Book Chapter Template

Device fingerprint as a transmission Security paradigm

Pantea, Nadimi Goki, CNIT Photonic Networks and Technologies PNT Lab, Pisa, Italy - TeCIP Institute Scuola Superiore Sant'Anna, Pisa, Italy pantea.nadimigoki@santannapisa.it

Thomas, Teferi Mulugeta, TeCIP Institute Scuola Superiore Sant'Anna, Pisa, Italy

Nicola, Sambo, TeCIP Institute Scuola Superiore Sant'Anna, Pisa, Italy

Roberto, Caldelli, Florence Research Unit CNIT, Florence, Italy - Universitas Mercatorum, Rome, Italy

Ramin, Solaimani, Universitas Mercatorum, Rome, Italy

Luca, Potì, CNIT Photonic Networks and Technologies PNT Lab, Pisa, Italy - Universitas Mercatorum, Rome, Italy

Abstract

Optoelectronics plays a crucial role in the field of telecommunications and networks. Specifically, optoelectronic constructions serve as sources, detectors, and light controllers in communication and optical network systems. One of the requirements of a secure system is evaluating the optical components of optoelectronic assemblies and ensuring their security against malicious attacks. To address this, we introduce the concept of optical fingerprints in optical communications and networks. This concept includes reading the fingerprints of devices, sub-systems, and systems to address services that comprise security, authentication, identification, and monitoring. Using optical fingerprints as a signature of optical fibers, it becomes possible to identify and evaluate any optical component of optoelectronic assemblies through their pigtail.

Keywords: Security, Authentication, Identification, Monitoring, Optical fingerprints, Optical physical unclonable functions, Digital Signature, Optical network, Communication systems

1. Introduction

The rapid development of optical telecommunication technologies has necessitated the evolution of telecommunication security techniques and protocols. The increasing adoption of fiber optic communication systems, which constitute the foundation of global telecommunications infrastructure [1], poses challenges to ensuring the accessibility and confidentiality of networks and data in the presence of adversarial attacks. Adversarial potency is constantly increasing through the utilization of high-performance devices and the exploitation of intensive machine learning algorithms to enhance attack effectiveness.

Security and confidentiality within the open systems interconnection (OSI) (framework, which describes the functions of networking or telecommunications systems), are primarily governed by the upper layers. The OSI security architecture, recommended by ITU-T, establishes a standard for data security by identifying the attacks, security services, and security mechanisms. In this model, security protocols are applied from the top layer down. The application layer, which is the layer most users interact with, may include end-to-end cryptography (e.g., WhatsApp messages are encrypted to be recognized just by users). Additionally, the presentation and session layers, which are responsible for syntax processing and creating communication channels between devices, respectively, may benefit from data cryptography. The transport layer, responsible for transmitting the data across network connections, can utilize protocols such as Secure Sockets Layer (SSL) or Transport Layer Security (TLS). These protocols provide authentication between parties, data integrity, and digital signature. The network layer, which handles the routing of the data, is responsible for security at the network level using functions such as packet authentication, cryptography, and integrity (e.g., Internet Protocol Security – IPsec). In contrast, admission control performs a check at the link layer to guarantee the proposed connection. Wireless systems developed Wi-Fi Protected Access (WPA) protocols to add protection mainly to wireless computer networks. Regarding the physical layer (PHY), security implementation is typically lacking as the establishment of optimal security protocols at this level remains a worldwide problem.

Despite security and confidentiality primarily being addressed at the upper layers, the implementation of physical layer security offers an extra level of protection that is currently lacking in communication networks and remains a significant global technical challenge. With that objective in mind, we introduce Optical Identification (OI), a novel method that aims to implement a novel (ID) technique for enhancing physical layer security (PLS).

Despite the numerous studies, suggestions, and experimental works reported on physical layer security (PLS) [2,3], there remains a significant need to establish a practical and effective protocol or technique for physical layer security. In [4,5], PLS has been defined through keys generated by digital signal processing (DSP). The disadvantage of such a method is its vulnerability to digital attacks, similar to other cryptography-based PLS [6]. The PLS enhancement through the monitoring of optical communication with quantum-level sensitivity using a quantum pilot tone, as proposed in [7], or more commonly through the Quantum key distribution (QKD) [8-9] provides intrinsic security. However, these approaches are not cost-effective and often challenging to implement. Recently, an approach for boosting PLS was introduced with a subcarrier identification process in the receiver DSP [10], which is vulnerable if attackers have knowledge of the transceiver DSP configurations. The investigation of PLS-based optical chaos communication has explored various structures [11,12,13]. However, the impracticality of this approach arises from the high-level synchronization requirement between the transmitter and the receiver [14]. Additionally, the security of chaotic communication can be compromised by the problems created by the feedback loop of the chaotic system [15]. A viable approach has been proposed lately, in [16] and [17], involving the use of optical steganography to hide messages below the noise level, thereby ensuring secure communication. Although this technique is practical, it cannot detect the existence of an eavesdropper. This technique has vulnerability to adversaries who know the system and are able to acquire and analyze the whole spectrum [18,19]. In recent investigations of security techniques, physical unclonable function (PUF), as a new approach for PLS, attracted considerable attention.

The PUF approach is based on the material's physical features, in which a physical device provides unique output for a given input thanks to its unclonable and

unpredictable response. These types of devices are usually implemented in complementary metal-oxide-semiconductor (CMOS) [20,21]. PUF overcomes the disadvantages of computational cryptography, steganography, and other techniques, and its security level is subject to the difficulty of cloning the function response [22,23]. So, a specific input function called challenge (*Challenge*) ends with the individual output function called response (*Response*). New challenges will not end with the same response, and every single challenge has its unique response. The significant fact about PUFs is that any PUF material has its own unique function, which means applying the same challenge to two different PUF materials results in two different responses. This feature makes PUFs a strong security technique, and a viable alternative to today's techniques based on cryptography. It is worth mentioning that the term PUF includes several technical and technological categories. Among them, electrical PUF has been considered in [24] as a PLS technique, however, this technique is not practical because both the transmitter and receiver should have access to the same PUF to synchronize their channel [25]. Optical PUF (OPUF), based on the optical token, has also been investigated in several studies to generate secure cryptography keys [26] and for authentication applications [27].

