IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Date of publication xxxx 00, 0000, date of current version xxxx 00, 0000.

Digital Object Identifier

Noise Level Modulation for Secure Optical Communications

STEFANO CAPUTO[1], SILVIA VICIANI[2], STEFANO GHERARDINI[2], GIACOMO BORGHINI[1], FRANCESCO CATALIOTTI[2], and LORENZO MUCCHI[1,2] (Senior Member, IEEE)

[1]Dept. of Information Engineering, University of Florence, via di S. Marta 3, 50139, Firenze, Italy (e-mail: name.surname@unifi.it)
[2]National Institute of Optics of CNR (CNR-INO), Italy (e-mail: name.surname@ino.it)

Corresponding author: Lorenzo Mucchi (e-mail: lorenzo.mucchi@unifi.it).

This work was partially supported by the European Union under the Italian National Recovery and Resilience Plan (NRRP) of NextGenerationEU, partnership on "Telecommunications of the Future" (PE00000001 - program "RESTART").

ABSTRACT Noise Level Modulation (NLM) is a robust physical-layer security technique which uses the injection of random phase noise into the transmitted signal to provide confidentiality in optical networks. The legitimate receiver can seamlessly recover the information by utilizing a feedback loop, while eavesdropping attempts fail, irrespective of the attacker's location or computational capabilities.
This paper outlines the theoretical and implementation principles of NLM when applied to full fiber-optic networks. Our findings reveal that NLM can attain a complete secrecy rate while ensuring compatibility with existing optical devices and protocols. We also propose a practical fiber optic-based implementation scheme, providing a thorough analysis of its variations from the theoretical framework. Furthermore, we delve into the challenges associated with NLM in the context of secure full optical communication systems and explore potential future directions.

INDEX TERMS Optical communications, physical layer security, noise injection, noise modulation, information theoretical security.

I. INTRODUCTION

Optical communication stands as a cornerstone of modern society, underpinning the high-speed, high-capacity, and cost-effective transmission of information across vast distances [1]. Utilizing light waves as carriers, optical communication systems bridge transmitters and receivers through a variety of channels, including optical fibers, free space, and atmospheric media. This mode of communication boasts several advantages over its radio frequency and electrical signal counterparts, offering higher bandwidth, lower attenuation, reduced interference, minimal power consumption, and enhanced security. The widespread adoption of optical communication spans a multitude of applications, encompassing telecommunications, the internet, data centers, broadcasting, sensing, imaging, and even the realm of quantum information. As a pivotal force behind the evolution of cutting-edge technologies like artificial intelligence, big data, cloud computing, and 5G networks, optical communication is a dynamic field ripe with research and innovation opportunities. Its continued development promises not only to propel scientific and technological progress but also to elevate the quality of human life.

In the intricate web of global communications, fiber optical networks are the lifelines that transmit vast amounts of data with astonishing speed and fidelity. The integrity of these networks is not just a technical requirement but a critical safeguard for the functioning of modern society. In the context of optical communication, security thus emerges as a paramount concern, safeguarding the confidentiality, integrity, and availability of information coursing through optical channels [2]. The systems are susceptible to a spectrum of attacks, ranging from fiber cutting and tapping to jamming, eavesdropping, and spoofing. Such malicious activities pose threats to data privacy, signal quality, and the seamless operation of networks [3]. To counter these vulnerabilities, the development of robust detection and prevention methodologies is critical. Enhancing the resilience and robustness of optical communication systems is not merely a technical challenge but a necessity for maintaining the trust and reliability that society places in these networks. As we delve deeper into the digital age, ensuring the security of optical communication infrastructures becomes an imperative that parallels their technological advancement.

In the realm of communication security, physical layer

security emerges as a critical shield against a myriad of threats [4]. This security layer is fundamental in safeguarding the integrity and confidentiality of data as it traverses the physical medium of fiber optics. Unlike higher-level encryption methods that protect data at the software level, physical layer security is ingrained in the hardware itself, offering a first line of defense that is both robust and inherently difficult to breach. Techniques such as optical encryption and quantum key distribution are employed to ensure that any attempt to intercept or tamper with the data can be instantly detected and mitigated. By leveraging the unique properties of light and the laws of quantum mechanics, physical layer security provides a level of protection that is not only resilient to conventional hacking strategies but also prepared for the future challenges posed by quantum computing [5]. As optical networks continue to expand their role in the global communication infrastructure, the implementation of physical layer security becomes indispensable, acting as the guardian of our digital conversations [6].

A. RELATED WORKS

Classical security approaches in optical communications are based on mathematical algorithms that encrypt and decrypt the data transmitted over optical channels. These approaches rely on the assumption that the computational complexity of breaking the encryption is too high for any attacker to achieve. However, these approaches are vulnerable to quantum attacks, which exploit the quantum properties of light to break the encryption schemes. Therefore, there is a need for new encryption techniques that are based on physical principles and that can resist quantum attacks. Some examples of these techniques are quantum key distribution (QKD) and physical layer encryption (PLE).

Physical-layer security (PLS) is a security approach which is essentially proposed in wireless optical channels, and not very frequently in fiber optics [7]. The authors in [8] investigate the tradeoff between information rates and confidentiality (secrecy capacity) in optical fibers, considering different channel dynamics.

PLS exploits any kind of randomness sources in the telecommunication system to produce a random decision variable for the eavesdropper, with the effect that the attacker cannot demodulate any symbol correctly [9]. Although in radio frequency (RF) communications, the noise (intrinsic in the equipment or in the channel or artificially generated) is often used to produce confidentiality, in optical fibers this method is not fully explored.

In the following a review of papers in literature that propose a security mechanism for fiber optics communications, using any kind of noise sources is reported. The paper [10] introduces a novel data encryption method in the physical layer using a broadband optical noise-like signal shared between Alice and Bob. This signal is employed to create a secret key for secure information transmission via the one-time-pad technique. The paper evaluates the scheme's features and assesses its compatibility with current fiber-optic communication infrastructure.

In [11], a novel scheme combining chaotic encryption and noise masking key-accompanying transmission is proposed to achieve high security and capacity over seven-core fiber. It uses a dual-polarization IQ modulator to generate a 3D-OFDM signal, encrypted by a chaotic signal and masked by a noise signal, which also carries the key information extracted at the receiver using a correlation algorithm. The authors in [12] investigate an optical chaotic-based secure fiber-optic communication system using an externally modulated laser to generate a chaotic optical signal that hides the data signal. The study in [13] focuses on secure communication in modern fiber optic networks, specifically with a multi-mode fiber (MMF) channel and a potential eavesdropper, leveraging artificial noise (AN) and statistical knowledge of the eavesdropper's channel to maximize the average secrecy rate. An overview of physical-layer attacks in optical networks can be found in [14], and the fundamentals of PLS in optical wireless networks are discussed in [15], [16].

As mentioned before, current security approaches for optical communications are based on mathematical algorithms that assume the computational complexity of breaking the encryption is too high for any attacker to achieve. However, this assumption may not hold in the future, as quantum computers could potentially break these algorithms in polynomial time using Shor's algorithm [17]. Other approaches rely on the secure distribution and management of keys, which can be challenging and costly in large-scale networks [18]. Moreover, the keys can be compromised by various attacks, such as eavesdropping, interception, or tampering. In addition, these methods introduce overhead and latency in the encryption and decryption processes, which can affect the performance and efficiency of the optical communication systems.

B. OUR CONTRIBUTION

Noise level modulation (NLM) is a PLS technique that intrinsically provides confidentiality by modulating the information with noise [19]. The noise used in the NLM system is the one generated by the equipment (transmitter/receiver). As a PLS technique, the NLM approach aims to avoid the demodulation of the physical signal instead of relying on an encryption algorithm whose breaking time is dependent on the computational power of the attacker. The benefits of this technique can be summarized as follows:

- The proposed technique does not require any prior secret key exchange or key management between the sender and the receiver, as the noise is generated randomly and locally at the transmitter. Therefore, it simplifies the security protocol and reduces the cost and complexity of key distribution.
- The proposed technique does not suffer from physical attacks, such as fiber cutting, tapping, or jamming, as the noise masks the information and makes it indistinguishable from the background noise. Therefore, it enhances

the resilience and robustness of the communication system.

Although the concept behind NLM is known [20], there is no paper in literature that tries to apply it to a full optical communication system. In this paper we aim to give the theoretical foundation of full optical noise level modulation, showing the reliability and the security of such a system. Theoretical analysis is reported for both the decision variable of the legitimate receiver and the demodulation attempts of the eavesdropper. The results show how the optical NLM is able to guarantee full secrecy rate, while still assuring the correct demodulation of the transmitted symbol to the legitimate receiver.

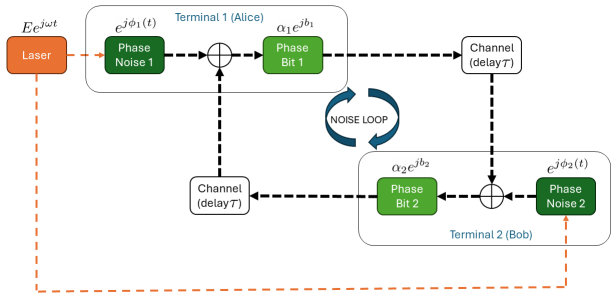
Although the NLM technique has been already studied in the RF domain [21], no attempts are present in literature to adapt it to fiber optical channels. In particular, the challenge is to change the entire NLM system, moving from an additive white Gaussian noise as in RF to a phase noise as in fiber optics. In addition, this paper aims to give an insight on the equipment, materials and scheme to realize the NLM in optical fiber networks, whose implementation is not straightforward for the reasons detailed below.

