CHAPTER

Secure Communication in Fiber-Optic Networks

11

Ben Wu, Bhavin J. Shastri, and Paul R. Prucnal
Princeton University, Princeton, NJ, USA

INFORMATION IN THIS CHAPTER

- Confidentiality
- Privacy and optical steganography
- Availability

INTRODUCTION

Optical networks form the backbone of the Internet and are an integral constituent of the physical layer of these networks. Since the physical layer forms the bottom layer in the open systems interconnection (OSI) model [1], the performance and security of the physical layer and especially optical networks have a critical influence on the six layers above it. For example, the channel capacity of the optical network determines the resources available for encryption processes in the upper layer. The security approach in upper layers is limited by both the processing speed of electronic devices and the capacity availability in the optical network. Fundamental improvements can be achieved for the entire network by increasing the optical network's performance in terms of channel capacity, data rate, and processing speed. Furthermore, the security of the optical network has an impact on the security of the entire communication system. Since it is inherently risky to build a security system on top of a physical infrastructure that is already under threat [2], defending against threats to the optical network also benefits the security of the upper layer.

Optical network security can be effectively protected by fiber-based methods, including all-optical signal processing [3–5], optical key distribution [6–8], optical steganography [9–11], and optical chaos-based communication [12–14]. Fiber-based devices do not radiate an electromagnetic signature and are immune to electromagnetic interference, so the adversary can neither eavesdrop from the leaked information to free space nor jam the fiber channel with electromagnetic waves. Another motivation for securing the network based on optical approaches is that fiber-based devices

Emerging Trends in ICT Security. DOI: http://dx.doi.org/10.1016/B978-0-12-411474-6.00011-6

have low latency and high processing speed; thus, the network is protected without compromising its transmission speed. Moreover, studies in the optical layer security aim at increasing the capacity of the fiber network instead of consuming the available capacity of the fiber-optic network. For example, optical steganography demonstrates that noise in the public channel can also be used as a stealth channel for private data transmission [11]. Optical key distribution develops a separate channel with higher security level to carry the key information for data encryption [6].

In this chapter, we classify optical fiber security techniques by the threat they can address. In the section titled "Confidentiality" we discuss confidentiality of data communications and summarize the application of optical encryption and optical code-division multiple access (CDMA) in protecting the confidentiality. We also analyze an optical key distribution method for the encryption and decryption process. In the section titled "Privacy and Optical Steganography" we describe different approaches to optical steganography and analyze its functions in transmitting private data without being detected. In the section titled "Availability" we examine methods for assuring network availability, including anti-jamming and optical chaos-based communication. Throughout the chapter, we briefly describe the experimental schemes used and compare the different physical techniques. We also analyze the application and relation of each technique to the various threats that exist in the network.

Confidentiality

Data confidentiality ensures that confidential data is not disclosed to an unauthorized user in the network [15]. In an optical fiber network, the eavesdropper may receive residual crosstalk from an adjacent channel [16] or by physically tapping the optical fiber [17]. Optical encryption and optical coding can effectively protect the confidentiality of the physical layer network and satisfy the high speed requirements of modern networks. As fiber-based devices do not generate electromagnetic radiation, optical encryption and coding processes are immune to attacks based on the electromagnetic signature of the signal. In this section, we first provide examples of optical encryption and analyze its applications in secure communication. Next, we briefly summarize an optical CDMA technique. Lastly, we describe the key distribution methods for the encryption and coding.

Optical encryption

Encryption protects data transmission by encrypting the original data into cipher text. Without knowing the key for the encryption process, the eavesdropper cannot recover the data. Optical encryption has been widely studied in literature [3,4,18–22]. Compared with electronic circuits, optical processing and transmission devices have lower latency and higher speed. Another motivation for optical encryption is that fiber-based devices do not generate an electromagnetic signature. The signal in the fiber neither radiates an electromagnetic signal nor is it jammed by external electromagnetic interference. Although, compared to electronic encryption, optical encryption has limited functionality, it still plays an important role in areas that require both strong security and fast processing speed. For example, optical encryption could be especially important in the area of high-frequency trading.

