Physical Layer Security in Optical Networks

Dimitris Syvridis, Evangelos Pikasis, Charidimos Chaintoutis

Physical Layer Security based on data encryption or modulation parameter encoding

Dimitris Syvridis[1], Evangelos Pikasis[2] and Charidimos Chaintoutis[2][0000-0001-8328-2135]

[1] Dept. of Informatics and Telecommunications
National and Kapodistrian University of Athens, Athens, Greece
[2] Eulambia Advanced Technologies Ltd., Ag. Paraskevi, Greece
dsyvridi@di.uoa.gr

Abstract. In this paper we 'll discuss technological alternatives related to physical layer security of optical communication systems and networks. In the introduction, an overview of confidentiality and availability issues of the optical networks will be discussed, focusing mainly in the physical layer-related solutions. In the following paragraphs we'll provide two distinct approaches for the physical layer encryption. The first is based on a One-Time-Pad implementation using synchronized true random sequences. The second uses cryptographic keys generated by Photonic Physical Unclonable Function devices for scrambling the Orthogonal Frequency Division Multiplexing subcarriers.

Keywords: Physical layer, Optical Chaos, Physical Unclonable Function, OFDM Scrambling.

1 Introduction

Nowadays communication networks support all crucial human activities from personal communications to financial transactions, massive data management, industrial processes, energy infrastructures, health/medical data exchange, transport, etc. Military communications is another highly demanding area in terms of security. Although a lot of attention has been given to the performance of the networks, such as bandwidth and latency, security aspects become more and more crucial for obvious reasons. Since the communication systems and networks, especially those based on fiber-optic media, were not designed from the ground up taking security aspects into account, the current solutions are mainly applied at the upper network layers rather than employing a holistic new approach. Particularly in the physical layer of the networks insufficient progress in security has been made. Facing the potential threats at the lower network levels, will significantly impact the security aspects at the higher layers as well.

There are different types of threats related to the physical layer of the optical network. A first group of threats are those related to availability, targeting at performance degradation or even complete interruption of the network operation. Fiber infrastructure disasters, unintentional (e.g. natural disaster related) or intentional (malicious human actions aiming at interruption of communication links or injection jamming signals) are among the physical layer threats to be considered [1]. Electromagnetic pulse

(EMP) attack is also another possible threat. Although the communication channel (optical fiber) will not be affected by EMP, all electronic / optoelectronic components related to the network operation will be damaged or malfunction depending on the strength of the electromagnetic field.

Another potential threat is related to the confidentiality, targeting at accessing data by unauthorized users for eavesdropping or even traffic monitoring / analysis. Although optical fiber is considered safer compared to wireless channels, possible means that could be used by an eavesdropper is optical fiber tapping or information extraction based on adjacent channel interference / crosstalk. Encryption and coding [2] are means for ensuring confidentiality in an optical network. Encryption is either at the optical or electronic level and it requires cryptographic key distribution / sharing between transmitter and receiver. In general, an XOR operation between the key and the data is the means for encrypting the data with the cryptographic key. There are different methods to implement optical XOR gates such as Four Wave Mixing in a SOA, cross gain modulation, cross phase modulation, etc. In the electrical domain, the most commonly used means of encryption rely on AES ciphers. These symmetrical encryption schemes are based on substitution-permutation networks and have several efficient software and hardware implementations [3]. Concerning coding, optical CDMA [4] is the most common approach, following the principles of the corresponding method used in the wireless systems. Alternative solutions based on chaos encrypted communications have been also proposed and demonstrated [5].

Key generation is based on specific software implementations or employing different types of random processes. Software based implementations rely on pseudorandom number generators whereas those obtained by statistically random physical phenomena such as thermal noise, photoelectric effect, amplified spontaneous emission [6] or other quantum phenomena are true random number sequences. Concerning key distribution, quantum technologies appear to provide the ultimate security [6-9], either in the form of DV-QKD or CV-QKD, exploiting the particle or the wavelength nature of light respectively. However, although QKD may provide an effective way to achieve unconditional security, a number of successful hacking on commercial QKD has been reported [10] as well as deficiencies in the theory behind the specific implementations [11, 12]. At the same time, Britain's National Cyber Security Centre disclosed a document in 2016 about security risks of QKD and its inefficient cost performance, and possible future threats being yet unknown [13].