The development of quantum computing and quantum cryptography pose a threat to the conventional encryption algorithms based on mathematical complexity. Despite QKD can be seen as a solution to provide knowledge of ongoing passive attack in a legitimate link, it does not face consequent denial of service (DoS). These impacts can motivate the research and innovation of optical NLM as a promising security technique that can provide secure optical communication, beyond encryption. Optical NLM can also complement or integrate with other security techniques, such as physical layer encryption, to achieve optimal security and performance.

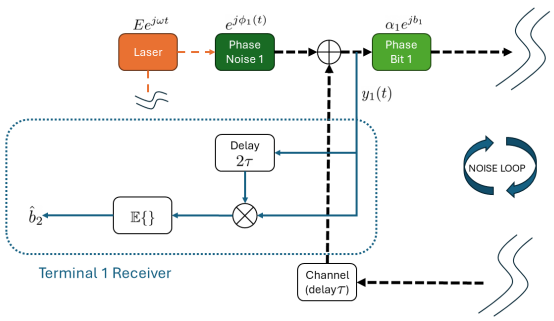
The remaining sections are organized as follows. Section II describes the system model and gives the fundamentals equations of the full optical NLM system. Section III reports the reliability analysis for the legitimate terminals, while Section IV provides the information-theoretical security analysis. Section V describes a potential hardware experimental solution for the NLM scheme and discusses the correspodning challenges. Section VI shows the numerical results, and Section VII concludes the manuscript.

II. SYSTEM MODEL

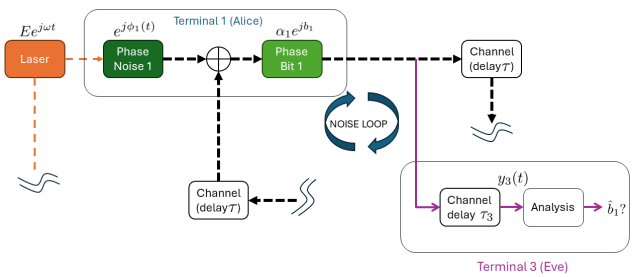
The optical noise level modulation scheme is depicted in Fig. 1a, while the legitimate receiver scheme is reported in Fig. 1b and the eavesdropper receiver scheme is in Fig. 1c. The laser source (the orange block in Fig. 1a) produces the optical signal which undergoes a phase shift (the dark green block). This signal is then added to the incoming signal from the optical channel transmitted by the other terminal). Subsequently the signal is modulated with the information bit of the terminal (the light green box) and then transmitted over the fiber optic to the other terminal. As it can be seen from Fig. 1a, the two legitimate terminals (Terminal 1 is



(a) Optical noise level modulation scheme.



(b) Receiver scheme for Terminal 1.



(c) Receiver scheme of the eavesdropper (Eve). Eve is attempting to demodulate the bit transmitted from Alice to Bob. The parameter τ_3 denotes the delay between Alice and Eve.

FIGURE 1: Noise level modulation scheme: (a) general scheme; (b) receiver scheme for the legitimate Terminal 1; (c) receiver scheme for the eavesdropper Terminal 3 (Eve).

ALICE and Terminal 2 is BOB) exchange their bits at the same time over the fiber optic. Each bit, together with the received signal, is modulated by a phase noise generator before transmission. This mechanism draws a loop, where the two information bits are merged together and modulated by the two independent phase noises. It is important to note that both legitimate terminals are transmitting (Tx) and receiving (Rx) at the same time. For the sake of simplicity, we can denote the Terminal 1 as Alice and the Terminal 2 as Bob, but both of them can be either the Tx or the Rx.

Following the main scheme in Fig. 1a, let us assume that the laser amplitude is constant, i.e., $E(t) = E$ and that the laser frequency is constant, i.e, $\omega(t) = \omega$. Moreover, let us assume that the constant phase of the laser source is negligi-

ble. Then, we define the signal transmitted by Terminal 1 and 2 (Alice and Bob), initially without closing the loop, as:

$$x_1(t) = \alpha_1 E e^{j\omega t} e^{j\phi_1(t)} e^{jb_1} \quad (1)$$

$$x_2(t) = \alpha_2 E e^{j\omega t} e^{j\phi_2(t)} e^{jb_2} \quad (2)$$

where E is the electric filed intensity of the laser source, b_1 and b_2 are the information bits (taking the values 0, π) exchanged by the two legitimate terminals, and $\phi_1(t)$ and $\phi_2(t)$ are the noise processes introduced by the phase modulators in Fig. 1a. The phase noise from both the laser and the fiber, which includes fluctuations in the optical phase due to the laser's output and the fiber's transmission, is assumed to be included in the phase noise $\phi_1(t)$ and $\phi_2(t)$ of the NLM loop scheme. The parameters α_1 and α_2 attenuate the signal and they will play the role of loop stability controllers that can be implemented by using a splitter or a dissipating mirror.

Now, let us close the loop between Terminals 1 and 2. The signal received by Terminal 1 can be written as

$$r_1(t) = \alpha_2 e^{jb_2} \left[r_2(t-\tau) + E e^{j\omega(t-\tau)} e^{j\phi_2(t-\tau)} \right] \quad (3)$$

where $r_2(t-\tau)$ denotes the signal received by Terminal 2, delayed by the time τ that is proportional to the physical distance from Bob to Alice (and vice versa in our setting). In addition, for Terminal 1, the decision variable is

$$y_1(t) = r_1(t) + E e^{j\omega t} e^{j\phi_1(t)} . \quad (4)$$

After some calculations, and after one complete loop ($L = 1$), we have

$$y_1(t) = \alpha_1\alpha_2 e^{jb_1} e^{jb_2} E e^{j\omega(t-2\tau)} e^{j\phi_1(t-2\tau)} + \alpha_2 e^{jb_2} E e^{j\omega(t-\tau)} e^{j\phi_2(t-\tau)} + E e^{j\omega t} e^{j\phi_1(t)} . \quad (5)$$

Hence, if the following assumptions hold

$$\mathbb{E}\{e^{j\phi_1(t)} e^{j\phi_2(t)}\} = 0 \quad (6)$$

$$\mathbb{E}\{e^{j\phi_1(t)} e^{j\phi_1(t-\tau)}\} = \delta(\tau) , \quad (7)$$

then the autocorrelation $R_{y_1y_1}(2\tau) \equiv \mathbb{E}\{y_1^*(t) y_1(t-2\tau)\}$ in the single loop becomes

$$R_{y_1y_1}(2\tau) = \alpha_1\alpha_2 e^{jb_1} e^{jb_2} E^2 . \quad (8)$$

Taking the real part

$$\mathtt{Re}\{R_{y_1y_1}(2\tau)\} \sim \alpha_1\alpha_2 E^2 \cos(b_1 + b_2); \quad (9)$$

thus, since Terminal 1 knows b_1, it can easily estimate the angle b_2 in the range $[0, \pi]$, i.e.,

$$\hat{b}_2 = \arccos\left(\mathrm{sgn}\left(\mathtt{Re}\{e^{-jb_1} R_{y_1y_1}(2\tau)\}\right)\right) . \quad (10)$$

After L loops, adopting a more comfortable notation, we have

$$y_1(t) = \sum_{\ell=1}^{L-1} (\beta_1\beta_2)^\ell n_1(t - 2\ell\tau) + \sum_{\ell=1}^{L-1} (\beta_1\beta_2)^{\ell-1} \beta_2\, n_2(t - (2\ell-1)\tau) + n_1(t) \quad (11)$$

where $\beta_i \equiv \alpha_i e^{jb_i}$ and $n_i(t) \equiv E e^{j\omega t} e^{j\phi_i(t)}$ with $i = 1, 2$.

III. RELIABILITY ANALYSIS

Let us assume, without loss of generality, that the Terminal 1 is trying to recover the bit b_2 sent by the Terminal 2.

In order to demonstrate the reliability capability of the system after L loop, it is better to write $y_1(t)$ as an autoregressive signal:

$$y_1(t) = \alpha_1\alpha_2 e^{jb_1} e^{jb_2} y_1(t-2\tau) + \alpha_2 e^{jb_2} E e^{j\omega(t-\tau)} e^{j\phi_2(t-\tau)} + E e^{j\omega t} e^{j\phi_1(t)} . \quad (12)$$

One thus gets

$$R_{y_1y_1}(2\tau) = \mathbb{E}\{y_1^*(t) y_1(t-2\tau)\} = \alpha_1\alpha_2 e^{jb_1} e^{jb_2} \sigma_{y_1}^2(t) \quad (13)$$

where also $\sigma_{y_1}^2(t) \equiv \mathbb{E}\{y_1^*(t) y_1(t)\}$ obeys an autoregressive equation of order 1, i.e.,

$$\sigma_{y_1}^2(t) = E^2 + \alpha_2^2 E^2 + \alpha_1^2\alpha_2^2 \sigma_{y_1}^2(t-2\tau) \quad (14)$$

under the assumptions (6) and (7). Thus, by introducing $E^2 + \alpha_2^2 E^2 \equiv \lambda$ and $\alpha_1^2\alpha_2^2 \equiv \mu$, one obtains

$$\sigma_{y_1}^2(2L\tau) = \lambda\left(1 + \mu + \ldots + \mu^L\right) = \lambda \sum_{k=0}^{L} \mu^k . \quad (15)$$

The geometric series $\sum_{k=0}^{L} \mu^k$ is convergent for $|\mu| < 1$ and equal to

$$\sum_{k=0}^{L} \mu^k = \frac{1 - \mu^{L+1}}{1 - \mu} .$$

Accordingly, one finally has that

$$\sigma_{y_1}^2(t) = \frac{(E^2 + \alpha_2^2 E^2)\left(1 - (\alpha_1\alpha_2)^{2(L+1)}\right)}{1 - \alpha_1^2\alpha_2^2} \quad (16)$$

with $|\alpha_1^2\alpha_2^2| < 1$ for convergence purposes. One can thus observe that for L (number of loops) large, the value of $\sigma_{y_1}^2(t)$ converges to the stationary value

$$\sigma_{y_1}^2(\infty) = \frac{E^2(1 + \alpha_2^2)}{1 - \alpha_1^2\alpha_2^2} . \quad (17)$$

From (13), since Terminal 1 knows b_1, we can estimate the angle b_2 using (10) as in the $L = 1$ case. This demonstrate that Terminal 1 (Alice) is able to demodulate correctly the information bit sent by Terminal 2 (Bob), also in the generic case of L sufficiently large.