In this Chapter, we introduce the concept of optical identification by reading the optical fingerprint in optical communications and networks, exploiting OPUF. Which is a practical technique to enhance network PLS based on OPUF. The fundamental principle of the proposed technique is to identify networks, optical links, systems, sub-systems, network elements, and any optical component of optoelectronic assemblies, that possess optical fiber or fiber pigtail. The proposed technique is carried out based on the following procedures: in the first step, the optical fingerprint of the device under test (DUT) is read and stored. The fingerprint is generated using the Rayleigh backscattering pattern (RBP) of the fiber (or fiber pigtail), which is considered a strong OPUF [28]. In this manner, every DUT possesses its unique fingerprint. The second step is DUT identification through the simple technique of comparison between a stored fingerprint and the DUT to be identified. We demonstrate the validation of fingerprints through several different metrics including security, uniqueness, unpredictability, unlclonability, and reproducibility. The benefit of our proposed technique is that it does not require receiver-transmitter synchronization [25] or the fabrication of OPUF [29] as the inherent feature of the fibers serves as our proposed OPUF.

The proposed method can be used for communication security, authentication, identification, and monitoring purposes, both in point-to-point communication and optical networks. It could be considered an effective security implementation to evaluate the optical components of optoelectronic assemblies and ensure their security against malicious attacks.

The following sections will provide a detailed description of the proposed technique. Section 2 presents an overview of Physical Unclonable Functions, which form the security basis of the proposed method. Section 3 introduces the concept of optical fingerprints in networks and communication systems. The performance evaluation of Optical Identification (OI) is described in Section 4. Section 5 shows possible applications and discussion. Finally, conclusions are summarized in Section 6.

2. An overview of PUF

Physical Unclonable Functions (PUFs) [30] can be considered like biometrics [31] for physical objects such as sensors, devices, integrated circuits and so on. In fact, as it happens for living beings, and for humans in particular, in which biometrics (e. g. fingerprints, DNA) can be adopted to identify and distinguish different exemplars and

subjects, PFUs can be similarly used to make a distinction among diverse physical objects involved in a specific process. The reference to the word "physical" indicates that PUFs are generated by resorting to some physical characteristics that are intrinsically present within a certain electronic device. Such features are generally embedded during the fabrication step and are usually due to some small manufacturing imperfections induced by the construction procedure itself. Such imperfections are randomly generated but remain persistent within each device and, above all, they grant distinctiveness among each different physical object; this desirable aspect can be effectively exploited for security mechanisms in various application scenarios such as IoT (Internet of Things). The other particularly interesting aspect concerns the adjective "unclonable" that means these features, and especially the measurements they determine, cannot be easily duplicated in order to induce a falsification and/or exchange an identity. In addition to this, PUFs do not need to be stored within an electronic memory as it normally happens for a digital secret, but they intrinsically belong to the physical object as a classical fingerprint. This is advantageous because, for instance, specific secure hardware solutions are not required and, furthermore, it is more difficult to perpetrate invasive attacks. This can be better understood, if we imagine using a PUF to generate a cryptographic root key for a specific device. In this case, such a key is created by the PUF and neither any key injection is required, nor it can be copied from one device to be used onto another one. The crypto key does not need to be stored anywhere but it can be recovered from the device's fingerprint whenever it is necessary during, for example, an authentication procedure.

PUF-based security systems can be generally implemented as identification mechanisms based on a well-known *challenge-response pairs (CRPs) protocol*. As evidenced in Equation 1, each time a PUF receives a "challenge" (CH) as input, it outputs a "response" that is highly difficult to be predicted and replicated.

$$PUF_A(CH_i) \neq PUF_A(CH_j), \ \forall i \neq j \tag{1}$$

A PUF-based circuit can be seen as a black-box model where the input Challenge is processed by the function F(.), whose characteristics are determined by the PUF itself; the resulting output is the Response such that Response =F(Challenge). The internal behavior of the function F(.) (namely the PUF) is strictly correlated to the peculiar inner manufacturing variabilities and cannot be manipulated.

PUFs can be categorized in different ways, anyway, a primary mode for their classification is to subdivide them in soft and strong PUFs. Such a distinction is basically related to the number of challenges, when this number is quite limited, they are generally indicated as soft ones and, on the contrary, in the case, such value is higher (e.g., a complete determination of the CRPs would not be possible within a feasible time) they are labeled as strong PUFs. Other important characteristics that permit to catalogue PUFs concern uniqueness and reliability. The term uniqueness is intended that the response provided by a PUF is different for different input challenges (see Equation 1) and, furthermore, the same input challenge should generate distinctive output responses when applied to diverse PUFs (as evidenced in Equation 2).

$$PUF_A(CH_i) \neq PUF_B(CH_i), \qquad \forall A \neq B \tag{2}$$

The distinctiveness between to diverse PUF's output are generally evaluated in terms of Hamming distance when it is a binary vector/matrix, but other kinds of

measurements can be adopted such as mean squared error (MSE) or cross-correlation (CC). Diversely, the term *reliability* regards the capacity of a PUF to provide always the same answer when a fixed challenge is passed as input (i.e. an intra-Hamming distance that should be ideally equal to zero). *Reliability* has not to be confused with *steadiness*, though they are strictly related each other; *steadiness* refers to the degree of response variability but possibly determined by some changes occurred in the operative scenario such as variations in temperature or electric supply or even due to aging effect [32].