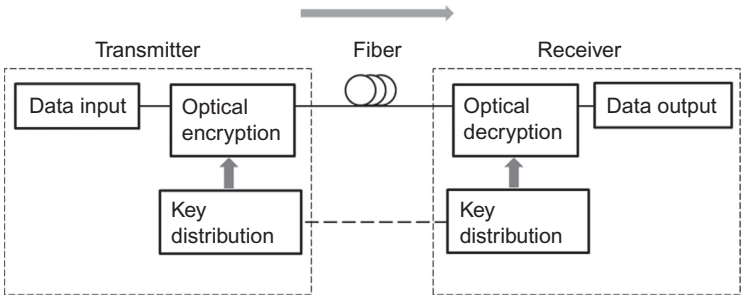

FIGURE 11.1

Schematic diagram for optical encryption.

Optical encryption includes the encryption and decryption process together with the key distribution between the transmitter and receiver (Figure 11.1). In this section, we discuss the encryption and decryption process; the key distribution method is summarized in the section titled "Optical Key Distribution." Optical exclusive OR (XOR) logic operation has been widely studied to achieve optical encryption and decryption. The optical XOR gate can be integrated into a conventional optical CDMA system and improve the overall security performance [18].

Various techniques have been developed and experimentally demonstrated to achieve the XOR operation. Chan et al. employed four-wave mixing (FWM) in a semiconductor optical amplifier (SOA) to achieve an XOR gate operating up to 20Gb/s [4]. Fok et al. investigated polarization sensitivity of an XOR gate based on FWM in a highly nonlinear fiber [19]. Other techniques, including cross polarization modulation [20], cross gain modulation [21], and cross-phase modulation [22], have also been studied to achieve optical XOR operation. These optical XOR operation methods successfully achieve all-optical data encryption. The XOR-encrypted data is protected from detection without compromising the speed for data transmission.

Optical CDMA

Optical CDMA protects data confidentiality by using a code pattern to represent "0" and "1" bits [23–28]. Multiple users with different (orthogonal) codes can share the same channel to transmit data simultaneously. Optical CDMA can be divided into two categories: coherent optical CDMA and incoherent optical CDMA. A typical coherent optical CDMA system uses spectral-phase encoding, which gives different phase shifts to the coherent spectral components at the transmitter. To decode the signal, conjugate phase shifts are used at the receiver. A typical incoherent optical CDMA scheme is called wavelength-hopping time-spreading (WHTS). WHTS uses incoherent pulses on different wavelengths to represent a code sequence (Figure 11.2). Within each code sequence, each pulse has a different delay and occupies a different time chip in each bit. The receiver for a desired code sequence compensates for the delays of the different pulses to form an autocorrelation peak (ACP). Applying the same delay compensation to the other undesired code sequences forms a cross-correlation function, and due to the orthogonal nature of the codes, this results in multiple-access interference (MAI). To improve the signal-to-noise (SNR) ratio, an optical thresholder can be used to suppress the MAI [29].

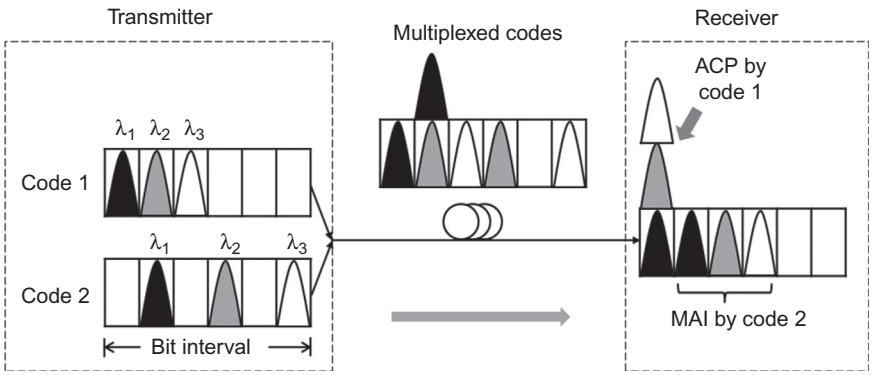

FIGURE 11.2

Schematic diagram for wavelength-hopping time-spreading optical CDMA (ACP: autocorrelation peak; MAI: multiple-access interference).

