

Article

Covert Key Generation and Distribution Based on Gain Switching Laser

Yibo Liu ¹, Huatao Zhu ^{2,*} , Feng Jiang ¹, Tong Xu ¹, Haijing Li ¹, Xin Zhang ², Shuyan Chen ³ and Shisi Chen ⁴¹ School of Information and Communication, National University of Defense Technology, Wuhan 430010, China² Faculty No. 3, Information Support Force Engineering University, Wuhan 430010, China³ 32683 Division of the PLA Joint Logistics Support Force, Wuhan 430014, China⁴ Air Force Early Warning Academy, Wuhan 430019, China

* Correspondence: zhuhuatao2008@163.com; Tel.: +86-1351-250-2156

Abstract

This article proposes and experimentally demonstrates a covert key distribution scheme based on the phase fluctuation of a gain-switched laser diode (GSLD). The gain-switched pulse is used to generate the covert signal through spectral broadening and temporal spreading. The amplified spontaneous emission (ASE) light is used to generate ASE noise in the public channel. Eavesdroppers cannot perceive signals hidden in the public noise. The experimental results show that the correlation coefficient of the key waveforms reaches 0.95, and the scheme's key generation rate (KGR) reaches 1.88 Gbit/s through a 25 km single-mode fiber (SMF). Moreover, the binary bitstreams have passed the NIST statistical test suite. The covert key distribution scheme proposed in this article provides an efficient way for the method of "one-time-pad" key distribution in high-speed optical communication systems.

Keywords: covert key distribution; physical layer security; random number generation; key extraction; optical communication; optical covert communication

1. Introduction

Optical communication has transcended the physical limitations of traditional optical fibers and has deeply integrated with artificial intelligence across multiple layers and functionalities. Optical communication security must address the inherent risk of information interception over physical channels. Therefore, encryption remains the foremost priority in ensuring the security of optical communication, with key generation and distribution forming the foundation of encrypted communication.

Key distribution encompasses classical optical key distribution and quantum key distribution. Currently, within the field of quantum key distribution, researchers have successfully implemented a non-repetitive quantum key distribution scheme that operates over a distance of 500 km using coherent light sources [1].

Classical optical key distribution exploits the inherent randomness found in the physical attributes of light pulses [2]. Properties such as intensity [3], phase [4–7], and polarization [8–10] serve as sources of random entropy for key generation. However, these methods do not effectively conceal the signals derived from the random entropy source during transmission, rendering the encrypted information susceptible to interception. If an eavesdropper intercepts the encrypted data and is knowledgeable about the encryption technique, they can easily decipher the key information.



Received: 11 June 2026

Revised: 26 June 2026

Accepted: 26 June 2026

Published: 29 June 2026

Copyright: © 2026 by the authors.

Licensee MDPI, Basel, Switzerland.

This article is an open access article distributed under the terms and conditions of the [Creative Commons Attribution \(CC BY\)](https://creativecommons.org/licenses/by/4.0/) license.

This article proposes a covert key distribution method aimed at enhancing classical key distribution systems by incorporating covert capabilities. In this method, a gain-switched laser diode (GSLD) generates covert optical pulses characterized by random phase fluctuations. These pulses possess a continuous spectrum, resulting in a low power spectral density. Consequently, the spectrum and temporal pulse transmitted through a single-mode fiber (SMF) do not attract the attention of potential eavesdroppers, thereby facilitating covert key distribution. This approach significantly improves the system's ability to remain undetected, thus achieving physical-layer covert key distribution in classical optical systems. The GSLD can produce high-repetition-rate pulsed lasers through direct modulation of the gain within the laser cavity, with pulse widths reaching tens of picoseconds. The generation of optical pulses using a GSLD is a straightforward, cost-effective, and easily adjustable method. Furthermore, the GSLD is influenced by carrier concentration, exhibits relaxation oscillation effects, and produces frequency chirping. As a result, it can generate laser pulses with a broad spectrum and wide pulse width, unconstrained by the Fourier transform limit, a characteristic that renders it highly suitable for covert communications.

We also analyze the impact of amplified spontaneous emission (ASE) noise in the public channel on the key error rate in the proposed covert key distribution scheme. A notch filter is introduced, with its bandwidth specifically designed to align with the spectrum of public optical noise. This approach represents an optimized scheme for matched filtering that effectively leverages public optical noise. We investigate the influence of matched filter bandwidth on key consistency to facilitate reliable key extraction in environments characterized by public channel noise. The covert key distribution scheme presented in this article provides an efficient method for secure, high-speed key distribution, enabling practical one-time-pad key distribution for applications such as quantum noise stream ciphers and high-speed secure optical communication.