In this paper we present two different approaches targeting at the physical layer encryption. The first demonstrates a photonic implementation of the "One-Time Pad" encryption scheme based on mutually injected semiconductor lasers, operating in the chaotic regime and continuously generating synchronized ultrafast true random number sequences. These sequences are then used for encryption of the data to be transmitted [14]. The second is based on a cryptographic key generation using a novel Photonic Physical Unclonable Function device. These keys are used for scrambling the modulation parameters of transceivers included in the communication system.

2 One-time-pad data encryption using synchronized true random sequences

2.1 One-time-pad encryption system

The proposed One-Time-Pad encryption system capable to operate at Gb/s rates is based on synchronized broadband chaotic analog signals that are the seed for ultrafast TRBS generation. Each user's transceiver has access to this locally generated TRBS that is synchronized with the TRBSs generated by other users, through a background fiber network that supports broadband chaotic signal generation and synchrony. User #1 encodes the data that wishes to send with the appropriate FEC convolutional code and applies a XOR operation with the locally generated TRBS (Figure 1). The encrypted data follows the desired transmission path in the network to reach the legitimate recipient (user #2), where the decoding process takes place. User's #2 locally generated TRBS participates also to a XOR operation in order to provide the initially encoded data to the decoder and obtain finally the initial data. Contrariwise, the opposite communication from user #2 to user #1 is supported using the same methodology and the same TRBS generators. Convolutional coding in forward error correction (FEC) methods is included to minimize or eliminate synchronization error between analog chaotic signals that results in errors in TRBSs' synchrony.

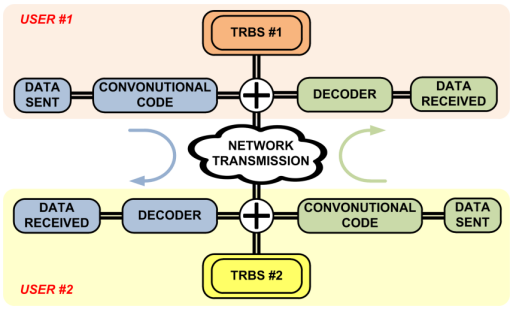

Fig. 1. One-time-pad bi-directional encryption system using synchronized ultrafast TRBS generators and FEC methods for error-free secure communications.

2.2 Optical system for the chaos synchronization

Each user participates in the optical network configuration with the appropriate hardware equipment; its specifications and properties can guarantee broadband chaotic signal emission, which can be potentially converted to a TRBS under a pre-determined methodology. At the same time, through the appropriate network bi-directional topology, it can guarantee very high level of chaotic signal synchronization. In the mutual optical injection topology of Figure 2, users hold at their premises identical DFB semiconductor lasers (SLs) and photodetectors. (PDs). The SLs are interactively coupled with an identical DFB SL hub at the other edge of the network, through polarization

control, optical routing and amplification. Its location can be at km distance as demonstrated by the inclusion of a 3.5km fiber transmission spool. The SL hub offers a drive force for mutual injection and operation of the users' SLs at the coherence collapse regime. Although the process is polarization sensitive using a polarization scrambler or polarization tracker could be a possible solution to the polarization problem.

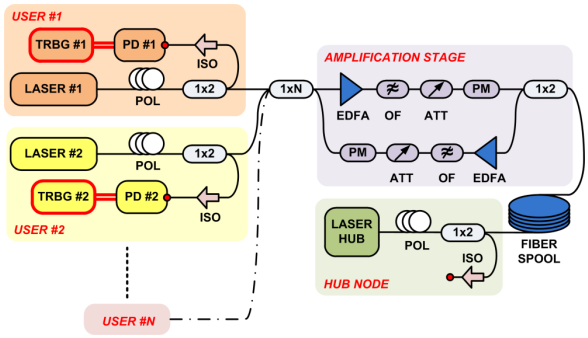

Fig. 2. Optical system of mutually injected semiconductor DFB lasers for broadband and synchronized chaotic signal emission. POL: polarization controller, 1x2 and 1xN: optical coupler with 2 or N equal splitting ratio inputs, ISO: optical isolator, PD: 10GHz photoreceiver, EDFA: 25dB-gain erbium-doped fiber amplifier, OF: optical filter with FWHM=0.36nm, ATT: optical attenuator, PM: inline power monitor, TRBG: true random bit generator. Black line connections are fiber-optic links; red line connections are high-frequency electrical links.