In an optical CDMA network, multiple users have their multiplexed codes overlapped, so without knowing the code used by a particular user, the eavesdropper can neither separate the pulses within each code nor recover the autocorrelation peak. However, for a point-to-point link with only one pair of transmitters and receivers, the data security may be vulnerable to attack [30]. To secure point-to-point links, Wang et al. propose a method to divide the original data stream into multiple data streams and then generate multiplexed signals. The experiment results indicate that the system is robust against various types of attack models [31].

Optical key distribution

Although the optical encryption and optical coding can effectively protect the confidentiality of the physical layer, the key for the encryption and decryption process should be distributed in a secure way between the authorized users. The key can be transmitted at a lower rate than the encrypted data but requires a higher security level. Quantum key distribution can effectively protect the encryption process by encoding the key information on the quantum states of a single photon. In 1984, Bennett and Brassard proposed using non-orthogonal polarization states of photons to transmit digital information [32]. This is now known as the BB84 protocol. After it was experimentally demonstrated in 1992 [33], different approaches have been used to achieve key exchange [6,7,34].

One important property for quantum key distribution is that it can indicate the existence of an eavesdropper trying to receive any information about the key. This is because of the unique property of quantum mechanics, in which the measurement of a certain parameter in a system also disturbs this parameter. Although the quantum channel provides a high security level to the key distribution, the requirement of single photon transmission and detection leads to difficulty in practically realizing the system. The transmission range and data rate is limited by the noise and attenuation in the single photon transmission channel. To achieve a longer range and higher data rate, classic quantum distribution also has been studied [8,35]. Scheuer et al. use a large fiber laser

to exchange the key so that each user can compare the received signal with his or her own key to obtain the key generated by the other user. Compared to quantum key distribution, this system allows longer ranges and a higher key-establishing rate [8].

Privacy and optical steganography

Privacy ensures individual control of what information may be received or collected and to whom the information may be transmitted or disclosed [15]. Although data encryption can protect the original data in a signal channel from being received by the eavesdropper, it cannot protect the existence of the channel from being detected. In some instances, the system is already under threat if the adversary knows the existence of a private channel. The aim of optical steganography in a fiber communication network is to hide signals in the existing public channels so that the eavesdropper can neither receive the signals nor detect the existence of the hidden channel [9,36–39]. The hidden channel, which carries the stealth signals, is designed in such a way that no one, apart from the intended recipient, can detect the existence of the signal in either the time domain or the spectral domain. To bury the stealth channel in the noise that already exists in the system, the power of the stealth signal is typically 10 dB–20 dB lower than the public channel [11].

Optical steganography was first proposed and experimentally demonstrated by Wu et al. [9]. The basic approach in optical steganography is to temporally stretch a short optical pulse through chromatic dispersion. Without using the right dispersion compensation at the receiver, the stretched signal is buried in the system noise of the public channel. In the spectral domain, because the spectral width of the optical pulse is on the order of several nanometers, which is much wider than the public channel spectrum, the optical spectrum of the stealth channel merges into the background noise of the public channel.

