Tapping Eavesdropper Designs against Physical Layer Secret Key in Point-to-Point Fiber Communications

Wenxiu Hu, Zhuangkun Wei, Sergei Popov, *Senior Member, IEEE, Fellow, Optica*, Mark Leeson, *Senior Member, IEEE,* Tianhua Xu *Member, IEEE*

***Abstract*—With the growing demand for service access and data transmission, security issues in optical fiber systems have become increasingly important and the subject of increased research. Physical layer secret key generation (PL-SKG), which leverages the random but common channel properties at legitimate parties, has been shown to be a secure, low-cost, and easily deployed technique as opposed to computational-based cryptography, quantum, and chaos key methods that rely on precise equipment. However, the eavesdropper (Eve) potential for current PL-SKG in fiber communications has been overlooked by most studies to date. Unlike wireless communications, where the randomness comes from the spatial multi-paths that cannot be all captured by Eves, in fiber communications, all the randomness (from transmitted random pilots or channel randomness) is contained in the signals transmitted inside the fiber. This, therefore, enables a tapping Eve to reconstruct the common features of legitimate users from its received signals, and further decrypt the featured-based secret keys. To implement this idea, we designed two Eve schemes against polarization mode distortion (PMD) based PL-SKG and the two-way cross multiplication based PL-SKG. The simulation results show that our proposed Eves can successfully reconstruct the legitimate common feature and the secret key relied upon, leading to secret key rate (SKR) reductions of between three and four orders of magnitude in the PL-SKG schemes studied. As a result, we reveal and demonstrate a novel eavesdropping potential to provide challenges for current physical layer secret key designs. We hope to provide more insightful vision and critical evaluation on the design of new physical layer secret key schemes in optical fiber links, to provide more comprehensively secure, and intelligent optical networks.**

***Index Terms*—fiber communications, fiber tapping, eavesdropping, physical layer security, secret key generation.**

I. Introduction

Data transmission demands have been raised significantly in recent years, to confront the large increase in civil and commercial communications. As an essential role in our daily communication systems, optical fiber communication has consequently experienced great traffic growth, which leads to a new security issue [1]. Traditional cryptography relies on computational complexity to pursue secret key generation, management, and distribution [2], however, this ceases to be guaranteed with the development and access of more powerful computers by an eavesdropper (Eve).

An alternative idea is to use common physics to generate shared secret keys at two legitimate parties. The most well-known example is the quantum key distribution (QKD). This exploits the quantum mechanism (e.g., indeterminacy and entanglement) which is unique to the two legitimate parties and thereby has been proved to enable them to generate a shared secret key [3], [4]. The main challenge is the extremely high cost of the devices to generate a cipher key with a high secret key rate (SKR), especially to meet Gbps levels of transmission. Another example leverages optical chaos systems that are identically deployed at two legitimate parties [5]–[8]. The challenges in this approach are (i) the static key sources make it vulnerable to known-plaintext attacks [9], and (ii) practical implementation difficulties due to the strong restriction of deploying identical chaos systems.

Recently, physical layer secret key generation (PL-SKG) has been proposed and studied to secure wireless [10]–[14] and optical [15]–[18] communications, leveraging the random and reciprocal channel properties extracted by two legitimate parties (Alice and Bob) to generate a shared secret key. From a theoretical point of view, PL-SKG can be categorized into two families. The first one purely exploits the channel state information (CSI) as the common random feature. In the context of fiber communications, such randomness comes from (i) phase fluctuation in Mach-Zehnder interferometers (MZIs) [15], (ii) mode mixing (MM) [19], (iii) phase fluctuations between orthogonal polarization modes in delay interferometers (DIs) [20], (iv) dynamic Stokes parameters (SPs) in single-mode fiber (SMF) [21], and (v) polarization mode dispersion (PMD) [16], [22]. Leveraging these induced sources of channel randomness, Alice and Bob send a public pilot sequence and construct the common features by their received signals that involve the common CSI, which will then be passed to the quantization [23], [24], the information reconciliation (IR) [25] and the privacy amplification (PA) [26] modules for the final cipher key generation. One challenge for the aforementioned pure CSI-based PL-SKG is that the SKR cannot meet the industrial requirement due to insufficient channel randomness (the SKR is $<$ 1 kbps). To address this, the second method employs further devices to improve the SKR. For example, Hajomer *et al.* [17] use an active polarization scrambler to accelerate the common dynamics of the state of polarization

This work is supported by EU Horizon 2020 MSCA Grant 101008280 (DIOR) and UK Royal Society Grant (IES\R3\223068). *(Corresponding author : Tianhua Xu)* W. Hu and M. Leeson are with School of Engineering, University of Warwick, Coventry CV4 7AL, United Kingdom. Zhuangkun Wei is with the School of Aerospace, Transport, and Manufacturing, Cranfield University, MK43 0AL, UK. T. Xu is with School of Engineering, University of Warwick, Coventry CV4 7AL, United Kingdom, with Tianjin University, Tianjin 300072, China, and also with University College London (UCL), London WC1E 6BT, United Kingdom (tianhua.xu@ieee.org). Sergei Popov is with KTH Royal Institute of Technology, Stockholm 16440, Sweden.

(SOP) for Alice and Bob, deriving a higher SKR (200 kbps).

To further speed up the SKR, two-way cross multiplication methods have been proposed [27]–[30] and implemented in fiber communications [18], whereby extra randomness is induced by the random transmitted signals instead of the public pilot sequences. To be specific, Alice and Bob send random signals to each other and crossly multiply their sent and received signals as the common feature for PL-SKG. In this view, the randomness of the common feature involves (i) the channel randomness and (ii) the two random signal spaces, which therefore gives rise to a higher SKR as opposed to pure CSI-based PL-SKGs.

However, all of the aforementioned works considered an Eve that employed only simple brute force decoding, and eavesdropping research has been overlooked by most of the studies. In wireless communications, an Eve that is a half-wavelength away from Alice and Bob has difficulty in decrypting the PL-SKG, since the wireless channel randomness arises from spatial multi-paths, which are difficult to be all monitored by potential Eves [31]. By contrast, in fiber communications, the randomness induced by either channel or signal level is all reflected by the signals transmitted inside the fiber. In this view, a tapping Eve [32] has the potential to reconstruct Alice's and Bob's common features, via its received signals that contain all the channel and signal level randomness. Hence, this provides motivation for our work here, which aims to design a more efficient Eve than brute force. To implement this idea, we propose two Eve designs against (i) the PL-SKG based on PMD randomness, i.e., the works in [16], [22], and (ii) the two-way cross multiplication PL-SKG as a combination of [16] and [18]. Simulation results demonstrate our designed tapping Eve, which is able to reduce SKR by between *three* and *four* orders of magnitude. Thus, we aim to design a smarter Eve to provide challenges for current PL-SKG approaches. We hope to provide a more insightful vision and critical evaluation of the design of new PL-SKG methods in optical fiber links, to provide more comprehensively secure, and intelligent optical networks.

II. System Model

In this work, we consider a point-to-point fiber communication model (see Fig. 1(a)). Two legitimate nodes, Alice and Bob, aim to generate secret keys leveraging the channel reciprocity and randomness of the single mode fiber (SMF) between them. Standard PL-SKG contains four parts, shown in Fig. 1(b): 1) channel feature construction, 2) key quantization, 3) information reconciliation and 4) privacy amplification, where common features serve as the only source of randomness for the following three steps. Hereby, we focus on how the tapping Eve can reconstruct Alice's and Bob's channel features which their further secret keys rely upon.

The channels from Alice to Bob and from Bob to Alice are denoted as $\mathbf{H}_{AB}(\omega), \mathbf{H}_{BA}(\omega) \in \mathbb{C}^{2\times 2}$, which can be expressed as [16]:

$$\begin{aligned}\mathbf{H}_{AB}(\omega)=&\prod_{n=1}^{N_{AB}} l(\omega)\mathbf{S}(-\theta_n)diag\left(\begin{bmatrix} e^{-\frac{j}{2}(\overline{\Delta}_\tau\omega+\phi_n)} \\ e^{\frac{j}{2}(\overline{\Delta}_\tau\omega+\phi_n)}\end{bmatrix}\right)\mathbf{S}(\theta_n),\\ \mathbf{H}_{BA}(\omega)=&\prod_{n=N_{AB}}^{1} l(\omega)\mathbf{S}(-\theta_n)diag\left(\begin{bmatrix} e^{-\frac{j}{2}(\overline{\Delta}_\tau\omega+\phi_n)} \\ e^{\frac{j}{2}(\overline{\Delta}_\tau\omega+\phi_n)}\end{bmatrix}\right)\mathbf{S}(\theta_n)\\ =&\mathbf{H}_{AB}^T(\omega),\end{aligned} \tag{1}$$

where ω is the angular speed. N_{AB} is the number of fiber segments for simulation. $l(\omega) \triangleq e^{-\frac{d_z\cdot att}{2}-\frac{j}{2}\frac{D\lambda^2 d_z\omega^2}{2\pi c}}$ is the chromatic dispersion (CD) component, with d_z the simulation step size, att the attenuation parameter, $c = 3\times 10^8 ms^{-1}$ the light speed, λ the reference wavelength, and D the dispersion parameter at λ. θ_n, ϕ_n are the random rotation angle and phase for nth segment of fiber, evenly distributed over $[0, 2\pi)$, $\mathbf{S}(\cdot)$ is the 2×2 rotation matrix, and $\overline{\Delta}_\tau$ is average differential group delay. Here, we initially ignore the cross-phase modulation (XPM) and self-phase modulation (SPM) nonlinear fiber properties, since including XPM/SPM cannot guarantee the channel reciprocity for PL-SKG in Alice and Bob. We will discuss the case with nonlinear XPM/SPM in Section IV concerning simulations.

