Physical Encoding in Optical Layer Security

Zhenxing Wang, Mable P. Fok and Paul R. Prucnal

Princeton University, Princeton, NJ, 08544, USA;
e-mail: {zhenxing, mfok, prucnal}@princeton.edu

Abstract

Data security at the physical layer of optical networks, or optical layer security, has received considerable research attention due to the rapid growth of optical network capacity [1]. Among various optical layer approaches, optical code-division multiple access (OCDMA) systems are considered to be promising because of the physical encoding and decoding processes comprising these systems. Generally, physical encoding is an important concept in the field of optical layer security, which implements encoding to the transmitted optical signals, and protects the transmitted data from attack. In this paper, we provide an overview of various OCDMA systems, and discuss the impact of different physical encoding methods on OCDMA systems, in terms of security assurance. Furthermore, we introduce the application of physical encoding to optical steganography and optical transmission with wireless CDMA for security improvement.

Keywords: optical networks, physical encoding, physical layer security, optical layer security, OCDMA.

Journal of Cyber Security and Mobility, 83–100.

1 Introduction

The exponential growth of the Internet usage has been accompanied by a greater need to assure security of the sensitive information it carries. Data security issues become important in various applications in the Internet, from personal, commercial, to military communications. Numerous cryptographic protocols have been proposed to protect the data and the network systems [2, 3]. These protocols are usually implemented on higher layers of the network protocol stack.

Optical networks, which employ optical fibers as transmission channels, form the backbone of the Internet infrastructure. Due to the dramatic increase in bandwidth requirement and accessibility of optical networks, techniques to ensure data security in the optical transmission layer are receiving increased research interest. In this paper, we refer data security in optical transmission layer as optical layer security. Optical layer security aims to enhance network security by ensuring security at the physical layer (the lowest layer of the protocol stack), i.e., providing an additional layer to secure the network system. Moreover, optical layer security allows real-time operation in line with the transmission speed of today's ultra-fast optical link (up to 100 Gb/s), which is extremely challenging for the higher layer security protocols.

Optical code-division multiple-access (OCDMA) systems are widely considered as a good candidate to provide optical layer security [4, 5]. OCDMA systems utilize unique optical code patterns to carry data and to achieve signal multiplexing of different users. Data security in OCDMA systems comes from the physical signal encoding and decoding processes [5], because a corresponding process is required to decode the code pattern in order to successfully receive the transmitted data. When the encoding and decoding information is kept secret, the data security is ensured.

The idea of OCDMA encoding can be extended to any physical encoding method. Physical encoding imposes complex encoding onto the physical transmitted signals through optical devices. After the physical encoding, the original optical signal carrying data is transformed to an unpredictable form. When the transformed signals are transmitted through optical links, the adversary cannot intercept the data directly from the transmitted signals without the corresponding physical decoding process. Physical encoding is implemented through fast optical processes, and therefore can achieve high encoding speeds

in line with the data rates in optical links. Overall physical encoding is an important way to provide optical layer security.

Physical encoding can be applied in many applications in optical networks for security purposes. In this paper, we provide a survey of physical encoding schemes that have been demonstrated, and discuss how each physical encoding scheme helps to achieve different security objectives in various optical transmission systems While data security includes several components, such as confidentiality, availability, and integrity, as discussed in [1], we are keeping the focus of this paper on providing confidentiality in a system, which corresponds to the capability of a system to keep the transmitted data from eavesdropping or interception.

In this paper, we first give a brief introduction to a typical OCDMA system in Section 2 and provide a detailed analysis of confidentiality of an OCDMA system in Section 3. In Section 4, we discuss several physical encoding schemes based on the OCDMA systems to improve confidentiality. In Section 5 we introduce two different applications other than the OCDMA system, which utilize physical encoding for security enhancement. Finally, Section 6 concludes the whole discussion on physical encoding.

2 A Brief Introduction to OCDMA Systems

In fiber-optic communication systems that utilize a return-to-zero (RZ) data format, a binary bit is represented by an optical pulse. With on-off keying (OOK) modulation, the presence of an optical pulse represents bit "1", while the absence of a pulse represents bit "0", as shown in Figure 1. In OCDMA systems, bits are transmitted using code patterns instead of a single optical

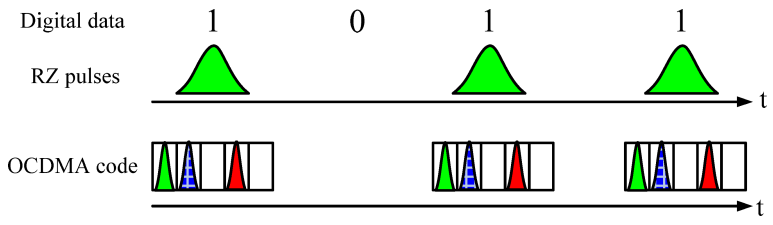


Figure 1 Schematics of OOK modulation on RZ optical pulses and OCDMA codes to transmit a binary data stream.

pulse. The use of code pattern is to allow multiple access where multiple users are transmitting simultaneously in a single fiber.

