Secure key generation using an ultra-long fiber laser: transient analysis and experiment

Avi Zadok,[1,*] Jacob Scheuer,[2] Jacob Sendowski,[1] and Amnon Yariv[1]

[1]*Department of Applied Physics, California Institute of Technology, MC 128-95, 1200 E. California Blvd., Pasadena, CA 91106, USA*

[2]*School of Electrical Engineering, Faculty of Engineering, Tel-Aviv University, Ramat-Aviv, Tel-Aviv 69978, Israel*

[*]*Corresponding author: avizadok@caltech.edu*

Abstract: The secure distribution of a secret key is the weakest point of shared-key encryption protocols. While quantum key distribution schemes could theoretically provide unconditional security, their practical implementation remains technologically challenging. Here we provide an extended analysis and present an experimental support of a concept for a classical key generation system, based on establishing laser oscillation between two parties, which is realized using standard fiber-optic components. In our *Ultra-long Fiber Laser* (UFL) system, each user places a randomly chosen, spectrally selective mirror at his/her end of a fiber laser, with the two-mirror choice representing a key bit. We demonstrate the ability of each user to extract the mirror choice of the other using a simple analysis of the UFL signal, while an adversary can only reconstruct a small fraction of the key. The simplicity of this system renders it a promising alternative for practical key distribution in the optical domain.

OCIS codes: (060.4785) Optical security and encryption; (140.3510) Lasers, fiber; (060.2330) Fiber optics communications.

References and links

1. S. Singh, *The Code Book: The science of secrecy from ancient Egypt to quantum cryptography* (Fourth Estate, 1999).
2. G. Vernam, "Cipher printing telegraph systems for secret wire and radio telegraphic communications," J. Am. Inst. Electr. Eng. **45**, 109-116 (1926).
3. C. H. Bennett, and G. Brassard, "Quantum public key distribution system," IBM Tech. Discl. Bull. **28**, 3153-3163 (1985).
4. A. K. Ekert, "Quantum cryptography based on Bell's theorem," Phys. Rev. Lett. **67**, 661-663 (1991).
5. N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," Rev. Mod. Phys. **74**, 145-195 (2002).
6. P. W. Shor, and J. Preskill, "Simple proof of security of the BB84 quantum key distribution protocol," Phys. Rev. Lett. **85**, 441-444 (2000).
7. L.-M. Duan, M. D. Lukin, J. I. Cirac, and P. Zoller, "Long-distance quantum communication with atomic ensembles and linear optics," Nature **414**, 413-424 (2001).
8. M. Aspelmeyer, H. R. Bohm, T. Gyasto, T. Jennewein, R. Kaltenbaek, M. Lindenthal, G. Molina-Terriza, A. Poppe, K. Resch, M. Taraba, R. Ursin, P. Walther, and A. Zeilinger, "Long distance free space distribution of quantum entanglement," Science **301**, 621-623 (2003).
9. I. Marcikic, H. de Riedmatten, W. Tittel, H. Zbinden, M. Legre, and N. Gisin, "Distribution of time-bin entangled qubits over 50 km of optical fiber," Phys. Rev. Lett. **93**, 180502 (2004).
10. R. J. Hughes, G. L. Morgan, and C. G. Peterson, "Quantum key distribution over a 48-km optical fiber network," J. Mod. Opt. **47**, 533-547 (2000).
11. C. Gobby, Z. L. Yuan, and A. J. Shields, "Quantum key distribution over 122 km of standard telecom fiber," Appl. Phys. Lett. **84**, 3762-3764 (2004).
12. W.-Y. Hwang, "Quantum key distribution with high loss: towards global secure communication," Phys. Rev. Lett. **91**, 057901 (2003).
13. H.-K. Lo, X. Ma, and K. Chen, "Decoy state quantum key distribution," Phys. Rev. Lett. **94**, 230504 (2005).
14. X.-B. Wang, "Beating the photon-number-splitting attack in practical quantum cryptography," Phys. Rev. Lett. **94**, 230503 (2005).
15. Z. L. Yuan, A. R. Dixon, J. F. Dynes, A. W. Sharpe, and A. J. Shields, "Gigahertz quantum key distribution with InGaAs avalanche photodiodes," Appl. Phys. Lett. **92**, 201104 (2008).

#100223 - $15.00 USD Received 15 Aug 2008; revised 15 Sep 2008; accepted 1 Oct 2008; published 3 Oct 2008