2. Principles and Experiment Setup

Figure 1 shows the system setup of covert key distribution, which consists of a public channel and a covert channel. In the public channel, ASE noise in the optical network poses a concern. For optical bandpass filtering and optical notch filtering, a wavelength-selective switch with a 6.25 GHz slice bandwidth is used. The sample rate of the local oscillator is 2.5 GHz [11]. Two optical tunable delay lines are used for an asymmetric Mach–Zehnder interferometer. The public transmitter emits no signal. In the covert channel, a distributed feedback (DFB) laser is used to generate the GSLD optical pulse. By adjusting bias current and modulation current, the spectrum of the optical pulse becomes continuous. The optical pulse is then transmitted to a dispersive compensating fiber (DCF) for temporal spreading. An optical notch filter (ONF) is used to remove the interference of the public channel. After in-phase embedding, the covert optical pulse is combined with public optical noise. They are transmitted through a 25 km SMF, which has a dispersion of $16 \text{ ps}/(\text{nm} \cdot \text{km}) \cdot 25 \text{ km} = 400 \text{ ps}/\text{nm}$. An Erbium-doped fiber amplifier (EDFA) is employed to amplify the transmitted signal. After amplification, an optical bandpass filter (OBPF) is employed to detect covert optical pulses. In the receiver (RX), a photodiode (PD) and analog-to-digital converter (ADC) are used to convert covert signals into binary bitstreams.

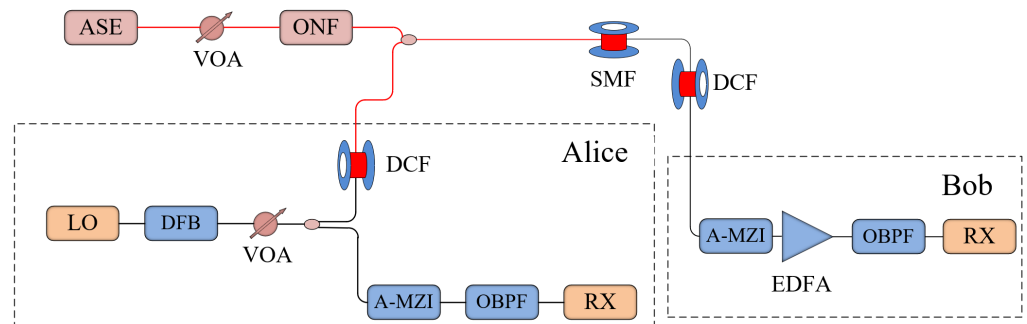


Figure 1. System setup of the covert key distribution method. LO, local oscillator; DFB, distributed feedback; VOA, variable optical attenuator; OBPF, optical bandpass filter; OC, optical coupler; A-MZI, asymmetric Mach-Zehnder interferometer; RX, receiver; ASE, amplified spontaneous emission; ONF, optical notch filter; DCF, dispersion-compensating fiber; SMF, single-mode fiber; EDFA, Erbium-doped fiber amplifier.

The carrier concentration $N(t)$, photon concentration $S(t)$, and optical phase $\theta(t)$ in the DFB laser can be described using the following rate equations [12,13]:

$$\begin{aligned}\frac{dN(t)}{dt} &= \frac{I(t)}{qV} - \frac{N(t)}{\tau_n} - \frac{v_g \alpha (N(t) - N_{tr})}{S(t)\epsilon + 1} S(t) + F_N(t) \\ \frac{dS(t)}{dt} &= \frac{v_g \alpha (N(t) - N_{tr})}{S(t)\epsilon + 1} S(t) - \frac{S(t)}{\tau_p} + \frac{N(t)\beta}{\tau_n} + F_S(t) \\ \frac{d\theta(t)}{dt} &= \frac{\gamma}{2} v_g \alpha (N(t) - \bar{N}) + F_\theta(t),\end{aligned}\quad (1)$$

$I(t)$ denotes injection current; q denotes charge of an electron; V denotes volume of the active region; τ_n denotes carrier lifetime; v_g denotes group velocity; α denotes linear material gain coefficient; ϵ denotes nonlinear gain compactness factor; N_{tr} denotes transparent carrier concentration; τ_p denotes photon lifetime; β denotes spontaneous emission factor; γ denotes line width enhancement factor; and $\bar{N}$ denotes average number of charge carriers. $F_i(t)$ uses a Langevin noise source, and spontaneous emission is taken into account. Thus, the continuous optical spectrum can be generated by adjusting the bias current and modulation current of the GSLD [14]. An optical pulse has short wavelengths and a wide spectral width. DCF spreads optical pulses in the time domain and reduces the peak amplitude of the covert pulse in the covert channel. The equation for pulse broadening by DCF is expressed as

$$\Delta T = L \frac{d^2 \beta}{d\omega^2} \Delta \omega = L \beta_2 \Delta \omega \quad (2)$$

