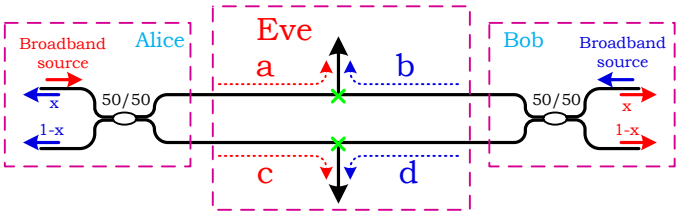

Fig. 4. Eavesdropper tapped into the system.

be done only if the phase difference between two interfering optical waves has a very narrow (by the optical scale) bandwidth, which is accessible with electronics. This holds only in the two cases: (1) Bandwidths of both optical fields are so narrow, that their difference is also narrowband; and (2) Bandwidth of the fields is large, but the phases are correlated such that their difference fluctuates much slower and can be measured with electronics. Those two cases are usually referred to as coherent addition of light.

An obvious requirement for such a measurement to be successful is that both optical fields must exist at the same physical location. If this is not true and they are separated by at least a few dozen meters, phase fluctuations connected with the transport of light across the separating distance can lead to significant measurement errors. A similar problem arises if the fields are broadband and are correlated but with a significant shift in time, i.e. one of them should be delayed to meet the condition (2). The only way to delay optical signals is to let it propagate over some distance, but this, in turn, leads to additional phase fluctuations.

Our proposed key establishment scheme, Fig. 1, uses a large-scale fiber Mach-Zehnder interferometer, which is set up between the two parties: Alice and Bob, such that they keep the couplers terminating the interferometer in protected locations. If the lengths of the interferometer arms are equal, a very broadband optical signal used as the input will satisfy the coherence conditions, and the output power, or the splitting coefficient, will fluctuate at a slow frequency. Alice and Bob can track these changes and use this function to generate a secret key. As mentioned earlier, these power fluctuations are due to the ever-changing optical path length, which is a result of thermal and mechanical effects in the fibers. If the distance between Alice and Bob is relatively long (a few km and more), phase fluctuations in the interferometer are large enough to create a unique pattern measurable only by Alice and Bob but not by Eve. It can be easily converted to a secret key, which then can be used for conventional cryptography.

Below we analyze possible vulnerabilities of the system and formulate an adversary model that we use throughout this work. We also summarize all necessary precautions that should be taken to ensure proper security of the system against eavesdropping.

3.1. Phase measurements by the adversary

If a broadband light source with a bandwidth beyond the capabilities of electronics is used by legitimate users, the assumptions about light interference stated above imply that the only way for Eve to perform phase measurement is if the signals from the two arms of the interferometer can be mixed such that coherence condition is satisfied. That means that Eve must ensure that the the two alternative light paths to the mixing point have the same lengths.

A possible strategy for Eve is illustrated in Fig. 4. She taps into both fibers as shown, dividing the interferometer into four segments: a, b, c, and d. If the length of segment a is equal to that of c, Eve can see interference between a and c, disclosing phase fluctuations in the left part of the interferometer. Similar she can see phase fluctuations in the right part of the interferometer by interfering signals from b and d.

#191857 - $15.00 USD Received 14 Jun 2013; revised 15 Sep 2013; accepted 17 Sep 2013; published 30 Sep 2013

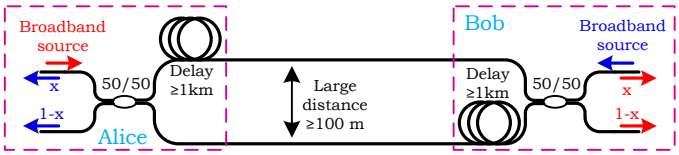

Fig. 5. System with added delays and physical separation between the arms of interferometer.

From a practical point of view, even this simple job requires precise optics, electronics and significant of engineering art to be successful. Eve needs to make sure that her setup, including tapping into the interferometer, precise optical path length adjustments and the effects of a light mixing tool, do not introduce any phase jitter significant for the operation of the legitimate key extraction algorithm. Moreover, since the measurable quantity is light intensity, but not the phase itself, she needs to perform corresponding analysis to extract phase fluctuations in both parts of the original interferometer and add them together to obtain the expected phase difference in the interferometer as a whole. Even so, she won't have the exact pattern observed by Alice and Bob since there is an ambiguity in choosing a constant phase shift between the two signals.

