Radio-Frequency Spectrum Coding in Ultra-Long Fibre Laser Based Cryptography

K. Krupa[1], A. Tonello[1], S. Boscolo[2,*], A. Barthélémy[1], V. Kermène[1], A. Desfarges-Berthelemot[1], B. M. Shalaby[1], S. K. Turitsyn[2], J. D. Ania-Castañón[3]

[1]Université de Limoges, XLIM, UMR CNRS 7252, 123 Av. A. Thomas, 87060 Limoges, France
[2]Aston Institute of Photonic Technologies, Aston University, Birmingham B4 7ET, United Kingdom
[3]Instituto de Óptica, IO-CSIC, C/ Serrano 121, Madrid, 28006, Spain
[*]Corresponding author: s.a.boscolo@aston.ac.uk

ABSTRACT

We propose a new approach for secret key exchange involving the variation of the cavity length of an ultra-long fibre laser. The scheme is based on the realisation that the free spectral range of the laser cavity can be used as an information carrier. We present a proof-of-principle demonstration of this new concept using a 50-km-long fibre laser to link two users, both of whom can randomly add an extra 1-km-long fibre segment.

Keywords: fibre lasers, fibre optics communications, optical security and encryption.

1. INTRODUCTION

The intrinsic low linear losses of optical fibres at telecommunication wavelengths and the availability of lumped or distributed devices for optical amplification enable fibre lasers with cavity length of several hundred kilometre scale [1]. The feasibility of extending the laser cavity over the whole communication link connecting the two parties, forming an ultra-long fibre laser (UFL), has raised ground-breaking possibilities in communications and particularly in secure communications. An innovative concept of a key-distribution system based on an erbium-doped or Raman gain UFL has been recently proposed and demonstrated [2-5]. In this scheme, each of the two users (conventionally called Alice and Bob) places a randomly chosen, spectrally selective mirror at his/her end of the fibre laser, with the two-mirror choice representing a key bit. The security in this scheme stems from lasing states that have lost distinguishability, from the perspective of a potential eavesdropper, because of their symmetry. The key is coordinated from dynamic changes of the laser Bragg reflectors and from lasing state characterisation by the legitimate end users. While the classical UFL scheme does not ensure the same security as ideal quantum key distribution, its prospective application offers a practical and secure way to distribute secret keys, in which security is set from technological bounds. The quest for a simple classical key distribution scheme, employing standard, readily available components and facilitating long-link ranges and high bit rates, still remains relevant.

In this work we describe a new way of exchanging a secret key over an UFL link, which relies on random changes of the free spectral range (FSR) of the laser cavity rather than on random changes of the cavity losses [6]. Consequently, unlike the previously proposed UFL scheme, our laser is always above the lasing threshold, and operates in alternating rapid transient and steady-state modes keeping the same optical bandwidth. The key idea of our work is based on the simple observation that the FSR of a laser cavity can be used as an information carrier and, hence, processing the FSR traces can make the information bits available all along the cavity. Measurement of the few-kilohertz-wide FSR can be performed, e.g., by a real-time analysis of the electrical signal supplied by a photodiode that detects one of the laser outputs. Specifically, in this scheme, referred to as radio-frequency shifting key exchange (RFSKE), the FSR is switched between different values by simply adding or subtracting fibre segments of given lengths to or from the cavity. This can be easily implemented by using 1×N switches with N different optical fibre paths so to change the cavity length in a predesigned way. In our implementation N=2, and two out of four possible combinations of cavity length choices give the same value of FSR, which entails the possibility of having an undetectable bit of information. Instead of a random insertion of optical band-pass filters (BPFs), here we use the periodic filtering of the cavity to modify the laser spectrum in a way that it carries the information bits itself. The principle of switching the laser frequency, for instance, by changing the laser cavity length, is a known technique to induce coherent optical transient phenomena in metrology for molecular diagnostics [7,8]. A similar scenario naturally occurs in frequency-shifted feedback lasers, where the cavity is modified during the course of time by an inline frequency shifter [9,10]. Note also incidentally that the idea of secret key exchange using a combination of short and long path lengths reminds a quantum optics cryptographic scheme known as the Franson interferometer [11]. However, to the best of our knowledge, this is the first time that the concept of FSR coding for secret key exchange is considered in the context of UFL cryptography.

