





Article

# Protecting Physical Communications in 5G C-RAN Architectures through Resonant Mechanisms in Optical Media

Borja Bordel Sánchez <sup>1,\*</sup> , Ramón Alcarria <sup>2</sup> , Tomás Robles <sup>3</sup>  and Antonio Jara <sup>4</sup> 

<sup>1</sup> Escuela Politécnica Superior, Universidad Alfonso X el Sabio, UAX, Avenida Universidad, 1, Villanueva de la Cañada, 28691 Madrid, Spain

<sup>2</sup> Department of Geospatial Engineering, Universidad Politécnica de Madrid, UPM Campus Sur, Km 7.5 de la Autovía de Valencia, 28031 Madrid, Spain; ramon.alcarria@upm.es

<sup>3</sup> Department of Information Systems, Universidad Politécnica de Madrid, UPM Campus Sur, Km 7.5 de la Autovía de Valencia, 28031 Madrid, Spain; tomas.robles@upm.es

<sup>4</sup> Institute of Information Systems, University of Applied Sciences Western Switzerland (HES-SO), Techno-Pôle 3, 3960 Sierre, Valais, Switzerland; jara@ieee.org

\* Correspondence: bbordel@etsisi.upm.es; Tel.: +34-91-067-3922

Received: 23 June 2020; Accepted: 21 July 2020; Published: 23 July 2020



**Abstract:** Future 5G networks are characterized by three basic ideas: enhanced mobile broadband communications, massive machine-type communications, and ultra-low-latency communications. Any of these requirements needs, to be fulfilled, the implementation of high-efficiency technologies at all levels. This includes some of the costliest mechanisms in terms of computational time and bitrate: information protection solutions. Typical techniques in this area employ complex algorithms and large protocol headers, which strongly reduces the effective baud rate and latency of future 5G networks and communications. This is especially relevant in the access network, which in 5G networks will follow a cloud-based architecture, where thousands of different devices must communicate, before aggregating all those streams to be sent to the backbone. Then, new and more efficient mechanisms are needed in the cloud radio access networks (C-RAN) for future 5G systems. Therefore, in this paper it is proposed a novel information protection scheme for C-RAN architectures based on resonant phenomena in optical fibers communicating the fronthaul and backhaul in 5G networks. Resonant structures and physical nonlinearities generate a chaotic signal which may encrypt and hide at physical level every communication stream in a very efficient manner. To evaluate the proposed mechanism, an experimental validation based on simulation techniques is also described and results discussed.

**Keywords:** 5G networks; steganography; chaotic encryption; resonant optical structures; C-RAN architecture

## 1. Introduction

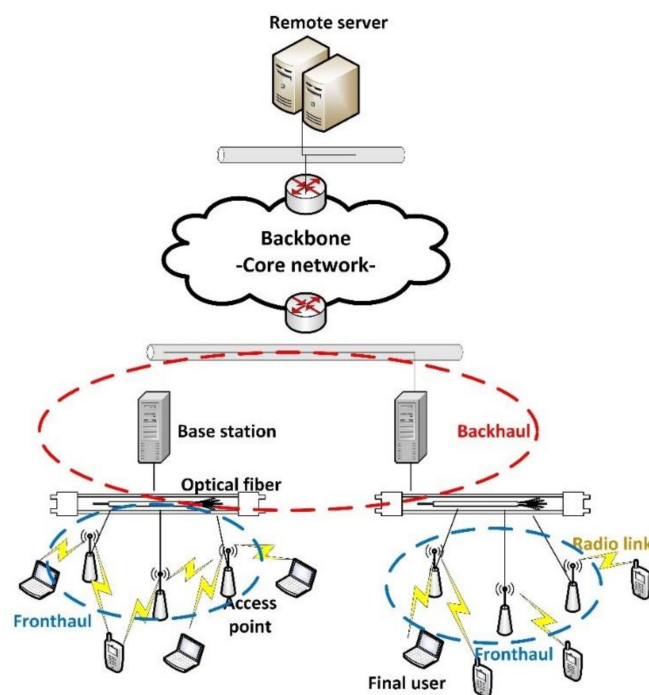
Many different architectures and paradigms have been proposed as an optimal solution for implementing future 5G networks [1]. From multi-frequency schemes combining microcells and macrocells [2]; to virtual infrastructures managed through commercial mechanisms such as Kubernettes [3]. Any case, all authors agree any solution for future 5G networks must guarantee three basic characteristics. Namely:

- Enhanced Mobile Broadband Communications (eMBC) [4]: Mobile nodes and devices must be provided with very high-speed communication links. Typically, experts indicate that effective bitrate should be above 50 Mbps.

- Ultra-Reliable Low Latency Communications (URLLC) [5]: Communication links supported by 5G networks must guarantee a very low delay and jitter in transmissions with remote nodes. According to most authors, jitter must be null and communication delays be below 10 (ten) milliseconds.
- Massive Machine-Type Communications (MMTC) [6]: In future 5G networks thousands of nodes and devices in pervasive infrastructures and dense deployments must communicate concurrently. All of them must be provided with eMBC and URLLC, and mobile networks must be able to handle these scenarios.

More efficient algorithms, communication protocols and network architectures are needed to meet these requirements. However, before all these engineering considerations, physical media connecting machines to be communicated must have a capacity high enough to support eMBC, URLLC and MMTC, all together and at the same time [7].

Nowadays, wireless links present much higher latencies and lower capacity than most modern wired transmission mechanisms [8], specifically than modern optical fiber technologies. Nevertheless, wireless channels are essential to guarantee mobility, the basic characteristic of mobile networks. Thus, in future 5G networks (as in novel 4G+ network deployments), physical media are following a hybrid approach [9]. A large number of wireless radio access points are placed close to final users, so transmission delays in those channels go down at the same time their physical capacity goes up (as the effective radio Signal-to-Noise ratio is higher). Besides, as several radio access points are deployed, it is easier to manage dense environments and pervasive infrastructures. Then, all these radio access points (and radio links) are communicated through high capacity optical fiber links to the base station, where data are processed and managed. This access network, then, communicates with the core network using traditional TCP/IP or Multiprotocol Label Switching (MPLS) solutions. The resulting physical infrastructure is usually known as Cloud Radio Access Network or C-RAN [10] (see Figure 1).



**Figure 1.** Scheme of C-RAN architectures in future 5G networks.

C-RAN infrastructures are, in general words, composed of a fronthaul network (made of proximity radio access points), and a backhaul network, where full capacity base stations are included.

Both networks are communicated through high performance optical links. Final users get connected to the fronthaul using radio mechanisms, which must be also adapted to meet the requirement of 5G networks. The backhaul may communicate to the backbone (or core network) using efficient packet communication technologies such as MPLS.

Access points in the 5G fronthaul are designed to forward messages in a very fast and efficient manner, as they have limited decision and processing capabilities (which are mainly deployed in base stations). Then, every solution deployed together with these access points in the fronthaul must fulfill these principia. In this context, one of the most critical mechanisms in terms of computational requirements and processing delay are cryptographic solutions and information protection schemes.

Currently, most common and secure cryptographic schemes are based on complex mathematical problems and high entropy random number generators. These approaches are, however, characterized by large processing delays and a very sparse scalability. Besides, in some occasions, huge redundancies are added, highly reducing the finally provided effective bitrate. Block ciphers, asymmetric keys, secure sessions, and similar solutions based on, for example, elliptic curves are typical solutions presenting these problems [11]. However, lighter cryptographic approaches [12] have been proved to be unsecure against some of the most typical attacks; and (what is more worrying) against modern and future cyber-physical attacks [13]. Then, a totally new and innovative approach is required to communicate access points in the fronthaul and base stations in the backhaul (where large processing resources are available).

Therefore, in this paper we propose a new solution addressing this problem. To provide secure communications in C-RAN architectures we are using a cryptographic solution at physical level, taking advantage of unclonable and non-linear behaviors and effects of optical fiber wires connecting the fronthaul and the backhaul. The proposed technology provides security to communications at physical layer, using only physical signals and mechanisms. Formally, the proposed technique generates an intrinsic Physical Unclonable Function based on resonance structures in optical rings, which produces a chaotic key which is mixed with private information using different techniques such as chaotic masking or modulation. Chaotic schemes may be vulnerable when supported by traditional processing nodes, but chaotic signals generated in optical rings are unclonable, so nobody can replicate their behavior even if they know their design and how the proposed technology operates. As this novel solution works at physical level, delays and bitrate are almost non affected, meeting the requirements of 5G networks.

The structure of the paper is as follows: Section 2 presents the state-of-the-art on information protection mechanisms for 5G networks and current C-RAN solutions. Section 3 describes the main proposal, including the mathematical foundations. Section 4 includes an experimental validation analyzing the performance of the proposed solution. Finally, Section 5 shows the conclusions and future work.

## 2. State of the Art on 5G Security Solutions and C-RAN Solutions

In this section we review the state of the art on C-RAN solutions, focusing on security mechanisms for future 5G networks. Section 2.1 discusses works on general C-RAN technologies and Section 2.2 focuses on 5G security solutions.

### 2.1. C-RAN Architectures, Solutions, and Characteristics

In C-RAN architectures, baseband processing, that is usually distributed among base stations in mobile networks [14], is centralized in a cloud computing center [15]. Two basic elements are identified in C-RAN architectures: the remote radio heads (RRH) and the Baseband processing units (BBU). RRH include all the hardware infrastructure (antennas, reception chains, etc.) required to communicate with the user devices. RRH are deployed in remote places near the users. The network of RRH is named as fronthaul. The fronthaul communicates through dedicated physical links (typically optical links) to the backhaul, a network where BBU are deployed. BBU include all the processing capabilities

required to manage communications between the mobile network and/among the users [16]. In 4G scenarios (most common approach nowadays), these BBU are hardware servers located between 20 and 40 km away [17]. This new network design reduces the energy consumption but may be costly in terms of CAPEX (as many large physical servers are needed). Besides, for very dense environments, this approach based on fixed physical server may, eventually, get congested.

Then, in future 5G scenarios, BBU are envisioned to be virtual entities, probably maintained through a small pool of data centers in the cloud [18]. This new approach reduces even more the energy consumption, greatly reduces the CAPEX of mobile networks, and allows a dynamic resource management, so congestion is less probable.

