


Article

Information Leakage Rate of Optical Code Division Multiple Access Network Using Wiretap Code

Rongwo Xu, Leiming Sun, Jianhua Ji *, Ke Wang and Yufeng Song 

College of Electronics and Information Engineering, Shenzhen University, Shenzhen 518060, China; 2100432075@email.szu.edu.cn (R.X.); 2350434003@email.szu.edu.cn (L.S.); wong@szu.edu.cn (K.W.); yfsong@szu.edu.cn (Y.S.)

* Correspondence: jjh@szu.edu.cn

Abstract: Secrecy capacity is usually employed as the performance metric of the physical layer security in fiber-optic wiretap channels. However, secrecy capacity can only qualitatively evaluate the physical layer security, and it cannot quantitatively evaluate the physical layer security of an imperfect security system. Furthermore, secrecy capacity cannot quantitatively evaluate the amount of information leakage to the eavesdropper. Based on the channel model of an optical CDMA network using wiretap code, the information leakage rate is analyzed to evaluate the physical layer security. The numerical results show that the information leakage rate can quantitatively evaluate the physical layer security of an optical CDMA wiretap channel, and it is related to transmission distance, eavesdropping position, confidential information rate and optical code.

Keywords: optical CDMA; physical layer security; secrecy capacity; information leakage rate



Citation: Xu, R.; Sun, L.; Ji, J.; Wang, K.; Song, Y. Information Leakage Rate of Optical Code Division Multiple Access Network Using Wiretap Code. *Entropy* **2023**, *25*, 1384. <https://doi.org/10.3390/e25101384>

Academic Editor: T. Aaron Gulliver

Received: 22 August 2023

Revised: 13 September 2023

Accepted: 25 September 2023

Published: 26 September 2023



Copyright: © 2023 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) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

Fiber-optic communication systems are vulnerable to various types of physical layer attacks [1]. For example, an eavesdropper (Eve) can extract a portion of the transmitted signal by bending the fiber. In this way, Eve can recover the original signal and cannot be detected easily by legitimate users [2]. Quantum key distribution (QKD) can theoretically provide absolute security, but it cannot support high-speed data streams, such as a key rate of only 0.014 bps under a 833 km optical fiber transmission distance [3].

The physical layer security of fiber-optic networks is increasingly important because it guarantees the confidentiality of information without compromising the computing power of Eve, and it eliminates the key distribution and management required by traditional encryption techniques [4–7]. In 1975, Wyner proposed the wiretap channel model and secrecy capacity [8]. Secrecy capacity was defined as the maximum achievable system transmission rate at which Eve could not gain any useful information about a message. Later, it was extended to broadcast channels with confidential messages and Gaussian wiretap channels [9,10]. Kyle Guan et al. analyzed the security of space-division multiplexed fiber-optic communication systems and used distortion as a quantitative metric for secrecy. They investigated how the rate of reliable communication between the legitimate transmitter–receiver pair could be chosen to maximize reconstruction errors of Eve [11]. Then, they further analyzed the information theoretic security of multiple-input–multiple-output space-division multiplexed fiber-optic communication systems in the presence of multiple Eves [12]. Physical layer security is an important performance parameter of optical code division multiple access (OCDMA), which can improve the security of optical fiber transmission systems [13]. Yeteng Tan et al. proposed a novel secure communication scheme based on OCDMA technology, and secrecy capacity was employed to evaluate the physical layer security level [14]. The secrecy capacity of a quantum secure direct communication system was studied [15]. Andrew Lonnstrom et al. proposed a method for optimizing the information theoretic secure goodput of a multiple-input–multiple-output

degraded wiretap channel using inverse precoding [16]. In order to quantify the security of specific coding schemes, the rate distortion of multimode optical fiber communication systems was studied [17].

A wiretap code can be designed by choosing two code rates, namely, the codeword rate R_b and the rate of transmitted confidential information R_s [18]. The redundancy rate $R_e = R_b - R_s$ is used to confuse Eve. In order to ensure the reliability and security, we must ensure $R_b \leq C_B$ and $R_e \geq C_E$, where C_B and C_E are the main channel capacity and the wiretap channel capacity, respectively. When the main channel is better than the wiretap channel, secrecy capacity is defined as $C_S = C_B - C_E$, which is the difference between the main channel capacity and the wiretap channel capacity. Secure communication can be achieved as long as $R_s \leq C_S$.

