Laser Nonlinearity based Optical Physical Unclonable Function with Random Fiber Bragg Grating

Kaiyu Liu, Hanwen Luo, Lei Deng, Qi Yang, Deming liu, Zhijun Yan,* AND Mengfan Chen*
National Engineering Research Center for Next Generation Internet Access System, School of Optical and Electronic Information, Huazhong University of Science and Technology (HUST)
Wuhan 430074, China
*Corresponding author: yanzhijun@hust.edu.cn , chengmf@mail.hust.edu.cn

***Abstract*—We propose and experimentally demonstrated an optical physical unclonable function based on the inner nonlinearity of a distributed feedback laser and an external random-fiber-Bragg-grating. The reliability and randomness are verified.**

***Keywords*—physical unclonable functions, semiconductor laser, random fiber Bragg gratings**

I. INTRODUCTION

In the era of the Internet of Things, data security is facing more complex risks and challenges than past. As a primitive that extract secrets from the physical characteristics of hardware structures, Physical unclonable function (PUF) is a reliable method to resist external intrusion attacks against digital memory [1]. It uses unclonable nonlinearity of hardware devices to generate challenge-response pairs (CRPs) in real time, meaning difficult to imitate.

PUFs are widely used in identity authentication, secret key generation, etc [1,2]. A variety of electronic PUF designs [3,4] have made considerable progress in the field of integrated circuits. When focusing on the application in optical network, Optical PUFs (O-PUFs) have natural advantages, such as broader bandwidth and higher processing rates. O-PUFs usually show more complex physical behavior, meaning more difficult to be cloned [5].

Early schemes use the camera to detect the scattering 2D image of Inhomogeneous Structures [6]. In recent years, the design of O-PUFs based on micro-nano optical structures, optical devices, or optical chaos has gradually received attention. In 2017, Grubel, et al validate an O-PUF realized using guided-wave nonlinear silicon photonic devices [7]. It is directly compatible with both planar semiconductor fabrication and optical communications hardware. In 2022, Monet F, et al designed Random Optical Grating by Ultraviolet or ultrafast laser Exposure (ROGUE). [8] They lead to the idea of producing PUFs by making use of backscatter scattering of ROGUE.

Semiconductor laser also has unique inner nonlinear effect, which can be described by classic Lang-Kobayashi (LK) equations. Such nonlinearity has already been applied in many fields, including optical chaos, optical frequency comb, etc. [9,10]. In 2022, Valerio Anovazzi-Lodi proposed a PUF-like authentication method using two chaotic lasers [11]. Through simulation, they proved the feasibility of designing PUF based on the parameter sensitivity of chaotic laser. Although the inner nonlinearity of laser has unique characteristics and a certain unclonability in theory, it is hard to control, with parameter space also limited.

Here we design an active-passive cooperative laser nonlinearity-based physical unclonable function (LN-PUF) structure based on distributed feedback (DFB) laser and random fiber Bragg grating (RFBG). We use RFBG placed behind a laser to provide additional unclonable parameter dimension, making up for the limitations on laser nonlinearity. Through experiment, the proposed scheme shows similar randomness with other O-PUF schemes but has higher reliability at low cost and low implementation complexity.

II. PRINCIPLE

Fig. 1 (a) shows the basic structure of the proposed LN-PUF and the experimental device for obtaining CRPs. CRPs are the embodiment of PUF's unique physical characteristics on input and output. By inputting an input challenge signal to the PUF, you can get an output response signal that is not related (or has a very low correlation) to the challenge signal. For the same PUF, the same input always obtains consistent output, while for different PUFs, consistent output cannot be obtained. Inside the LN-PUF module, the challenge signal undergoes the nonlinear transformation of the DFB laser, and the output light will be injected into the RFBG to generate the backscatter light. The backscatter light is then converted into the response electrical signal by the PD. The electrical signal is subjected to a post processing algorithm to obtain a digital response signal. Here, the challenge signal and the response signal constitute a group of CRPs.

The PUF is reflected in the nonlinear fingerprint characteristics of DFB laser and the complex multi-wavelength reflection phenomenon of the random grating, which are difficult to replicate. The advantages of this design lie in 1) The LN-PUF structure shows low implementation complexity; 2) The reflection spectrum of RFBG can increase the non-clonability of the structure and hide the characteristic parameters of DFB laser; 3) The RFBG has the advantage of stable performance and free insertion and removal in practice, facilitating system updates.