Each of the operations performed by Eve, in the real world, introduces distortions and errors compared to the pure signal measured by Alice and Bob. Slow phase drift in Eve's setup is also unavoidable, so even in this case Eve will have additional randomness not observed by Alice and Bob. As we mentioned earlier, although there are no fundamental limits preventing Eve from successful eavesdropping, there are always many practical/realistic limitations.

To increase protection of the system from such an attack, Alice and Bob may create strong asymmetry in the system by placing additional spans of fiber at their protected locations, as shown in Fig. 5. The length of these fiber spans should be large enough to create randomness comparable with the randomness generated by unprotected fibers. In this case to satisfy the coherence condition for the two light fields, Eve will have to apply a delay matching the length of the additional fiber spans, i.e. she will need to use the same length of fiber to match it. The fibers used by Eve cause practically unavoidable random phase fluctuations in the delay line, which will corrupt her measurements. A similar modification improving the scheme's security may involve increasing the physical separation of the two interferometer fibers. If the fibers are installed at a significant distance from each other, Eve will have to necessarily cover this distance with her fibers, which also introduces additional phase distortions.

It has to be mentioned here that there exist methods of partial phase stabilization in fiber optical links, which have had improvement recently [25, 29, 33, 34]. However, there is always some residual phase jitter, which is required to make the feedback in such schemes work. From a conceptual point of view, unavoidable phase distortions introduced by the Eve's setup lead to poor predictability of the signal measured by Alice and Bob.

3.2. Active intrusion attack

All hardware implementations of even flawless key distribution techniques, such as quantum cryptography, have a number of vulnerabilities connected with particular hardware realization, which may not distinguish between correct system operation and a smart intrusion into the system. This is supported by a number of successful attacks performed against commercial quantum key distribution systems [35–38]. In this sense our system is not an exception and needs to be protected from such attacks.

To stay within specifications, the system has to make sure that the measured intensity fluctuations are the result of interference between two broadband optical signals. Both conditions

#191857 - $15.00 USD Received 14 Jun 2013; revised 15 Sep 2013; accepted 17 Sep 2013; published 30 Sep 2013

of being broadband and being a result of interference are essential here. For example, Eve may cut both fibers of the interferometer and send an intensity-modulated signal through one of the fibers to Alice and Bob. Alice and Bob still will observe intensity fluctuations, but those will be under total control by Eve. In this case, the interference condition is not met. Alternatively, Eve can use narrowband spectral filters, to limit optical bandwidth of the signal received by legitimate users. This will make the phase measurable by a standard heterodyne method, thus disclosing the distributed key. This violates the requirement of receiving broadband light.

If both conditions are met, then the system will work properly. Therefore, constant monitoring of incoming light is important for system security. The first condition is measurable by tapping into both fibers before the coupler and monitoring optical power. Each of the arms should have no intensity modulation, while their interference result is modulated due to the phase fluctuations. The second condition may be easily tested by looking at interference of the same signals with an additional delay in one of the arms. If the delay is larger than the coherence time for the broadband light, no power fluctuations will be seen. If a narrowband light is substituted instead, its coherence time is much larger and thus two beams will interfere giving the same pattern as the main system output.

3.3. Other considerations

The essential point behind the adversary model that we use in this work is Eve's inability to make direct measurements of optical phase in a broadband optical signal and her inability to transmit (delay) optical signals via long distances without introducing extra phase jitter. Again, we note that these limitations are not fundamental, but are rather based on the practical difficulty of implementing these tasks. Besides the two assumptions mentioned above, several other assumptions are important.

As most other schemes, including quantum key distribution, the proposed technique does not provide authentication, which makes it potentially vulnerable to man-in-the-middle type attack. In our analysis, we assume that Alice and Bob have access to an authenticated public channel, which can be listened to but not modified by Eve. This allows them to exchange information for constructing correlated bit sequences from the analog waveforms and to perform error correction in the obtained raw keys. To prevent a man-in-the-middle attack, Alice and Bob may choose to publicly exchange some portion of the generated key to make sure the interferometer is set up directly between them and not between each of them and Eve.

