Osaka University Knowledge Archive

| | |
|---|---|
| Title | Studies on Secure M-ary Optical Code Division Multiplexing Using a Single Multi-port Encoder/Decoder |
| Author(s) | Kodama, Takahiro |
| Citation | 大阪大学, 2012, 博士論文 |
| Version Type | VoR |
| URL | https://hdl.handle.net/11094/1187 |
| rights | |
| Note | |

*Osaka University Knowledge Archive : OUKA*

https://ir.library.osaka-u.ac.jp/

Osaka University

# Doctoral Dissertation

# Studies on Secure M-ary Optical Code Division Multiplexing Using a Single Multi-port Encoder/Decoder


## Takahiro Kodama

**Division of Electrical, Electronic, and Information Engineering**

**Graduate School of Engineering**

## Osaka University


**2011**

# Preface

This dissertation treats M-ary optical code division multiplexing using a single multi-port encoder/decoder, which is based on the reseach the author carried out during his Ph. D. course at the Division of Electrical, Electronic, and Information Engineering, Graduate School of Engineering, Osaka University. The dissertation is organized as follows:

Chapter 1 is a general introduction, where the background and problem of current encryption technologies on the Internet are briefly reviewed. Then, physical layer security technologies for high secure network for the next generation, is introduced. Finally, the motivation of this study including the reason to focus attention on the optical code division multiplexing (OCDM) /optical code division multiple access (OCDMA) is also presented.

Chapter 2 describes the optical encoding/decoding technique. Moreover, the confidentiality evaluation methods of bit-ciphered and block-ciphered (M-ary) OCDM are also described in this chapter. Finally, we introduce the properties of multi-port encoder/decoder (E/D) and phase shift keyed (PSK) OC which are suitable for M-ary OCDM system.

Chapter 3 extends M-ary OCDM system with exclusive OR (XOR) using a single multi-port E/D, which is used the optical implementation of the cipher block chaining (CBC) mode. Then, we experimentally demonstrate 16-ary OCDM system with XOR. With this system, we achieve its 50 km transmission for the first time.

Chapter 4 extends polarization multiplexed (POL-MUX) M-ary OCDM system using a single multi-port E/D. Then, we experimentally demonstrate POL-MUX 256-ary OCDM system. In conventional M-ary OCDM, the number of OC is limited by the port count of multi-port E/D, and it would be desirable if the M-ary number can be increased without increasing the number of OC. By using POL-MUX M-ary OCDM method, the number of $M$ can be increased. Moreover, the physical confidentiality is also improved. We also discuss and analyze the corresponding data security in terms of data confidentiality.

Chapter 5 extends M-ary OCDM system using multidimensional codes. Multidimensional codes consist of OC combinations generated by a single multi-port E/D. Therefore, high M-ary number is achieved by using these codes. We experimentally demonstrate the operation principle of 4096-ary OCDM system for the first time. Then, we show that the impairment due to multiple access interference affects the system performance. We also analyze the data confidentiality. Moreover, we propose M-ary OCDMA-based passive optical network (PON) system, that uses a multi-port E/D in the central office and in the users premises. Finally, we show the feasibility of a 10 Gbps, 4096-ary OCDMA-based PON system using multidimensional code by numerical simulation.

From all the obtained results, it is concluded that, the proposed M-ary OCDM using a single multi-port E/D has the feasibilities of properly operations. Each proposed technique can be expected to support secure

optical access networks.

All the results described in the dissertation were published in IEEE/OSA Journal of Lightwave Technology, Optics Express, Proceedings of Optical Fiber Communication Conference and National Fiber Optic Engineers Conference (OFC/NFOEC2009, OFC/NFOEC2011), Proceedings of The Conference on Lasers and Electro-Optics and The Quantum Electronics and Laser Science Conference (CLEO/QELS 2009), Proceedings Updating Quantum Cryptography and Communications (UQCC 2010), and domestic conferences in Japan which are shown in the list of publications by the author.

Takahiro Kodama

*Osaka Japan*
*2011*

# Acknowledgements

The present research has been carried out during my tenure of doctorial course at the Division of Information and Communications Technology, in the Division of Electrical, Electronic, and Information Engineering, Graduate School of Engineering, Osaka University, under the guidance of Prof. Ken-ichi Kitayama.

First of all, I would like to express my deepest sense of appreciation to Prof. Ken-ichi Kitayama for his professional instruction, continuous encouragement, and a number of stimulating discussions. His keen insight and a wealth of creative ideas have always indicated pertinent ways to construct the framework of this research. I have also learned so much precious things through my collaboration with him, which have further developed my ability as a researcher.

I am profoundly indebted to Prof. Noboru Babaguchi and Associate Prof. Akihiro Maruta of Electrical, Electronic, and Information Engineering for careful reviews of this dissertation and suggestions to improve this dissertation.

I wish to express my sincere thanks to many professors in the Division of Electrical, Electronic, and Information Engineering.

Associate Prof. Akihiro Maruta has generously spent a lot of time answering my question and providing technical advice. The discussions with him intrigued my interest to technical aspects of optical signal processing. His comments and criticism have been invaluable in accomplishing this dissertation. I also thank Assistant Prof. Yuki Yoshida.