Many different works and applications based on the C-RAN paradigm have been reported, specially for those future engineered systems based on pervasive infrastructures where thousands of devices must communicate [10]. Each one of these applications understand the letter C in a different way: Cloud [17], Centralized processing [19], Cooperative radio [20], Collaborative [21] or Clean [22]. However, most common works try to describe the pending challenges for C-RAN solutions such as new virtualization techniques [23], or strict delay and jitter requirements [24].

Some authors apply C-RAN mechanisms to improve the support of nonuniform traffic and scalability in mobile networks [25]. Techniques such as statistical multiplexing [26] and dynamic resource allocation have been described [27]. Other authors are applying C-RAN paradigm to several different types of networks, such as Wireless Sensor Networks, to reduce energy consumption through the creation of community resource pools [28]. Moreover, some technologies to manage BBU through remote dashboards have been reported [29]. However, most common works on C-RAN applications try to deal with interferences, so the effective bitrate and global delay is improved. Different approaches to reduce the inter-cell interference [30] or employ interference paths constructively [24] may be found.

Finally, different innovative use cases about 5G C-RAN technologies applied to other popular systems have been reported. One of the most common examples is 5G C-RAN for IoT [31], although solutions for Wireless Sensor Networks [32] may be also found.

The security solution proposed in this paper is adequate for any of the previously described technologies and systems, as no computational resources are required. It must be only guaranteed that the fronthaul and the backhaul are connected using optical media.

## 2.2. Security Technologies for C-RAN Architectures

Works on security and 5G networks, as 5G technologies are still under discussion, tend to be very theoretical and abstract. Most articles on this topic present models or logical architectures where security functionalities are identified and described [33], but access networks are managed as a monolithic component where the internal organization is not addressed. In this sense, most common works are only focused on identifying future threats to 5G networks [34,35], such as saturation attacks, TCP-level attacks, resource theft or signaling storms.

Articles describing security solutions in a more detailed manner, are always focused on a particular paradigm or approach to implement future 5G networks. Several authors, then, analyze security solutions for 5G networks when implemented through virtual network functions. A large catalogue of solutions has been reported in this context. From access control mechanisms based on traffic engineering [36], to very specific technologies to prevent IMSI-cracking attacks [37], Denial of Service attacks [38] and identity verification [39]. On the contrary, other works analyze and discuss about enhanced security solutions that are envisioned to be included in future standards by the 3GPP organization [40].

However, all these works are only addressing security issues in the radio channel between the base station (regardless its internal configuration) and the mobile user. Thus, three topics are usually discussed: user authentication, securitization of wireless links and security policies to be implemented in the user equipment. The specific problems associated to C-RAN architectures are not analyzed.

In fact, a second important group of proposals about security in 5G networks is focused in Radio Access Networks, but only in the radio segment. Lightweight security solutions for resource constrained devices have been reported [41], in particular to guarantee device authentication. Techniques to guarantee service availability and data privacy (through electromagnetic noise or data processing techniques) [42] may be also found. Although in these works, sometimes, access network is considered as two-segment network, solutions are not describing how this structure affects or modifies the technology operation. So, no specific solution to preserve security in communications between those segments is analyzed.

Some authors specifically refer the fronthaul and backhaul networks in their works [43]. Nevertheless, these works are still initial and only discuss about how to integrate security recommendations (for example, from the International Telecommunication Union) in 5G networks. No technological detail is provided.

Security solutions for 5G networks at physical layer are probably the most reported technologies. Although, as previously said, most works are analyzing the security threats, challenges and opportunities [44–46]; some specific technologies have been reported. In particular, technologies based on different channel estimators to prevent spoofing attacks in the wireless media have been described [47]. Contrary to these previous solutions, the proposed technique in this paper is focused on the wired media, connecting the fronthaul and the backhaul.

Finally, a sparse collection of security technologies specifically designed for C-RAN architectures may be found. However, in this case, the security policies are still focused either on the mobile service (authentication, impersonation attacks, etc.), or the wireless radio link [48]. Different mechanisms to authenticate user devices in C-RAN architecture have been proposed, but most of them are defined at service level using, for example, XML files and SOAP interfaces [49]. Any case, most numerous works on security and C-RAN architectures are focused on radio channels. Secure handovers [50] and secure downlinks [51,52] in heterogenous wireless access networks have been described. Although all these solutions are designed at message exchange (logical level). Other techniques at radio level for Massive Input Massive Output (MIMO) have been also reported [53,54], although they are focused on communications between user devices and wireless access points. Communications between the fronthaul and the backhaul are, once more, not addressed.

At this point, we are briefly analyzing previous proposals about chaotic intrinsic Physical Unclonable Functions (PUF) in optical media.

No work on this topic applied to 5G networks has been reported. However, some generic proposals about these technologies may be found. In general, chaos in optical and resonant media and structures is analyzed as secondary effect which must be removed to improve the signal quality [55]. Although some practical implementation of resonant structures for intrinsic PUF using optical fibers have been reported [56]. In all these cases, nevertheless, the objective of these PUFs is to create a numerical pseudorandom key to feed a standard encryption scheme [57] or an external and specific modulation component [58]. On the other hand, most practical implementation of chaotic systems in optical communications are based on non-linear effects in laser [59,60], what requires a complex control solution to manipulate optical signals. Contrary to all these works, in our proposal we are taking advantage of two different “random” effects (non-linearities and resonant structures) to provide an entire cryptographic solution at physical level. No algorithm or digital signal processing instrument or software is required. Only physical optical components organized in a specific manner are needed.

### 3. A New Protection Solution for Communications at Physical Layer in C-RAN Architectures

In this Section, the proposed new security technology for C-RAN architectures is described. First, we are discussing about the non-linear phenomena in optical fiber links that may be employed to create chaos at physical level and, then, generate a PUF. The proposed PUF will take advantage of resonant structures to embed the chaotic masking and modulation cryptographic scheme in the optical media (Section 3.2). In Section 3.3, resonant structures and non-linearities in optical fibers



are analyzed together, so the produced chaotic signals and masking information is deduced and mathematically defined. Finally (Section 3.4), the whole cryptographic system is presented as an information protection infrastructure.

### 3.1. Non-Linear and Unclonable Effects in Optical Fibers

In standard optical communication systems, linear dynamics are employed to model the signal transmission [61]. This approach is very successful to design effective communication mechanisms, maximizing the link distance and signal quality. Nevertheless, in this approach, all non-linear effects are grouped and modeled as different distortion sources which must be removed or controlled in order to preserve the Signal-to-Noise ratio [61]. However, a very interesting characteristic of all these non-linearities must be considered: they are unclonable.

Non-linearities in optical media are caused by unpredictable and uncontrollable phenomena during manufacturing, the raw material composition and, even, the molecular structure of transmission media. Nowadays, it is impossible to create two optical fiber wires with identical non-linearities, even for manufacturers. An even if the fiber to be replicated is known. These unclonable effects, if exploited, can generate unclonable signals, as response to certain stimuli (or challenges). The resulting functionality is known as intrinsic Physical Unclonable Function (PUF).

In optical media, non-linearities can be stimulated using external nonlinear pumping power sources. However, this approach requires additional active components, energy and complex and precise control mechanisms. Then, in this work, to build the proposed PUF we employ passive non-linear effects which are present in an intrinsic manner in every optical medium: signal modulation due to variations in the refraction index.

In linear models, refraction index in silicon optical fibers  $\eta$  is constant (1). However, due to several uncontrollable effects, this refraction index  $\eta$  changes and varies when the silicon material is under an electromagnetic field  $\vec{E}$  (2) with wavelength  $\lambda$  in vacuum. Our silicon material is also absorbent in that wavelength, with a ratio of  $\alpha$  dB/m. In the most general case, the function  $f_\eta$  that governs the behavior of the refraction  $\eta$  index is unknown:

$$\eta = \eta_0 \quad (1)$$

$$\eta = \eta(\vec{E}) = f_\eta(\vec{E}) \quad (2)$$

Without loss of generality we assume the transmission medium is placed in a cartesian system. We also assume, as in commercial optical fibers, that the media has a cylindrical geometry and it is placed matching the longitudinal axis to z-axis. Then, the electromagnetic field  $\vec{E}$  may be developed according to cylindrical unitary vectors  $\{\vec{r}, \vec{\phi}, \vec{z}\}$  in that space (3). Moreover, although unknown, the function describing the behavior of refraction index  $\eta$  may be developed using the Taylor's theorem, and the McLaurin series if the Taylor polynomial is developed around zero (4). To make easier future manipulations, this McLaurin series may be also expressed using the gradient operator  $\nabla$ :

$$\vec{E}(t, r, z) = E_r(t, r, \phi, z) \cdot \vec{r} + E_\phi(t, r, \phi, z) \cdot \vec{\phi} + E_z(t, r, \phi, z) \cdot \vec{z} \quad (3)$$

$$\eta = f_\eta(\vec{E}) = f_\eta(E_r, E_\phi, E_z) = f_\eta(\vec{0}) + \sum_{k=0}^{\infty} \frac{1}{k!} \sum_{k_1+k_2+k_3=k} \binom{k}{k_1 \cdot k_2 \cdot k_3} \frac{\partial^k f_\eta(\vec{0})}{\partial E_r^{k_1} \cdot \partial E_\phi^{k_2} \cdot \partial E_z^{k_3}} (E_r^{k_1} \cdot E_\phi^{k_2} \cdot E_z^{k_3}) \quad (4)$$

$$\eta = \sum_{k=0}^{\infty} \frac{1}{k!} (\nabla f_\eta(\vec{0}) \cdot [E_r + E_\phi + E_z])^k \quad (5)$$

This Taylor polynomial may be expressed in a more compact manner, considering new variables  $\eta_k$  (6)–(7) as:

$$\eta_k = \frac{1}{k!} \left( \nabla f_{\eta} \left( \vec{0} \right) \right)^k, \quad (6)$$

$$\eta = \sum_{k=0}^{\infty} \eta_k \cdot (E_r + E_{\phi} + E_z)^k \quad (7)$$

To make implementable and measurable this infinite series (7), the Taylor polynomial must be truncated, considering a maximum order  $N_{max}$  (8). Some polynomials are well-known and have specific names. For example, if  $N_{max} = 1$ , the resulting phenomena is known as Pockels effect; and the second order them ( $k = 2$ ) is known as Kerr effect:

$$\eta \approx \sum_{k=0}^{N_{max}} \eta_k \cdot (E_r + E_{\phi} + E_z)^k \quad (8)$$

As the maximum order  $N_{max}$  goes up, the real impact of nonlinear effects goes down. However, all of them contribute to generate the final and unclonable signal.

