High-Speed Long-Range Physical-Layer Key Distribution Assisted by Neural Networks

Xinran Huang
Department of Electronic Engineering
Shanghai Jiao Tong University
Shanghai, China
everan@sjtu.edu.cn

Liuming Zhang
Department of Electronic Engineering
Shanghai Jiao Tong University
Shanghai, China
lm.zhang@sjtu.edu.cn

Zhi Chai
Department of Electronic Engineering
Shanghai Jiao Tong University
Shanghai, China
chaizhi2021@sjtu.edu.cn

Zanwei Shen
Department of Electronic Engineering
Shanghai Jiao Tong University
Shanghai, China
n.shen@sjtu.edu.cn

Weisheng Hu
Department of Electronic Engineering
Shanghai Jiao Tong University
Shanghai, China
wshu@sjtu.edu.cn

Xuelin Yang
Department of Electronic Engineering
Shanghai Jiao Tong University
Shanghai, China
x.yang@sjtu.edu.cn

***Abstract*—We propose and demonstrate the unidirectional physical-layer secure key generation and distribution in fiber networks using neural networks, with a Gb/s key generation rate demonstrated over 100-km standard single-mode fiber.**

Keywords—secure key generation and distribution, unidirectional transmission, neural networks

I. Introduction

The growth of the information industry has witnessed the fast development of optical fiber networks. However, the optical fibers are transparent to fiber-tapping attacks and the transmitted information can be easily eavesdropped. Consequently, secure key generation and distribution (SKGD) is indispensable for data security enhancement in fiber [1]. Conventionally, SKGD is deployed at the upper layer of a network using the public-key algorithm, relying on computational complexity, which is threatened by the fast advancement of quantum computers [2].

Recently, physical-layer SKGD schemes using the unique optical feature variations in fiber have attracted much attention and could provide information-theoretic security [3-7]. They extracted secure keys from passive environmental fluctuations with a low key generation rate (KGR) less than kb/s or introduced active channel disturbing mechanism for higher KGR beyond Gb/s. Among these schemes, the key consistency was ensured by the channel reciprocity via bidirectional optical transmission. However, to increase the KGR, high-speed electro-optical modulators were applied for active channel disturbing, and the asymmetric bandwidth for bidirectional transmission may degrade the quality of channel reciprocity and limit the achievable KGR [5]. Alternatively, wideband external random sources can be distributed symmetrically to the legal users via additional fiber links, but it was not fully compatible with the current fiber infrastructure [6,7].

Here, we propose and demonstrate a unidirectional SKGD scheme using neural networks (NNs), where the channel reciprocity is reproduced by NNs. The proposed scheme alleviates the requirement of high-speed optical devices to ensure bidirectional symmetrical transmission, and long coherent time for long-range SKGD. Therefore, the proposed scheme enables high-speed and long-range SKGD. An error-free KGR of 3.8 Gb/s is experimentally demonstrated over 11 km standard single-mode fiber (SSMF). Moreover, an error-free KGR of 3.3 Gb/s is numerically simulated over 100 km SSMF.

II. Principles

The schematic diagram of the proposed SKGD scheme with unidirectional transmission using NNs is depicted in Fig. 1 [8], including three main stages: channel probing, NN training, and NN processing.

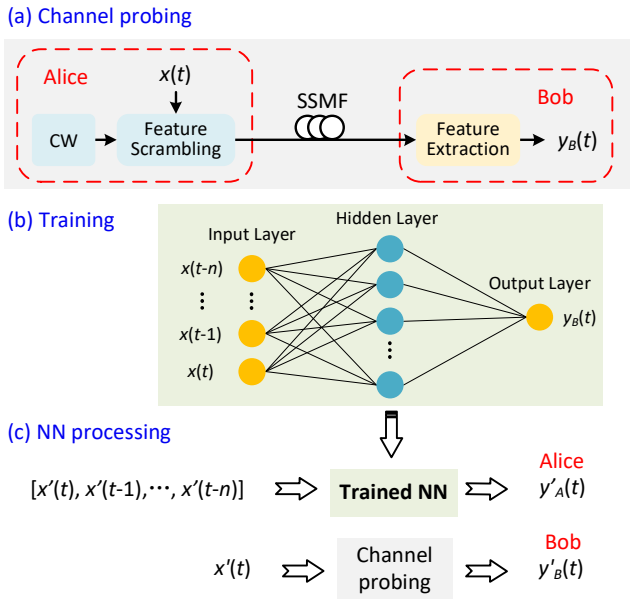

Fig. 1. Schematic diagram of the proposed SKGD scheme.