I am also greatly indebted to Prof. Shozo Komaki, Prof. Tetsuya Takine, Prof. Seiichi Sampei, Prof. Kyo Inoue, Prof. Zen-ichiro Kawasaki, Prof. Takashi Washio, Prof. Riichiro Mizoguchi, Associate Prof. Masayuki Matsumoto, Associate Prof. Shin-ichi Miyamoto, and Associate Prof. Takahiro Matsuda for their guidance regarding my whole tenure in Osaka University.

I particularly appreciate Dr. Naoya Wada, Dr. Nobuyuki Kataoka, Dr. Tetsuya Miyazaki, Dr. Yoshihiro Tomiyama, Mr. Hiroyuki Sumimoto, and Ms. Takako Sugimoto of Ultrafast Photonic Network Group, the National Institute of Information and Communications Technology for their edifying teaching and great support for experiments. Special thanks go to Dr. Naoya Wada for his instruction, encouragement, and discussions in research. Dr. Nobuyuki Kataoka frequently came to see me and always encouraged me. He also provided me with valuable comments from his experience in OCDMA research. Most of results shown in this dissertation are actually obtained through their instructions and discussions. If it were not their eager support, these works should not be accomplished.

I greatly appreciate Prof. Gabriella Cincotti of Applied Electronics, University Roma Tre. She gave me a lot of precious advisement in terms of numerical simulation. She also pointed out the configuration of my research journal papers.

I also greatly appreciate Prof. Xu Wang of Engineering and Physical Sciences and Joint Research Institute for Integrated Systems, Heriot-Watt University. He supported and gave me a lot of opportunities to discuss during the period of study abroad in the United Kingdom.

I would also like to thank Mr. Hiroshi Fujinuma of NTT Electronics Corporation for his cooperation to fabricate the new device of my research.

I really thank Prof. Kenji Taniguchi, Prof. Masanori Ozaki, and Associate Prof. Masatoshi Fujimura of Global COE program, “Center for Electronic Devices Innovation” for supporting by a grant, and giving a lot of valuable opportunity to attend international activities.

I would like to express my gratitude to all the past and present colleagues in the Photonic Network Laboratory of Division of Information and Communications Technology in the Division of Electrical, Electronic, and Information Engineering, Graduate School of Engineering, Osaka University. They have always provided encouragement and their friendship to me both in research and private life. Special thanks go to Dr. Yuji Miyoshi, Dr. Shaowei Huang, Mr. Naoki Nakagawa, Mr. Shinji Tomofuji, Mr. Shogo Tomioka, Mr. Seiki Takagi, Mr. Nozomi Hashimoto, Mr. Iori Takamatsu, Mr. Yusuke Tanaka, Mr. Ryousuke Matsumoto, and Mr. Keitaro Tatsumi who provided me with valuable suggestions, and devoted a lot of time to me in fruitful discussions.

I also thank Prof. Shigeru Saito who is the professor in my undergraduate age and belongs to Division of Photonics, Ritsumeikan University. He devoted a lot of time to teach me the basics of the optical communication technology.

I am grateful to the Global COE Program “Center for Electronic Devices Innovation”, the ICOM Research Foundation, Hara Research Foundation, and Showa-houkoukai Research Foundation for financially supporting the research work.

Finally, I would like to thank my parents, Shun-ichi and Mayumi, my brother, Yoshihiro, my sister, Mai, my grand mother, Tokie, for their deep understanding, support, and love during the whole period of my life.

# Contents

**Preface** ..... i

**Acknowledgements** ..... iii

**Chapter 1 Introduction** 1

1.1 Demand of Secure Photonic Network ..... 1
1.2 Photonic Layer Security Technology ..... 3
1.3 Trend of Optical Access Network ..... 4
1.4 Security Issues of Optical Access Network ..... 5
1.5 Overview of the Discussions ..... 6

**Chapter 2 Overview of Optical Code Division Multiplexing** 9

2.1 Introduction ..... 9
2.2 Principle of Optical Encoding/Decoding ..... 9
2.2.1 Optical Encoding ..... 9
2.2.2 Optical Decoding ..... 11
2.3 Bit-ciphered Optical Code Division Multiplexing ..... 13
2.4 Block-ciphered (M-ary) Optical Code Division Multiplexing ..... 15
2.5 Modeling of Confidentiality Evaluation ..... 16
2.6 PSK Optical Code Generated by Multi-port Encoder/Decoder ..... 19
2.6.1 Configuration of Multi-port Encoder/Decoder ..... 19
2.6.2 Correlation Property ..... 21
2.6.3 Dispersion Effect to Optical Coded Signal ..... 24
2.7 Conclusion ..... 28

**Chapter 3 M-ary OCDM System with XOR** 29

3.1 Introduction ..... 29
3.2 16-ary OCDM System with XOR ..... 29
3.3 Experiments ..... 32
3.3.1 Experiment without XOR ..... 32
3.3.2 Experiment with XOR ..... 35
3.4 Conclusion ..... 38

**Chapter 4 M-ary OCDM System Using Polarization Multiplexing** **39**
4.1 Introduction ····· 39
4.2 256-ary OCDM System Using Polarization Multiplexing ····· 40
4.3 Experiments ····· 43
4.4 Data Confidentiality Analysis ····· 47
4.5 Conclusion ····· 49