Now, in order to evaluate if the resulting expression defines a nonlinear dynamic, we must find the differential equations describing the behavior of the electromagnetic field in the optical media under study. As commonly assumed, in our optical media there are not electrical charges or external currents. The magnetic permeability is equal to the permeability in the vacuum,  $\mu_0$ . Then, the Maxwell's equations in the optical media may be simplified (9).  $\epsilon_0$  is the vacuum's electrical permittivity and  $\vec{H}$  is the magnetic field generated in the medium:

$$\begin{aligned} \nabla \cdot (\eta^2 \epsilon_0 \cdot \vec{E}) &= 0, \\ \nabla \times \vec{E} &= -\mu_0 \frac{\partial \vec{H}}{\partial t}, \\ \nabla \cdot (\mu_0 \cdot \vec{H}) &= 0, \\ \nabla \times \vec{H} &= \frac{\partial (\eta^2 \epsilon_0 \cdot \vec{E})}{\partial t}. \end{aligned} \quad (9)$$

Calculating the rotational of Faraday's law, and employing the Ampere's law, we can obtain a differential equation for obtaining the electrical field (10). The obtained vector equation may be split into two different scalar equations (11). Besides, although energy also propagates in a radial way ( $E_r \neq 0$ ), radial signals tend to disappear in the open space, they do not remain within the optical fiber and then they cannot be used for communication purposes. Therefore, we are considering only  $E_z$  component is employed to communicate and received by the final user:

$$\Delta \vec{E} = -\mu_0 \epsilon_0 \frac{\partial^2 (\eta^2 \cdot \vec{E})}{\partial t^2}, \quad (10)$$

$$\begin{aligned} \Delta E_r &= -\mu_0 \epsilon_0 \frac{\partial^2 (\eta^2 \cdot E_r)}{\partial t^2}, \\ \Delta E_{\phi} &= -\mu_0 \epsilon_0 \frac{\partial^2 (\eta^2 \cdot E_{\phi})}{\partial t^2}, \\ \Delta E_z &= -\mu_0 \epsilon_0 \frac{\partial^2 (\eta^2 \cdot E_z)}{\partial t^2}. \end{aligned} \quad (11)$$

With these considerations, and employing the Newton notation for temporal derivatives, the Laplacian operator and the Cauchy product, we can obtain the final expression which should be resolved using the adequate numerical method (12). First, the contour problem should be resolved. This process is not analyzed in this paper, as we are focusing on temporal dynamics employed to generate signals with cryptographic applications. Any case, the contour problem is solved through the

continuity conditions in the geometric space  $r = R$ , where  $R$  is the radix of the optical fiber (optical fibers are open media and fields must be continuous in the transitions with open space).

$$\begin{aligned}
& \frac{\partial^2 E_i}{\partial r^2} + \frac{1}{r} \frac{\partial E_i}{\partial r} + \frac{1}{r^2} \frac{\partial^2 E_i}{\partial \phi^2} + \frac{\partial^2 E_i}{\partial z^2} = -\mu_0 \varepsilon_0 (2\eta \ddot{\eta} E_i + 4\eta \dot{\eta} \dot{E}_i + \eta^2 \ddot{E}_i), \\
& \frac{\partial^2 E_i}{\partial r^2} + \frac{1}{r} \frac{\partial E_i}{\partial r} + \frac{1}{r^2} \frac{\partial^2 E_i}{\partial \phi^2} + \frac{\partial^2 E_i}{\partial z^2} = \\
& = -\mu_0 \varepsilon_0 2E_i \left[ \sum_{k=0}^{N_{max}} \eta_k \cdot k \cdot (k-1) \cdot (E_r + E_\phi + E_z)^{k-2} \cdot (\ddot{E}_r + \ddot{E}_\phi + \ddot{E}_z) \right] \left[ \sum_{k=0}^{N_{max}} \eta_k \cdot (E_r + E_\phi + E_z)^k \right] - \\
& -4\mu_0 \varepsilon_0 \left[ \sum_{k=0}^{N_{max}} \eta_k \cdot k \cdot (E_r + E_\phi + E_z)^{k-1} \cdot (\dot{E}_r + \dot{E}_\phi + \dot{E}_z) \right] \left[ \sum_{k=0}^{N_{max}} \eta_k \cdot (E_r + E_\phi + E_z)^k \right] \dot{E}_i - \\
& -\mu_0 \varepsilon_0 \left( \left[ \sum_{k=0}^{N_{max}} \eta_k \cdot (E_r + E_\phi + E_z)^k \right] \right)^2 \cdot \ddot{E}_i, \\
& \frac{\partial^2 E_i}{\partial r^2} + \frac{1}{r} \frac{\partial E_i}{\partial r} + \frac{1}{r^2} \frac{\partial^2 E_i}{\partial \phi^2} + \frac{\partial^2 E_i}{\partial z^2} = \\
& = -\mu_0 \varepsilon_0 2E_i (\ddot{E}_r + \ddot{E}_\phi + \ddot{E}_z) \left[ \sum_{k=0}^{N_{max}} \sum_{i=0}^k \eta_{k-i} \cdot \eta_k \cdot k \cdot (k-1) (E_r + E_\phi + E_z)^{2k-2-i} \right] - \\
& -4\mu_0 \varepsilon_0 \dot{E}_i (\dot{E}_r + \dot{E}_\phi + \dot{E}_z) \left[ \sum_{k=0}^{N_{max}} \sum_{i=0}^k \eta_{k-i} \cdot \eta_k \cdot k \cdot (E_r + E_\phi + E_z)^{2k-1-i} \right] - \\
& -\mu_0 \varepsilon_0 \ddot{E}_i \left[ \sum_{k=0}^{N_{max}} \sum_{i=0}^k \eta_{k-i} \cdot \eta_k \cdot (E_r + E_\phi + E_z)^{2k-i} \right], \\
& i \in \{r, \phi, z\}.
\end{aligned} \tag{12}$$

Then, after solving the contour problem, we obtain an independent function  $F(t, r, \phi, z)$  for the Laplacian operator (depending on the spatial geometry of the medium), and considering that  $\eta_k$  coefficients are unknown parameters (whose values depend on manufacturing processes and other uncontrollable phenomena), we can finally obtain a temporal dynamic describing the temporal problem governing the scenario under study (13). In the initial value problem, the initial conditions may be freely selected as they are not controllable in real scenarios. As can be seen, the resulting dynamic presents high-order polynomial terms which show non-linear behavior:

$$\begin{aligned}
& F(t, r, \phi, z) = \\
& = E_i (\ddot{E}_r + \ddot{E}_\phi + \ddot{E}_z) \left[ \sum_{k=0}^{2N_{max}-2} a_k \cdot (E_r + E_\phi + E_z)^k \right] + \\
& + \dot{E}_i (\dot{E}_r + \dot{E}_\phi + \dot{E}_z) \left[ \sum_{k=0}^{2N_{max}-1} b_k \cdot (E_r + E_\phi + E_z)^k \right] + \\
& + \ddot{E}_i \left[ \sum_{k=0}^{2N_{max}} c_k \cdot (E_r + E_\phi + E_z)^k \right], \\
& i \in \{r, \phi, z\}.
\end{aligned} \tag{13}$$

### 3.2. Resonant Structures in Optical Fibers

The obtained expressions (13) are nonlinear, they define a PUF, but this condition is not enough to guarantee the generation of signals with cryptographic applications (which must be pseudo-random, as chaotic signals). In order to obtain those uncontrollable (chaotic) signals two main requirements must be fulfilled. First, at least three state variables must be defined in the dynamic. The Poincaré-Bendixon theorem establishes that dynamics with order below three only generate periodic or fixed trajectories [62] (without cryptographic applications). Then, at least three different state variables must be defined. Second, the dynamic must show an unstable behavior. In fact, erratic dynamics must have, at least, one expansion direction to support the uncontrollable behavior of those signals.

Resonant structures may be employed to meet both requirements, especially if a cavity-like structure is created, where the Akimoto instability may be found [56]. The original Akimoto system was made of four mirrors and a dielectric linear medium (see Figure 2), forcing the optical beams



to circulate in a square ring. In that system, similar to a resonant cavity, if the dielectric medium presents any nonlinearity (i.e., in any realistic implementation), the electromagnetic signals could be unbounded depending on the excitation signal. Although this infrastructure may support erratic behaviors, it presents two main disadvantages: the construction is complex (mixing two different dielectric materials, mirrors, etc.); and the behavior of the system depends on the excitation signals (what is impractical as communication signals should not be restricted). In this Section we investigate a different cavity-like structure (so the Akimoto instability is present), including new non-idealities such as polarization changes, so the resulting infrastructure supports unstable solutions by its geometry and characteristics, independently from the excitation signal.

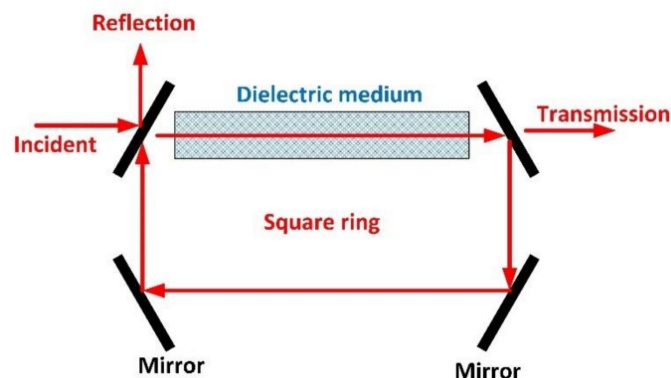


Figure 2. Traditional Akimoto's system.

A traditional cavity-like structure (see Figure 3) is composed of two reflective walls, and a dielectric medium to support the signal transmission. In that structure, three different electrical signals must be considered to study the temporal evolution of the system: the input signal  $\vec{E}_{in}$ , the signal circulating inside the cavity  $\vec{E}_n^c$  (indicating  $n$  the number of circulations the signal does inside the cavity) and the output signal  $\vec{E}_{out}$ . Besides, each reflective wall is characterized by a duple of positive real parameters  $\{\rho_i, \xi_i\}$ , where  $\rho_i$  is the amplitude reflection coefficient and  $\xi_i$  is the amplitude transmission coefficient. No phase change is induced by reflective walls. It is important to note that  $\rho_i + \xi_i = 1$ .