In the SMF model described in Eq. (1), the channel reciprocity is represented by $\mathbf{H}_{AB}(\omega) = \mathbf{H}_{BA}(\omega)^T$, which is deduced by the reversed order of $1, \cdots, N_{AB}$ fiber segments. The channel randomness is induced by the PMD effect, which is related to differential group delay (DGD) caused by the birefringence phenomenon in a long-haul optical fiber. Typically, the average DGD parameter $\overline{\Delta}_\tau$ is determined by the PMD coefficient and the fiber length, denoted by L_{AB}, i.e., $\overline{\Delta}_\tau = PMD_{coefficient}\cdot\sqrt{L_{AB}}$, which, however, is insufficient to maintain enough channel randomness for PL-SKG [16]. To address this, the work in [16] adopts randomly spliced polarization maintaining fibers (RSPMF) at both the ends of Alice and Bob, which is able to generate enough randomness for PL-SKG by ensuring $\overline{\Delta}_\tau > 0.25T_B$ (T_B is the bit period).

To pursue eavesdropping, the fiber tapping Eve is considered in this work, which is assumed to intercept the signals transmitted from Alice and Bob [32]. As such, the channels from Alice to Eve and from Bob to Eve, denoted as $\mathbf{H}_{AE}(\omega), \mathbf{H}_{BE}(\omega) \in \mathbb{C}^{2\times 2}$, can be modeled by replacing B and A of $\mathbf{H}_{AB}(\omega)$ and of $\mathbf{H}_{BA}(\omega)$ with E in Eq. (1), respectively.

III. Eavesdropping Designs

In this section, two types of Eve design are elaborated against the CSI and the two-way-based PL-SKG schemes, respectively. Both of them aim to obtain the secret keys by reconstructing the common channel features of Alice and Bob, since the channel feature is the only source of randomness for the PL-SKG. The essential idea comes from the following fact. In contrast to wireless communications where the channel randomness is induced by the multi-path that cannot be all captured by Eves, in fiber communications, all the randomness (either from channel phases or from signal spaces) can be

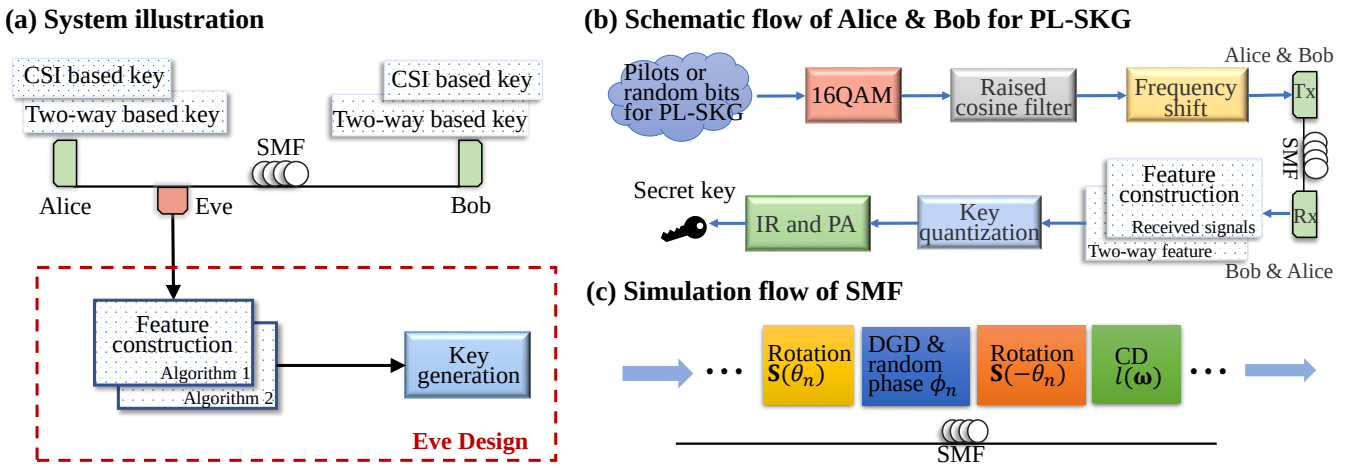

Fig. 1. Illustration of Alice, Bob and Eve model in fiber communications: (a) the system illustration and the schematic flow of our Eve design, (b) the schematic flows of Tx and Rx (can both be Alice and Bob) for PL-SKG, and (c) the simulation flow of SMF.

observed by a tapping Eve. This thereby enables the tapping Eve to reconstruct the common features of Alice and Bob and further reconstruct their feature-derived secret key.

A. Problem Formulation

To validate our idea, we provide two eavesdropping schemes targeting the two currently established PL-SKG methods. With the help of the Alice, Bob and Eve -based SMF model, the purpose of this work is to design tapping Eve schemes to reconstruct the shared secret key generated by Alice and Bob. In the following, two Eve schemes are elaborated against PL-SKGs using (i) only random CSI, and (ii) two-way randomness combined CSI.

B. Eavesdropping CSI-based PL-SKG

1) CSI-based PL-SKG method: To generate the shared secret key via the reciprocal CSI, Alice and Bob first send public and identical pilot sequences to each other in two consecutive time slots. This time division mode aims to guarantee the common features from the received signals, i.e., (a) the (quasi) static fluctuation phases from Alice to Bob and from Bob to Alice in a short time duration, and (b) the sent pilots undergo the channels with the same wavelength (rather than the full-duplex mode with different up-link and down-link wavelengths). We denote the sent pilots from Alice and Bob as $\mathbf{u}(\omega) = [u_x(\omega), u_y(\omega)]^T$. Then, the received signals at Alice and at Bob, denoted as $\mathbf{r}_A(\omega) = [r_{A,x}(\omega), r_{A,y}(\omega)]^T$ and $\mathbf{r}_B(\omega) = [r_{B,x}(\omega), r_{B,y}(\omega)]^T$, are expressed as:

$$\begin{aligned}\mathbf{r}_A(\omega) &= \mathbf{H}_{BA}(\omega)\cdot\mathbf{u}(\omega) + \mathbf{n}_A = \mathbf{H}_{AB}^T(\omega)\cdot\mathbf{u}(\omega) + \mathbf{n}_A,\\ \mathbf{r}_B(\omega) &= \mathbf{H}_{AB}(\omega)\cdot\mathbf{u}(\omega) + \mathbf{n}_B.\end{aligned} \tag{2}$$

where $\mathbf{n}_A$ and $\mathbf{n}_B$ are the receiving noise components. It is deduced from Eq. (2) that $\mathbf{r}_A(\omega)$ and $\mathbf{r}_B(\omega)$ share common features, i.e.,

$$\begin{aligned}Cov(r_{A,x}(\omega), r_{B,x}(\omega)) &\geq |u_x(\omega)|^2\mathbb{D}(h_{11}(\omega))\\ Cov(r_{A,y}(\omega), r_{B,y}(\omega)) &\geq |u_y(\omega)|^2\mathbb{D}(h_{22}(\omega))\end{aligned} \tag{3}$$

where $h_{ij}(\omega)$ is the (i,j)th element of $\mathbf{H}_{AB}^T(\omega)$, and $\mathbb{D}(\cdot)$ represents the variance. In Eq. (3), the equality holds when h_{ij} is independent from each other, and therefore serves as a lower-bound correlation between the received signals of Alice and Bob. As such, $\mathbf{r}_A$ and $\mathbf{r}_B$ can be used to generate the shared secret key by the quantization method, i.e., [16]

$$k_a = \begin{cases} 1, & \varphi_a > \gamma_1^{(a)},\\ 0, & \varphi_b < \gamma_0^{(a)},\end{cases} \quad a \in \{A, B\}, \tag{4}$$

where $\gamma_1^{(a)} = \mathbb{E}(\varphi_a) + \alpha\sqrt{\mathbb{D}(\varphi_a)}$ and $\gamma_0^{(a)} = \mathbb{E}(\varphi_a) - \alpha\sqrt{\mathbb{D}(\varphi_a)}$ are the quantisation thresholds, with quantization threshold parameter $\alpha \in [0, 1)$, and $\mathbb{E}(\cdot)$ the expectation. In Eq. (4), φ_a is enumerating $Re[r_{A,x}(\omega)], Im[r_{A,x}(\omega)], Re[r_{B,x}(\omega)]$ and $Re[r_{B,y}(\omega)]$. From Eq. (4), the quantized secret key between Alice and Bob is obtained. Here, it is noted that the use of upper/lower thresholds aims to discard unreliable features (e.g. contaminated by noise, or with low correlations). To be specific, when the correlations of Alice's and Bob's common features are low, a large upper/lower threshold gap can effectively discard the uncorrelated features, leaving the number of remained keys to equal (approximately) that of matched keys. This further reduces the burden of the following key reconciliation step, e.g. an easier design of the forward error correction (FEC) code, to achieve the key reconciliation at Alice and Bob.

