photonics

MDPI

Article

Resilience to Passive Attacks of a Secure Key Distribution System Based on an Ultra-Long Fiber Laser Using a Bi-Directional EDFA

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

[1] Institute for Systems and Computer Engineering, Technology and Science (INESC TEC), Rua do Campo Alegre, 687, 4150-179 Porto, Portugal
[2] Faculdade de Ciências, Universidade do Porto, Rua do Campo Alegre, 687, 4150-179 Porto, Portugal
* Correspondence: orlando.frazao@inesctec.pt

Abstract: In this paper, we study 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. A similarity was observed in the spectra for both secure configurations of the system and no signature that would allow an eavesdropper to obtain the secure state of the system was observed during the state transitions.

Keywords: UFL; SKD; bi-directional EDFA

Citation: Soares, B.; Robalinho, P.; Guerreiro, A.; Frazão, O. Resilience to Passive Attacks of a Secure Key Distribution System Based on an Ultra-Long Fiber Laser Using a Bi-Directional EDFA. *Photonics* **2022**, *9*, 825. https://doi.org/10.3390/photonics9110825

Received: 3 October 2022
Accepted: 1 November 2022
Published: 3 November 2022

1. Introduction

Many encryption protocols require the transmission of a secret key between two parties before communication between them can take place [1]. 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 the fundamental properties of quantum mechanics [2–4]. Although quantum key distribution (QKD) provides theoretically unconditional security [5], its practical implementation remains technologically challenging [6–10] and the search for classically based alternatives continues to be relevant [11–13]. Such methods include the synchronization of lasers in the chaotic regime [14,15], optical code division multiple access [16,17], and Johnson-like noise over electrical transmission lines [18].

In this paper, we focus our attention on a system based on an ultra-long fiber laser (UFL) that utilizes standard fiber optic components proposed by Scheuer et al. [11]. This scheme, unlike the ideal implementation of QKD, is not unconditionally secure, relying instead on the technological difficulty of an eavesdropper's ability to gain access to the shared key. However, such unconditional security has not been a necessary pre-requisite for many encryption schemes, such as public key-encoding schemes, which rely on the computational difficulty on the part of the eavesdropper, rather than an absolute security proof. In this work, we propose a novel configuration using a bi-directional EDFA that allows us to halve the fiber length required in the standard configuration. The paper is structured as follows: first, we discuss the principle of the 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 relating to our setup in particular.

2. Principle of Operation

The setup used for the UFL key distribution system (KDS) is shown in Figure 1a. 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 that 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) 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 the mirror states used, only that Alice's and Bob's differ from one another. Thus, a bit value of '0', for example, can be assigned 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 states, to deduce the other's choice, while preventing Eve from obtaining access to the exchanged key bit. This protocol for key distribution using UFL is summarized in Table 1.