Different kinds of PUFs exist, one of the first examples of an optical PUF is probably the system introduced in [33]. Such a system is constituted by an input laser beam directed towards a stationary scattering medium afterward the speckle output pattern is recorded. In this case, the challenge is based on the laser XY location and its polarization while the response is the associated speckle pattern. Such a pattern is strongly dependent on the input location/polarization since multiple scattering events can occur inside the scattering medium. A simple example of a soft PUF is represented by the "power-on" state of an SRAM. In fact, though an SRAM cell is symmetric, manufacturing anomalies can induce a tendency toward a logical ''0'' or ''1' when the power is switched on. This variability is random across the entire SRAM and this determines a univocal fingerprint that can provide a distinctiveness. Another interesting kind of soft PUF can be determined by the acquisition process of digital images (videos). In fact, when a photo is taken, the camera sensor, which is composed of a two-dimensional array of CCDs (Charge Coupled Devices), is hit by light photons whose energy is then converted into electron charges. Due to manufacturing imperfections in the silicon wafer, each cell of the camera's sensor differently answers to a uniform incoming light. Consequently, this determines the superimposition, onto each content it takes (images and/or videos), of a systematic noise, named PRNU (Photo Response Non-Uniformity noise [34]) Such a noise is not perceivable and does not degrade the visual quality of the acquired contents, but it effectively constitutes a sort of fingerprint that is embedded within the image pixels. Such a fingerprint can be successively extracted by means of high-pass filtering and compared with the available reference fingerprints of different cameras to perform a source identification similar to what happens for the association process between the gun and the bullet in ballistics.

Though the possible advantages are significant, PUFs are anyway prone to security issues as well as other security mechanisms and these crucial aspects have to be carefully tackled in relation to the application scenario where PUFs are adopted for security purposes. Above all, the reliability of the verification system has to be assessed in order to avoid false alarms and missing detections, furthermore, PUFs are not immune to malicious security attacks such as spoofing attacks and have to be properly designed to effectively deal with personal data management and user privacy.

3. Optical fingerprint

Clearly, physical elements possess distinctive fingerprints, much like humans do. While we have the capability to identify and potentially render them impervious to cloning, this notable feature remains underutilized in communication systems and networks. The scope of our research covers the concept of optical fingerprinting (ID); where in every photonic device, optoelectronic component, sub-system, or system is assigned an exclusive fingerprint extracted from their physical characteristics and the non-ideality of the optical object in physical process. This approach serves as an effective security technique. By assuming the ability to read these fingerprints, we

model security, authentication, identification, and monitoring in point-to-point communication and extend it to optical networks.

3.1 Concept

A point-to-point communication system can be represented by three essential sub-systems: transmitter, channel, and receiver (Figure 1). As previously mentioned in the introduction, each sub-system possesses its unique fingerprint, which may be labeled as ID_{TX}, ID_{Ch}, and ID_{RX} respectively. We make the initial assumption that each fingerprint can be acquired independently, forming a strong basis for our analysis.

Passive sub-system: In this scenario, where the channel is considered to be a passive sub-system, three potential security approaches may be envisaged:

1. The transmitter reads ID_{Ch} and ID_{RX} to ensure that the information will pass the designated channel and reaches the intended receiver;
2. The receiver reads ID_{TX} and ID_{Ch} to determine the sender's identity and the physical path of transmission;
3. The transmitter reads $ID_{RX,}$ while the receiver acquires ID_{TX} enabling both sub-systems to identify each other. Additionally, they can also verify ID_{Ch} to ensure the integrity of the communication path.

In this simple case, each signature can be a sufficiently long binary sequence that can be compared to stored signatures for the purpose of identification. A binary XOR operation would be enough for such a comparison. In a real system, a signature match will occur with a certain probability $P_{x,}$ which represents X the specific sub-system, and $0 \leq P_x \leq 1$.

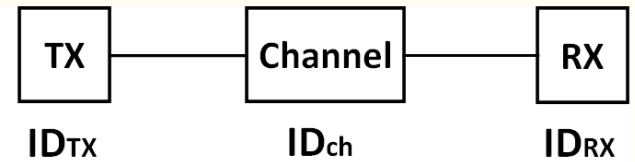

Figure 1. Point-to-point communications system. ID_{TX}, ID_{Ch} and ID_{RX} are physical signatures for the transmitter, channel, and receiver respectively.

Active sub-system: In a slightly more advanced scenario, when the channel is an active sub-system that includes devices, the method is extended to enable reading and validating the signature of the entire system and/or every single sub-system. A direct extension can be represented as illustrated in Figure 2, which depicts a network architecture comprising N subsystems each with its unique identifier ID_i where $1 \leq i \leq N$ ('i' represents the i*th* subsystem). In an optical network, sub-systems can encompass various components such as transceivers, optical fibers, optical nodes, as well as, filters, optical cross-connects, reconfigurable optical add/drop multiplexers, and more. The signature (ID) of each sub-system will be generated and stored in a database. The identification of each subsystem ID_i will be evaluated based on a certain probability (P_i), which represents the likelihood of the ID being correct. Any sub-system within the network has the capability to identify other sub-systems and, if necessary, validate each sub-system or even the entire path. In Figure 2, a specific path is highlighted in bold. ID_1 has a connection with ID_i through ID_k, ID_6, ID_{k-1}, ID_9, ID_{k-2}, ID_{10}, and ID_{k+3}. Similar to the previous scenario of point-to-point communication, in this case as well, there is a possibility that ID_1 may want to verify the path and/or receiver (IDi). ID_1 will have the capability to evaluate the probability 'Pi' for each identification, indicating the likelihood that the sub-system is the

expected one. In the case of independent interrogation of sub-systems, it will be easy to evaluate the probability of any sub-set of subsystems or even the entire path by simply multiplying independent probabilities, Thus, the probability can be calculated as follows:

$$p_{path} = \prod_{i\epsilon\{path\}} p_i \tag{3}$$

where P_{path} represents the probability of passing through all subsystems included in the path. In the real system, Pi <1 so that even $P_{path} < 1$. By utilizing the thresholding operation, it is possible to validate, the security of the path (as well as the individual sub-systems) with a specific probability. Furthermore, with the capability to independently acquire the fingerprint of each individual sub-system, the system can identify whether any changes have occurred in the path and discover the location of the changes. This approach provides a robust framework for enhancing, authentication, identification, and monitoring. In a more generic approach, it is important to note that the acquisition of signatures may exhibit correlation, rendering them no longer independent. In this case, a more intricate model based on the specific identification technique must be developed, However, we postpone this approach to future studies.