2) Eavesdropping design: In CSI-based PL-SKG, the randomness is totally induced from the channel. So, the Eve design here is to estimate the channel matrix $\mathbf{H}_{AB}(\omega)$. We denote the received signals at Eve from Alice and from Bob as $\mathbf{z}_A(\omega) = [z_{A,x}(\omega), z_{A,y}(\omega)]^T$, and $\mathbf{z}_B(\omega) = [z_{B,x}(\omega), z_{B,y}(\omega)]^T$, which are expressed as:

$$\mathbf{z}_A(\omega) = \varrho\cdot\mathbf{H}_{AE}(\omega)\cdot\mathbf{u}(\omega) + \boldsymbol{\epsilon}_A, \tag{5a}$$

$$\mathbf{z}_B(\omega) = \varrho\cdot\mathbf{H}_{BE}(\omega)\cdot\mathbf{u}(\omega) + \boldsymbol{\epsilon}_B, \tag{5b}$$

where $\boldsymbol{\epsilon}_A$ and $\boldsymbol{\epsilon}_B$ are the added noise contributions. ϱ denotes the tapping gain, which is determined by the specific tapping methods (e.g., the bend loss in [32]). Then, the eavesdropping

has two steps. 1) Eve uses $\mathbf{z}_A(\omega)$ and $\mathbf{z}_B(\omega)$ to estimate $\mathbf{H}_{AE}(\omega)$ and $\mathbf{H}_{BE}(\omega)$. 2) Eve reconstructs $\mathbf{H}_{AB}(\omega)$ via its estimations of $\mathbf{H}_{AE}(\omega)$ and $\mathbf{H}_{BE}(\omega)$.

It is noticed that Eqs. (5a)-(5b) are under-determined for the estimation of the 2×2 matrices $\mathbf{H}_{AE}(\omega)$ and $\mathbf{H}_{BE}(\omega)$. To overcome this, we deem $\mathbf{H}_{AE}(\omega) \approx \mathbf{H}_{AE}(\omega + \Delta_\omega)$ and $\mathbf{H}_{BE}(\omega) \approx \mathbf{H}_{BE}(\omega + \Delta_\omega)$ with a small Δ_ω. As such, Eqs. (5a)-(5b) can be re-written as:

$$[\mathbf{z}_A(\omega), \mathbf{z}_A(\omega + \Delta_\omega)] \approx \varrho \mathbf{H}_{AE}(\omega) \cdot [\mathbf{u}(\omega), \mathbf{u}(\omega + \Delta_\omega)] \tag{6a}$$

$$[\mathbf{z}_B(\omega), \mathbf{z}_B(\omega + \Delta_\omega)] \approx \varrho \mathbf{H}_{BE}(\omega) \cdot [\mathbf{u}(\omega), \mathbf{u}(\omega + \Delta_\omega)] \tag{6b}$$

Then, from Eqs. (6a)-(6b), $\mathbf{H}_{AE}(\omega)$ and $\mathbf{H}_{BE}(\omega)$ can be estimated as:

$$\hat{\mathbf{H}}_{AE}(\omega) = \frac{1}{\varrho}[\mathbf{z}_A(\omega), \mathbf{z}_A(\omega + \Delta_\omega)] \cdot [\mathbf{u}(\omega), \mathbf{u}(\omega + \Delta_\omega)]^{-1}, \tag{7a}$$

$$\hat{\mathbf{H}}_{BE}(\omega) = \frac{1}{\varrho}[\mathbf{z}_B(\omega), \mathbf{z}_B(\omega + \Delta_\omega)] \cdot [\mathbf{u}(\omega), \mathbf{u}(\omega + \Delta_\omega)]^{-1}. \tag{7b}$$

After the estimations of the Alice-Eve and Bob-Eve channels, Eve will reconstruct the channel between Alice and Bob. Given the concatenation property of fiber channels, the Alice to Bob channel can be expressed as the concatenated channels from Alice to Eve and from Eve to Bob, i.e.,

$$\mathbf{H}_{AB}(\omega) = \mathbf{H}_{EB}(\omega) \cdot \mathbf{H}_{AE}(\omega) \overset{(a)}{=} \mathbf{H}_{BE}^T(\omega) \cdot \mathbf{H}_{AE}(\omega). \tag{8}$$

where (a) is due to the channel reciprocity, i.e., $\mathbf{H}_{BE}^T(\omega) = \mathbf{H}_{EB}(\omega)$. In this view, Eve is able to reconstruct the channel between Alice and Bob by estimating $\hat{\mathbf{H}}_{AE}(\omega)$ and $\hat{\mathbf{H}}_{BE}(\omega)$, i.e.,

$$\hat{\mathbf{H}}_{AB}(\omega) = \hat{\mathbf{H}}_{BE}^T(\omega) \cdot \hat{\mathbf{H}}_{AE}(\omega) \tag{9}$$

With the help of Eq. (9), the signals received at Alice and Bob can be also reconstructed by Eve via the public pilot sequence $\mathbf{u}(\omega)$, i.e.,

$$\hat{\mathbf{r}}_A(\omega) = [\hat{r}_{A,x}(\omega), \hat{r}_{A,y}(\omega)]^T = \hat{\mathbf{H}}_{AB}^T(\omega) \cdot \mathbf{u}(\omega), \tag{10a}$$

$$\hat{\mathbf{r}}_B(\omega) = [\hat{r}_{B,x}(\omega), \hat{r}_{B,y}(\omega)]^T = \hat{\mathbf{H}}_{AB}(\omega) \cdot \mathbf{u}(\omega). \tag{10b}$$

Then, Eve is able to reconstruct the secret key between Alice and Bob, by assigning φ_E enumerating $Re[\hat{r}_{A,x}(\omega)], Im[\hat{r}_{A,x}(\omega)], Re[\hat{r}_{B,x}(\omega)]$ and $Re[\hat{r}_{B,y}(\omega)]$, and taking φ_E into Eq. (4).

3) Eavesdropping Algorithm: After the description of the eavesdropping design, we give here the detailed algorithm dealing with the discrete-time pilot sequence and received signals. The detailed algorithm is shown in Algo. 1. The inputs are (i) the discrete-time domain pilot sequence (with length K), denoted as $\tilde{\mathbf{u}} = [\tilde{\mathbf{u}}_x^H, \tilde{\mathbf{u}}_y^H]^H$ with $\tilde{\mathbf{u}}_x, \tilde{\mathbf{u}}_y \in \mathbb{C}^{1\times K}$, and (ii) the discrete-time signals received by Eve from Alice and Bob, denoted as $\tilde{\mathbf{z}}_A = [\tilde{\mathbf{z}}_{A,x}^H, \tilde{\mathbf{z}}_{A,y}^H]^H$ and $\tilde{\mathbf{z}}_B = [\tilde{\mathbf{z}}_{B,x}^H, \tilde{\mathbf{z}}_{B,y}^H]^H$ with $\tilde{\mathbf{z}}_{A,x}, \tilde{\mathbf{z}}_{A,y}, \tilde{\mathbf{z}}_{B,x}, \tilde{\mathbf{z}}_{B,y} \in \mathbb{C}^{1\times K}$. Step 1 is to transform the discrete-time signals into the frequency domain via the fast Fourier transform (FFT). Steps 2-6 are repeated for each discrete frequency domain. Step 3 is to estimate the channels from Alice to Eve and from Bob to Eve for the kth discrete frequency, i.e., $\hat{H}_{AE}[k]$ and $\hat{H}_{BE}[k]$. Step 4 is to reconstruct the channel from Alice to Bob at the kth discrete time via channel reciprocity and the cascaded property. Step 5 is to recover the received signals at Alice and Bob (in the discrete frequency domain), using the estimated channel and the public pilot sequence. Step 7 is to regenerate the shared secret key between Alice and Bob using Eq. (4). The output is then Eve's regenerated secret keys.

Algorithm 1: Eve scheme against CSI-based PL-SKG

Input: Public discrete time pilot sequence $\tilde{\mathbf{u}} = [\tilde{\mathbf{u}}_x^H, \tilde{\mathbf{u}}_y^H]^H$, and Eve received discrete time signals from Alice and Bob, i.e., $\tilde{\mathbf{z}}_A = [\tilde{\mathbf{z}}_{A,x}^H, \tilde{\mathbf{z}}_{A,y}^H]^H$ and $\tilde{\mathbf{z}}_B = [\tilde{\mathbf{z}}_{B,x}^H, \tilde{\mathbf{z}}_{B,y}^H]^H$.