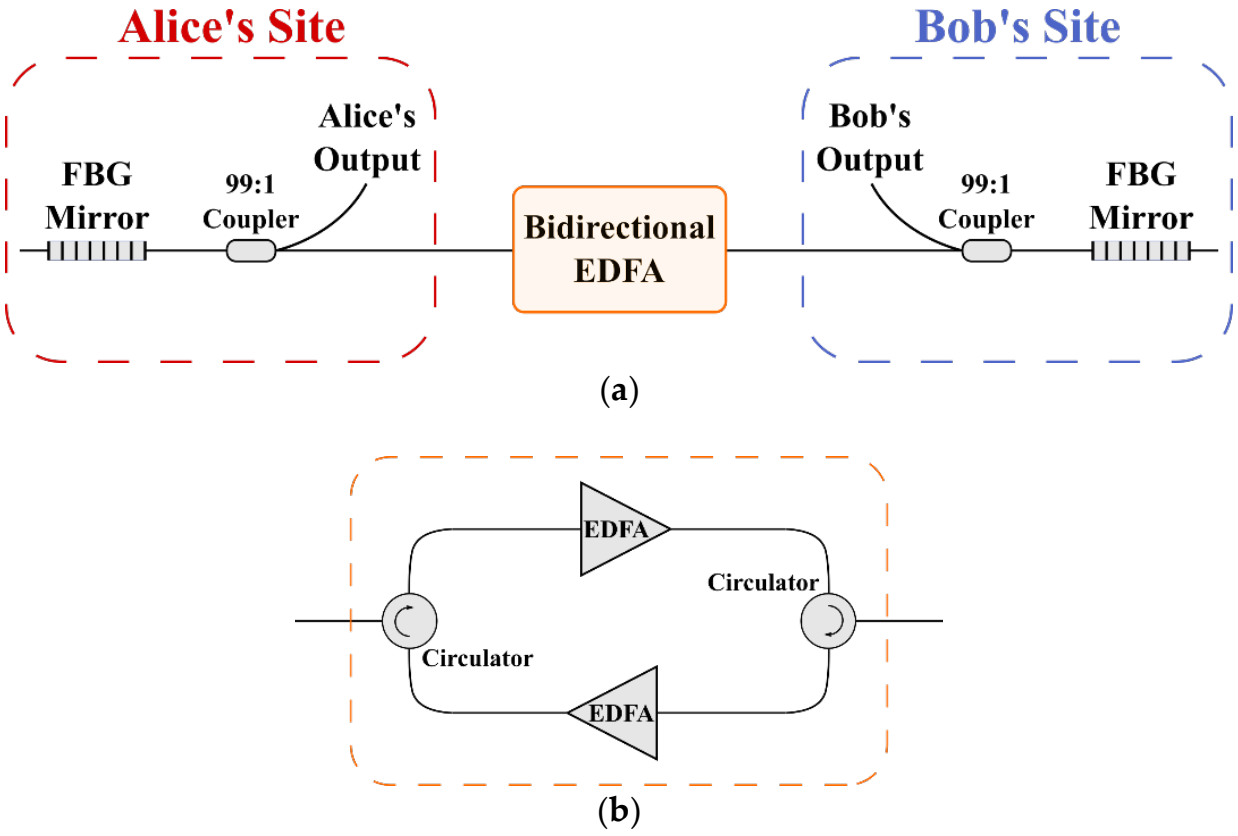


Figure 1. (**a**) Experimental setup; (**b**) internal schematic of the bidirectional EDFA utilized.

Table 1. Protocol for a key distribution system using an ultra-long fiber laser. 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

There are two possible configurations to the UFL setup: one with lasing-secure states and one with non-lasing-secure states. The latter was introduced by Kotlicki et al. [13] as an alteration to the standard lasing scheme proposed in [11]. It establishes the secure states

below the lasing threshold, thus ensuring that the spectra of the secure states are mostly noise and harder to distinguish between each other. For this reason, it is this latter lasing scheme that we use in our setup.

Security of the System

The security of the system can be tested with regard to either passive or active attacks [11,12,19,20]. Active attacks are characterized by the tampering of the cavity by the injection of light into it, while passive attacks require only the tapping of the optical signal on the part of the eavesdropper [19,20]. The focus of this study will be on passive attacks, which can further be divided into spectral, temporal, or combined attacks. Spectral attacks rely on the analysis of the spectrum of the optical signal at its steady state. Temporal attacks, on the other hand, rely on monitoring the evolution of the optical field in the cavity over time, as the transition between secure and non-secure states may transmit information regarding the secure state's mirror choice. The third class of attacks, a combination of spectral and temporal attacks, is the most difficult to defend against, relying on the spectral analysis of the residual signal coming from each user's terminal while in a secure state.

3. Materials and Methods

The experimental setup is shown in Figure 1a.

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. The fiber gratings used for Alice and Bob had a peak reflectivity of 53.3% at 1560.80 nm and 65.84% at 1560.85 nm, respectively. Each user was further equipped with a 99:1 coupler in order to perform measurements of the cavity's signal. The link length of the cavity was 1 km. The gain of the system was provided by a customized bidirectional EDFA from MWTechnologies, whose internal schematic is depicted in Figure 1b.

It consists of two circulators and two conventional EDFAs, i.e., an erbium-doped fiber and a co-directional pump at 980 nm, with each pump capable of being independently controlled by separate voltage sources. To perform the measurements required for the experiment, an optical spectrum analyzer (OSA) model "AQ6370D" with wavelength range of 600 nm to 1700 nm from Yokogawa was used. Time domain measurements were performed with an InGaAs photodetector (model "PDA10CS-EC" from Thorlabs) and an oscilloscope (model "TDS1002C-EDU" from Tektronix).

4. Results

To study the spectral response of the system, all possible states of the UFL were selectively chosen one by one and their results read in the OSA. The obtained spectra of the four possible states of the UFL (read in Alice's output) are depicted in Figure 2. The pump powers used in the EDFA were of 1.49 V, corresponding to -26.93 dBm of total power, and 1.64 V, corresponding to -22.68 dBm of total power. These were chosen so that the non-secure states were obtained near the lasing threshold. While the spectra for the non-secure states present 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. To test if Eve would indeed be able to differentiate between both spectra, a two sample Kolmogorov–Smirnov test was performed. Thus, a max deviation D of 0.04795 and a p value of 0.20003 was obtained. For an alpha level of 0.05, our results show that $p > \alpha$ and we can thus accept the null hypothesis that the two samples came from the same distribution.