16. N. Lutkenhaus, "Security against individual attacks for realistic quantum key distribution," Phys. Rev. A **61**, 052304 (2000).
17. W. Tittel, J. Brendel, H. Zbinden, and N. Gisin, "Long-distance Bell-type tests using energy-time entangled photons," Phys. Rev. A **59**, 4150-4163, (1999).
18. P. G. Kwiat, A. M. Steinberg, R. Y. Chiao, P. H. Eberhard, and M. D. Petroff, "High efficiency single photon detectors," Phys. Rev. A **48**, R867-870 (1993).
19. A. Tanaka, M. Fujiwara, S. W. Nam, Y. Nambu, S. Takahashi, W. Maeda, K.-I. Yoshino, S. Miki, B. Baek, Z. Wang, A. Tajima, M. Sasaki, and A. Tomita, "Ultra fast quantum key distribution over a 97 km installed telecom fiber with wavelength division multiplexing clock synchronization," Opt. Express **16**, 11354-11360 (2008).
20. H. Takesue, S. W. Nam, Q. Zhang, R. H. Hadfield, T. Honjo, K. Tamaki, and Y. Yamamoto, "Quantum key distribution over a 40-dB channel loss using superconducting single photon detectors," Nat. Photon. **1**, 343-348 (2007).
21. L. Tancevski, I. Andonovich, and J. Budin, "Secure optical network architecture utilizing wavelength hopping / time spreading codes," IEEE Photon. Technol. Lett. **7**, 573-575 (1995).
22. D. D. Sampson, G. Pendock, and R. A. Griffin, "Photonic code-division multiple-access communications," Fiber Integr. Opt. **16**, 129-157 (1997).
23. T. H. Shake, "Security performance of optical CDMA against eavesdropping," IEEE J. Lightwave Technol. **23**, 655-670 (2005).
24. T. H. Shake, "Confidentiality performance of spectral-phase-encoded optical CDMA," IEEE J. Lightwave Technol. **23**, 1652-1663 (2005).
25. J.-P. Goedgebuer, L. Larger, and H. Porte, "Optical cryptosystem based on synchronization of hyperchaos generated by a delayed feedback tunable laser diode," Phys. Rev. Lett. **80**, 2249-2252 (1998).
26. A. Argyris, D. Syvridis, L. Larger, V. Annovazzi-Lodi, P. Colet, I. Fischer, J. Garcia-Ojalvo, C. R. Mirasso, L. Pesquera, and K. A. Shore, "Chaos-based communications at high bit rates using commercial fiber-optic links," Nature **438**, 343-346 (2005).
27. R. Pappu, R. Recht, J. Taylor, and N, Gershenfeld, "Physical one way functions," Science **297**, 2026-2030 (2002).
28. J. Scheuer, J. and A. Yariv, "Giant fiber lasers: a new paradigm for secure key distribution," Phys. Rev. Lett. **97**, 140502 (2006).
29. R. L. Rivest, A. Shamir, and L. M. Adleman, "A method for of obtaining digital signatures and public key cryptosystems," Commun. ACM **21**, 120-126 (1978).
30. G. Brassard, "A note on the complexity of cryptography," IEEE Trans. Inf. Theory **IT-25**, 232-233 (1979).
31. G. A. Barbosa, "Fast and secure key distribution using mesoscopic coherence states of light," Phys. Rev. A **68**, 052307 (2003).
32. B. Alpern, ad F. B. Schneider, "Key exchange using keyless cryptography," Info. Proc. Lett. **16**, 79-81 (1983).
33. J. R. Barry, E. A. Lee, and D. G. Messerschmitt, *Digital Communication* (Kluwer Academic Publisher, 3rd Ed. 2004).
34. C. K. Madsen, and J. H. Zhao, "A general planar waveguide autoregressive optical filter," IEEE J. Lightwave Technol. **14**, 437-447 (1996).
35. S. Wolf, "Unconditional security in cryptography," Lectures on data security **1561**, 217-250 (1999).
36. A. D. Wyner, "The wire-tap channel," Bell Syst. Tech. J. **54**, 1355-1387 (1975).
37. M. Anand, E. Cronin, M. Sherr, M. A. Blaze, and S. Kannan, "Security protocols with isotropic channels," Technical report MS-CIS-06-18, Department of Computer and Information Science, University of Pennsylvania (2006).

1. Introduction

The need for secure key distribution has created a large interest in physical-layer based cryptographic protocols, which may provide powerful complementary capabilities to those of the more traditional, information theory based coding systems [1, 2]. The most widely known example is that of quantum key distribution (QKD) protocols [3-20], in which the key is generated by measurements of the quantum mechanical properties of single photons. However, practical implantation of the idea is complicated [7-11]: technological challenges include the reliable, high yield generation of single photons [5, 16, 17], the compensation for fiber channel variations [5], and the development of low noise, single photon detectors operating at the telecommunication wavelength of 1550 nm [5, 18-20]. QKD is facing a major hurdle in overcoming fiber losses, which may not be compensated for using optical amplifiers [5]. Recently, the introduction of decoy states had allowed for the use of faint coherent pulses [12-14], and avalanche InGaAs photo-detectors were successfully used in GHz clock rate experiments [15]. Nonetheless, present day QKD demonstrations must rely on either complicated, sensitive detection schemes, or on sophisticated, cutting edge components [15,

#100223 - $15.00 USD Received 15 Aug 2008; revised 15 Sep 2008; accepted 1 Oct 2008; published 3 Oct 2008

19-20]. The quest for a simpler, classical secure key generation scheme therefore remains meaningful.

Optical code division multiple access (OCDMA) schemes are often discussed in the context of secure communication (see for example [21, 22]). The decoding of OCDMA data requires prior knowledge of individual user codes. In many cases, the available code space is large enough to render a brute-force code search by an intruder impractical. However, as pointed out by Shake [23, 24], OCDMA techniques suffer from inherent security disadvantages. First, an OCDMA encoder using a fixed code represents a linear time-invariant (LTI) system [23]. If the encoder's input waveform is ever compromised, an intruder can use standard linear analysis to solve for its impulse response [23]. Furthermore, OCDMA transmitters repeatedly broadcast the code itself over a large number of bits [23, 24]. An eavesdropper equipped with sophisticated detectors may tap the OCDMA network with a sufficient signal to noise ratio (SNR) to recover the code [23, 24]. Frequent code changes and a low power transmission can make the intruder's task more difficult, though not impossible [23, 24].

Another promising scheme for secure optical communication is based on the synchronization of lasers in the chaotic regime [25]. On the transmitter side, a delayed, non-linear current feedback loop is used to generate chaotic variations to the wavelength of a semiconductor laser diode [25]. The confidential message provides the initial condition of the feedback loop. That initial condition can be recovered using an identical laser diode and feedback loop on the receiver side [25]. The potential of the scheme was demonstrated by a field test, operating at multi gigabit per second (Gb/s) rates over 120 km of standard fiber [26]. One weakness of the system, however, is its dependence on a small number of hardware parameters which are difficult to reconfigure. An unauthorized user may reconstruct or commandeer a network receiver, and decode the confidential messages, while the legitimate users remain unaware of such an attack. Another previously proposed optical implementation of one-way functions was based on the speckle patterns generated by scattering in a random medium [27]. Although the cloning of scattering tokens is impossible [27], they must be physically distributed among legitimate users.