The numerical results on the reliability performance of the proposed system are shown in Sec. VI.

IV. SECURITY ANALYSIS

In this section we aim to demonstrate that the information leakage to the eavesdropper is negligible, i.e., the amount of information that the eavesdropper is able to extract from its received signal is zero. We distinguish two cases: 1) Eve overhears the channel between Alice and Bob when the loop is already on (steady-state analysis); 2) Eve overhears the channel from the very first round of the loop (transitory-state analysis). We assume a single eavesdropper scenario and we assume that Eve knows how the NLM works.

A. CASE 1: EVE OVERHEARS THE CHANNEL BETWEEN ALICE AND BOB (STEADY-STATE ANALYSIS)

Let us assume, without loss of generality, that Eve is overhearing the channel between the Terminal 1 (Alice) and the Terminal 2 (Bob), as in Fig. 1c.

Since both Alice and Bob decode information by performing the autocorrelation of the received signal, here we assume that also Eve opts to compute the autocorrelation of the signal taken from channel. The received signal for Eve (the third unwanted terminal) would be

$$y_3(t) = \alpha_1 e^{jb_1} y_1(t-\tau_3) \tag{18}$$

which can also be written as an autoregressive signal

$$\begin{aligned} y_3(t) \quad &= \alpha_1 e^{jb_1} e^{j\phi_1(t-\tau_3)} E e^{j\omega(t-\tau_3)} \\ &+\alpha_1\alpha_2 e^{jb_1} e^{jb_2} e^{j\phi_2(t-\tau-\tau_3)} E e^{j\omega(t-\tau-\tau_3)} \\ &+\alpha_1\alpha_2 e^{jb_1} e^{jb_2} y_3(t-2\tau) \end{aligned} \tag{19}$$

under the hypothesis that Eve's receiver has no noise and that, without loss of generality, Eve is listening at the channel from Alice to Bob. The parameter τ_3 indicates the propagation delay between Alice and Eve, and thus denotes the asynchrony between the time when Alice sends information to Bob and the time when Eve takes $y_3(t)$.

The best that Eve can do is to extract the autocorrelation of the received signal. First of all, Eve has to try to get the autocorrelation peak, which is unknown. In such a case,

$$\begin{aligned} R_{y_3y_3}(\tau+\tau_3) = \mathbb{E}\{y_3(t)y_3^*(t-\hat{\tau})\} = 0, \\ \forall \hat{\tau} \neq 2k\tau \ \text{ with } \ k = 1, 2, \cdots \end{aligned} \tag{20}$$

However, if Eve is able to estimate exactly the propagation delay τ between Alice and Bob, thus by setting $\hat{\tau} = 2\tau$, then the autocorrelation that Eve can extract for L large is

$$\begin{aligned} R_{y_3y_3}(2\tau) &= \mathbb{E}\{y_3(t)y_3^*(t-2\tau)\} \\ &= \alpha_1\alpha_2 e^{jb_1} e^{jb_2} \sigma^2_{y_3} = \alpha_1^3\alpha_2 e^{jb_1} e^{jb_2} \sigma^2_{y_1}(\infty)\,. \end{aligned} \tag{21}$$

Even in this worst case, the output is proportional to the XOR of the bits, thus it is not possible to come up with the value of each specific bit, without knowing one of them.

In order to try different strategies, Eve could decide to participate to the loop by injecting its own phase noise. Thus, if Eve injects the noise $n_3(t) = E_3 e^{j\omega_3 t} e^{j\phi_3(t)}$, its received signal becomes

$$\begin{aligned} y_3(t) \quad &= \alpha_1 e^{jb_1} e^{j\phi_1(t-\tau_3)} E e^{j\omega(t-\tau_3)} \\ &+\alpha_1\alpha_2 e^{jb_1} e^{jb_2} e^{j\phi_2(t-\tau-\tau_3)} E e^{j\omega(t-\tau-\tau_3)} \\ &+\alpha_1\alpha_2 e^{jb_1} e^{jb_2} y_3(t-2\tau) + \underbrace{E_3 e^{j\omega_3 t} e^{j\phi_3(t)}}_{n_3(t)}. \end{aligned} \tag{22}$$

Since the noise process $\phi_3(t)$ is uncorrelated[1] to those injected by Alice $\phi_1(t)$ and Bob $\phi_2(t)$, Eve would not have any additional benefit, thus meaning that (21) holds. In addition, if Eve injects noise, it performs basically an active attack and the legitimate nodes could detect the presence of an attacker.

[1]The noises $\phi_1(t)$ and $\phi_2(t)$ are random stochastic processes that cannot be replicated by an adversary.

1) Information leakage to the eavesdropper

Let us now assume, without loss of generality, that Eve is eavesdropping the channel between Alice and Bob, aiming to recover the information of the bit b_1 sent by Alice to Bob. The amount of information on the bit b_1, which the eavesdropper can get by analysing the observed signal, is given by the mutual information

$$I(b_1; y_3) = H(y_3) - H(y_3|b_1) \tag{23}$$

that is also known as the information leakage to the eavesdropper. In Eq. (23), $H(\cdot)$ is the Shannon entropy and $H(\cdot|\cdot)$ denotes the corresponding conditional entropy [22]. In order to calculate the mutual information $I(b_1; y_3)$, we need to detail the random variable (RV) $y_3(t)$ in (19) for any time t. Apart from multiplying factors, the first term in the right-hand-side of (19) is a RV composed by the product of the exponential of a discrete-time complex Bernoulli RV e^{jb_1} and a continuous-time complex standard Cauchy RV $e^{j\phi_1}$ obeying Eqs. (6) and (7). In fact, if we assume that ϕ_1 is a uniform RV in $[-\pi, \pi]$, then $\xi = e^{j\phi_1}$ has probability density function (PDF) equal to $f_\Xi(\xi) = \frac{1}{\pi(1+\xi^2)}$, i.e., ξ is a standard Cauchy RV.

The eavesdropper sees b_1 as a Bernoulli RV $\mathrm{Ber}(0.5)$ with probability 0.5, since the bit b_1 can assume values $0, \pi$ with equal probability 0.5. Since b_1 is a $\mathrm{Ber}(0.5)$ RV, its exponential is still a $\mathrm{Ber}(0.5)$ RV.

To calculate the PDF of a product between a $\mathrm{Ber}(0.5)$ (e^{jb_1}) and a standard Cauchy RV ($e^{j\phi_1}$), we can use the Lemma 1 and Theorem 1 reported in the appendix (Sec. VII).

Similar considerations can be made for the second term in the right-hand-side of (19). Moreover, in order to compute the mutual information on the bit b_1 obtained by Eve (always under the hypothesis of large L), we need to derive also the distribution of a $\mathrm{Ber}(0.5)$ RV multiplied by a Gaussian RV $\mathcal{N}(0, \sigma)$ with zero mean and variance σ^2, which refers to the last term in the right-hand-side of (19). The PDF of the product between the RVs $\mathrm{Ber}(0.5)$ and $\mathcal{N}(0, \sigma)$ is provided by the Theorem 2 in the appendix (Sec. VII).

Using these results we can calculate Eve's mutual information (23). Given that the Shannon entropy of a Gaussian RV $\mathcal{N}(0, \sigma)$ is $\log(2\pi e\sigma^2)$ [23] and the Shannon entropy of a Cauchy RV with unitary scale parameter is $\log(4\pi)$ [24], the first term in the right-hand-side of (23) can be written as

$$\begin{aligned} H(y_3) &= H(e^{jb_1}e^{j\phi_1}) + H(e^{jb_1}e^{jb_2}e^{j\phi_2}) + H(e^{jb_1}e^{jb_2}y_3) \\ &= \log(4\pi) + \log(4\pi) + \log\left(2\pi e\sigma^2_{y_3}\right), \end{aligned} \tag{24}$$

while the second term of (23) is

$$\begin{aligned} &H(y_3|b_1) = \\ &H(e^{jb_1}e^{j\phi_1}|b_1) + H(e^{jb_1}e^{jb_2}e^{j\phi_2}|b_1) + H(e^{jb_1}e^{jb_2}y_3|b_1) \\ &\quad = H(e^{j\phi_1}) + H(e^{jb_2}e^{j\phi_2}) + H(e^{jb_2}y_3) \\ &\quad = \log(4\pi) + \log(4\pi) + \log\left(2\pi e\sigma^2_{y_3}\right). \end{aligned} \tag{25}$$

Thus, Eq. (23) simplifies as

$$I(b_1;y_3) = 2\log(4\pi) + \log\left(2\pi e\sigma_{y_3}^2\right) - 2\log(4\pi) - \log\left(2\pi e\sigma_{y_3}^2\right) = 0\,. \quad (26)$$

This demonstrate that the mutual information $I(b_1;y_3)$ is zero for the eavesdropper, i.e., Eve cannot recover any information about the legitimate bit from the signal, no matter the computational power owned by the eavesdropper. This result also highlights that the proposed system provides a full secrecy rate, i.e., each transmitted bit is a secure bit. It is important to note that the entropy of the RV in (19) is given by the sum of three entropies as in (24), since the three terms inside (19) are independent RVs [23]. The three RVs are independent if we assume (6) and (7).