A continuous-wave laser (CW) acts as the optical carrier in the proposed SKGD scheme. A high-speed feature scrambler is placed on Alice's side to perform feature modulation, driven by the high-speed random signal $x(t)$. Afterwards, the optical signals will have random variations of optical features, such as state of polarization (SOP), optical phase, etc. After transmission over the unique fiber channel, feature extraction will be performed on Bob's side to obtain the key waveform $y_B(t)$. The channel-related key waveform $y_B(t)$ is generally uncorrelated with the driving signal $x(t)$, as revealed in reference [7]. Consequently, obtaining the unique channel response directly from the driving signal $x(t)$ to the key waveform $y_B(t)$ is quite challenging for Alice and Bob.

During the NN training, a NN is applied to reconstruct the unique channel response and acquire the channel-related key waveform $y_B(t)$ on Alice's side. The mapping from $x(t)$ to

$y_B(t)$ is learned by NN, where $x(t)$ and $y_B(t)$ are used as the input and target values.

In the NN processing, the driving signal will be updated to $x'(t)$ by Alice, and channel probing will be performed again. Meanwhile, the driving signal $x'(t)$ is input to the trained NN by Alice. Afterwards, Bob will receive an updated channel-related key waveform $y_B{}'(t)$, while Alice will obtain $y_A{}'(t)$ output by the trained NN. Thanks to the strong nonlinear characterization and fitting capabilities of the NN, the waveforms $y_A{}'(t)$ and $y_B{}'(t)$ are highly correlated and further utilized for key extraction. From the other respective, the NN simulates the transmission from the opposite direction (Bob to Alice) with the same configuration. The employment of NN reproduces the channel reciprocity and alleviates the requirement of high-speed bidirectional electro-optical devices. Resultantly, the achievable KGR only depends on the unidirectional bandwidth of the high-speed electro-optical scramblers. Moreover, the training and processing of NN are achieved via digital signal processing (DSP) and the proposed scheme is fully compatible with the current fiber infrastructure without additional fiber links.

III. Setup and Results

The experimental setup of the proposed SKGD scheme using polarization modulation is shown in Fig. 2 (a). The wavelength, linewidth, and power of the CW were 1550 nm, 100 kHz, and 10 dBm, respectively. The optical carrier was randomly modulated by a Sagnac interferometer-based polarization scrambler (SIPS) [8], whose structure is shown in Fig. 2(b). The SIPS was composed of a circulator (CIR), a polarization beam splitter (PBS), and a 10 GHz phase modulator (PM). The driving signals $x(t)$ were pseudo-random signals generated by MATLAB and loaded into the arbitrary waveform generator (AWG) with a sampling rate of 20 GSa/s. After the propagation over an 11-km SSMF, a feature extractor (FE) was utilized to obtain the key waveforms. The structure of FE is shown in Fig. 2(c), where a polarization controller (PC) was applied for SOP adjustment and a polarizer (POL) converted SOP fluctuations into intensity fluctuations via polarized light interference, and the fluctuations of the optical signals were then detected by a 10 GHz photodetector (PD). The signals were then recorded by an oscilloscope (OSC) with a sampling rate of 20 GSa/s.

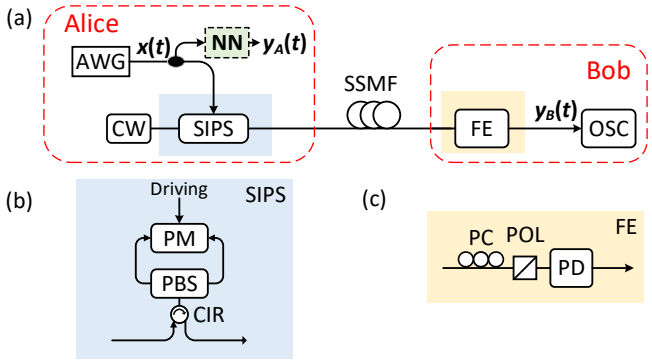

Fig. 2. (a) Experimental setup of the proposed SKGD scheme, (b) Structure of SIPS, and (c) Structure of feature extractor (FE).