Optical steganography has been experimentally demonstrated to be compatible with public channels with various modulation formats, including return-to-zero (NRZ) on-off-keying (OOK) [40], non-return-to-zero (RZ) OOK [41], OOK optical CDMA [42], and differential (quadrature) phase-shift keying (DPSK/DQPSK) [43]. To further improve the privacy of the stealth channel, a temporal phase mask is designed to provide additional phase shift to the stretched stealth data (Figure 11.3) [44]. Each stealth data bit is covered by a 16-chip phase mask. To demodulate the data, both the dispersion and the phase mask need to be matched between the transmitter and receiver.

Recently, another approach for optical steganography was proposed to carry the stealth signal in the system noise [11] (Figure 11.4). Instead of stretching the optical pulse to mimic the noise, this method directly employs the amplified spontaneous emission (ASE) noise from amplifiers that are conventionally used to boost the signal in the fiber channel. The ASE noise from erbium-doped fiber amplifiers (EDFA) is the most prevalent noise in fiber communication systems. Since the ASE noise carrying the stealth signal has identical optical spectral properties to the ASE noise that originally existed in the system, an eavesdropper cannot differentiate whether it is signal ASE or noise ASE in the spectral domain. In the time domain, the short coherence length properties of the ASE noise provide a large key space between the transmitter and receiver. Phase modulation is used on the stealth channel at the transmitter. To demodulate the signal at the receiver, the optical

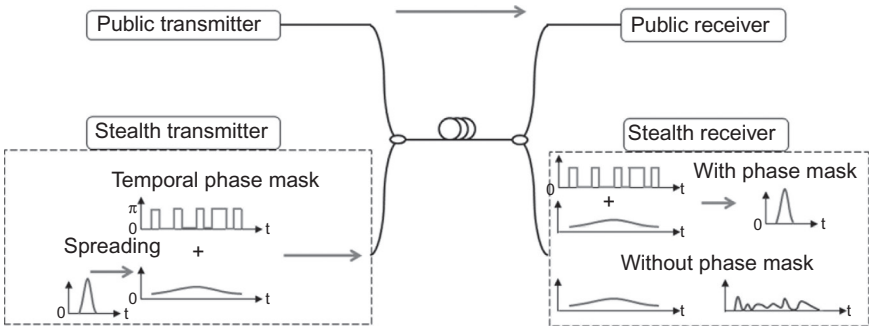

FIGURE 11.3

Schematic diagram for temporal phase modulation on spread stealth pulses.

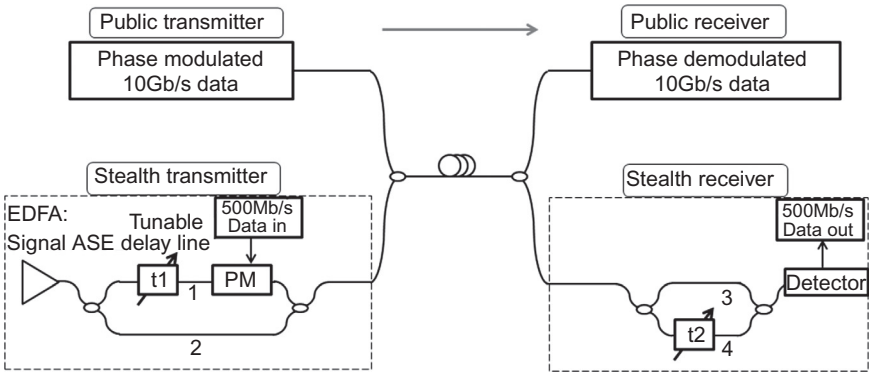

FIGURE 11.4

Schematic diagram for optical steganography based on amplified spontaneous emission noise (EDFA: erbium-doped fiber amplifier; ASE: amplified spontaneous emission; PM: phase modulator).

path length difference between the transmitter and the receiver has to be matched to be within the coherence length of the ASE noise, which is extremely short and nearly impossible to determine. If an eavesdropper tries to steal the private signal without information about the delay length difference, only noise with constant power is received. The optical path length difference at the transmitter is designed to be over 10^4 times longer than the coherence length of ASE and is deliberately changed in a dynamic fashion, so that, even if an unintended receiver finds the length difference using a quick scanning technique, it cannot follow the rapid changes of the delay length.