We also assume that the key distribution algorithm is known by Eve. Eve may tap into the arms of the interferometer and make any practically possible measurements of the transmitted light. She is assumed to know all characteristics of the particular experimental realization, meaning any practically measurable quantities. What she cannot do is to predict or indirectly measure phase fluctuations in the fibers, based on measurements of the environment where the fibers are placed. Even if it is potentially tractable for unprotected spans of fiber, fiber spans kept at protected areas controlled by Alice and Bob introduce additional randomness, completely unpredictable by Eve.

A strong advantage of the proposed approach is that the main source of randomness used for key generation is a many kilometer long distributed system rather then a local noise source, which can be controlled or affected by the adversary. Thus any attempts of controlling the system locally fail because there is enough randomness created by the uncontrolled parts of the system. One potential vulnerability, which is easily avoided, is artificial creation of excessive phase noise by Eve, such that it provides much stronger phase fluctuations than the system normally has. In this case most of the entropy in the generated key will be caused by Eve rather than by normal phase fluctuations. To prevent this, system designers should estimate the expected key generation rate and shutdown the system if it experiences much faster phase fluctuations.

#191857 - $15.00 USD Received 14 Jun 2013; revised 15 Sep 2013; accepted 17 Sep 2013; published 30 Sep 2013

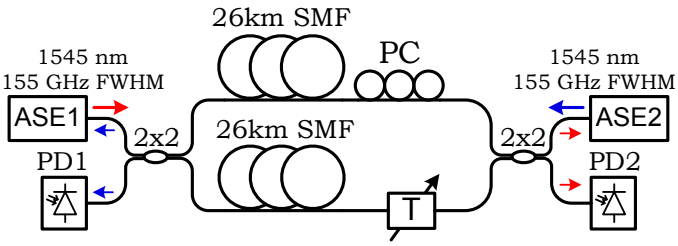

Fig. 6. Experimental setup. ASE – broadband amplified spontaneous emission source; PD – photodiode; 2x2 – 50/50 fiber coupler; SMF – single-mode fiber; PC – polarization controller; T – variable delay line.

In other words, key generation rate should not exceed the entropy rate of the normal phase fluctuations in the fibers, even if the *measured* phase fluctuations allow for a significantly faster key generation.

4. Experimental realization

4.1. Experimental setup

Our experimental setup is schematically shown in Fig. 6. It contains two independent broadband amplified spontaneous emission (ASE) sources, ASE1 and ASE2. Each of them is an erbium-doped fiber amplifier (EDFA) working without input signal and a thin film bandpass filter, limiting the bandwidth to 155 GHz FWHM. Central wavelengths of the two sources are the same within the precision of the available off-the-shelf filters used. The signal is then pre-amplified to reach the power of approximately +6 dBm at the interferometer input. The single-mode fiber used in the interferometer is a standard Corning SMF-28e fiber. The arms of the interferometer also contain a polarization controller (PC) and a variable delay line (T), to allow relative polarization and length adjustment of the two arms. The total length of the interferometer is approximately 26 030 m, which corresponds to the total propagation delay of 127.5 μs. Photodetectors used in the setup are broadband pre-amplified DC-coupled GaAs PIN photodiodes, going up to 10 GHz frequency.

Adjustment of the interferometer includes two steps: equalization of the arm lengths and tuning the polarizations and optical powers. The first one is the most critical, because without length equalization beating between the signals in the two arms is very broadband (roughly 150 GHz) and thus cannot be measured. The coherence length of the signals $L_{coh} \approx c/\Delta\nu \approx$ 2 mm. The measured spectrum of the signal used is shown in Fig. 7(a). Due to its noise-like nature the spectrum is also very noisy on top. When the arms of the interferometer are exactly equal, the amplitude of detected power oscillations is maximal, but changing the delay in one of the arms decreases it until no oscillations are observed. The measured amplitude of oscillations versus change of the delay is shown in Fig. 7(b) with black markers. Ideally, the shape of this curve should be the same as the Fourier transform of the signal spectrum, which is shown in the figure as a red line. Both shapes are very similar, however the experimental one does not decay to zero in its minima.