On Alice's side, the key waveform $y_A(t)$ can be obtained with a trained NN. Mathematically, the key waveform $y_B(t)$ on Bob's side can be expressed as [8],

$$y_B(t) = E_x^2\cos^2\alpha + E_y^2\sin^2\alpha + n(t) + E_xE_y\sin 2\alpha\,\cos[\phi_+(t) - \phi_-(t-\tau) + \phi_{SMF}] \quad (1)$$

where E_x and E_y are the amplitudes of two orthogonally polarized components, α is the angle of POL, $\phi_+(t)$ and $\phi_-(t)$ are the phase variations induced by the PM along respectively and related to the driving signal, τ is the time delay originating from the length difference of the pigtails of PM and PBS; and ϕ_{SMF} is the phase difference of the two orthogonal polarization modes induced by the fiber channel. Specifically, the PM-induced phase variations can be expressed as [8],

$$\phi_\pm(t) = g\int_{z=0}^{L} e^{-\alpha_e z} V\left(t - \frac{L(1\pm1)}{2c_o} + \left(\pm\frac{z}{c_o} - \frac{z}{c_e}\right)\right)dz \quad (2)$$

where g is a constant, L and α_c are the length and the electrical attenuation coefficient of PM's electrode, $V(t)$ is the voltage decided by the driving signals $x(t)$, and c_o and c_e are the velocities of the optical and RF signals, respectively. According to Eq. (2), the PM-induced phase variations are integral for $x(t)$ over time of $(L/c_o + L/c_e)$. Therefore, $y_B(t)$ is a nonlinear function of $[x(t), x(t-1), \ldots, x(t-N)]$, where N is determined by $(L/c_o + L/c_e)$ and τ. Under such circumstances, the NN is utilized for the fitting of mapping from multiple inputs of $[x(t), x(t-1), \ldots, x(t-N)]$ towards a single target $y_B(t)$.

In the experiment, one million samples of $x(t)$ and $y_B(t)$ were collected and normalized to [0,1]. 90% of the samples were utilized for the NN training, where the percentages of the training set, validation set, and testing set were 70%, 15%, and 15%, respectively. The validation set was used to evaluate the network generalization, which stopped the NN training when the performance of NN was no longer improved. Once the training process stopped, the rest 10% of the samples were utilized as $x'(t)$ and $y_B{}'(t)$ for NN processing. The applied NN here was a three-layer fully connected network with one input layer, one hidden layer, and one output layer, where the number of neurons in each layer was 60, 91, and 1, respectively. The activation function was $Sigmoid(x) = 1/[1+\exp(-x)]$. The network was trained using the Levenberg-Marquardt backpropagation algorithm [9]. The mean square error (MSE) between the NN output and the target value $y_B(t)$ was utilized as the loss function in the NN training.

Meanwhile, the simulation was implemented using commercial *Optisystem15* software to evaluate the performances of the proposed scheme for long-range SKGD. In the simulation, the optical carrier was modulated using a Mach-Zender interferometer (MZI) based polarization scrambler driven by an external random signal generated by MATLAB [5]. After transmission over 100 km SSMF, the optical carrier was first amplified with an erbium-doped fiber amplifier (EDFA) with a gain of 20 dB and a noise figure of 4 dB. The other settings in the simulation were the same as those in the experiment, including the setup, the NN structure, the training and processing stages of NN.

The experimental results are presented in Fig. 3. Fig. 3 (a) shows the key waveforms measured by Alice (upper) and Bob (lower), where high similarity can be observed. Quantitively, the corresponding cross-correlation function is depicted in Fig. 3 (b), where a high CC of 0.9439 at zero

delay is obtained, verifying the feasibility of the proposed scheme.

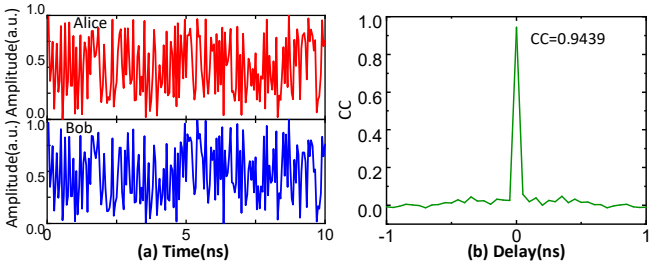

Fig. 3. Experimental results of 3.8 Gb/s KGR over 11 km SSMF, (a) Key waveforms, and (b) Cross-correlation function.