In the experiment, the coherence length of ASE noise is measured to be 372 μm or 1.24 ps in terms of optical delay, and the optical path length difference between path 1 and 2 at the transmitter is 6 m (Figure 11.4). The eavesdropper needs to search for a 372 μm length in a 6 m space to find the matching condition. To make acquisition even more difficult, this delay can be changed dynamically. The bit error rate (BER) measurement of the channel shows that a low BER can only be

achieved at the receiver when the unknown delay is properly tuned within the coherence length of ASE noise. If the matching condition is not satisfied, the BER is so large that it cannot be measured. To further increase the key space, dispersion is used as another key parameter between the transmitter and the receiver [45]. Since the keys for the delay length and the dispersion are mutually orthogonal, the expansion to two dimensions increases the key space geometrically. Using dispersion as another key in an ASE system also benefits from the wide spectrum of ASE noise. The wide optical spectrum of the ASE noise makes the signal nosier with relatively smaller dispersion, so besides the delay length, the dispersion also must be matched between the transmitter and receiver to demodulate the data.

In addition to protecting the privacy of data transmission, a hidden channel in the public network can also be applied to other security techniques for countering other possible threats. For example, the stealth channel can be used to transmit information having a high security level requirement, such as the key distribution for the encrypted public channel. The stealth channel can also be used to carry the users' information about the public channel, so the receiver can identify whether the information in the public channel comes from an authorized user.

Availability

Jamming and anti-jamming

"Availability" is an aspect of security that ensures that a network service is not denied to authorized users. One possible threat to network availability is to jam a signal channel with strong noise. Optical steganography based on ASE noise, discussed in the last section, can effectively protect the availability when the signal is carried by ASE, which covers the entire transmission band (known as the "C band") for fiber optic communications [11]. This increases the difficulty of carrying out malicious jamming, and even if the adversary could jam the entire C band, there would be no bandwidth left for its own data communication. Another potential solution to ensure availability uses waveband conversion. In this scheme, multiple wavebands are used for communication. If the current waveband gets jammed, the data channel can be either up-converted or down-converted to a new waveband range. Waveband conversion can be implemented with a periodically-poled lithium niobate ($LiNbO_3$) material, resulting in a low power penalty and BER [46].

Optical chaos-based communications

Chaos-based communications provide an approach for transmitting confidential data with a high level of robustness [13]. The broadband chaotic signal not only enhances the robustness of the data transmission to a narrow band interference or malicious jamming, it can also be used to jam the communication of adversaries. In contrast to optical steganography, which aims to reduce the amplitude of the stealth signal to as small as possible, the strategy of chaos-based communications is to mask the confidential data with much stronger chaos. The generation of the chaos is based on the input signal, so only the receiver that has knowledge on how the chaos is generated can reproduce the chaos and cancel it to recover the signal.

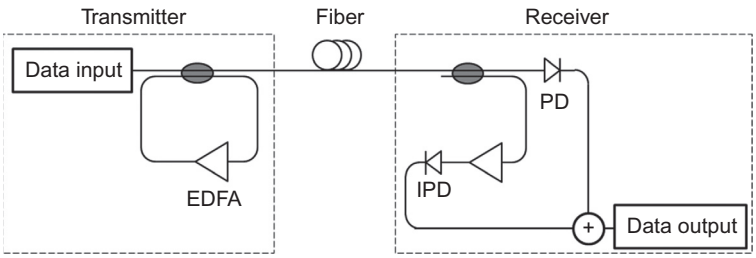

FIGURE 11.5

Schematic diagram for optical chaos communication (PD: photodiode; IPD: sign-inversing photodiode).