**Chapter 5 M-ary OCDM System Using Multidimensional Optical Codes** **51**
5.1 Introduction ····· 51
5.2 Multidimensional Optical Code Processing ····· 52
5.3 4096-ary OCDM System Using Multidimensional PSK Optical Codes ····· 53
5.4 Experiments ····· 57
5.5 System Performance Analysis ····· 58
5.6 Data Confidentiality Analysis ····· 61
5.7 Extension to Multiple Access: M-ary OCDMA ····· 63
5.7.1 System Configuration ····· 63
5.7.2 Performance Analysis of 4096-ary OCDMA System ····· 64
5.8 Conclusion ····· 66

**Chapter 6 Conclusions** **67**

**Acronyms** ····· **69**

**List of Symbols** ····· **73**

**Bibliography** ····· **75**

**List of Publications** ····· **83**

# Chapter 1

# Introduction

## 1.1 Demand of Secure Photonic Networks

The data transmission of valuable information, such as military or financial transactions, medical records, and confidential intellectual property, has currently been relying on the Internet via high speed, large capacity optical networks, thanks to the cost effectiveness of Internet protocol (IP) networks. A loss of data confidentiality on the Internet would have a tremendous impact on society as a whole and the information security of communication systems has currently become our primary concern. The main objective is the protection of confidentiality, integrity and availability (CIA) which are known as the CIA triad [1]. Each category has different branches, which are listed in Fig 1.1. Issues arising in the different branches are distinct through overlapping. According to the International Organization for Standardization (ISO) definition of CIA, confidentiality means which information is not made available or disclosed to unauthorized individuals, entitles or processes; integrity means which data have not been altered or destroyed in an unauthorized manner; and availability indicates being accessible and usable upon demand by an authorized entity.

In the current Internet, various security protocols and mechanisms are utilized to protect the CIA triad. At the boundary between transport layer (layer 4) and session layer (layer 5), secure socket layer (SSL) can tunnel an entire network's traffic. In network layer (layer 3), Internet Protocol

security (IPsec) is a common and standards-based security protocol. In data link layer (layer 2), the virtual private network (VPN), uses of a combination of Ethernet and generalized multiprotocol label switching (GMPLS). All these secure protocols and mechanisms are based on modern cryptographies such as Secure Hash algorithm 1 (SHA-1) for integrity protection and authenticity and advanced encryption standard (AES) for confidentiality.

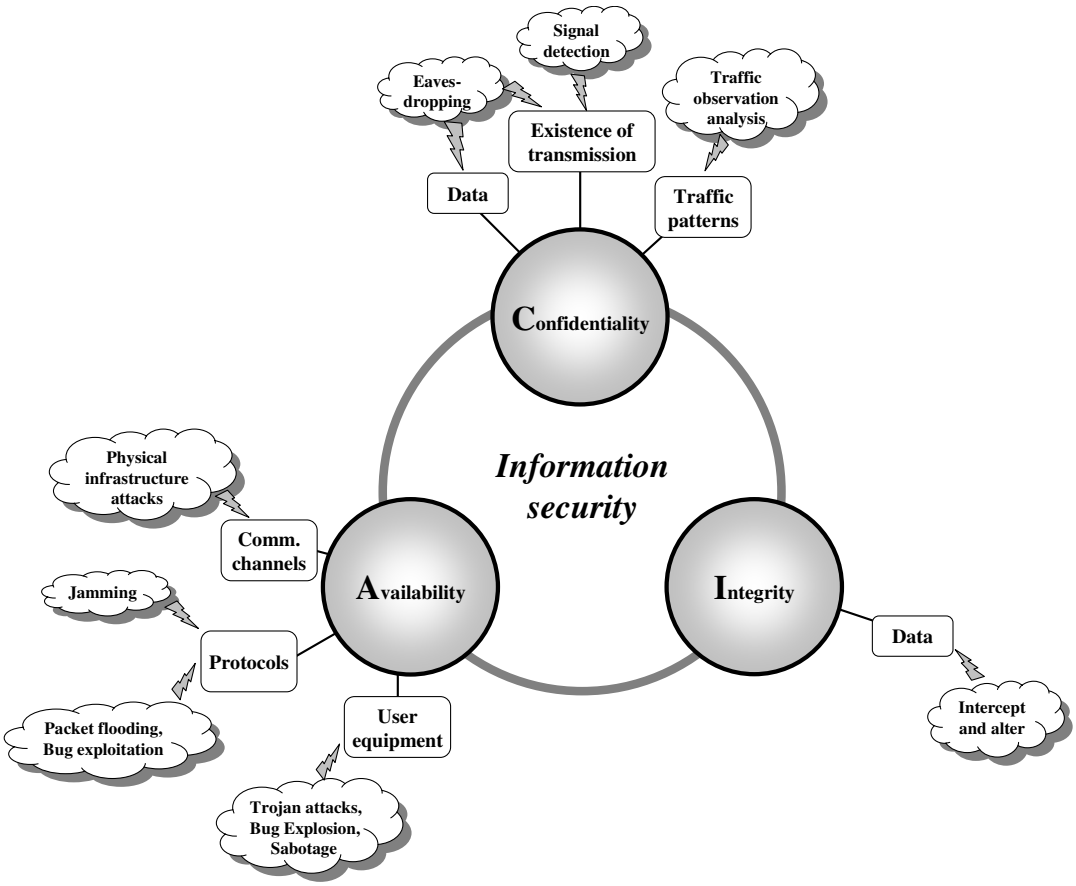



Fig. 1.1: Overall picture of information security.