However, for a long-distance fiber-optic communication system, when Eve is close to the transmitter, Eve can obtain a higher signal-to-noise ratio (SNR) than the legitimate users. Although we can reduce the channel capacity of Eve by sending artificial noise [19], the system still cannot guarantee the physical layer security. On the other hand, because Eve's location is unknown, there are several different cases of security in the whole communication link. (1) $C_S \geq R_s$: in this case, the communication system can achieve perfect security. (2) $0 < C_S < R_s$: in this case, some confidential information is leaked to Eve. (3) $C_S = 0$: in this case, Eve can obtain all the confidential information. Therefore, secrecy capacity can only qualitatively evaluate the physical layer security under perfect security conditions; it cannot quantitatively evaluate the physical layer security under imperfect security conditions. Moreover, secrecy capacity cannot quantitatively evaluate the information leakage.

In this paper, we investigate the information leakage rate of an OCDMA network using wiretap code. The rest of this paper is organized as follows: In Section 2, we propose the channel model of the OCDMA network using wiretap code and theoretically analyze the information leakage rate of the fixed-rate wiretap code. The numerical results and discussions will be given in Section 3. The conclusion will be given in Section 4.

2. System Model and Theoretical Analysis

Figure 1 depicts the channel model based on OCDMA using wiretap code. At the transmitter, Alice outputs confidential information M , which is encoded by a wiretap channel encoder and an OCDMA encoder. Then, an n -vector X^n is transmitted through the fiber channel. The length of the fiber link is L , and the legitimate user Bob receives Y^n . After using a matched OCDMA decoder and optically amplified receiver (OAR), Bob can recover confidential information via the wiretap channel decoder. On the other hand, Eve intends to obtain useful information at extraction location l with an extraction ratio x . According to Kerckhoffs's principle [20], Eve knows the data rate, coding type and code length, but does not know the specific optical code used by the legitimate user. Hence, Eve receives Z^n and can only use an unmatched OCDMA decoder. The wiretap system adopts random coding. The confidential information rate is $R_s = H(M)/n$, where $H(M)$ is the entropy of M . The codeword rate is $R_b = H(X^n)/n$, where $H(X^n)$ is the entropy of X^n . The wiretap code is constructed by generating 2^{nR_b} codewords. For each message $u = \{1, 2, 3, \dots, 2^{nR_s}\}$, we randomly select one codeword from $v = \{1, 2, 3, \dots, 2^{n(R_b - R_s)}\}$. The OCDMA encoder uses optical orthogonal code $(F, W, 1, 1)$, where F is the code length, W is the code weight and the autocorrelation and cross-correlation limits are 1.

At the receiver, OAR includes an erbium-doped fiber amplifier (EDFA), an optical filter, a photodiode, a low-pass electrical filter (LPF) and a decision circuit, as shown in Figure 2. In this system, the noise mainly includes shot noise, signal-spontaneous beat noise, spontaneous-spontaneous beat noise, thermal noise and dark current noise.

At the transmitter, P is the optical power of chip "1" after the OCDMA encoder. The optical fiber attenuation coefficient is a , and the chip power P_l at the position l is [21]

$$P_l = \frac{P}{10^{al/10}} \quad (1)$$

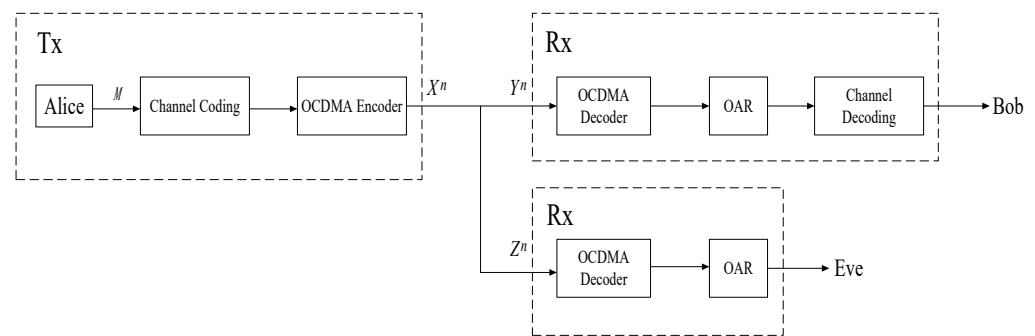


Figure 1. Channel model based on OCDMA using wiretap code.

