Secure long-range and high bit-rate distribution of shared key using dark states ultra-long fiber laser (UFL

Jacob Scheuer[1],*
[1]School of Electrical Engineering, Tel-Aviv University, Ramat-Aviv, Israel 69978

ABSTRACT

We present and demonstrate a unique type of secure key distribution utilizing ultra-long fiber laser (UFL). A 500km long secure key distribution link based on Raman gain UFL is demonstrated experimentally. An error-free distribution of a random key with an average bit-rate of 100Hz between the users is demonstrated and the key is shown to be unrecoverable to an eavesdropper employing either time or frequency domain passive attacks.

1. INTRODUCTION

Many highly secure cryptographic systems utilize a secret key for ciphering the confidential information, where the key is shared only by legitimate users. The secure generation and distribution of this secret key are probably the weakest points of the shared-key encryption paradigm [1]. An attractive approach to overcome this problem is to employ physical layer protocols, where the most notably concepts are quantum cryptography schemes [2-4]. Quantum key distribution (QKD), based on the quantum mechanical properties of single photons, could theoretically provide unconditional security [2-4]. However, the practical implementation of QKD systems remains technologically challenging [4-6], and the key-establishing rates and ranges of such systems are inherently limited by channel loss and detector noise [4, 5]. Moreover, recent studies have shown that some commercial QKD systems can be completely broken by exploiting the non-ideal nature of their components [7]. Although the specific breach exploited in [7] was fixed, any practical QKD system essentially employs non-ideal components rendering it vulnerable to various attack strategies which do not necessarily target the quantum mechanical properties of the system. Here we demonstrate secure key distribution over a 500km long link using an alternative scheme which is based on establishing laser oscillation between the two communicating parties and realized using standard fiber-optic components. Each of the two users located at the ends of our Ultra-long Fiber Laser (UFL) [8-10] system places a randomly chosen, spectrally selective mirror at his/her end of a fiber laser, with the choice of mirrors representing a single key bit [11-]. This choice of mirror combination set the UFL in one of four possible states that exhibit different spectral and temporal properties. We demonstrate the ability of each user to extract the exact choice of mirrors, thus enabling the establishment of a shared key while an adversary tapping the link cannot reconstruct the generated key using neither temporal nor spectral attack strategies. The simplicity and the enhanced performance of this system render it a promising alternative for secure and practical key distribution in the optical domain.

2. THE UFL CONCEPT

Figure 1 depicts a schematic of the UFL based key distribution system (KDS). For simplicity, a ring laser configuration is realized although a Fabry-Perot configuration can be employed as well. The UFL-KDS consists of a long erbium doped fiber laser with Alice at one hand and Bob at the other. Alice and Bob both have an identical set comprising two spectrally dependent mirrors where each mirror in the set has its peak reflectivity at a different frequency: ω_A and ω_B. Alice and Bob can independently choose one of these mirrors and use it as a laser reflector at their end. If they both choose identical mirrors, a clear signal develops at ω_A (0, 0 state) or at ω_B (1, 1 state). However if one chooses complementary mirrors, (1, 0 or 0, 1 state), there is insufficient gain in the UFL to establish lasing. This is achieved by placing narrow bandwidth interferometeric filters in the cavity and a specific choice of mirror frequencies as outlined in the next section. In these cases, an eavesdropping adversary, Eve, can only detect noise and is unable to determine which user chose which mirror. The absence of signal allows for very fast measurements which give Alice and Bob an indication that the other party chose the complementary mirror, thus allowing them to agree on a key bit. For example, if Bob chooses ω_A and Alice chooses ω_B (0, 1 state), both set a logical key bit to "1". Similarly, if Bob chooses ω_B and Alice chooses ω_A mirror (1, 0 state), both set a logical key bit to "0". Continuous, synchronized selections of mirrors can be used to securely generate the entire key.

