This article has been accepted for publication in IEEE Journal of Quantum Electronics. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/JQE.2021.3134966

Challenge-Response Authentication Scheme with Chaotic Lasers

Valerio Annovazzi-Lodi, *Senior Member, IEEE,* Lorenzo Lombardi*, Member, IEEE,* and Giuseppe Aromataris

***Abstract*—In this paper, we numerically evaluate a hardware-based method for authentication using a pair of twin chaotic lasers. This method belongs to the PUF (Physically Unclonable Function) class; however, it does not require storing the response of the hardware in a database, because both users own the same hardware (one of the twin chaotic lasers), producing, on the fly, the same response, i.e., the same chaotic waveform, when subject to the same stimulus (injection from a third laser) in the same working conditions (local injection, pump current). A bit sequence can be easily obtained from the chaotic waveforms by electronic processing, and authentication consists in comparing the sequences produced by the twin lasers. This scheme is proposed above all for authentication of a client in an unsecure environment to a server in a secure environment, but it can be used also for peer-to-peer authentication.**

Both the case of open- and close-loop chaotic lasers are considered. Simulations are based on the Lang-Kobayashi model.

***Index Terms*—Optical chaos, Communication system security, Authentication, Synchronization**

I. Introduction

Privacy and security in data transmission is one of the most important topics in modern telecommunication systems. One of the most critical security challenges is the identification of an authorized user. Authentication [1] is the process of verifying the user identity (in an unsecure environment), before giving access to the system resources (in a secure environment).

A common element which is required to enable the above procedure is a secret which an adversary cannot obtain or duplicate.

While in most cases authentication procedures are based on software algorithms, hardware-based methods are increasingly gaining attention, especially for the Internet of Things (IoT) applications.

Among them, Physical Unclonable Functions (PUFs) have been proposed as an alternative to standard authentication protocols [2,3,4].

With PUFs, secret data are derived from complex physical characteristics of ICs or other electronic devices, rather than storing them in a digital memory of the unsecure environment. For example, a volatile secret can be generated from the random delay characteristics of wires, transistors, or memory elements [5]. Because of the random parameter variation during an IC fabrication process, the secret is extremely difficult to predict or extract. The typical authentication scheme consists of sending a stimulus (challenge) from the server to the user, to be applied to the device, so that a response is produced. The response is sent back to the server and compared to what stored in the server database, in the secure environment.

Secrets in the unsecure environment only exist when the circuit is on. This requires the adversary to generate his attack while the IC is running to get the secret, a significantly harder job than discovering non-volatile stored keys.

In the optoelectronic domain, semiconductor lasers are possible candidates for such method of authentication. The dispersion of their parameters is already exploited in chaos-based steganography [6,7]. In a proposed scheme [8,9], two lasers (the Slaves) are driven to chaos by optical injection from a third laser (the Driver, DRV), and the chaotic waveform produced by one Slave laser (SL1) is used to hide a message. The message can be recovered by subtracting the identical chaos generated by the other Slave laser (SL2). This is possible only for an authorized recipient, who owns a laser SL2 which is (almost) identical to SL1, i.e., if the Slaves are twins. Moreover, proper operating conditions are required, resulting in the slave lasers being synchronized.

While such a laser pair can be owned by two authorized users (devices are usually selected from the same wafer), it is very difficult for an adversary to match his device to the twin pair, and, thus, to get chaos synchronization and recover the message. Private transmission based on synchronized chaotic lasers [6,7] has been widely studied in

Manuscript received …

The authors are with the Dipartimento di Ingegneria Industriale e dell'Informazione, Università degli Studi di Pavia, 27100 Pavia, Italy (e-mail: valerio.annovazzi@unipv.it; lorenzo.lombardi@unipv.it; giuseppe.aromataris@unipv.it; corresponding author: Valerio Annovazzi-Lodi).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier…

This article has been accepted for publication in IEEE Journal of Quantum Electronics. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/JQE.2021.3134966

the literature. Digital transmission on a metropolitan network [10] has been performed years ago, and integrated-optics modules for chaotic transmitters and receivers [11] have been developed.

In this paper, we show that the strong dependence of the chaotic waveform, from laser parameters, can be exploited to realize an authentication scheme based on twin lasers.

II. The Authentication scheme

In Fig.1 we show a possible client-server implementation. It is based on the standard three-laser setup [8,9,12].

The driver laser DRV is routed to chaos by delayed optical feedback using a mirror. Slave lasers SL1,2 are in the chaotic regime, either due to delayed optical feedback from a local mirror (close loop) [12], or just because of injection from DRV (open loop) [9]. In suitable operating conditions, both slaves produce the same chaotic waveform, i.e., they are synchronized.