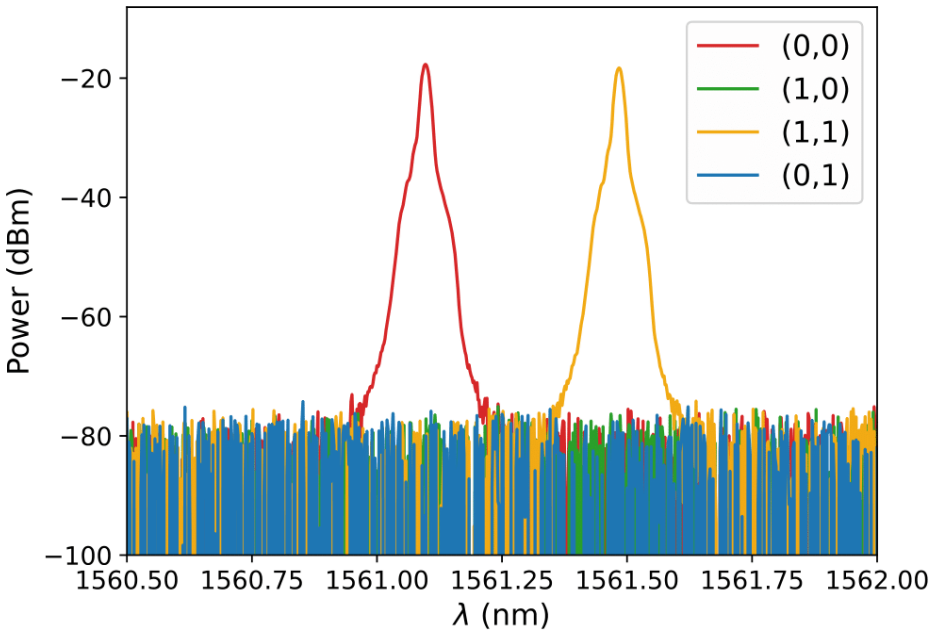
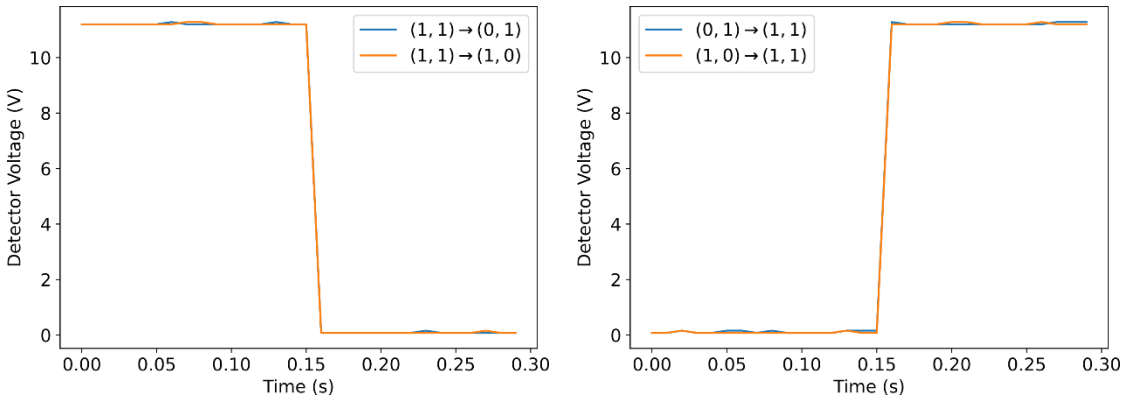


Figure 2. Optical spectrum of the four states of the UFL-KDS.

As expected, Eve would not find it technologically easy to access Alice's and Bob's mirror choice.

To study the temporal response of the system, transitions from secure to non-secure states and vice versa were effectuated and measured with a photodetector and oscilloscope. To counteract the transmission of useful information to Eve that may occur between transitions of the mirror state, both pumps of the EDFA were switched off between such transitions. Since no signal travels along the fiber when Alice and Bob are choosing their mirror state, a signature of a secure state is less likely to occur on a build-up or a downfall of the cavity's signal. Figure 3 shows the transitions between the non-secure state (1,1) and both possible secure states, and vice versa. Again, a two-sample Kolmogorov–Smirnov test was performed, having obtained a p value of 1.0 for the (1,1)→ (x,x) transitions and a p value of 0.80796 for the (x,x) →(1,1) transitions. In both cases, assuming an alpha of 0.05, the null hypothesis can be accepted and thus no useful information is gained by Eve. Similar results were obtained using the (0,0) non-secure state instead of (1,1).