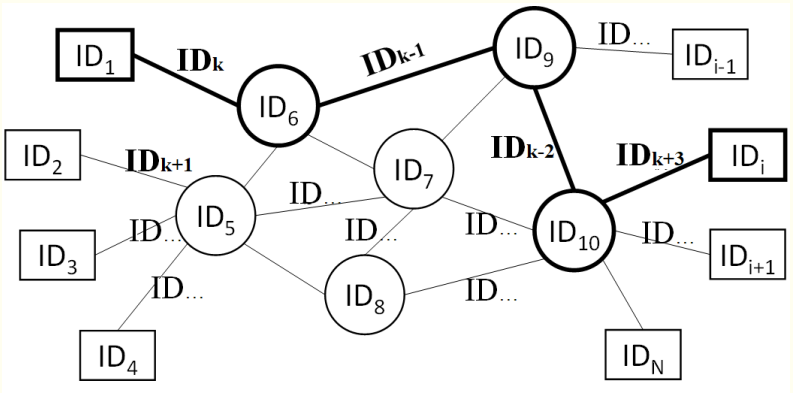

Figure 2. Network architecture example. Each sub-system has its own physical signature (ID), including transceivers, nodes, and links.

In both scenarios, in the ideal case when a perfect match is achieved (P_x=1), security is guaranteed, and five operations become possible:

1. *Layer security*: If an attack is conducted on one of the identified sub-systems, the match is disrupted, and the attack is unsuccessful.
2. *Authentication*: Authentication can be automatically provided once the sub-system is securely identified.
3. *Identification*: Once the sub-system is securely identified, authentication can be automatically granted.
4. *Monitoring*: By continuously verifying the signature, any changes in the system can be identified.
5. *QoT estimation*: The identification method based on "signature" could enhance the accuracy of estimation.

Regarding network device census [35], it is common, for the network operators to have limited knowledge of all the fiber types deployed in a network. This situation poses challenges to the quality of transmission estimation, leading to increased estimation inaccuracies. As a result, network operators may need to adopt higher

network margins than initially anticipated, with a consequent underestimation of the optical reach and an increase in the costs for regeneration [36].

We consider the Rayleigh backscattering pattern (RBP), which is a robust OPUF, due to the inherent imperfections in the fabrication process to generate the fingerprint. The RBP of an optical fiber can be measured using optical frequency domain reflectometry OFDR, and this measurement can be converted into a digital signature which becomes the unclonable and unique signature of each sub-system. In the next sections generating a signature (ID) will be explained in detail.

3.2 Signature

We propose to use the Rayleigh backscattering pattern (RBP) as a signature of the optical fiber. This approach enables us not only to identify the fiber link but also to identify any optical and optoelectronic sub-systems through their pigtail. The Rayleigh backscattering phenomenon that occurs when optical fibers are stimulated by propagating light is an optical physical unclonable function (OPUF), due to the random density fluctuations caused by the fabrication process [37]. The acquisition of RPB can be accomplished through the utilization of an optical frequency or time domain reflectometry (OFDR or OTDR) technique [38,39]. In this work, we consider the coherent OFDR (COFDR) since it allows us to increase the sensitivity and resolution [40,41]. COFDR is implemented as follows:

1. A continuous wave (CW) laser emitting light with an amplitude of E_0 is used in the experiment. The laser frequency is linearly swept over time with a sweep rate of $\boldsymbol{\gamma}$, and propagates into the fiber under test (FUT).
2. The RBP refers to the photocurrent obtained after self-coherent balance detection. It can be mathematically modeled as follows:

$$I(t) = E_0^2 \sum_{i=1}^{n} \sqrt{R_i}\, cos(2\pi\gamma t\tau_i) \tag{4}$$

when there are n reflection points with reflectivity $\boldsymbol{R_i}$ and roundtrip time $\boldsymbol{\tau_i}$ [37,41].

It should be noted that in this work the random phase noise is disregarded, and all signatures are simulated based on a fiber pigtail length of 0.5m. The RBP is measured using the COFDR technique with a sweep time of 0.5s. For long-distance measurements, where the distance exceeds half of the laser coherence length, it is crucial to appropriately compensate for phase nois and frequency sweeping nonlinearity. This compensation method is described in detail in reference [41].

The RBP-based signatures rely on the OPUF challenge-response protocol. Thus, any stimulus (called challenge) maps a unique result (called response) and provides a challenge-response pair (CRP). The following CRP protocol procedure is to generate the signature:

Challenge (C): The frequency-modulated continuous wave (FMCW) parameters on the Tx side represent the challenge.

Challenge parameters: (i) sweep rate (γ=Hz/s), which indicates the rate at which the frequency changed in FMCW; (ii) sweep range (ΔF=$\lambda_{stop} - \lambda_{start}$), which indicates the distance between the start and stop wavelength in FMCW; and the value of (iii) stop and (iv) start sweep wavelengths. Every single parameter has an important role in the spatial resolution and quality of the obtained RBP. This fact is beyond the scope of this work and is clarified in [41].

Response (R): The obtained RBP represents the response.