where ΔT indicates broadening index, L indicates transmitting distance, β_2 indicates group velocity dispersion coefficient, and $\Delta \omega$ indicates optical pulse spectral width. It can be seen that the amount of optical pulse broadening is related to the spectral width of the light source and the total dispersion generated during transmission. Pulse broadening over a given transmission distance increases with the spectral width of the light source. Therefore, the optical pulse broadening can be increased by widening the spectral width of the light source, or by using DCF fibers or fiber gratings with larger dispersion to increase the amount of optical pulse broadening. In the covert key distribution system proposed in this article, the main function of the DCF is to temporally broaden the GSLD pulse. The broadened GSLD pulse is embedded at the same frequency into the ASE noise of the public channel. This allows the GSLD pulse to be hidden in the ASE noise of the public channel during transmission in the SMF in the time domain. Therefore, the optical pulse is stretched to a signal whose amplitude is similar to the amplitude of ASE noise in the public

channel. The covert optical pulse thus becomes hidden in the time–frequency domain, ensuring covertness.

3. Results and Discussion

3.1. Covertness

The covertness is proven in both the time domain and the spectrum domain. In the time domain, the waveform of the GSLD pulse is temporally spread by DCF. In the spectrum domain, the power of the spectrum is attenuated to lower the OSNR characterization. Both temporal pulse spreading via DCF and power attenuation are responsible for hiding the signal within ASE noise. Not only does DCF extend the waveform, but it also transmits the signal drowned in noise. Figure 2 shows the spectrum of the optical pulse generated by GSLD with modulation power 20 dBm and bias current 60 mA. Excessive modulation current and insufficient bias current may lead to excessive power in the spectrum. It will affect the covert performance. In addition, the spectrum of the optical pulse is located at wavelengths between 1547.0 nm and 1548.7 nm.

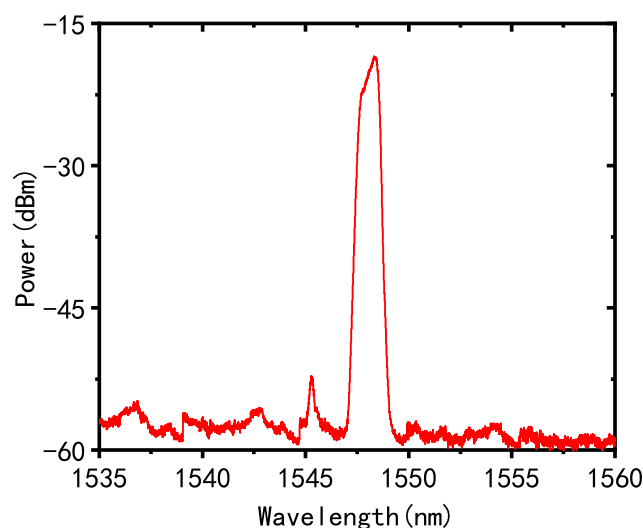


Figure 2. The spectrum of narrowband optical pulse generated by the GSLD under modulation power 20 dBm and bias current 60 mA.

Figure 3 shows the spectrum of the combined public optical noise and covert optical pulse. The covert optical pulse has a 24.5 dB attenuation using an attenuator. Excessive attenuation will make the covert optical signal undetectable after transmission. This will impact the consistency. Insufficient attenuation will lead to an excessive power spectral density of the covert optical pulse. This will impact the covertness. The public optical noise is filtered by an ONF with a center wavelength of 1547.9 nm and a 3 dB bandwidth of 150 GHz. The spectrum only shows noise characteristics for Eve, which reveals that using an attenuator can reduce the power spectrum density of the optical pulse to be similar to the public optical noise. Thereby, in the frequency domain, the covert optical pulse is hidden in public optical noise.

After eliminating the effect of polarization on the optical signal-to-noise ratio (OSNR), the formula for the OSNR can be expressed as [15]

$$OSNR = \frac{P_s}{P_n} \left(\frac{B_n}{B_r} \right) \quad (3)$$

where P_s represents the power of the covert signal, P_n represents the power of the noise of ASE noise of the public signal, B_n represents the noise equivalent bandwidth, and B_r

represents the resolution bandwidth. By overwhelming the signal with ASE noise, an OSNR of 0 dB can be achieved, and eavesdroppers cannot obtain the phase encoding. According to signal detection theory, under an additive white Gaussian noise (AWGN) channel, the eavesdropper's detection problem can be modeled as a binary hypothesis test. When OSNR = 0 dB, the signal-to-noise power ratio equals 1, and the detection probability for any non-zero false alarm probability does not exceed 0.5. This is equivalent to random guessing and cannot provide a reliable decision on the presence of a signal.