OCDMA systems can be categorized into two major groups: incoherent OCDMA systems and coherent OCDMA systems. Incoherent OCDMA implements the encoding through intensity modulation in the temporal domain and/or the wavelength domain [6, 7]. A typical incoherent OCDMA system is a 2-dimentional OCDMA scheme called wavelength-hopping time-spreading (WHTS) [8–10].

A WHTS code uses incoherent optical pulses (called chip pulses) at different wavelengths and assigns them to different time slots in one bit interval. In the example displayed in Figure 2, a WHTS code consists of three short optical pulses, each of them occupies one out of nine time slots (called time chips). The WHTS code is essentially a combination of a wavelength-hopping and time-spreading pattern. To receive the desired code, a decoder is used to align all the WHTS code's chip pulses into one chip interval, to generate an auto-correlation peak (ACP), as displayed in Figure 2. In a multiple-access channel, each WHTS code is transmitted simultaneously with other codes. The presence of codes that do not match with the decoder appears as cross-correlation peaks and causes multiple-access interference (MAI) after decoding. MAI can be minimized if all the WHTS codes in the multiple-access channel are orthogonal. The mathematical definition of WHTS codes' orthogonality is described in [8, 9].

On the other hand, coherent OCDMA employs specific phase pattern to create codes in the spectral domain or the temporal domain. One typical coherent OCDMA scheme is spectral-phase encoding (SPE) [5, 11]. As shown in Figure 3, a mode-locked laser (MLL) is utilized as the optical source which

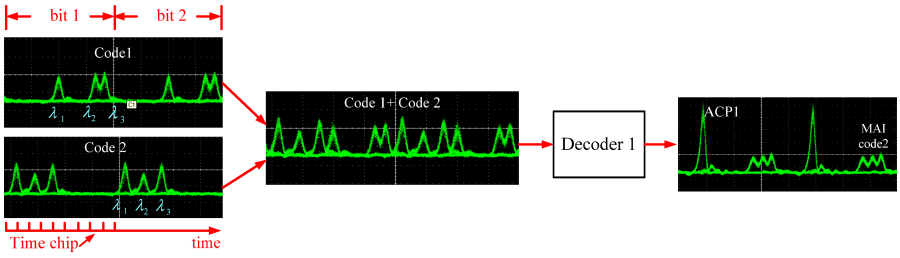
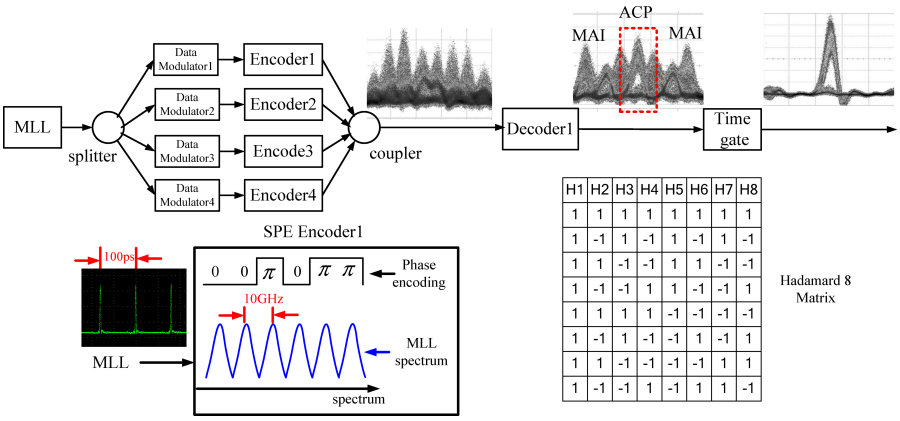


Figure 2 An illustration of WHTS codes and the decoding process.



H1	H2	H3	H4	H5	H6	H7	H8
1	1	1	1	1	1	1	1
1	-1	1	-1	1	-1	1	-1
1	1	-1	-1	1	1	-1	-1
1	-1	-1	1	1	-1	-1	1
1	1	1	1	-1	-1	-1	-1
1	-1	1	-1	-1	1	-1	1
1	1	-1	-1	-1	-1	1	1
1	-1	-1	1	-1	1	1	-1

Figure 3 Illustration of an SPE system and a Hadamard-8 matrix. In the matrix, the element "1" means 0 phase shift and "−1" means π phase shift (The three photos of the SPE's experimental results on the top are taken from [5]).

generates very short repeating optical pulses (<3 ps). In the spectral domain, the optical pulses are represented by a series of coherent spectral components. After passing through a SPE encoder, different spectral components experience different phase shifts, forming a SPE code pattern. At the receiver, the SPE decoder performs conjugation of phase shift to each spectral component, so that all the spectral components become in-phase again and an ACP is generated. In the multiple-access channel as shown in Figure 3, other SPE codes after the desired decoder will result in cross-correlation peaks, or the MAI, which will not interfere with the ACP when the SPE codes in the multiple-access channel are orthogonal. After decoding time gating can be used to isolate the ACP from the MAI. A common orthogonal SPE code set is Hadamard code, which is represented by a Hadamard matrix H_N, as shown in Figure 3. The details of SPE codes' orthogonality are illustrated in [5]. Micro-ring-resonators (MRR) can be used as the SPE encoder and decoder [11], with which the phase shift for each specific spectral component is easily adjusted to create any intended code patterns.

