2.5 Gbps Error-free Physical Layer Key Distribution based on Signal Hiding over 80-km SSMF

Kongni Zhu, Yuang Li, Mingrui Zhang, Yajie Li, Yongli Zhao, Jie Zhang*

State Key Laboratory of Information Photonic and Optical Communication (IPOC), Beijing University of Posts and Telecommunications (BUPT), Beijing, China

**jie.zhang@bupt.edu.cn*

Abstract: We propose a physical layer key distribution scheme based on signal hiding and concatenated coding. Experimental results demonstrate that an error-free key can be obtained with the key generation rate of 2.5 Gbps over the 80-km standard single-mode fiber.

1. Introduction

Optical fiber communication without the secure key faces information leakage due to the long distance and complex environment, so it is urgent to seek a suitable secure key generation and distribution (SKGD) scheme. Quantum key distribution with theoretical unconditional security faces some practical challenges [1], so classical SKGD schemes have attracted attention [2–7]. Zaman et al. utilized the polarization mode dispersion effect as a randomness source to generate the key [2]. Then, an error-free SKGD scheme was proposed by combining the birefringence distribution with the state of polarization [3]. For a greater KGR, a high-speed chaotic polarized scrambler [4] and an optical chaos signal [5] was introduced. By employing amplified spontaneous emission source, an error-free key generation rate (KGR) of 10.1 Gbps was achieved over 10-km standard single-mode fiber (SSMF) [6]. On the other hand, a secure and error-free key distribution scheme using a Raman ultra-long fiber laser was researched to achieve the 500-km key distribution distance with the KGR of 100 bps [7]. However, the above schemes require the introduction of an external random source, additional device, or special structure to realized high-speed or long-range key distribution.

In this paper, we propose a SKGD based on signal hiding and concatenated coding in coherent optical system, which is compatible with the current fiber infrastructure without the pre-shared information, external random source, and additional device. By obtaining an error-free key with KGR of 2.5 Gbps over the 80-km SSMF, a record high bit rate-distance product of 200 Gbps·km is successfully achieved.

2. Scheme principles

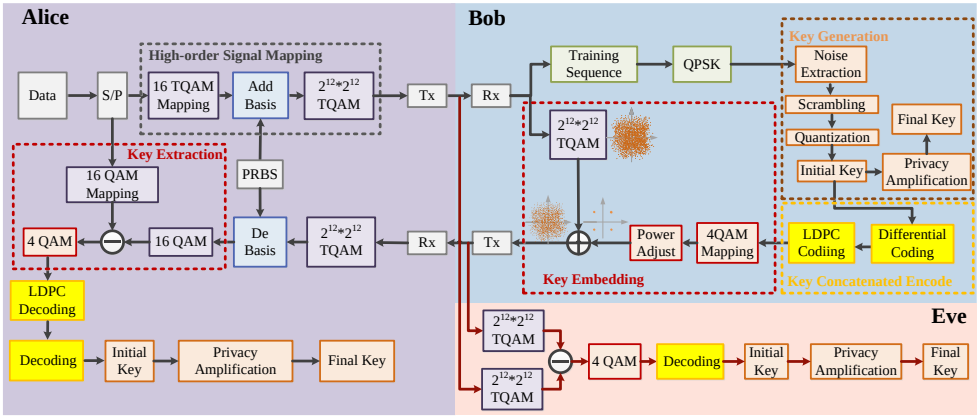


Fig. 1. The diagram of key generation and distribution scheme with signal hiding and concatenated coding.

Fig. 1 shows the diagram of the proposed SKGD scheme, which is mainly divided into four parts: high-order TQAM signal mapping, key generation, key concatenated coding including LDPC coding and differential coding, and key distribution including key embedding and extraction. We assume that Alice and Bob are legitimate parties, and Eve is an attacker who can steal signals with the best eavesdropping condition. It is worth emphasizing that only Alice knows basis states and pilot symbols, and only Bob knows the scrambling rules and quantization parameters.