The ultra-long fiber laser (UFL) [28] key distribution system described in this work is not algorithmically and absolutely secure, as QKD ideally would be. Such unconditional security, though, has not been a mandatory pre-requisite for the application of cryptosystems, as many public key encoding schemes rely on the computational difficulty of eavesdropping rather than on a security proof [29, 30]. Promising optical schemes achieved major practical benefits by allowing some relaxation of the unconditional security requirement of QKD. For example, Barbosa [31] had used mesoscopic coherent states in a proposed key generation scheme that is scalable to optical communication rates, and could allow for optical amplification. The UFL system further extends optical key generation towards the classical light regime. Consequently, it requires only readily available, low cost standard fiber-optic components, and its key-establishing rate decreases only linearly with distance [28]. While an intruder may, in principle, obtain some partial knowledge of the UFL generated key, this knowledge can be reduced by any arbitrary amount by means of relatively simple strategies, as discussed below. Unlike OCDMA transmitters, the UFL terminals do not broadcast a fixed code for extended periods, and the generation of subsequent key bits is uncorrelated. As opposed to chaos synchronization based architectures, an intruder may not introduce a replicated UFL terminal and remain undetected.

In previous work [28], the UFL concept was introduced and a preliminary, steady state based security analysis was presented. In this paper, two significant advancements are provided. First, the security analysis is extended to include a more powerful adversary model, based on tapping into transient signals following the UFL switch on. Numerical simulations show that the UFL system is considerably more vulnerable to such transient-based attacks, than to eavesdropping at its steady state. Nevertheless, the security of the system can be restored using simple measures. Second, a first experimental demonstration of the UFL system is provided. In the experiment, two users separated by a 25 km long fiber link

#100223 - $15.00 USD Received 15 Aug 2008; revised 15 Sep 2008; accepted 1 Oct 2008; published 3 Oct 2008

generated a 1000 bit long key, with an error ratio of only 0.6%. The key generation rate was 167 b/s. An intruder tapping the link could recover only 65% of the key bits, which provide him/her with only a marginal knowledge gain over random guessing. The extended security analysis and experimental demonstration substantiate the UFL system as a potential alternative strategy for secure key generation in the optical domain. The system may provide better security than that of other classical approaches, while its implementation is significantly simpler than that of QKD.

The remainder of this paper is organized as follows: Sec. II briefly reiterates the principle of operation of the UFL system [28]. Numerical simulations and results are described in Sec. III, and the experimental work is presented in Sec. IV. A brief discussion is provided is Sec. V.

2. Principle of operation

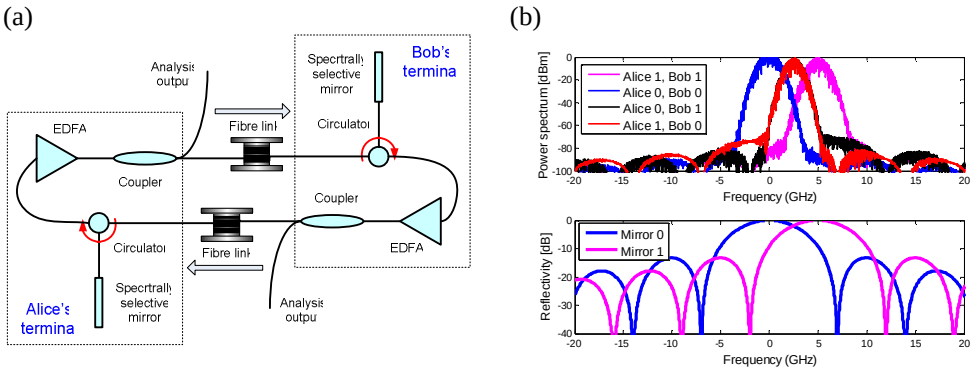

Fig. 1. (a). Schematic of the UFL system. (b). Top: simulated steady state UFL spectra for the four possible combinations of mirror choices by Alice and Bob. The spectra for (0,1) and (1,0) mirror choices are distinguishable only in their weak spectral side lobes. Bottom: reflectivity profiles $|r_0(\omega)|^2$, $|r_1(\omega)|^2$ of '0' and '1' mirrors used in simulations: $r_0(\omega) = 0.75 \cdot \mathrm{sinc}^2(\omega/\Delta\omega)$, $r_1(\omega) = 0.75 \cdot \mathrm{sinc}^2[(\omega - \omega_{sep})/\Delta\omega]$, with a spectral width of $\Delta\omega = 2\pi \cdot 7\,\mathrm{GHz}$, and a frequency separation of $\omega_{sep} \equiv 2\pi(f_1 - f_0) = 2\pi \cdot 5$ GHz. The EDFAs small signal gain, saturation power and noise figure are: $10\log_{10} G_0 = 17\,\mathrm{dB}$ above transparency, $P_{sat} = 13\,\mathrm{dBm}$ and $NF = 3\,\mathrm{dB}$.