3 Confidentiality Analysis of OCDMA Systems

Data confidentiality of OCDMA systems inherently comes from the physical encoding and decoding process. A matched decoder is needed to successfully

decode and receive the desired code. When the OCDMA codes are not known by the adversary, or the adversary cannot build the exact decoder, he would not able to extract the data from the encoded signal. Therefore, optical layer security can be enhanced through physical encoding. However, it requires a detailed analysis on the confidentiality performance of an OCDMA system, as well as the difficulty that an adversary will confront to obtain the desired data information.

We would like to illustrate several concepts before the confidentiality analysis. First of all, different types of OCDMA systems have different confidentiality performance due to the difference in encoding/decoding schemes and codes in use. Thus, different types of OCDMA systems should be analyzed separately. Secondly, beside the coding scheme, the data modulation format also contributes to the confidentiality performance. OOK modulation has been shown to be vulnerable to eavesdropping [12] because the signal's energy levels for bit "1" and "0" are different and can be easily distinguished even without a correct decoder. To overcome the shortcomings of OOK, 2-code-keying modulation can be employed in both coherent and incoherent OCDMA systems, where two different codes are used to represent bit "1" and "0", such that the energy levels for all the bits are the same. Our discussion in the rest of this section is all based on 2-code-keying system, and we will talk about other modulation formats in later sections.

In a multiple-access OCDMA network, part of the system consists of signal from a single user (here we call them single-user channels), while part of the system may consist of signals from multiple users (named as multi-user channels). Data confidentiality is proved to be poor in a 2-code-keying single-user channel, where only one OCDMA signal is present at any specific time [12–14]. Since only two codes exist in one single-user channel representing bit "1" and "0", respectively, it is not difficult to distinguish the optical signal of these two codes from the signal's amplitude, wavelength, or phase. Therefore, data confidentiality in OCDMA systems mainly is based on the presence multiple users.

In a multi-user WHTS system, different WHTS codes are mixed into one transmission channel, and without the knowledge of which code is in use, it is difficult to find all the pulses belonging to the desired WHTS code. However, since WHTS codes employ *incoherent* chip pulses to constitute the codes, each chip pulse of a WHTS code already carries all the data information (as shown

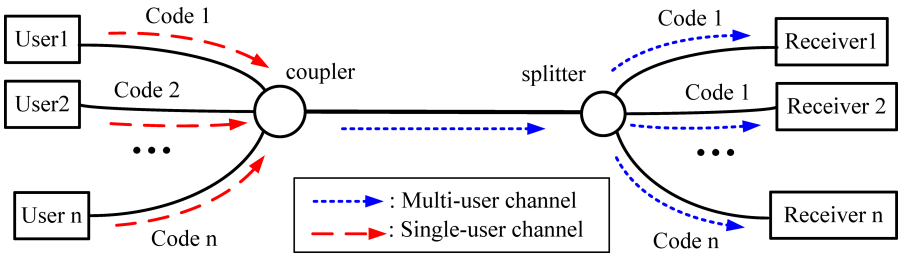


Figure 4 Single-user and multi-user channels in an OCDMA system.

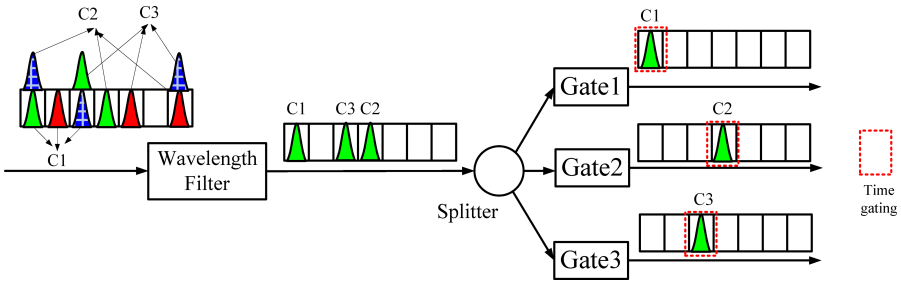


Figure 5 Detecting the data carried by WHTS codes in a multi-user channel without a decoder.

in Figure 4). Since the chip pulses of WHTS codes do not exactly overlap in the temporal domain, it is possible for an adversary to isolate each chip pulse of the desired WHTS code and intercept the data. Figure 5 illustrates a way to separate a WHTS code chip pulses from a multi-user channel consists of three users, through wavelength filtering and optical time gating. By isolating a single chip pulse of the code, the adversary can obtain the data information by detecting it with a photodetector. A detailed description on WHTS system's confidentiality can be found in [15].

The above approach to compromise WHTS systems do not apply to coherent OCDMA systems because of their coherence properties [5]. In a coherent system, the adversary has to find the entire code pattern of the user and build a matched decoder to intercept the data. A possible way for the adversary to find the desired codes is an exhaustive search of all the possible codes, called a brute-force attack. The effectiveness of brute-force attacks greatly depends on the number of possible codes in an available code set — the code cardinality. However, since the coherent codes in the channel have to be orthogonal, the number of available codes in an orthogonal code set is limited. For an N-chip

SPE, the code cardinality is only N. Therefore, if the adversary knows the code set in use, he only needs at most N trials to find one desired code [5]. Unfortunately, the information of SPE set is often public. For example, the SPE system generally utilizes the Hadamard code set.