*kobys@eng.tau.ac.il; Phone: +972-3-6407559; Fax: +972-3-6423508; www.eng.tau.ac.il/~kobys/

Broadband Access Communication Technologies XII, edited by Benjamin B. Dingel,
Katsutoshi Tsukamoto, Spiros Mikroulis, Proc. of SPIE Vol. 10559, 1055902
© 2018 SPIE · CCC code: 0277-786X/18/$18 · doi: 10.1117/12.2295753

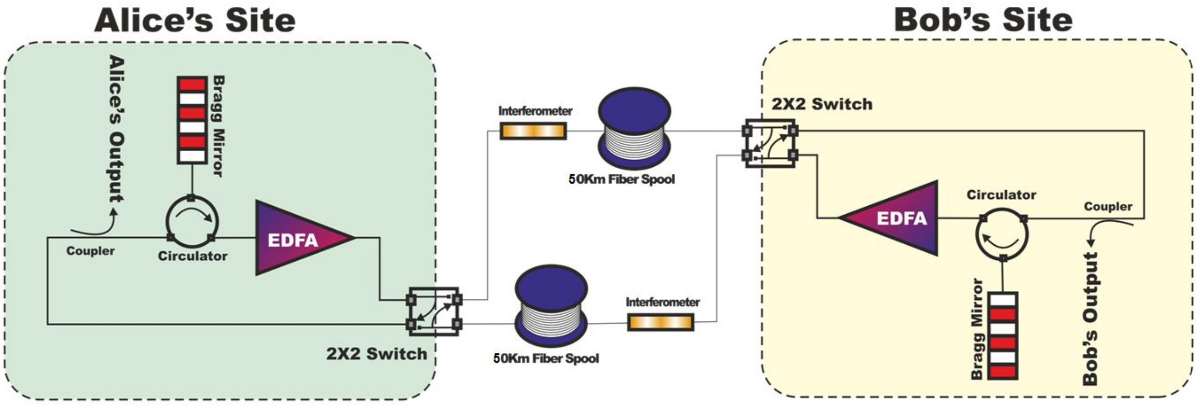

Figure 1. Schematic of the UFL key distribution system

3. EXPERIMENTAL RESULTS

For the practical realization of the UFL KDS we realized a ring fiber laser incorporating four Raman pump sources and two circulators at the end-user terminals. Each user terminal consists of a fast electro-optic switch allowing the user to connect one of two fiber Bragg gratings (FBGs) which constitute his/her choice of the key-bit. The FBGs in each set have a reflection band of ~0.05nm and their peak reflectivities are set to1555.15nm and 1555.55nm.

The most important aspects of any key distribution scheme are the security level, the range of the link, the key bit-rate and the bit error rate (BER). The last aspect is directly related to the attainable bit-rate because errors necessitate the incorporation of error correction mechanisms which reduce the bit-rate. Unsurprisingly, there aspects are not independent, and in many cases enhanced security is attained at the expense of shorter link rages and lower key bit-rates. The employment of privacy amplification, for example, directly sacrifices raw key-bits (and consequently the bit-rate) in order to reduce the information that can be extracted by potential eavesdroppers. Similar tradeoffs are exhibited by The UFL scheme and higher security level is obtained at the expense to the bit-rate.

Generally speaking, *passive* cryptographic attacks on the UFL systems can be classified as spectral, temporal or combined attacks. Such attack is characterized by tapping the optical signal in the laser and analyzing its properties in order to extract information on the exchanged bits. *Active* attack strategies, on the other hand, essentially *actively* tamper with the cavity and inject light into it. When dealing with classical encryption schemes, passive attacks are generally preferred as they are more difficult to detect than active ones.