In this setup, the challenge is the DRV injection, and the response is the chaotic waveform produced by the Slave SL2. The reference response in the secure environment is the chaotic waveform generated by SL1, receiving the same injection from DRV. Only if SL1 and SL2 are twins, or have very similar parameters, the two responses match and authorization is granted.

A convenient way of comparing the two responses, in the digital domain, is the generation of binary sequences from the chaotic waveforms by standard electronic processing, using e.g., Schmitt triggers with a properly selected threshold. Matching of the bit sequences is then evaluated by a suitable digital comparator block (EXOR). The response can be sent back to the secure environment by a wired or RF electrical link (as in Fig.1) or by an optical link. The optical paths in Fig.1 may be in fiber or in free space.

A specific advantage of the proposed scheme is that the responses of the chaotic lasers need not to be stored, not even in the secure environment, but are produced on the fly at both ends of the connection, which increases security.

In the client-server setup of Fig.1, the Driver is included in the secure (server) environment.

Peer to peer schemes can be also considered. In this option, the setup of Fig.1 would be modified in that the DRV is external from the environment of both users and is managed by a third-party provider. In this case the DRV sends the same stimulus to the slaves SL1, SL2 of each user, and each user can compare the other user's bit sequence with his own, to find if they match. Since security is entirely provided by the slave lasers matching, the DRV emission can be shared between different pairs of users, as suggested in [13] for a different application.

In practice, as in most PUF based methods, some errors must be tolerated [2], because perfect synchronization is hardly observed in experiments.

This limitation in the synchronization quality has little impact on security in the proposed application, provided that the bit sequence is long enough. It has also little impact in steganography, where it simply increases the BER of the recovered signal. However, it causes another possible application of the proposed scheme, i.e., the cryptographic key exchange [14,15], to be difficult to implement, since in this case the bit sequences must be strictly identical.

In the following, the propagation delay is assumed to be negligible, i.e., the client (the unit asking for access) is next to the server (the unit giving access).

This is, for example, the case of a safe, where the block 'secure environment' in Fig.1 plays the role of the lock, while the block 'unsecure environment' plays the role of an optoelectronic key, by which only the authorized user is allowed to open the safe.

In other cases, a propagation delay must be considered along the challenge and response paths. It can be measured, e.g., by a probe pulse generated by the DRV, and then compensated, by using a suitable delay line or a memory in the secure environment.

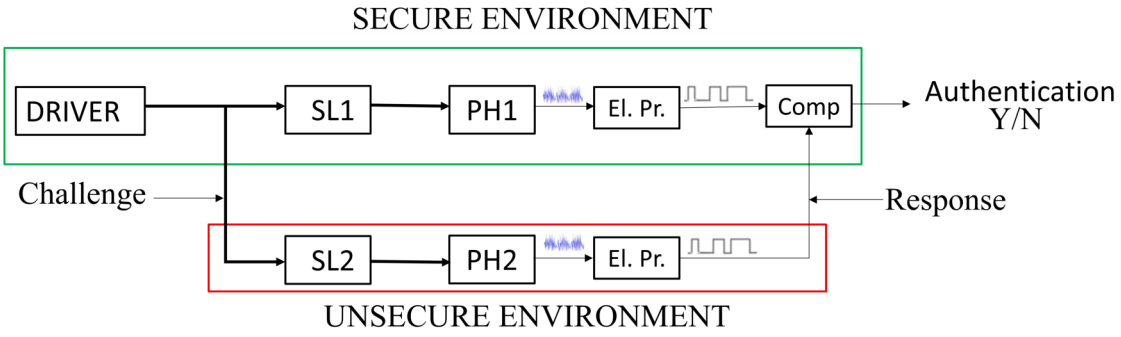


Fig.1 Authentication scheme based on twin lasers SL1 and SL2, synchronized by injection from a common driver (PH: photodiode, El. Pr.: Electronic processing, Comp: comparator). Bold lines are optical paths, light lines are electrical paths. Chaotic waveforms and the obtained bit sequences are also shown.