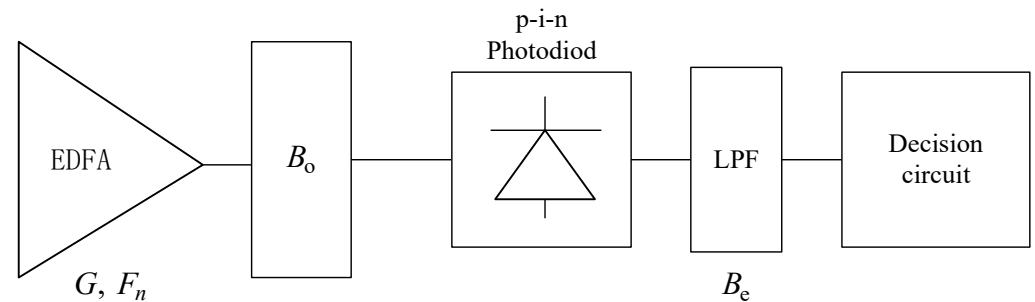


Figure 2. Model of optical amplifier receiver.

Because Eve adopts an unmatched decoder, the cross-correlation value of optical orthogonal code is 1. Therefore, the optical power of Eve's receiver is

$$P_{Eve} = xP_l \quad (2)$$

The legitimate user adopts a matched decoder, and the autocorrelation peak value of optical orthogonal code is W . Hence, the optical power of Bob's receiver is

$$P_S = (1 - x) \frac{WP}{10^{\alpha L/10}} \quad (3)$$

When the user data are "1", the mean current value and the total noise are expressed as [22]

$$I_{m1} = R_c(GP_S + P_{ASE}) \quad (4)$$

$$\begin{aligned} \sigma_{m1}^2 &= \sigma_{sh1}^2 + \sigma_{s-sp1}^2 + \sigma_{sp-sp}^2 + \sigma_{th}^2 + \sigma_d^2 \\ &= 2eB_eR_c(GP_S + P_{ASE}) + 2\frac{B_e}{B_o}GR_c^2P_S P_{ASE} + \frac{B_e}{B_o}(R_cP_{ASE})^2(2B_o - B_e) \\ &\quad + (4k_B T/R)B_e + 2eI_d B_e \end{aligned} \quad (5)$$

where R_c is the receiver responsivity, B_o is the optical bandwidth, G is the amplifier gain, e is electron charge and N_{sp} is the spontaneous radiation factor. Amplified spontaneous radiation noise power is $P_{ASE} = 2h\nu N_{sp}(G - 1)B_o$ and R is the receiver load resistance. Photodetector bandwidth $B_e = (3/4)FR_b$, T is the temperature, k_B is Boltzmann constant and I_d is dark current.

When the user data are "0", the mean current value and the total noise are expressed as [22]

$$I_{m0} = R_cP_{ASE} \quad (6)$$

$$\begin{aligned} \sigma_{m0}^2 &= \sigma_{sh0}^2 + \sigma_{sp-sp}^2 + \sigma_{th}^2 + \sigma_d^2 \\ &= 2eB_eR_cP_{ASE} + 2\frac{B_e}{B_o}GR_c^2P_S P_{ASE} + \frac{B_e}{B_o}(R_cP_{ASE})^2(2B_o - B_e) \\ &\quad + (4k_B T/R)B_e + 2eI_d B_e \end{aligned} \quad (7)$$

The bit error rate (BER) of legitimate users can be calculated by

$$P_e = \frac{1}{2} \operatorname{erfc}\left(\frac{Q}{\sqrt{2}}\right) \approx \frac{\exp(-Q^2/2)}{Q\sqrt{2\pi}} \quad (8)$$

where $Q = (I_{m1} - I_{m0}) / (\sigma_{m1} + \sigma_{m0})$, $\operatorname{erfc}()$ is the complementary error function. Similarly, Eve's BER can be calculated.

It is assumed that the probability of user data being "0" and "1" is equal, and the channel is simplified to a binary symmetric channel model with an error transmission probability P_e , as shown in Figure 3.

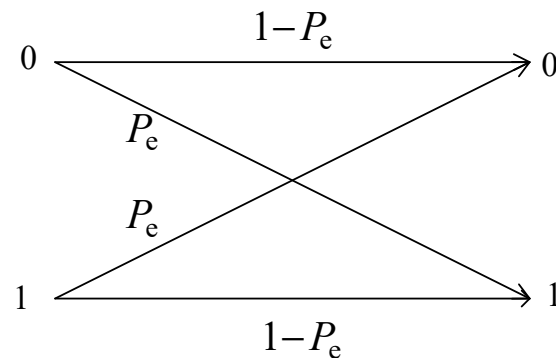


Figure 3. Binary symmetric channel model.