In contrast to security technologies for the aforementioned layers, security protection in layer 1 has not been attracting much attention. In fact, physical protection of routers, interface cards, and optical fibers has been outside the scope of cryptographic research. The importance of layer 1 security should be stressed because once a security breakdown occurs, a quick stopgap measure will not be easily implemented, but it takes a painfully long time to remedy a physically damaged photonic layer. This is in sharp contrast to the vulnerability in which the upper layers can be restored

in a relatively short time by patching software or releasing new codes online. It should be noted that the security is said to be a chain of trust, and the weakest part is the security level of the whole system. There have been studies on photonic network security. Medard et al. raised early on that security issues of the physical layer, suggesting possible attacks such as crosstalk attacks at optical nodes and fiber tapping [2]. This was followed by studies on monitoring and localization techniques of crosstalk attacks [3], [4], quality of service (QoS) degrading/disruptive attacks [5], such as optical amplifier gain competition attacks, and low-power QoS attacks [6]. Kartalopoulos suggested a possible method of implementing quantum cryptography in optical networks [7]. However, a comprehensive study taking into account physical-level security issues in photonic network remains to be studied.

One may simply assume that network facilities and outside plants can be physically isolated from adversaries. However, optical fiber cables are exposed to physical attacks in customer premises owing to the wide use of fiber-to-the-home (FTTH) systems, and tapping of the optical signal from a fiber could be easily done by using inexpensive equipment [8]. Recently, risk of information leakage occurring in a fiber cable has been pointed out [9]. A small fraction of optical signals, even in a coated fiber, often leaks into adjacent fibers in a cable at the bending points. The amount of light leakage is small but detectable with a photon counting detector. Although, the optical signal in fiber may be encrypted using modern cryptography in the upper layers, its security is not entirely free from constant threats. For example, it was reported that the 768-bit Rivest, Shamir, and Adleman (RSA) cryptosystem was broken by collaborating computing by an international team of Japanese, French, and German researchers in December 2009 [10]. To overcome these problems, demand for high-level photonic layer security technology is growing.

## 1.2 Photonic Layer Security Technology

The data cannot be recovered from the ciphertext by an eavesdropper without any knowledge of the encryption key. This makes encryption an effective way of securing a signal and enhancing the confidentiality of a network. There has been considerable effort to develop optical architectures for implementing fast encryption functions in the optical domain.

Recently, progress has been made in security technologies for layer 1, especially for the photonic layer. Such technologies include quantum key distribution (QKD) which is based on a NO-GO theorem that non-orthogonal quantum states cannot be perfectly discriminated nor copied without errors [11], secure communications using optical chaos (SCOC) which have been studied for secure

communications by masking transmitted data from third parties [12], a quantum noise randomized cipher (QNRC) which can be regarded as a kind of stream cipher enhanced by quantum noise randomization [13], optical code division multiplexing (OCDM) and optical code division multiple access (OCDMA) which have a good data confidentiality using optical code (OC) [14], [15]. All rely on direct control of physical properties of light and hence, are implemented in the photonic domain. They may be referred to as the photonic layer 1 security technology (PL1sec). They can useful for protecting confidential data in photonic networks.

# 1.3 Trend of Optical Access Network

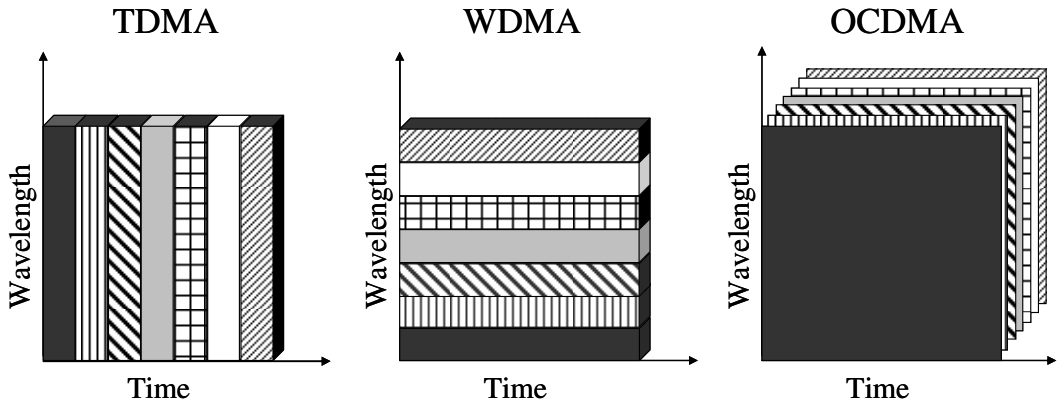



Fig.1.2: Optical access technologies.

In current optical access network, the massive growth of bandwidth in access networks promotes the progress of passive optical networks (PON) system because of the user-shared cost effective facilities. Well known existing optical access techniques include time division multiple access (TDMA), wavelength division multiple access (WDMA) [16], [17], and OCDMA based on OCDM. Figure 1.2 compares the schematic representation of the above technologies.