This article has been accepted for publication in IEEE Journal of Quantum Electronics. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/JQE.2021.3134966

PARAMETER	DRIVER	TWIN SL1/SL2	UNIT
Linewidth enhancement factor	$\alpha = 3.3$	$\alpha = 3$	
Photon lifetime	$\tau_p = 2.3$	$\tau_p = 2.0$	ps
Carrier lifetime	$\tau_s = 1.7$	$\tau_s = 2.0$	ns
Gain coefficient	$\xi = 6.9 \cdot 10^{-13}$	$\xi = 8.1 \cdot 10^{-13}$	$m^3 \cdot s^{-1}$
Carrier density at transparency	$N_0 = 1.26 \cdot 10^{24}$	$N_0 = 1.10 \cdot 10^{24}$	m^{-3}
Threshold current	$I_{th} = 12.4$	$I_{th} = 11.0$	mA
Laser cavity roundtrip time	$\tau_{in} = 8.0$		ps
Solitary laser pulsation	$\omega = 1.2177 \cdot 10^{15}$		$rad \cdot s^{-1}$
External cavity roundtrip time	$\tau = 0.3$		ns
Active region efficiency	$\eta = 1$		
Active region volume	$V = 8.0 \cdot 10^{-17}$		m^3
Active region emission area	$A = 2.0 \cdot 10^{-13}$		m^2
Non linear gain coefficient	$\varepsilon = 2.5 \cdot 10^{-23}$		m^3
Confinement factor	$\Gamma = 0.36$		
Spontaneous emission factor	$\beta = 1.0 \cdot 10^{-6}$		
Active medium refractive index	$n = 3.0$		
Stimulated emission cross section	$\zeta = 1.0 \cdot 10^{-20}$		m^2
Photodiode responsivity	$\sigma = 1.0$		$A \cdot W^{-1}$

Table I: Model Parameters

III. NUMERICAL MODEL

The well-known Lang-Kobayashi equation set [16], modified to take into account external injection [6,7] has been used to model the different lasers of the setup of Fig.1. This mathematical model is widely accepted for chaos investigations [6,13]. It provides fast numerical integration, even if it does not take into account the technological details of devices. Even though the three-laser scheme has been already used for steganography, the application we propose in this paper is different, since bit sequences from chaotic waveforms are generated and compared, detecting errors, instead of hiding and extracting a message from chaos. This requires a different analysis and new simulations. Also, the selection of the DRV, and thus the optimization of the whole system is different, as it will be explained in Sect.IV.

The equations for DRV, SL1, SL2 are obtained by varying index J in eqs.1-3:

$$\begin{aligned}\frac{dE_J(t)}{dt} &= \frac{1}{2}(1+i\alpha)\left[G_J(t)-\frac{1}{\tau_p}\right]E_J(t)+\\ &+\frac{K_J}{\tau_{in}}E_J(t-\tau)exp(-i\omega\tau)+\\ &+\Delta_{D,J}\frac{K_{D,J}}{\tau_{in}}E_T(t-T_{D,J})exp(-i\omega T_{D,J})+\\ &+F_{sp,J}(t)+L_{E,J}(t)\end{aligned} \tag{1}$$

$$\frac{dN_J(t)}{dt} = \frac{\eta}{eV}I_J - \frac{N_J(t)}{\tau_s} - G_J(t)\,|E_J(t)|^2 + L_{N,J}(t) \tag{2}$$

$$G_J(t) = \frac{\xi\left[N_J(t)-N_0\right]}{1+\varepsilon\Gamma\,|E_J(t)|^2} \tag{3}$$

For $J=D$, $J=S1$ we have the set describing DRV/SL1 (the secure environment: D stands for DRV, S1 for SL1). Coefficient $\Delta_{D,J}$ is zero for $J=D$.

For $J=D$, $J=S2$ we have the set describing DRV/SL2 (the unsecure environment: D stands for DRV, S2 for SL2). Coefficient $\Delta_{D,J}$ is zero for $J=D$.

In eqs. 1-3, $E_J(t)$ is the slowly varying, complex electric field, $N_J(t)$ the carrier density, $G_J(t)$ the linear gain coefficient, I_J the pump current, e the electron charge and K_J the feedback parameter from the external mirror (K_J =0 for the open loop) and τ is the external cavity roundtrip time. For $J=S1, S2$ the terms $K_{D,J}/\tau_{in}$ and $T_{D,J}$ represent the injection rate and the propagation time from the driver to the slaves, respectively. For simplicity, in the simulations we have taken $T_{D,J}=0$. Other parameters are listed in Table I. Spontaneous emission term $F_{sp,J}(t)$ and Langevin noise terms $L_{E,J}(t)$ and $L_{N,J}(t)$ [17] have been also included. This numerical model is discussed in detail in [9,12].