The main channel capacity is

$$C_B = \max\{I(X^n; Y^n)\} = 1 - h(P_e) \quad (9)$$

where $h(P_e) = -P_e \log(P_e) - (1 - P_e) \log(1 - P_e)$. After calculating the BER of Eve, the channel capacity of Eve can also be obtained.

Partial secrecy is usually quantified by the equivocation. In this paper, we use fractional equivocation, which is defined as [10]

$$\Delta = \frac{H(M|Z^n)}{H(M)} \quad (10)$$

$H(M|Z^n)$ is denoted as the entropy of residual uncertainty at Eve. Therefore, in a partial secrecy scenario, the maximum achievable fractional equivocation can be obtained from the following equation [23]:

$$\Delta = \begin{cases} 1, & \text{if } C_E \leq C_B - R_s \\ \frac{C_B - C_E}{R_s}, & \text{if } C_B - R_s < C_E < C_B \\ 0, & \text{if } C_B \leq C_E \end{cases} \quad (11)$$

Given the transmission rate of confidential information R_s , the information leakage rate can be obtained [23]:

$$R_L = \frac{I(M; Z^n)}{n} = (1 - \Delta)R_s \quad (12)$$

Hence, the lower bound of the information leakage rate is obtained:

$$R_L = \begin{cases} 0, & \text{if } C_E \leq C_B - R_s \\ h(P_m) - h(P_w) + R_s, & \text{if } C_B - R_s < C_E < C_B \\ R_s, & \text{if } C_B \leq C_E \end{cases} \quad (13)$$

Here, P_m and P_w are the BER of Bob and Eve, respectively. The lower bound of the information leakage rate of Equation (13) represents the minimum secret information which is obtained by Eve.

3. Numerical Result and Discussion

In this section, we use MATLAB software for numerical analysis. The system parameters are as follows: The extraction ratio is 1%, the bit rate is 10 Gbit/s, the optical wavelength is 1550 nm, the EDFA gain $G = 20$ dB, the EDFA noise index $F_n = 5$ dB, $B_o = 62.43$ GHz, $B_e = 52.5$ GHz, $R_c = 0.8$ A/W, $\alpha = 0.2$ dB/km, $I_d = 2$ nA, $T = 300$ K and $R = 50 \Omega$. Legitimate users use optical orthogonal code (7,2,1,1). In order to meet the reliability requirement, the transmitted power must be designed to ensure Bob's BER $\leq 10^{-9}$. In this case, the channel capacity of legitimate users is close to 1 bit/symbol.

Figure 4 shows the relationship between the secrecy capacity, information leakage rate and the eavesdropping distance of Eve. The transmission distance of Alice and Bob is 100 km, $R_b = C_B$ and $R_s = 0.9R_b$. With the increase in the eavesdropping distance, the SNR of Eve will deteriorate. Hence, the secrecy capacity gradually increases. As can be seen from Figure 4, when the eavesdropping distance is 62 km, $C_S = R_s$. In a $[0, 62]$ km link, $C_S \leq R_s$, Eve can obtain some confidential information. In a $[62, 100]$ km link, $R_s \leq C_S$, Eve will not obtain any information. Therefore, the secrecy capacity can only qualitatively describe which link segment is secure and which link segment is insecure, and cannot quantitatively evaluate the security of the whole link.