We build a challenge-response link containing challenge generator and LN-PUF, as shown in Fig. 1 (a). In the challenge generator module, the laser diode (LD) emits the light with the wavelength of 1550nm. The arbitrary waveform generator (AWG) drives the phase modulator (PM) through the electrical amplifier (EA) to generate a phase modulated pseudo-random bit sequence for optical injection. The polarization is adjusted to align with the DFB laser by the polarization controller (PC). The challenge optical signal is then injected to the LN-PUF structure after the erbium- doped

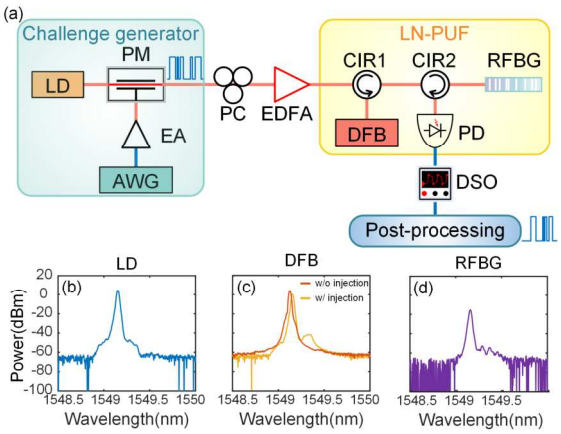

Fig 1. (a) Experimental setup. (b) spectrum of LD in free running state, (c) spectrum of DFB laser in free running state and spectrum of DFB laser under injection, (d) spectrum of RFBG back scattering

optical fiber amplifier (EDFA). In the LN-PUF, the challenge signal undergoes the nonlinear transformation of the DFB laser. After circulator1 (CIR1) and CIR2, the reflected light is injected into the RFBG for random backscatter. The back-scattering light enters the photodiode (PD) for opto-electrical conversion. The electrical response signal is obtained through a digital oscilloscope (DSO). Finally, the binary digital response sequence is obtained after the post-processing algorithm. The digital input and output challenge-response link are then established.

Next, we illustrate the optical nonlinear transform that occur inside the DFB laser: With a current injection, electron-hole recombination in the active region radiates photons with corresponding energy. Then these photons will be reflected by each grating on the active layer surface. DFB laser oscillates utilizing optical coupling formed by gratings with equal spacing along the longitudinal direction. Fig. 1 (b) shows the spectrum of the LD in free running state. When the 1550nm driven light is injected into the DFB laser, the Bragg reflection is generated through multiple gratings with equal spacing distribution inside the DFB laser, and the reflected light becomes the output of the DFB laser after coupling. Fig. 1 (c) shows the spectrum of the DFB laser in free running state or under the challenge signal injection respectively. The beat phenomenon in the DFB laser will lead to a secondary peak appearing next to the main peak. The RFBGs used in this letter are manufactured by writing a randomly spaced grating array in the fiber core, and their reflection spectrum are formed by the superposition of multiple F-P interferences. Thus, the fiber parameters and backscattering characteristics of RFBGs are difficult to regenerate. Fig. 1 (d) shows the backscattering spectrum of the RFBG, which exhibits more complex nonlinear characteristics than its injection, optimizing PUF performance.

III. Experimental Setup and Results

To prove the potential of LN-PUF in optical network security applications, we prepare two RFBGs to represent legal and illegal PUF compositions, and the remaining devices are shared under experimental conditions. In practice, illegal PUF DFB lasers can also be different from legitimate ones Then we compare the differences of CRPs in inter or intra-groups. Fig. 1 (a) shows the experimental settings for extrac-

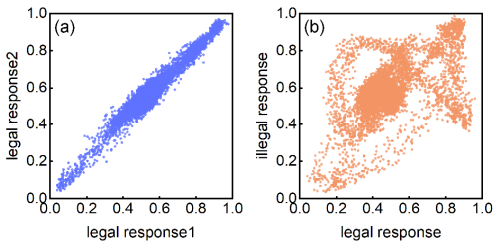

Fig 2. (a) correlation diagram between legal response1 and legal response2 (b) correlation diagram between legal response and illegal response.

-ting CRPs. For the sake of simplicity, the modulation format of the challenge signal is set as OOK.