(1) High-order signal mapping: According to the method of encrypting low-order signal to higher-order signal in quantum noise stream cipher (QNSC), Alice generates $2^{2+10}\times2^{2+10}$ TQAM signal with 2-bit data and 10-bit basis states in In-phase (I) and Quadrature-phase (Q) components [8], and sends it to Bob.

(2) Key generation: Bob extracts noise of system according to the received and known training sequences (TS), which is true random noise with Gaussian distribution. After scrambling and quantization, he can obtain the initial key. Because only Bob knows the scrambling rules and quantization parameters, Eve cannot get the same initial key as it of Bob.

(3) Concatenated coding: Differential coding is performed before LDPC coding for the initial key. It ensures that the incorrect key is obtained when the key error rate (KER) is higher than the FEC threshold of LDPC.

(4) Key embedding: The encoded initial key is mapped into 4 QAM, and its average symbol energy is adjusted to P_{key}. P_{key} is smaller than the average symbol energy of Bob's received TQAM signal P_{TQAM} to realize the key signal hiding, and their ratio is $R_p = P_{key} / P_{TQAM}$. Then the key signal S_{key} is embedded into the high-order TQAM signal S_{TQAM} to generate an overlapped signal ($S_{key} + S_{TQAM}$). Finally, Bob sends the overlapped signal back to Alice.

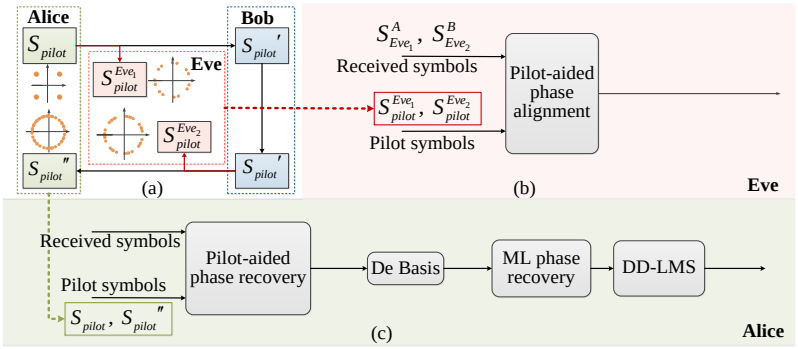
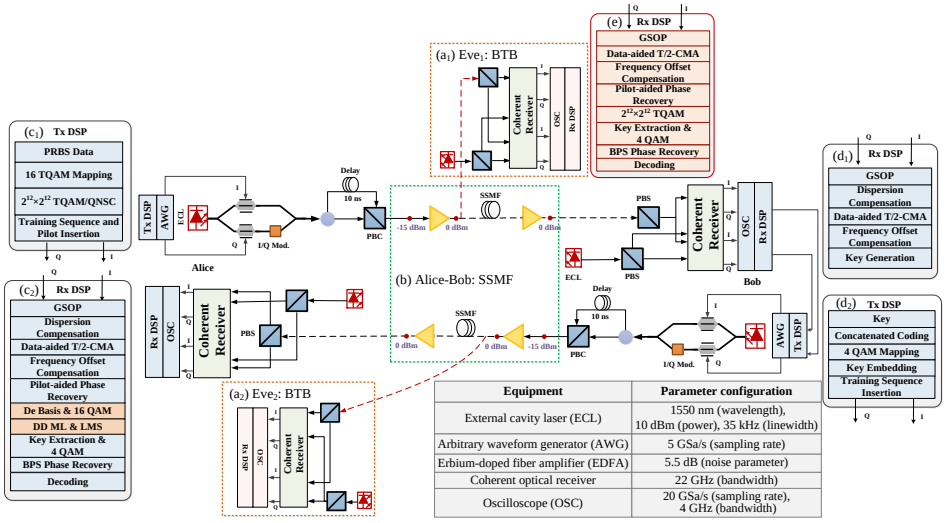


Fig. 3. (a) Pilot symbols of Alice and Eve; (b) -(c) Algorithm block diagram of Eve and Alice.