The second stage of adjustments is required to ensure that light polarizations at the output coupler are not orthogonal to each other and the powers are approximately equal. If polarizations are orthogonal, the light fields do not interfere and the output power is just one half of the sum of the input powers, i.e. it remains constant. If two polarizations are aligned, the interference result spans from zero (destructive interference) to the sum of the input powers (constructive interference). This is correct if the two interfering light fields have the same in-

#191857 - $15.00 USD Received 14 Jun 2013; revised 15 Sep 2013; accepted 17 Sep 2013; published 30 Sep 2013

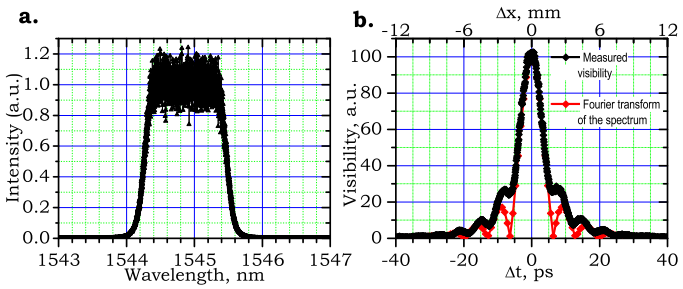

Fig. 7. Characteristics of the broadband optical signal used in the experiments: a. optical spectrum of the signal; b. measured visibility of interference vs. time delay (length change) and the Fourier transform of the signal spectrum.

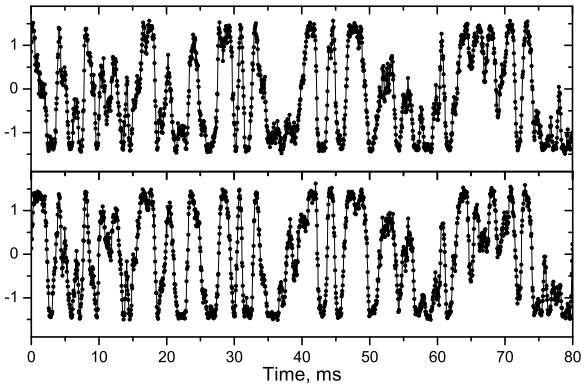

Fig. 8. An example of the waveforms measured by Alice and Bob at the two ends of the 26 km long Mach-Zehnder interferometer. The signals are highly correlated, however, they have noticeable differences due to a finite time of light propagation in the interferometer.

tensity, which is always the case in this setup. Any offsets from these ideal conditions slightly decrease the depth of the observed oscillations, however as long as oscillations are visible, it is possible to use them for generation of the key.

4.2. Key extraction

Once the hardware is set up and functioning, Alice and Bob need a protocol for extracting binary keys from the received analog waveforms, measured by photodetectors. Similar algorithms were explored in a series of publications about wireless physical layer security [39, 40]. In the present work we focus our attention on estimating the achievable key generation rate, which is one of potential figures of merit for key distribution techniques.

Implementation of any key extraction scheme requires knowledge of statistical properties of raw waveforms. In our demonstration we digitized obtained waveforms using a 16-bit data acquisition board (National Instruments USB-6211) at a sampling rate of 20 kHz. An example of measured waveforms is shown in Fig. 8, where two signals measured by Alice and Bob are shown versus the same time scale. The waveforms look similar, however there are noticeable differences between them. The differences appear mainly because of the finite time it takes for light to go through the interferometer, so the state of the fiber may be different for the forward and backward light waves. Thus interference conditions may be also slightly different resulting in discrepancies between the received waveforms.