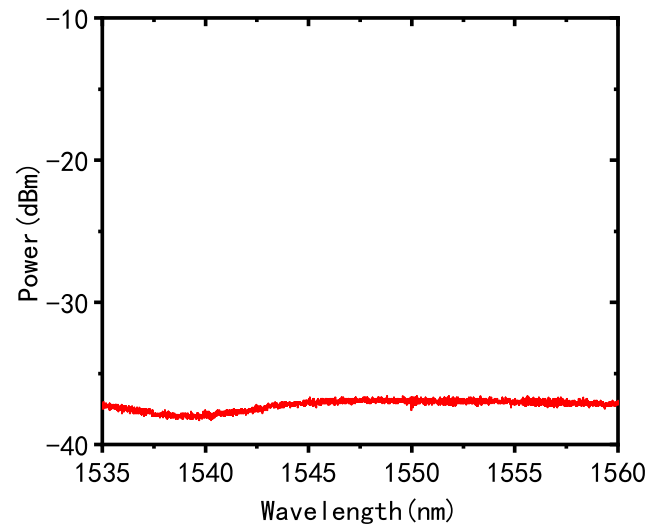


Figure 3. Spectrum of the ASE light source with a notch filter coupled after the GSLD-produced pulse attenuated by 24.5 dB.

Figure 4 shows the waveform and eye diagram of the public optical noise with pulse width 25 nm and power -7.7 dBm. Figure 5 shows the waveform and eye diagram of the combined public optical noise and covert optical pulse. After attenuating the covert optical pulse, the power of the covert optical pulse is attenuated to -19.9 dBm. The waveform and eye diagram only show noise characteristics for Eve, which reveals that using DCF can spread the waveform of the optical pulse to be similar to the public optical noise. Thereby, in the time domain, a covert optical pulse is hidden in public optical noise. In summary, the covertness of this key distribution system can be guaranteed.

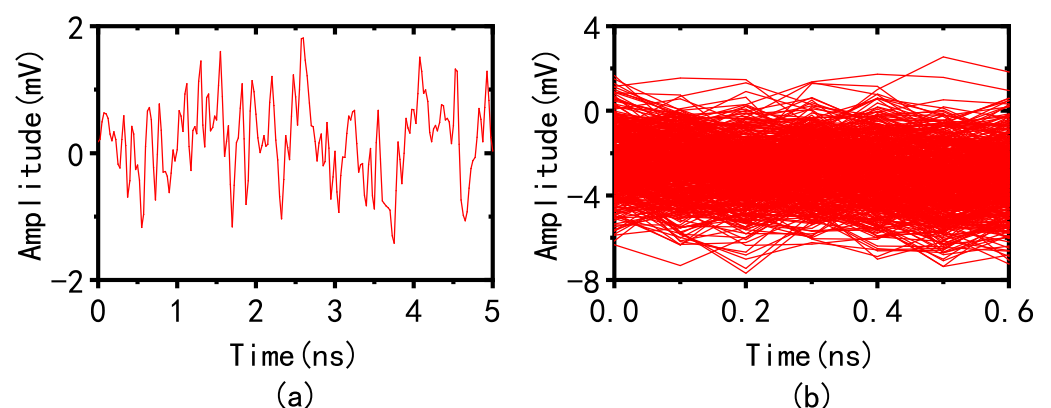


Figure 4. (a) Waveform and (b) eye diagram of ASE light source with a pulse width of 25 nm and a power of -7.7 dBm.

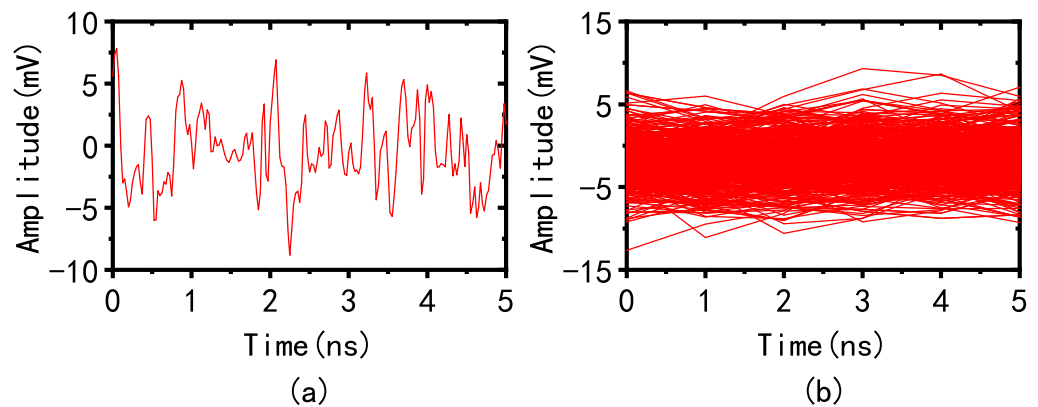


Figure 5. (a) Waveform and (b) eye diagram of the combined public optical noise and covert optical pulse.