To summarize this section, we illustrated the principles of physical encoding in OCDMA systems. We analyzed confidentiality of OCDMA systems by discussing approaches to break the physical encoding in different OCDMA systems. Our analysis shows that a normal single-user or multi-user OCDMA system cannot guarantee the security of the transmitted data. Additional measures are required based on the above systems to improve the confidentiality performance, which will be discussed in the next section.

4 Enhanced Physical Encoding on OCDMA Systems

In this section, we will introduce several enhanced physical encoding approaches. These approaches take the OCDMA systems as platforms to improve the whole system's confidentiality.

4.1 M-ary Modulation

In Section 3 we introduced the 2-code keying modulation to represent bit "1' and bit "0" with two different codes. This idea can be extended to M-ary modulation, which sends one out of M available codes at each time interval that a code takes. In this case since there are M possibilities, $\log_2$(M) bits information are transmitted at each code interval. A 4-ary WHTS system (shown in Figure 6) [16].

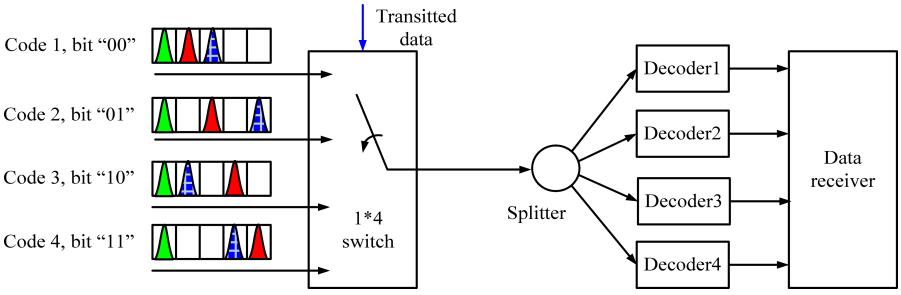


Figure 6 Schematic of a 4-ary WHTS system.

The confidentiality improvement by M-ary modulation is described as follows. First, the adversary needs to find all the M codes sent from the user, instead of just two codes in a 2-code-keying system. Secondly, the adversary needs to figure out what bit information each of the M codes represents. To find out all the bit information from M codes, the adversary will need at most $M!$ trials with a brute-force search. Moreover, M-ary modulation will also improve the WHTS system's resistance against the attacks discussed in Section 3 [15].

4.2 OCDMA Code Transformation

Although code cardinality is limited in an orthogonal coherent OCDMA code set, there are many other ways to build the code set apart from the Hadamard codes. If the whole code set is unknown, the adversary cannot find the desired code using an exhaustive search inside the code set.

One method to build an unpredictable orthogonal SPE code set is proposed in [17]. The new N-chip SPE code set W_N is derived from the existing Hadamard code set, and can be described via a matrix multiplication.

$$W_N = D_N H_N \tag{1}$$

where D_N is a diagonal matrix, and its on-diagonal elements can be arbitrary phase shift $e^{j\phi_n}$ where $\phi_n \in [0, 2\pi]$ and $n = 1, 2, \ldots, N$.

Each specific D_N yields a different orthogonal SPE code set. Essentially, this code transformation applies an additional encoding D_N to the Hadamard code set. As an example, if $N = 16$, ϕ_n is quantified to be any one of the following eight values, $\phi_n = \pi/4^*$ m, $m = 0, 1, 2, \ldots, 7$. The number of possible SPE code sets now is enlarged to 8^{16}, which makes it impractical to find the desired code set using brute force attacks without the knowledge of D_N. In practice, the implementation of D_N can be achieved by adding another SPE encoder after the Hadamard encoders [17].

4.3 Dynamic code scrambling

In Section 3, the OCDMA systems we discussed are all *static*, meaning that the codes used by each user do not change over time. This configuration gives the adversary enough time to compromise the OCDMA system. Dynamic

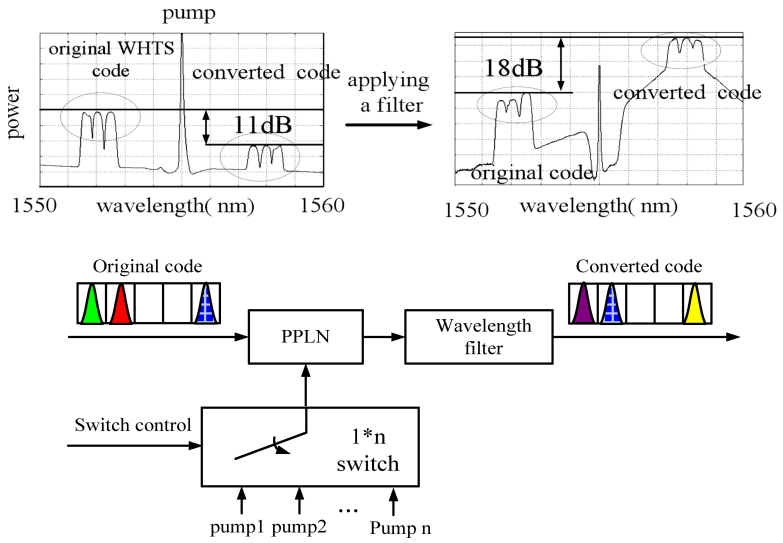


Figure 7 Top: WHTS code conversion in the wavelength domain using PPLN waveguides; Bottom: schematic of dynamic WHTS code scrambling.