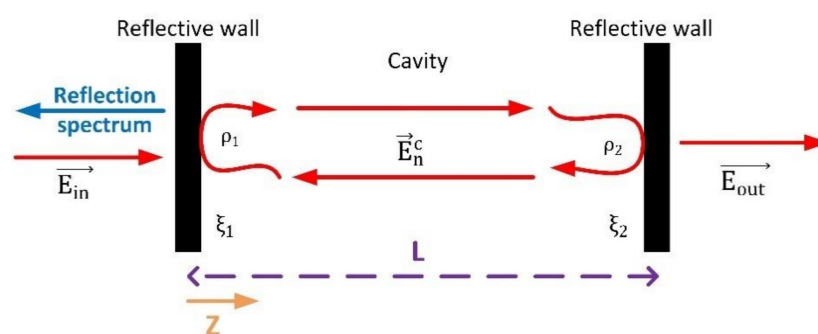


Figure 3. Resonant cavity-like infrastructure.

If the input signal  $\vec{E}_{in}$  is a plane wave and the cavity is ideal, the mathematical expression of  $\vec{E}_n^c$  may be easily deduced (14) using the ray theory for electromagnetic waves. In that expression  $L$  indicates the length of the cavity (geometric conditions). Now, we are introducing a new realistic non-ideality: interferences inside the cavity. In real optical media, as energy circulates, changes in signal polarization may occur or different transmission modes could be excited. These circulating signals do not match the input signal and, then, it appears a destructive interference. The incident signal and the signal in the cavity cannot be totally added, cause in the interference process some energy

is destroyed. To model this situation different strategies may be found but, in this paper, we are using a coupling coefficient  $\gamma$  depending on the wavelength of the optical carrier  $\lambda$ , the first order refraction index  $\eta_0$ , and the geometry of the cavity (15). In our model, this coefficient is, in general, an unknown function and may be modeled using, as previously said, Taylor series (16), and considering a maximum order of  $M_{max}$  polynomial terms:

$$E \rightarrow_n^c = \xi_1 \cdot (\rho_1 \cdot \rho_2)^n \cdot \vec{E}_{in}(t, r, \phi, 2nL), \tag{14}$$

$$E \rightarrow_n^c = \gamma(\lambda, R, L, \eta_0) \cdot \xi_1 \cdot (\rho_1 \cdot \rho_2)^n \cdot \vec{E}_{in}(t, r, \phi, 2nL), \tag{15}$$

$$\begin{aligned} \gamma &= \gamma(\lambda, R, L, \eta_0) = \\ \gamma(\vec{0}) &+ \sum_{k=0}^{\infty} \frac{1}{k!} \sum_{k_1+k_2+k_3+k_4=k} \binom{k}{k_1 \cdot k_2 \cdot k_3 \cdot k_4} \frac{\partial^k \gamma(\vec{0})}{\partial \lambda^{k_1} \cdot \partial R^{k_2} \cdot \partial L^{k_3} \cdot \partial \eta_0^{k_4}} (\lambda^{k_1} \cdot R^{k_2} \cdot L^{k_3} \cdot \eta_0^{k_4}) = \\ &= \sum_{k=0}^{\infty} d_k \cdot (\lambda + R + L + \eta_0)^k \approx \sum_{k=0}^{M_{max}} d_k \cdot (\lambda + R + L + \eta_0)^k. \end{aligned} \tag{16}$$

Although the reflection spectrum is useful for certain applications, in cryptographic applications we need strong signals, so we are focusing on the output signal  $\vec{E}_{out}$ . As may be seen, with each circulation in the cavity, a part of the energy is getting out (17), so output optical carrier is time variant (modulated) with a frequency depending on the cavity length, known as resonance frequency  $f_r$  (18); being  $c_{light}$  the light speed in the vacuum:

$$\vec{E}_{out}(n, r, \phi, z) = \xi_2 \cdot E \rightarrow_n^c \tag{17}$$

$$f_r = \frac{c_{light}}{2L\eta} \approx \frac{c_{light}}{2L\eta_0} \tag{18}$$

Any case, standard frequencies in communication signals are much slower than light speed in optical media and, then, than resonance frequencies. Thus, we can consider the variations caused by energy circulating in the cavity as a transitory convergence phenomenon; and we must, then, study the long-term response. This response may be obtained just adding all the partial outputs (19):

$$\begin{aligned} \vec{E}_{out}(t, r, \phi, z) &= \lim_{n \rightarrow \infty} \vec{E}_{out}(n, r, \phi, z) \\ &= \sum_{n=0}^{\infty} \xi_2 \cdot \xi_1 \cdot \gamma(\lambda, R, L, \eta_0) \cdot (\rho_1 \cdot \rho_2)^n \cdot \vec{E}_{in}(t, r, \phi, 2nL). \end{aligned} \tag{19}$$

Considering the cylindrical geometry of optical fibers, only components propagating in the z-axis could operate in a resonant cavity (20). Besides, as  $\rho_i$  and  $\xi_i$  parameters are positive but below the unit, and, because of the energy absorption, the magnitude of electromagnetic waves reduces with each circulation (21). Then, the series may be added, and the result is convergent (22):

$$\begin{aligned} \vec{E}_{out}(t, r, \phi, z) &= E_z^{out}(t, r, \phi, z) \cdot \vec{z} = \\ &= \left( \sum_{n=0}^{\infty} \xi_2 \cdot \xi_1 \cdot \gamma(\lambda, R, L, \eta_0) \cdot (\rho_1 \cdot \rho_2)^n \cdot E_z^{in}(t, r, \phi, 2nL) \right) \cdot \vec{z}, \end{aligned} \tag{20}$$

$$\|E_z^{in}(t, r, \phi, 2nL)\| < \|E_z^{in}(t, r, \phi, 2(n+1)L)\| \forall n \in \mathbb{N} \tag{21}$$

$$E_z^{out}(t, r, \phi, z) = \xi_2 \cdot \xi_1 \cdot \gamma(\lambda, R, L, \eta_0) \cdot \sum_{n=0}^{\infty} (\rho_1 \cdot \rho_2)^n \cdot E_z^{in}(t, r, \phi, 2nL) = S < \infty. \tag{22}$$

The challenge in the obtained expression (22) is to calculate the components  $E_z^{in}$  of the electromagnetic waves on the surface of the second reflective wall. Besides, in WDMA (Wavelength-division multiple access) systems the superposition principle should be employed to analyze each optical carrier separately.

### 3.3. Generating Chaotic Resonant Phenomena in Optical Links

The obtained mathematical expression (22) for a cavity-like infrastructure may be easily replicated but using a much more simple and compact solution: an optical ring (see Figure 4). This ring is connected to a main link through a coupler characterized by a coupling parameter  $\kappa$  and  $\delta$  insertion losses. Then, this all-pass ring represents a resonant cavity satisfying some simple relations (23). This solution, moreover, can be easily integrated into optical links connecting the fronthaul and the backhaul in C-RAN architectures:

$$\begin{aligned}\rho_1 &= \sqrt{1 - \delta}, \\ \rho_2 &= \sqrt{1 - \kappa}, \\ \xi_1 &= 1 - \delta, \\ \xi_2 &= \kappa \cdot \sqrt{1 - \kappa}.\end{aligned}\quad (23)$$

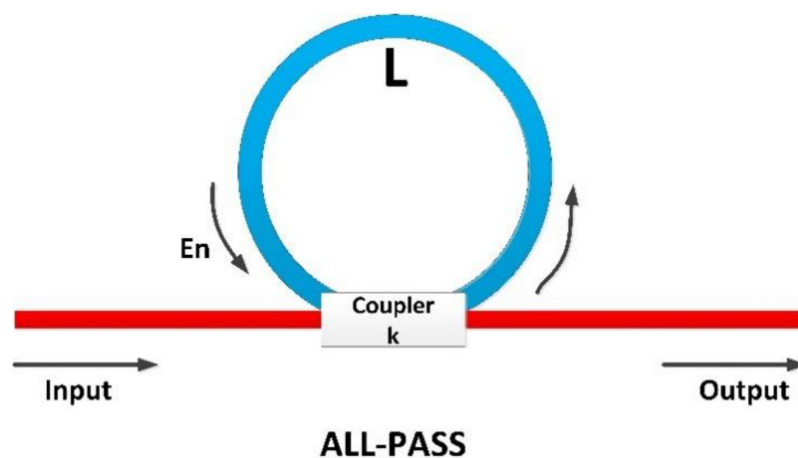


Figure 4. Cavity-like all-pass ring resonator.

Now, as these all-pass rings are made of optical fibers, components  $E_z^{in}$  may be calculated using the previously obtained non-linear dynamic expression (13). At this point, the problem is well posed and all conditions to guarantee the generation of erratic signals with cryptographic applications are met.

Any case, these conditions are necessary but no sufficient, so we must numerically evaluate if the obtained model can support the expected behavior. Specifically, the referred erratic behavior is mathematically known as chaos. Several different methods to analyze if a non-linear dynamic generates chaos can be employed. Because of its low computational complexity and high visibility, we are using the Lyapunov exponents.

Lyapunov exponents are a measurement that indicates the relative evolution of two trajectories that are as close as desired in the initial point. There is one exponent for each state variable in a dynamic. Chaotic dynamics must diverge in one direction (Lyapunov's exponent is positive), but they must converge in another one to avoid the hole trajectory to diverge. This equilibrium is, in fact, the origin of chaos. Then, we are evaluating the maximum Lyapunov exponent, analyzing (at the same time) the trajectory is not divergent.

In real applications, although many parameters have been previously introduced, only five are configurable: the wavelength of the optical carrier  $\lambda$ , the length of the ring  $L$ , the radius of the optical fiber  $R$ , and the characteristics of the coupler, the coupling parameter  $\kappa$  and the insertion losses  $\delta$ .