2.3 True random bit generation

At the next level, the synchronized photo-detected signals at each user's premises are converted from their analog form to binary sequences in order to support one-time-pad encryption. The emerging digital sequences shall meet the criteria of randomness in order to play the role of encryption random key generators. Each measured sample is digitized under a single-bit or a multi-bit methodology via analog-to-digital (A/D) conversion. In order to obtain identical true random sequences from all users participating in the network tow conditions are required: (i) the chaotic analog signals emitted by the different users shall preserve high-quality synchronization, and (ii) these analog signals shall lead after digitization verified TRBSs. These prerequisites imply identical steps and parameterization of the post-processing procedures, as well as identical hardware modules used by all users.

2.4 One-time-pad performance

Each legitimate user that coupled to the optical network, fulfilling some predetermined conditions, can generate the synchronized and random key sequences. The level of synchrony error of the users' analog signals attained at the optical layer is translated as an error rate of the generated digital keys. The larger the cross-correlation value between the two analog signals is, the smaller the error rate between the two TRBSs will be. As it can be seen from fig. 3, for sufficiently low error rate between the keys generated by

the two users, extremely high-quality synchronization is needed. For example, and assuming FEC (1/2), the required cross correlation between the chaotic signals is in the order of 0.999. This is exactly the key point for the security of the proposed system. If an eavesdropper attempts to intervene and tap even a minor fraction of the chaotic signal shared between the legitimate users, the synchronization quality will immediately degrade and the communication between the two users will collapse.

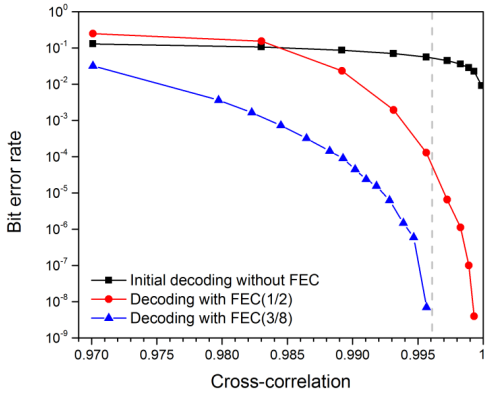

Fig. 3. Error rate for the key generation vs. cross-correlation between the chaotic signals of the two users.

3 Photonic PUFs as physical root of trust for OFDM-based optical communication systems

PUFs have been recently proposed as a physical root of trust that uniquely combines key storage and generation procedures. Thus, the CIA triad of security objectives (Confidentiality, Integrity, and Authentication) can be achieved by exploiting cryptographic primitives that are hardened by properties of the actual physical world. Essentially, a PUF is the physical analogue of a one-way mathematical function, based on an unclonable, non-reproducible and complex physical mechanism. Combined with their deterministic operation, PUFs are appropriate for cryptographic key generation on demand, eliminating the need for key storage (no key-at-rest property) in secure Non-Volatile Memory modules (NVM). In this way, keys cannot be found by an attacker who has accessed the device and compromised all the memory contents. Additionally, in this way, it is possible to provision keys for devices that are rapidly scaling in numbers, year after year. The basic concept behind PUFs has been materialized in various different implementations with the main differentiation being between optical/photonic PUFs as introduced in [16]. and silicon-based PUFs as introduced in [17]. The idea behind PUFs is to use unavoidable, implicit defects present in the manufacturing process of a hardware token in order to make a digital ‘fingerprint’ of the token. In general, when an extrinsic excitation (Challenge) is presented to a PUF, a corresponding output (Response) is generated. This response is determined by a complex physical function that is unique to each token or PUF instance, as shown in Fig. 4. Using the same challenge,

different PUFs produce a different response. The combination of the challenge and its corresponding response lead to the creation of unique challenge–response pairs (CRPs). The uniqueness of the responses of different PUFs under the same challenge (unclonability) and the uniqueness of the responses of the same PUF under different challenge (unpredictability) have made PUFs useful for a wide variety of applications, spanning from authentication and secret key storage [17, 18], cryptographic key generation [19], software–hardware interconnection [20], and tamper detection [21] to shielding systems against code-reuse attacks [12] and cyber-hardening blockchain applications [23]. So far, the spotlight of attention has been mainly focused on silicon-cast PUFs, whose principle of operation is based on exploiting uncontrollable variations in operational parameters [17, 24]. Existing implementations include ring-oscillators [17, 25], arbiter