code scrambling aims to switch the codes being used to other codes before an adversary finds the correct code, thus protecting the codes from compromising. One way to achieve code scrambling is WHTS code conversion through a nonlinear optical process [18]. As shown in Figure 7 (top part), a WHTS code can be converted to other wavelengths through a periodically-poled lithium-niobate (PPLN) waveguide when a strong optical pump signal is injected at the same time. When the pump wavelength is switching dynamically, the converted WHTS code will dynamically hop in the wavelength domain as shown in Figure 7 (bottom part). The selection of the pump wavelength forms a physical encoding pattern and should be keep secret from the adversary.

Besides the three approaches described above, other approaches have also been proposed to improve confidentiality of OCDMA systems. One approach is all-optical exclusive-or (XOR) encryption [19–21]. By an all-optical XOR gate, the original data can be encrypted with a secure key, which is called a "one-time pad" [22]. All-optical XOR encryption is able to achieve ultra-fast encryption speed compared to electrical encryption. A complete discussion on all-optical XOR encryption can be found in [1].

5 Physical Encoding in Other Optical Layer Security Aspects

So far our discussion of physical encoding only focuses on coding in an OCDMA system. The concept of physical encoding can also be applied to other fields for confidentiality provision in optical networks. In this section, we will discuss two applications with physical encoding, which are optical steganography and optical transmission by wireless CDMA.

5.1 Temporal Phase Encoding in Optical Steganography

Steganography aims at hiding the transmitted messages in plain sight, so that no one will realize the existence of the secret message, except the sender and the recipient. Optical steganography applies this concept to optical communications and send secret data message through a "stealth channel", which is hidden under public data transmission in optical networks [23, 24].

In principle, optical steganography employs short optical pulses as the signal source, which has a relatively broad spectrum and can be stretched temporally through a highly dispersive device, as illustrated in Figure 8. Due to the chromatic dispersion experienced, the original pulses get substantially stretched and their peak amplitudes are reduced to a very low level, such that the entire stretched pulses can be buried under the transmission of public channels and the system noise. It is difficult to find the existence of the stealth signal in the public channel from either the temporal domain or the spectral domain. To receive the stealth data, the stretched stealth pulses are recovered through a matched inverse dispersion. The secret message is retrieved after the pubic signals are removed. Previous research have illustrated that

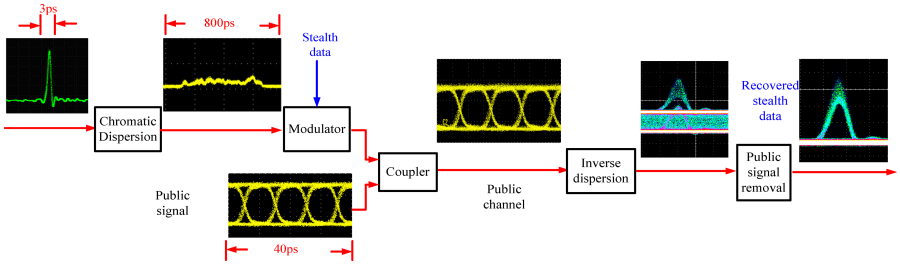


Figure 8 Principle of optical steganography.

optical steganography has good compatibility with various types of public channels [25–27].

Even though the stealth channel is buried under public channels in both the temporal and the spectral domains, the privacy of the stealth signal still cannot be guaranteed. Since pulse stretching is realized through linear chromatic dispersion, the adversary can apply a tunable chromatic dispersion to the optical signal in the public channel to search for the existence of the stealth channel. Once the stealth signal is identified, the dispersion can be further tuned to fully recover the stealth pulses. Such an attack dramatically reduces the stealth channel's privacy.

To address this potential threat, temporal phase encoding is proposed to apply onto the stretched stealth pulses before they are sent into the public channels [27, 28]. The additional encoding process is displayed in Figure 9. One temporal phase mask is imposed on the stretched stealth signal to implement phase encoding. After phase encoding, different portions of the stretched pulse experience different phase shifts. In order to fully recover the stealth pulses, an inverse phase mask is required at the receiver in addition to the matched dispersion compensation. If the adversary lacks the phase encoding information, he cannot fully recover the stealth pulses even with the right dispersion compensation, and will obtain a distorted signal as displayed in Figure 9.