A schematic of the UFL system is shown in Fig. 1(a). The system consists of a fiber link with a terminal at each end, one controlled by Alice and the other by Bob. Each terminal includes an Erbium doped fiber amplifier (EDFA) and a set of two spectrally selective mirrors. The peak reflectivity frequencies of the two mirrors in the set are f_0 (mirror '0'), and f_1 (mirror '1'). In each bit cycle, both Alice and Bob randomly choose one of the mirrors ('0' or '1') as an end mirror of the UFL. The combination of mirror choices is identified through measurements of the UFL spectrum, and represents a single bit. Mirror choices (0,0) or (1,1) lead to oscillations near f_0 or f_1, respectively. An eavesdropper (Eve) measuring peak frequencies f_0 or f_1, can thus easily infer the corresponding mirror choices. These data are thus discarded. The choices (1,0) and (0,1) lead (both) to oscillation close to $f_c \equiv \frac{1}{2}(f_0 + f_1)$. If Eve measures f_c, she can not easily determine which arrangement, (1,0) or (0,1), was used. Alice, knowing her own mirror choice, can determine the complementary choice of Bob, and vice versa. The two of them can therefore assign, for example, a logical '1' to the choice of (1,0), and a logical '0' to (0,1). The UFL principle of operation is analogous to the idea of "keyless cryptography", proposed by Alpern and Schneider as early as 1983 [32]. In that scheme, Alice and Bob anonymously post their uncorrelated choices of binary strings on a public blackboard, and only they can recognize the generator of individual messages [32].

#100223 - $15.00 USD Received 15 Aug 2008; revised 15 Sep 2008; accepted 1 Oct 2008; published 3 Oct 2008

3. Numerical simulations

We refer to the optical field propagating from Alice to Bob as $E_+(\omega)$, ω denoting the optical frequency, and to the field propagating from Bob to Alice is $E_-(\omega)$. The fields are normalized so that the integral $\int |E_\pm(\omega)|^2 d\omega$ represents optical power. The EDFAs used in both terminals are assumed to be identical, characterized by their small signal gain coefficient G_0, saturation output power P_{sat} and noise figure NF. $r_A(\omega)$ and $r_B(\omega)$ are the spectral reflectance profiles of the mirrors chosen by Alice and Bob, respectively. The fiber spans connecting the two terminals are both of length L, and have the same propagation constant β.

The build-up of the lasing signal within the UFL following switch-on may be evaluated by the following set of iterative, coupled equations [28]:

$$E_+^{l+1}(\omega) = E_-^l(\omega)\exp(-j\beta L) r_A(\omega)\exp(G_+^l/2) + E_s(\omega) \tag{1}$$

$$E_-^{l+1}(\omega) = E_+^l(\omega)\exp(-j\beta L) r_B(\omega)\exp(G_-^l/2) + E_s(\omega)$$

In Eq. (1), $E_\pm^l(\omega)$ denote the optical fields in both directions of propagation, following l one way trips within the UFL. The gain coefficients $G_\pm^l$ are determined by the overall input power of the EDFAs:

$$G_\pm^l = \frac{G_0}{1 + \int |E_\mp^l(\omega)|^2 d\omega / P_{sat}} \tag{2}$$

The gain coefficients are assumed to be frequency independent within the reflectivity windows of the mirrors. This is a reasonable assumption, since the reflectivity bandwidths of the mirrors employed in the experiments are below 0.05 nm. The additive term $E_s(\omega)$ in Eq. (1) represents the random phase optical field of the Amplified Spontaneous Emission (ASE) of the EDFAs. The power of the ASE field within a frequency window of width $d\omega$ is assumed to be independent of ω:

$$|E_s(\omega)|^2 d\omega = h\nu \cdot NF[\exp(G_\pm) - 1] \cdot d\omega \tag{3}$$

Here, $h\nu$ is the energy of a single photon, and $G_\pm^l$ are used in the evaluation of $E_\pm^l(\omega)$.

Figure 1(b) shows examples of the simulated UFL steady state spectra $P_+(\omega) \equiv |E_+^l(\omega)|^2 d\omega$, $l >> 1$, for the four possible combinations of mirror choices. When the choices of mirrors are (0,0) or (1,1), the central lasing frequency is f_0 or f_1, correspondingly. The spectra obtained for (1,0) and (0,1) mirror choices, representing '1' and '0' bits, are both centered at f_c and their main lobes are identical. In order to distinguish between the two, Eve must examine the spectral side lobes, whose steady state power is 60 dB lower than that of the main lobe. The difference in the available signal power sets an inherent imbalance between the task of Alice and Bob and that of Eve, as one-way functions do in public key, data encoding schemes [29, 30].

Our previous analysis of the UFL security was restricted to its steady state operation [28]. However, a close examination of the build up phase of the UFL following switch-on reveals that the power within the side-lobes is higher, and their asymmetry is more pronounced, than at steady state. Figure 2(a) shows simulated plots of $|E_+^l(\omega)|^2 d\omega$ for (0,1) mirror choice, generating a '0' bit, for different values of l following the UFL switch-on. During the few initial propagation cycles, these spectra bear a residual signature of Alice's choice of mirror,

#100223 - $15.00 USD Received 15 Aug 2008; revised 15 Sep 2008; accepted 1 Oct 2008; published 3 Oct 2008

and hence the key bit. This signature decreases gradually as the UFL approaches steady state. Even though these spectrally asymmetric transient signals are weak, they could disclose the key to Eve, and care must be taken to conceal them.

For example, Eve can use the difference in optical power between the first left hand spectral side lobe and the first right hand side lobe as her decision variable V_E. Figure 2(b) shows simulated probability distribution functions of V_E, taken 3 ms following the switch-on of a 25 km long UFL, for (0,1) and (1,0) mirror choices. Let us denote these functions as $P_{01}(V_E)$ and $P_{10}(V_E)$, respectively. Here, V_E is normalized by the mean side lobe power. In order to quantify the performance of Eve's attack, we assume that Eve has a prior knowledge of the distributions in Fig. 2(b). For each reading of her variable, Eve would guess that the particular bit was '0' if $P_{01}(V_E) > P_{10}(V_E)$, and vice versa. This decision criterion was shown to be optimal for binary data in the presence of noise [33]. In the ideal case of equal histograms, Eve would guess correctly only 50% of the bits, whereas if the histograms are entirely non-overlapping she can obtain 100% of the bits. In Fig. 2(b), $P_{01}(V_E)$ and $P_{10}(V_E)$ overlap only minimally, and Eve can correctly identify 95% of the bits.