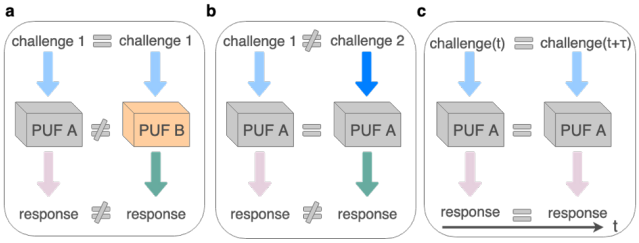

Fig. 4. Representation of the typical PUF properties. (a) Unclonability: same challenges but different PUFs provide different responses, (b) Unpredictability: different challenges to the same PUF provide different response, (c) Robustness: time-invariant operation

PUFs [26], static random-access memory (SRAM) PUFs [27] to mention a few. Despite their merits in terms of integration, unclonability, and robustness, the underlying physical scrambling mechanism, in most cases, is rather simplistic, resulting to enhanced vulnerability to modelling attacks [28, 29]. The arsenal of adversaries is enhanced through various side-channel attacks [30, 31]. Emerging PUF implementations based on nanofabrication procedures [32], hold great promise, but current results are focused on providing proof of concept and do not evaluate their cryptographic performance.

Photonic PUF implementations are based on the combination of the coherent interaction of a laser beam with the randomness of a disordered physical medium (fig.5). The medium could be a material containing randomly positioned micro-structures that act as scatterers [16], or an optical fiber [34, 35]. A laser source illuminates a transparent, inhomogeneous medium (PUF's token), the goal being to produce unique interference patterns (speckle) which are subsequently captured as images (responses). The recorded images undergo a post-processing procedure, via hashing algorithms, and every hashed response is mapped to a **unique bit-string output**. In this way unique **Challenge-Response Pairs** are acquired. While the physical characteristics of the PUF token, that enable the extraction of the unique responses, are permanent in nature, the information extraction from PUFs (and other noisy sources, like biometrics) is a probabilistic procedure; on a single challenge, a different response may be produced, due to the uncontrollable and random evaluation noise. In order to ensure robust operation

under the effect of noise, the mapping of each image to a unique bit-string and its recovery is achieved through fuzzy extractor algorithms [36].

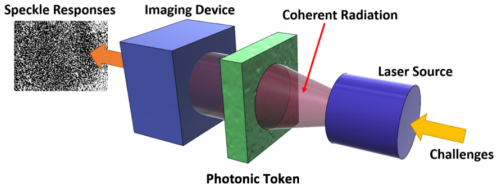

Fig. 5. Conceptual representation of a p-PUF

The fuzzy extractor scheme comprises two phases: the enrolment and the verification phase. The former corresponds to the first time that a challenge is applied whereby the output string is generated along with a set of public helper data, while the latter represents the noisy rerun of the measurement during which the same result is recreated by using the helper data produced in the enrolment phase. A simple schematic of the described procedure is depicted in Fig. 6.

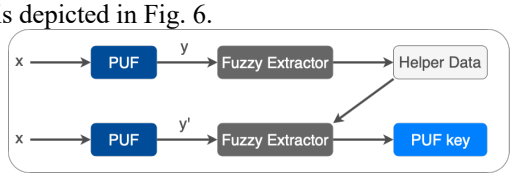

Fig. 6. Fuzzy extraction: enrolment and reconstruction phase for the generation of PUF keys. x represents a challenge; y is the initial PUF response for challenge x during enrolment and y' is the PUF's response for the same challenge under the presence of noise

The security properties of the p-PUFs are based on the complexity of the underlying physical mechanism, with its complexity rendering p-PUFs more secure than their electronic counterparts. For example, a modelling attack would require partitioning the PUF token into wavelength-sized voxels and solving Maxwell's equations for each possible arrangement [33]. We should mention here that secret keys provide security based on the fact that they are completely random (and thus unpredictable). PUF responses, have a high degree of randomness, but are usually not completely random. Fuzzy extraction algorithms, apart from accurate key reproduction, also remedy the uniformity problem by employing "randomness extractors". Randomness extractors (i.e., universal hash functions) convert a high entropy input into a shorter, uniformly distributed output. Following this procedure, some of the source's entropy is "sacrificed" to acquire uniformly distributed random keys. We should mention here that the public nature of the fuzzy extractor's helper data (the pieces of information used for accurate response reproduction) poses no security risk; helper data do not contain any useful information for an adversary that could take hold of them.