3.2. Consistency and Randomness

After transmitting 25 km SMF and an asymmetric Mach–Zehnder interferometer (A-MZI), the power of the combined public optical noise and covert optical pulse is -24.0 dBm. An EDFA is used to amplify the combined signal and the power of the amplified signal is 0 dBm. To detect the covert optical pulse, an OBPF is used and the power of the detected covert optical pulse is -10.9 dBm. The OSNR after the dispersion-compensating fiber is 0 dB, and eavesdroppers cannot obtain the phase encoding. The OSNR after the amplifier (before the bandpass filter) is 20.5 dB, and the OSNR after the bandpass filter is 22 dB.

Figure 6 shows the waveforms of Alice and Bob after filtering out the public optical noise, while Figure 7 shows the waveforms of Alice and Bob without filtering out public optical noise. The comparison reveals that if the public optical noise is not filtered out, the noise will significantly affect the waveform of the optical pulse.

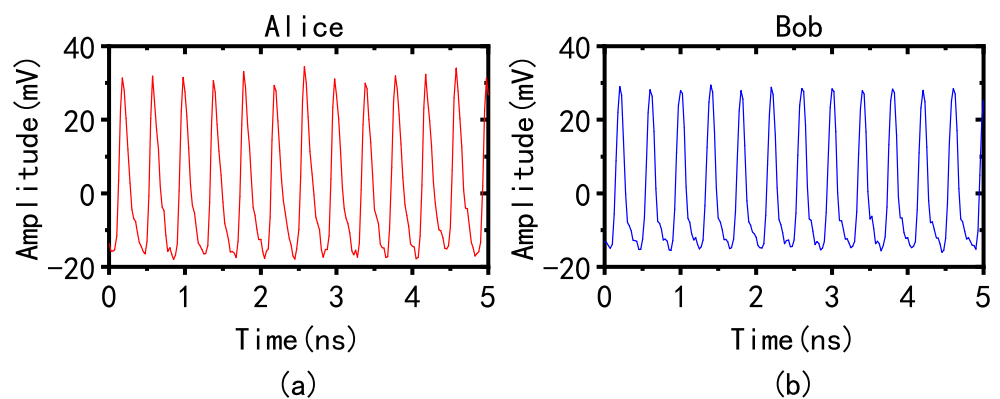


Figure 6. Waveform of (a) Alice and (b) Bob after filtering ASE noise.

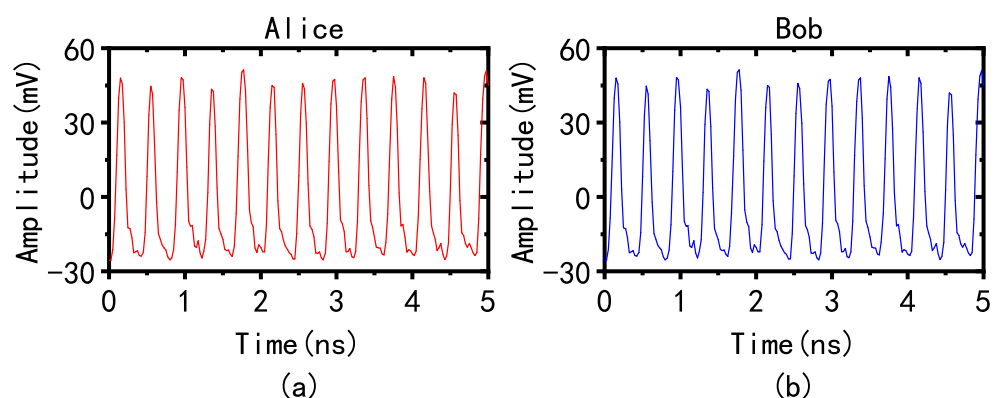


Figure 7. Waveform of (a) Alice and (b) Bob without filtering ASE noise.

Figure 8 shows the impact of introducing public optical noise on consistency from the perspective of the correlation coefficient. The correlation coefficient after filtering out public optical noise reached 0.95. At the same time, the correlation coefficient dropped from the peak value of 0.95 to 0 within a 0.4 ns time delay. Theoretically, the system's consistency is limited only by the filter's bandwidth and center wavelength.

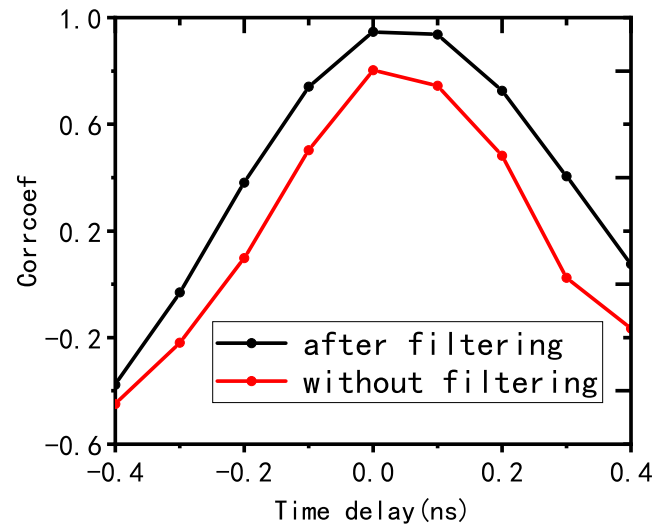


Figure 8. Consistency analysis from correlation.