2. OPERATION PRINCIPLE AND EXPERIMENTAL SET-UP

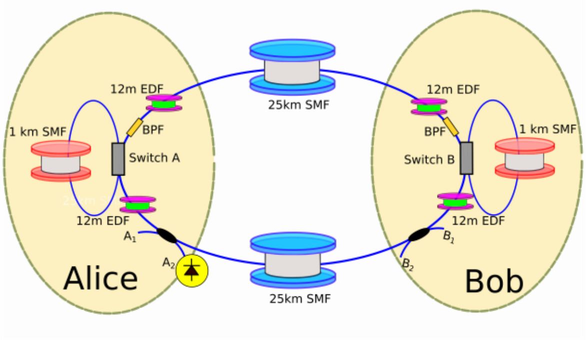

Figure 1. Schematic of the experimental set-up. BPF, band-pass filter; EDF, erbium-doped fibre; SMF, single-mode fibre.

Figure 1 depicts a schematic of the UFL-based RFSKE system. The system consists of a bidirectional, 50-km-long ring fibre laser, in which in order to exchange a key bit, Alice and Bob independently choose to add a 1-km-long segment of fibre or let the cavity length unchanged, with the corresponding indicator functions being '1' and '0', respectively. Both Alice and Bob have their own random number generators to select one of the two possible options each time. Thus, the laser has a length determined by the combination of users' random choices and taking on the values: 50 km (0,0 state), 51 km (0,1 or 1,0 state) and 52 km (1,1 state), and hence, random is also the FSR. A potential eavesdropper, Eve, measuring the FSR in the (0,0) or (1,1) state can easily infer the corresponding cavity length choices and therefore, the bits in these cases are rejected. However, in the (1,0) and (0,1) states leading both to the same FSR, Eve is unable to determine from a measure of FSR which user chose which length, thus rendering the key-bit exchange secure. Alice, knowing her own length choice, can determine the complementary choice of Bob, and vice versa. The two of them can therefore assign, for example, a logical 'H' to the (1,0) state and a logical 'L' to (0,1). Once the distinguishable states (0,0) and (1,1) are removed, the remaining sequence of states (0,1) and (1,0) will represent a random sequence of binary symbols 'H' and 'L', which can then be used as a key for encrypting and decrypting a message exchanged between Alice and Bob over a standard transmission system.

The two single-mode fibre drums in Fig. 1 play the role of an existent public infrastructure. Each of the two bays, called Alice and Bob, provides two allowed access points to the bidirectional ring through 90/10 tap couplers with the terminals A_1, A_2, and B_1, B_2. Each bay has two 12-m-long segments of erbium-doped fibre (EDF) that are core pumped by a 980-nm diode. A 5-nm-wide optical BPF centred at the fixed wavelength of 1559 nm is placed in the middle of each bay. These filters only limit the spectral window in use and do not play any direct role in coding. The optical power at the laser output ports is approximately 80 μW when the laser is operated slightly above threshold. An electro-optic ceramic switch is placed close to each fixed filter. A transistor-transistor logic signal can reconfigure the laser by changing the state of the switch from *bar* to *cross* mode. In *bar* (0) mode, the switch simply connects the main input to the main output; in *cross* mode (1), the switch adds an extra propagation over 1 km of fibre in a 'loop in loop' configuration. A computer-generated random number is sent to a microprocessor unit (Arduino DUE) that controls the state of both switches via two logic level shifters. The detection of the laser output is ensured by a 1-GHz indium gallium arsenide photodiode connected to the analogue input of the same microprocessor unit that provides a 12-bit analogue to digital conversion. The numerical Fourier transform is then computed on the computer to obtain the FSR.