3.1 PUF-enabled subcarrier scrambler module, to cyber-harden OFDM-based communications

The three primary 5G NR diverse use cases which defined by 3GPP [37] are: Ultra Reliable Low Latency Communications (URLLC), Enhanced Mobile Broadband (eMBB) and Massive Machine Type Communications (mMTC). Some potential applications for 5G networks include gaming, Virtual reality applications, Vehicle to vehicle, Internet of Things (IoT) and machine to machine communications (M2M). Some of the key requirements that need to be achieved by a modulation scheme, in order to support all the aforementioned applications are [38]:

- Capable of handling high data rate wide bandwidth signals
- Able to provide low latency transmissions
- Capable of fast switching between uplink and downlink for TDD systems
- Interworking between high and low frequency bands
- Enable the possibility of energy efficient communications

Orthogonal Frequency Division Multiplexing (OFDM) has been an outstanding choice for 4G networks providing significant spectrum efficiency and performance improvement in frequency-selective channels. The Cyclic-Prefix (CP) OFDM is the predominant candidate for 5G networks for the cases of downlink and uplink in the sub-6GHz frequency band and for the mmWave range [39]. A typical block diagram of an OFDM RF transceiver with the subcarrier scrambler module is depicted in Fig.7. In the case of the OFDM transmitter, a high bit rate stream after the parallel to serial converter is driven to QAM mapper and the mapping process forms the buffered bit stream to QAM symbols. In a conventional OFDM system, the complex stream is given as input to the IFFT stage, modulating each subcarrier with QAM symbols. In this scheme, an extra stage, a **PUF-based scrambler**, is added performing re-distribution of the subcarriers across the frequency domain. The scrambler module performs the subcarrier scrambling operation exploiting the unique responses of the p-PUF module. The unique bit-string responses are used as seeds that feed a pseudo RNG (pseudo-Random Number Generator). Thus, a scrabbling number sequence is produced, and the subcarriers are scrabbled accordingly. A Cyclic Prefix (CP) in order to combat the multipath is added and afterwards the produced complex OFDM signal is RF up-converted, amplified by power amplifier (PA) and radiated from the antenna.

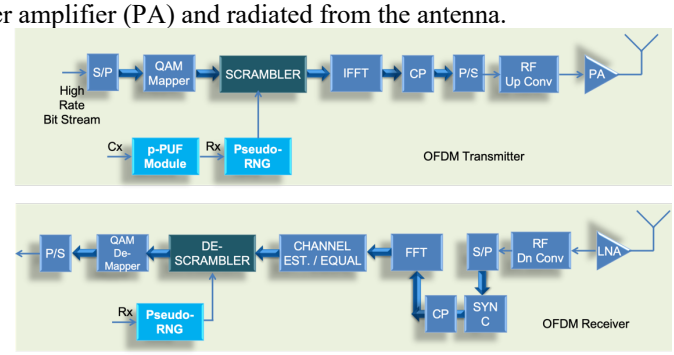

Fig. 7. A typical block diagram of an OFDM transceiver

At the receiver side, the reverse operations include synchronization, frequency domain estimation/equalization and de-scrambling. It must be noted that the process of the frequency estimation and equalization is not affected from the scrambling method. Under this scheme, the bit and power loading methods cannot be used. After the handshaking process, the net bit rate of the proposed system is the OFDM net bit rate. Given that the PUF response (used as seed for the pseudo-RNG) is precisely reproduced, and the pseudo-RNG algorithm is known, the de-scrambling sequence would precisely follow the scrabbling one.