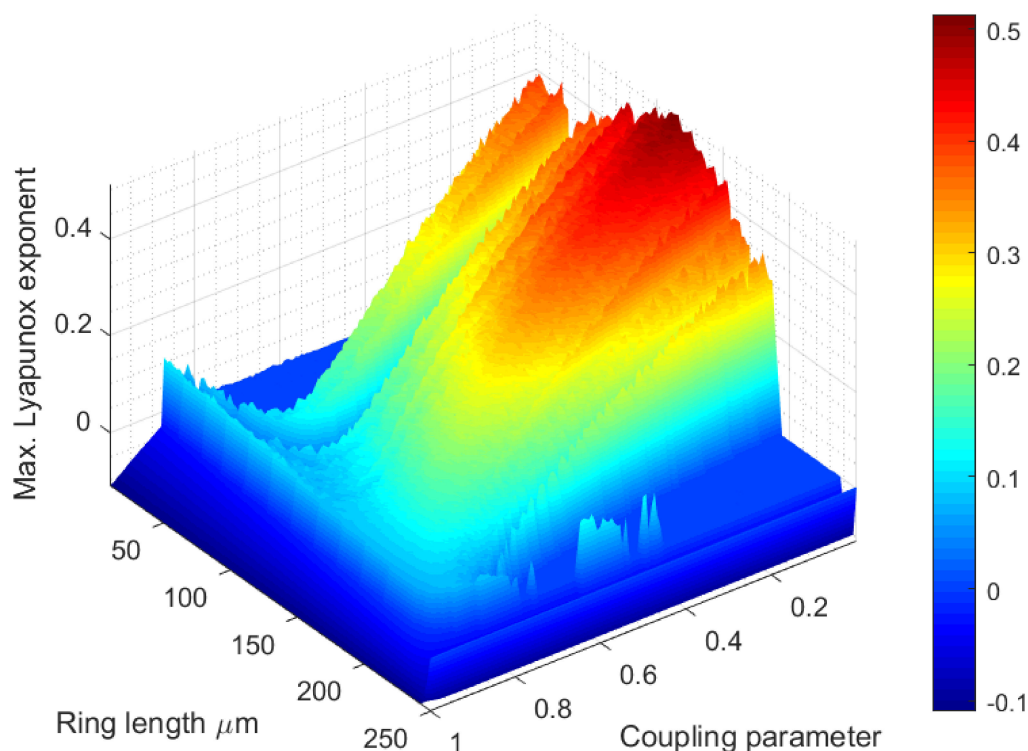
More typically, only the length of the ring  $L$  and the coupling parameter  $\kappa$  can be freely fixed, as commercial devices present fix values for almost every other parameter. Besides, unknown parameters  $a_k$ ,  $b_k$ ,  $c_k$  and  $d_k$  cannot be controlled (as said for Physical Unclonable Functions). Thus, to select values for those parameters we are using a Montecarlo method (several numerical evaluations for different values are performed), and the mean values resulting from these studies are taken the final results. Table 1 represents the selected values for the other parameters. Values for Montecarlo

experiment and electromagnetic waves are taken from embedded models in MATLAB software (the software we used for this numerical analysis).

**Table 1.** Selected values for the Lyapunov numerical study.

Parameter	Value	Comments
$\delta$	0.1 dB	Common commercial value
$\lambda$	1500 nm	Common value
$\vec{E}_{in}$	$\cos\left(\frac{2\pi}{\lambda}c_{light}\cdot t\right)$	Elemental harmonic signal
R	5 $\mu m$	Common commercial value

Figure 5 shows the obtained results for the maximum Lyapunov exponent and different values of the ring length  $L$  and the coupling parameter  $\kappa$ .



**Figure 5.** Lyapunov maximum exponent: bidimensional diagram.

As can be seen, the maximum Lyapunov exponent is positive for large areas and combinations of different ring lengths and coupling parameters. Although values are not very high and represent a moderate complex chaos, the obtained results are similar to which generated by other dynamics successfully applied to cryptography (as the Lorenz dynamic) [63]. Thus, the proposed model can be employed in security applications in future C-RAN architectures.

### 3.4. Information Protection Infrastructure

At this point, the proposed solution can generate an unclonable chaotic signal when excited with an optical signal. However, in order to apply the proposed scheme in practical situations, a whole cryptographic mechanism is required. Figure 6 shows that system.

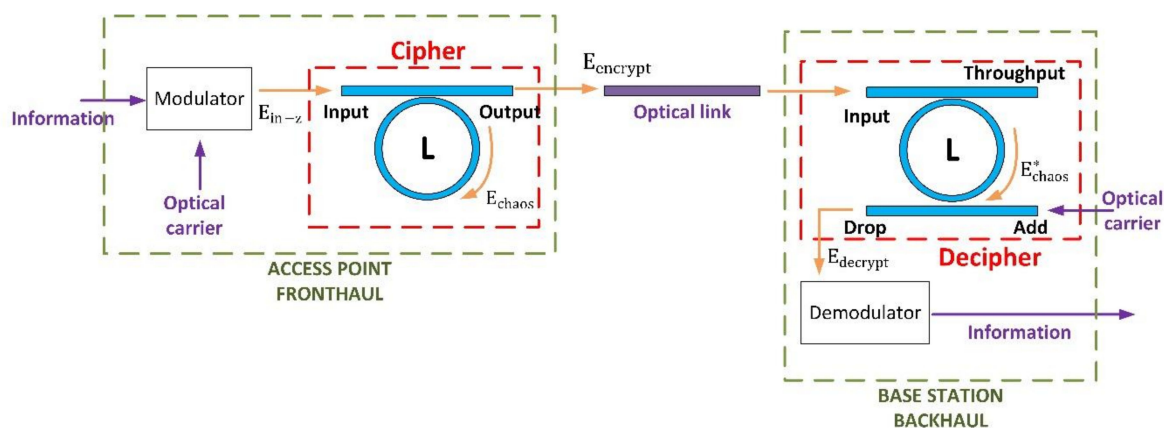


Figure 6. Proposed information protection scheme for C-RAN architectures.

As can be seen, the proposed system includes three different parts: (i) the transmitter, where a cipher at physical level based on the previously described PUF and chaotic signals is included; (ii) an optical fiber link connecting the access point (transmitter) and the base station (receptor) in the C-RAN architecture; and (iii) a receptor, where a complementary resonant ring is included to cancel the chaotic noise in the optical signal and recover the clear information.

As all nonlinearities in the system are additive, and using the superposition principle, we can assume the encrypted signal  $E_{encrypt}$  at physical level in the transmitter is the addition of two signals (24): the original information signal  $E_{info}$  (associated to linear effects in the optical fiber), and the chaotic masking signal (associated to uncontrollable nonlinear phenomena)  $E_{chaos}$ :

$$E_z^{out}(t, r, \phi, z) = E_{encrypt}(t) = E_{info} + E_{chaos} \tag{24}$$

The chaotic signal  $E_{chaos}$  can only be obtained using the previously described nonlinear dynamic (22), but the information signal  $E_{info}$  may be related to the incident wave  $E_{in}$  through the traditional linear theory (25), and being  $\alpha$  the linear attenuation caused by the energy absorption of materials in the optical fiber:

$$E_{info} = E_{in-z} \cdot e^{-\alpha L} \cdot \cos\left(\frac{2\pi}{\lambda} \frac{c_{light}}{\eta_0} t - \frac{2\pi}{\lambda} L\right). \tag{25}$$

The proposed cipher is an all-pass ring resonator made of optical fiber, which (at the same time) produces the chaotic signal  $E_{chaos}$  and mixes it with the clear information  $E_{info}$ , using a chaotic making scheme (where the chaotic signal hides the original information). This encryption (masking) mechanism is supported by the physical structure of the ring, and its electromagnetic response when excited with the optical carrier. No computational infrastructure of resource is needed. All operations are performed at physical level.

Then, the access point in the fronthaul and the base station in the backhaul are connected through an optical link. This link is connected to a receptor where the chaotic masking process is reversed (decryption). To do that, the decipher includes a new ring resonator, which must be built using the exact same optical fiber than the ring in the cipher (to ensure both have the same nonlinearities). This new ring, however, follows an add-drop paradigm. The encrypted signal  $E_{encrypt}$  is introduced in the “input” port. This ring is, besides, excited in the “add” port using an “empty” optical carrier (26) in the same wavelength than the encrypted signal. Then, if the optical fiber is exactly the same than the one employed in the cipher, the same chaotic signal  $E_{chaos}^*$  will be generated in the ring (27). Couplers in the transmitter and receptor to be as similar as possible. This chaotic signal is added to the

encrypted signal in the “throughput” port (28), but it is subtracted in the “drop” port (this result may be easily deducted using the ray theory for optical waves) (29):

$$E_{add}(t, r, \phi, z) = \cos\left(\frac{2\pi c_{light}}{\lambda \eta_0} t\right), \quad (26)$$

$$E_z^{out*}(t, r, \phi, z) = E_{chaos}^* + E_{add} = E_{chaos} + E_{add}, \quad (27)$$

$$E_{through}(t, r, \phi, z) = E_z^{out*} + E_{encrypt}, \quad (28)$$

$$\begin{aligned} E_{drop}(t, r, \phi, z) &= E_{encrypt} - E_z^{out*} = E_{info} + E_{chaos} - (E_{chaos} + E_{add}) = \\ &= E_{info} + \cos\left(\frac{2\pi c_{light}}{\lambda \eta_0} t\right). \end{aligned} \quad (29)$$

The decrypted signal  $E_{decrypt}$  is, then, directly obtained (the chaotic masking is removed). And only a peak of optical power in the frequency of the carrier is added (30). However, this spurious energy will be removed in the demodulation and detection device. The original private information is then recovered in the base station with no computational cost (only physical phenomena are employed). Some distortion caused by transmission degradation may appear, but how resilient to these effects is the proposed scheme will be later evaluated. Furthermore, if chaotic signals are weak in the employed optical fiber, they can be always strengthened using optical amplifiers with no computational consumption:

$$E_{decrypt} = E_{drop} = E_{info} + \cos\left(\frac{2\pi c_{light}}{\lambda \eta_0} t\right) \quad (30)$$

#### 4. Experimental Validation and Results

In order to evaluate the performance of the proposed technology, we are carrying out a validation composed of two experiments. The first experiment was focused on the performance of the solution as security and information protection technology. The second experiment was focused on analyzing the proposed technique from the telecommunication engineering point of view.