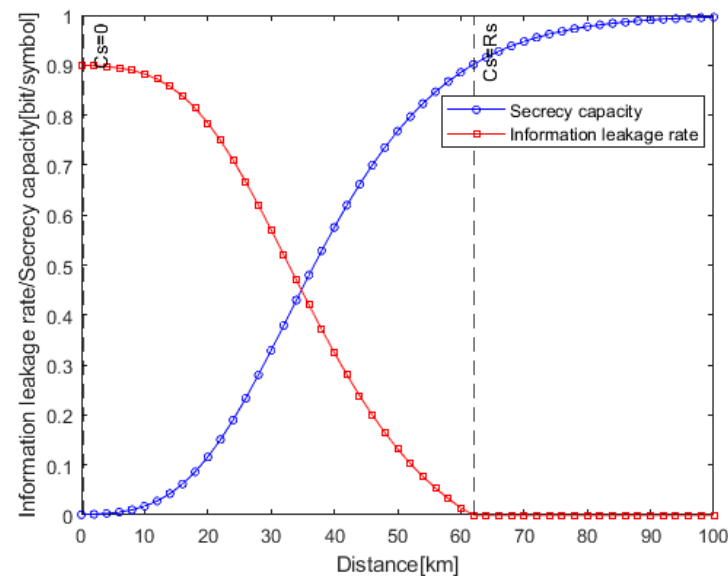


Figure 4. Relationship between secrecy capacity, information leakage rate and eavesdropping distance ($R_s = 0.9R_b$, $P_m = 10^{-9}$, OOC (7,2,1,1)).

In a fiber-optic communication system, it is generally impossible to guarantee that the whole link has perfect security. Therefore, it is necessary to use the information leakage rate to quantitatively evaluate physical layer security in imperfect secure links. As can be seen from Figure 4, with the increase in the eavesdropping distance, the information leakage rate remains unchanged at first, then gradually decreases, and finally reduces to zero. In the $[0, 0.2]$ km link, the information leakage rate is equal to R_s , which corresponds to secrecy capacity of 0. This distance is defined as the complete interception distance. At this time, Eve can obtain all the confidential information. In the $[0.2, 62]$ km link, the information leakage rate is less than R_s , which means that some confidential information is leaked to Eve. Hence, this distance is defined as the partial interception distance. In the $[62, 100]$ km link, the information leakage rate is equal to 0, which means that the secrecy capacity is no less than R_s . At this point, the link is perfectly secure, and no confidential information is leaked to Eve. This distance is defined as the safe transmission distance.

By calculating the information leakage rate of different eavesdropping distances, the physical layer security of the whole link can be quantitatively evaluated. For example,

R_L will be 0.784 bit/symbol, 0.57 bit/symbol and 0.324 bit/symbol for eavesdropping distances of 20 km, 30 km and 40 km, respectively.

Figure 5 is the information leakage rate under different optical orthogonal codes. It is shown that the information leakage rate of OOC (7,3,1,1) is lower than that of OOC (7,2,1,1). The reason for this is that, whether using OOC (7,3,1,1) or OOC (7,2,1,1), Eve can only obtain one chip pulse by using an unmatched decoder. The legitimate user can obtain three chip pulses by using OOC (7,3,1,1), while it can obtain two chip pulses by using OOC (7,2,1,1). Therefore, by using OOC (7,3,1,1), Alice can achieve reliable transmission at lower chip power. This reduces Eve's receiving power, resulting in a decrease in the eavesdropping channel capacity.

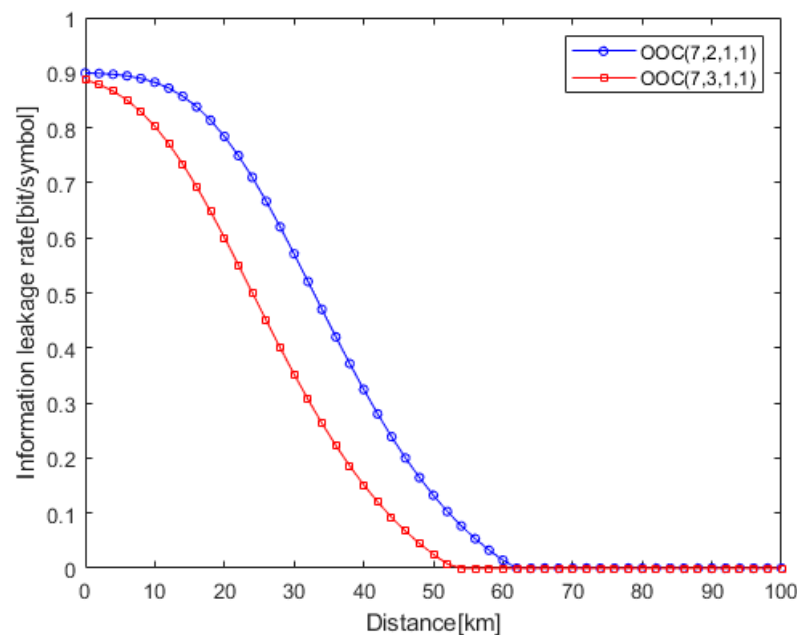


Figure 5. Information leakage rate under different optical orthogonal codes ($R_s = 0.9R_b$, $P_m = 10^{-9}$).