(**a**) (**b**)

Figure 3. Cavity signal when transitioning from: (**a**) non-secure to secure states and (**b**) vice versa.

The study of the spectral temporal response was made by taking advantage of the 0 nm span measurements enabled by the OSA. The results were taken from Alice's output for the signal at $\lambda_{0,0}$ and $\lambda_{1,1}$ between several transitions of UFL states and are represented in Figure 4. As mentioned before, the pumps of the EDFA were switched off between transitions and the graphics of Figure 4 were obtained as follows: between 0 and ~200 time units, the UFL was in a non-secure state; between ~200 and ~400, the pumps were switched off and the peak reflectivity of one of the FBG mirrors was switched; between ~400 and ~600, the pumps were turned on and thus the UFL was in a secure state; between ~600 and ~800, the pumps were again switched off and the relevant FBG mirror was switched back to its initial state; and finally, from ~800 to ~1000, the pumps were switched on and the UFL returned to its original non-secure state.

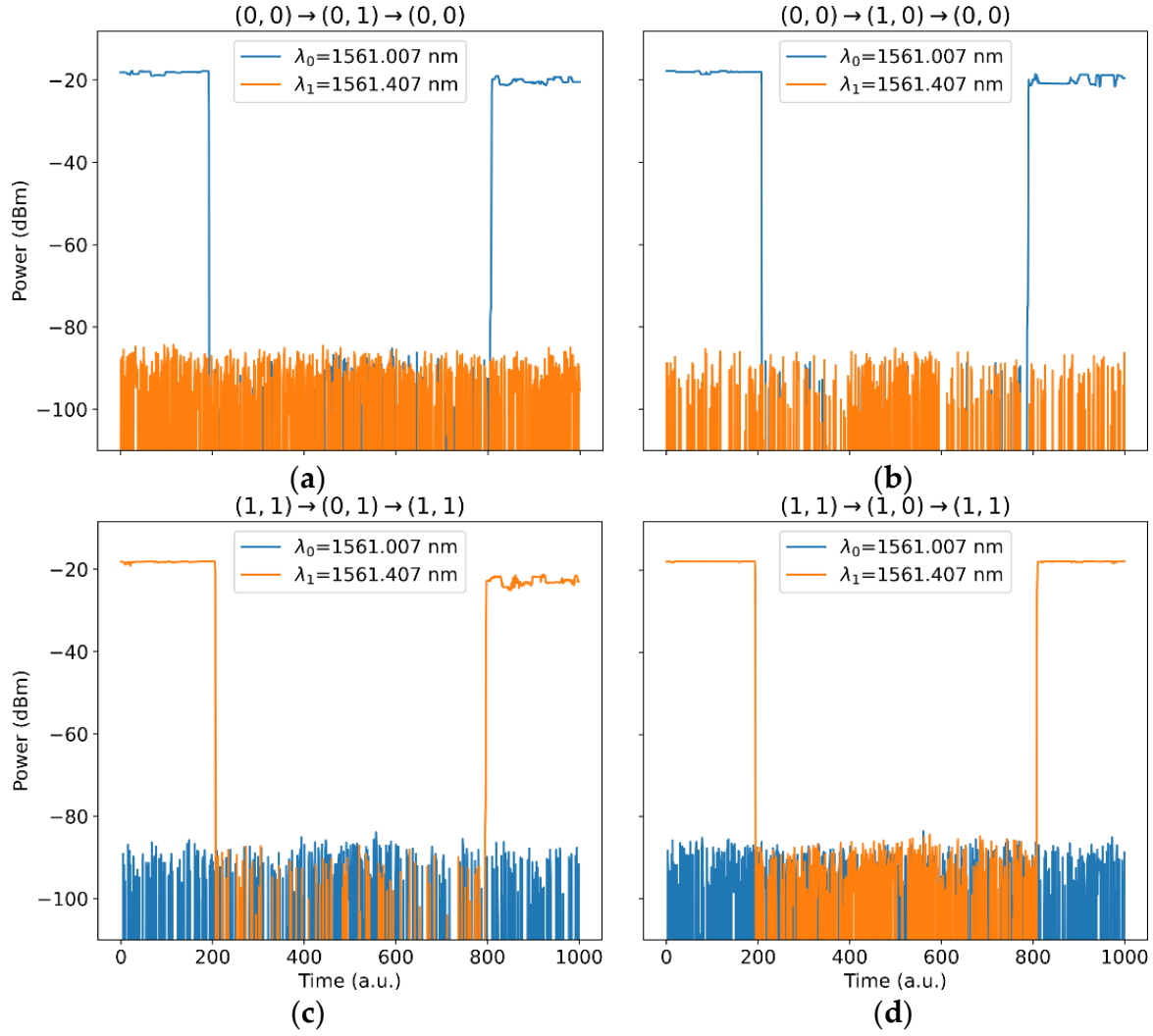


Figure 4. Cavity signal at Alice's output filtered at λ_0 and λ_1 for the transitions: (**a**) (0,0)→ (0,1)→ (0,0); (**b**) (0,0)→ (1,0)→ (0,0); (**c**) (1,1)→ (0,1)→ (1,1) and (**d**) (0,0)→ (0,1)→ (0,0).

As the results of Figure 4 were taken at Alice's terminal, it would be necessary to read the residual signal filtered through her FBG for these measurements to be useful to Eve. In other words, the signal measured at λ_A needs to be greater than that at λ_B for the system in the state (A,B), with A,B $\in \{0, 1\}$. As it can be observed, the power level of the secure states is similar to the optical noise of the system and, therefore, hard to differentiate.

5. Discussion

5.1. Improvments

The achievable link length of the UFL protocol will be restricted by the power of the EDFA used. With the currently available commercial EDFA of 20 dBm [21], it is expected that a length of 80 km is achievable. On the other hand, the process of increasing the bit-rate of the setup, both to generally accelerate 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 must 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 [13], which results in a maximum frequency of $f = c/3dn$ bps, where d is the length of the link and n is 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. [22], including using wavelength division multiplexing (WDM), or improving the 50% efficiency of the secure bit transmission.

5.2. Vulnerabilities

As previously discussed, even in its theoretical ideal case, the UFL protocol is still susceptible to attacks, relying instead on an eavesdropper's technological difficulty in distinguishing 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 [11,13], the paper by Garcia-Escartin et al. [23] 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 represent important future work in the study of the reliability of the UFL protocol.

6. Conclusions

The 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 was 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.

In future work, we shall perform a more in-depth set of statistical tests to further examine the ability of an eavesdropper to overcome the security of this protocol.

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

Author Contributions: Conceptualization, O.F.; methodology, B.S. and P.R.; validation, B.S. and P.R.; writing—original draft preparation, B.S.; writing—review and editing, A.G. and O.F.; supervision, A.G. and O.F. All authors have read and agreed to the published version of the manuscript.