In addition to the effect of public optical noise on the consistency of the key distribution system, the bandwidth of the OBPF can also affect waveform consistency. Figure 9 shows the variation in waveform consistency and Key Error Rate (KER) as the bandwidth of the OBPF changes. When the 3 dB bandwidth is less than 150 GHz, the main reason for the decrease in waveform consistency and increase in KER is the loss of a covert optical pulse. In addition to the decrease in consistency, reducing the filter bandwidth also lowers the randomness of key generation. When the filter bandwidth is greater than 150 GHz, the main reason for the decrease in waveform consistency and increase in KER is the introduction of public optical noise.

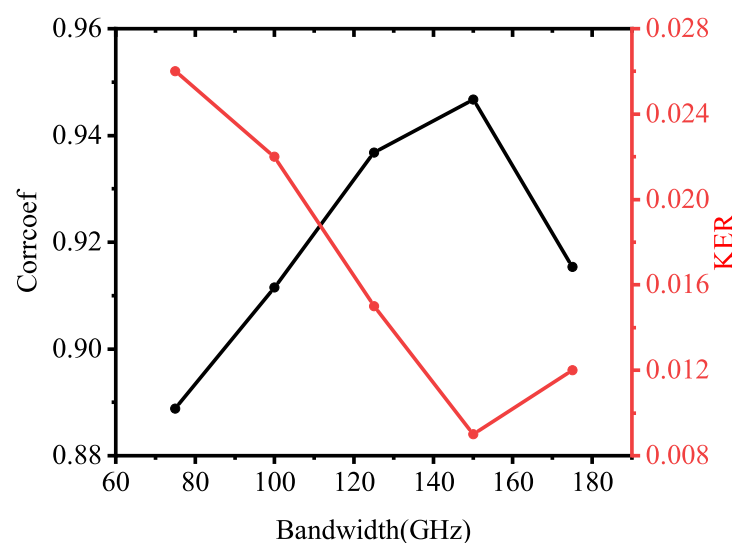


Figure 9. Curve of consistency and Key Error Rate (KER) variation with optical notch filter bandwidth.

To obtain the digitized binary bit sequence, the signals have been digitized using a double threshold quantization scheme. The signals are judged by the quantization with binary “0” and “1” as high and low threshold. The two thresholds can be expressed by

$$\begin{aligned} q_+ &= \text{mean} + \epsilon \times \text{variance} \\ q_- &= \text{mean} - \epsilon \times \text{variance} \end{aligned} \quad (4)$$

where q_+ and q_- indicates the high and low thresholds. ϵ is a scalar parameter; it decides the final value of the thresholds. By changing the value of scalar ϵ , different Key Generation Rates (KGRs) and Key Error Rates (KERs) can be acquired. Figure 10 shows how KGR and KER vary with the value ϵ . It can be seen that even if we choose a large value of ϵ , such as $\epsilon = 8$, the KGR still reaches 2.17 Gb/s, with a KER under 1%, providing a sufficient performance for post-processing steps such as information reconciliation and privacy amplification. Considering that the frequency of the phase noise reaches the THz level, the performance can be improved by employing collection devices with a wider bandwidth and a higher sampling rate. Then BCH code-based information reconciliation is performed. The code structure is set as (8191,7125), which has a correction capability of 1%. After information reconciliation, Alice and Bob share totally identical key sequences. Finally, the SHA3-256 hash function is employed in privacy amplification to remove the leaked information during reconciliation. The compressive ratio is set at 0.13 in SHA3-256. So, the final error-free KGR of 1.88 Gbit/s is achieved, which is obtained by

$$KGR_{final} = KGR_{quantization}(1 - v_{PA}) \quad (5)$$

where $KGR_{quantization} = 2.17$ Gb/s after quantization, and $v_{PA} = 0.13$ is the ratio of discarded bits in privacy amplification. Figure 11 shows the results of NIST tests performed on 5×10^5 keys randomly obtained by Bob, which verifies the randomness of the key distribution system. Figure 12 shows two indicators, CumulativeSums and Frequency, and the different test results obtained after dividing the generated binary bit key into 10 equal parts. A frequency test is used to check whether the bits ‘0’ and ‘1’ are equal. The CumulativeSums test is used to detect whether there is a systematic bias in a sequence. The results in Figure 12 indicate the randomness of the generated binary bitstreams.