1 Pursue Fourier transform on $\tilde{\mathbf{u}}$, $\tilde{\mathbf{z}}_A$ and $\tilde{\mathbf{z}}_B$, i.e., $\mathbf{u} = [\mathbf{u}_x^H, \mathbf{u}_y^H]^H$ with $\mathbf{u}_x = \text{fft}(\tilde{\mathbf{u}}_x)$ and $\mathbf{u}_y = \text{fft}(\tilde{\mathbf{u}}_y)$, $\mathbf{z}_A = [\mathbf{z}_{A,x}^H, \mathbf{z}_{A,y}^H]^H$ and $\mathbf{z}_B = [\mathbf{z}_{B,x}^H, \mathbf{z}_{B,y}^H]^H$ with $\mathbf{z}_{A,x} = \text{fft}(\tilde{\mathbf{z}}_{A,x})$, $\mathbf{z}_{A,y} = \text{fft}(\tilde{\mathbf{z}}_{A,y})$, $\mathbf{z}_{B,x} = \text{fft}(\tilde{\mathbf{z}}_{B,x})$ and $\mathbf{z}_{B,y} = \text{fft}(\tilde{\mathbf{z}}_{B,y})$;

2 **for** $k = 1, \cdots, K$ **do**

3 Compute $\hat{\mathbf{H}}_{AE}[k] = 1/\varrho[\mathbf{z}_A[k], \mathbf{z}_A[k+1]] \cdot [\mathbf{u}[k], \mathbf{u}[k+1]]^{-1}$, $\hat{\mathbf{H}}_{BE}[k] = 1/\varrho[\mathbf{z}_B[k], \mathbf{z}_B[k+1]] \cdot [\mathbf{u}[k], \mathbf{u}[k+1]]^{-1}$;

4 Reconstruct $\hat{\mathbf{H}}_{AB}[k] = \hat{\mathbf{H}}_{BE}^T[k] \cdot \hat{\mathbf{H}}_{AE}[k]$;

5 Reconstruct Alice's and Bob's received signals via pilot sequence, i.e., $\hat{\mathbf{r}}_A[k] = \hat{\mathbf{H}}_{AB}^T[k] \cdot \mathbf{u}[k]$ and $\hat{\mathbf{r}}_B[k] = \hat{\mathbf{H}}_{AB}[k] \cdot \mathbf{u}[k]$;

6 **end**

7 Regenerate secret key k_E by assigning φ_E enumerating $Re[\hat{r}_{A,x}[1:K]], Im[\hat{r}_{A,x}[1:K]], Re[\hat{r}_{B,x}[1:K]]$ and $Re[\hat{r}_{B,y}[1:K]]$, and taking φ_E into Eq. (4);

Output: Eve's regenerated secret key k_E.

C. Eavesdropping against Two-Way based PL-SKG

1) Operation of Two-way PL-SKG: In the two-way cross multiplication-based PL-SKG method, Alice and Bob send random signals to each other in two consecutive time slots, denoted by $\mathbf{v}_A(\omega); \mathbf{v}_B(\omega) \in \mathbb{C}^{2\times 1}$ in terms of the frequency domain. Then, they multiply their sent and received signals as the common feature, i.e.,

$$\begin{aligned} \psi_A &= \boldsymbol{\xi}_A(\omega)^T \cdot \mathbf{v}_A(\omega) \\ &\overset{(a)}{=} \mathbf{v}_B(\omega)^T \cdot \mathbf{H}_{AB}(\omega) \cdot \mathbf{v}_A(\omega) + \mathbf{n}_A^T \cdot \mathbf{v}_A(\omega), \\ \psi_B &= \mathbf{v}_B(\omega)^T \cdot \boldsymbol{\xi}_B(\omega) \\ &= \mathbf{v}_B(\omega)^T \cdot \mathbf{H}_{AB}(\omega) \cdot \mathbf{v}_A(\omega) + \mathbf{v}_B(\omega)^T \cdot \mathbf{n}_B, \end{aligned} \tag{11}$$

where $\boldsymbol{\xi}_A(\omega) = \mathbf{H}_{BA}(\omega) \cdot \mathbf{v}_B(\omega) + \mathbf{n}_A$ and $\boldsymbol{\xi}_B(\omega) = \mathbf{H}_{AB}(\omega) \cdot \mathbf{v}_A(\omega) + \mathbf{n}_B$ are the received signals at Alice and Bob, with $\mathbf{n}_A, \mathbf{n}_B \sim \mathcal{CN}(\mathbf{0}, \sigma_n^2 \mathbf{I}_2)$ the noise component ($\mathbf{I}_2$ is the 2×2 identity matrix). In Eq. (11), step (a) follows by taking the expression for $\boldsymbol{\xi}_A(\omega)^T$, and then replacing $\mathbf{H}_{BA}(\omega)^T$ with $\mathbf{H}_{AB}(\omega)$ using (1). As such, ψ_A and ψ_B share random and common feature $\mathbf{v}_B(\omega)^T \mathbf{H}_{AB}(\omega) \mathbf{v}_A(\omega)$. Then, the quantization method can be used to generate the shared secret key, by assigning φ_a ($a \in \{A, B\}$) enumerating

Algorithm 2: Eve scheme against two-way based PL-SKG

Input: Eve received signal from Alice and Bob, i.e., $\tilde{\boldsymbol{\zeta}}_A = [\tilde{\boldsymbol{\zeta}}_{A,x}^H, \tilde{\boldsymbol{\zeta}}_{A,y}^H]^H$ and $\tilde{\boldsymbol{\zeta}}_B = [\tilde{\boldsymbol{\zeta}}_{B,x}^H, \tilde{\boldsymbol{\zeta}}_{B,y}^H]^H$.

Take Fourier transform of $\tilde{\boldsymbol{\zeta}}_A$ and $\tilde{\boldsymbol{\zeta}}_B$, i.e., $\boldsymbol{\zeta}_A = [\boldsymbol{\zeta}_{A,x}^H, \boldsymbol{\zeta}_{A,y}^H]^H$ and $\boldsymbol{\zeta}_B = [\boldsymbol{\zeta}_{B,x}^H, \boldsymbol{\zeta}_{B,y}^H]^H$ with $\boldsymbol{\zeta}_{A,x} = \text{fft}(\tilde{\boldsymbol{\zeta}}_{A,x})$, $\boldsymbol{\zeta}_{A,y} = \text{fft}(\tilde{\boldsymbol{\zeta}}_{A,y})$, $\boldsymbol{\zeta}_{B,x} = \text{fft}(\tilde{\boldsymbol{\zeta}}_{B,x})$ and $\boldsymbol{\zeta}_{B,y} = \text{fft}(\tilde{\boldsymbol{\zeta}}_{B,y})$;

for $k = 1, \cdots, K$ **do**

  Compute feature $\psi_E[k] = \boldsymbol{\zeta}_B[k]^T \cdot \boldsymbol{\zeta}_A[k]$;

end

Regenerate secret key k_E by assigning φ_E enumerating $Re[\psi_E[1:K]]$ and $Im[\psi_E[1:K]]$ and taking φ_E into the quantization method, i.e., Eq. (4);

Output: Eve's regenerated secret key k_E.

$Re[\psi_A], Im[\psi_A], Re[\psi_B]$ and $Im[\psi_B]$, and taking φ_a into the quantization method in Eq. (4).

2) Eavesdropping Design: In this section, we expound our eavesdropping scheme, which aims to reconstruct the common feature and the secret key relying on it. Here, we assume a tapping Eve in the SMF between Alice and Bob that passively receives the random signals sent from Alice and Bob. As such, the received signals from Alice and Bob, denoted as $\boldsymbol{\zeta}_A(\omega), \boldsymbol{\zeta}_B(\omega) \in \mathbb{C}^{2\times 1}$, are:

$$\begin{aligned} \boldsymbol{\zeta}_A(\omega) &= \varrho \cdot \mathbf{H}_{AE}(\omega) \cdot \mathbf{v}_A(\omega) + \boldsymbol{\epsilon}_A, \\ \boldsymbol{\zeta}_B(\omega) &= \varrho \cdot \mathbf{H}_{BE}(\omega) \cdot \mathbf{v}_B(\omega) + \boldsymbol{\epsilon}_B. \end{aligned} \tag{12}$$

In Eq. (12), ϱ represents the tapping gain, determined by the specific tapping methods (e.g., the bend loss in [32]). $\boldsymbol{\epsilon}_A, \boldsymbol{\epsilon}_B \sim \mathcal{CN}(0, 2\sigma_n^2 \mathbf{I}_2)$ are the received noise signals from Alice and Bob respectively. Then, Eve is able to reconstruct the common feature of Alice and Bob, denoted as ψ_E, by:

$$\begin{aligned} \psi_E &= \frac{1}{\varrho^2} \cdot \boldsymbol{\zeta}_B(\omega)^T \cdot \boldsymbol{\zeta}_A(\omega) \\ &= \mathbf{v}_B(\omega)^T \cdot \mathbf{H}_{BE}(\omega)^T \cdot \mathbf{H}_{AE}(\omega) \cdot \mathbf{v}_A(\omega) + \varepsilon \\ &= \mathbf{v}_B(\omega)^T \cdot \underbrace{\mathbf{H}_{EB}(\omega) \cdot \mathbf{H}_{AE}(\omega)}_{Alice \to Eve \to Bob} \cdot \mathbf{v}_A(\omega) + \varepsilon \\ &= \mathbf{v}_B(\omega)^T \cdot \mathbf{H}_{AB}(\omega) \cdot \mathbf{v}_A(\omega) + \varepsilon \end{aligned} \tag{13}$$

where $\varepsilon \triangleq \mathbf{v}_B(\omega)^T \cdot \mathbf{H}_{BE}(\omega)^T \cdot \boldsymbol{\epsilon}_A/\varrho^2 + \boldsymbol{\epsilon}_B^T \cdot \mathbf{H}_{AE}(\omega) \cdot \mathbf{v}_A(\omega)/\varrho^2 + \boldsymbol{\epsilon}_B^T \cdot \boldsymbol{\epsilon}_A/\varrho^2$. It is compared with Eq. (11) that ψ_E and ψ_A (ψ_B) shares the same feature $\mathbf{v}_B(\omega)^T \mathbf{H}_{AB}(\omega) \mathbf{v}_A(\omega)$. This, therefore, enables Eve to reconstruct the shared secret key between Alice and Bob by assigning φ_E enumerating $Re[\psi_E]$ and $Im[\psi_E]$ and taking φ_E into the quantization method, i.e., Eq. (4).