The experimental parameters are set as follows: the half-wave voltage of PM is 3.5V, the AWG voltage is 200mV, the free running current of the modulation rate 5Gbit/s DFB laser is set to 30mA, the output optical power is 4.4dBm, and the central wavelength is 1549.13nm. We input a 5 Gbit/s multi-cycle OOK sequence as a digital challenge. The sampling rate of DSO is 100G sample/s to obtain a response analog waveform. The analog waveform is quantized into a binary sequence by a post-processing algorithm. The binary sequence of the input OOK signal and the response binary sequence constitute a pair of CRPs. By comparing the CRPs, the performance of LN-PUF can be tested.

Fig. 2 (a) and (b) show the correlation diagram between the two response processes of the same set of PUFs and different set of PUFs respectively under the same challenge signal. The correlation diagrams can preliminarily explain the consistency and sensitivity of analog CRPs of LN-PUF.

Then, the output light of the DFB laser is injected into the RFBG. Due to the unique reflection intensity of different wavelengths, the multiple peaks of the injected light will lead to non-cloning differences in the light intensity of the reflection spectrum. As expected, different LN-PUFs show unique spectral and temporal pulse response behaviors. This preliminarily proves the PUF performance of the LN-PUF design.

We use a dual-threshold quantization algorithm to process the analog response signal. The basic principle is as follows.

$$\begin{cases} T_{up} = mean + \varepsilon * std \\ T_{down} = mean - \varepsilon * std \end{cases} \quad (1)$$

$$A(y) = \begin{cases} 1 & if\ C(y) > T_{up} \\ 0 & if\ C(y) < T_{down} \end{cases} \quad (2)$$

where, $T_{up}(T_{down})$ represents the high (low) threshold value calculated from the mean value $mean$, standard deviation value std, and the manually selected scalar ε. $C(y)$ represents the sequence of analog signals used for quantification, and $A(y)$ represents binary sequence after dual-threshold quantization. Sampling values between T_{up} and T_{down} are discarded.

When the value of ε becomes larger, the effective digits of the extracted sequence will be smaller, but the consistency of the sequence will be higher at the same time. Considering the effectiveness and reliability of the extraction process, we finally choose to set ε to 0.3. Besides, it is necessary to align and normalize the analog signals $A(y)$ and $A'(y)$ before quantization. Two columns of sequences will share the positional sequence number of the discarded analog values, and discard the inconsistent parts to ensure their sequence len-

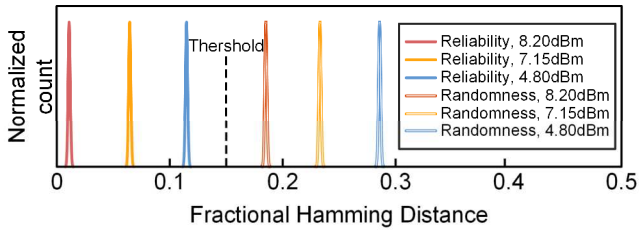

Fig 3. the reliability and randomness FHD values of legal or illegal LN-PUF CRPs under different laser injection intensities

-gth is consistent.

To evaluate the function of the proposed PUF, we mainly consider the reliability and randomness of the PUF output. They are evaluated by fractional Hamming distance (FHD). The calculation formulas are as follows:

$$FHD(R_A, R'_A) = \frac{1}{n}\sum_{i=1}^{n} R_A \oplus R'_A \quad (3)$$

$$FHD(R_A, R_B) = \frac{1}{n}\sum_{i=1}^{n} R_A \oplus R_B \quad (4)$$

where R_A and R'_A represents the n-bit response obtained by injecting the same challenge signal into the PUF A at different times. $FHD(R_A, R'_A)$is used to measure the difference between the two legal responses, representing the probability of a single response bit changes. The ideal value is 0. $R_A$and R_B represent the extracted response signal of PUF A and PUF B under the same challenge injected. $FHD(R_A, R_B)$ represents the probability of different bits of R_A and R_B. When the answer process of PUF is completely random and independent of each other, the ideal value of $FHD(R_A, R_B)$ is 50%, which indicates that there is no correlation between the answer bit sequences.

To find the best value, we set another variable as the optical power of injected DFB laser. By adjusting EDFA, we measure $FHD(R_A, R'_A)$ and $FHD(R_A, R_B)$ when the injection intensity is 4.8dBm, 7.15dBm and 8.2dBm respectively. Firstly, we register the LN-PUF device with 10 analog response sequences injected and sampled by the PRBS15 encoded OOK sequence. Then we quantize 10 analog response sequences from the legal LN-PUF and 10 analog response sequences from illegal LN-PUF to compare their FHD values. In addition, we also calculate the correlation coefficient (CC) of the two analog signal sequences after alignment and normalization as an auxiliary judgment.