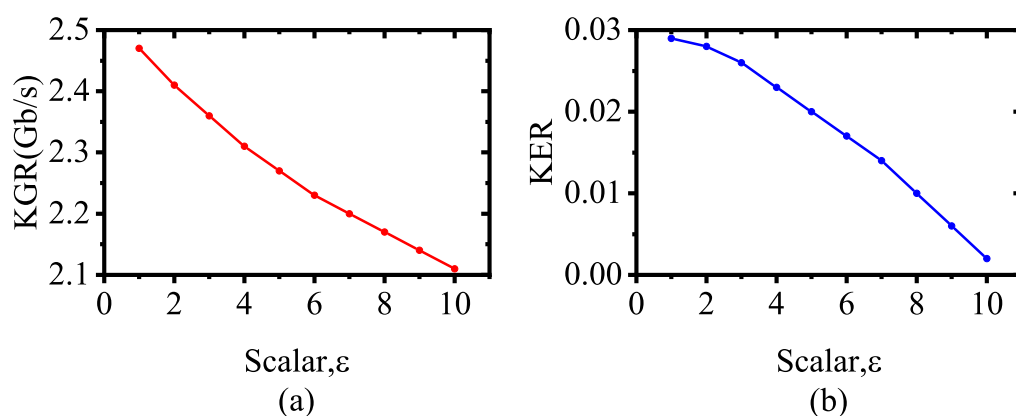


Figure 10. (a) KGR and (b) KER under different ϵ .

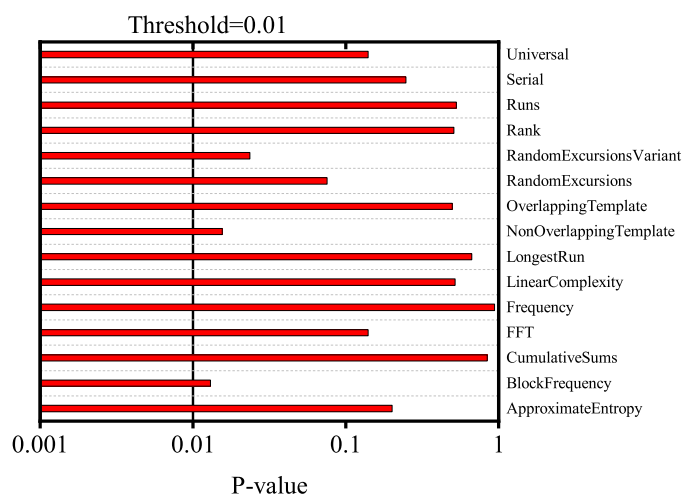


Figure 11. NIST test results under 5×10^5 bits of key.

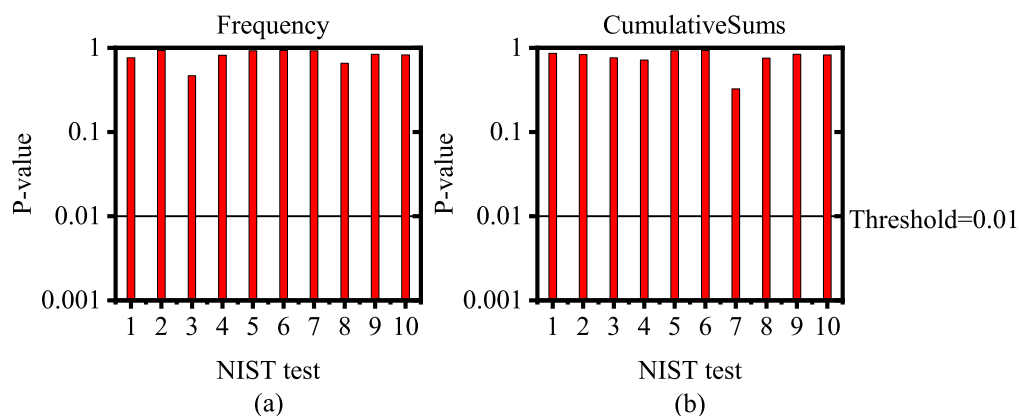


Figure 12. (a) Frequency and (b) CumulativeSums test results.

4. Conclusions

A physical-layer covert key distribution scheme is proposed and investigated in this work. The scheme focuses on quantifying its covertness based on the system's signal-to-noise power ratio. The key consistency is evaluated by considering the effects of ASE noise suppression and bandwidth. The signal, embedded with ASE optical noise, is successfully transmitted through a 25 km SMF. It demonstrates the robustness and feasibility of the proposed covert scheme in a practical public channel. Finally, the signal is post-processed with digital signal processing schemes, including BCH coding. The system delivers a final key distribution rate of 1.88 Gbit/s with a bit agreement rate of 0.95. The covert key distribution method established in this work provides an efficient way for realizing high-speed 'one-time-pad' key distribution.

Author Contributions: Conceptualization, Y.L. and H.Z.; methodology, H.Z.; software, Y.L.; validation, Y.L., H.Z. and X.Z.; formal analysis, F.J.; investigation, T.X.; resources, H.L.; data curation, S.C. (Shuyan Chen); writing—original draft preparation, Y.L.; writing—review and editing, Y.L.; visualization, S.C. (Shisi Chen); supervision, H.Z.; project administration, H.Z.; funding acquisition, H.Z. All authors have read and agreed to the published version of the manuscript.