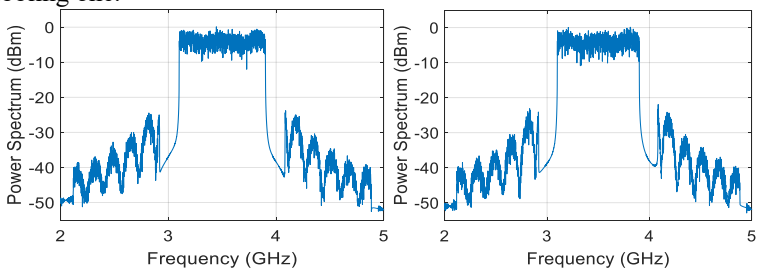

Fig. 8. The power spectrum of the RF up-converted of the (a) unscrambled and (b) scrambled OFDM signal

The power spectrum of an (a) un-scrambled and (b) scrambled OFDM up-converted signal to 3.5GHz carrier frequency, as well as the time traces for these two cases are shown in Figs. 8,9 respectively. As can be observed, the power spectra of the up-converted OFDM signals are different as well as the time traces for the two cases.

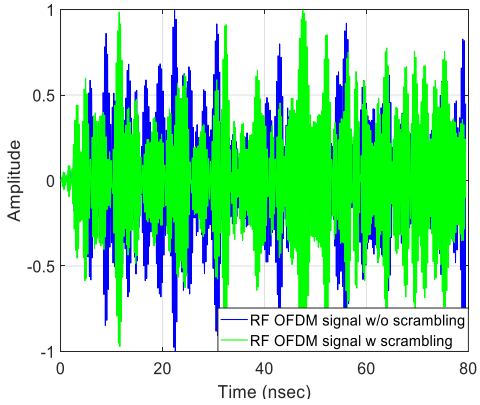

Fig. 9. Un-scrambled and scrambled up-converted OFDM time traces

In order to quantify the difference between the unscrambled and scrambled OFDM signals we employ the cross-correlation metric, as is depicted in Fig. 10. As can be seen, the maximum of the cross-correlation of the OFDM signal with itself is 0.97, while in the second case is 0.023.

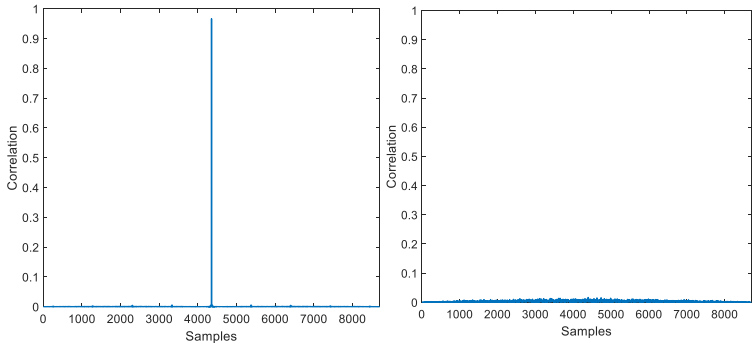

Fig. 10. Cross-correlation of the OFDM signal with itself and between the un-scrambled and scrambled up-converted OFDM signal

Compared with single carrier schemes, OFDM systems exhibit high peak-to-average power ratio (PAPR). The high value of PAPR is one of the detrimental aspects of OFDM systems since the OFDM signal is greatly affected by the non-linear effects of RF power amplifier (PA), causing serious in-band distortions as well as adjacent channel interference. The scrambling process doesn't affect the PAPR distribution as depicted in Fig.11, where complementary cumulative distribution function (CCDF) denotes that a probability distribution of the PAPR of OFDM symbols is over a certain threshold.

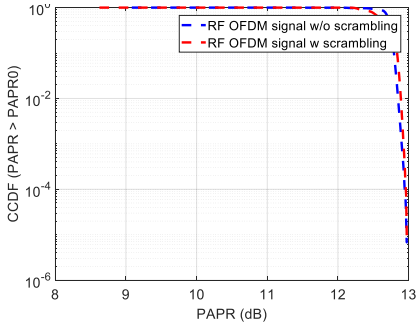

Fig. 11. CCDF curves for the scrambled and unscrambled scheme.

As can be seen from all the above graphs, the effect of the scrambling process on the basic characteristics of an OFDM signal is negligible, providing the security of the communication system.