Figure 6 shows the relationship between the information leakage rate and eavesdropping distance under different R_s . With the decrease in R_s , the information leakage rate decreases. This is because Eve will receive more redundant information, resulting in less confidential information. This indicates that redundant information can effectively improve the physical layer security. On the other hand, with the decrease in R_s , the distance range with no information leakage increases, that is, the safe transmission distance increases.

We consider an extreme case where $R_s = R_b$, that is, the system does not use wiretap code. As shown in Figure 6, even at 100 km, Eve can obtain confidential information. The reason for this is that the transmitted information has no redundancy information. From the perspective of secrecy capacity, this shows that the whole optical fiber link is insecure. However, from the perspective of the information leakage rate, the security of the whole link can be evaluated quantitatively.

Figure 7 shows the relationship between different R_s and information leakage rates at a certain eavesdropping distance d_e . As can be seen from Figure 7, with the increase in the eavesdropping distance, the information leakage rate will decrease. This indicates that the information leakage rate and transmission efficiency are restricted mutually. Under a certain eavesdropping distance, when R_s is less than a threshold, the information leakage rate will be equal to 0, that is, perfect secrecy will be achieved. As the eavesdropping distance increases, the threshold for perfect secrecy will increase, that is, a higher rate of confidential information can be transmitted. For example, to achieve perfect secrecy, R_s should be no larger than 0.1 bit/symbol for $d_e = 20$ km, while R_s should be no larger than 0.3 bit/symbol for $d_e = 30$ km.

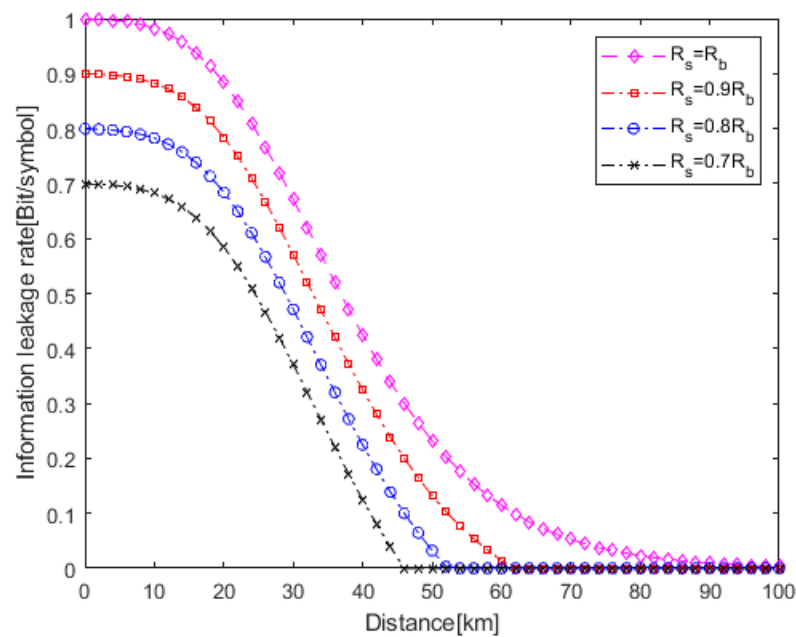


Figure 6. Relationship between information leakage rate and eavesdropping distance under different R_s ($P_m = 10^{-9}$, OOC (7,2,1,1)).