B. CASE 2: EVE OVERHEARS THE CHANNEL FROM THE VERY FIRST ROUND (TRANSITORY-STATE ANALYSIS)

In the previous section we have demonstrated that when the NLM is running (the signals are both looping from Alice to Bob and viceversa), there is no information leakage to Eve. In this section we investigate what happens if Eve is overhearing the channel from the very beginning, i.e., when the loop just starts ($L = 0$). If the eavesdropper is overhearing the NLM channel from the very beginning of the transmission, it is able to get also the first sending from Terminal 1 to 2, where only one bit b_1 is modulated. Hence, similar to before, let us assume (without loss of generality) that Eve is overhearing the channel from Alice to Bob from the first instant of the transmission.

In this case the signal observed by Terminal 3 (Eve) is

$$y_3^{[L=0]}(t) = \alpha_1 e^{jb_1} e^{j\phi_1(t-\tau_3)} E e^{j\omega(t-\tau_3)} \quad (27)$$

where τ_3 is the propagation delay of the eavesdropping channel from Terminal 1 (Alice) to Terminal 3 (Eve). As it can be seen, (27) depends only on one bit b_1, thus Eve could analyze this signal to extract the information sent by Terminal 1 (Alice) to Terminal 2 (Bob). In order to see if Eve can extract information from that signal, we derive the mutual information.

The mutual information of b_1 and y_3 can be calculated as

$$\begin{aligned} I(b_1;y_3^{[L=0]}) &= H(y_3^{[L=0]}) - H(y_3^{[L=0]}|b_1) \\ &= H\left(e^{jb_1}e^{j\phi_1(t-\tau_3)}\right) - H\left(e^{j\phi_1(t-\tau_3)}\right) \\ &= \log(4\pi) - \log(4\pi) = 0\,, \end{aligned} \quad (28)$$

i.e., the leakage of information to the eavesdropper is zero. Eq. (28) can be derived by using Theorem 1 as well as by observing Eqs. (24) and (25).

Additional possibilities for the eavesdropper to try to detect the information bits could be to correlate the start signal (27) with the steady-state signal (e.g., after one loop) (19). It is easy to show that under the assumptions (6) and (7) we have

$$\mathbb{E}\{y_3^{[L=0]}(t)y_3^*(t)\} = \alpha_1^2 E^2 \quad (29)$$

Let's assume without loss of generality that Eve tries to correlate the very first signal coming from Alice to Bob ($L = 0$) with the signal in the same channel once a complete loop is ended ($L = 1$). Then, Since $\alpha_1^2 E^2$ does not depend on the bits, Eve cannot recover any information.

V. HARDWARE IMPLEMENTATION

In this section, we propose an experimentally realizable optical setup, based on polarization-maintaining fiber components at telecom wavelength (1550 nm), for the demonstration of the basic mechanisms underlying the NLM technique described in the previous sections. The hardware implementation scheme is shown in Fig. 2.

The light source used to carry the information is a single frequency diode laser, emitting at 1550 nm, thermally stabilized and controlled by a low-noise current driver, to provide a laser field with constant amplitude and frequency. The source is equipped with an optical isolator to reduce the feedback noise. The optical signal is injected, by means of a 1×2 fiber coupler, into two terminals (Alice and Bob) that can be used both as transmitters and receivers. Before starting the communication loop, a phase noise ϕ is introduced in both terminals. The phase noise is inserted into the fiber network by using 2 fiber-coupled phase modulators (MOD1 for Alice and MOD3 for Bob) driven by a random signal. The loop is realized by two 2×2 fiber couplers, with 50:50 coupling ratio, which combine the signal coming from Alice with the signal coming from Bob. The contribution of phase noise due to both the laser and the fiber is included in the phase noise intentionally inserted into the loop.

Alice and Bob encode two different information bits (b_1 and b_2 respectively) in the optical signal by changing its phase through two additional fiber-coupled phase modulators (MOD2 for Alice and MOD4 for Bob). Specifically, a binary 0 is represented by a phase shift of π degrees, while a binary 1 is represented by no phase shift.

In Fig. 2, the detection of the received message is shown only for the Alice terminal. A 2×2 fiber coupler, with 99:1 coupling ratio, is inserted inside the loop to collect a small portion of the signal and to send it to a phase-sensitive detection scheme that allows the measurement of the optical autocorrelation function. The autocorrelator setup is a Michelson interferometer, realized with two 2×2 fiber couplers with 50:50 coupling ratio, and a moving stage equipped with a corner cube mirror to introduce a variable path difference between the two interferometric arms. The received message b_2 is extrapolated by the measured autocorrelation when the time difference between the two interferometric paths is equal at 2τ.

The eavesdropping is simulated by the terminal Eve, where a phase-sensitive detection scheme (equal to the autocorrelator used by Alice) is employed to eavesdrop the signal transmitted by Alice and Bob.

A. IMPLEMENTATION SCHEME: RELIABILITY ANALYSIS

$$
\begin{aligned}
&\mathbb{E}\left\{y_3^{[L=0]}(t-\tau_3)y_3^{*[L=1]}(t-2\tau-\tau_3)\right\} = \mathbb{E}\Big\{\left[\alpha_1 e^{jb_1}e^{j\phi_1(t-\tau_3)}Ee^{j\omega(t-\tau_3)}\right]\\
&\cdot\ \left[\alpha_1 e^{jb_1}e^{j\phi_1(t-\tau_3)}Ee^{j\omega(t-\tau_3)} + \alpha_1\alpha_2 e^{jb_1}e^{jb_2}e^{j\phi_2(t-\tau-\tau_3)}Ee^{j\omega(t-\tau-\tau_3)} + \alpha_1^2\alpha_2 e^{jb_2}e^{j\phi_1(t-2\tau-\tau_3)}Ee^{j\omega(t-2\tau-\tau_3)}\right]^*\Big\}\\
&= \underbrace{\mathbb{E}\Big\{\left[\alpha_1 e^{jb_1}e^{j\phi_1(t-\tau_3)}Ee^{j\omega(t-\tau_3)}\right]\cdot\left[\alpha_1 e^{jb_1}e^{j\phi_1(t-\tau_3)}Ee^{j\omega(t-\tau_3)}\right]^*\Big\}}_{=\alpha_1^2E^2}\\
&+ \underbrace{\mathbb{E}\Big\{\left[\alpha_1 e^{jb_1}e^{j\phi_1(t-\tau_3)}Ee^{j\omega(t-\tau_3)}\right]\cdot\left[\alpha_1\alpha_2 e^{jb_1}e^{jb_2}e^{j\phi_2(t-\tau-\tau_3)}Ee^{j\omega(t-\tau-\tau_3)}\right]^*\Big\}}_{=0 \text{ since } (6)}\\
&+ \underbrace{\mathbb{E}\Big\{\left[\alpha_1 e^{jb_1}e^{j\phi_1(t-\tau_3)}Ee^{j\omega(t-\tau_3)}\right]\cdot\left[\alpha_1^2\alpha_2 e^{jb_2}e^{j\phi_1(t-2\tau-\tau_3)}Ee^{j\omega(t-2\tau-\tau_3)}\right]^*\Big\}}_{=0 \text{ since } (7)} = \alpha_1^2E^2
\end{aligned}
\tag{30}
$$

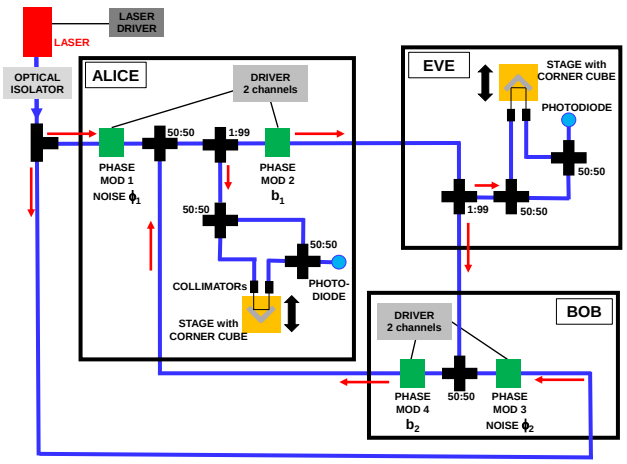


FIGURE 2: Real-world fiber optic based implementation scheme of the full optical noise level modulation system.