4 Conclusion

In this paper we presented two different approaches for the physical layer encryption. The first is based in an optical implementation of the One-Time-Pad cryptographic scheme. We have shown that almost perfect synchronization between mutually injected

chaotic lasers placed at the premises of two communicating users leads to the continuous generation of synchronized true random number sequences. These sequences can be used for encrypting / decrypting the data streams exchanged between the two users. The second is based on optical implementation of a Physical Unclonable Function and its application a key generator for scrambling the OFDM subcarriers in a typical 5G communication scheme.

References

1. R. Rejeb, M. S. Leeson and R. J. Green, "Fault and Attack Management in All-Optical Networks," IEEE Commun. Mag., vol. 44, no. 11, 2006, pp. 79-86.
2. Wang Z, Fok MP, Prucnal PR. Physical encoding in optical layer security. J Cyber Secur Mobility 2012:83!100.
3. Schneier, Bruce, et al. "The Twofish team's final comments on AES Selection." AES round 2.1 (2000): 1-13.)
4. Wang Z, Xu L, Chang J, Wang T, Prucnal PR. Secure optical transmission in a point-to-point link with encrypted CDMA codes. IEEE Photonics Technol. Lett 2010;22(19):1410-2
5. Argiris A, Syvridis D, Larger L, Lodi VA, Colet P, Fischer I, et al. Chaos-based communications at high bit rates using commercial fibre-optic links. Nat 2006;438(17):343-6.
6. Argyris A., Pikasis E., Deligiannidis S., Syvridis D., Sub-Tb/s physical random bit generators based on direct detection of amplified spontaneous emission signals. J. Lightwave Techn. Vol 30, no. 9, 2012, pp. 1329-1334
7. Rosenberg D, Harrington JW, Rice PR, Hiskett PA, Peterson CG, Hughes RJ, et al. Long-distance decoy-state quantum key distribution in optical fiber. Phys Rev Lett 2007;98:010503-1-010503-4.
8. Hadfield RH, Habif JL, Schlafer J, Schwall RE, Nam SW. Quantum key distribution at 1550 nm with twin superconducting single-photon detectors. Appl Phys Lett 2006;89:241129-1
9. Scheuer J, Yariv A. Giant fiber lasers: a new paradigm for secure key distribution. Phys Rev Lett 2006;97:140502-1-140502-4.
10. Lydersen, L., Wiechers, C., Wittmann, C., Elser, D., Skaar, J., and Makarov, V., "Hacking commercial quantum cryptography systems by tailored bright illumination." Nature photonics4(10), 686-689 (2010). https://doi.org/10.1038/nphoton.2010.214
11. Yuen, H. P., "Universality and The Criterion 'd' in Quantum Key Generation," arXiv:0907.4694v1, quant-ph (2009).
12. Yuen, H. P., "Fundamental Quantitative Security In Quantum Key Generation," Physical Review A, 82(6), 062304, (2010). https://doi.org/10.1103/PhysRevA.82.062304
13. The British governmental white paper, "Quantum Key Distribution," National Cyber Security Centre, a part of GCHQ in Britain, 4thOct. (2016).
14. Wu BB, Narimanov EE. A method for secure communications over a public fiber-optical network. Opt Express 2006;14(9):3738!51.
15. Argyris A., Pikasis E., Syvridis D., Gb/s One Time Pad Data Encryption with Synchronised Chaos Based True Random Bit Generation. J. Lightwave Techn. Vol 34, no. 22, 2016
16. Pappu, R., Recht, B., Taylor, J., et al.: 'Physical one-way functions', Science, 2002, 297
17. Gassend, B., Clarke, D., Van Dijk, M., et al.: 'Silicon physical random functions'. Proc. of the 9th ACM Conf. on Computer and Communications Security ACM, 2002, pp. 148-160
18. Ruhrmair, U., Devadas, S., Koushanfar, F.: 'Security based on physical unclonability and disorder', in 'Introduction to hardware security and trust' (Springer, USA, 2012), pp. 65-102
19. Suh, G.E., Devadas, S.: 'Physical unclonable functions for device authentication and secret key generation'. 2007 44th ACM/IEEE Design Automation Conf. DAC'07, 2007, pp. 9-14