The phase shifts applied to each portion of the stretched pulse can be arbitrary (not just restricted to 0 and π). Therefore the number of possible phase masks can be very large. For example, if the phase mask has $N = 32$ chips, and the phase shift Φ is one of the following eight values, $\Phi = \pi/4^{*}\,\mathrm{m}$ $(m = 0, 1, 2, \ldots, 7)$, then the phase mask has 8^{32} possibilities. With phase

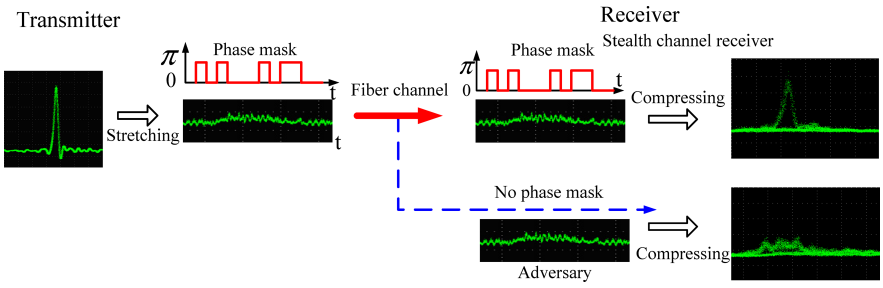


Figure 9 A demonstration of temporal phase encoding in optical steganography to improve privacy.

encoding, it is difficult for the adversary to find the existence of the stealth channel. Without the phase mask information, even if the adversary is aware of the presence of a stealth channel, the possibility for the adversary to recover the stealth signal and obtain the secret message is still very low. A detailed quantitative analysis is provided in [28] on the effectiveness of such physical encoding.

5.2 Optical Transmission with Encoded wireless CDMA Codes

Similar to OCDMA systems, wireless CDMA also has the capability of providing confidentiality because of the similar encoding and decoding process. One typical type of wireless CDMA code is the pseudo-random sequences such as the m-sequences [29]. In a multiple-access channel, the multiplexed wireless CDMA signal is an analog noise-like signal. The correct decoder is required to generate an ACP for data reception.

Due to the analog property of the multiplexed wireless CDMA signal, it is not practical to employ wireless CDMA in high-speed optical communication. However, this idea becomes possible because of the recent development of digital signal processing (DSP) technologies. One advantage of applying wireless CDMA codes in optical communications is the wider available spectrum in fiber-optic channels, compared with the limited spectrum in wireless channels. Therefore, a high speed transmission can be supported in the fiber-optic channels.

Although wireless CDMA encoding can provide data confidentiality, it is still possible for an adversary to find the desired codes in a standard wireless CDMA system (here the word "wireless" is just used to differentiate the codes from OCDMA codes). The reason is similar to the case of coherent OCDMA systems. In a standard wireless CDMA system, the wireless CDMA codes are all orthogonal and the wireless code set is standardized. Based on the standard of the wireless CDMA code set, the code can be easily derived by a few simple detections [30].

In order to address the confidentiality problem, additional encoding is proposed to apply to the standard wireless CDMA code set [31]. The proposed encoding is the advance encryption standard (AES) [1], which can be treated as a special type of physical encoding onto the wireless CDMA code patterns. After AES encryption, the wireless CDMA codes become

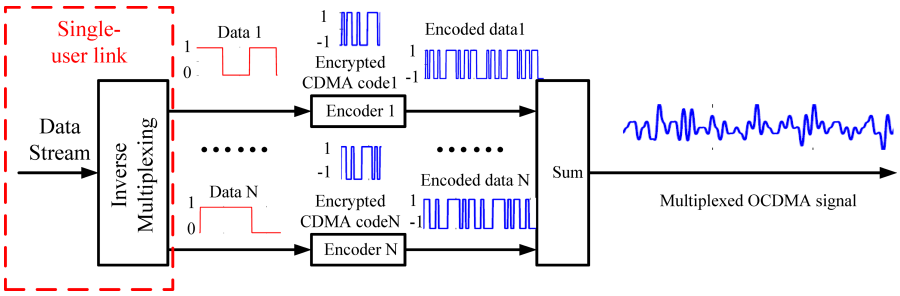


Figure 10 Schematic diagram of AES encryption on standard wireless CDMA system.

unpredictable and are not necessarily orthogonal to each other any more. The adversary now cannot find the code information and intercept the data. Therefore the system confidentiality is improved through the AES encryption. Compared to direct AES encryption, this system allows a higher transmission rate, because the AES encryption on wireless CDMA codes can be operated offline. Moreover, experimental results show that transmission performance of the non-orthogonal codes after encryption can still be maintained within an acceptable level [31].

The improved wireless CDMA system can be modified to build a single-user optical transmission link through inverse data multiplexing [31]. As displayed in Figure 10, the original data stream is divided into multiple sub-streams, and each sub-stream is encoded by an encrypted CDMA code. All of the encoded sub-streams combine together to form a multiplexed signal and is used to modulate the optical carrier for optical transmission. Since the inverse multiplexing process, the data encoding/decoding process, and the code encryption process can be implemented onto one single chip, the multiple encoding and encryption processes do not induce much additional hardware cost. Therefore, a cost-effective solution is provided to build a secure single-user optical link.