3) Eavesdropping Algorithm: After the elaboration of the Eve design, we provide the detailed algorithm for discrete-time received signals, with details shown in Algo. 2. The inputs are the discrete-time signals received by Eve from Alice and Bob, denoted as $\tilde{\boldsymbol{\zeta}}_A = [\tilde{\boldsymbol{\zeta}}_{A,x}^H, \tilde{\boldsymbol{\zeta}}_{A,y}^H]^H$ and $\tilde{\boldsymbol{\zeta}}_B = [\tilde{\boldsymbol{\zeta}}_{B,x}^H, \tilde{\boldsymbol{\zeta}}_{B,y}^H]^H$ with $\tilde{\boldsymbol{\zeta}}_{A,x}, \tilde{\boldsymbol{\zeta}}_{A,y}, \tilde{\boldsymbol{\zeta}}_{B,x}, \tilde{\boldsymbol{\zeta}}_{B,y} \in \mathbb{C}^{1\times K}$. Step 1 is to transform the discrete-time signals into the frequency domain via the FFT. Steps 2-4 are performed for each discrete frequency. Step 3 is to construct the feature $\psi_E[k]$ via the received signals from Alice and from Bob. Step 5 is to regenerate the shared secret key between Alice and Bob by taking the constructed feature $\psi_E[1:K]$ into Eq. (4). The output is then Eve's regenerated secret keys.

IV. Numerical Simulations

In this section, we evaluate our proposed two Eve schemes via simulation. Here, two scenarios are considered: (i) the linear system provided by Eq. (1), and (ii) the nonlinear system with the Kerr effect (see Section IV. C for details). The detailed simulation configurations are provided in Table I. Here our considered fiber link between Alice and Bob includes 5 sub-channels, with the central frequency of $1.9355 \times 10^5 GHz$ and the channel spacing of 40GHz, and the central sub-channel (i.e., $1.9355 \times 10^5 GHz$) is allocated for Alice and Bob to produce the PL-SKG, and the other four sub-channels are fully filled with random data. Such an implementation is to simulate a feasible PL-SKG scheme in wavelength division multiplexing (WDM) optical fiber networks.

The simulation modules are illustrated via Fig. 1(b)-(c). In Fig. 1(b), the key generation steps at Alice and Bob are provided. Alice and Bob first create the 16-Quadrature Amplitude Modulation (16-QAM) signals via the input bits (either the public pilot bits or the random bits). Then, these signals pass the root-raised cosine (RRC) filter and frequency shift for modulation. The modulated signals are next transmitted by Tx, and received by Rx. The received signals at Alice and Bob then serve as the input of feature construction modules using Eq. (2) and Eq. (11) for CSI-based and two-way-based secret keys, respectively. After the feature construction module, secret keys at Alice and Bob can be generated by the key quantization module, i.e., Eq. (4), and further the information reconciliation and the privacy amplification modules. In our simulation, we only consider the first two steps, i.e., the feature construction that is the target of our Eve schemes attacking on, and the key quantization by which features are transformed into binary keys, to enable the evaluation of our tapping Eve designs. Fig. 1(c) illustrates the simulation flow of the SMF channel, whereby the transmitted signals from Alice (Bob) go through the N_{AE} (N_{BE}) and N_{AB} segment steps for the receiving at Eve and Bob (Alice).

With the help of the simulation setting and modules mentioned above, we evaluate our proposed Eve designs against CSI-based and two-way based PL-SKG in the following.

A. Performance of proposed Eve against CSI-based PL-SKG

We first evaluate our designed Eve against the CSI-based PL-SKG. Fig. 2 provides an illustration of the received signals at Alice and Bob, and Eve's estimated values. Three results are revealed here. First, it is observed from Fig. 2 that the received signals at Alice and at Bob are not the same but have a high correlation; whilst the normalized root mean square error (NRMSE) between $\mathbf{r}_A$ and $\mathbf{r}_B$ is approximately 0.4, the correlation coefficient of $\mathbf{r}_A$ and $\mathbf{r}_B$, i.e., $\rho_{\hat{r}_A, \hat{r}_B}$ approaches 0.87, which is similar to the result in [16]. Second, our designed Eve is able to successfully estimate the received

TABLE I
SIMULATION PARAMETERS

Parameters	**Configurations**
Fibre length between Alice and Bob	$L_{AB} = 10$ km
Number of segments between Alice and Bob	$N_{AB} = 20$
Number of segments between Alice and Eve	$N_{AE} = N_{BE} = 10$
Simulation step size	$d_z = 0.5$ km
Attenuation parameter	$att = 0.2$ dB km^{-1}
Referenced wavelength	$\lambda = 1550$ nm
Dispersion parameter at λ	$D = 17$ ps nm^{-1} km^{-1}
Rotation angle at nth segment	$\theta_n \sim \mathcal{U}[0, 2\pi)$
Phase at nth segment	$\phi_n \sim \mathcal{U}[0, 2\pi)$
Type of pilots: (i) public; (ii) random	32-Gbaud 16-QAM
Length of transmitted pilots	$K = 2^{20}$
Transmitted power	$P_t \in [-20, 10]$ dBm
Tapping gain	$\varrho = -15$ dB [32]
Average DGD parameter	$\overline{\Delta_\tau} = 8$ps, enhanced by RSPMF [16]

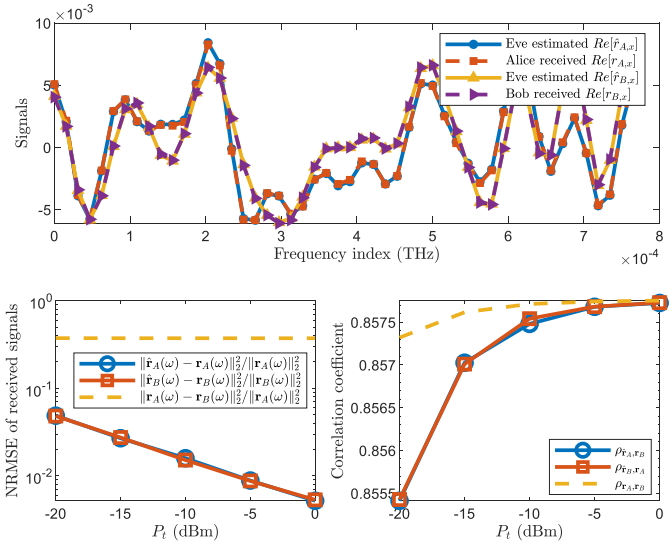

Fig. 2. Illustration of Eve's estimated Alice and Bob received signals in the CSI-based PL-SKG method. The NRMSE results show the accuracy of Eve's estimation. Also, the correlation coefficient reveals that (i) there is a high correlation between Alice's and Bob's received signals for the secret key, and (ii) there are comparable correlations between Eve's estimated Alice's received signal and Bob's received signals, which suggests that our proposed Eve has successful key reconstruction potential.

signals at Alice and Bob, respectively. This is also validated via the NRMSE of Eve's estimated received signals and the actual received signals at Alice and Bob in Fig. 2, where NRMSEs $\|\hat{\mathbf{r}}_A - \mathbf{r}_A\|_2/\|\mathbf{r}_A\|_2$ and $\|\hat{\mathbf{r}}_B - \mathbf{r}_B\|_2/\|\mathbf{r}_B\|_2$ are of the order of 10^{-2}. Third, the correlation coefficients between Eve's estimated Alice's (Bob's) received signals and the Bob's (Alice's) received signals are comparable to that between Alice and Bob, i.e., $\rho_{\hat{\mathbf{r}}_A,\mathbf{r}_B} \approx \rho_{\hat{\mathbf{r}}_B,\mathbf{r}_A} \approx \rho_{\mathbf{r}_A,\mathbf{r}_B}$. This indicates the Eve's the potential to reconstruct the CSI-based secret key between Alice and Bob and we further analyze this via Fig. 3.