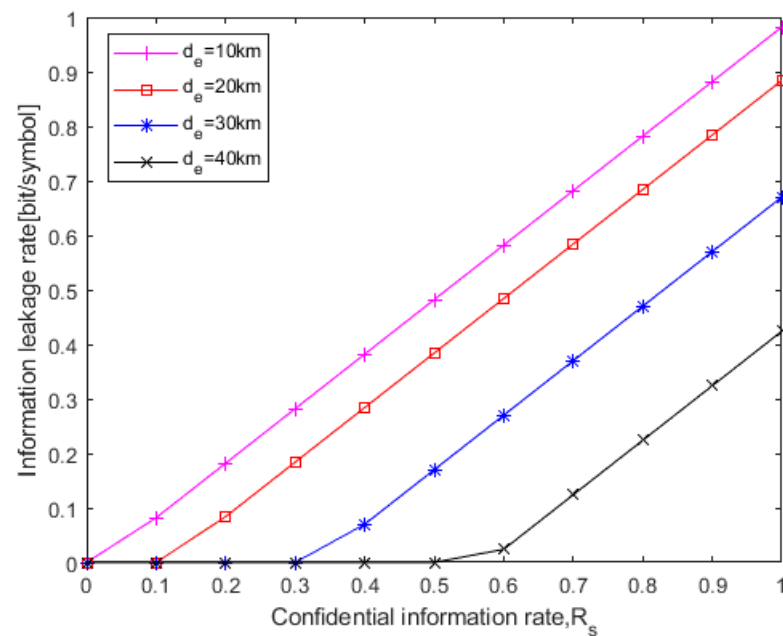


Figure 7. Relationship between different R_s and information leakage rate at a certain eavesdropping distance ($P_m = 10^{-9}$, OOC (7,2,1,1)).

4. Conclusions

Based on the OCDMA network using wiretap code, the information leakage rate is used as the performance metric to evaluate the physical layer security. The relationship between eavesdropping distance, confidential information rate and information leakage rate is quantitatively analyzed from the perspective of a partial security system. The results show that the information leakage rate decreases with the increase in the eavesdropping position. With the increase in the confidential information rate, the information leakage rate will decrease. It is also shown that the information leakage rate and transmission efficiency are restricted mutually.

Unlike secrecy capacity, the information leakage rate can quantitatively evaluate the security of the entire fiber link, which allows designers to have a clearer understanding of the physical layer security of communication systems. Considering practical systems, it is necessary to study the information leakage rate using finite length encoding. In future work, we will investigate the physical layer security of specific error correction code.

Author Contributions: Conceptualization, writing, R.X.; methodology, L.S.; review and editing, J.J.; software, K.W.; resources, Y.S. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the National Natural Science Foundation of China (NSFC) (61671306); the Fundamental Research Project of Shenzhen (JCYJ20200109105216803, JCYJ201908081436-11709).

Institutional Review Board Statement: Not applicable.

Data Availability Statement: Some codes generated or used during this study are available from the corresponding author upon request.