The simulation results are shown in Fig. 4. For long-range SKGD over 100 km SSMF, Alice and Bob can share highly-correlated key waveforms as depicted in Fig. 4(a). The cross-correlation function is shown in Fig. 4(b), where the peak CC at zero delay is 0.9527, verifying the feasibility of the proposed long-range SKGD.

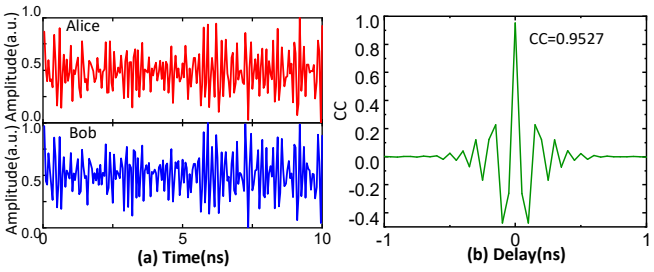

Fig. 4. Simulation of 3.3 Gb/s KGR over 100 km SSMF. (a) Key waveforms, and (b) Cross-correlation function.

IV. Key Extraction and Security Analyses

After measuring the analog key waveforms, post-processing is conducted to extract secret binary keys. During the quantization stage, a double-threshold quantizer (DTQ) converts analog key waveforms into binary key bits,

$$Q(y) = \begin{cases} 1 & \text{if } M(y) > q+ \\ 0 & \text{if } M(y) < q- \end{cases} \quad q\pm = \text{mean} \pm \varepsilon \times \text{std} \qquad (3)$$

where *mean* and *std* are the mean value and standard variation of the analog sequence M, and ε is a scalar controlling the guard interval.

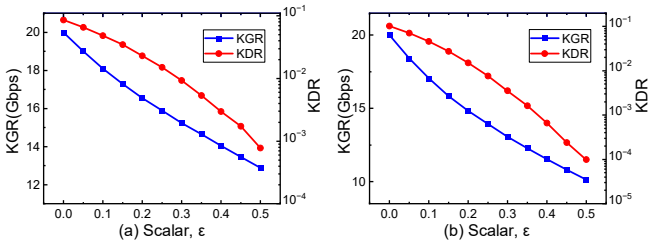

Fig. 5. KGR and KDR performance with respect to the scalar of (a) the experimental results, and (b) the simulation results.

The two critical key performances, KGR and key disagreement rate (KDR) are highly related to the scalar. The KGR and KDR performances with respect to the scalar ε are depicted in Fig. 5, where both the key performances of the experimental results and the simulation results are presented. A larger ε will lead to a lower KDR since the guard interval is enlarged. However, the KGR decreases as well since more samples are discarded. For a trade-off between KGR and KDR, $\varepsilon = 0.3$ is chosen in both the experiment and the simulation. Resultantly, KGR=15.2 Gb/s and KDR=0.92% in the experiment, and a KGR of 13.1 Gb/s with a KDR of 0.35% is obtained in the simulation.

After quantization, information reconciliation is applied, to obtain identical key bits for legal users. A (65535, 50175) Bose-Chaudhuri-Hocquenghem (BCH) code is utilized with a correction capability of 1.99% in the experiment. For the simulation, a (16383, 14202) BCH code is applied with an error correction capability of 1%. Accordingly, Alice and Bob can share error-free key bits both in the experiment and in the simulation.

Finally, the key secrecy and key randomness are further enhanced by privacy amplification. SHA3-256 algorithm with a compressive ratio of 25% is adopted here. The KGR achieved in the experiment and the simulation are 3.8 Gb/s, and 3.3 Gb/s, respectively. The randomness of the final key bits is evaluated using the National Institute of Standards and Technology (NIST) test suite with 1.5×10^6 key bits [10]. The NIST test results for both experiment results and simulation results are shown in Fig. 6. The excellent randomness of the final key bits is verified with all the returned P-values >0.01.

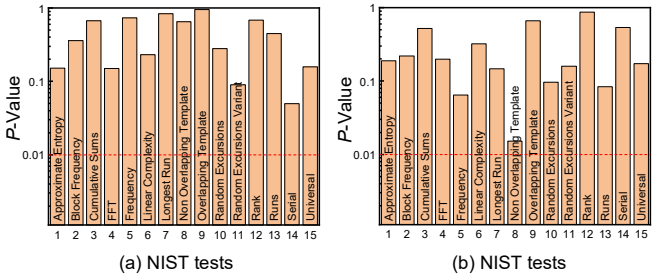

Fig. 6. NIST test results (a) Experiment of 3.8 Gb/s KGR over 11 km SSMF, and (b) Simulation of 3.3 Gb/s KGR over 100 km SSMF.