In Fig. 3, we provide the key match rate versus the transmitted power P_t, for a range of different threshold parameters Eq. 4, namely $\alpha \in \{0.5, 0.2, 0.1, 0\}$. The key match rate is defined as the ratio of matched keys after the quantization over all transmitted pilots. It is seen firstly that for each fixed threshold

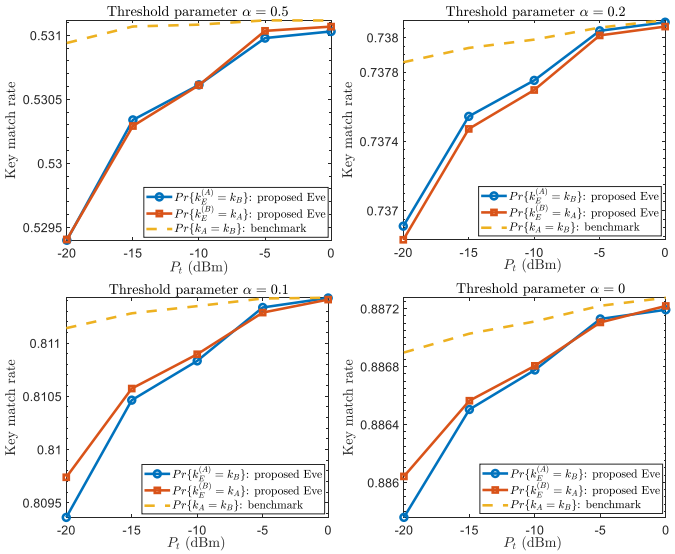

Fig. 3. Key match rate between our proposed Eve and Alice using CSI-based PL-SKG method for the range of threshold parameter values $\alpha = 0.5, 0.2, 0.1, 0$.

parameter α, all the key match rates, i.e., $Pr\{k_E^{(A)} = k_B\}$, $Pr\{k_E^{(B)} = k_A\}$ and $Pr\{k_A = k_B\}$, increase with the growth of the transmitted power P_t since this translates directly to a higher signal to noise ratio (SNR) for Alice's and Bob's received signals and Eve's estimations. Then, it is observed that with the decrease of the quantization threshold parameter α, the key match rates increase. For instance, when α decreases from 0.5 to 0.1, $Pr\{k_E^{(A)} = k_B\}$ increases from 0.52 to 0.81. This is because a larger threshold parameter α provides a higher upper-threshold γ_1 and a smaller lower-threshold γ_0, which leads to the increased number of discarded features (located within the wider threshold gap). It seems that a larger threshold gap can decrease the number of matched keys, however, it can help reduce the complexity of the further key reconciliation step. Moreover, we observe that the key match rates between Eve and Alice (Bob) are comparable to that between Alice and Bob. For example, with a fixed threshold parameter of $\alpha = 0.2$, $Pr\{k_E^{(A)} = k_B\} \approx Pr\{k_E^{(B)} = k_A\} \approx Pr\{k_A = k_B\} \approx 0.73$. This is because our designed Eve is able to estimate the channels between Alice and Bob, and subsequently reconstruct Alice's and Bob's received signals for key generation, using the known information of the public pilot sequences.

We further analyze the available key rate of CSI-based PL-SKG, in the face of our designed Eve, which is defined as $Pr\{k_A = k_B \neq k_E^{(A)} \neq k_E^{(B)}\}$, since the available keys between Alice and Bob should be (i) identical, i.e., $k_A = k_B$ and (ii) different to Eve, i.e., $k_A \neq k_E^{(A)}$ and $k_A \neq k_E^{(B)}$. In Fig. 4, it is seen that our proposed Eve can produce a reduction of almost *four* orders of magnitude in the available key rate between Alice and Bob. That means that the secret key rate in [16], [22] will reduce from $128bps$ to $0.01bps$, under our tapping Eve attacks. This is attributed to the potential of our designed Eve to estimate the channels between Alice and Bob, and subsequently reconstruct Alice's and Bob's

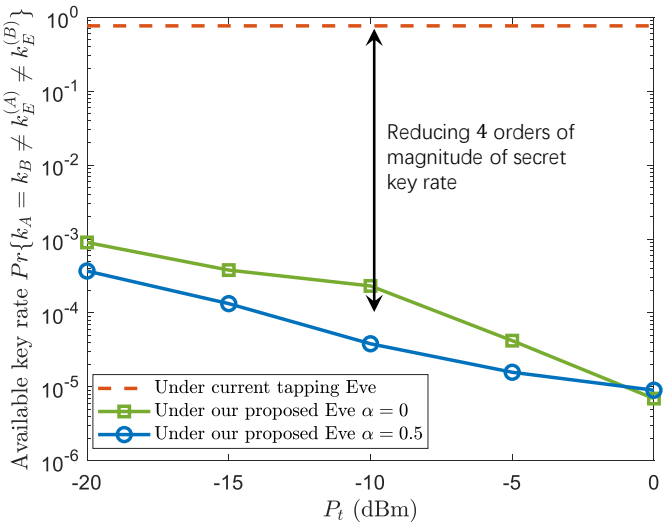

Fig. 4. Available key rate with CSI-based PL-SKG between Alice and Bob under our proposed Eve, i.e., $Pr\{k_A = k_B \neq k_E^{(A)} \neq k_E^{(B)}\}$. Almost a four-order-of-magnitude reduction in available key rate is obtained by our proposed Eve, with CSI-based PL-SKG.

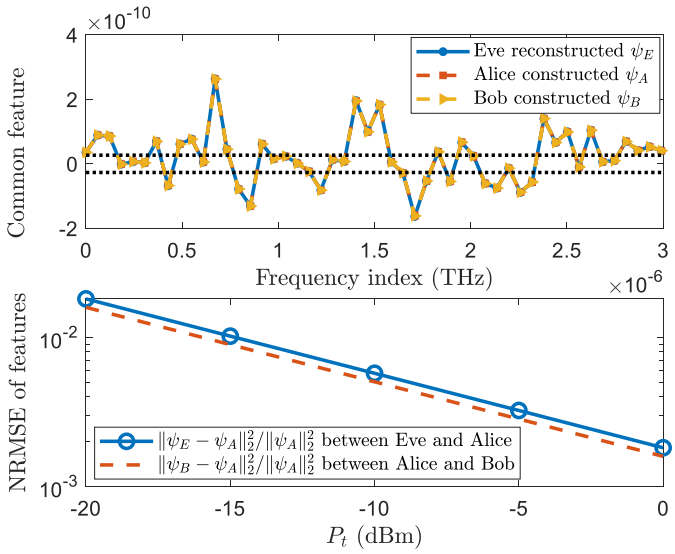

Fig. 5. Illustration of common feature reconstruction of our proposed Eve in two-way PL-SKG method, and the normalized RMSE of Eve's reconstructed features.

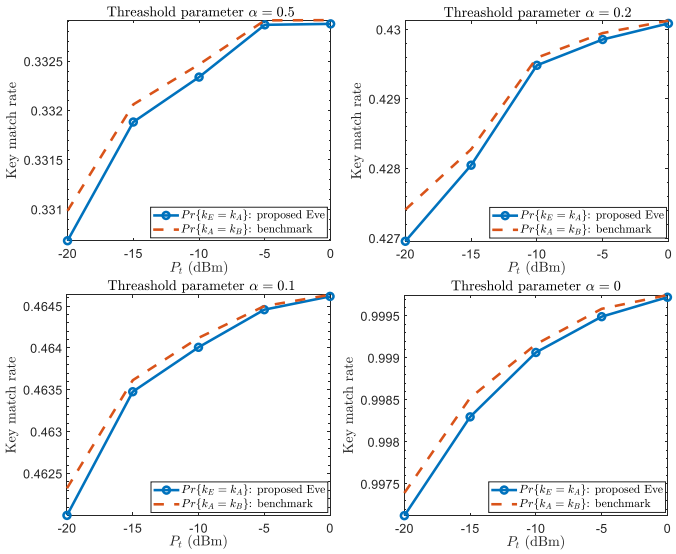

Fig. 6. Key match rate between our proposed Eve and Alice using two-way PL-SKG method with threshold parameters $\alpha = 0.5, 0.2, 0.1, 0$.

received signals for key generation, using the known public pilot sequences. As such, combining the results from Fig. 2-4, our proposed Eve demonstrates a new eavesdropping threat to CSI-based PL-SKG in fiber communications.

B. Performance of proposed Eve against two-way PL-SKG

The proposed Eve against the two-way cross multiplication-based PL-SKG is evaluated in the following. Fig. 5 provides an illustration of the features constructed at Alice and Bob, and reconstructed by our proposed Eve, i.e., ψ_A, ψ_B, and ψ_E. It is first seen that the features constructed by Alice and Bob, and reconstructed by Eve share a great commonality. This can be further validated by feature NRMSEs between Alice and Bob and between Alice and Eve, computed as $\|\psi_E - \psi_A\|_2/\|\psi_A\|_2$ and $\|\psi_B - \psi_A\|_2/\|\psi_A\|_2$, which are similar and all approach 0, matching the theoretical results by comparing Eq. (11) with Eq. (13). This, therefore, indicates our designed Eve's ability to reconstruct the secret key generated by Alice and Bob via their common features ψ_A and ψ_B.