Figure 1.3 shows the recent trend of optical access network. Recently, the capacity of standardized time division multiplexing (TDM)-PON is reached to 10 Gbit/s (bps) [18], [19]. Therefore, 10 G TDM-PON will appear in the near future. On the other hand, wavelength division multiplexing (WDM)-PON is also considered as Next-Generation (NG)-PON which is an evolutional growth of gigabit-PON. In order to realize more effective future optical access network, NG-PON2 coming after NG-PON1 will bring a revolution change and is planned to be standardized by 2015. NG-PON2 includes several technology candidates such as 40/100 G TDMA, dense wavelength division

multiple access (DWDMA), OCDMA, orthogonal frequency division multiple access (OFDMA) [20].

OCDMA and OFDMA are suitable for optical distribution network (ODN) compatible, and they have unique advantages over TDMA and WDM. Unique advantages of OCDMA include asynchronous "tell-and-go" multiple access capability, soft-capacity on demand, low-latency access due to all-optical en/decoding, and high data confidentiality [21-26].

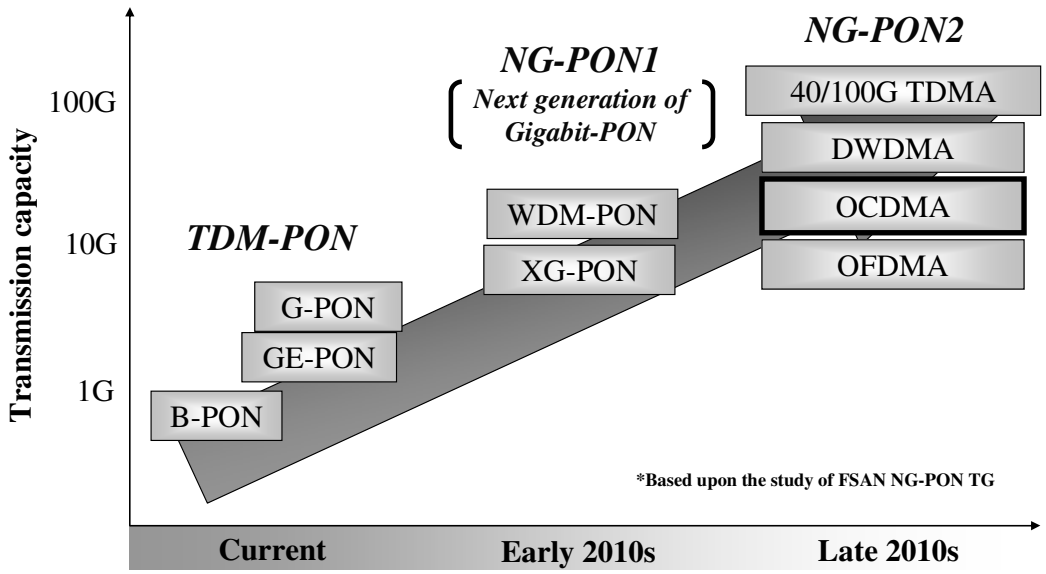



Fig 1.3: Recent trend of optical access network.

# 1.4 Security Issues of Optical Access Network

Access networks will be an easy target for security attacks since the optical signals are at a relatively low bit rate and most of the facilities, such as optical fiber cables, are installed in the open outside plant. Moreover, PON systems, in which an optical fiber is shared by typically up to 32 users, have been widely deployed in access networks, as shown in Fig. 1.4. This point-to-multipoint network topology is inherently prone to security threats, for example, tapping by detecting the leakage of light signal at the bent portion and spoofing by connecting an unauthorized optical network unit (ONU). To prevent such attacks, encryption, such as AES for payload data and authentication for individual ID of the ONU, is generally used for communication between the

optical line terminal (OLT) and each ONU. Thus, PON systems provide reasonable security using currently available techniques. However, it seems worth pursuing newly emerging PL1 security technologies in the long run. Jamming by injecting high power light from the optical fiber is another possible attack, which would paralyze the PON with the breakdown of the receiver, leading to service denial, as shown in Fig. 1.4. This can be prevented by isolating the drop fiber from the optical splitter. For example, jamming light can be shut out by attaching an optical gate, controlled by a photovoltaic module to the fiber [27].

OCDMA originally possesses to provide security functions such as jamming resistance, covertness, and authentication. Nevertheless, confidentiality is one of the most important and widely needed types of security, and beginning chapter 2 will focus primarily on confidentiality.