It is worth observing that there is a small difference between the theory exposed in Secs. III-IV and the hardware implementation of the optical NLM scheme in Fig. 2. This difference is due to the fact that, in the real implementation, the optical receiver can only extract the square module of the incoming signal. In the implementation scheme, the photodiode at the legitimate node (e.g., Alice) receives as input the signal

$$|y_1(t) + y_1(t-2\tau)|^2\,,$$

which is different from receiving $y_1(t)$ only, as in Sec. III. Thus, the successive expectation yields $\mathbb{E}\{|y_1(t) + y_1(t-2\tau)|^2\}$ and not $\mathbb{E}\{y_1(t)y_1(t-2\tau)\}$ as in (13). However, this difference can be easily overcome by noting that

$$
\begin{aligned}
y_1(t) + y_1(t-2\tau) &= \left(1 + \alpha_1\alpha_2 e^{jb_1}e^{jb_2}\right)y_1(t-2\tau)\\
&+ \alpha_2 e^{jb_2}Ee^{j\omega(t-\tau)}e^{j\phi_2(t-\tau)} + Ee^{j\omega t}e^{j\phi_1(t)}\,.
\end{aligned}
\tag{31}
$$

Thus, reminding Eqs. (6) and (7), we have

$$
\begin{aligned}
\mathbb{E}\{|y_1(t)+y_1(t-2\tau)|^2\} &= \underbrace{2\,\alpha_1\alpha_2\,\mathrm{Re}\left\{e^{jb_1}e^{jb_2}\right\}\sigma_{y_1}^2(t)}_{\text{real part of } R_{y_1y_1}(2\tau) \text{ as in (13)}} +\\
&+ \underbrace{(1+\alpha_1^2\alpha_2^2)\sigma_{y_1}^2(t) + E^2(1+\alpha_2^2)}_{K>0}
\end{aligned}
\tag{32}
$$

where K is an always positive bias. In order to recover the decision variable, whose sign is related to the bit transmitted by the other node, it is enough to remove both the constant bias from (32) and the contribution of the own bit b_1, i.e.,

$$\hat{b}_2 = \arccos\left(\frac{\mathbb{E}\{|y_1(t)+y_1(t-2\tau)|^2\} - K}{2\alpha_1\alpha_2\sigma_{y_1}^2(t)}\right) - b_1\,. \tag{33}$$

Therefore, the theory described in Sec. III is still valid.

The bias K can be either calculated as $(1+\alpha_1^2\alpha_2^2)\sigma_{y_1}^2(t)+E^2(1+\alpha_2^2)$ or estimated at the receiver. It is important to note that K is not constant but it becomes constant after some loops, such that $\sigma_{y_1}^2(t)$ is well approximated by $\sigma_{y_1}^2(\infty)$ as in (16) and (17). This means that the first estimated bit has to be neglected since it could be not reliable.

Actually, the expectation in (32) cannot be realized in a real-world scenario. In fact, the decision variable can be written as in (34). Taking the expectation $\mathbb{E}\{\}$ of (34) would make the undesired terms to vanish, thanks to assumptions (6) and (7). Unfortunately, in a real scenario, the expectation has to be replaced by a time average. In a time average, in particular if it is calculated over a short amount of time (number of loops), the undesired terms cannot be neglected completely.

In addition, we have to note that the desired term is summed to an always positive constant term $E^2(1+\alpha_2^2)$, which has no relevance, and a term $(1+\alpha_1^2\alpha_2^2)|y_1(t-2\tau)|^2$ that is an always positive RV with a Chi-Square distribution (since it comes from a product of two Gaussian RVs). This means that the probability density function (PDF) of the observed received signal is not symmetric. Thus, the optimal threshold to decide on the sign of the transmitted symbol is not in the middle of the PDFs, as we can see in Fig. 3a.

$$
\begin{aligned}
z &= |y_1(t)+y_1(t-2\tau)|^2 = \Big[y_1(t)+y_1(t-2\tau)\Big]\cdot\Big[y_1(t)+y_1(t-2\tau)\Big]^* \\
&= \Big[\left(1+\alpha_1\alpha_2 e^{jb_1}e^{jb_2}\right)y_1(t-2\tau)+\alpha_2 e^{jb_2}Ee^{j\omega(t-\tau)}e^{j\phi_2(t-\tau)}+Ee^{j\omega t}e^{j\phi_1(t)}\Big] \\
&\cdot \Big[\left(1+\alpha_1\alpha_2 e^{jb_1}e^{jb_2}\right)y_1(t-2\tau)+\alpha_2 e^{jb_2}Ee^{j\omega(t-\tau)}e^{j\phi_2(t-\tau)}+Ee^{j\omega t}e^{j\phi_1(t)}\Big]^* \\
&= \left(1+\alpha_1\alpha_2 e^{jb_1}e^{jb_2}\right)^2|y_1(t-2\tau)|^2+\alpha_2^2E^2+E^2 \\
&+ \underbrace{E\alpha_2 e^{jb_2}\left(1+\alpha_1\alpha_2 e^{jb_1}e^{jb_2}\right)\cdot\Big[y_1(t-2\tau)e^{j\phi_2(t-\tau)}+y_1^*(t-2\tau)e^{-j\phi_2(t-\tau)}\Big]}_{\text{undesired term 1}} \\
&+ \underbrace{E\left(1+\alpha_1\alpha_2 e^{jb_1}e^{jb_2}\right)\cdot\Big[y_1(t-2\tau)e^{j\phi_1(t)}+y_1^*(t-2\tau)e^{-j\phi_1(t)}\Big]}_{\text{undesired term 2}}+\underbrace{2E^2\alpha_2\cos\left(b_2+\phi_2(t-\tau)-\phi_1(t)\right)}_{\text{undesired term 3}} \\
&= \underbrace{2\alpha_1\alpha_2 e^{jb_1}e^{jb_2}|y_1(t-2\tau)|^2}_{\text{desired term}}+\underbrace{(1+\alpha_1^2\alpha_2^2)|y_1(t-2\tau)|^2}_{\text{always positive RV}}+\underbrace{E^2(1+\alpha_2^2)}_{\text{constant term}}+\text{undesired terms 1, 2 and 3}\,.
\end{aligned}
\tag{34}
$$

Let's figure out how to find the optimal threshold in case of non symmetric PDFs of the two symbols. Let's note that our decision variable, after the time average, assumes the form

$$\overline{z}=\frac{1}{L}\sum_{l=1}^{L}z_l=(a\cdot b+c)\sigma_{y_1}^2+d+w \tag{35}$$

where z_l is the decision variable at the end of the lth loop, L is the number of loops, $a=2\alpha_1\alpha_2$ is a constant, $b=e^{jb_1}e^{jb_2}$ is a Bernoulli(0.5) RV, $c=1+\alpha_1^2\alpha_2^2$ is a constant, $d=E^2(1+\alpha_2^2)$ is a constant, and w is a Gaussian RV that takes into account the non vanished contribution of the undesired terms in (34) after the time average. Since our goal is to find the sign of b_2 knowing the sign of b_1, we can draw two hypothesis with equal probability: $\mathcal{H}_0: b=1$ and $\mathcal{H}_1: b=-1$. In this case, the decision rule is to choose the hypothesis that has the highest posterior probability, i.e., decide for $b=+1$ if $P(\overline{z}|b=+1)>P(\overline{z}|b=-1)$, and decide $b=-1$ otherwise. The optimal threshold can be defined as the value of $\overline{z}$ that makes the posterior probabilities of both hypotheses equal, i.e., $P(\overline{z}|b=+1)P(b=+1)=P(\overline{z}|b=-1)P(b=-1)$, which indeed is equivalent to $P(\overline{z}|b=+1)=P(\overline{z}|b=-1)$ since the prior probabilities are equal.

Let's focus on the case $b=-1$. In this case, we decide correctly if $\overline{z}-d\leq\epsilon_1$, where $\epsilon_1=(a-c)\sigma_{y_1}^2+w$. The RV ϵ_1 is the sum of two independent RVs, a Chi Square $(a-c)\sigma_{y_1}^2$ and a Gaussian w. Assuming that the threshold is z_0, we decide correctly if $\overline{z}-d\leq z_0$, whose probability is given by

$$P(\overline{z}-d\leq z_0|b=-1)=P(\epsilon_1\leq z_0|b=-1). \tag{36}$$

Analogously, in the case $b=+1$ we have a correct decision if $\overline{z}-d>z_0$, whose probability is given by

$$P(\overline{z}-d>z_0|b=1)=P(\epsilon_2>z_0|b=1) \tag{37}$$

where $\epsilon_2=(a+c)\sigma_{y_1}^2+w$ is again the sum of two independent RVs, a Chi Square $(a+c)\sigma_{y_1}^2$ and a Gaussian w. The optimal threshold z_0 can be derived by imposing that

$$P(\epsilon_1\leq z_0|b=-1)=P(\epsilon_2>z_0|b=1) \tag{38}$$

Taking in mind that the two RVs ϵ_1 and ϵ_2 both have a non symmetric PDF, the threshold z_0 is not in the middle point of the PDFs. To compute the threshold, we have to impose that

$$\int_{-\infty}^{z_0}f_{\epsilon_1}(\epsilon_1)d\epsilon_1=\int_{z_0}^{\infty}f_{\epsilon_2}(\epsilon_2)d\epsilon_2 \tag{39}$$

where $f_{\epsilon_1}(\epsilon_1)$ and $f_{\epsilon_2}(\epsilon_2)$ denote the PDF of ϵ_1 and ϵ_2, respectively.