All these experiments were implemented using a simulation scenario. The selected simulation scenario represented a quite realistic application scenario of 5G networks, although the number of final devices, access point or base station does not affect the described technology. Then, a fronthaul composed of one hundred access points and a backhaul composed of twenty base station is considered (similar values may be currently found in metropolitan areas). The distance between both elements was fixed to 3 km (a standard value in real scenarios). Besides, the access points are provided with the proposed cipher and the base station with the corresponding decipher. All the simulations were performed using the MATLAB 2019a software, where specific models for optical communications are embedded. All simulations were performed using a Linux architecture (Linux 16.04 LTS) with the following hardware characteristics: Dell R540 Rack 2U, 96 GB RAM, two processors Intel Xeon Silver 4114 2.2G, HD 2TB SATA 7,2K rpm. Optical communications were designed to work on the second optical window. Table 2 describes the values for all relevant parameters in the proposed simulations [64]. Parameters that are not included in Table 2 are employed as independent or control variables.

**Table 2.** Selected values for the experimental validation.

Parameter	Value	Comments
$\delta$	0.1 dB	Common commercial value
$\lambda$	1310 nm	Second optical window
$E_{in}$	-	Random sequences of bits
R	5 $\mu$ m	Common commercial value

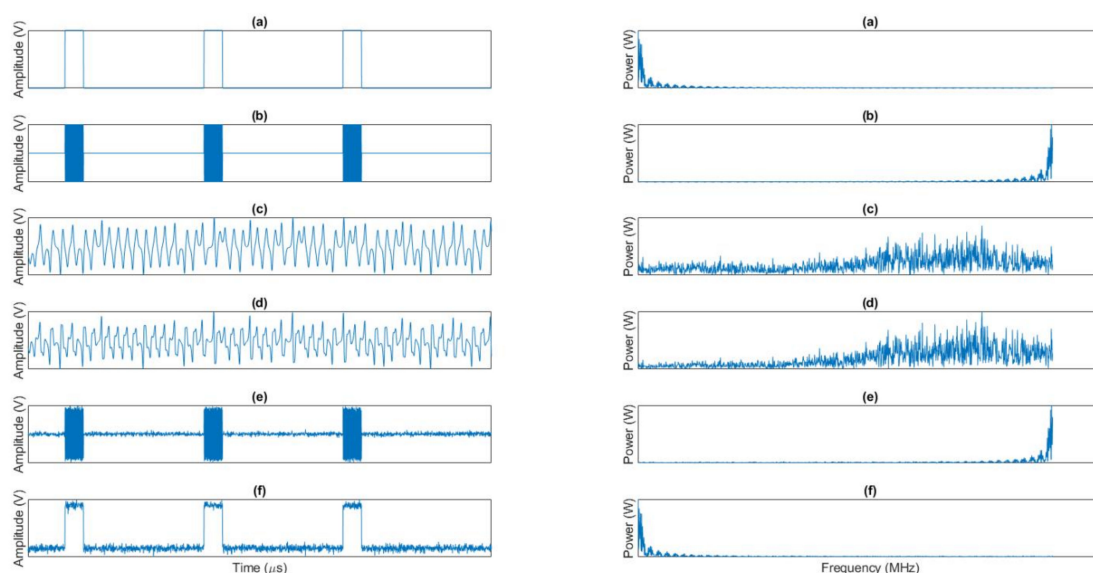


Modulation in the modeled C-RAN architecture was OOK (On-Off Keying) modulation. The frequency of information to be transmitted was 150 MHz, to meet the requirements and characteristic of future 5G networks are envisioned nowadays.

Using this simulation scenario and software, two experiments were designed. The first one evaluates how strong is the proposed cryptographic scheme using two techniques: a heuristic technique comparing the original and the encrypted signal in the temporal and the frequency domains; and an evaluation of the mutual information indicator between the raw information signal and the encrypted signal. This second technique was based on several different simulation scenarios where different chaotic signals were induced varying the ring length and the coupling parameters. Each chaotic signal was represented by its maximum Lyapunov exponent. Final results were calculated with the average of twelve different simulations for each situation, and the average for all considered access points and bases stations. Besides, each simulation represented an operation time of seventy-two (72) hours. To enable the calculation of the mutual information, original and encrypted signals were quantified using symbol composed of twenty (20) bits. Then, 2048 different values could be defined.

The second experiment was focused on the performance of the proposed solution from the telecommunication engineering point of view. Two basic and relevant indicators were evaluated: the Bit Error Rate (BER) and the relative error (or error dispersion) between the original and the decrypted signals at physical level. The experiment is repeated for different types of chaos and when differences in the coupler are observed. As in the first experiment, final results were calculated with the average of twelve different simulations for each situation (and the average for all considered access points and bases stations), and each simulation represented 72 h of operation.

Figure 7 shows a comparison between most relevant signals in the proposed information protection scheme in both domains: temporal and frequency. For clarity, only a short time and most relevant frequencies are showed. Besides, all amplitude, time and frequency scales have been normalized, as (in this case) we are only focusing on waveforms.



**Figure 7.** Comparison among the most relevant signals in the time (left) and frequency (right) domain.

As can be seen, original information (a) is recovered in a high-quality manner (f), as only some additive noise (probably some residual chaotic signal) is affecting the received information. Despite this fact, in the optical link, the chaotic signal (c) masks and hides the modulated information signal (b), so the encrypted signal (d) is totally erratic and no pattern may be easily detected. In the frequency spectrum the phenomenon is similar, as chaotic signals presents large and sparse spectrum being able to hide even signals in 5G broadband communications.

However, in order to analyze if sophisticated techniques could find any residual private information in the chaotic masked signal, we are obtaining the mutual information between the modulated signal and the chaotic signal for different types of chaos. Figure 8 shows the obtained results. Mutual information has been normalized in order to make independent the results from the symbol scheme selected to quantify signals. To complement this result, the entropy (according to Shannon's definition) of the chaotic signal is also obtained.

As can be seen, the normalized mutual information gets closer to the unit as the Lyapunov exponent goes up and the complexity of generated chaos grows up. That means that, as chaos gets more complex, the encrypted signal does not contain any amount of private information and, then, no technique (although very exhaustive) can break the proposed encryption. This evolution is caused by the higher entropy of chaotic signals as maximum Lyapunov exponent goes up. Figure 8 also shows how entropy tends to 0.5 bits (maximum entropy and randomness) as Lyapunov exponents grow.

As stated in Section 3, couplers in the receptor and transmitter must be selected as similar as possible. However, it may be very complicated or impossible to obtain two identical devices. Thus, a key question to answer is how differences in those devices affect the system performance. The experiment is also repeated for different types of chaos. Figures 9 and 10 show the obtained results about this experiment.

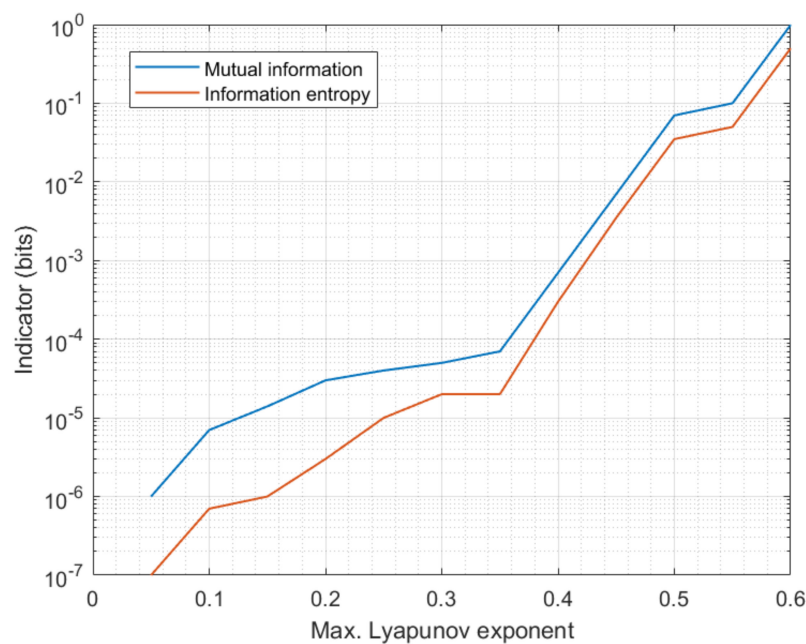


Figure 8. Mutual information between the encrypted and clear signals.

The obtained results show that BER up to  $10^{-5}$  may be achieved for medium complexity chaos when couplers are exactly the same device, although error bursts may appear (with a duration of some milliseconds). These bursts, any case, do not affect the long-term performance. The relative error (or error dispersion) may be also low, reaching a value of  $10^{-3}$  for medium complexity chaos signals. If differences are observed between couplers in the transmitter and the receptor, the BER and error dispersion grows exponentially as differences between couplers are higher. This error rates are near 100% when coupling parameters are different in more than 10%, regardless the type of chaos being generated. Besides, it can be observed how error dispersion goes up faster than BER, as bit recognition mechanisms are prepared to tolerate even high levels of distortion. In a standard scenario with differences around 0.0001% in the coupling parameters (a quite real value), the BER is around  $10^{-4}$  and error dispersion around  $10^{-2}$ .

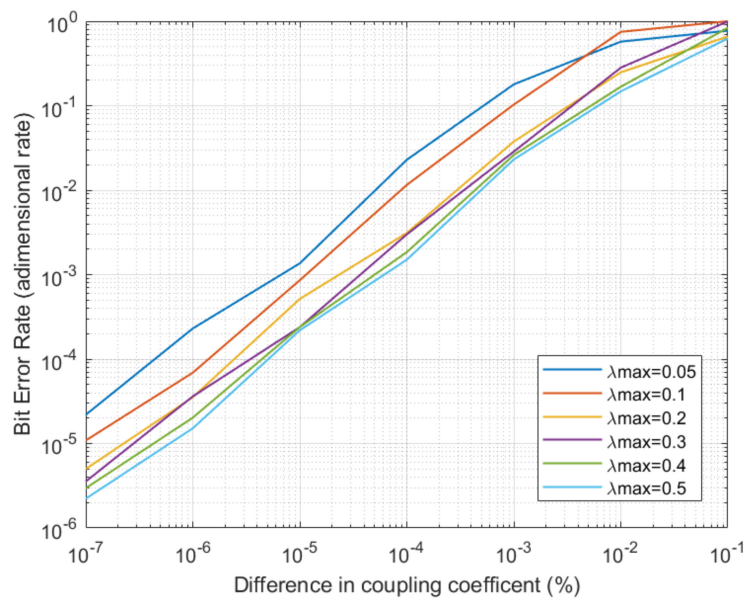


Figure 9. Evolution of BER for different system configurations.

