Network Authentication with Synchronized Chaotic Lasers

Lorenzo Lombardi
Dep. Electrical Computer Biomed. Eng.
University of Pavia
Pavia, Italy
lorenzo.lombardi@unipv.it

Valerio Annovazzi-Lodi
Dep. Electrical Computer Biomed. Eng.
University of Pavia
Pavia, Italy
valerio.annovazzi@unipv.it

Giuseppe Aromataris
Dep. Electrical Computer Biomed. Eng.
University of Pavia
Pavia, Italy
giuseppe.aromataris@unipv.it

***Abstract*—We numerically study a hardware method for network authentication, where a pair of matched (twins) chaotic lasers generate the same chaos when they synchronize, being subject to the same optical injection from a third chaotic laser. One of the lasers is in the secure environment, the other in the unsecure environment, and authorization is granted only if the two responses match. As in other PUF (Physically Unclonable Functions) related schemes, security is based on unavoidable differences between nominally identical but physically separate devices, and, more specifically, to the sensitivity of chaos to laser parameter dispersion.**

Keywords—chaos, optical feedback, network security

I. INTRODUCTION

Chaos in lasers has been studied for more than two decades for applications to secure data transmission [1,2]. Different methods have been proposed, and chaos-protected digital communication on a metropolitan network [3] has been demonstrated years ago. In a widely investigated steganographic scheme [4,5], two lasers (called 'Slaves') are driven to chaos by optical injection from a third laser (the Driver, DRV). The chaotic waveform produced by one Slave laser (SL1) is used to hide a message. The Authorized recipient, who owns a laser SL2 which is almost identical to SL1 (they are 'twins'), can recover the message by subtracting the chaos generated by his laser. For the Adversary, instead, it is very difficult to generate an identical chaotic waveform, because of the unavoidable differences between nominally identical but physically different devices.

In a previous paper [6], we have shown that the strong dependence of the chaotic waveform, from laser parameters, can be exploited to realize an authentication scheme based on twin lasers. This method belongs to the class of Challenge-Response methods based on PUF (Physically Unclonable Functions) [7,8]. In steganographic applications, two topologies have been studied in the literature [1,2]: the close loop, which offers better security, in which the isolated SL lasers are already chaotic, and the open loop, where SL1,2 are chaotic only due to injection from DRV, which is chaotic in both cases.

In [6] we have considered in detail the basic open loop case, demonstrating that it offers a good security level, while the close loop was only preliminary evaluated without sweeping parameters. In this contribution, we would like to investigate in detail the close loop, to check if the increased complexity of the scheme, with respect to the open loop, offers a better performance also when applied to authentication.

II. THE AUTHENTICATION SCHEME

The proposed authentication scheme is shown in Fig.1.

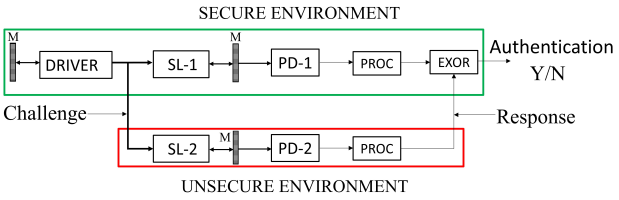

Fig.1. Authentication scheme based on chaotic lasers (M: mirrors, PD: photodiodes, PROC: electronic processing)

The driver laser DRV is routed to chaos by delayed optical feedback, provided by a mirror, and injects (the challenge) two Slave lasers SL1,2. Slave lasers also work in the chaotic regime, due to delayed optical feedback from (partial) mirrors, which were not present in the open loop. If SL1,2 have very well-matched parameters (lasers are 'twins'), in suitable operating conditions they synchronize, i.e., they produce the same chaotic amplitude modulation (the response), as shown in Fig.2.

A convenient way of comparing challenge and response is the generation of binary sequences from the chaotic waveforms by electronic processing, using e.g., Schmitt triggers with a properly selected threshold, after a low pass filter. The response in the unsecure environment, in the digital domain, is thus the bit stream produced by Slave SL2. The reference response in the secure environment is the bit stream generated by SL1. Matching of the bit sequences is then evaluated by a suitable digital comparator block (EXOR). Only if the two responses match (up to a small error bit-count, as usual with PUFs) authorization is granted.

While the Authorized user can own a SL2 laser which is twin to SL1 (for example, they can be both selected from the same wafer), getting a matched laser is a very difficult task for the Adversary (Fig.3). Moreover, the Authorized user can train his system by optimizing pump current and optical injection (the 'external parameters') to minimize errors, before using it in the field. This is not possible for the Adversary, who can only sweep these parameters, and try many different lasers and working points.