As usual, the electric fields are normalized in [$m^{-3/2}$], and their true value (in [V/m]) is given by:

$$E_{True}(t) = \left(\xi\hbar\omega\frac{Z_0}{n\zeta}\right)^{\frac{1}{2}}E(t) \tag{4}$$

where $\hbar$ is the Planck constant, n is the active medium refractive index, ζ is the stimulated emission cross-section, $Z_0 = (1/\epsilon_0 c)$ the vacuum impedance (ϵ_0, vacuum permittivity and c, speed of light).

In simulations, the laser pairs have been assumed to work at the same optical frequency. In an experimental setup the frequency mismatch (due, e.g., to current difference) is usually minimized by a suitable temperature trimming.

In all simulations, the shot noise of the pump currents,

This article has been accepted for publication in IEEE Journal of Quantum Electronics. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/JQE.2021.3134966

and the Johnson noise of the typical 50Ω load resistance of high frequency photodiode amplifiers (not shown in Fig.1) have been taken into account. It has been found that the effect of such noise in minimal. Simulations were made in the Matlab environment.

IV. Simulations with Twin Lasers

Simulation parameters are shown in Table I. Parameters were initially taken identical for SLs (perfect twin pair) and were the same as in our previous works [9,12]. Instead, a larger mismatch has been introduced for the DRV parameters, to have a very low correlation between the chaotic waveforms produced by DRV and the SLs. This is important if the adversary has access to DRV (e.g., in a peer-to-peer scheme where DRV is shared): the bit sequence, which can be obtained directly from the DRV, must be completely different from that produced by the SLs. The original parameter set offered a sufficiently low correlation between SLs and DRV for steganography, where a BER of the adversary of the order of 10^{-2} is high enough for secure operation. However, the application to authentication requires a better DRV selection.

For the DRV we assumed I_D=23.4 mA, K_D=0.2 throughout all our numerical investigations. This working point has been selected since the driver laser exhibits a large chaotic spectrum due to optical feedback. Moreover, it ensures low correlation between DRV and SL chaos.

On the other hand, the pump currents of SL1 and SL2 and the injection power from DRV into SL1 and SL2 lasers have been swept in the numerical analysis.

By numerical simulations, we have looked for a working point for the twin pair where i) the correlation between DRV and SL1/2 is low, ii) the correlation between SL1 and SL2 is high, even with a small parameter mismatch (see Sect.5). We have finally selected for both Slave lasers a pump current of 51 mA and an optical injection level from the driver K_{DS}=0.14.

For the close loop we have further assumed K_S=0.01 and τ=0.3 ns for the injection level and for the time of flight from each local mirror to each slave.

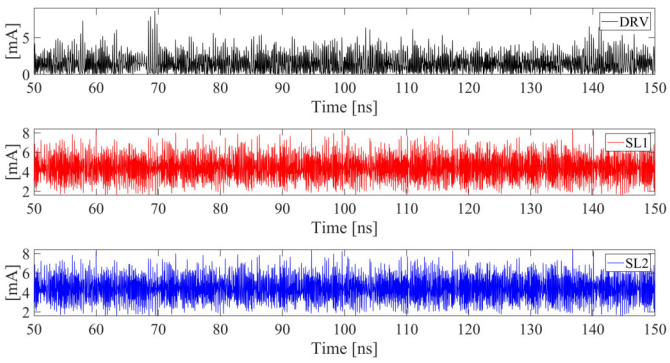


Fig.2 Typical time series from chaotic waveforms generated by DRV, and by twin SL1 and SL2 (open loop). The SL1/SL2 chaotic waveforms are identical, because the lasers are twins and synchronized. Instead, DRV/SL chaos is significantly different as required for security.

The different evolution of the DRV with respect to SL1,2 is evident by considering the chaotic waveforms in the time domain. In Fig. 2, time series taken from longer simulations are shown for the open loop. The length of these samples has been selected in order to show the chaotic regime in some detail.

We observe that the selection of the working point for DRV and the SLs is not critical. Other values of I_D and K_D can be found which produce a large chaotic spectrum and low correlation between DRV and the SLs. However, in the present analysis we have kept, whenever possible, the same parameter values of [9,12]: only some parameters of the DRV have been changed, and thus its pump current. Also, the pump currents of the SLs have been optimized accordingly.

From the chaotic waveforms, by applying a 1 GHz low-pass filters to each output, followed by an optimized threshold comparator, we have obtained the required bit sequences (see in Fig.3 a sample for the open loop). Since the SL parameters are the same, the bit sequences are also identical (as the chaotic waveforms of Fig.2), but they are significantly different from those extracted from the DRV. The coincidence rate on a long (128 bit) sequence is next to the optimum condition (50%) of complete uncorrelation between sequences produced by DRV and by SL1,2.