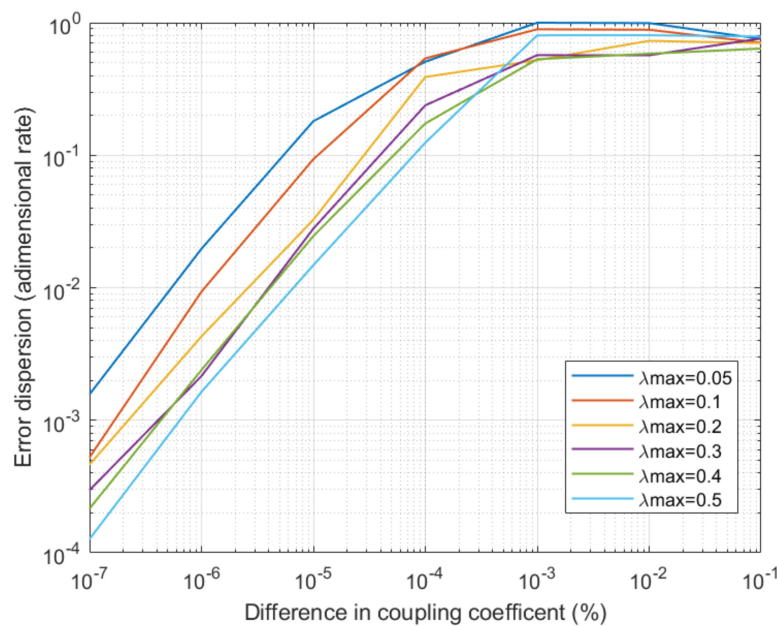


Figure 10. Evolution of error dispersion for different system configurations.

## 5. Conclusions and Future Works

In this paper, it is proposed a novel information protection scheme for C-RAN architectures based on resonant phenomena in optical fibers communicating the fronthaul and backhaul in 5G networks. Resonant structures (specifically optical rings) and physical nonlinearities generate an unclonable chaotic signal which may encrypt and hide at physical level every communication stream in a very efficient manner. The proposed model includes two novelties: a more complex representation of refraction indices in optical fibers (affected by uncontrollable nonlinearities), and the consideration of random and unknown destructive interferences in the optical ring.

The resulting system is generating a chaotic signal with a similar complexity to other existing chaotic dynamics in the state of the art for cryptographic applications.

The experimental validation shows the proposed solution totally masks the private information being protected, in terms of waveform and information. Besides, in real scenarios, a Bit Error Rate around  $10^{-4}$  may be achieved. In future works, the proposed mechanism will be deployed using real commercial components, in order to analyze its performance in realistic applications.

**Author Contributions:** Conceptualization, methodology, formal analysis, investigation, writing—original draft preparation, B.B.S.; formal analysis, resources, data curation, visualization, R.A.; software, supervision, project administration, funding acquisition, T.R.; investigation, visualization, writing—review and editing, A.J. All authors have read and agreed to the published version of the manuscript.

**Funding:** This research was funded by Fundación Universidad Alfonso X el Sabio through the “Ayudas para publicaciones UAX-Santander 2019” program. The publication was produced as a result of the research stays of Ramón Alcarria (José Castillejo’s 2017 grant) and Borja Bordel (grant number FPU15/03977) and collaboration of Antonio Jara in MOSI-AGIL-CM programme (grant P2013/ICE-3019) led by Tomas Robles.

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

## References

1. Panwar, N.; Sharma, S.; Singh, A.K. A survey on 5G: The next generation of mobile communication. *Phys. Commun.* **2016**, *18*, 64–84. [[CrossRef](#)]
2. Sánchez, B.B.; Sanchez-Picot, A.; De Rivera, D.S. Using 5G Technologies in the Internet of Things Handovers, Problems and Challenges. In Proceedings of the 2015 9th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing, Blumenau, Brazil, 8–10 July 2015; pp. 364–369.
3. Bordel, B.; Alcarria, R.; Robles, T.; Sánchez-De-Rivera, D. Service management in virtualization-based architectures for 5G systems with network slicing. *Integr. Comput. Eng.* **2019**, *27*, 77–99. [[CrossRef](#)]
4. Gamage, H.; Rajatheva, N.; Latva-Aho, M. Channel coding for enhanced mobile broadband communication in 5G Systems. In Proceedings of the 2017 European Conference on Networks and Communications (EuCNC), Oulu, Finland, 12–15 June 2017; pp. 1–6.
5. Pocovi, G.; Shariatmadari, H.; Berardinelli, G.; Pedersen, K.; Steiner, J.; Li, Z. Achieving Ultra-Reliable Low-Latency Communications: Challenges and Envisioned System Enhancements. *IEEE Netw.* **2018**, *32*, 8–15. [[CrossRef](#)]
6. Bockelmann, C.; Pratas, N.K.; Nikopour, H.; Au, K.; Svensson, T.; Stefanovic, C.; Popovski, P.; Dekorsy, A. Massive machine-type communications in 5g: Physical and MAC-layer solutions. *IEEE Commun. Mag.* **2016**, *54*, 59–65. [[CrossRef](#)]
7. Kowalski, J.M.; Nogami, T.; Yin, Z.; Sheng, J.; Ying, K. Coexistence of enhanced mobile broadband communications and ultra reliable low latency communications in mobile front-haul. In Proceedings of the Broadband Access Communication Technologies XII, Washington, DC, USA, 23 May 2018; Volume 10559, p. 105590C. [[CrossRef](#)]
8. Ge, X.; Cheng, H.; Guizani, M.; Han, T. 5G wireless backhaul networks: Challenges and research advances. *IEEE Netw.* **2014**, *28*, 6–11. [[CrossRef](#)]
9. Ranaweera, C.; Wong, E.; Nirmalathas, A.; Jayasundara, C.; Lim, C. 5G C-RAN With Optical Fronthaul: An Analysis From a Deployment Perspective. *J. Lightwave Technol.* **2018**, *36*, 2059–2068. [[CrossRef](#)]
10. Wu, J.; Zhang, Z.; Hong, Y.; Wen, Y. Cloud radio access network (C-RAN): A primer. *IEEE Netw.* **2015**, *29*, 35–41. [[CrossRef](#)]
11. Mareca, P.; Bordel, B. An intra-slice chaotic-based security solution for privacy preservation in future 5G systems. In *World Conference on Information Systems and Technologies*; Springer: Cham, Switzerland, 2018; pp. 144–154.
12. Bordel, B.; Orue, A.B.; Alcarria, R.; Sánchez-De-Rivera, D. An Intra-Slice Security Solution for Emerging 5G Networks Based on Pseudo-Random Number Generators. *IEEE Access* **2018**, *6*, 16149–16164. [[CrossRef](#)]
13. Bordel, B.; Alcarria, R.; Robles, T.; Sánchez, B.B. Stochastic and Information Theory Techniques to Reduce Large Datasets and Detect Cyberattacks in Ambient Intelligence Environments. *IEEE Access* **2018**, *6*, 34896–34910. [[CrossRef](#)]
14. Kardaras, G.; Lanzani, C. Advanced multimode radio for wireless & mobile broadband communication. In Proceedings of the 2009 European Wireless Technology Conference, Rome, Italy, 28–29 September 2009; pp. 132–135.

15. Quek, T.Q.; Peng, M.; Simeone, O.; Yu, W. *Cloud Radio Access Networks: Principles, Technologies, and Applications*; Cambridge University Press: Cambridge, UK, 2017.
16. Lin, Y.; Shao, L.; Zhu, Z.; Wang, Q.; Sabhikhi, R.K. Wireless network cloud: Architecture and system requirements. *IBM J. Res. Dev.* **2010**, *54*, 4:1–4:12. [[CrossRef](#)]
17. Checko, A.; Christiansen, H.L.; Yan, Y.; Scolari, L.; Kardaras, G.; Berger, M.S.; Dittmann, L. Cloud RAN for Mobile Networks—A Technology Overview. *IEEE Commun. Surv. Tutor.* **2014**, *17*, 405–426. [[CrossRef](#)]
18. Bordel, B.; De Rivera, D.S.; Alcarria, R. Virtualization-based techniques for the design, management and implementation of future 5G systems with network slicing. In *World Conference on Information Systems and Technologies*; Springer: Cham, Switzerland, 2018; pp. 133–143.
19. Venkatarman, H.; Trestian, R. *5G Radio Access Networks: Centralized RAN, Cloud-RAN and Virtualization of Small Cells*; CRC Press: Boca Raton, FL, USA, 2007.
20. Simeone, O.; Gambini, J.; Bar-Ness, Y.; Spagnolini, U. Cooperation and cognitive radio. In Proceedings of the 2007 IEEE International Conference on Communications, Glasgow, UK, 24–28 June 2007; pp. 6511–6515.
21. Lien, S.-Y.; Hung, S.-C.; Hsu, H.; Chen, K.-C. Collaborative radio access of heterogeneous cloud radio access networks and edge computing networks. In Proceedings of the 2016 IEEE International Conference on Communications Workshops (ICC), Kuala Lumpur, Malaysia, 23–27 May 2016; pp. 193–199.
22. Marsch, P.; Da Silva, I.; Bulakci, O.; Tesanovic, M.; El Ayoubi, S.E.; Rosowski, T.; Kaloxylou, A.; Boldi, M. 5G Radio Access Network Architecture: Design Guidelines and Key Considerations. *IEEE Commun. Mag.* **2016**, *54*, 24–32. [[CrossRef](#)]
23. Agrawal, R.; Bedekar, A.; Kolding, T.; Ram, V. Cloud RAN challenges and solutions. *Ann. Telecommun.* **2017**, *72*, 387–400. [[CrossRef](#)]
24. Holma, H.; Toskala, A. *LTE Advanced: 3GPP Solution for IMT-Advanced*; John Wiley & Sons: Hoboken, NJ, USA, 2012.
25. Liu, C.; Sundaresan, K.; Jiang, M.; Rangarajan, S.; Chang, G.-K. The case for re-configurable backhaul in cloud-RAN based small cell networks. In Proceedings of the 2013 Proceedings IEEE INFOCOM, Turin, Italy, 14–19 April 2013; pp. 1124–1132.
26. Werthmann, T.; Grob-Lipski, H.; Proebster, M. Multiplexing gains achieved in pools of baseband computation units in 4G cellular networks. In Proceedings of the 2013 IEEE 24th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC), London, UK, 8–11 September 2013; pp. 3328–3333.
27. Checko, A.; Holm, H.; Christiansen, H. Optimizing small cell deployment by the use of C-RANs. In Proceedings of the European Wireless 2014; 20th European Wireless Conference, Barcelona, Spain, 14–16 May 2014; pp. 1–6.
28. Jinling, H. TD-SCDMA/TD-LTE evolution Go Green. In Proceedings of the 2010 IEEE International Conference on Communication Systems, Singapore, 17–19 November 2010; pp. 301–305.
29. Bansal, M.; Mehlman, J.; Katti, S.; Levis, P. Openradio: A programmable wireless dataplane. In *Proceedings of the First Workshop on Hot Topics in Software Defined Networks*; ACM: New York, NY, USA, 2012; pp. 109–114.
30. Yang, K. Interference management in LTE wireless networks [Industry Perspectives]. *IEEE Wirel. Commun.* **2012**, *19*, 8–9. [[CrossRef](#)]
31. Beyene, Y.D.; Jantti, R.; Tirkkonen, O.; Ruttik, K.; Iraj, S.; Larmo, A.; Tirronen, T.; Torsner, A.J. NB-IoT Technology Overview and Experience from Cloud-RAN Implementation. *IEEE Wirel. Commun.* **2017**, *24*, 26–32. [[CrossRef](#)]
32. Darsena, D.; Gelli, G.; Verde, F. Cloud-Aided Cognitive Ambient Backscatter Wireless Sensor Networks. *IEEE Access* **2019**, *7*, 57399–57414. [[CrossRef](#)]
33. Arfaoui, G.; Bisson, P.; Blom, R.; Borgaonkar, R.; Englund, H.; Felix, E.; Klaedtke, F.; Nakarmi, P.K.; Naslund, M.; O’Hanlon, P.; et al. A Security Architecture for 5G Networks. *IEEE Access* **2018**, *6*, 22466–22479. [[CrossRef](#)]
34. Ahmad, I.; Kumar, T.; Liyanage, M.; Okwuibe, J.; Ylianttila, M.; Gurtov, A. Overview of 5G Security Challenges and Solutions. *IEEE Commun. Stand. Mag.* **2018**, *2*, 36–43. [[CrossRef](#)]
35. Ahmad, I.; Kumar, T.; Liyanage, M.; Okwuibe, J.; Ylianttila, M.; Gurtov, A. 5G security: Analysis of threats and solutions. In Proceedings of the 2017 IEEE Conference on Standards for Communications and Networking (CSCN), Helsinki, Finland, 18–20 September 2017; pp. 193–199.