6 Conclusion

In this paper, we introduced the concept of physical encoding to provide optical layer security and present a survey of various optical approaches to implement physical encoding. We introduced OCMDA systems and analyzed possible ways to compromise the OCDMA systems and intercept

the transmitted data. We also discussed several enhanced physical encoding schemes and illustrated how these approaches help to improve the confidentiality of OCDMA systems. Finally, we discussed physical encoding in optical stegangraphy, and a wireless-CDMA optical transmission system for confidentiality enhancement. Although a number of physical encoding approaches have been proposed, this field is still at its early research stage. More research efforts on this field, both theoretical and experimental, are expected in the near future.

References

[1] M.P. Fok, Z. Wang, Y. Deng, and P.R. Prucnal. Optical layer security in fiber-optic networks. *IEEE Transactions on Information Forensics and Security*, 6(3):725–736, September 2011.

[2] Douglas R. Stinson. *Cryptography: Theory and Practice*. CRC press, 2002.

[3] W. Trappe and L.C. Washington. *Introduction to Cryptography with Coding Theory*. 2nd edition, Prentice Hall, July 2005.

[4] A. Stok and E.H. Sargent. The role of optical CDMA in access net-works. *IEEE Commun. Mag.*, 40(9):83–87, 2002.

[5] S. Etemad, A. Agarwal, T. Banwell, J. Jackel, R. Menendez, and P. Toliver. OCDM-based optical layer 'security' scalable to 100 Gbits/s for existing WDM networks [Invited]. *J. Opt. Netw.*, 6:948–967, 2007.

[6] P.R. Prucnal, M.A. Santoro, and T.R. Fan. Spread spectrum fiber-optic local area network using optical processing. *Electron. Lett.*, 4(5):547–554, 1986.

[7] G.-C. Yang and W.C. Kwong. Two-dimensional spatial signature patterns. *IEEE Trans. Commun.*, 44(2):184–191, 1996.

[8] C.S. Brès, Y.-K. Huang, I. Glesk, and P.R. Prucnal. Scalable asynchronous incoherent optical CDMA [Invited]. *J. Opt. Netw.*, 6:599–615, 2007.

[9] P.R. Prucnal, *Optical Code Division Multiple Access: Fundamentals and Applications*. (Taylor and Francis, New York, 2006).

[10] Y. Deng, Z. Wang, K. Kravtsov, J. Chang, C. Hartzell, M.P. Fok, and P.R. Prucnal. Demonstration and analysis of asynchronous and survivable optical CDMA ring networks. *IEEE J. Opt. Commun. Net.*, 2(4):159–165, April 2010.

[11] A. Agarwal, P. Toliver, R. Menendez, S. Etemad, J. Jackel, J. Young, T. Banwell, B.E. Little, S.T. Chu, W. Chen, J. Hryniewicz, F. Johnson, D. Gill, O. King, R. Davidson, K. Donovan, and J. Delfyett. Fully programmable ring-resonator-based integrated photonic circuit for phase coherent applications. *J. Lightwave Technol.*, 24:77–87, 2006.

[12] T.H. Shake. Security Performance of Optical CDMA Against Eavesdropping. *J. Lightwave Technol.*, 23:655–670, 2005.

[13] T.H. Shake. Confidentiality performance of spectral-phase-encoded optical CDMA. *J. Lightwave Technol.*, 23:1652–1663, 2005.

[14] Z. Jiang, D.E. Leaird, and A.M. Weiner, Experimental investigation of security issues in O-CDMA. *J. Lightwave Technol.*, 24:4228–4234, 2006.

[15] Z. Wang, J. Chang, and P.R. Prucnal. Theoretical analysis and experimental investigation on the security performance of incoherent optical CDMA code. *J. Lightwave Technol.*, 28(12):1761–1769, 2010.

[16] C.S. Brès, I. Glesk, R.J. Runser, T. Banwell, P.R. Prucnal, and W.C. Kwong, Novel M-ary architecture for optical CDMA using pulse position modulation. *18th Annual Meeting of the IEEE Lasers and Electro-Optics Society (LEOS)*, p. 967, 2005.

[17] R.C. Menendez, P. Toliver, S. Galli, A. Agarwal, J. Jackel, J. Young, S. Etemad, Anjali Agarwal, and T. Banwell. Network applications of cascaded passive code translation for WDM-compatible spectrally phase-encoded optical CDMA. *J. of Lightwave. Technol.*, 23(10):3219–3231, 2005.

[18] Z. Wang, A. Chowdhury, and P.R. Prucnal. Optical CDMA code wavelength conversion using PPLN to improve transmission security. *IEEE Photon. Technol. Lett.*, 21:383–385, 2009.

[19] N. Kostinski, K. Kravtsov, and Paul R. Prucnal. Demonstration of an all-optical OCDMA encryption and decryption system with variable two-code keying. *IEEE Photonics Technology Letters*, 20(24): December 2008.

[20] Z. Wang, Y.-K. Huang, Y. Deng, J. Chang, and P.R. Prucnal. Optical encryptionwith OCDMA code swapping using all-optical XOR logic gate. *IEEE Photon. Technol. Lett.*, 21(7): 411–413, 2009.

[21] M.P. Fok and P.R. Prucnal. All-optical encryption based on interleaved waveband switching modulation for optical network security. *Optics Letters*, 34(9):1315–1317, April 2009.

[22] C.E. Shannon. Communication theory of secrecy systems. *Bell System Technical Journal*, 28(4):656–715, 1949.