Eq. (39) does not have a closed-form solution, but it can be evaluated numerically. To simplify this evaluation, we propose four different approximations about the distribution of the RVs ϵ_1 and ϵ_2, based on which type of assumptions we make on the RVs $\sigma_{y_1}^2$ and w:

1) The decision is computed as in (33), i.e., we consider the RV $\sigma_{y_1}^2$ as constant and the RV w (the undesired terms) as negligible. This approach is analogous to the approach defined for radio communication systems [21].
2) We consider the RV w negligible, and thus ϵ_1 and ϵ_2 are Chi Square distributed RVs; the optimal threshold is computed as in (39).
3) We consider $\sigma_{y_1}^2$ approximated as a Gaussian RV (for the central limit theorem); thus, ϵ_1 and ϵ_2 are both Gaussian distributed RVs; the optimal threshold is computed as in (39).
4) We consider that ϵ_1 is a Gaussian RV (if w dominates the joint PDF $\epsilon_1=(a-c)\sigma_{y_1}^2+w$ when $b=-1$), while ϵ_2 is a Chi Square RV (in the case $\sigma_{y_1}^2$ dominates the corresponding joint PDF when $b=+1$); the optimal threshold is computed as in (39).

The accuracy of the proposed assumptions are compared with the optimal threshold in Monte Carlo simulations as reported in Sec. VI.

B. IMPLEMENTATION SCHEME: SECURITY ANALYSIS

Analogously, in the experimental scheme (Fig. 2), we consider that Eve detects, in the very worst case, the quantity

$|y_3(t) + y_3(t-2\tau)|^2$ and not $y_3(t)y_3(t-2\tau)$ as in (21). Again, this is not a problem, in fact

$$\mathbb{E}\{|y_3(t) + y_3(t-2\tau)|^2\} = 2\alpha_1\alpha_2 \,\mathrm{Re}\left\{e^{jb_1}e^{jb_2}\right\}\sigma^2_{y_3}(t) + (1+\alpha_1^2\alpha_2^2)\sigma^2_{y_3}(t) + \alpha_1^2E^2(1+\alpha_2^2)\,. \quad (40)$$

After some loops, $\sigma^2_{y_3}(t)$ converges to

$$\sigma^2_{y_3}(\infty) = \frac{\alpha_1^2E^2(1+\alpha_2^2)}{1-\alpha_1^2\alpha_2^2} = \alpha_1^2\sigma^2_{y_1}(\infty)\,.$$

Therefore, even if Eve could remove the bias from (40), it will still obtain something that is related to the XOR of the two information bits. In conclusion, the theory described in Sec. IV is still valid.

It is worth noting that although this paper does not include experimental results, the proposed implementation scheme is feasible for experiments set up with fiber optics and, in our opinion, it deserves further experimental research studies. Moreover, defining the implementation setup gave us the opportunity to consider the difference between the theoretical scheme and the practical implementation scheme, which is discussed in Sec. III, IV and V. In particular, the full optical implementation of the NLM scheme forces us to modify the reception scheme compared to the theoretical scheme, since the photodetector (at the receiver side) extracts the squared modulus of the signal, and not the autocorrelation. In Sec. V we demonstrate that the features of the theoretical NLM scheme are still valid, even with the proposed hardware implementation scheme.

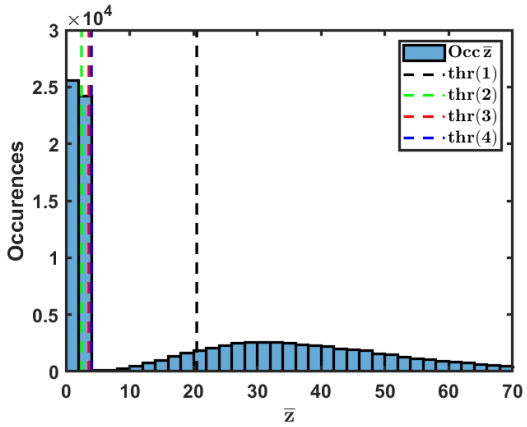
VI. NUMERICAL RESULTS

In this section we provide the numerical results of the proposed full optical noise-loop system. In particular, we show here both the reliability and security performance. Let us first show the reliability results for the decision variables given, respectively, by the theoretical analysis (13) and the implementation scheme (35). The numerical results are taken from Monte Carlo simulations, implemented in MATLAB, with 100 000 bits sent and a variable number L of loops. We recall that in the NLM scheme, to produce the decision variable, the loop is run L times for each bit.

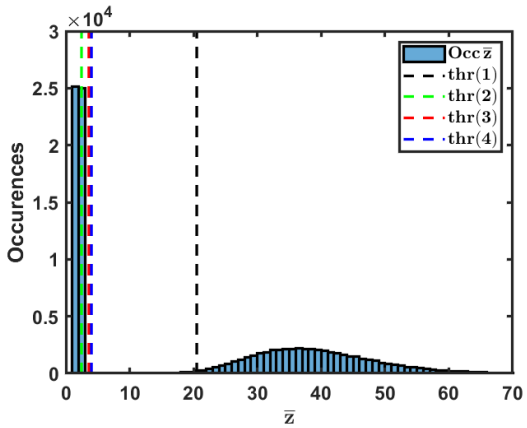
Figs. 3a and 3b show the occurrences of the values of the decision variable $\overline{z}$ in (35) over 100 000 bits. The optimal thresholds are reported in the figures, in order to show that as the number of loops L increases, the two branches of the PDF of $\overline{z}$ shrink and any threshold between 2.5 and 20.51 becomes optimal (Table 1), since for a large L the two branches of the PDF are very well separated (see Fig. 3b in comparison with Fig. 3a).

Let us now discuss briefly the thresholds shown in Figs. 3a–3b:

- Threshold (1) is calculated as the mean point of the two mean points of the distributions of $b = -1$ and $b = +1$; this threshold is located much more towards the mean point of the distribution of $b = +1$ (see Fig. 3a);



(a) $L = 5$



(b) $L = 100$

FIGURE 3: Histogram of the decision variable's values (35) with a number of loops $L = 5$ (a) and $L = 100$ (b), for 100 000 bits sent. For each approximation method, we report the optimal thresholds in Table 1.

TABLE 1: Threshold for the 4 approximation methods to compute the optimal decision threshold as in (39).

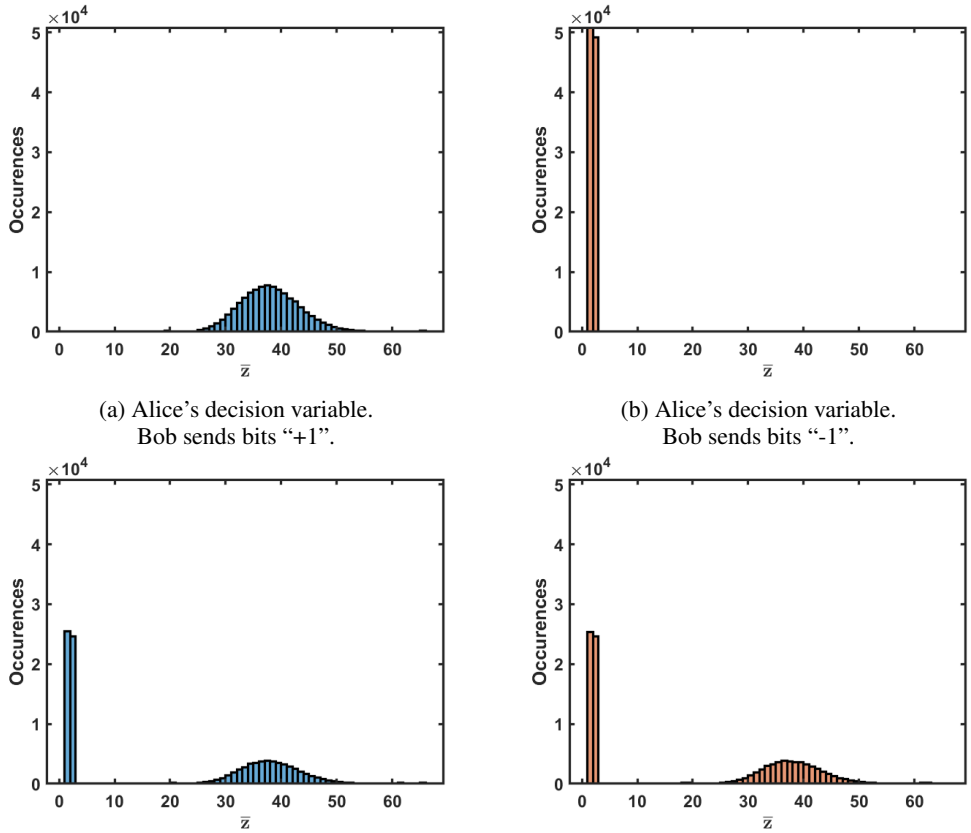
Methods	Number of Loops [L]						
	5	10	20	50	100	250	400
(1)	20.51	20.51	20.51	20.51	20.51	20.51	20.51
(2)	2.45	2.45	2.5	2.5	2.5	2.5	2.5
(3)	3.6	3.3	3.15	3.05	3.05	3	3
(4)	4	4.05	4.05	4.05	4.05	4.05	4.05

- Threshold (2) is located more towards the mean of the distribution of $b = -1$ since the undesired terms w is not negligible when $b = -1$;
- Threshold (3) considers both the distribution as Gaussian, while the distribution of $b = +1$ tends to be Chi-Square instead of Gaussian since the contribution of w is negligible;
- Threshold (4) is set considering the accurate distribution of $b = -1$ (Gaussian) and $b = +1$ (Chi-Square).