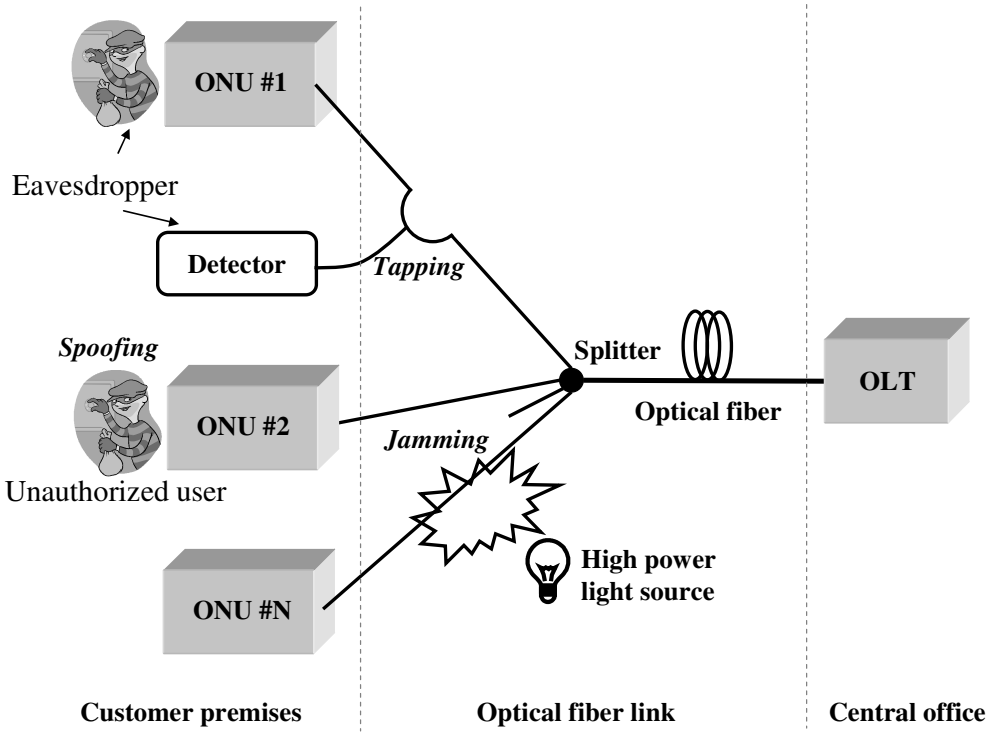



Fig. 1.4: Security threats in PON system.

# 1.5 Overview of the Dissertation

In the following chapters, some OCDM/OCDMA techniques of enhancing confidentiality are discussed. As a method to improve the confidentiality of the block-ciphered M-ary OCDM system,

there are two approaches, such as improving the block-cipher mode and increasing the number of *M*. Chapter 3 introduces block-ciphered M-ary OCDM system using cipher block chaining (CBC) mode which is said to be high confidentiality than usual electronic codebook (ECB) mode. In chapter 4 and 5, the number of *M* can be achieved compared with the conventional M-ary OCDM under the same OC number. All M-ary OCDM systems of Chapters 3, 4 and 5 are summarized in Table 1.1. The contents of each chapter are summarized as follows:

Table 1.1: Comparison of all M-ary OCDM systems.

| **System name** | **Ary number** (Bit block size) | **OC number** | **Block-cipher mode** | **Chapter number** |
|---|---|---|---|---|
| **M-ary OCDM system with XOR** | 16 (4) | 16 | ***CBC*** | 3 |
| **M-ary OCDM system using polarization multiplexing** | ***256*** *(8)* | 16 | ECB | 4 |
| **M-ary OCDM system using multidimensional optical codes** | ***4096*** *(12)* | 15 | ECB | 5 |

Chapter 2 describes the optical encoding/decoding technique. Moreover, the confidentiality evaluation methods of bit-ciphered and block-ciphered OCDM are also described in this chapter. Finally, we introduce the properties of multi-port encoder/decoder (E/D) and PSK OC which are suitable for M-ary OCDM system.

Chapter 3 gives an explanation of M-ary OCDM system with XOR using a single multi-port E/D, which is used the optical implementation of the CBC mode. Then, we experimentally demonstrate 16-ary OCDM system with XOR. With this system, we also demonstrate 50km transmission for the first time.

Chapter 4 discusses polarization multiplexed (POL-MUX) M-ary OCDM system using a single multi-port E/D. Then, we experimentally demonstrate POL-MUX 256-ary OCDM system. In conventional M-ary OCDM, the number of OC is limited by the port count of multi-port E/D, and it would be desirable if the M-ary number can be increased without increasing the number of OC. By using POL-MUX M-ary OCDM method, the number of *M* can be increased. Moreover, the physical confidentiality is also improved. We also discuss and analyze the corresponding data security in terms of data confidentiality.

Chapter 5 discusses M-ary OCDM system using multidimensional codes. Multidimensional codes

consist of OC combinations generated by a single multi-port E/D. Therefore, high M-ary system is achieved by using these codes. We experimentally demonstrate the operation principle of 4096-ary OCDM system for the first time. Then, we show that the impairment due to multiple access interference affects the system performance. We also analyze the data confidentiality. Moreover, we discuss an extension M-ary OCDM to multiple access, M-ary OCDMA-based PON system, that uses a multi-port E/D in the central office and in the users premises. Finally, we show the feasibility of a 10 Gbps, 4096-ary OCDMA-based PON system using multidimensional code by numerical simulation.

Chapter 6 gives the conclusions of the dissertation by summarizing the overall results.

# Chapter 2

# Overview of Optical Code Division Multiplexing

## 2.1 Introduction

The OCDM technology has gained attention for the secure optical access network based on PON. A key issue in the OCDM approach is the method of enhancing the data confidentiality. In Section 2.2, fundamentals of an optical encoding and decoding are described. Sections 2.3 and 2.4 describes the bit-ciphered and block-ciphered OCDM schemes, respectively. Section 2.5 shows the method of confidentiality analysis and compares these methods. Section 2.6 describes multi-port E/D and PSK OC.