A specific advantage of the proposed scheme is that the responses need not to be stored, not even in the secure environment, but they are produced on the fly, which improves security. Moreover, the challenge changes at each attempt.

978-1-6654-7899-1/22/$31.00 ©2022 IEEE

In our previous paper [6], the proposed authentication method was evaluated for the open loop by the Lang-Kobayashi (L-K) numerical model [5,9]. In this contribution, we investigate the close loop, adding to the model two more parameters, i.e., for each SL, the mirror reflectivity and the flight time to its mirror. For the Authorized user we have assumed a 2% parameter mismatch, in the L-K model, of SL2 respect to SL1, and 3-10% for the Adversary. For both, we compute the number of errors on a 128-bit sequence. As anticipated, for the Authorized user external parameters have been optimized, while for the Adversary they are only swept.

First, simulations were performed for the Authorized user, getting the results of Table 1. For the Adversary, since each single percentage of mismatch would result into more than 56 million combinations (which requires a long machine time), we started from the results obtained with constant nominal values for the two new parameters. From them, we have selected the combinations giving the least number of errors, and only for these lasers we have swept the two new parameters, for approximately 7 million combinations. In this way, we have been able to get results for a mismatch of 4%, 5% (Table1) and 7% in a relatively short time. Simulations up to 10% are in progress.

The threshold error number to be tolerated (9) has been selected to have a 100% authentication rate for the Authorized user, with a 2-error margin over the minimum of 7 in Table1. In Table 2, the performance of the authentication system is shown for different percentages of mismatch. The results for the open loop are also reported [6] in Tables 1, 2, for comparison.

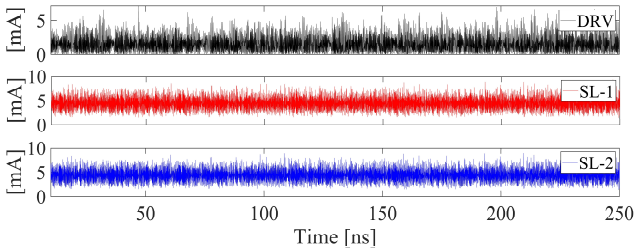

Fig.2. Chaotic waveforms for DRV, and twins SL1 and SL2 (close loop)

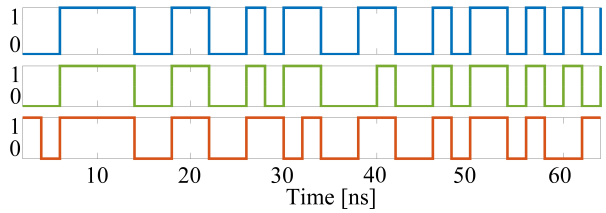

Fig.3. Typical bit sequences from SL1 (Reference), SL2 (Authorized user), and SL2 (Adversary) in the close loop scheme

Data in Table 2 demonstrate the good performance of the proposed authentication method, with both open and close loop, since the success rate for the Adversary is never larger than 0.0052%. Also, the close loop operates much better than the open loop, and thus it represents a convenient solution, in spite of its more complex setup.

Experimental evaluation of the authentication scheme will be the next step. It will take advantage of the already performed experiments on chaos-secured transmission [1,2,5], and on the possible implementation in integrated optics, already employed for chaos transmission [10].

	Open Loop		Close Loop	
	Auth	Adv	Auth	Adv
Max	4	91	7	85
Min	0	0	1	2
Med	2	60	5	50

Table 1. Error number on a 128-bit sequence for Authorized user (2% mismatch) and for Adversary (5% mismatch) with open and close loop.

% Mismatch	Open Loop		Close Loop	
	Auth	Adv	Auth	Adv
2	100%	-	100%	-
4	-	0.0052%	-	0.00053%
5	-	0.0036%	-	0.00056%
7	-	0.0044%	-	0.00090%

Table 2. Authentication success rate for the open and for the close loop, for Authorized user (2% mismatch) and for Adversary (4, 5, 7%)

III. Conclusions

We have analyzed a new authentication method based on chaotic lasers, finding that it performs well in two proposed versions, and that the close loop, where the lasers are intrinsically chaotic, performs far better than the previously investigated open loop.

References

[1] 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.

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

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

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

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

[6] V. Annovazzi-Lodi, L. Lombardi, G. Aromataris, "Challenge-Response Authentication Scheme with Chaotic Lasers", *IEEE J. Quantum Electron.,* vol. 58, n. 1, paper 2000107, Feb. 2022.

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

[8] A. Babaei, G. Schiele, "Physical Unclonable Functions in the Internet of Things: State of the Art and Open Challenges", *Sensors*, vol.19, paper 3208, July 2019.

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

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