By changing FMCW parameters i.e. changing the challenge, the RBP will change accordingly. Therefore, if we stimulate the fiber with various challenges we can extract different RBP patterns from the same fiber. It is important to note that due to the characteristics of the PUF, each challenge will result in a unique response, meaning that different challenges will not produce the same response (as illustrated in Figure 3). As a result of this characteristic, even if an adversary gains access to the fiber, they cannot generate the desired signature without using the correct challenge.

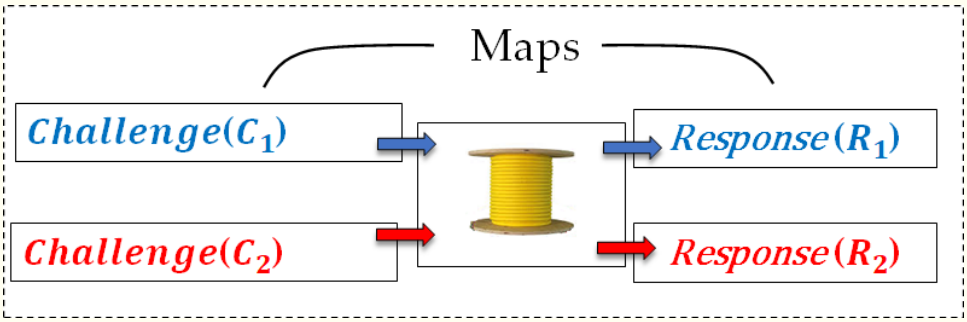

Figure 3. By changing the challenge, the response will be changed. Therefore, even if the adversary has access to the fiber, he cannot generate the intended signature without applying the correct challenge.

To generate the signature only a single challenge (e.g., C_1) will be applied, and the corresponding response (e.g., R1) will be used to create the binary signature (ID), which will then be stored in the database (Figure 4). For identification, the same challenge will be used.

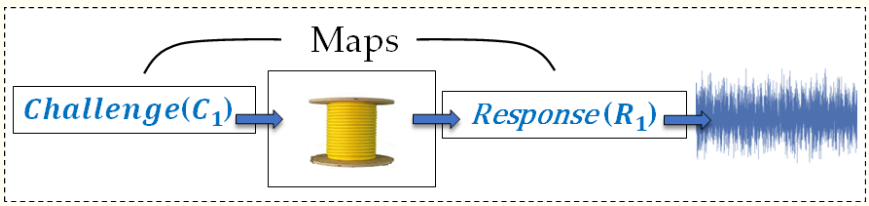

Figure 4. OPUF protocol to generate OPUF-based signature. Challenge 1 (C_1) ends with response 1 (R_1) which is a specific pattern of RBS of fiber (shown in blue) associated with the specific challenge C_1.

Using a single-bit analog-to-digital converter (ADC) the RBP is digitized with N samples. Part of the RBP will be selected to generate the binary signal [42]. Depending on the scenario and type of signature, it is straightforward to use quick response (QR) codes to represent signatures.

4. **System Identification and Performance Evaluation**

The identification process can be carried out using either Hamming distance (HD) [43] or the Pearson cross-correlation coefficient (XCOR-C) [42] between the stored signature and the intended signature. Both techniques thoroughly enable us to distinguish the noisy signature from the imposter one, as illustrated in Figure 5.

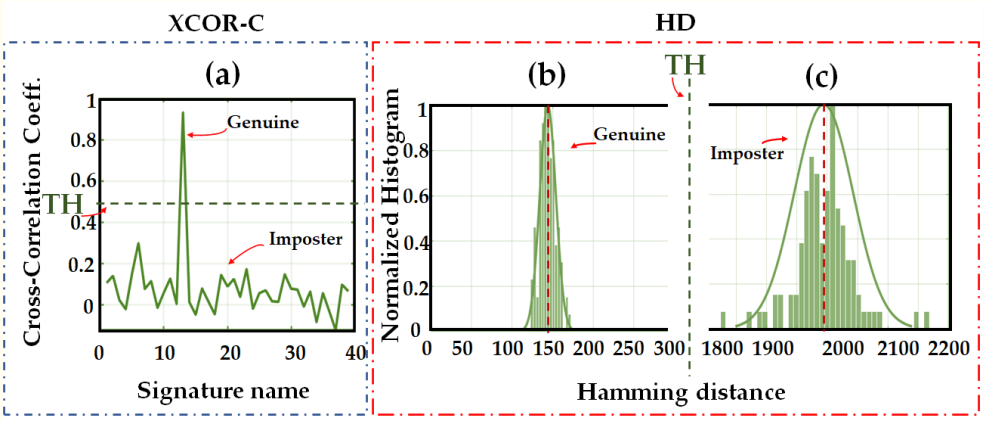

Figure 5. Two different identification methods: Cross-Correlation Coefficient (XCOR-C) between the original signature, (a) and a bunch of signatures, that among them the genuine signature is detected (peak). The histogram of Hamming distance (HD) between original signature, (b) and a bunch of noisy signatures (mean 144), (c) and a bunch of imposters (mean 1994). Defined threshold: green dashed line.

In both techniques, it is possible to define a threshold (TH) can be defined to determine whether the signature should be accepted or rejected as genuine Consequently, the decision rule will be as follow for each method:

XCOR-C: if obtained *XCOR-C,* between the intended signature and the original one, is below a certain threshold, the signature will be considered an imposter. Conversely, if the XCOR-C is above the TH, it will be deemed a genuine signature (Figure 5a).

HD: if obtained *HD,* between the intended signature and the original one, is beyond a certain threshold, the signature will be considered an imposter. On the other hand, if it is below the TH, it will be deemed genuine (Figure 5b-c).