## 2.2 Principle of Optical Encoding/Decoding

### 2.2.1 Optical Encoding

There are a number of different optical encoding schemes, which can be classified according to

their operation principle as incoherent or coherent schemes, or according to their processing dimensions as one-dimensional (1-D), or two-dimensional (2-D) schemes. Figure 2.1 shows an illustration of these classifications.

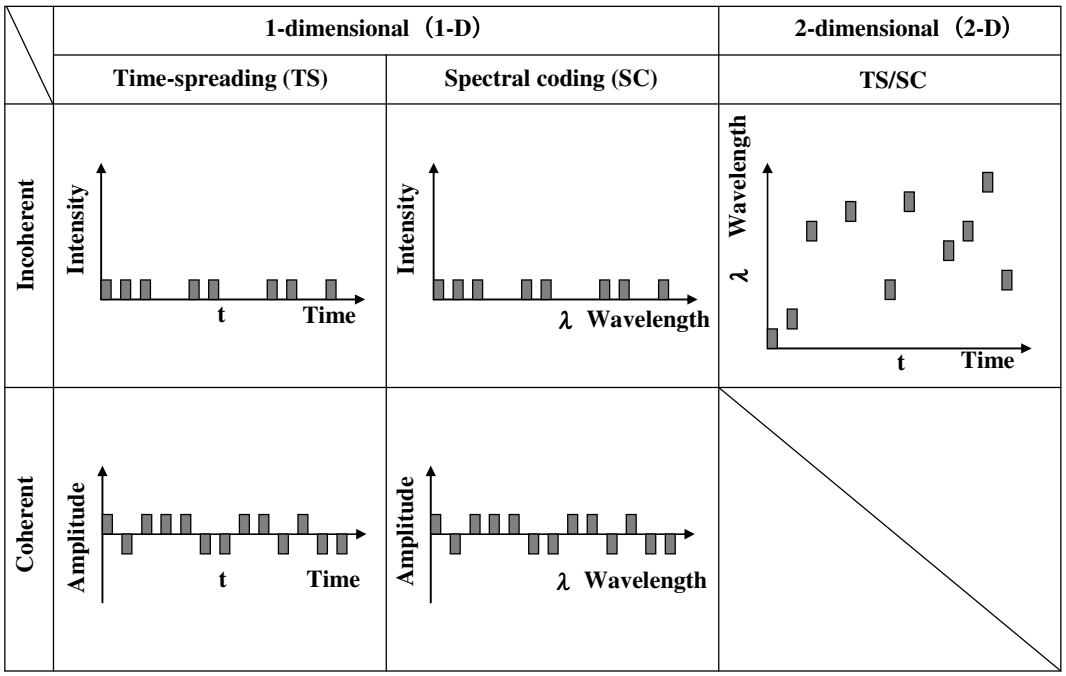



Fig. 2.1: Classification of different optical encoding schemes.

In incoherent scheme, the coding is performed on optical power basis, therefore, the OCs are handled in unipolar (0, 1) manner, which results in disadvantages such as small code size, low optical power and bandwidth efficiency, and poor correlation property [21, 22, 24, 25, 28-39]. In contrast, coherent schemes, which work on a field-amplitude basis, process OCs are handled in the bipolar (-1, +1) manner all optically; thus coherent schemes are superior to incoherent schemes in the overall performance [24, 25, 28-30, 40-48]. On the other hand, OCs could be processed in either the time domain [32-34, 43-48] or the wavelength domain in 1-D schemes, and in wavelength and time domains [35-39] simultaneously in 2-D schemes.

Hereafter, a focus will be on the coherent approach. There are two encoding schemes; encoding in time domain and that in wavelength domain. As shown in Fig. 2.2, the encoder generates phase-shift keying (PSK) signals with *N* time-resolved chip pulse code within one bit time duration in which the phase shift of each chip pulse represents a code sequence [49-51]. On the other hand, as shown in Fig. 2.3, the spectrum encoder creates *N* space-resolved code [32, 52, 53].

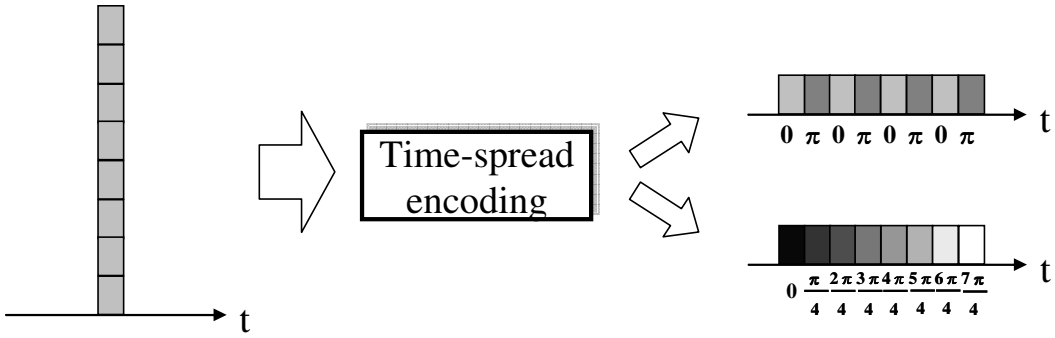



Fig. 2.2: Encoding model of TS-OC.

