Secure key distribution using an ultra-long fiber laser with bi-directional EDFA

Beatriz Soares[1*], *Ariel* Guerreiro[1,2], and *Orlando* Frazão[1]

[1]INESC TEC, Institute for Systems and Computer Engineering, Technology and Science, Rua do Campo Alegre, 687, 4150-179 Porto, Portugal
[2]Faculdade de Ciências da Universidade do Porto, Rua do Campo Alegre, 687, 4150-179 Porto, Portugal

Abstract. In this paper we describe the implementation of a secure key distribution system based on an ultra-long fiber laser with a bi-directional erbium doped fiber amplifier. The resilience of the system was tested against passive attacks from an eavesdropper, having been observed a similarity in spectrum for both secure configurations of the system.

1 Introduction

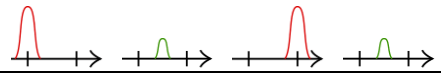
Many encryption protocols require the transmission of a secret key between two parties before communication between them can take place. The distribution of this key constitutes one of the weakest links in this type of communication system and is the driving force for the development of unconditionally secure key distribution schemes based on fundamental properties of quantum mechanics. With this in mind, a system based on a ultra-long fiber laser (UFL) that utilizes standard fiber optic components was proposed by Scheuer *et al.* [1]. This scheme, unlike the ideal implementation of QKD, is not unconditionally secure, relying instead on the technological difficulty of an eavesdropper to get access to the shared key. Such unconditional security has not, however, been a necessary pre-requisite for many encryption schemes, such as public key encoding schemes, which rely on the computational difficulty on part of the eavesdropper, rather than an absolute security proof.

In this paper we first discuss the principle of operation of the UFL key distribution system, next we present and analyse the results obtained for our own experimental implementation of the system, and finally, we discuss possible improvements and vulnerabilities of the protocol, both in general and to our setup, in particular.

2 Principle of operation

The setup used for the UFL key distribution system (KDS) is shown in figure 1. The scheme consists of a long erbium doped fiber laser that connects two users, Alice and Bob, positioned at opposing sides of the laser. Each user possesses an identical mirror which can be selected to have its peak reflectivity at two different frequencies, which can be assigned as f_0 and f_1. For the exchange of a single key bit, Alice and Bob choose, randomly and independently, one of these mirror states to reflect at. If both of them make the same choice of mirror state, there will be enough gain in the cavity to surpass the lasing threshold and a clear signal at either f_0 or f_1 will form, thus giving a potential eavesdropper (Eve) an easy access to the arrangement of both mirrors. However, if Alice and Bob choose different mirrors states, only a small signal at $f_c = 1/2\,(f_0 + f_1)$ will develop, and Eve will not be able to easily determine the exact configuration of mirror states used, only that Alice's and Bob's differ from one another. Thus, it can be assigned, for example, a bit value of '0' to the configuration of (Alice: f_0; Bob: f_1) and a bit value of '1' to the configuration of (Alice: f_1; Bob: f_0), which will allow Alice and Bob, knowing their own mirror state, to deduce the others choice, while preventing Eve getting access to the exchanged key bit. This protocol for key distribution using UFL is summed up in table 1.

Table 1. Protocol for a key distribution system using an UFL. Only when Alice and Bob choose different mirror states are the bits kept in order to obtain the sift-key.

Alice's mirror	0	0	1	1
Bob's mirror	0	1	1	0
UFL signal				
Sift-key	-	0	-	1

3 Experimental Implementation

3.1 Experimental Setup

The experimental setup is shown in figure 1 (a).

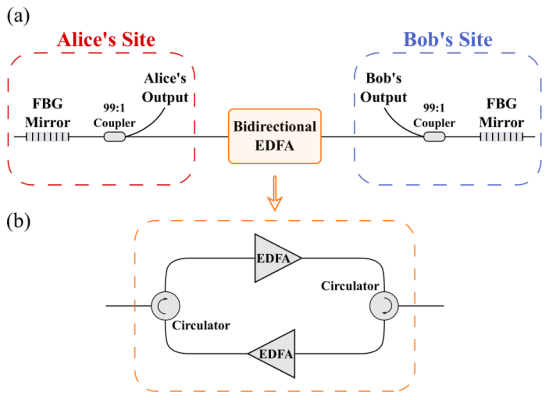


Fig. 1. (a) Lab setup and (b) internal schematic of the bidirectional EDFA utilized.

* Corresponding author: beatrizgsoares97@gmail.com

It consists of two separate users, Alice and Bob, each with a fiber Bragg grating (FBG) mounted on a translation stage, allowing for the manual tuning of their peak reflectivity wavelengths by application of mechanical tension. Each user was further equipped with a 99:1 coupler in order to perform measurements on the cavity's signal. The gain of the system was provided by a customized bidirectional EDFA, whose internal schematic is depicted in figure 1 (b).