In order to successfully implement the identification process, it is essential for the acquired signatures to be reproducible. This means that when measurements are taken at different times, they should consistently result in the same signature as the original one stored in the database. Due to the measurement noises, there may be slight deviations between the obtained signature and the original one. However, these deviations are still discernible and distinguishable from the imposter signature. This fact has been shown in Figures 5 b, c. Regarding Figure 5 b, c, the mean value of the HD histogram of the noisy signatures is about 144, while the mean value of the HD histogram of the imposter signatures is around 1994. This fact demonstrates the reproducibility as well as the level of security of signatures. The security of the generated signatures relies on the intrinsic unclonability of the OPUF [44-46]. That means the obtained signatures are unique, unclonable, and unpredictable either digitally or physically.

To describe the security validation technique, we assume to have a long binary word provided by the process of fingerprint identification. Such ID is encoded and converted to the two-dimensional (2D) binary image comprising 60 × 60 pixels, Figure 6. To assess the robustness of the IDs against digital cloning, we conducted an investigation into their resistance to brute force trials (BFT attacks). This type of attack requires nondeterministic exponential time for data decryption, which shows their robustness in front of digital cloning. We investigate the security level of the generated ID (QR code) against BFTs by considering the number of identical bits in each row of the code with the following process.

The encoded binary image was divided into 60 one-dimensional segments (rows), each including 60 bits, Figure 6. Therefore, according to equation 5, there are $C_k(n)$ pairs of 1D segments, $C_2(60) = 1770$ pairs for each binary image of 60×60 bits.

$$C_k(n) = \frac{n!}{k!(n-k)!} \tag{5}$$

As a metric for security validation, we consider the Hamming distance between the pairs of 1D segments. The Hamming distance between a pair of 1D segments refers to the number of non-identical bits that need to be flipped in order for two segments to be similar. The crucial point is that 1D segments with too short or too long Hamming distances are relatively easy to decipher through BFTs, where a Hamming distance equal to half of the segment length ensures maximum uniqueness [47].

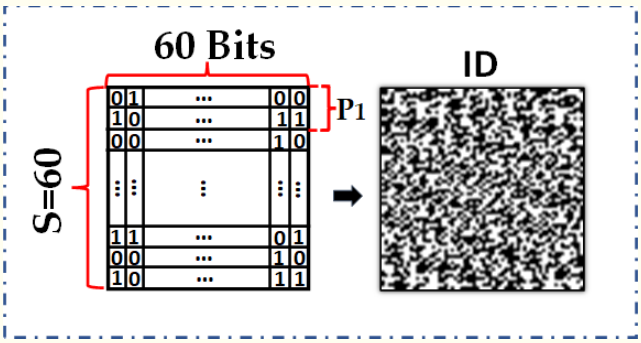

Figure 6. The system's ID. (left) 2D binary ID data consists of 60 segments (S), each including 60 bits (60x60) bits. (right) The QR code. P1: a pair of sequences.

The Hamming distance histogram of 1770 segment pairs is illustrated in Figure 7, which goes like a Gaussian distribution with a mean value of around 29, ensuring close to maximum uniqueness of the 1D segments. The histogram demonstrates the need for a large number of BFT trials to decipher a single segment of a binary image. this indicates that a significant number of BFTs would be required to decipher the entire 2D image. (i.e., ID).

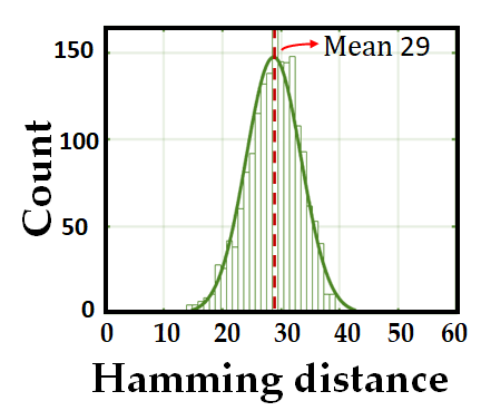

Figure 7. Validation of the ID robustness against BFT attacks. Histogram of the Hamming distance between the $C_2(60) = 1770$ pairs of 1D segments. The obtained mean value is about 29 using a Gaussian fit, which shows close to maximum uniqueness for the 1D segment, and thus for the ID (2D).

It should be noted that the signature length can be defined based on the expected level of security from the signatures [42].

5. Discussion

Based on the proposed technique, any network or its fiber-optical constituent element can be identified and authenticated. Thereby, any attack, whether physical or digital, can be detected. Physically invading the system will cause a change in the system signature that could confirm the presence of an imposter. Even digital invaders with advanced machine learning (ML) knowledge cannot predict the system's signature [48] since every system or device has its unique and unpredictable signature.

Device identification (DI) through Optical Identification (OI) through the optical signature is a perfect security complementary tool to the networks and guarantees the security of the systems, sub-systems, and devices. Such a DI identification method may find applications within several use cases. It can be used in applications related to classic network security, Quantum network security [43], network census, or network quality of transmission (QoT) [42, 49]. Depending on the scenarios, applications, and the required level of security the CRP database will be generated and used for identification implementation. Regarding network security, OI can be implemented for different network scenarios [50] to identify, authenticate, and monitor networks.

6. Conclusion

This chapter introduces the concept of Optical Identification (OI) for network security purposes at the physical layer in optical communication systems and networks. The unique fingerprint of each physical subsystem enables direct identification, offering new strategies for transmission security, layer security, authentication, identification, and monitoring. This approach allows for the identification of each network's component just using its pigtail (or the fiber itself for a link), without the need for an additional device operating directly at the physical layer. Such a novel security layer concept will play a key role when linked to other security strategies that come from upper OSI layers.

This approach might open an innovative way to impact network security at several layers. The reproducibility and uniqueness of the IDs' have been demonstrated using Hamming distances, ensuring reliable identification. The security validation of the proposed model has been investigated, demonstrating its robustness against various attack types, both physical and digital. The proposed model encompasses various methods and strategies for generating and exerting identification databases.