A similar result has been found for the close loop in ideal conditions.

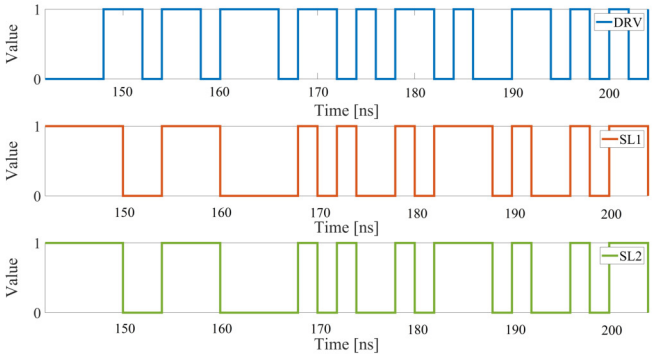


Fig.3 Sample bit sequences extracted from DRV compared to those produced by twin slaves SL1/SL2 in optimized conditions for the open loop. The SL1/SL2 sequences are identical, while the DRV/SL correlation is very low.

V. Laser Parameter Mismatch

Though a high-quality synchronization, and a virtually zero error count, can be achieved in idealized conditions, it is important to investigate the effect of mismatch of internal laser parameters (α, τs, τp, ξ) between SL1 and SL2, to better evaluate both feasibility and security, since in real operating conditions "twin" lasers have small unavoidable differences.

We have assumed a mismatch of up to 2% in the internal parameters of the SL2 laser with respect to the SL1 for the

This article has been accepted for publication in IEEE Journal of Quantum Electronics. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/JQE.2021.3134966

authorized user, and a mismatch from 3% to 10% for the adversary.

In a previous paper [9], it has been shown that in the three-laser scheme, synchronization decrease due to a small internal parameter mismatch can be at least partially compensated by acting on the SL2 external parameters: pump current and injection. Thus, in simulations we have swept these parameters for SL2, in order to minimize errors, as one would do experimentally.

However, it must be recognized that the authorized user and the adversary are in very different working conditions. The authorized user can train his system, by comparing his own bit sequence (SL2) with that produced by SL1, before using his system for authentication in the field. (This training is typical of PUF based authentication methods).

On the contrary, this is not possible for the adversary, who can only sweep all internal and external parameters without any knowledge of the SL1 parameters and without any feedback on the bit sequence error number, until he possibly reaches the minimum error number required for authentication.

Thus, the errors to be considered in the case of the authorized user are only the residual errors after optimizing the external parameters (pump current and injection). In the case of the adversary, instead, all errors must be taken into account.

	Open Loop		Close Loop	
	Auth	Adv	Auth	Adv
Max	4	91	10	89
Min	0	0	1	2
Med	2	60	6	53

Table II: Detected bit errors (open loop)

To investigate the system performances, we have considered, both for the open and for the close loop, the error rate, as a function of parameter mismatch, for a 128-bit sequence (2 ns bit time), by varying all internal parameters of SL2 (α ,τs, τp, ξ) in more than 2 million possible combinations.

In more detail, for each mismatch from 1% to 10% (step 1%), errors have been detected for all combinations of internal parameters: this includes changing all values by a positive or negative amount; in other cases, some parameters are varied by the nominal mismatch, while others have been varied by a lower mismatch or have kept their nominal values.

Note that different combinations represent different physical devices, since it is not possible to trim internal parameters on a specific device.

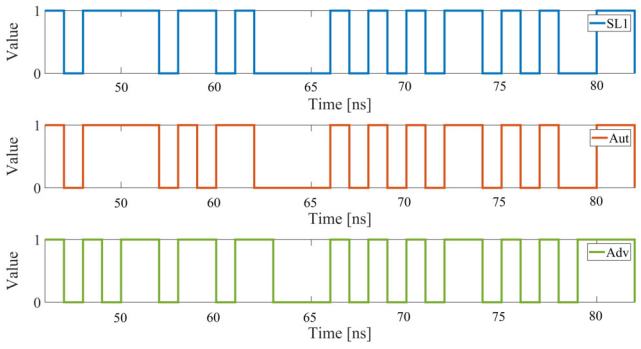
For the close loop, we have kept the nominal values of K_S=0.01 and τ=0.3 ns to be conservative, since these parameters can be easily trimmed, instead. Nevertheless, having two more parameters to be optimized obviously requires an additional effort to the adversary, and this is a specific advantage of the close loop scheme.