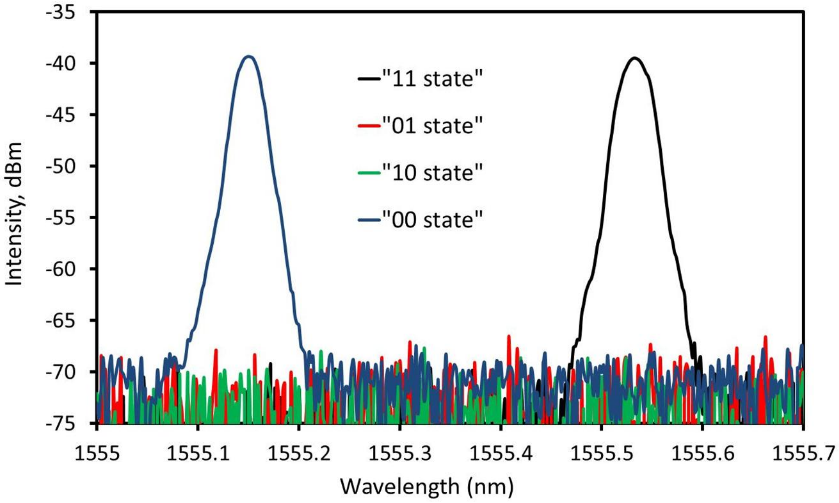

Figure 2. Real (blue) and imaginary (green) parts of the refractive index for subluminal (left) and superluminal (right) laser media.

Spectral attacks are based on attempts to extract information on the choice of mirrors by analyzing the spectrum of the signal in the UFL. In order to be resilient to such attack strategies, the spectra of the secure states must be practically indistinguishable. Figure 2 depicts the lasing spectra of the four possible states of the system, exhibiting lasing signal when both end mirrors are set to the same wavelength and none when the mirrors are different. Clearly, the spectra of the two secure states ('1, 0' and '0, 1') which are just optical noise are indistinguishable, thus not exposing the exchanged bit. Note, the spectra depicted in Fig. 2 was attained after long integration and averaging times in order to eliminate random noise which may obscure the signature of the mirrors choice made by the users. In a practical scenario, the adversary integration time is limited to a single bit-exchange time slot, rendering this task extremely difficult and challenging. Thus, a direct spectral analysis of the UFL lasing/non-lasing state does not constitute a useful attack strategy on the UFL.

The UFL system can also be attacked in the time-domain by monitoring the temporal evolution of the field in the cavity. Though might seem hopeless, as no signal is built up in the cavity in a secure bit state, it might be possible to extract the choice of mirrors by spectral-temporal analysis of the transients when the laser switches between secure and non-secure bits states. When the UFL is in a non-secure state, the choice of mirrors is known to everyone. Therefore, by tracing the spectral evolution of the field in a transition to and out of non-secure states it may be possible to obtain some information on the choice of mirrors. Nevertheless, this class of attacks can be prevented by introducing additional switches into the cavity which physically disconnect the user terminals from the main cavity fiber before the mirrors are switched [14].

The third class (combined spectral temporal attacks) is probably the most difficult one to defend against. This class of attacks can exploit the feedback mechanism incorporated into the UFL in order to detect the residual signal emerging from the users mirrors when the UFL is in one of the secure state. When the system is in a secure state, the noise emerging from the optical amplifiers is filtered by the users mirrors and although lasing is not built up, the signal emerging from the users' end terminals following the switch-on of the UFL contain the spectral signature of each user's choice of mirror. If Eve taps the signals close to the users' terminals, filter them at ω_0 and ω_1 and compares the intensities, she might be able to detect these signatures [14].