The key match rates between Eve and Alice and between Alice and Bob are compared in Fig. 6, in which $Pr\{k_E = k_A\}$ and $Pr\{k_A = k_B\}$ versus the transmitted power P_t for a range of threshold parameters $\alpha \in \{0.5, 0.2, 0.1, 0\}$ are provided. To avoid confusion, the key match rate here is again that after the quantization step but before further IR and PA, since the quantization result serves as the seed for further key agreement and amplification processes. We first observe that given a fixed threshold parameter, e.g., $\alpha = 0.1$, both $Pr\{k_E = k_A\}$ and $Pr\{k_A = k_B\}$ increase from 0.4625 to 0.4645, as the transmitted power P_t increases from -20dBm to 0dBm. This is because a large P_t gives rise to a high SNR (i) of Alice's and Bob's constructed features, and (ii) of Eve's reconstructed feature based on its received signals from Alice and Bob. Then, it is seen that with the decrease of the threshold parameter α, $Pr\{k_E = k_A\}$ and $Pr\{k_A = k_B\}$ increase. For example, when α decreases from 0.2 to 0, $Pr\{k_E = k_A\}$ increases from 0.42 to 0.99. This is because a large threshold parameter α leads to a large upper-threshold γ_1 and a small lower-threshold γ_0, which makes the number of available keys small and thereby results in a low key match rate after quantization. Third, we observe that the key match rates between Eve and Alice (Bob) are comparable to that between Alice and Bob. For example, using a fixed threshold parameter of $\alpha = 0.1$, $Pr\{k_E = k_A\} \approx Pr\{k_A = k_B\} \approx 0.46$. This is because our designed Eve is able to reconstruct the common features of Alice and Bob via the tapped signals from Alice and from Bob, which can be theoretically validated by comparing Eq. (11) with Eq. (13).

We further analyze how much our designed Eve reduces the available key rate of Alice and Bob with two-way cross

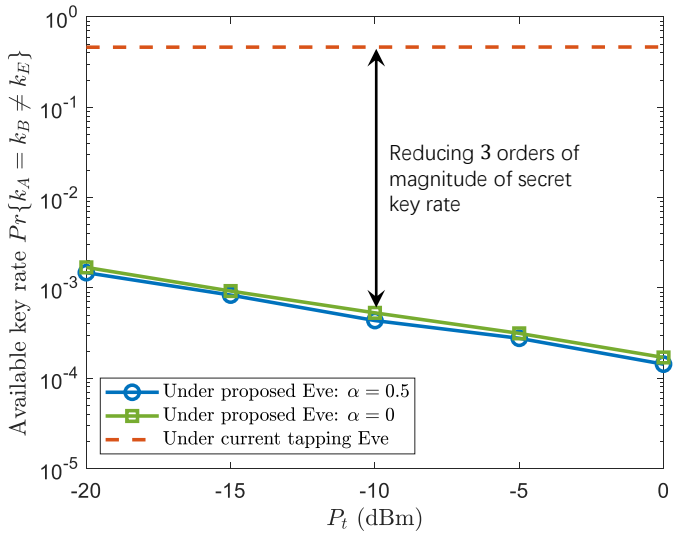

Fig. 7. Available key rate with two-way PL-SKG between Alice and Bob under our proposed Eve, i.e., $Pr\{k_A = k_B \neq k_E\}$. A three-order-of-magnitude reduction of the available key rate is obtained by our proposed Eve

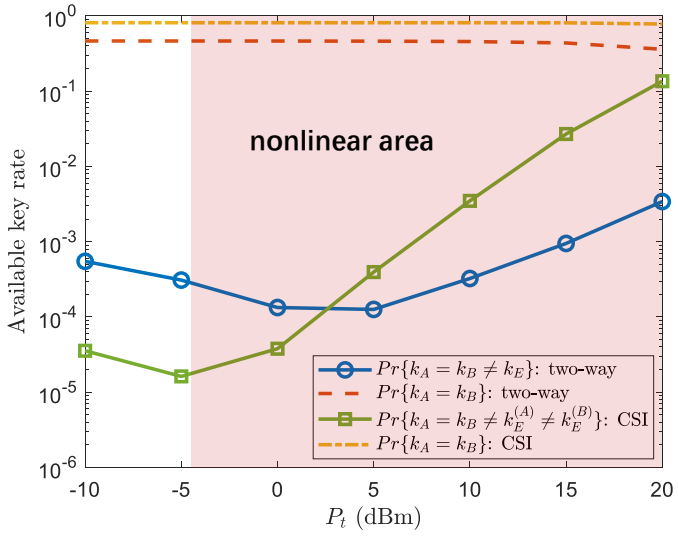

Fig. 8. Available key rate using our proposed Eve with fiber nonlinearity.

multiplication-based PL-SKG. Here, the available key rate is defined as $Pr\{k_A = k_B \neq k_E\}$, as the available keys between Alice and Bob should be (i) identical, i.e., $k_A = k_B$ and (ii) different from Eve, i.e., $k_A \neq k_E$. From Fig. 7, we can observe that our proposed Eve can reduce the available key rate between Alice and Bob by three orders of magnitude. Since the secret key rate is $\log_2 10^{66} = 220bps$ for the two-way PL-SKG in [18], our tapping Eve design can reduce it to $0.22bps$. This is attributed to the ability of our proposed Eve to reconstruct the common feature of Alice and Bob for key generation. As such, given the results from Fig. 5-7, our proposed Eve also provides a new eavesdropping threat on the two-way cross multiplication-based PL-SKG in fiber communications.

C. When encountering fiber nonlinearity

We next evaluate the performance of PL-SKGs and the designed Eve with fiber nonlinearity. The nonlinearity is induced by SPM/XPM with the nonlinear parameter taken as $\iota = 1.2$ W^{-1}km^{-1}. The channel model in Eq. (1) is modified to the split-step Fourier model [33]:

$$\begin{bmatrix} s^{(x)}_{n|n-1}(t) \\ s^{(y)}_{n|n-1}(t) \end{bmatrix} = \text{fft}\left(\mathbf{A}_n(\omega)\cdot \text{ifft}\left(\begin{bmatrix} s^{(x)}_{n-1}(t) \\ s^{(y)}_{n-1}(t) \end{bmatrix}\right)\right)$$

$$\begin{bmatrix} s^{(x)}_{n}(t) \\ s^{(y)}_{n}(t) \end{bmatrix} = \begin{bmatrix} s^{(x)}_{n|n-1}(t) \\ s^{(y)}_{n|n-1}(t) \end{bmatrix} \odot \begin{bmatrix} e^{j\eta\left(\left|s^{(x)}_{n|n-1}(t)\right|^2 + \frac{2}{3}\left|s^{(y)}_{n|n-1}(t)\right|^2\right)} \\ e^{j\eta\left(\left|s^{(y)}_{n|n-1}(t)\right|^2 + \frac{2}{3}\left|s^{(x)}_{n|n-1}(t)\right|^2\right)} \end{bmatrix} \quad (14)$$

In Eq. (14), $[s^{(x)}_n(t), s^{(y)}_n(t)]^T$ is the output signal of nth simulated fiber segment, and $[s^{(x)}_0(t), s^{(y)}_0(t)]^T$ is the fiber input. $\mathbf{A}_n(\omega) \triangleq l(\omega)\mathbf{S}(-\theta_n)diag([e^{-\frac{j}{2}(\overline{\Delta}_\tau\omega+\phi_n)}, e^{\frac{j}{2}(\overline{\Delta}_\tau\omega+\phi_n)}]\mathbf{S}(\theta_n)$ represents the PMD and CD effects. $\eta = \iota(1-e^{-att\cdot d_z})/att$ represents the nonlinear coefficient.

From Eq. (14), it may be noticed as expected that when the transmitted power P_t is large, the nonlinear effect will be enhanced. In the context of PL-SKG, such nonlinearity will destroy the channel reciprocity for both legitimate key generation and Eve's key reconstruction. We show this via Fig. 8, which plots the available key rate as a function of the transmitted power P_t. It is first observed that when our designed Eve is not present, $Pr\{k_A = k_B\}$ with both CSI-based PL-SKG and two-way cross multiplication-based PL-SKG decreases with increasing nonlinearity (increasing P_t). This is because the fiber nonlinearity destroys the channel reciprocity between Alice and Bob, which then leads to a decreased secret key rate between Alice and Bob. Then, it is seen that the nonlinearity also affects the eavesdropping ability of our proposed Eve schemes. For our designed Eve against two-way PL-SKG, the available key rate, i.e., $Pr\{k_A = k_B \neq k_E\}$ increases from an order of 10^{-4} to 10^{-2}. This is even worse for our proposed Eve against CSI-based PL-SKG, where the available key rate, i.e., $Pr\{k_A = k_B \neq k_E^{(A)} \neq k_E^{(B)}\}$ increases to 10^{-1}. This is because the non-linearity represented by Eq. (14) deteriorates the channel estimation and the feature reconstruction of Eve, which will degrade the eavesdropping performance when used in the secret key reconstruction. This is also the reason why the Eve against two-way PL-SKG scheme outperforms the Eve against CSI-based PL-SKG scheme in the non-linear region (which behaves reversely as the linear regime). The accuracy of channel estimation, which forms the basis of the CSI-based scheme, is reduced by the non-linear effects in the optical fiber. Yet, the two-way scheme does not require channel estimation. Even so, it is noticed from Fig. 8 that with our designed Eves, the available key rates are still very low (i.e., an order of 10^{-1} for CSI-based PL-SKG, and an order of 10^{-2} for two-way based PL-SKG). This thereby demonstrates the eavesdropping ability of our designed Eves, even with the fiber channel nonlinearity.