We assume that Eve has a shot-noise limited detector, that her detection bandwidth optimally matches the spectral width of the side-lobes, and that she is using the entire rise time of the UFL to average out the measurement noise. We further assume that Eve can tap 10% of the UFL power undetected, even though our experiments show that such power losses can be identified by Alice and Bob. Subject to this model, simulations show that the mean value of $|V_E|$ is 20 dB above the shot noise equivalent power, and 30 dB above the level of the beat noise among the multiple UFL modes and the amplified spontaneous emission of the EDFAs. Therefore, an attack strategy based on the asymmetry of time resolved spectra is feasible and poses a relevant threat.

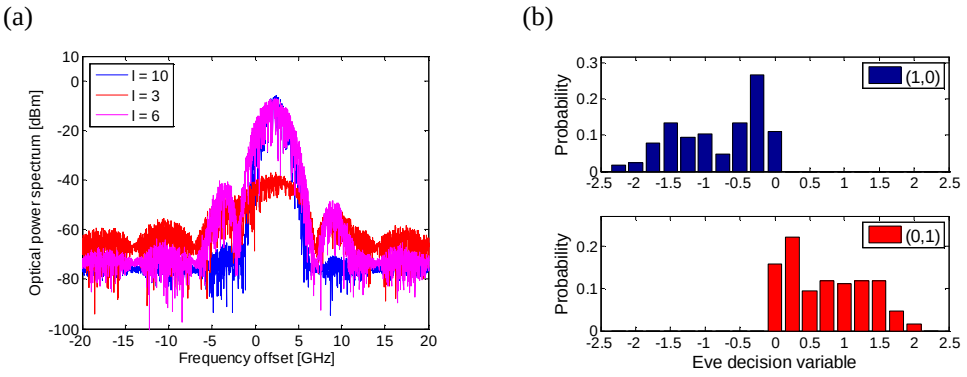

Fig. 2. (a). Simulated time resolved spectra of the UFL signal, with mirrors choice of (0,1) corresponding to a '0' bit. The spectra were calculated after 3 (red), 6 (magenta) and 10 (blue) one-way propagation cycles following the UFL switch-on. (b). Simulated histograms of the difference between the power in the left hand side lobe and that of the right hand side-lobe, 3 ms following switch-on of a 25 km long UFL. Using such time-resolved spectral measurements, Eve can recover 95% of the key.

In response to this adversary model, Alice and Bob can improve the security of the UFL engaging several strategies: First, a narrow-band, intermediate spectral filter, with a central frequency of f_c and a bandwidth narrower than $f_1 - f_0$, may be added in each terminal [28]. The intermediate filter would lower the side-lobe power significantly. The amplifiers gain can be reduced close to the lasing threshold, limiting the available power in the link to the necessary minimum. In addition, Alice and Bob may introduce random, uncorrelated variations to the peak reflectivity frequency of their mirrors, within a limited span surrounding

#100223 - $15.00 USD Received 15 Aug 2008; revised 15 Sep 2008; accepted 1 Oct 2008; published 3 Oct 2008

their nominal values of either f_0 or f_1. Such frequency variations introduce uncertainties to the UFL time resolved spectra. Finally, an additive, broadband optical noise source can be coupled to the output of the terminals, in order to conceal the residual side-lobes. Even though some of these measures were proposed in previous work [28], their impact on time resolved spectra based attacks was not quantified. Using these techniques, we demonstrate next that the difference between the side lobe powers could become either random, or too weak to detect.

The combination of lower EDFA gain, intermediate filters and random variations to the peak reflectivity frequencies leads to a substantial overlap between $P_{01}(V_E)$ and $P_{10}(V_E)$ (Fig. 3(a)). Due to the mirror frequencies variations, Eve can only recover 75% of the key bits. In addition, the ratio of mean $|V_E|$ to the shot noise equivalent power is reduced to 7 dB, and the ratio of mean $|V_E|$ to the optical beat noise is lowered to 6 dB. Eve can try to reduce her error ratio by moving her spectral filters further away from the main lobe, making V_E less susceptible to mirror frequency variations. However, in doing so Eve's measurement SNR would deteriorate even further. Eve's partial knowledge can be reduced further with cascading several intermediate filters inside the terminals. For example, Eve can only recover 60% of the key if two filters are used (Fig. 3(b)).

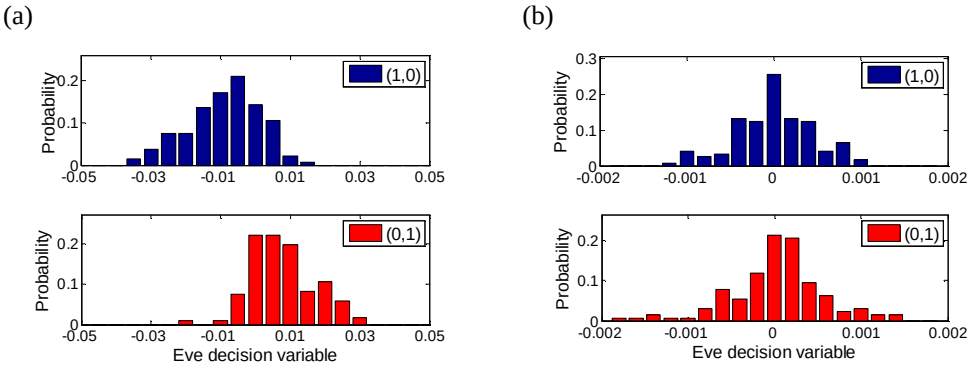

Fig. 3. Simulated histograms of the difference between the power in the left hand side lobe and that of the right hand side-lobe, 3 ms following the switch-on of a 25 km long UFL. The terminals include intermediate narrowband filters, with a 3 dB full width of 2.5 GHz and a 20 dB full width of 3.75 GHz. The small signal gain of the EDFAs was reduced to $10\log_{10} G_0 = 7\,\mathrm{dB}$. In addition, the peak reflectivity frequencies of the mirrors were randomly varied between bits, within a range of 2.5 GHz surrounding the nominal values. (a). One filter included in each terminal. (b). Two filters cascaded in each terminal