Only Alice knows pilot symbols, so Bob cannot recovery phase with pilot and Eve can only make phase alignment based on pilot symbols she received. Alice can extract the key signal from 16 QAM signals with basis states, but Eve obtains the key signal from $2^{12}\times2^{12}$ TQAM signals. The detail of recovering $2^{12}\times2^{12}$ TQAM signal to 16 QAM signal are given in [8]. Therefore, Alice can further employ some existing algorithms to process 16 QAM signal to extract key signal, but they are not effective for ultra-high-order signal, especially the signal with special modulation format. It causes the difference between Alice and Eve and ensures the security of the proposed scheme. In the proposed scheme, after recovering 16 QAM, ML carrier phase recovery (CPR) algorithm is used to eliminate the residual phase noise, and a T-spaced post decision-directed least mean square (DD-LMS) equalizer is used to compensate residual inter symbol interference and device penalty [9]. The specific processing flow is shown in Fig. 2. After extracting 4 QAM key signal, Alice implements decoding to get the error-free initial key and the final key is obtained through the privacy amplification (PA).

3. Experiments

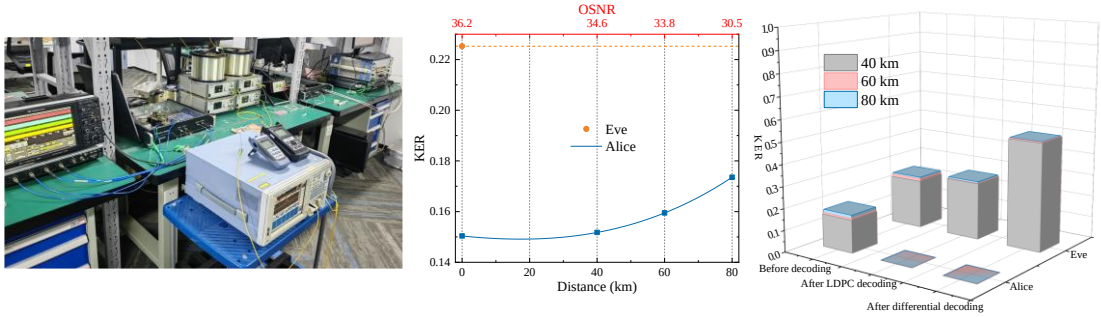


Equipment	Parameter configuration
External cavity laser (ECL)	1550 nm (wavelength), 10 dBm (power), 35 kHz (linewidth)
Arbitrary waveform generator (AWG)	5 GSa/s (sampling rate)
Erbium-doped fiber amplifier (EDFA)	5.5 dB (noise parameter)
Coherent optical receiver	22 GHz (bandwidth)
Oscilloscope (OSC)	20 GSa/s (sampling rate), 4 GHz (bandwidth)

Fig. 4. Experimental structure diagram. (a_1) -(a_2) BTB system for Eve; (b) SSMF system for Alice and Bob; (c_1) -(c_2) Alice's DSP; (d_1) -(d_2) Bob's DSP; (e) Eve's DSP

Fig. 4 shows a dual polarization coherent optical communication system over several kilometers SSMF and equipment parameters, where Eve has the best eavesdropping condition (back- to-back system) as shown in Fig. 4(a_1) and Fig. 4(a_2).