Chaos-based communications have been demonstrated in electronic circuits at bandwidths of tens of kilohertz; the low latency property in the fiber network enables the possibility of optical chaos communications with higher data rates [12,47]. Argyris et al. have demonstrated optical chaos-based communications with data rates higher than 1 Gb/s and bit-error rates lower than 10^{-7} [13]. In their experiment, the optical chaos-covered signal was transmitted over a 120 km distance in a commercial optical network over the metropolitan area of Athens, Greece. In an optical chaos communications system, the optical chaos is generated by fiber loops and an EDFA [14,48]. At the transmitter, the original data is coupled into the fiber loop and amplified by the EDFA (Figure 11.5). While the amplified signal is circulated and coupled back to the transmission line each time it goes through the coupler, the original signal in the transmission line is covered by a sequence of amplified signals, each having a time delay τ. The value of τ depends on the length of the fiber loop. At the receiver, the chaos-masked signal is split by another fiber coupler, and one of them goes through an open loop to regenerate the chaos. The EDFA at the receiver must be matched with the one at the transmitter. A pair of photodiodes and a sign-inverting photodiode is used to receive the chaos-masked signal and regenerated chaos. By summing the photocurrent from the two photodiodes, the chaos generated at the receiver and chaos from the transmitter is cancelled, so the signal is recovered. Besides providing confidentiality to the network, chaos-based communications also brings a high level of robustness to data transmission. By spreading the narrowband signal into a wideband signal, chaos-based communication can both create desired jamming and avoid malicious jamming.

Summary

In this chapter, we summarize the optical fiber-based techniques for protecting network security from potential threats. Optical encryption—specifically, optical XOR logic gates—is discussed. Because optical processing has low latency and is immune to electromagnetic interference, optical encryption is especially important in areas that require a high level of security without compromising the processing speed. Optical code division multiple access techniques and their application to defending the threat against data confidentiality are summarized. We also discuss methods for improving the security of point-to-point links. Both classic and quantum key distribution in the

fiber channel are discussed. Optical steganography techniques for protecting the privacy of networks are discussed. A recently developed optical steganography method is also introduced. Instead of mimicking the noise in the system, this novel method uses the noise itself to carry the data. Optical steganography based on ASE noise also has potential applications to protect the availability of the network. The technique of waveband conversion and its applications on anti-jamming and assurance of channel availability are discussed. Finally, schemes for chaos-based communication are described. Chaos-based communication can be used to either enhance the robustness of a desired data transmission or to jam an unwanted channel. Although a variety of approaches have been proposed and demonstrated to protect multiple threats in the physical layer of an optical network, much work remains to further develop and apply these results.

References

[1] Zimmermann H. OSI reference model-the ISO model of architecture for open systems interconnection. IEEE T Commun 1980;28(4):425−32.

[2] Fok MP, Wang Z, Deng Y, Prucnal PR. Optical layer security in fiber-optic networks. IEEE T Inf Foren 2011;6(3):725−36.

[3] Vahala K, Paiella R, Hunziker G. Ultrafast WDM Logic. IEEE J Sel Toptics Quantum Electron 1997;3(2):698−701.

[4] Chan K, Chan CK, Chen LK, Tong F. Demonstration of 20-Gb/s all-optical XOR gate by four-wave mixing in semiconductor optical amplifier with RZ-DPSK modulated inputs. IEEE Photon Technol Lett 2004;16(3):897−9.

[5] Wang Z, Fok MP, Prucnal PR. Physical encoding in optical layer security. J Cyber Secur Mobility 2012:83−100.

[6] Rosenberg D, Harrington JW, Rice PR, Hiskett PA, Peterson CG, Hughes RJ, et al. Long-distance decoy-state quantum key distribution in optical fiber. Phys Rev Lett 2007;98:010503-1-010503-4.

[7] Hadfield RH, Habif JL, Schlafer J, Schwall RE, Nam SW. Quantum key distribution at 1550 nm with twin superconducting single-photon detectors. Appl Phys Lett 2006;89:241129-1-241129-3.