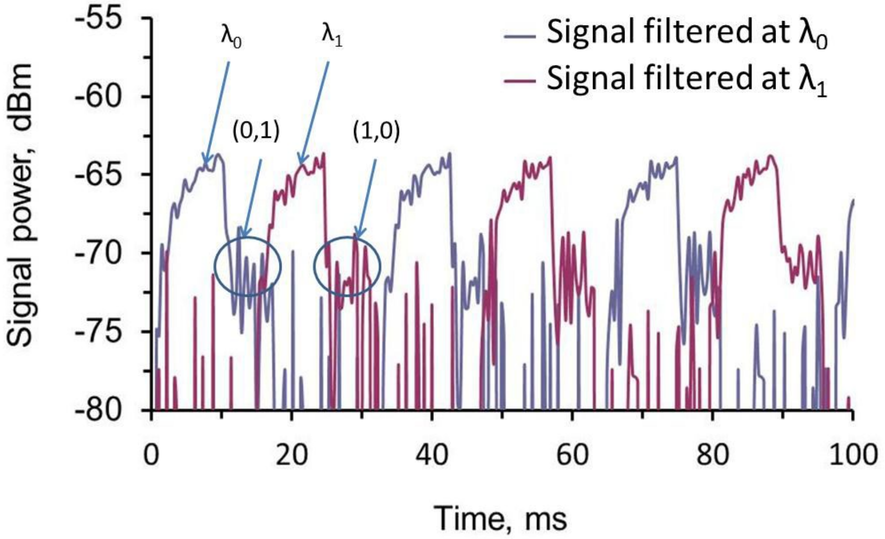

Figure 3. Time traces of the signal near Alice's terminal, filtered at ω_0 and ω_1 when the UFL is continuously switches between secure and non-secure states (reprinted from [13]).

Figure 3 depicts time traces of the signal near one of the terminals, filtered at ω_0 and ω_1 when the UFL is switched between secure and non-secure states [(0,0)→(0,1)→(1,1)→(1,0)]. When the UFL is in the secure (0, 1) state the signal at ω_0 is stronger than when it is in the secure (1, 0) state. Correspondingly, the signal at ω_1 is stronger when the UFL is in the secure (1, 0) state and fainter when it is in the secure (0, 1) state. Thus, with this approach the adversary can gain complete knowledge of the exchanged key. Overcoming this vulnerability requires reducing of the signal level in the secure-states below the detection limit of the adversary, by reducing the gain. The inset of Fig. 4 depicts the time trace of the signal filtered at ω_0 where the pump was reduced close to the lasing threshold level for the *non-secure* states. Clearly, now there is no difference between the levels of the measured signal at ω_0 when the UFL is any of the secure states. Note that Alice and Bob's ability to exchange the key is not affected because they only need to distinguish between the (lasing) non-secure states and the (non-lasing) secure states. The detection problem of the adversary is substantially more difficult than that of the users, which gives them a dominant technological lead.

Figure 4 depicts the dependence of the adversary probability to correctly guess an exchanged key-bit as a function of the UFL signal power when in a secure state. When the power level in the UFL is high, (strong pump), the probability of correctly guessing the key-bit is high, thus rendering the scheme non-secure. However, when the pump level is decreased, this probability o decreases rapidly reaching ~55% when the UFL signal level reaches -73dBm (close to lasing threshold). This is a relatively low success probability (compared to the ideal case of 50%) which can be further reduced by using techniques such as privacy amplification, etc. Ultimately, if the UFL gain is set such that the signal measured by Eve in the secure (non-lasing) state is below the shot-noise detection limit then the probability her success of correctly guessing the key-bit can be reduced to 50% (i.e. no knowledge of the key). In addition, amplified spontaneous emission noise sources can be used to symmetrize the noise spectrum on both sides and conceal the spectral response of the mirrors corresponding to the two different states.