For the security of the proposed scheme, a passive eavesdropper Eve is assumed here, where she could tap into the fiber. However, due to the channel uniqueness, Eve's waveforms $y_B'(t)$ will be uncorrelated with the channel-dependent key waveforms $y_A'(t)$ and $y_B'(t)$. Meanwhile, the well-trained NN is not accessible to Eve since $x(t)$ and $y_B(t)$ are unknown to her. On the other hand, even if Eve could acquire the well-trained NN, she is unable to the correct key waveforms since $x'(t)$ is kept on Alice's side and cannot be derived from $y_E'(t)$. Therefore, the proposed scheme is robust against passive attacks.

Moreover, an active attacker Eve is considered, where she imitates Alice and tries to perform the SKGD stage shown in Fig. 1. In such a scenario, the physical-layer authentication can be applied on Bob's side to avoid such attacks [11].

V. Conclusion

We propose and demonstrate the unidirectional physical-layer SKGD scheme in fiber networks using NNs. The feasibility and robustness of the proposed scheme are verified by short-reach and long-range transmissions. An error-free KGR of 3.8 Gb/s is experimentally demonstrated over 11 km SSMF, and an error-free KGR of 3.3 Gb/s is achieved over 100 km SSMF in simulation. The proposed scheme can be a promising candidate for future high-speed long-range SKGD, to enhance data security in fiber networks.

References

[1] M. P. Fok, Z. Wang, Y. Deng, and P. R. Prucnal, ‘‘Optical layer security in fiber-optic networks,’’ *IEEE Trans. Inf. Forensic Secur.*, vol. 6, no. 3, pp. 725–736, 2011.

[2] F. Arute *et al.*, “Quantum supremacy using a programmable superconducting processor,” *Nature*, vol. 574, no. 7779, pp. 505-510, 2019.

[3] L. Zhang, A. A. E. Hajomer, X. Yang, and W. Hu, “Error-free secure key generation and distribution using dynamic Stokes parameters,” *Opt. Express*, vol. 27, no. 20, pp. 29207-29216, 2019.

[4] C. Huang, P. Y. Ma, E. C. Blow, P. Mittal, and P. R. Prucnal, “Accelerated secure key distribution based on localized and asymmetric fiber interferometers,” *Opt. Express,* vol. 27, no. 22, pp. 32096-32110, 2019.

[5] L. Zhang, A. A. E. Hajomer, W. Hu, and X. Yang “2.7 Gb/s Secure Key Generation and Distribution Using Bidirectional Polarization Scrambler in Fiber,” *IEEE Photon. Technol. Lett.,* vol. 33, no. 6, pp. 289-292, 2021.

[6] W. Shao, M. Cheng, L. Deng, *et al.*, “High-speed secure key distribution using local polarization modulation driven by optical chaos in reciprocal fiber channel,” *Opt. Lett.*, vol. 46, no. 23, pp. 5910-5913, 2021.

[7] P. Huang, Y. Chao, H. Peng, *et al.*, “Gbit/s secure key generation and distribution based on the phase noise of an amplified spontaneous emission source,” *Appl. Optics*, vol. 61, no. 7, pp. 1711-1717, 2022.

[8] L. Zhang, X. Huang, Z. Chai, Z. Shen, W. Hu, and X. Yang, “Unidirectional physical-layer key distribution in fiber assisted by neural networks,” *Opt. Lett.*, vol. 47, no. 16, pp. 4263-4266, 2022.

[9] B. M. Wilamowski, and H. Yu, “Improved computation for Levenberg-Marquardt training”, *IEEE Trans. Neural Netw.*, vol. 21, no. 6, pp. 930-937, 2010.

[10] A. Rukhin *et al.*, “A statistical test suite for random and pseudorandom number generators for cryptographic applications,” *Nat. Inst. Standards Technol.*, Washington, DC, USA, Tech. Rep. 800-22 Revision 1a, 2010.

[11] L. Kang, L. Zhang, X. Huang, W. Hu, and X. Yang, “Hardware Fingerprint Authentication in Optical Networks Assisted by Anomaly Detection,” *IEEE Photon. Tech. Lett.*, vol. 34, no. 19, pp. 1030-1033, 2022.