The external parameters (pump current and injection) have been swept with respect to their nominal values. This in fact resulted in a partial compensation of the internal parameter mismatch, which can be exploited both by the authorized user and by the adversary. Slave injection was changed by moving K_{DS} from 0 to 0.8 by 0.04 steps; pump current was changed up to 80 mA by 0.5 mA steps.

For mismatch values up to 2% the errors have been detected after sweeping internal parameters and optimizing synchronization, by acting on the external parameters, and this represents the performance of the authorized user. For mismatch values of 3% and over, instead, errors have been detected by simply sweeping internal and external parameters (without optimization), and this represents the performance of the adversary.

A large difference in the maximum and mean error count of the authorized user with respect to the adversary was always found, and increased, as expected, with the mismatch gap between the SL2 of the authorized user and that of the adversary. In Table II we compare, for both the open loop and the close loop configuration, the performance of the authorized user and of the adversary, showing the maximum, mean and minimum number of errors. In this table, we have selected a mismatch of 2% for the authorized user and of 5% for the adversary. From the results of our simulations, this represents a reasonable and conservative choice and demonstrates both the feasibility (assumed mismatch is not too small for the authorized user) and the security (assumed mismatch is not too large for the adversary) of the authentication system.

As expected, the close loop was found to be more sensitive to parameter variation, so that the number of errors for the authorized user is larger for the close loop with respect to the open loop. Both for the open and for the close loop, however, a large difference in the error count of the authorized user with respect to the adversary is found in Table II. It is interesting to observe that the mean error number for the adversary is next to 50%, which is what we would expect from a completely random response.



This article has been accepted for publication in IEEE Journal of Quantum Electronics. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/JQE.2021.3134966

Fig.4 Sample bit sequences for the open loop: SL1 (secure environment), SL2 in optimized conditions (Aut: authorized user, 2% mismatch) and SL2 in typical conditions (Adv: adversary, 5% mismatch).

In Fig.4, we show for the open loop a section of a 128-bit sequence, to allow for a comparison of the SL1 pattern (the reference produced in the secure environment) with the SL2 pattern in optimized conditions (authorized user) and with the SL2 pattern in typical conditions (adversary).

We note that the mismatch results into unperfect synchronization and thus, into some errors even for the authorized user.

We also observe from Table II that the minimum number of errors is zero (open loop) or next to zero (close loop) for both users, because not only the authorized user, but also the adversary has a chance, by sweeping parameters, of getting a true matched pair, guessing also the correct external parameters. However, this event is very unlikely, as shown in Fig.5, where the error histogram is shown for the adversary with the open loop.

Even though the error number represents a valuable assessment of the system quality, the percentage of authentication success, for the authorized user vs. the adversary, is the datum that more directly describes the performance of our system for in-field applications. This is shown in Table III.

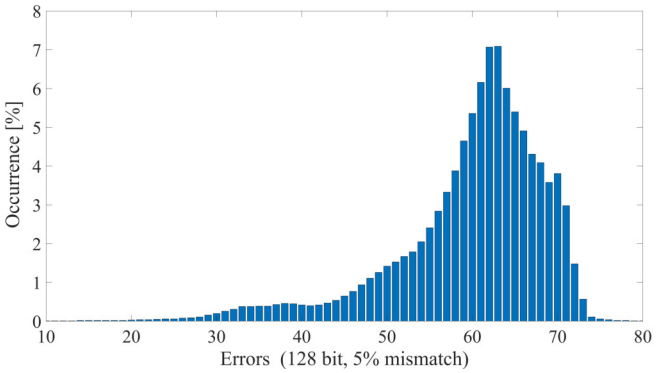


Fig.5 Open loop error occurrence for the adversary

As anticipated, in a practical system some errors in the bit sequence must be tolerated, due to unavoidable small differences of SL2 with respect to SL1, even for the authorized user. The acceptable error number should be selected, in order to have no authentication failures for the authorized user, and a very low success probability for the adversary. This also depends on the length of the bit sequence.

In Tab. III we have assumed that an error count of 6 bits (out of 128) can be tolerated for the open loop and an error count of 12 for the closed loop, which is more sensitive to mismatch. These error thresholds represent a suitable trade-off between security and feasibility since, from Tab. II, the maximum error count for the authorized user is 4 with the open loop and 10 with the close loop. As in Tab. II, the authorized user works in optimized conditions, while the adversary can only sweep his laser parameters.

	Open Loop		Close Loop	
	Auth	Adv	Auth	Adv
Rate	100%	0.0036%	100%	0.0024%

Table III: Authentication success rate (open loop)

From Tab. III, we find that a very well performant authentication system can be designed, with a 100% probability of success for the authorized user, while the adversary has less than 0.01%, both with the open and with the close loop.