[23] B.B. Wu and E.E. Narimanov. A method for secure communications over a public fiber-optical network. *Optics Express*, 14(9):3738–3751, 2006.

[24] B.B. Wu and E.E. Narimanov, Analysis of stealth communications over a public fiber-optical network. *Opt. Express*, 15:289–301, 2007.

[25] Y.K. Huang, B. Wu, I. Glesk, E.E. Narimanov, T. Wang, and P.R. Prucnal. Combining cryptographic and steganographic security with self-wrapped optical code division multiplexing techniques. *Electronics Letters*, 43(25):1449–1451, December 2007.

[26] K. Kravtsov, B. Wu, I. Glesk, P.R. Prucnal, and E. Narimanov. Stealth transmission over a WDM network with detection based on an all-optical thresholder. *IEEE/LEOS Annual Meeting 2007*, pp. 480–481, paper WH2.

[27] Z. Wang and P.R. Prucnal. Optical steganography over a public DPSK channel with asynchronous detection. *IEEE Photon. Technol. Lett.*, 23:48–50, January 2011.

[28] Z. Wang, M.P. Fok, L. Xu, J. Chang, and P.R. Prucnal. Improving the privacy of optical steganography with temporal phase masks. *Optics Express*, 18(6):6079–6088, 2010.

[29] S.W. Golomb. *Shift Register Sequences*. Holden-Day, San Francisco, 1967.

[30] M. Tafaroji and A. Falahati. Improving code division multiple access security by applying encryption methods over the spreading codes. *IET Commun.*, 1(3):398–404, 2007.

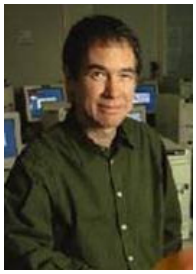
[31] Z. Wang, L. Xu, T. Wang, and P.R. Prucnal. Secure optical transmission in a point-to-point link with encrypted wireless CDMA codes. *IEEE Photon. Technol. Lett.*, 22:1410–1412, 2010.

Biography

Zhenxing Wang received his B. S. degree in electronics from Peking University, Beijing, China, in 2006. He is currently pursuing his Ph.D. degree in the Department of Electrical Engineering, Princeton University, Princeton, NJ. His research covers various types of technologies on optical signal processing, and optical communications. Zhenxing's major research areas include optical layer security, optical steganography, and optical OFDM, etc.

Mable P. Fok (S'02–M'08) received the B. Eng., M.Phil., and Ph.D. degrees in electronic engineering from the Chinese University of Hong Kong (CUHK), Hong Kong, in 2002, 2004, and 2007, respectively. She was a Visiting Researcher at the University of California, Los Angeles (UCLA) and the University of California, Santa Barbara (UCSB) during 2005 and 2006, respectively, where she was engaged in research on supercontinuum generation in nonlinear fibers with the former and all-optical processing of advanced modulation format signals with the later. Currently, Mable is an associate research scholar in the Department of Electrical Engineering at Princeton University. She has published over 120 journal and conference papers. Her recent research interest is on hybrid analog/digital processing of optical signals based on neuromorphic algorithm and developing new techniques to enhance physical layer information security in optical communications network.

Dr. Fok is the recipient of the Special Merit in 2008 Hong Kong Institution of Science Young Scientist Awards, First Prize in 2007 IEEE Hong Kong Section Postgraduate Student Paper Contest, the 2006 Optical Society of America Incubic/Milton Chang Student Travel Grant Award, the 2005 IEEE Lasers and Electro-Optics Society Graduate Student Fellowship Award, and the 2005 Thomas HC Cheung Postgraduate Scholarship in Science and Engineering from the Hong Kong Association of University Women.



Paul R. Prucnal received his A.B. from Bowdoin College, and his M.S., M.Phil. and Ph. D. from Columbia University, where he was a faculty member until 1988, when he joined Princeton as a Professor of Electrical Engineering. From 1990 to 1992, Professor Prucnal served as Founding Director of Princeton's Center for Photonics and Optoelectronic Materials. He has also held positions as Visiting Professor at the University of Tokyo and University of Parma. Professor Prucnal is the inventor of the "Terahertz Optical Asymmetric Demultiplexer," an ultrafast all-optical switch, and is credited with doing seminal research in the areas of all-optical networks and photonic switching, including the first demonstrations of optical code-division and optical time-division multi-access networks in the mid-1980's. With DARPA support in the 1990's, his group was the first to demonstrate a 100 gigabit/sec photonic packet switching node and optical multiprocessor interconnect, which was nearly one hundred times faster than any system with comparable functionality at that time. For the past several years his research has focused again on optical CDMA as well as physical layer security in optical networks. He has published over 200 journal papers and holds 17 patents. He is currently an Area Editor of the IEEE Transactions on Communications for optical networks. He was general chair of the OSA Topic Meeting on Photonics in Switching in 1999, is an IEEE Fellow, an OSA Fellow, and a recipient of the Rudolf Kingslake Medal from the SPIE. In 2005, he was the recipient of a Princeton University Engineering Council Award for Excellence in Teaching, and in 2006, the recipient of the Graduate Mentoring Award in Engineering at Princeton.