In the above numerical study, a bound on Eve's partial knowledge of the UFL generated secret key is established, for a particular adversary model. In setting this bound, it has been assumed that Eve is only restricted by signal uncertainties introduced by Alice and Bob, and by the fundamental detection noise. Eve's knowledge is strongly affected by the specific intermediate filter used by Alice and Bob. Perfectly sharp filters with a flat pass-band would reduce Eve's knowledge of the key to zero. As illustrated in the specific numerical example, Eve's knowledge can be restricted considerably with use of advanced, real-world achievable optical filters, such as auto-regressive moving-average filters [34]. Finally, privacy amplification techniques can be introduced to lower Eve's knowledge of the key even further [35, 36].

4. Experiment

The experimental setup used in our UFL system demonstration is shown in Fig. 4(a). The spectrally selective mirrors are implemented by fiber Bragg gratings (FBGs). During each bit exchange cycle, the peak reflectivity frequencies of Alice's and Bob's FBGs is tension-tuned

#100223 - $15.00 USD Received 15 Aug 2008; revised 15 Sep 2008; accepted 1 Oct 2008; published 3 Oct 2008

to either f_0 or f_1. The frequency separation $f_1 - f_0$ is 3 GHz. The terminals are connected by two 25 km long spans of standard single-mode fiber. Eve's tapping coupler is placed at the very beginning of the fiber span connected to Alice's terminal output port. Each terminal is buffered from the fiber spans by a 2X2 voltage controlled optical switch. When the switches are set to reflection mode, the UFL is effectively split into two local loops at the terminals, with no light transmitted outside the terminals. This mode of operation is used for individually tuning the peak reflectivity frequencies of the FBGs to f_0 or f_1, while literally leaving Eve "in the dark". Once the tuning is completed, the two switches are simultaneously set to transmission mode and the UFL is re-established. Light from a 30 nm wide, external noise source is coupled to the input of each EDFA, and the UFL is set to operate close to the lasing threshold. The peak reflectivity frequencies of both FBGs are randomly varied in between bits, within a range of ±500 MHz around either f_0 or f_1. The small signal gain, saturation power and noise figure of the terminals' EDFAs are 20 dB, 13 dBm and 4.5 dB, respectively. The nominal peak reflection wavelength, peak power reflectivity and full width at half maximum of the FBG mirrors are 1549.9 nm, 0.75 and 6 GHz, respectively.

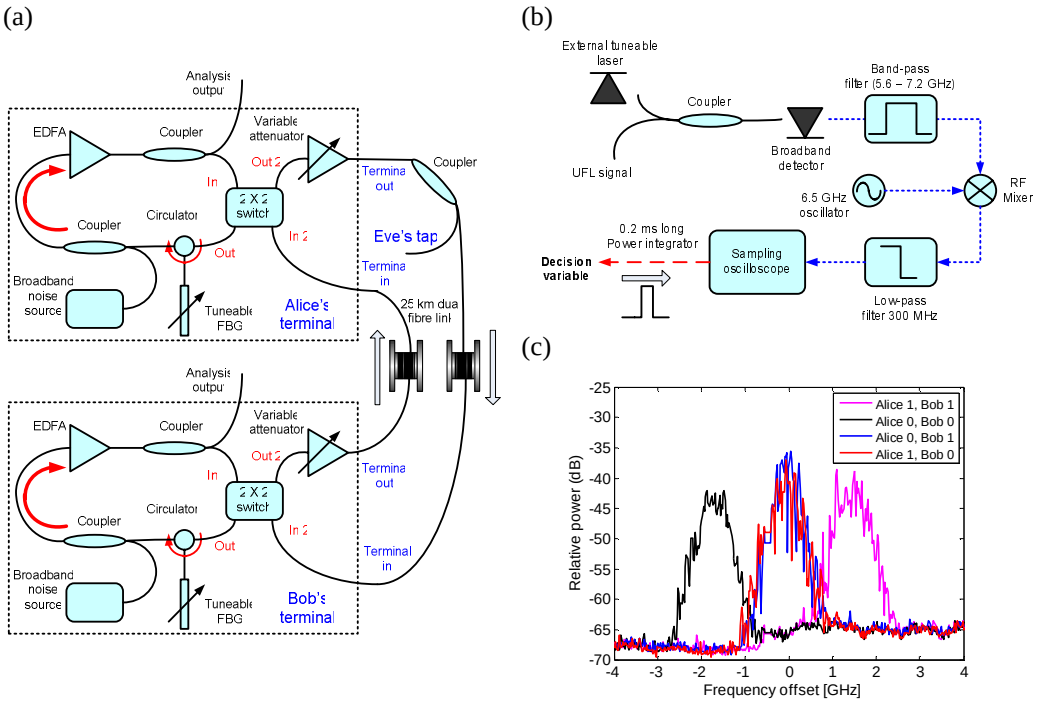

Fig. 4. (a). Experimental setup. (b). Detection scheme for calculating Alice, Bob, and Eve's decision variables. Black solid lines indicate optical signals. Blue dashed lines indicate RF electrical signals. The red line indicated off-line software processing of the sampled data. (c). Measured steady state spectra of the UFL subject to all four combinations of mirror choices.