#191857 - $15.00 USD Received 14 Jun 2013; revised 15 Sep 2013; accepted 17 Sep 2013; published 30 Sep 2013

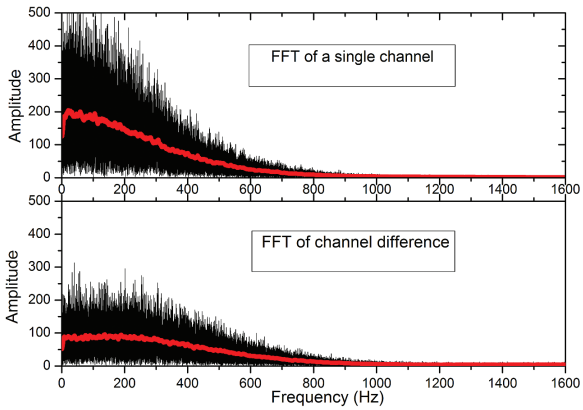

Fig. 9. FFT power spectrum of a single channel and a difference between the two channels. The power suppression of the channel difference at frequencies below 400 Hz is due to high correlation of the waveforms at low frequencies.

To visualize this we calculated power spectra for one of the measured channels and for the difference between the two channels. Both spectra are presented in Fig. 9. As follows from the figure, spectral components above 400 Hz are almost decorrelated, resulting in the same spectrum on both plots, while lower frequencies exhibits significantly lower power for the difference than for a single channel. This indicates strong correlation between the two channels at frequencies lower 400 Hz.

From a theoretical point of view, obtaining correlated waveforms, requires that the state of the fiber does not significantly change for the time of flight, equal to $\tau \approx 130\mu s$, which results in the maximum frequency of correlated fluctuations $\nu_{max} = \Delta\varphi/(2\pi\tau) = 380$ Hz, if the phase error is $\Delta\varphi = \pi/10$. This reasonable agreement between the experiment and the theory suggests that our simple model is adequate for the system.

Another interesting figure is the linear correlation coefficient and its behavior under time shifts. Since correlations between the two signals are linear, i.e. waveforms just repeat each other, the linear correlation coefficient is a good measure of waveform similarity. In Fig. 10 we show auto- and cross-correlation functions with respect to the time shift. Cross-correlation at zero time shift, i.e. maximum cross-correlation, shows how similar the two waveforms are, while the width of the correlation curves indicates the decorrelation time. As follows from the figure, the maximal cross-correlation coefficient is 0.75 so one can expect significant similarities between the waveforms. The full decorrelation time for our realization is less than 2 ms, so the system has no memory longer than 2 ms. Any two measurements taken with the time interval between them larger than 2 ms results in completely independent numbers.

Based on the provided analysis, we implemented a simple key extraction protocol, which uses level crossings or excursions [40]. First, the waveforms are scaled to get unity variance and shifted to remove any DC offset. Then each waveform is processed to find continuous blocks of samples with values $|x_i| > 0.9$, which is an empirically chosen threshold. Each such block represents an "excursion" potentially suitable for extracting a bit of information. Then Alice tells Bob time indexes of starting and ending samples in each of the found excursions. This implies that Alice and Bob have synchronized clocks, which could be easily done using global GPS-based timing. Bob compares excursions that he found with those found by Alice, and if they overlap labels the sample in the middle of the overlapping region. When labeling, Bob must ensure that the time distance between adjacent labeled samples is larger than the decorrelation time, to avoid any correlations between bits in the raw key. Based on the labeled

#191857 - $15.00 USD Received 14 Jun 2013; revised 15 Sep 2013; accepted 17 Sep 2013; published 30 Sep 2013

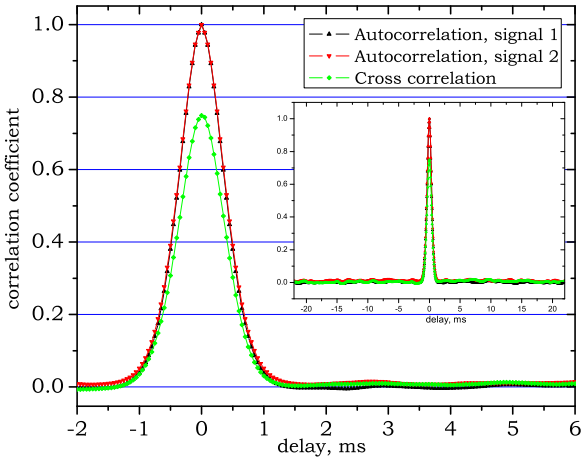

Fig. 10. Autocorrelation functions for the two signals measured by Alice and Bob and cross-correlation between them. The inset shows the same correlation functions for a larger time span, which confirms full decorrelation for time periods larger 2 ms.

indexes, he constructs his raw key using bit '1' if the value lies above the positive threshold and '0' if it lies below the negative threshold. He also sends all labeled indexes to Alice and she constructs her raw key in the same manner.