3. RESULTS AND DISCUSSION

The left panel of Fig. 2 depicts the optical spectra of the laser for the four possible states as obtained from measurements taken close to the lasing threshold and for two distinct laser central wavelengths. A common feature of all spectral profiles is a sharp peak with a 3-dB width of 0.11 nm and located at 1560.5 nm or 1560.7 nm. Importantly, the (0,1) and (1,0) states have closely similar spectra (subplots c) and d)). This would make it difficult for Eve to deduce the states by measuring the optical spectrum. To reduce the unavoidable irregularities in the spectra due to the different spectral responses of the switches at the different driving voltages, we included an additional tuneable 100-GHz optical BPF into the laser cavity. This filter simply makes the optical spectra more similar to each other and does not play any role in information coding. The laser system was on hold during the time of the optical spectrum analysis. The filter's inclusion made it possible to manually change the central wavelength of the laser and thus, show that in principle our laser can work at different wavelengths. In the application of our FSR-based key exchange protocol we used electronic control to keep the laser central wavelength fixed.

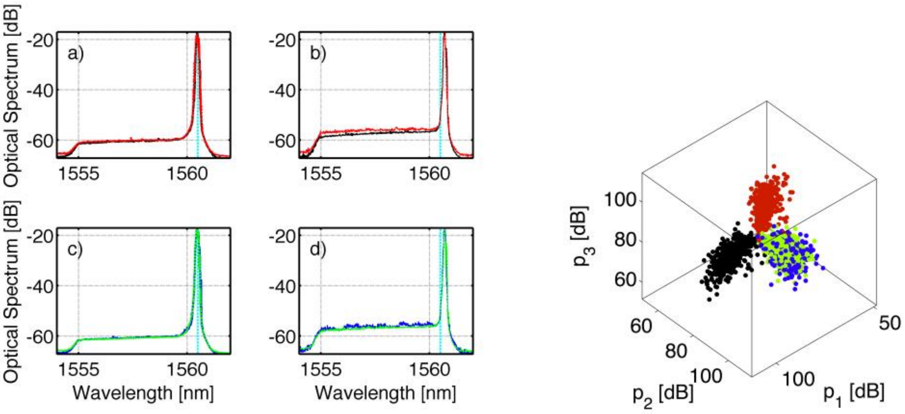

Figure 2. Left: Optical spectra of the ultra-long fibre laser for the four states and for two possible central wavelengths: 1560.5 nm (subplots a) and c)) and 1560.7 nm (subplots b) and d)). The vertical line shows the 1560.5-nm wavelength for ease of reading. The black curves are for state (0,0), the red curves are for state (1,1), the blue curves are for states (0,1) and the green curves for state(1,0). Right: Example of constellation diagram summarising the output readings of 2000 experimentally generated random states of the laser. The red dots are for state (1,1), the black dots are for state (0,0), the blue dots are for state (0,1) and the green dots are for state (1,0). Adapted from Ref. 6.