20. Tuyls, P.: 'Towards hardware-intrinsic security: foundations and practice' (Springer Science & Business Media, Germany, 2010)
21. Kursawe, K., Sadeghi, A.-R., Schellekens, D., et al.: 'Reconfigurable physical unclonable functions-enabling technology for tamper-resistant storage', 2009
22. Qiu, P., Lyu, Y., Zhai, D., et al.: 'Physical unclonable functions-based linear encryption against code reuse attacks'. 2016 53nd ACM/EDAC/IEEE Design Automation Conf. (DAC)
23. Chaintoutis, C., et al. Optical PUFs as physical root of trust for blockchain-driven applications. IET Software (2018)
24. Suh, G. E. & Devadas, S. Physical Unclonable Functions for Device Authentications and Secret Key Generation. In Proc. 44th Annu. Conf. Des. Autom. 9-14
25. Maiti, A. & Schaumont, P. Improving the quality of a Physical Unclonable Function using configurable Ring Oscillators. Proc. of the Int. Conf. on Field Programmable Logic and Applications 703-707 (IEEE. https://doi.org/10.1109/FPL.2009.5272361 (2009).
26. Lee, J. W. et al. A technique to build a secret key in integrated circuits for identification and authentication applications. In Proc. of the IEEE Symposium on VLSI Circuits. Digest of Technical Papers 176-179 https://doi.org/10.1109/VLSIC.2004.1346548 (IEEE, 2004).
27. Xu, X., Rahmati, A., Holcomb, D. E., Fu, K. & Burleson, W. Reliable Physical Unclonable Functions Using Data Retention Voltage of SRAMCells. IEEE Trans. Comput. Des. Integr. Circuits Syst. 34, 903-914 (2015)
28. Nguyen, P. H., Sahoo, D. P., Chakraborty, R. S. & Mukhopadhyay, D. Efficient Attacks on Robust Ring Oscillator PUF with Enhanced Challenge-Response Set. In Proc. of the Design, Automation & Test in Europe Conference & Exhibition (DATE) 641-646 (IEEE, 2015).
29. Hospodar, G., Maes, R. & Verbauwhede, I. Machine learning attacks on 65nm Arbiter PUFs: Accurate modeling poses strict bounds on usability. In Proc. of the 2012 IEEE International Workshop on Information Forensics and Security (WIFS) 37-42
30. Tajik, S., Ganji, F., Seifert, J. P., Lohrke, H. & Boit, C. Laser fault attack on physically unclonable functions. In Proc. of 2015 Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC) 85-96 https://doi.org/10.1109/FDTC.2015.19 (IEEE, 2016).
31. Mahmoud, A., Ruhrmair, U., Majzoobi, M. & Koushanfar, F. Combined Modeling and Side Channel Attacks on Strong PUFs. IACR Cryptology ePrint Archive (2013).
32. Gao, Y., Ranasinghe, D.C., Al-Sarawi, S.F., Kavehei, O. & Abbott, D. Emerging Physica Unclonable Functions with Nanotechnology. IEEE Access 4, 61-80 (2016)
33. Ruhrmair, U., Hilgers, C., Urban, S., et al.: 'Optical pufs reloaded', Eprint. Iacr.Org, 2013
34. Akriotou, M., Mesaritakis, C., Grivas, E., et al.: 'Random number generation from a secure photonic physical unclonable hardware module'. Proc. of the 2018 ISCIS Security Workshop, Imperial College London, 2018
35. Mesaritakis, C., Akriotou, M., Kapsalis, A., et al.: 'Physical unclonable function based on a multi-mode optical waveguide', Sci. Rep., 2018, 8, (1), p.9653
36. Armknecht, F., Maes, R., Sadeghi, A.-R., et al.: 'A formalization of the security features of physical functions'. 2011 IEEE Symp. on Security and Privacy, 2011, pp. 397-412
37. ITU-R SG05, "Draft new Report ITU-R M. - Minimum requirements related to technical performance for IMT-2020 radio interface(s)," February 2017
38. X. Lin, J. LI, R. Baledmair, T. Cheng, S. Parkvall, D. Larsson, H. Koorapaty, M. Frenne, S. Falahati, A. Grovlen and K. Werner, "5G new radio: Unveiling the essentials of the next generation wireless access technology."
39. TS 38.211, "NR; Physical channels and modulation," V15.1.0, April 2018. Available online: http://www.3gpp.org/ftp//Specs/archive/38_series/38.211/38211 -f10.zip, accessed on June 18, 2018.