Figure 4(b) shows the detection scheme used to generate the time dependent decision variables $V_{AB}(t)$ for Alice and Bob, and $V_E(t)$ for Eve. The UFL signal, emerging from either the analysis output ports of the terminals or from the eavesdropping coupler, is initially down-converted to the Radio Frequency (RF) domain through heterodyne beating with an external tunable laser of optical frequency f_{lo}. The difference in frequencies $f_{lo} - f_c$ is set to fall

#100223 - $15.00 USD Received 15 Aug 2008; revised 15 Sep 2008; accepted 1 Oct 2008; published 3 Oct 2008

within the bandwidth of a broadband detector. The detected photo-current is observed using an electrical RF spectrum analyzer, or processed further.

Figure 4(c) shows the measured spectra of the UFL at all four possible mirror choices. The spectra for (1,0) and (0,1) choices are indistinguishable. Such a spectral reconstruction, however, requires many seconds. More realistically, Alice, Bob and Eve have to identify the key bit within several round-trip propagation cycles. To that end, the detector output waveform is filtered using an RF spectral window, with a pass-band of 5.6 – 7.2 GHz (see Fig. 4(b)). This filter eliminates the baseband terms, whose spectral width is of the order of 1 GHz, from the detected signal. The signal at the filter output retains only the heterodyne beating term, the electrical power spectrum of which is proportional to the optical power spectrum of the UFL. That signal is down-converted again, using RF mixing with a voltage-controlled oscillator, of frequency $f_{VCO} = 6.5$ GHz. Finally, the signal is amplified and filtered by a 300 MHz-wide low-pass filter, and sampled by a digitizing oscilloscope. The sequence of spectral down-conversion and filtering stages is equivalent to the application of a 600 MHz wide optical band pass filter, centered at a frequency $f_{lo} + f_{VCO}$. Such a narrow filter is unavailable to us in the optical domain. By tuning f_{lo}, different portions of the UFL spectrum are analyzed separately.

For the generation of Alice or Bob's decision variable $V_{AB}(t)$, f_{lo} is tuned to satisfy $f_{lo} + f_{VCO} = f_c$. Figure 5(a) shows $V_{AB}(t)$ for two different key bits, one with complementary mirror choices by Alice and Bob, and the other with identical choices. When the mirror choices of Alice and Bob are complementary, the UFL central frequency is close to f_c and the magnitude of $V_{AB}(t)$ increases following the UFL switch-on. This build-up of the signal power is an indication of the secure generation of a single key bit. On the other hand, when Alice and Bob choose identical mirrors, the lasing frequency of either f_0 or f_1 is detuned from $f_{lo} + f_{VCO}$ by approximately 1.5 GHz, and no build-up is observed in $V_{AB}(t)$. Figure 5(b) shows the histograms of the root-mean-square (RMS) values of $V_{AB}(t = 3\ \text{ms})$, for 1000 random bits. As seen in the figure, a clear distinction between securely generated bits and those who should be discarded is established. The probability of Alice or Bob making a wrong decision is 0.006.

Eve's decision variable $V_E(t)$ is calculated by detuning the local oscillator from $f_c - f_{VCO}$ by a frequency offset Δf, in attempt to recover residual spectral asymmetries. Figure 6 shows the histograms of the RMS value of $V_E(t = 3\ \text{ms})$ for 1000 bits. As seen in the figure, the ranges of Eve's decision variable for (1,0) and (0,1) choice bits overlap almost entirely. Eve's error probability was 30-40% for all examined values of Δf and t. The range of Δf was restricted to ±1 GHz by the noise floor of our detection scheme.

#100223 - $15.00 USD Received 15 Aug 2008; revised 15 Sep 2008; accepted 1 Oct 2008; published 3 Oct 2008

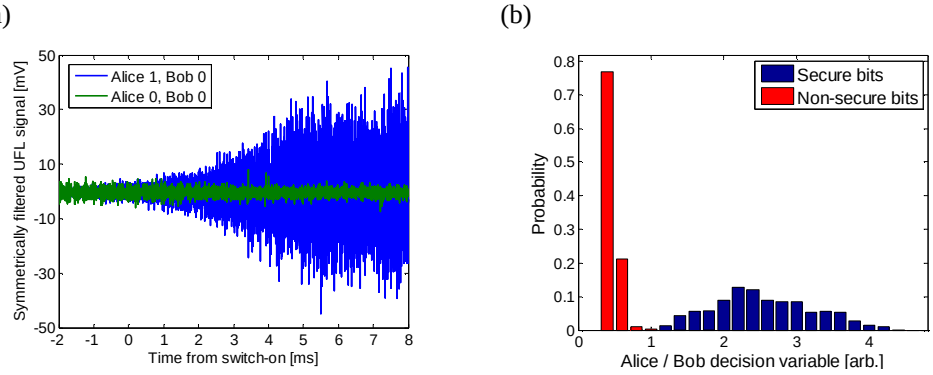

Fig. 5. (a). Alice and Bob's decision variable $V_{AB}(t)$, versus time following switch-on. Significant signal power is observed when Alice and Bob share a secure key bit (blue, complementary mirror choices), no signal is observed when information represented by mirror choices is non-secure (green, identical mirror choices). (b). Histogram of the RMS value of $V_{AB}(t)$, taken 3 ms after the switch-on of the UFL. Blue: the decision variable distribution for secure bits, (1,0) and (0,1) mirror choices. Red: the distribution for non-secure bits, (1,1) and (0,0) choices. Setting a threshold value for $V_{AB}(t)$, 994 out of 1000 bits are properly categorized.