The crucial point of the proposed RFSKE scheme lies in a fast detection of the FSR through the analysis of the electrical signal emitted by a photodiode. It is useful to recall here that the time-domain analysis of the intensity of a light field $I(t)$ relies on the acquisition of the fourth-order correlation function of the field (see, e.g., Ref. 9). We note that a change in FSR originating in a change in cavity length is reflected by a slight frequency shift of a component or tone of the radio-frequency spectrum of the laser. Therefore, to shorten the acquisition time and/or to facilitate the reading of the laser states, one can inspect those tones that are located at frequencies multiple of the basic FSR: the higher the multiple order the larger the tone's frequency shift. Because the laser radio-frequency spectrum takes the form of a frequency comb, when the frequency shift of a given tone exceeds the tone's bandwidth, the corresponding change in cavity length can easily be detected. However, the frequency detuning being measured should not exceed half of the FSR; this situation is somewhat similar to that entailed by a recently proposed scheme of dual-comb spectroscopy [12]. In our proof-of-principle experiment, we analysed the electrical signal from the photodiode with a radio-frequency spectrum analyser, and we found that the FSR was approximately 4-kHz wide. By looking at the radio-frequencies close to 20 kHz, which represents a multiple of five of the FSR, we observed that a change of 2% in laser length (1 km) brings a frequency shift of 0.4 kHz, which is a multiple of five of a 2% change in FSR. This confirmed the point made above. The proposed RFSKE protocol enables one to write bits of information into physical hertz of the spectrum with an efficiency that can be higher than that of laser cryptographic systems based on a random hopping of the laser optical central wavelength [3]. In our implementation of the scheme, the numerical Fourier transform is used to detect the hopping in central frequency arising from a change in cavity length. Since the state of the laser is stored in an equivalent radio-frequency bandwidth, with the RFSKE scheme, the available optical bandwidth can be fully utilised to make multiple pairs of users sharing a common fibre link and using different laser channels work in parallel. The results in the left panel of Fig. 2 show that the laser central wavelength can be easily modified by fine tuning of the 100-GHz filter. This confirms the potential of extending the proposed RFSKE scheme to a parallel cascade laser configuration in which each of M lasers operates at a different central wavelength: Alice and Bob would then operate M subsystems centred at different wavelengths and connected to the common public network fibre by multiplexers/de-multiplexers. The transmission speed would increase by a factor of M in such case.

The buffer of our analogue-to-digital converter has a size of 20 000 sampled values, corresponding to a temporal window of 20 ms. In principle, such a temporal window would allow for random generation and reading of 50 laser states per second, although one has to set apart some time for the laser transients (the round trip light time in the cavity is 0.24 ms). The principle of our coding/decoding process was tested by randomly generating 2000 laser states and reading the electrical output signal from the photodiode. The decision step is also of critical importance for a fast evaluation of the FSR. Once the 20 000 samples were received and Fourier transformed, the strategy that we adopted to detect the FSR was again based on monitoring the fifth harmonic of the signal spectrum, as this proved to be effective in our case. We evaluated the spectral intensities p_1, p_2 and p_3 of the signal $I(t)$ at the respective frequencies 20.4 kHz, 20 kHz and 19.6 kHz, thereby generating a triplet of values (p_1, p_2, p_3) for each data acquisition. The compliance bandwidth of the spectral profiles was 0.2 kHz. Each reading and signal processing operation can be represented as a point in the three-dimensional space of the (p_1, p_2, p_3) parameters which plays the role of a constellation diagram, as shown in the right panel of Fig. 2. Once the three values are calculated for each reading, if the condition $p_1>p_2>p_3$ is satisfied, a decision is made in favour of the longest possible laser cavity (0,0 state). Similarly, the condition $p_1<p_2<p_3$ identifies the shortest cavity (1,1 state). The two states (0,1) and (1,0) are in principle indistinguishable since they both attain the same frequency position. In our measurements, we kept track of the random number generated by the computer so that to detect wrong decisions. Two thousand laser states were generated randomly, and their signatures could be recognised from the FSR and the known choices of Alice and Bob in the 98.95% of cases. The results obtained are summarised in the right panel of Fig. 2. Different laser states are rendered with points of different colours by the random number generator: black indicates the (0,0) state, red is for the (1,1) state, blue is for (0,1) and green is for (1,0). The distinguishability of the symbols at the receiver is visualised in this constellation diagram by the net distinction among the point clouds of the same colour (corresponding to the same switch settings). An error would be visualised in the diagram as a point of a different colour from the surrounding cloud. The indistinguishability of the secure bit states from the perspective of an external eavesdropper is visualised by an overlap of the blue and green clouds: in this volumetric region the probability of Eve confusing the (0,1) state with the (1,0) state is very close to the ideal case of 50% (i.e., no knowledge of the key). Such a probability is drastically reduced for the legitimate users since they can keep track of their own random choice; this fact is represented in the diagram by the coexistence of the two colour clouds in the same volume. We would like to note that the time-domain fluctuations of the laser induce changes of several orders of magnitude in the elements of the triplets, and such values are plotted on a logarithmic scale.