Future works will be dedicated to extending the technique applications and to further investigating the signature robustness against malicious attacks. These ongoing efforts aim to enhance the security performance of the proposed model and pave the way for new advancements in the field of network security.

Acknowledgments

This research was funded by HORIZON-JU-RIA (101096909), HORIZON-RIA (101092766), it was also partially supported by project SERICS (PE00000014) under the NRRP MUR program funded by the EU - NGEU.

Conflict of Interest

The authors declare no conflict of interest.

References

1. Andy H. Fiber optic cable market-growth, trends, Covid19 impact, and forecast (2021-2026). Mordor Intelligence; 2021. Report ID: 4773602.

2. Wyner AD. The Wire-Tap Channel. Bell System Technical Journal. 1975 Oct;54(8):1355–87.

3. Zhou X, McKay MR. Secure Transmission With Artificial Noise Over Fading Channels: Achievable Rate and Optimal Power Allocation. IEEE Trans Veh Technol. 2010 Oct;59(8):3831–42.

4. He J, Giddings R, Jin W, Tang J. DSP-Based Physical Layer Security for Coherent Optical Communication Systems. IEEE Photonics Journal. 2022 Oct;14(5):1–11.

5. Lei C, Lin R, Li Y, Wang B, Zhang M, Zhao Y, et al. Integration of Self-Adaptive Physical-Layer Key Distribution and Encryption in Optical Coherent Communication. J Lightwave Technol. 2023;1–8.

6. Gidney C, Ekerå M. How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits. Quantum. 2021 Apr 15;5:433.

7. Gong Y, Wonfor A, Hunt JH, Penty R. Physical layer security monitoring of optical communication using a quantum pilot tone signal. In: Conference on Lasers and Electro-Optics (2022), paper FTu4A4 [Internet]. Optica Publishing Group; 2022 [cited 2023 Jun 7]. p. FTu4A.4. Available from: https://opg.optica.org/abstract.cfm?uri=CLEO_QELS-2022-FTu4A.4

8. Bennett C, Brassard G. Quantum Cryptography: Public Key Distribution and Coin Tossing, Proc. of IEEE Int. Conf. on Comput. Sys. and Sign. Proces. 1984;

9. Cavaliere F, Prati E, Poti L, Muhammad I, Catuogno T. Secure Quantum Communication Technologies and Systems: From Labs to Markets. Quantum Reports. 2020 Mar;2(1):80–106.

10. Chen L, Jin W, He J, Giddings RP, Huang Y, Tang J. A Point-to-multipoint Flexible Transceiver for Inherently Hub-and-Spoke IMDD Optical Access Networks. J Lightwave Technol. 2023;1–12.

11. Wang L, Mao X, Wang A, Wang Y, Gao Z, Li S, et al. Scheme of coherent optical chaos communication. Optics Letters. 2020;45(17):4762–5.

12. Antonik P, Gulina M, Pauwels J, Rontani D, Haelterman M, Massar S. Spying on chaos-based cryptosystems with reservoir computing. In IEEE; 2018. p. 1–7.

13. Liang X, Zhang C, Luo Y, Wang X, Qiu K. Secure Encryption and Key Management for OFDM-PON Based on Chaotic Hilbert Motion. J Lightwave Technol. 2023 Mar 15;41(6):1619–25.

14. Chen W, Mu P. Research on methods of enhancing physical layer security of optical fiber communication system in the smart grid. In IOP Publishing; 2022. p. 012002.

15. Jiang N, Zhao A, Liu S, Zhang Y, Peng J, Qiu K. Injection-locking chaos synchronization and communication in closed-loop semiconductor lasers subject to phase-conjugate feedback. Opt Express, OE. 2020 Mar 30;28(7):9477–86.

16. Wohlgemuth E, Yoffe Y, Attia I, Imran M, Lakshmijayasimha PD, Marotta A, et al. A Field Trial of Multi-Homodyne Coherent Detection Over Multi-Core Fiber for Encryption and Steganography. J Lightwave Technol, JLT. 2023 May 1;41(9):2723–35.

17. Wu B, Wang Z, Tian Y, Fok MP, Shastri BJ, Kanoff DR, et al. Optical steganography based on amplified spontaneous emission noise. Opt Express, OE. 2013 Jan 28;21(2):2065–71.

18. Rout H, Mishra BK. Pros and Cons of Cryptography, Steganography and Perturbation techniques. IOSR Journal of Electronics and Communication Engineering.

19. Mishra R, Bhanodiya P. A review on steganography and cryptography. In IEEE; 2015. p. 119–22.

20. Y. Kamal K, Muresan R, Al-Dweik A. CMOS-Based Physically Unclonable Functions: A Review and Tutorial [Internet]. 2021 Jun [cited 2023 Jun 7]. Available from: https://www.techrxiv.org/articles/preprint/CMOS-Based_Physically_Unclonable_Functions_A_Review_and_Tutorial/14753109/1

21. Tarik FB, Famili A, Lao Y, Ryckman JD. Scalable and CMOS compatible silicon photonic physical unclonable functions for supply chain assurance. Sci Rep. 2022 Sep 19;12(1):15653.

22. Zhang L, Fong X, Chang CH, Kong ZH, Roy K. Highly reliable memory-based Physical Unclonable Function using Spin-Transfer Torque MRAM. In: 2014 IEEE International Symposium on Circuits and Systems (ISCAS). 2014. p. 2169–72.

23. Mesaritakis C, Akriotou M, Kapsalis A, Grivas E, Chaintoutis C, Nikas T, et al. Physical Unclonable Function based on a Multi-Mode Optical Waveguide. Sci Rep. 2018 Jun 25;8(1):9653.

24. Shakiba-Herfeh M, Chorti A, Vincent Poor H. Physical layer security: Authentication, integrity, and confidentiality. Physical Layer Security. 2021;129–50.