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

References

1. Iqbal, M.Z.; Fathallah, H.; Belhadj, N. Optical fiber tapping: Methods and precautions. In Proceedings of the 8th International Conference on High-capacity Optical Networks and Emerging Technologies, Riyadh, Saudi Arabia, 19–21 December 2011; IEEE: Piscataway, NJ, USA, 2011; pp. 164–168.
2. Yilmaz, K.; Deniz, A.; Yuksel, H. Experimental Optical Setup to Measure Power Loss versus Fiber Bent Radius for Tapping into Optical Fiber Communication Links. In Proceedings of the 2021 International Conference on Electrical, Computer and Energy Technologies (ICECET), Cape Town, South Africa, 9–10 December 2021; IEEE: Piscataway, NJ, USA, 2021; pp. 1–6.
3. Wang, S.; Yin, Z.Q.; He, D.Y.; Chen, W.; Wang, R.Q.; Ye, P.; Zhou, Y.; Fan-Yuan, G.-J.; Wang, F.-X.; Chen, W.; et al. Twin-field quantum key distribution over 830-km fibre. *Nat. Photonics* **2022**, *16*, 154–161. [\[CrossRef\]](#)
4. Ma, Y.; Liu, B.; Ren, J.; Mao, Y.; Wu, X.; Ullah, R.; Chen, S.; Wan, Y.; Bai, Y.; Zhong, Q.; et al. A Coalesce Security System of PDM and SDM Based on a Flexible Configuration of Multi-channel Keys. *J. Light. Technol.* **2022**, *41*, 1364–1374. [\[CrossRef\]](#)
5. Hu, W.; Wei, Z.; Popov, S.; Leeson, M.; Xu, T. Tapping Eavesdropper Designs against Physical Layer Secret Key in Point-to-Point Fiber Communications. *J. Light. Technol.* **2022**, *41*, 1406–1414. [\[CrossRef\]](#)
6. Cao, Y.; Zhang, L.; Huang, X.; Hu, W.; Yang, X. Real-time post-processing for physical-layer secure key distribution in fiber networks. *Opt. Commun.* **2023**, *529*, 129068. [\[CrossRef\]](#)
7. Wang, X.; Yang, X.; Wang, D.; Liu, B.; Zhang, L.; Yang, Z.; Zhu, H.; Wu, B. Demonstration of a Key Distribution Scheme Based on the Masking Effect of Fiber Channel Noise in Power Transmission System. *Photonics* **2023**, *10*, 26. [\[CrossRef\]](#)
8. Wyner, A.D. The wire-tap channel. *Bell Syst. Tech. J.* **1975**, *54*, 1355–1387. [\[CrossRef\]](#)
9. Csiszár, I.; Körner, J. Broadcast channels with confidential messages. *IEEE Trans. Inf. Theory* **1978**, *24*, 339–348. [\[CrossRef\]](#)
10. Leung, Y.C.S.; Hellman, M. The Gaussian wire-tap channel. *IEEE Trans. Inf. Theory* **1978**, *24*, 451–456. [\[CrossRef\]](#)
11. Guan, K.; Song, E.C.; Soljanin, E.; Winzer, P.J.; Tulino, A.M. Physical layer security in space-division multiplexed fiber optic communications. In Proceedings of the 2012 Conference Record of the Forty Sixth Asilomar Conference on Signals, Systems and Computers (ASILOMAR), Pacific Grove, CA, USA, 4–7 November 2012; IEEE: Piscataway, NJ, USA, 2012; pp. 654–658.
12. Guan, K.; Winzer, P.J.; Tulino, A.M.; Soljanin, E. Physical layer security of space-division multiplexed fiber-optic communication systems in the presence of multiple eavesdroppers. In Proceedings of the 2015 IEEE Global Communications Conference (GLOBECOM), San Diego, CA, USA, 6–10 December 2015; IEEE: Piscataway, NJ, USA, 2015; pp. 1–6.
13. Shake, T.H. Confidentiality performance of spectral-phase-encoded optical CDMA. *J. Light. Technol.* **2005**, *23*, 1652. [\[CrossRef\]](#)
14. Tan, Y.; Pu, T.; Zhou, H.; Zheng, J.; Su, G.; Liu, J. Design and performance analysis of a novel secure communication system based on optical code division multiple access technology. *Opt. Fiber Technol.* **2020**, *58*, 102254. [\[CrossRef\]](#)
15. Liu, X.; Luo, D.; Lin, G.; Chen, Z.; Huang, C.; Li, S.; Zhang, C.; Zhang, Z.; Wei, K. Fiber-based quantum secure direct communication without active polarization compensation. *Sci. China Phys. Mech. Astron.* **2022**, *65*, 120311. [\[CrossRef\]](#)
16. Lonnstrom, A.; Jorswieck, E.; Haufe, D.; Czarnecki, J.W. Robust secure goodput for massive mimo and optical fiber wiretap channels. In Proceedings of the 2017 IEEE 18th International Workshop on Signal Processing Advances in Wireless Communications (SPAWC), Sapporo, Japan, 3–6 July 2017; IEEE: Piscataway, NJ, USA, 2017; pp. 1–5.
17. Song, E.C.; Soljanin, E.; Cuff, P.; Poor, H.V.; Guan, K. Rate-distortion-based physical layer secrecy with applications to multimode fiber. *IEEE Trans. Commun.* **2014**, *62*, 1080–1090. [\[CrossRef\]](#)
18. Klinc, D.; Ha, J.; McLaughlin, S.W.; Barros, J.; Kwak, B.J. LDPC codes for the Gaussian wiretap channel. *IEEE Trans. Inf. Forensics Secur.* **2011**, *6*, 532–540. [\[CrossRef\]](#)

19. Pham, T.V.; Hayashi, T.; Pham, A.T. Artificial-noise-aided precoding design for multi-user visible light communication channels. *IEEE Access* **2018**, *7*, 3767–3777. [[CrossRef](#)]
20. Ferguson, N.; Schneier, B. *Practical Cryptography*; Wiley: New York, NY, USA, 2003; Volume 141.
21. Agrawal, G.P. *Fiber-Optic Communication Systems*; John Wiley & Sons: Hoboken, NJ, USA, 2012.
22. San, V.V.; Hoàng, V.V. Accurate estimation of receiver sensitivity for 10 Gb/s optically amplified systems. *Opt. Commun.* **2000**, *181*, 71–78. [[CrossRef](#)]
23. He, B.; Zhou, X.; Swindlehurst, A.L. On secrecy metrics for physical layer security over quasi-static fading channels. *IEEE Trans. Wirel. Commun.* **2016**, *15*, 6913–6924. [[CrossRef](#)]

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.