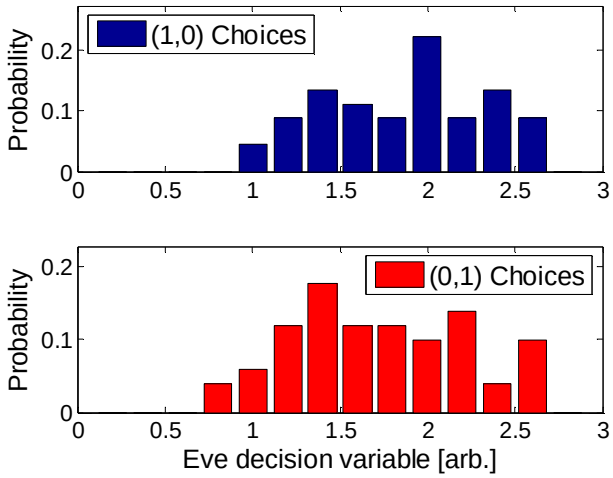

Fig. 6. Histogram of the RMS value of Eve's decision variable $V_E(t = 3\text{ ms})$, with a spectral detuning of Δf = 600 MHz Blue: 500 different '0' bits. Red: 500 different '1' bits.

5. Summary

In this work, the security analysis of the UFL system is extended to include an attack based on time resolved spectral asymmetries. This specific attack strategy takes advantage of an inherent weak point of the UFL approach - its spectrally asymmetric build up phase. Nonetheless, numerical simulations show that the security of the key generation can be maintained in the presence of this attack strategy through the inclusion of intermediate filters and random mirror frequency variations. Even with his strategy Eve can only marginally increase her knowledge of the key (~10%). The robustness of system against time / frequency domain attacks is also demonstrated in the proof of concept experiment.

The experimental key generation rate of 167 b/s is relatively modest, compared with that achieved in recent QKD demonstration [19, 20]. While the UFL system is at a disadvantage

#100223 - $15.00 USD Received 15 Aug 2008; revised 15 Sep 2008; accepted 1 Oct 2008; published 3 Oct 2008

over the relatively short distance of 25 km, its key generation rate decays only linearly with the link length, rather than exponentially [28]. The UFL key generation rate could be superior to that of QKD over very long links [28]. As a non-quantum based system, the usable distance of the UFL may be increased with off-the-shelf, inline EDFA modules. The duration of the UFL build-up period, however, would grow linearly with the length of the link. A longer link would therefore provide Eve with a longer averaging time for her measurements, and hence improve her SNR. In order to maintain a given security performance over a longer link, it is anticipated that Alice and Bob would need to employ more elaborate intermediate filters in their terminals, or cascade a larger number of such filters. While this requirement may raise the system cost and complexity, the solution paths are nevertheless feasible. Each terminal may also be equipped with a larger set of mirrors (more than two), enabling the generation of a multi-level key rather than a binary one.

Other intrusion strategies are of course possible. For example, Eve may try to actively probe the spectral reflectivity of Alice and Bob's mirrors, by injecting pulses at the terminal input and observing them at its output (see Fig. 4(a)). In propagation through the terminal, however, Eve's probe pulses are exposed to Alice and Bob. Due to the presence of intermediate filters and additive noise sources, Alice and Bob's signal to noise ratio in identifying such pulses will be far superior to that of Eve's measurements. Note also that the optical circulators prevent Eve from measuring counter-propagating signals (see Fig. 4(a)). In yet another potential approach, Eve may obtain a set of mirrors identical to those of Alice and Bob, and reconstruct a replica of the UFL terminals. Eve can try and direct a tapped portion of Alice's output signal, for example, into her own terminal, and introduce a secondary cavity. Studying the oscillations in this secondary cavity, Eve may gain information on Alice's choice of mirror. However, if Eve's choice of mirror does not match that of Bob, the UFL oscillations in the main cavity will be altered and expose her attack. In this respect, the UFL system is advantageous over chaos synchronization based systems [25]. In addition, the robust UFL signals are unlikely to be affected by neighboring wavelength division multiplexing channels, sharing the same fiber link.

From a theoretical standpoint, the UFL may be viewed as an optical implementation of an imperfect isotropic channel [32, 37]. An intruder into an isotropic channel can identify the sender of a public message with a probability ρ that is bound below 1 [37]. It was theoretically argued that the eavesdropper information gain in an imperfect isotropic channel can be made arbitrarily small [37]. Since the UFL concept is non-quantum based, setting an upper bound on ρ would be adversary model dependent. In this work, it has been demonstrated that ρ can be effectively bound below 1 when facing a time / frequency domain attack. However, the attack strategies surveyed above are by no means exhaustive. The quantitative analysis of substantially different attack approaches may have to start from first principles.

Much further work is required in order to fully quantify the extent of security provided by the UFL concept. Nevertheless, the extended analysis and the first experiment provide a major step in advancing this approach from an idea towards a system. The UFL would be considerably simpler to implement then QKD, and has potential to provide superior security to that of other classical optics approaches.

Acknowledgments

The authors thank Dr. Stephanie Wehner of the California Institute of Technology for her advice in the area of cryptography. A.Z. acknowledges the support of a post-doctoral research fellowship from the Center of Physics in Information (CPI), California Institute of Technology, and the Rothschild post-doctoral research fellowship from Yad-Hanadiv foundation, Jerusalem, Israel. J. Sch. acknowledges the support of the Advanced Communications Center, Tel-Aviv University, and the Horowitz Foundation.

#100223 - $15.00 USD Received 15 Aug 2008; revised 15 Sep 2008; accepted 1 Oct 2008; published 3 Oct 2008