V. Conclusion

We have revealed the eavesdropping potential for the current physical layer secret key in fiber communications. Unlike

wireless communications where the randomness comes from the spatial multi-paths that cannot be all captured by Eves, in fiber communications, all the randomness (from transmitted random pilots or channel randomness) is contained in the signals transmitted in fibers. This, therefore, enables the tapping Eve to reconstruct Alice's and Bob's common features by its received signals. To implement this idea, we designed two Eve schemes against the PMD-based PL-SKG and the two-way cross multiplication-based PL-SKG. The simulation results show that our proposed Eves can successfully reconstruct the legitimate common feature and the secret key relied upon, which therefore leads to an SKR reduction of between three and four orders of magnitude in the studied PL-SKG schemes. As a result, we uncovered the novel eavesdropping potential that is unique to fiber communications, and further challenged current physical layer secret key designs. We hope this can provide a more insightful vision and critical evaluation of the design of new physical layer secret keys in optical fiber links, and provide more comprehensively secure, and intelligent optical networks.

REFERENCES

[1] 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.

[2] J. Katz and Y. Lindell, *Introduction to modern cryptography*. CRC press, 2020.

[3] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," *Reviews of modern physics*, vol. 74, no. 1, p. 145, 2002.

[4] Y. Zhang, Z. Li, Z. Chen, C. Weedbrook, Y. Zhao, X. Wang, Y. Huang, C. Xu, X. Zhang, Z. Wang *et al.*, "Continuous-variable qkd over 50 km commercial fiber," *Quantum Science and Technology*, vol. 4, no. 3, p. 035006, 2019.

[5] A. Argyris, E. Pikasis, and D. Syvridis, "Gb/s one-time-pad data encryption with synchronized chaos-based true random bit generators," *Journal of Lightwave Technology*, vol. 34, no. 22, pp. 5325–5331, 2016.

[6] C. Xue, N. Jiang, Y. Lv, and K. Qiu, "Secure key distribution based on dynamic chaos synchronization of cascaded semiconductor laser systems," *IEEE Transactions on Communications*, vol. 65, no. 1, pp. 312–319, 2016.

[7] N. Jiang, C. Xue, D. Liu, Y. Lv, and K. Qiu, "Secure key distribution based on chaos synchronization of vcsels subject to symmetric random-polarization optical injection," *Optics letters*, vol. 42, no. 6, pp. 1055–1058, 2017.

[8] W. Zhang, C. Zhang, C. Chen, H. Zhang, W. Jin, and K. Qiu, "Hybrid chaotic confusion and diffusion for physical layer security in ofdm-pon," *IEEE Photonics Journal*, vol. 9, no. 2, pp. 1–10, 2017.

[9] Y. M. Al-Moliki, M. T. Alresheedi, and Y. Al-Harthi, "Physical-layer security against known/chosen plaintext attacks for ofdm-based vlc system," *IEEE Communications Letters*, vol. 21, no. 12, pp. 2606–2609, 2017.

[10] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," *IEEE Communications Surveys Tutorials*, vol. 16, no. 3, pp. 1550–1573, 2014.

[11] J. Zhang, T. Q. Duong, A. Marshall, and R. Woods, "Key generation from wireless channels: A review," *IEEE Access*, vol. 4, pp. 614–626, 2016.

[12] C. Ye, A. Reznik, and Y. Shah, "Extracting secrecy from jointly gaussian random variables," in *2006 IEEE International Symposium on Information Theory*, 2006, pp. 2593–2597.

[13] C. Ye, S. Mathur, A. Reznik, Y. Shah, W. Trappe, and N. B. Mandayam, "Information-theoretically secret key generation for fading wireless channels," *IEEE Transactions on Information Forensics and Security*, vol. 5, no. 2, pp. 240–254, 2010.

[14] X. Wu, Y. Song, C. Zhao, and X. You, "Secrecy extraction from correlated fading channels: An upper bound," in *2009 International Conference on Wireless Communications Signal Processing*, 2009, pp. 1–3.

[15] K. Kravtsov, Z. Wang, W. Trappe, and P. R. Prucnal, "Physical layer secret key generation for fiber-optical networks," *Optics Express*, vol. 21, no. 20, pp. 23 756–23 771, 2013.

[16] I. U. Zaman, A. B. Lopez, M. A. A. Faruque, and O. Boyraz, "Physical layer cryptographic key generation by exploiting pmd of an optical fiber link," *Journal of Lightwave Technology*, vol. 36, no. 24, pp. 5903–5911, 2018.

[17] A. A. Hajomer, L. Zhang, X. Yang, and W. Hu, "Accelerated key generation and distribution using polarization scrambling in optical fiber," *Optics Express*, vol. 27, no. 24, pp. 35 761–35 773, 2019.

[18] Y. Wu, Y. Yu, Y. Hu, Y. Sun, T. Wang, and Q. Zhang, "Channel-based dynamic key generation for physical layer security in ofdm-pon systems," *IEEE Photonics Journal*, vol. 13, no. 2, pp. 1–9, 2021.

[19] Y. Bromberg, B. Redding, S. M. Popoff, N. Zhao, G. Li, and H. Cao, "Remote key establishment by random mode mixing in multimode fibers and optical reciprocity," *Optical Engineering*, vol. 58, no. 1, p. 016105, 2019.

[20] A. A. Hajomer, X. Yang, A. Sultan, and W. Hu, "Key distribution based on phase fluctuation between polarization modes in optical channel," *IEEE Photonics Technology Letters*, vol. 30, no. 8, pp. 704–707, 2018.

[21] L. Zhang, A. A. Hajomer, X. Yang, and W. Hu, "Error-free secure key generation and distribution using dynamic stokes parameters," *Optics Express*, vol. 27, no. 20, pp. 29 207–29 216, 2019.

[22] I. U. Zaman, A. B. Lopez, M. A. Al Faruque, and O. Boyraz, "Polarization mode dispersion-based physical layer key generation for optical fiber link security," in *Novel Optical Materials and Applications*. Optica Publishing Group, 2017, pp. JTu4A–20.

[23] S. N. Premnath, S. Jana, J. Croft, P. L. Gowda, M. Clark, S. K. Kasera, N. Patwari, and S. V. Krishnamurthy, "Secret key extraction from wireless signal strength in real environments," *IEEE Transactions on Mobile Computing*, vol. 12, no. 5, pp. 917–930, 2013.

[24] S. Mathur, W. Trappe, N. Mandayam, C. Ye, and A. Reznik, "Radio-telepathy: extracting a secret key from an unauthenticated wireless channel," in *Proceedings of the 14th ACM international conference on Mobile computing and networking*, 2008, pp. 128–139.

[25] G. Brassard and L. Salvail, "Secret-key reconciliation by public discussion," in *Advances in Cryptology — EUROCRYPT '93*, T. Helleseth, Ed. Berlin, Heidelberg: Springer Berlin Heidelberg, 1994, pp. 410–423.

[26] R. Impagliazzo, L. A. Levin, and M. Luby, "Pseudo-random generation from one-way functions," in *Proceedings of the twenty-first annual ACM symposium on Theory of computing*, 1989, pp. 12–24.

[27] A. Khisti, "Secret-key agreement over non-coherent block-fading channels with public discussion," *IEEE Transactions on Information Theory*, vol. 62, no. 12, pp. 7164–7178, 2016.

[28] S. Sharifian, F. Lin, and R. Safavi-Naini, "Secret key agreement using a virtual wiretap channel," in *IEEE INFOCOM 2017 - IEEE Conference on Computer Communications*, 2017, pp. 1–9.

[29] S. Zhang, L. Jin, Y. Lou, and Z. Zhong, "Secret key generation based on two-way randomness for tdd-siso system," *China Communications*, vol. 15, no. 7, pp. 202–216, 2018.

[30] G. Wunder, R. Fritschek, and K. Reaz, "Recip: Wireless channel reciprocity restoration method for varying transmission power," in *2016 IEEE 27th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)*, 2016, pp. 1–5.

[31] Z. Wei, W. Guo, and B. Li, "A multi-eavesdropper scheme against ris secured los-dominated channel," *IEEE Communications Letters*, vol. 26, no. 6, pp. 1221–1225, 2022.

[32] M. Z. Iqbal, H. Fathallah, and N. Belhadj, "Optical fiber tapping: Methods and precautions," in *8th International Conference on High-capacity Optical Networks and Emerging Technologies*. IEEE, 2011, pp. 164–168.

[33] C. Behrens, "Mitigation of nonlinear impairments for advanced optical modulation formats," Ph.D. dissertation, UCL (University College London), 2012.