It consists of two circulators and two conventional EDFAs, i.e. an erbium-doped fiber and a co-directional pump, with each pump being able to be independently controlled by separate voltage sources. To perform the measurements required for the experiment, an optical spectrum analyser (OSA) model "AQ6370D" with wavelength range of 600 nm to 1700 nm from Yokogawa was used.

3.2 Experimental Results

The obtained spectrum of the four possible states of the UFL (read in Alice's output) are depicted in figure 3. The pump powers to the EDFA were chosen so the non-secure states were obtained near the lasing threshold. While the spectra for the non-secure states presents distinct well defined lasing peaks ($\lambda_{0,0}$=1561.098 nm at -17.703 dBm and($\lambda_{1,1}$=1561.484 nm at -18.280 dBm), the spectra for the secure states, (1,0) and (0,1), resemble optical noise and are thus difficult to distinguish. As expected, Eve would not find it technologically easy to access Alice's and Bob's mirror choice.

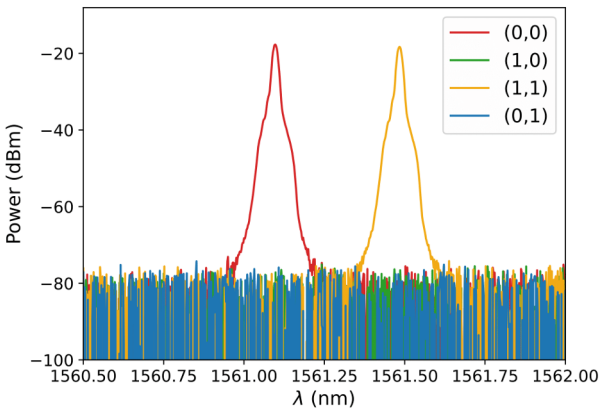


Fig. 2. Optical spectrum of the four states of the UFL-KDS.

4 Discussion

4.1 Improvements

The process of increasing the bit-rate of the setup, both to generally speed up the process and to give Eve less time to measure the cavity signal, is limited by the time required by Alice and Bob to identify the UFL state. That means the signal has to have enough time to pass through both mirrors and build up to a level capable of distinguishing a lasing from a non-lasing state. This translates to approximately 1.5 round trips [2], which results in a maximum frequency of $f = c/3dn$ bps, where d is the length of the link and n the refractive index of the fiber. This gives a maximum frequency in the order of 10^2 bps for a 100 km long link. Furthermore, the efficiency of a basic UFL protocol is only half of the total rate, as on average the number of secure bits sent will only be half of the total number. To address this relatively low effective bit-rate, modifications to the basic protocol have been proposed and numerically tested by Bar-Lev et al. [3], including using wavelength division multiplexing (WDM), or improving the 50% efficiency of the secure bit transmission.

4.2 Vulnerabilities

As previously discussed, even in its theoretical ideal case, the UFL protocol is still susceptible to attacks, relying instead on the technological difficulty of an eavesdropper to distinguish between different secure states. Some types of vulnerabilities not explored in this paper are those posed by active (as opposed to passive) attacks. Although they have been dismissed by most studies on the subject [1], [2], the paper by Garcia-Escartin et al. [4] suggests they need to be considered as important threats. The proposed attack is reliant on the ability of Eve to introduce a probing signal on the cavity, below the noise floor. She achieves this by spectrally broadening the signal using modulation, so that the total power is stretched out over the bandwidth of interest. While possible countermeasures were also proposed, to our knowledge, they have yet to be tested, and correspond to important future work in the study of the reliability of the UFL protocol.

5 Conclusions

Practical limitations of QKD have motivated searches for alternative, classically based solutions to key distribution. Accordingly, a system based on an ultra-long fiber laser has been proposed in previous studies. In this paper we discussed the basic operation principle of the UFL protocol, implemented our own UFL setup with a bidirectional EDFA and verified its feasibility as a secure key distribution system. Lastly, we discussed some possible improvements and vulnerabilities of the UFL protocol.

As the future of the UFL protocol goes and seeing most studies have been focused on passive attacks, it is important that the susceptibility to active attacks be fully tested to evaluate the viability of the protocol.

References

1. J. Scheuer, A. Yariv, Phys. Rev. Lett **97**, 1-4 (2006)
2. O. Kotlicki, J. Scheuer, Quantum Inf. Process **13**, 2293–2311 (2014)
3. D. Bar-Lev, J. Scheuer, Phys. Lett. Sect. A Gen. At. Solid State Phys. **373**, 4287–4296 (2009)
4. J. C. Garcia-Escartin, P. Chamorro-Posada, IEEE J. Sel. Top. Quantum Electron. **24**, 1–9 (2018)