Table 1 shows the optimal threshold for each of the four proposed approximation methods (1)–(4) described after

TABLE 2: Bit Error Rate for the 4 approximation methods to compute the optimal decision threshold as in (39).

Methods	Number of Loops [L]						
	5	10	20	50	100	250	400
(1)	$6.2 \cdot 10^{-2}$	$1.8 \cdot 10^{-2}$	$1.7 \cdot 10^{-2}$	$1.0 \cdot 10^{-2}$	$4.0 \cdot 10^{-3}$	$1.5 \cdot 10^{-4}$	$< 10^{-5}$
(2)	$1.2 \cdot 10^{-1}$	$8.4 \cdot 10^{-2}$	$3.3 \cdot 10^{-2}$	$4.3 \cdot 10^{-3}$	$1.9 \cdot 10^{-4}$	$< 10^{-5}$	$< 10^{-5}$
(3)	$4.4 \cdot 10^{-3}$	$1.6 \cdot 10^{-3}$	$1.5 \cdot 10^{-4}$	$< 10^{-5}$	$< 10^{-5}$	$< 10^{-5}$	$< 10^{-5}$
(4)	$7.2 \cdot 10^{-4}$	$1.0 \cdot 10^{-5}$	$< 10^{-5}$	$< 10^{-5}$	$< 10^{-5}$	$< 10^{-5}$	$< 10^{-5}$



(a) Alice's decision variable. Bob sends bits "+1".

(b) Alice's decision variable. Bob sends bits "-1".

(c) Eve's decision variable. Bob sends bits "+1".

(d) Eve's decision variable. Bob sends bits "-1".

FIGURE 4: Histogram of the values of **Alice**'s [subfigs. (a) and (b)] and **Eve**'s [subfigs. (c) and (d)] decision variable (35) with a number of loops $L = 100$ and 100 000 bits sent by Bob. The occurrences of the decision variable's values refer to the bits "+1" [subfigs. (a) and (c)] and "-1" [subfigs. (b) and (d)] sent by Bob.

Eq. (39). It is worth noting that for large L the method (1) is equivalent to the theoretical decision variable (33), in fact when $L \geq 400$ the term $\sigma^2_{y_1}(t)$ in (16) converges to $\sigma^2_{y_1}(\infty)$ in (17) and becomes constant. As we can appreciate in Table 1, method (4) converges very quickly to the final optimal value of the threshold, compared to the other methods apart method (1) whose threshold is constant since it considers the PDF of $\bar{z}$ as symmetric.

Table 2 shows the Bit Error Rate (BER) over 100 000 bits for each of the methods (1)–(4) by using the thresholds depicted in Table 1. Method (4) is the most accurate, even for low number of loops L, as expected. Method (1) requires $L = 400$ to reach the best performance (BER $\leq 1 \times 10^{-5}$), while method (4) just requires $L = 20$.

Let us now show the security performance of the proposed NLM system and let us assume we are in the worst case scenario, i.e., Eve is able to recover the exact propagation delay between Bob and Alice. Bob sends 100 000 bits, half of those are +1, other half are -1, both randomly distributed.

Figs. 4a and 4c show the occurrences of the values of Alice's and Eve's decision variable (35), respectively, over the bits "+1" sent by Bob and with $L = 100$. Analogously, Figs. 4b and 4d shows the occurrences of the values of Alice's and Eve's decision variable (35), respectively, over the bits "-1" sent by Bob.

As it can be appreciated, the PDF of Alice's decision variable in Figs. 4a, 4b has only one region, while the PDF of Eve's decision variable in Figs. 4c, 4d has always two regions. This means that Eve can only apply a threshold and

decide which bit has been sent by Bob. Since the two regions spanned by the PDFs have the same integral, Eve decides for +1 or -1 with equal probability, although only +1 or -1 are sent by Bob to Alice. This entails that Eve experiences a BER ≈ 0.5, when a binary signalling is used by the legitimate nodes.

As a summary, we can derive the following conclusions from the numerical results:

- Reliability (the capacity of Alice to correctly demodulate the bit sent by Bob):
  - Methods (4) can lead to a very low BER (over 100 000 bits sent) even with a low number of loops $L \geq 10$.
  - Method (1) can lead to a very low BER (over 100 000 bits sent) only with a large number of loops $L \geq 250$; this means that the theoretical result is valid only for large L, as expected.
- Security (the capacity of Eve to correctly demodulate the bit sent by Bob to Alice):
  - Even in the very worst-case scenario, Eve is not able to correctly recover the sign of the bit sent by the legitimate nodes.
  - Eve experiences a BER ≈ 0.5, while Alice can reach a BER $\leq 10^{-5}$ over 100 000 bits sent with $L \geq 10$.
  - We can affirm that the optical NLM is a full secrecy rate scheme, i.e., each sent bit is secure.

VII. CONCLUSIONS

This paper discusses a novel security technique called noise level modulation (NLM), which is a physical layer security (PLS) approach that provides confidentiality by modulating information with locally generated noise. Unlike traditional encryption, NLM does not depend on attackers' computational limits and eliminates the need for the prior exchange of a secret key, thus simplifying security protocols and reducing costs. NLM also enhances system resilience by making data indistinguishable from background noise, protecting them against physical attacks.

While the NLM concept is known, this paper establishes the theoretical foundation for full optical noise level modulation, demonstrating its reliability and security in a fiber-optic system. It identifies challenges in adapting NLM to fiber optical channels and provides insights on necessary equipment, materials, and schemes.

The rise of quantum computing and cryptography threatens traditional encryption, motivating further research in optical NLM as a promising security technique for secure optical communication. Optical NLM can complement or integrate with other security techniques, like quantum key distribution and physical layer encryption, to achieve optimal security and performance in future optical communication systems.

APPENDIX

Lemma 1. *Let u and v be two independent continuous RVs with PDF $f_U(u)$ and $f_V(v)$, respectively. The PDF of $z = uv$ is $f_Z(z) = \int_{-\infty}^{+\infty} f_U(u) f_V(\frac{z}{u}) \frac{1}{|u|} du$ [22].*

Theorem 1. *Let p be a discrete $\mathrm{Ber}(0.5)$ RV with alphabet $\mathcal{B} = \{-1, 1\}$ and with probability mass function (PMF) $F_P(p)$ and let q be a continuous standard Cauchy RV with PDF $f_Q(q)$. The RV $m = pq$ is still Cauchy distributed.*

Proof. Let us write down the PDF of m, $f_M(m)$. According to Lemma 1 with one of the two RVs discrete instead of continuous, we get

$$\begin{aligned} f_M(m) &= \sum_{p \in \mathcal{B}} F_p(p) f_q\left(\frac{m}{p}\right) \frac{1}{|p|} \\ &= \frac{1}{2} \frac{1}{\pi(1 + (m/p)^2)}\bigg|_{p=1} + \frac{1}{2} \frac{1}{\pi(1 + (m/p)^2)}\bigg|_{p=-1} \\ &= \frac{1}{\pi(1 + m^2)}. \end{aligned} \tag{41}$$

The PDF $f_M(m)$ of the RV $m = pq$ is the same of q, i.e., m is a standard Cauchy RV. □

Theorem 2. *Let p be a discrete $\mathrm{Ber}(0.5)$ RV with alphabet $\mathcal{B} = \{-1, 1\}$ and with PMF $F_P(p)$ and let q be a continuous $\mathcal{N}(0, \sigma_q)$ RV with PDF $f_Q(q)$. The RV $m = pq$ is $\mathcal{N}(0, \sigma_q)$.*

Proof. Let us write down the PDF of m, $f_M(m)$. According to Lemma 1 one has that

$$\begin{aligned} f_M(m) &= \sum_{p \in \mathcal{B}} F_p(p) f_q\left(\frac{m}{p}\right) \frac{1}{|p|} \\ &= \frac{1}{2} \frac{1}{\sqrt{2\pi\sigma_q^2}} e^{-\frac{m^2}{\sigma_q^2}} + \frac{1}{2} \frac{1}{\sqrt{2\pi\sigma_q^2}} e^{-\frac{m^2}{(-1)^2\sigma_q^2}} = \frac{1}{\sqrt{2\pi\sigma_q^2}} e^{-\frac{q^2}{\sigma_q^2}}. \end{aligned} \tag{42}$$

The PDF $f_M(m)$ of the RV $m = pq$ is the same of q, i.e., m is $\mathcal{N}(0, \sigma_q)$. □

REFERENCES

[1] R. Hui, Introduction to fiber-optic communications. Academic Press, 2020.

[2] B. Wu, B. J. Shastri, and P. R. Prucnal, "Secure communication in fiber-optic networks," in Emerging Trends in ICT Security. Elsevier, 2014, pp. 173–183. [Online]. Available: https://doi.org/10.1016/b978-0-12-411474-6.00011-6

[3] M. P. Fok, Z. Wang, Y. Deng, and P. R. Prucnal, "Optical layer security in fiber-optic networks," IEEE Transactions on Information Forensics and Security, vol. 6, no. 3, pp. 725–736, Sep. 2011. [Online]. Available: https://doi.org/10.1109/tifs.2011.2141990

[4] Physical Layer Security. Springer International Publishing, 2021. [Online]. Available: http://dx.doi.org/10.1007/978-3-030-55366-1

[5] J. Pfeiffer and R. F. H. Fischer, "Multilevel coding for physical-layer security in optical networks," in Photonic Networks; 19th ITG-Symposium, 2018, pp. 1–8.