The convenience of implementing a close loop system may seem questionable from the results of Table III, since there is apparently no significant security improvement with respect to the open loop. Moreover, the hardware implementation is more critical, and the laser matching requirements are stricter, also for the authorized user. Consider, however, that, as already stated, in the present analysis we have not varied the close loop parameters K_S and τ, to be conservative, since they are easily trimmable and do not represent different physical devices. But in a practical implementation, instead, the adversary has to sweep also these parameters, which represents an additional task and requires additional time.

A possible security improvement for both the open and the close loop could be obtained by a preliminary selection of lasers by the authorized user, i.e., by the exclusion of a limited number of parameter combinations (next to the maximum assumed tolerance). This would result into a full 100% success rate for the authorized user even with a reduced error count and threshold. For example, with reference to the case of Tab. II, III (close loop), a success rate of 100% can be obtained for the authorized user with a maximum error count of 8 (instead of 10), and a threshold of 10 (instead of 12), by removing four specific lasers. The corresponding authentication success rate for the adversary in this case will be more than halved (0.001% vs. 0.0024%).

Possible monolithic or hybrid integration of the proposed system include the InGaAsP technology, which has been already successfully used for cryptosystems based on laser synchronization schemes [11]. For a low-cost high-volume version, the system could take advantage of monolithic integration of CMOS Si/SiO2 devices [18], and of poly-silicon light emitting devices [19]. Moreover, techniques for better managing the low power signals propagating in the optical fibers, such as in [20], could improve performances.

As a final observation, we would like to point out that the security analysis performed in this paper is based on the assumption that the adversary can freely select his laser

parameters. In practice, however, it is difficult to really design and manufacture a laser with given internal parameters. Typically, the adversary can only try a large number of devices, randomly selected on an available laser ensemble. This task is even more difficult if the laser model can be kept secret. On the other hand, it is relatively easy for the authorized user to select a laser twin pair with very similar parameters, produced in close-proximity on the same wafer.

VI. Conclusions

In this paper we have numerically analyzed a three-laser scheme, which is suitable both for client-server and for peer-to-peer authentication. We found that the sensitivity to parameter mismatch is compatible with an experimental implementation. Moreover, this scheme offers, even in its simplest version based on the open loop, a high degree of security, and thus it represents an interesting alternative to other authentication methods.

References

[1] I. Velasquez, A. Caro, A. Rodriguez, "Authentication Schemes and Methods: a Systematic Literature Review", Information and Software technology vol.94, n.1, pp. 30-37, Jan. 2018.

[2] G. E. Suh and S. Devadas, "Physical Unclonable Functions for Device Authentication and Secret Key Generation," 2007 44th ACM/IEEE Design Automation Conference, San Diego, CA, 2007, pp. 9-14.

[3] Armin Babaei and Gregor Schiele, "Physical Unclonable Functions in the Internet of Things: State of the Art and Open Challenges", Sensors, vol.19, 3208, July 2019.

[4] T. Idriss, H. Idriss and M. Bayoumi, "A PUF-based paradigm for IoT security," 2016 IEEE 3rd World Forum on Internet of Things (WF-IoT), Reston, VA, 2016, pp. 700-705.

[5] Le Zhang et al., "Exploiting Process Variations and Programming Sensitivity of Phase Change Memory for Reconfigurable Physical Unclonable Functions" IEEE Transactions on Information Forensic and Security, vol. 9, no. 6, pp. 921-932, June 2014.

[6] S. Donati, C. Mirasso (Editors), "Feature Section on Optical Chaos and Applications to Cryptography," IEEE J. Quantum Electron. vol. 38, n. 9, pp. 1137-1196, Sep. 2002.

[7] L. Larger, J-P. Goedgebuer, (Editors), Special Number on "Criptography using Optical Chaos," Comptes Rendus de l'Academie des Sciences-Dossier de Physique, vol. 6, n. 5, May 2004.

[8] T. Yamamoto et al., "Common-chaotic-signal induced synchronization in semiconductor lasers," Opt. Exp., vol. 15, no. 7, pp. 3974–3980, July 2007.

[9] V. Annovazzi-Lodi, G. Aromataris, M. Benedetti, S. Merlo, "Private Message Transmission by Common Driving of Two Chaotic Lasers", IEEE Journal of Quantum Electronics, vol. 46, n. 2, pp. 258-264, Feb. 2010.

[10] A. Argyris et al., "Chaos-Based Communications at High Bit Rates Using Commercial Fiber-Optic Links," Nature vol. 438, pp. 343-346, Nov. 2005.