4. CONCLUSIONS

We have described a new approach to secret key exchange for laser cryptography, and carried out a proof-of-principle demonstration of this new concept. We have experimentally demonstrated how the radio-frequency spectrum of an UFL can be used to establish a secure communication between two parties. Although the demonstrated classical cryptographic scheme cannot ensure the same security level than that provided by idealised quantum key distribution systems, we believe that it represents an interesting trade-off solution to enforce the security of communication systems beyond the standard software protocols and employing conventional, off-the-shelf components. Limitations of the current implementation and future perspectives will be discussed at the conference. Our results open up new avenues to studies involving non-traditional schemes for secure communications. Furthermore, the radio-frequency monitoring of an UFL can be of interest for applications in diverse research fields, such as in distributed sensing.

ACKNOWLEDGEMENTS

This work was supported by the French National Research Agency (grants LABEX SIGMALIM and ANR 08-JCJC-0122 PARADHOQS), the European Research Council (project ULTRALASER), the Leverhulme Trust (grant RPG-278) and the Spanish MICINN project TEC2011-27314 (RAMAS). We also acknowledge support by the XLIM Institute (grant VIP2013).

REFERENCES

[1] J.D. Ania-Castañón *et al.*: Ultralong Raman fiber lasers as virtually lossless optical media, *Phys. Rev. Lett.*, vol. 96, pp. 023902(4), 2006.
[2] J. Scheuer, A. Yariv: Giant fiber lasers: A new paradigm for secure key distribution, *Phys. Rev. Lett.*, vol. 97, pp. 140502(4), 2006.
[3] A. Zadok *et al.*: Secure key generation using an ultra-long fiber laser: Transient analysis and experiment, *Opt. Express*, vol. 16, pp. 16680-16690, 2008.
[4] D. Bar-Lev, J. Scheuer: Enhanced key-establishing rates and efficiencies in fiber laser key distribution systems, *Phys. Lett. A*, vol. 373, pp.4287-4296, 2009.
[5] A. El-Taher *et al.*: Secure key distribution over a 500 km long link using a Raman ultra-long fiber laser, *Laser Photon. Rev.*, vol. 8, pp. 436-442, 2014.
[6] A. Tonello *et al.*: Secret key exchange in ultra-long lasers by radio-frequency spectrum coding, *Light Science Appl.*, vol. 4, e276, 2015; doi:10.1038/lsa.2015.49.
[7] R.G. Brewer, A.Z. Genack: Optical coherent transients by laser frequency switching, *Phys. Rev. Lett.*, vol. 36, pp. 959-962, 1976.
[8] A.Z. Genack, R.G. Brewer: Optical coherent transients by laser frequency switching, *Phys. Rev. A*, vol. 17, pp. 1463-1474, 1978.
[9] L.P. Yatsenko, B.W. Shore, K. Bergmann: Coherence in the output spectrum of frequency shifted feedback lasers, *Opt. Commun.*, vol. 282, pp. 300-309, 2009.
[10] K. Krupa *et al.*: Four-wave mixing in nonlinear fiber with two intracavity frequency-shifted laser pumps, *IEEE Photon. Technol. Lett.*, vol. 24, pp. 258-260, 2012.
[11] J.D. Franson: Bell inequality for position and time, *Phys. Rev. Lett.*, vol. 62, pp. 2205-2208, 1989.
[12] T. Ideguchi *et al.*: Adaptive real-time dual-comb spectroscopy, *Nat. Commun.*, vol. 5, article n. 3375, 2014.