[8] Scheuer J, Yariv A. Giant fiber lasers: a new paradigm for secure key distribution. Phys Rev Lett 2006;97:140502-1-140502-4.

[9] Wu BB, Narimanov EE. A method for secure communications over a public fiber-optical network. Opt Express 2006;14(9):3738−51.

[10] Fok MP, Prucnal PR. A compact and low-latency scheme for optical steganography using chirped fiber Bragg grating. Electron Lett 2009;45(3):179−80.

[11] Wu B, Wang Z, Tian Y, Fok MP, Shastri BJ, Kanoff DR, et al. Optical steganography based on amplified spontaneous emission noise. Opt Express 2013;21(2):2065−71.

[12] VanWiggeren GD, Roy R. Communication with chaotic lasers. Sci 1998;279(20):1198−200.

[13] Argris A, Syvridis D, Larger L, Lodi VA, Colet P, Fischer I, et al. Chaos-based communications at high bit rates using commercial fibre-optic links. Nat 2006;438(17):343−6.

[14] Yang L, Zhang L, Yang R, Yang L, Yue B, Yang P. Chaotic dynamics of erbium-doped fiber laser with nonlinear optical loop mirror. Opt Commun 2012;285:143−8.

[15] Stallings W. Cryptography and network security principles and practice. Pearson; 2011. p. 9−14 [Chapter 1].

[16] Furdek M, Skorin-Kapov N, Bosiljevac M, Sipus Z. Analysis of crosstalk in optical couplers and associated vulnerabilities. Proc 33rd Int Convention (MIPRO) 2010:461−6.

[17] Shaneman K, Gray S. Optical network security: Technical analysis of fiber tapping mechanisms and methods for detection & prevention. In: Proc IEEE Military Communications Conf (MOLCOM); 2004. p. 711–6.
[18] Fok MP, Prucnal PR. All-optical encryption based on interleaved waveband switching modulation for optical network security. Opt Lett 2009;34(9):1315–7.
[19] Fok MP, Prucnal PR. Polarization effect on optical XOR performance based on four wave mixing. IEEE Photon Technol Lett 2010;22(15):1096–8.
[20] Soto H, Erasme D, Guekos G. 5-Gb/s XOR optical gate based on cross-polarization modulation in semiconductor optical amplifier. IEEE Photon Technol Lett 2001;13(4):335–7.
[21] Kim JH, Jhon YM, Byun YT, Lee S, Woo DH, Im SH. All optical XOR gate using semiconductor optical amplifier without additional input beam. IEEE Photon Technol Lett 2002;14(10):1436–8.
[22] Jinno M, Matsuoto T. Ultrafast all-optical logic operation in a nonlinear Sagnac interferometer with two control beams. Opt Lett 1991;16(4):220–2.
[23] Prucnal PR. Optical code division multiple access: Fundamentals and applications. Taylor & Francis; 2006.
[24] Prucnal PR, Santoro MA, Fan TR. Spread spectrum fiber-optic local area network using optical processing. J Lightwave Technol 1986;4(5):547–54.
[25] Weiner AM, Heritage JP, Salehi JA. Encoding and decoding of femtosecond pulse. Opt Lett 1988;13(4):300–2.
[26] Brès CS, Huang Y-K, Glesk I, Prucnal PR. Scalable asynchronous incoherent optical CDMA [Invited]. J Opt Netw 2007;6(6):599–615.
[27] Goldberg S, Menendez R, nd Prucnal P. Towards a cryptanalysis of spectral-phase encoded optical CDMA with phase-scrambling. In: Proc Optical Fiber Communication, OThJ7; 2007.
[28] Wang Z, Chang J, Prucnal PR. Theoretical analysis and experimental investigation on the security performance of incoherent optical CDMA Code. J Lightw Technol 2010;28(12):1761–9.
[29] Kravtsov K, Prucnal PR, Bubnov MM. Simple nonlinear interferometer-based all-optical thresholder and its applications for optical CDMA. Opt Express 2007;15(20):13114–22.
[30] Jiang Z, Leaird DE, Weiner AM. Experimental investigation of security issues in O-CDMA. J Lightw Technol 2006;24(11):4228–34.
[31] Wang Z, Xu L, Chang J, Wang T, Prucnal PR. Secure optical transmission in a point-to-point link with encrypted CDMA codes. IEEE Photonics Technol. Lett 2010;22(19):1410–2.
[32] Bennett CH, Brassard G. Quantum cryptography: Public key distribution and coin tossing. In: Proc IEEE International Conference on Computers, Systems, and Signal Processing; 1984. p. 175–9.
[33] Bennett CH, Bessette F, Brassard G, Salvail L, Smolin J. Experimental quantum cryptography. J. Cryptology 1992;5(1):3–28.
[34] Gordon KJ, Fernandez V, Townsend PD, Buller GS. A short wavelength gigahertz clocked fiber-optic quantum key distribution system. IEEE J Quantum Electron 2004;40(7):900–8.
[35] Zadok A, Scheuer J, Sendowski J, Yariv A. Secure key generation using an ultra-long fiber laser: Transient analysis and exeperiment. Opt Express 2008;16(21):16680–90.
[36] Prucnal PR, Fok MP, Kravtsov K, Wang Z. Optical steganography for data hiding in optical networks. In: Proc the 16th Int Conf Digital Signal Processing (DSP), T3B.4; 2009.
[37] Wu BB, Prucnal PR, Narimanov EE. Secure transmission over an existing public WDM lightwave network. IEEE Photon Technol Lett 2006;18(17):1870–2.
[38] Wu BB, Narimanov EE. Analysis of stealth communications over a public fiber-optical network. Opt Expres 2007;15(2):289–301.
[39] Hong X, Wang D, Xu L, He S. Demonstration of optical steganography transmission using temporal phase coded optical signals with spectral notch filtering. Opt Express 2010;18(12):12415–20.