[11] D. Syvridis, A. Argiris, A. Bogris, M. Hamacher, I. Giles, "Integrated Devices for Optical Chaos Generation and Communications Applications," IEEE J. of Quantum Electron. vol. 45, n. 11, pp. 1421-1428, Nov. 2009.

[12] V. Annovazzi-Lodi, G. Aromataris, M. Benedetti, S. Merlo, "Secure data transmission on a free-space optics data link", IEEE Journal of Quantum Electronics, vol. 44, n. 11, pp. 1089-1095, Nov. 2008.

[13] V. Annovazzi-Lodi, G. Aromataris, M. Benedetti, M. Hamacher, S. Merlo, V. Vercesi, "Close-Loop Three-Laser Scheme for Chaos-Encrypted Message Transmission", Optical and Quantum Electronics, vol. 42, no. 3, pp. 143-156, Jan. 2011.

[14] L. Keuninckx et al., "Encryption Key distribution via Chaos Synchronization", Scientific reports vol. 7, 43428, Feb. 2017.

[15] A. Uchida, P. Davis, and S. Itaya, "Generation of information theoretic secure keys using a chaotic semiconductor laser," Appl. Phys. Lett. 83,,pp. 3213-3215, 2003.

[16] R. Lang and K. Kobayashi, "External Optical Feedback Effects on Semiconductor Injection Laser Properties," IEEE J. Quantum Electron. vol. 16, n. 3, pp. 347-355, March 1980.

[17] R. Ju, P. S. Spencer, and K. A. Shore, "The relative intensity noise of a semiconductor laser subject to strong coherent optical feedback," J. Opt. B, Quantum Semiclassical Opt., vol. 6, no. 8, pp. S775–S779, Aug. 2004.

[18] H. Xu, "Silicon Electro-optics modulator fabricated in standard CMOS technology as components for all silicon monolithic integrated optical systems", J. Micromechanical Eng., vol.31, paper 054001, 2021.

[19] K. Xu et al, "Light emission from a poly-silicon device with carrier injection engineering", Material Science and Engineering vol. B231, pp.28-31, 2018.

[20] E. G. Mironov et al., "Enhancing weak optical signals using a plasmonic Yagi-Uda nanoantenna array", IEEE Photonic Technology Letters, vol.26, no.22, pp.2236-2239, Nov.2014.

AUTHORS' BIOGRAPHIES

Valerio Annovazzi-Lodi (M'89-SM'99) was born in Novara, Italy, on November 7, 1955. He received the degree in Electronic Engineering from the University of Pavia, Pavia, Italy, in 1979. Since then he has been working at the Department of Electrical, Computer and Biomedical Engineering of the University of Pavia in the fields of electronics and electro-optics. His main research interests include injection phenomena and chaos in oscillators and lasers, cryptography, optical sensors, passive fiber components for telecommunications and sensing, optical amplifiers, transmission via diffused infrared radiation, micromechanical systems, human brain dynamics and language generation. In 1983 he became a Staff Researcher of the Department of Electronics (presently: Department of Electrical Computer and Biomedical Engineering) of the University of Pavia, in 1992 an Associate Professor and in 2001 a Full Professor of the same institution. He is the author of more than 100 papers and holds four patents.

Dr. Annovazzi-Lodi is a member of AEIT and a Senior Member of IEEE-Photonics Society.

Lorenzo Lombardi (M'20) was born in Tortona, Italy, in 1992. He received the Master Degree in Electronic Engineering (Track: Photonics) from University of Pavia, Pavia, Italy. He is currently pursuing the Ph.D. degree in Electronic, Computer and Electrical Engineering with the Optoelectronics Group of the Department of Electrical, Computer and Biomedical Engineering of the University of Pavia. His research interests include modelling of semiconductor lasers subject to optical injection, numerical analysis of optical chaos, and cryptographic communications systems.

Dr. Lombardi is a member of IEEE and of AEIT.

Giuseppe Aromataris was born in Siderno, Italy, in 1976. He received the degree in Physics in 2006 from the University of Milan, Italy, with a thesis on covariant quantum measurement of phase on coherent and squeezed states. He got the Ph.D. degree in Electronics Engineering from the University of Pavia, Italy, working on optical cryptography with the Optoelectronics group of the Department of Electrical, Computer and Biomedical Engineering.

His research interests include non-linear dynamics in optically injected semiconductor lasers, with regard, in particular, to numerical analysis on optical chaos synchronization and cryptographic communication systems.

Dr. Aromataris is a member of AEIT.