[6] D. Syvridis, E. Pikasis, and C. Chaintoutis, Physical Layer Security in Optical Networks. Springer International Publishing, 2020, p. 412–424. [Online]. Available: http://dx.doi.org/10.1007/978-3-030-38085-4_35

[7] S. Rothe, N. Koukourakis, H. Radner, A. Lonnstrom, E. Jorswieck, and J. W. Czarske, "Physical layer security in multimode fiber optical networks," Scientific Reports, vol. 10, no. 1, Feb. 2020. [Online]. Available: https://doi.org/10.1038/s41598-020-59625-9

[8] K. Guan, A. M. Tulino, P. J. Winzer, and E. Soljanin, "Secrecy capacities in space-division multiplexed fiber optic communication systems," IEEE Transactions on Information Forensics and Security, vol. 10, no. 7, pp. 1325–1335, Jul. 2015. [Online]. Available: https://doi.org/10.1109/tifs.2015.2405897

[9] Y.-S. Shiu, S. Y. Chang, H.-C. Wu, S. C.-H. Huang, and H.-H. Chen, "Physical layer security in wireless networks: A tutorial," IEEE wireless Communications, vol. 18, no. 2, pp. 66–74, 2011.

[10] O. Buskila, A. Eyal, and M. Shtaif, "Secure communication in fiber optic systems via transmission of broad-band optical noise," Optics Express, vol. 16, no. 5, p. 3383, 2008. [Online]. Available: https://doi.org/10.1364/oe.16.003383

[11] Y. Wan, J. Ren, B. Liu, Y. Mao, S. Chen, X. Wu, Y. Li, Y. Wu, L. Zhao, T. Sun, and R. Ullah, "Secure OFDM transmission scheme based on chaotic encryption and noise-masking key distribution," Optics Letters, vol. 47, no. 11, p. 2903, May 2022. [Online]. Available: https://doi.org/10.1364/ol.460052

[12] A. W. Abdulwahhab, A. K. Abass, M. A. Saleh, and F. F. Rashid, "Enhancing performance of optical chaotic-based secure fiber-optic communication system," Optical and Quantum Electronics, vol. 55, no. 5, Apr. 2023. [Online]. Available: https://doi.org/10.1007/s11082-023-04757-1

[13] E. Jorswieck, A. Lonnstrom, K.-L. Besser, S. Rothe, and J. W. Czarske, "Achievable physical-layer secrecy in multi-mode fiber channels using artificial noise," in 2021 17th International Symposium on Wireless Communication Systems (ISWCS). IEEE, Sep. 2021. [Online]. Available: https://doi.org/10.1109/iswcs49558.2021.9562176

[14] N. Skorin-Kapov, M. Furdek, S. Zsigmond, and L. Wosinska, "Physical-layer security in evolving optical networks," IEEE Communications Magazine, vol. 54, no. 8, pp. 110–117, 2016.

[15] M. Obeed, A. M. Salhab, M.-S. Alouini, and S. A. Zummo, "Survey on physical layer security in optical wireless communication systems," in 2018 seventh international conference on communications and networking (ComNet). IEEE, 2018, pp. 1–5.

[16] F. J. Lopez-Martinez, G. Gomez, and J. M. Garrido-Balsells, "Physical-layer security in free-space optical communications," IEEE Photonics Journal, vol. 7, no. 2, pp. 1–14, 2015.

[17] H.-L. Huang, D. Wu, D. Fan, and X. Zhu, "Superconducting quantum computing: a review," Science China Information Sciences, vol. 63, pp. 1–32, 2020.

[18] F. Xu, X. Ma, Q. Zhang, H.-K. Lo, and J.-W. Pan, "Secure quantum key distribution with realistic devices," Reviews of Modern Physics, vol. 92, no. 2, p. 025002, 2020.

[19] L. Mucchi, L. S. Ronga, and L. Cipriani, "A new modulation for intrinsically secure radio channel in wireless systems," Wireless Personal Communications, vol. 51, no. 1, pp. 67–80, Sep. 2008. [Online]. Available: https://doi.org/10.1007/s11277-008-9609-8

[20] L. Mucchi, L. S. Ronga, and E. D. Re, "Physical layer cryptography and cognitive networks," Wireless Personal Communications, vol. 58, no. 1, pp. 95–109, Apr. 2011. [Online]. Available: https://doi.org/10.1007/s11277-011-0290-y

[21] L. Mucchi, S. Caputo, P. Marcocci, G. Chisci, L. Ronga, and E. Panayirci, "Security and reliability performance of noise-loop modulation: Theoretical analysis and experimentation," IEEE Transactions on Vehicular Technology, vol. 71, no. 6, pp. 6335–6350, Jun. 2022. [Online]. Available: https://doi.org/10.1109/tvt.2022.3160094

[22] M. Bloch and J. Barros, Physical-Layer Security: From Information Theory to Security Engineering. Cambridge University Press, 2011.

[23] A. Lazo and P. Rathie, "On the entropy of continuous probability distributions (corresp.)," IEEE Transactions on Information Theory, vol. 24, no. 1, pp. 120–122, 1978.

[24] S. Verdú, "The cauchy distribution in information theory," Entropy, vol. 25, no. 2, p. 346, Feb. 2023. [Online]. Available: http://dx.doi.org/10.3390/e25020346

STEFANO CAPUTO received the Dr.Eng. degree (Laurea) in mechanical engineering and the Ph.D. degree in telecommunications engineering from the University of Florence, Florence, Italy, in 2016 and 2019, respectively. He is currently a Research Fellow with the University of Florence. His current research areas include theoretical modeling, algorithm design, and real measurements, mainly focused on: physical layer security and light cryptography, sensors and V2V/V2I communication in automotive field, visible light communications, localization, body area networks, and molecular communications.

SILVIA VICIANI received the University Degree in Physics and Ph.D. in Physics from the University of Florence (Italy) in 1997 and 2001, respectively. Between 2001 and 2004 she was at the National Research Council-National Institute of Optics (CNR-INO) in Florence (Italy), as Post-doctoral Scholar, working in the field of Quantum Optics. From 2004 to 2009 she was a fixed-term researcher at CNR-INO working in the field of Optics and Laser Spectroscopy and since 2009 she is a permanent researcher of the CNR-INO. Her current scientific interests concern the development and the realization of spectrometers in the infrared and far-infrared region, employed on ground and onboard several platforms (straospheric aircraft and balloons, drones, light aircraft and helicopters), for environmental, atmospheric and volcanic applications. She has been involved in national and international projects, both as participant and coordinator, and she was Principal Investigator of instruments during international measurement campaigns. She is author and co-author of 72 research articles in peer-reviewed literature and in book chapters.

STEFANO GHERARDINI received his M.Sc. in Electrical and Automation Engineering and Ph.D. in Information Engineering, curriculum Non-linear Dynamics and Complex Systems, from the University of Florence, Italy, in 2014 and 2018, respectively. His postdoc experience includes activities at the University of Florence, the European Laboratory for Non-linear Spectroscopy (LENS), the Italian National Institute of Optics (CNR-INO), and the Instituto Superior Técnico and Instituto de Telecomunicações in Lisbon, Portugal. Since December 2021, he has been a permanent researcher at CNR-INO, at Trieste Unit till January 2024 and now in Florence. He also hold the role of external collaborator at the International School for Advanced Studies (SISSA). His research interests are quantum thermodynamics, quantum statistical mechanics, large deviation theory, open quantum systems and decoherence, non-Markovianity, quantum communications and quantum sensing. Currently, his research activity concerns the theoretical investigation of out-of-equilibrium dynamics and stochastic thermodynamics in the quantum regime resorting to quantum fluctuations theorems.

GIACOMO BORGHINI is currently a Ph.D. student of the Information Department (DINFO) of University of Florence, Italy. He received the Laurea in telecommunication engineering in 2022, from the University of Florence. His Ph.D. research project concerns the study of physical layer security in 6G mobile networks. His research interests involve physical layer security, optical wireless communications and molecular communication systems. His research interests involve also artificial intelligence, specifically the detection of AI-generated artworks.

FRANCESCO CATALIOTTI is Full Professor of Structure of Matter at the University of Florence, Italy. He is a member of the Board of the Atomic, Molecular and Optical Physics Division of the European Physical Society and of the Research Council of the European Association of Metrological Institutes. His research activity concerns the physics of atoms and their interactions with laser radiation. He has coordinated several European projects related to quantum technologies. He was Italian representative in the FET Flagship Board of Funders and in the Board of the European Quantum Communication Infrastructure. Since 2021 he is Director of the National Institute of Optics of the National Research Council (CNR) and coordinates the participation of CNR to the Quantum Technologies initiatives of the Italian National Recovery and Resilience Plan.

LORENZO MUCCHI (M'98-SM'12) received the Laurea in telecommunications engineering and the Ph.D. in telecommunications and information society from the University of Florence, Italy, in 1998 and in 2001, respectively. He is an Associate Professor at the University of Florence, Italy. His research interests involve theory and experimentation of wireless systems and networks including physical-layer security, visible light communications, ultra-wideband techniques, body area networks, and interference management. Dr. Mucchi is serving as an associate editor of IEEE Transaction on Communications and IEEE Access, and he has been Editor-in-Chief for Elsevier Academic Press. He is part of the European Telecommunications Standard Institute (ETSI) Smart Body Area Network (SmartBAN) group (member 2013, chair 2022). He has been lead organizer and general chair of IEEE and EAI international conferences.