For key extraction, we used 500 000-sample blocks of data, representing 25-second time intervals. Each block was processed independently. The discussed simple method of key extraction demonstrated an average raw key generation rate of 160 bits/s with less than 4% bit errors between Alice and Bob. This relatively low bit error rate can be easily corrected using conventional information reconciliation and privacy amplification algorithms, e.g. using the *cascade* protocol popular in quantum key distribution [41]. The obtained secret key rate is probably not high enough for the true one-time-pad data encryption, as has been used in some modern quantum key distribution systems with key rates of 10s and even 100s of kbits/s [44]. However, use of the one-time-pad for encryption is generally avoided in modern cryptographic settings due to its malleability. That said, though, we note that a key generation rate of 160bps is not only more than sufficient for generating fresh key material to be used in symmetric encryption algorithms, such as AES, but also is comparable with the performance of current commercial systems, e.g. ID Quantique *Cerberis* providing around 400bps over 13 km [44]. In fact, typical higher layer security services, such as 802.1X, recommend that keys be changed on the order of once an hour, and our method is ideal for feeding such security services since it can refresh 256-bit keys several times per minute.

Another way of estimating achievable key generation rate is based on mutual information calculations between samples obtained by Alice and Bob. We used two different algorithms for mutual information estimation: one based on adaptive binning [42] and the other using k-nearest neighbor distance [43]. Mutual information for a single sample measured by Alice and Bob was found from a series of 500 000 samples taken at time intervals of 3 ms to ensure their independence. Both algorithms demonstrated very similar results equal to 0.51 ± 0.02 bits per measurement. Taking independent samples every 2 ms will results in the mutual information rate of more than 250 bits/sec. This is only slightly more than we obtained from a very simple excursion-based protocol because in this estimation we only assumed one sample per decorrelation time, while taking into account a shape of the waveform within this interval will result in a much larger value for mutual information. Thus, improvement of our algorithm towards

#191857 - $15.00 USD Received 14 Jun 2013; revised 15 Sep 2013; accepted 17 Sep 2013; published 30 Sep 2013

optimality should easily be able to deliver at least 250 secret key bits per second, and is part of our ongoing work.

5. Conclusion

We proposed and experimentally demonstrated a method for secret key distribution based on the physical properties of fiber optical communication lines. Unlike most of the other approaches to physical layer security in fiber optical networks, our method does not require any pre-shared secret information and works under the assumption that the adversary has a comprehensive knowledge about the system. Protection of the system is based on the practical incapability of measuring optical phase difference between two incoherent broadband beams of light.

The demonstrated key distribution method uses a large-scale Mach-Zehnder interferometer covering the entire distance between the communicating parties. Random variations of the optical phase in the interferometer arms causes correlated intensity fluctuations, which are, in turn, observed by the parties. A secret key is generated from the obtained fluctuation patterns, which are the same at both ends of the interferometer. One necessary requirement for achieving secure key distribution with this method is the availability of a public authenticated communication channel between the users to avoid a man-in-the-middle attack. Our laboratory demonstration, which is quantitatively very similar to what is used in commercially installed fiber links, showed a key generation rate of 160 bits/s over 26 km link with the average bit error rate of less than 4%. The use of more efficient key extraction algorithms is expected to result in a higher key generation rate. Overall, both the key generation rate and the maximum reach distance are comparable with those in commercial QKD systems, while using bi-directional EDFAs may help to substantially outperform QKD in terms of communication distance.

Acknowledgments

This work was supported in part by the Russian Ministry of Education and Science under the state contract 11.519.11.4009.

#191857 - $15.00 USD Received 14 Jun 2013; revised 15 Sep 2013; accepted 17 Sep 2013; published 30 Sep 2013