The experimental results show that the reliability of LN-PUF gradually increases and the randomness gradually decreases with the injection intensity increasing. Besides, there are obvious differences in the CRPs produced by different PUF copies. Fig. 3 shows that the average $FHD(R_A, R'_A)$ of legal LN-PUF copies gradually decreases from 0.1149 to 0.0110 (the ideal value is 0), and CC increases from 0.81081 to 0.97624; the average $FHD(R_A, R_B)$ of illegal LN-PUF copies decreased from 0.2858 to 0.1851 (the ideal value is 0.5), and CC was between 0.44194 and 0.55383. FHD values of legal LN-PUF and illegal LN-PUF have obvious interval differences. When the FHD value for judgment is introduced between the two regions, such as 0.15, different groups can be distinguished.

However, there is still a gap between the value of $FHD(R_A, R_B)$ and the ideal value (0.5). The CC of the illegal response and the legal response is around 0.54 instead of 0, matching the non-ideal result of FHD. The reasons are as follows: 1) The injection of the OOK challenge sequence causes a periodic gap in the response sequence. This is good for alignment and improves reliability, but reduces the difference between the illegal PUF challenge-response process; 2) The double threshold quantization process makes additional discards to ensure the final extracted sequence length is consistent, which undoubtedly sacrifices part of the randomness of PUF structure. These two deficiencies indicate that the current LN-PUF still needs to be improved.

LN-PUF can well perform the function of authentication because its reliability is higher than most O-PUFs. But we use OOK injection and adopt a special post-processing algorithm, which has a tradeoff with randomness. Therefore, when we design the LN-PUF structure or the post-processing algorithm, they should be adjusted according to the application scenario.

IV. Conclusion

In conclusion, we propose LN-PUFs and carry out a simple LN-PUF design based on DFB laser and RFBG. By testing different PUF copies, we prove the proposed design has stronger reliability than existing optical-PUF schemes, reaching the order of 0.01. This design has advantages in terms of price, complexity, and optical fiber transmission network construction, and can be well applied to physical layer information security. Besides, we make a discussion on the tradeoff between the reliability and randomness of PUF. When PUF is too sensitive to the initial value, its reliability is often affected, but its randomness may be improved.

Acknowledgment

This work was supported by the National Key Research and Development Program of China (2021YFB2900901); National Natural Science Foundation of China(62175077).

References

[1] C. Herder, M. D. Yu, F. Koushanfar and S. Devadas, "Physical Unclonable Functions and Applications: A Tutorial," in Proceedings of the IEEE, vol. 102, no. 8, pp. 1126-1141, Aug. 2014.

[2] G. Edward Suh and Srinivas Devadas, "Physical unclonable functions for device authentication and secret key generation," In Proceedings of the 44th annual Design Automation Conference, Association for Computing Machinery, pp. 9-14. 2007.

[3] Chen, Lanxiang. "A framework to enhance security of physically unclonable functions using chaotic circuits." Physics Letters A 382.18, pp. 1195-1201. 2018.

[4] Tehranipoor, Fatemeh, et al. "DRAM-based intrinsic physically unclonable functions for system-level security and authentication." IEEE Transactions on Very Large Scale Integration (VLSI) Systems 25.3, pp. 1085-1097. 2016

[5] Ruhrmair, Ulrich, and Jan Solter. "PUF modeling attacks: An introduction and overview." 2014 Design, Automation & Test in Europe Conference & Exhibition (DATE). 2014.

[6] Pappu, Ravikanth, et al. "Physical one-way functions." Science 297.5589 (2002): 2026-2030.

[7] Grubel, Brian C., et al. "Silicon photonic physical unclonable function." Optics Express 25.11 (2017): 12710-12721.

[8] Monet, Frédéric, Anthony Roberge, and Raman Kashyap. "Physical Unclonable Functions based on random gratings." Latin America Optics and Photonics Conference. Optica Publishing Group, 2022.

[9] Sciamanna, Marc, and K. Alan Shore. "Physics and applications of laser diode chaos." Nature photonics 9.3 (2015): 151-162.

[10] Cundiff, Steven T., and Jun Ye. "Colloquium: Femtosecond optical frequency combs." Reviews of Modern Physics 75.1 (2003): 325.

[11] Annovazzi-Lodi, Valerio, et al. "Challenge-Response Authentication Scheme With Chaotic Lasers." IEEE Journal of Quantum Electronics 58.1 pp.1-7, 2017.