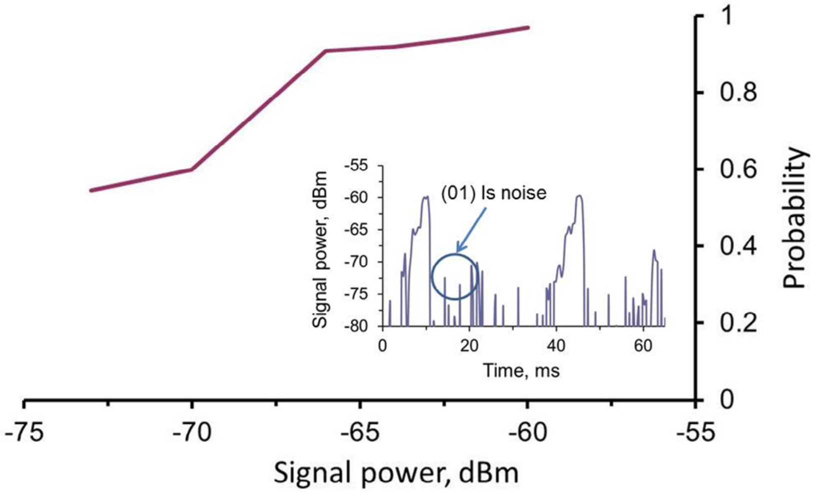

Figure 4. Success probability to guess the exchange bit as a function of the UFL power level; Inset – time trace of the signal near Alice's terminal, filtered at ω_0 when the power level of the secure states is reduced below the adversary detection limit. (reprinted from [13]).

4. CONCLUSIONS

Secure communication over 500km long UFL was experimentally demonstrated. The resilience to both spectral and temporal attack strategies was studied, demonstrating the high security level of the scheme. Key generation rates exceeding 100 bit/s are obtained in the present experimental scheme and can be substantially improved by employing fast electronic detection and analysis and by employing wavelength division multiplexing schemes. In addition, the key generation rate decreases linearly with the link length, thus making it highly attractive for long and secure communication links.

ACKNOWLEDGMENTS

This work was supported in part by the British Council BIRAX program and by Tel-Aviv University Cyber center.

REFERENCES

[1] S. Singh, The Code Book: The science of secrecy from ancient Egypt to quantum cryptography. London: Fourth Estate, (1999).

[2] C. H. Bennett, and G. Brassard, “Quantum public key distribution system,” IBM Tech. Discl. Bull. 28, 3153-3163 (1985).

[3] A. K. Ekert, “Quantum cryptography based on Bell’s theorem,” Phys. Rev. Lett. 67, 661-663 (1991).

[4] N. Gisin et al., “Quantum cryptography,” Rev. Modern Phys. 74, 145-195 (2002).

[5] 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).

[6] C. Gobby, Z. L. Yual, and A. J. Shields, “Quantum key distribution over 122 km of standard telecom fiber,” Appl. Phys. Lett. 84, 3762-3764 (2004).

[7] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, “Hacking commercial quantum cryptography systems by tailored bright illumination,” Nat. Photonics, vol. 4, no. 10, pp. 686–689, 2010.

[8] S. K. Turitsyn, J. D. Ania-Castañón, S. A. Babin, V. Karalekas, P. Harper, D. Churkin, S. I. Kablukov, A. E. El-Taher, E. V. Podivilov and V. K. Mezentsev, “270-km Ultralong Raman Fiber Laser”, Phys. Rev. Lett. 103, 133901 (2009).

[9] J. D. Ania-Castañón, T. J. Ellingham, R. Ibbotson, X. Chen, L. Zhang and S. K. Turitsyn, “Ultralong Raman Fiber Lasers as Virtually Lossless Optical Media”, Phys. Rev. Lett. 96, 023902 (2006).

[10] J. D. Ania-Castanon, V. Karalekas, P. Harperand S. K. Turitsyn, “Simultaneous Spatial and Spectral Transparency in Ultralong Fiber Lasers”, Phys. Rev. Lett. 101, 123903 (2008).

[11] J. Scheuer, and A. Yariv, “Giant fiber lasers: a new paradigm for secure key distribution,” Phys. Rev. Lett. 97, 140502 (2006).

[12] 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 (2008).

[13] A. El-Taher, O. Kotlicki, P. Harper, S. Turitsyn, and J. Scheuer, "Secure key distribution over a 500 km long link using a Raman ultra-long fiber laser", Laser Photonics Rev. 8, 436 (2014).

[14] O. Kotlicki and J. Scheuer, “Dark states ultra-long fiber laser for practically secure key distribution”, Quantum Inf. Process. 13, 2293 (2014).

[15] D. Bar-Lev and J. Scheuer, “Enhanced key-establishing rates and efficiencies in fiber laser key distribution systems“, Phys. Lett. A. 373, 4287 (2009).