Alice generates the data by the pseudo random number generator (PRNG), and maps to a 16 TQAM signal. After adding basis, the $2^{12} \times 2^{12}$ TQAM signal is obtained. I/Q data is converted to the electrical signal by an arbitrary waveform generator (AWG) with 5 GSa/s sampling rate. The signal is loaded onto optical carrier through an I/Q modulator. Each frame includes ~3.6% pilot symbols and ~6.4% QPSK-like TS. Bob detects and captures the signal by coherent optical receiver and a real-time oscilloscope with the sampling rate of 20 GSa/s. After simple processing and key generation, the differential coding and LDPC coding with code rate $R_{LDPC} = 1/3$ is performed. Bob maps the initial key into 4 QAM, embeds it into the received signal with R_p=0.03, and sends the overlapped signal back to Alice with the same settings. Then, Alice extracts key signal with her sent and received 16 QAM signals. The DSP modules of Alice and Bob are shown as Fig. 4(c) and Fig. 4(d). Eve steals signals from both transmitters, and her DSP modules are given in Fig. 4(e). Based on experiments, KERs before decoding with different distribution distances are shown in Fig. 5(b), and Fig. 5(c) gives KERs for each stage of decoding. After decoding, Alice can get the error-free initial key but KER of Eve's initial key is ~0.5.



(a) Experimental platform (b) KER versus distance (c) KER before and after decoding

Fig. 5. Experimental platform and results.

In order to further ensure the security of key distribution, PA is performed according to Eve's KER before decoding. The amount of information obtained by Eve is $t = n \times I(B:E) = n \times (1 - H(KER_{Eve}))$, where the length of the initial key n is 1.296×10^6. The compression ratio CR for PA is $(n-t-s)/n$ with s=512. Therefore, in the 80-km SSMF system, the final KGR is

$$KGR = (1 - 6.4\%\ TS - 3.6\%\ pilot) \times (5\ GBaud \times 2\ bit/symbol \times 2\ pol.) \times R_{LDPC} \times CR/2 \approx 2.5\ \text{Gbps} \quad (1)$$

4. Conclusion

A key distribution scheme based on signal hiding and concatenated coding is studied. By embedding key into high-order TQAM signal, this scheme is realized in an optical fiber communication system. Experimental results demonstrate that an error-free key can be obtained with a KGR of 2.5 Gbps over 80-km SSMF, which achieves the highest bit rate-distance product currently. Simultaneously, the proposed scheme does not require the pre-shared information and additional device. In addition, the proposed scheme is also suitable for single-fiber bidirectional systems.

5. References

[1] E. Diamanti, et al., "Practical challenges in quantum key distribution," npj Quantum Inf. **2**(1), 16025 (2016).
[2] I. U. Zaman, et al., "Physical layer cryptographic key generation by exploiting PMD of an optical fiber link," J. Lightw. Technol. **36**(24), 5903–5911 (2018).
[3] L. Zhang, et al., "Error-free secure key generation and distribution using dynamic Stokes parameters," Opt. Express **27**(20), 29207-29216 (2019).
[4] A. Hajomer, et al., "284.8-Mb/s Physical-layer cryptographic key generation and distribution in fiber networks," J. Lightw. Technol. **39**(6), 1595-1601 (2021).
[5] Shao, Weidong, et al, "High-speed secure key distribution using local polarization modulation driven by optical chaos in reciprocal fiber channel," Opt. Lett. **46**(23), 5910-5913 (2021).
[6] X. Huang, et al, "10 Gb/s physical-layer key distribution in fiber using amplified spontaneous emission," Opt. Lett. **48**(3), 586-589 (2023).
[7] El-Taher, Atalla, et al, "Secure key distribution over a 500 km long link using a Raman ultra-long fiber laser." Laser & Photonics Reviews **8**(3), 436-442 (2014).
[8] K. Zhu, et al., "Quantum Noise Stream Cipher Scheme with Triangular Quadrature Amplitude Modulation and Secret Probabilistic Shaping," Journal of Lightwave Technology, doi: 10.1109/JLT.2023.3321103 (2023).
[9] Y. Li, et al., "Analysis of the encryption penalty in a QAM-based quantum noise stream cipher," Opt. Express **31**(12), 19006-19020 (2023).