Funding: National Funds through the Portuguese funding agency, FCT - Fundação para a Ciência e a Tecnologia, within project UIDB/50014/2020.Beatriz Soares Paulo Robalinho acknowledges the support of the Foundation for Science and Technology (FCT), Portugal through the Grant 2022.11929.BD and 2020.04562.BD.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Data underlying the results presented in this paper are not publicly available at this time but may be obtained from the authors upon reasonable request.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Stinson, D.R. *Cryptography: Theory and Practice, Third Edition (Discrete Mathematics and Its Applications)*; CRC Press: Boca Raton, FL, USA, 2005.
2. Bennett, C.; Brassard, G. Quantum Cryptography: Public Key Distribution and Coin Tossing. In Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India, 10–12 December 1984; Volume 560.
3. Gisin, N.; Ribordy, G.; Tittel, W.; Zbinden, H. Quantum Cryptography. *Rev. Mod. Phys.* **2002**, *74*, 145. [CrossRef]
4. Ekert, A.K. Quantum Cryptography and Computation. In *Advances in Quantum Phenomena*; Beltrametti, E.G., Lévy-Leblond, J.-M., Eds.; Springer: New York, NY, USA, 1995; pp. 243–262. [CrossRef]
5. Shor, P.W.; Preskill, J. Simple Proof of Security of the BB84 Quantum Key Distribution Protocol. *Phys. Rev. Lett.* **2000**, *85*, 441. [CrossRef] [PubMed]
6. Duan, L.-M.; Lukin, M.D.; Cirac, J.I.; Zoller, P. Long-Distance Quantum Communication with Atomic Ensembles and Linear Optics. *Nature* **2001**, *414*, 413–418. [CrossRef] [PubMed]
7. Aspelmeyer, M.; Böhm, H.R.; Gyatso, T.; Jennewein, T.; Kaltenbaek, R.; Lindenthal, M.; Molina-Terriza, G.; Poppe, A.; Resch, K.; Taraba, M.; et al. Long-Distance Free-Space Distribution of Quantum Entanglement. *Science* **2003**, *301*, 621–623. [CrossRef] [PubMed]
8. Marcikic, I.; De Riedmatten, H.; Tittel, W.; Zbinden, H.; Legré, M.; Gisin, N. Distribution of Time-Bin Entangled Qubits over 50 Km of Optical Fiber. *Phys. Rev. Lett.* **2004**, *93*, 180502. [CrossRef] [PubMed]
9. Hughes, R.J.; Morgan, G.L.; Peterson, C.G. Quantum Key Distribution over a 48 km Optical Fibre Network. *J. Mod. Opt.* **2009**, *47*, 533–547. [CrossRef]
10. Gobby, C.; Yuan, Z.L.; Shields, A.J. Quantum Key Distribution over 122 km of Standard Telecom Fiber. *Appl. Phys. Lett.* **2004**, *84*, 3762–3764. [CrossRef]
11. Scheuer, J.; Yariv, A. Giant Fiber Lasers: A New Paradigm for Secure Key Distribution. *Phys. Rev. Lett.* **2006**, *97*, 1–4. [CrossRef] [PubMed]
12. Zadok, A.; Scheuer, J.; Sendowski, J.; Yariv, A. Secure Key Generation Using an Ultra-Long Fiber Laser: Transient Analysis and Experiment. *Opt. Express* **2008**, *16*, 16680. [CrossRef] [PubMed]
13. Kotlicki, O.; Scheuer, J. Dark States Ultra-Long Fiber Laser for Practically Secure Key Distribution. *Quantum Inf. Process.* **2014**, *13*, 2293–2311. [CrossRef]
14. Goedgebuer, J.P.; Larger, L.; Porte, H. Optical Cryptosystem Based on Synchronization of Hyperchaos Generated by a Delayed Feedback Tunable Laser Diode. *Phys. Rev. Lett.* **1998**, *80*, 2249. [CrossRef]
15. Argyris, A.; Syvridis, D.; Larger, L.; Annovazzi-Lodi, V.; Colet, P.; Fischer, I.; García-Ojalvo, J.; Mirasso, C.R.; Pesquera, L.; Shore, K.A. Chaos-Based Communications at High Bit Rates Using Commercial Fibre-Optic Links. *Nature* **2005**, *438*, 343–346. [CrossRef] [PubMed]
16. Shake, T.H. Confidentiality Performance of Spectral-Phase-Encoded Optical CDMA. *J. Light. Technol.* **2005**, *23*, 1652. [CrossRef]
17. Shake, T.H. Security Performance of Optical CDMA Against Eavesdropping. *J. Light. Technol.* **2005**, *23*, 655. [CrossRef]
18. Kish, L.B. Totally Secure Classical Communication Utilizing Johnson (-like) Noise and Kirchoff's Law. *Phys. Lett. A* **2006**, *352*, 178–182. [CrossRef]
19. El-Taher, A.; Kotlicki, O.; Harper, P.; Turitsyn, S.; Scheuer, J. Secure Key Distribution over a 500 km Long Link Using a Raman Ultra-Long Fiber Laser. *Laser Photonics Rev.* **2014**, *8*, 436–442. [CrossRef]
20. Scheuer, J. Secure Long-Range and High Bit-Rate Distribution of Shared Key Using Dark States Ultra-Long Fiber Laser (UFL). *SPIE* **2018**, *10559*, 1055902. [CrossRef]
21. Semiconductor Optical Amplifier, DWDM Amplifier. Available online: https://thorbroadcast.com/product/20-dbm-edfa-optical-amplifier.html (accessed on 29 September 2022).
22. Bar-Lev, D.; Scheuer, J. Enhanced Key-Establishing Rates and Efficiencies in Fiber Laser Key Distribution Systems. *Phys. Lett. Sect. A Gen. At. Solid State Phys.* **2009**, *373*, 4287–4296. [CrossRef]
23. Garcia-Escartin, J.C.; Chamorro-Posada, P. Hidden Probe Attacks on Ultralong Fiber Laser Key Distribution Systems. *IEEE J. Sel. Top. Quantum Electron.* **2018**, *24*, 1–9. [CrossRef]