[40] Wu BB, Agrawal A, Glesk I, Narimanov E, Etemad S, Prucnal P. Steganographic fiber-optic transmission using coherent spectral-phase-encoded optical CDMA. In: Proc CLEO/QELS, CFF5; 2008.
[41] Kravtsov K, Wu BB, Glesk I, Prucnal PR, Narimanov E. Stealth transmission over a WDM network with detection based on an alloptical thresholder. In: Proc IEEE/LEOS Annual Meeting; 2007. p. 480−1.
[42] Huang Y-K, Wu BB, Glesk I, Narimanov EE, Wang T, Prucnal PR. Combining cryptographic and steganographic security with self-wrapped optical code division multiplexing techniques. Electron Lett 2007;43(25):1449−51.
[43] Wang Z, Prucnal PR. Optical steganography over a public DPSK channel with asynchronous detection. IEEE Photon Technol Lett 2011;23(1):48−50.
[44] Wang Z, Fok MP, Xu L, Chang J, Prucnal PR. Improving the privacy of optical steganography with temporal phase masks. Opt Express 2010;18(6):6079−88.
[45] Wu B, Wang Z, Shastri BJ, Tian Y, Prucnal PR. Two dimensional encrypted optical steganography based on amplified spontaneous emission noise. In: Proc CLEO/QELS, AF1H; 2013.
[46] Wang Z, Chowdhury A, Prucnal PR. Optical CDMA code wavelength conversion using PPLN to improve transmission security. IEEE Photon Technol Lett 2009;21(6):383−5.
[47] Strogatz SH. Nonlinear dynamics and chaos with applications to physics, biology chemistry and engineering. Westview; 2000. p. 335−39 [Chapter 9].
[48] Abarbanel HDI, Kennel MB, Buhl M, Lewis CT. Chaotic dynamics in erbium-doped fiber ring lasers. Phys Rev A 1999;60(3):2360−74.