Funding: The work was supported by the National Natural Science Foundation of China (62471472, 62301569, 12404447); Independent Innovation Fund of National University of Defense Technology (ZK24-40); and Hubei Provincial Natural Science Foundation of China (2026AFA101).

Data Availability Statement: No new data were created.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Zeng, P.; Ma, X.; Liu, H.; Chen, T.Y.; Wu, W.; Pan, J.W. Implementation of repeaterless quantum key distribution over 502 km fibers. In Proceedings of the 2020 IEEE Photonics Conference (IPC), Vancouver, BC, Canada, 28 September–1 October 2020; pp. 1–2.
2. Cui, J.; Kong, W.; Liu, Z.; Ji, Y. Dynamic Secure Key Distribution Based on Dispersion Equalization and Cellular Automata for Optical Transmission. *Photonics* **2023**, *10*, 1308. [[CrossRef](#)]
3. Nakata, K.; Tomita, A.; Fujiwara, M.; Yoshino, K.I.; Tajima, A.; Okamoto, A.; Ogawa, K. Intensity fluctuation of a gain-switched semiconductor laser for quantum key distribution systems. *Opt. Express* **2017**, *25*, 622–634. [[CrossRef](#)] [[PubMed](#)]
4. Hajomer, A.A.; Yang, X.; Sultan, A.; Hu, W. Key distribution based on phase fluctuation between polarization modes in optical channel. *IEEE Photonics Technol. Lett.* **2018**, *30*, 704–707. [[CrossRef](#)]
5. Huang, P.; Chen, Y.; Peng, H.; Xiao, Q.; Jia, B. Gbit/s secure key generation and distribution based on the phase noise of an amplified spontaneous emission source. *Appl. Opt.* **2022**, *61*, 1711–1717. [[CrossRef](#)] [[PubMed](#)]
6. Marcomini, A.; Currás-Lorenzo, G.; Rusca, D.; Valle, A.; Tamaki, K.; Curty, M. Characterising higher-order phase correlations in gain-switched laser sources with application to quantum key distribution. *Epl Quantum Technol.* **2025**, *12*, 38.
7. Lu, X.; Shi, Y.; Lin, Z.; Ren, B.; Li, J.; Lei, J. Intelligent Reflective Surface-Aided Channel Phase Probing for Physical-Layer Key Generation in Transportation Systems. *IEEE Trans. Consum. Electron.* **2024**, *70*, 7056–7065. [[CrossRef](#)]
8. Zhang, L.; Hajomer, A.A.; Hu, W.; Yang, X. 2.7 Gb/s Secure Key Generation and Distribution Using Bidirectional Polarization Scrambler in Fiber. *IEEE Photonics Technol. Lett.* **2021**, *33*, 289–292. [[CrossRef](#)]
9. Huang, X.; Chai, Z.; Li, M.; Zhang, L.; Shen, Z.; Sun, W.; Yang, X. High-Speed Random Number Generation and Key Distribution in Fiber Networks Using Amplified Spontaneous Emission. In Proceedings of the 2023 23rd International Conference on Transparent Optical Networks (ICTON), Bucharest, Romania, 2–6 July 2023.
10. Barbosa, G.A. Fast and secure key distribution using mesoscopic coherent states of light. *Phys. Rev. A* **2003**, *68*, 052307. [[CrossRef](#)]
11. Zhang, X.; Xu, X.; Zhu, H.; Chen, S.; Xu, T.; Li, F. Weak RF signals detection based on all-optical multi-mode oscillation with high performance. *Opt. Express* **2026**, *34*, 4307–4317. [[PubMed](#)]
12. Fatadin, I.; Ives, D.; Wicks, M. Numerical simulation of intensity and phase noise from extracted parameters for CW DFB lasers. *IEEE J. Quantum Electron.* **2006**, *42*, 934–941.
13. Liu, D.; Yin, Y.; Cui, M.; Liu, Z.; Zhu, H. Time-Division Multiplexed Optical Covert Communication System Based on Gain-Switched Optical Pulses. *Photonics* **2024**, *11*, 376. [[PubMed](#)]
14. Fang, J.; Qi, Y.; Liang, Y.; Zeng, H. Stable, Tunable High-Repetition-Rate Operation of Gain-Switched Semiconductor Laser via Hybrid Current-Pulse-Width Control. *Photonics* **2026**, *13*, 536.
15. Lee, J.H.; Choi, H.Y.; Shin, S.K.; Chung, Y.C. A Review of the Polarization-Nulling Technique for Monitoring Optical-Signal-to-Noise Ratio in Dynamic WDM Networks. *J. Light. Technol.* **2006**, *24*, 4162–4171.

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.