25. Rothe S, Koukourakis N, Radner H, Lonnstrom A, Jorswieck E, Czarske JW. Physical Layer Security in Multimode Fiber Optical Networks. Sci Rep. 2020 Feb 17;10(1):2740.

26. Horstmeyer R, Judkewitz B, Vellekoop IM, Assawaworrarit S, Yang C. Physical key-protected one-time pad. Sci Rep. 2013 Dec 18;3(1):3543.

27. Silvério T, Dias LMS, Ramalho JFCB, Correia SFH, Fu L, Ferreira RAS, et al. Functional mobile-based two-factor authentication by photonic physical unclonable functions. AIP Advances. 2022 Aug 1;12(8):085316.

28. Du Y, Jothibasu S, Zhuang Y, Zhu C, Huang J. Unclonable Optical Fiber Identification Based on Rayleigh Backscattering Signatures. J Lightwave Technol, JLT. 2017 Nov 1;35(21):4634–40.

29. Nikolopoulos GM, Fischlin M. Quantum key distribution with post-processing driven by physical unclonable functions [Internet]. arXiv; 2023 [cited 2023 May 31]. Available from: http://arxiv.org/abs/2302.07623

30. Herder C, Yu MD, Koushanfar F, Devadas S. Physical Unclonable Functions and Applications: A Tutorial. Proceedings of the IEEE. 2014 Aug;102(8):1126–41.

31. Jain AK, Deb D, Engelsma JJ. Biometrics: Trust, But Verify. IEEE Transactions on Biometrics, Behavior, and Identity Science. 2022 Jul;4(3):303–23.

32. Kong J, Koushanfar F. Processor-Based Strong Physical Unclonable Functions With Aging-Based Response Tuning. IEEE Transactions on Emerging Topics in Computing. 2014 Mar;2(1):16–29.

33. Pappu R, Recht B, Taylor J, Gershenfeld N. Physical One-Way Functions. Science. 2002 Sep 20;297(5589):2026–30.

34. Chen M, Fridrich J, Goljan M, Lukas J. Determining Image Origin and Integrity Using Sensor Noise. IEEE Transactions on Information Forensics and Security. 2008 Mar;3(1):74–90.

35. Seve E, Pesic J, Delezoide C, Giorgetti A, Sgambelluri A, Sambo N, et al. Automated Fiber Type Identification in SDN-Enabled Optical Networks. J Lightwave Technol. 2019 Apr 1;37(7):1724–31.

36. Soumplis P, Christodoulopoulos K, Quagliotti M, Pagano A, Varvarigos E. Network Planning With Actual Margins. J Lightwave Technol. 2017 Dec 1;35(23):5105–20.

37. Ding Z, Yao XS, Liu T, Du Y, Liu K, Jiang J, et al. Compensation of laser frequency tuning nonlinearity of a long range OFDR using deskew filter. Opt Express, OE. 2013 Feb 11;21(3):3826–34.

38. Zhao S, Cui J, Suo L, Wu Z, Zhou DP, Tan J. Performance Investigation of OFDR Sensing System With a Wide Strain Measurement Range. J Lightwave Technol, JLT. 2019 Aug 1;37(15):3721–7.

39. Tsuji K, Shimizu K, Horiguchi T, Koyamada Y. Coherent optical frequency domain reflectometry for a long single-mode optical fiber using a coherent lightwave source and an external phase modulator. IEEE Photonics Technology Letters. 1995 Jul;7(7):804–6.

40. Ito F, Fan X, Koshikiya Y. Long-Range Coherent OFDR With Light Source Phase Noise Compensation. Journal of Lightwave Technology. 2012 Apr;30(8):1015–24.

41. Nadimi Goki P, Mulugeta TT, Caldelli R, Potì L. Optical Systems Identification through Rayleigh Backscattering. Sensors. 2023 Jan;23(11):5269.

42. Goki PN, Civelli S, Parente E, Caldelli R, Mulugeta TT, Sambo N, et al. Optical identification using physical unclonable functions [Internet]. arXiv; 2023 [cited 2023 Jun 7]. Available from: http://arxiv.org/abs/2305.02141

43. Peterson E. Developing Tamper-Resistant Designs with Zynq UltraScale+ Devices. 2018;

44. Rührmair U, Devadas S, Koushanfar F. Security based on physical unclonability and disorder. In: Introduction to hardware security and trust. Springer; 2011. p. 65–102.

45. Wali A, Dodda A, Wu Y, Pannone A, Reddy Usthili LK, Ozdemir SK, et al. Biological physically unclonable function. Commun Phys. 2019 Apr 26;2(1):1–10.

46. Pavanello F, O'Connor I, Rührmair U, Foster AC, Syvridis D. Recent Advances in Photonic Physical Unclonable Functions. In: 2021 IEEE European Test Symposium (ETS). 2021. p. 1–10.

47. Goki PN, Mulugeta TT, Sambo N, Caldelli R, Potì L. Network Authentication, Identification, and Secure Communication through Optical Physical Unclonable Function. In: European Conference on Optical Communication (ECOC) 2022 (2022), paper We565 [Internet]. Optica Publishing Group; 2022 [cited 2023 May 31]. p. We5.65. Available from: https://opg.optica.org/abstract.cfm?uri=ECEOC-2022-We5.65

48. Poti L, Goki PN, Mulugeta TT, Sambo N, Caldelli R. Optical Fingerprint: a Possible Direction to Physical Layer Security, Authentication, Identification, and Monitoring. In: 2022 61st FITCE International Congress Future Telecommunications: Infrastructure and Sustainability (FITCE) [Internet]. Rome, Italy: IEEE; 2022 [cited 2023 Jun 7]. p. 1–6. Available from: https://ieeexplore.ieee.org/document/9934467/