36. Namal, S.; Ahmad, I.; Gurtov, A.; Ylianttila, M.; Ahmad, I. SDN Based Inter-Technology Load Balancing Leveraged by Flow Admission Control. In Proceedings of the 2013 IEEE SDN for Future Networks and Services (SDN4FNS), Trento, Italy, 11–13 November 2013; pp. 1–5.
37. Khan, A.N.; Kiah, M.M.; Khan, S.U.; Madani, S.A. Towards secure mobile cloud computing: A survey. *Future Gener. Comput. Syst.* **2013**, *29*, 1278–1299. [[CrossRef](#)]
38. Chonka, A.; Abawajy, J. Detecting and Mitigating HX-DoS Attacks against Cloud Web Services. In Proceedings of the 2012 15th International Conference on Network-Based Information Systems, Melbourne, VIC, Australia, 26–28 September 2012; pp. 429–434.
39. Namal, S.; Ahmad, I.; Gurtov, A.; Ylianttila, M.; Ahmad, I. Enabling Secure Mobility with OpenFlow. In Proceedings of the 2013 IEEE SDN for Future Networks and Services (SDN4FNS), Trento, Italy, 11–13 November 2013; pp. 1–5.
40. Zhang, X.; Kunz, A.; Schroder, S. Overview of 5G security in 3GPP. In Proceedings of the 2017 IEEE Conference on Standards for Communications and Networking (CSCN), Helsinki, Finland, 18–20 September 2017; pp. 181–186.
41. Pan, F.; Wen, H.; Song, H.; Jie, T.; Wang, L. 5G security architecture and light weight security authentication. In Proceedings of the 2015 IEEE/CIC International Conference on Communications in China—Workshops (CIC/ICCC), Shenzhen, China, 2–4 November 2015; pp. 94–98.
42. Fang, D.; Qian, Y.; Hu, R.Q. Security for 5G Mobile Wireless Networks. *IEEE Access* **2018**, *6*, 4850–4874. [[CrossRef](#)]
43. Ahmad, I.; Liyanage, M.; Shahabuddin, S.; Ylianttila, M.; Gurtov, A. Design Principles for 5G Security. In *A Comprehensive Guide to 5G Security*; Wiley: Hoboken, NJ, USA, 2018; pp. 75–98.
44. Gao, Y.; Hu, S.; Tang, W.; Li, Y.; Sun, Y.; Huang, D.; Cheng, S.; Li, X. Physical Layer Security in 5G Based Large Scale Social Networks: Opportunities and Challenges. *IEEE Access* **2018**, *6*, 26350–26357. [[CrossRef](#)]
45. Wang, N.; Wang, P.; Alipour-Fanid, A.; Jiao, L.; Zeng, K. Physical-Layer Security of 5G Wireless Networks for IoT: Challenges and Opportunities. *IEEE Internet Things J.* **2019**, *6*, 8169–8181. [[CrossRef](#)]
46. Wu, Y.; Khisti, A.; Xiao, C.; Caire, G.; Wong, K.-K.; Gao, X. A Survey of Physical Layer Security Techniques for 5G Wireless Networks and Challenges Ahead. *IEEE J. Sel. Areas Commun.* **2018**, *36*, 679–695. [[CrossRef](#)]
47. Darsena, D.; Gelli, G.; Iudice, I.; Verde, F. Design and Performance Analysis of Channel Estimators Under Pilot Spoofing Attacks in Multiple-Antenna Systems. *IEEE Trans. Inf. Forensics Secur.* **2020**, *15*, 3255–3269. [[CrossRef](#)]
48. Tian, F.; Zhang, P.; Yan, Z. A Survey on C-RAN Security. *IEEE Access* **2017**, *5*, 13372–13386. [[CrossRef](#)]
49. Ran, C.; Guo, G. Security XACML access control model based on SOAP encapsulate. In Proceedings of the 2011 International Conference on Computer Science and Service System (CSSS), Nanjing, China, 27–29 June 2011; pp. 2543–2546.
50. Duan, X.; Wang, X. Authentication handover and privacy protection in 5G hetnets using software-defined networking. *IEEE Commun. Mag.* **2015**, *53*, 28–35. [[CrossRef](#)]
51. Yan, S.; Wang, W.-B. Physical layer security strategies for downlink heterogeneous cloud radio access networks. *J. China Univ. Posts Telecommun.* **2014**, *21*, 47–54. [[CrossRef](#)]
52. Park, S.-H.; Simeone, O.; Shitz, S.S. Fronthaul quantization as artificial noise for enhanced secret communication in C-RAN. In Proceedings of the 2017 IEEE 18th International Workshop on Signal Processing Advances in Wireless Communications (SPAWC), Sapporo, Japan, 3–6 July 2017; pp. 1–5. [[CrossRef](#)]
53. Xiao, K.; Gong, L.; Kadoch, M. Opportunistic Multicast NOMA with Security Concerns in a 5G Massive MIMO System. *IEEE Commun. Mag.* **2018**, *56*, 91–95. [[CrossRef](#)]
54. Wang, L.; Wong, K.-K.; El Kashlan, M.; Nallanathan, A.; Lambotharan, S. Secrecy and Energy Efficiency in Massive MIMO Aided Heterogeneous C-RAN: A New Look at Interference. *IEEE J. Sel. Top. Signal Process.* **2016**, *10*, 1375–1389. [[CrossRef](#)]
55. Yupapin, P.; Suwanchaoen, W. Chaotic signal generation and cancellation using a micro ring resonator incorporating an optical add/drop multiplexer. *Opt. Commun.* **2007**, *280*, 343–350. [[CrossRef](#)]
56. Ikeda, K.; Daido, H.; Akimoto, O. Optical Turbulence: Chaotic Behavior of Transmitted Light from a Ring Cavity. *Phys. Rev. Lett.* **1980**, *45*, 709–712. [[CrossRef](#)]
57. Pérez-Jiménez, M.; Sánchez, B.B.; Migliorini, A.; Alcarria, R. Protecting Private Communications in Cyber-Physical Systems through Physical Unclonable Functions. *Electronics* **2019**, *8*, 390. [[CrossRef](#)]



58. VanWiggeren, G.D.; Roy, R. Optical Communication with Chaotic Waveforms. *Phys. Rev. Lett.* **1998**, *81*, 3547–3550. [[CrossRef](#)]
59. Sciamanna, M.; Shore, K.A. Physics and applications of laser diode chaos. *Nat. Photonics* **2015**, *9*, 151–162. [[CrossRef](#)]
60. Virte, M.; Panajotov, K.; Thienpont, H.; Sciamanna, M. Deterministic polarization chaos from a laser diode. *Nat. Photonics* **2012**, *7*, 60–65. [[CrossRef](#)]
61. Willner, A. *Optical Fiber Telecommunications*; Academic Press: London, UK, 2019; Volume 11.
62. Moussu, R.; Pelletier, F. Sur le théorème de Poincaré-Bendixson. *Ann. l'Institut Fourier* **1974**, *24*, 131–148. [[CrossRef](#)]
63. Mareca, M.P.; Bordel, B.; Lopez, M.P.M.; Pilar, A. Improving the Complexity of the Lorenz Dynamics. *Complexity* **2017**, 2017. [[CrossRef](#)]
64. Bordel, B.; Alcarria, R. Physical Unclonable Functions based on silicon micro-ring resonators for secure signature delegation in Wireless Sensor Networks. *J. Internet Serv. Inf. Secur.* **2018**, *8*, 40–53.



© 2020 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<http://creativecommons.org/licenses/by/4.0/>).