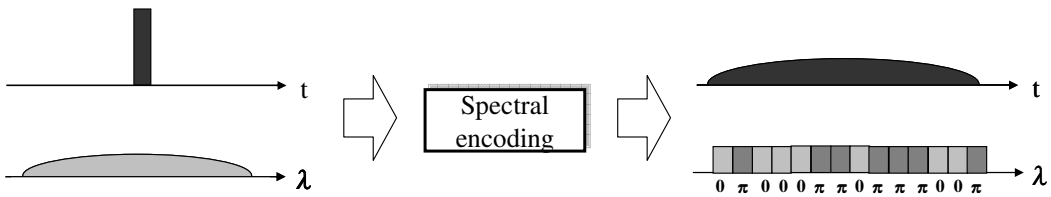



Fig. 2.3: Encoding model of SC-OC.

### 2.2.2 Optical Decoding

Matched filtering in optical domain is a basis of the optical decoding. In general, matched filtering is a detection technique which maximizes the signal-to-noise ratio of the received signal. The impulse response of matched filter $h_d(t)$ along with its Fourier spectrum $H_d(\omega)$ is the complex conjugate of optical encoder output, and it is given by

$$H_d(\omega) = H_e(\omega)^* \varepsilon^{-\mathbf{j}\omega\, t_0} \tag{2.1}$$

$$h_d(t) = h_e(t_0 - t) \tag{2.2}$$

where **j** denotes the imaginary unit, $h_e(t)$ denotes the function of OC, $H_e(\omega)$ denotes its Fourier spectrum, and $^*$ is complex conjugate unit. Then, the output of matched filter $u_0(t)$ is expressed by the convolution of the impulse responses of the encoder and the matched filter

$$
\begin{aligned}
u_0(t) &= \int_{-\infty}^{\infty} H_e(\omega) H_d(\omega) \varepsilon^{\mathrm{j}\omega t} d\omega \\
&= \int_{-\infty}^{\infty} \left| H_e(\omega) \right|^2 \varepsilon^{\mathrm{j}\omega(t-t_0)} d\omega \\
&= \int_{-\infty}^{\infty} h_e(t') h_e(t' - t + t_0) dt' \\
&\equiv \psi(t - t_0)
\end{aligned}
\tag{2.3}
$$

where $\psi(t)$ represents the auto-correlation function of the input OC. The matched filtering response can be physically realized in optical domain by time-reversing the input/output of the optical encoder. Two different schemes of optical decoding are illustrated in Figs. 2.4 and 2.5.

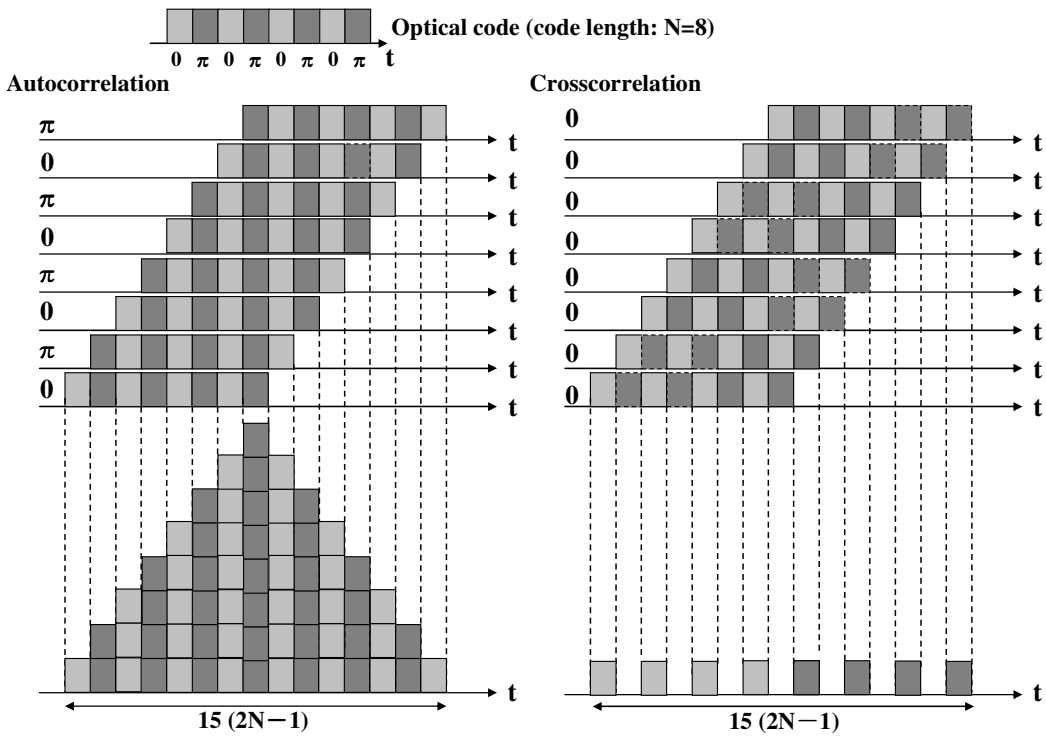



Fig. 2.4: Decoding model of TS-OC.

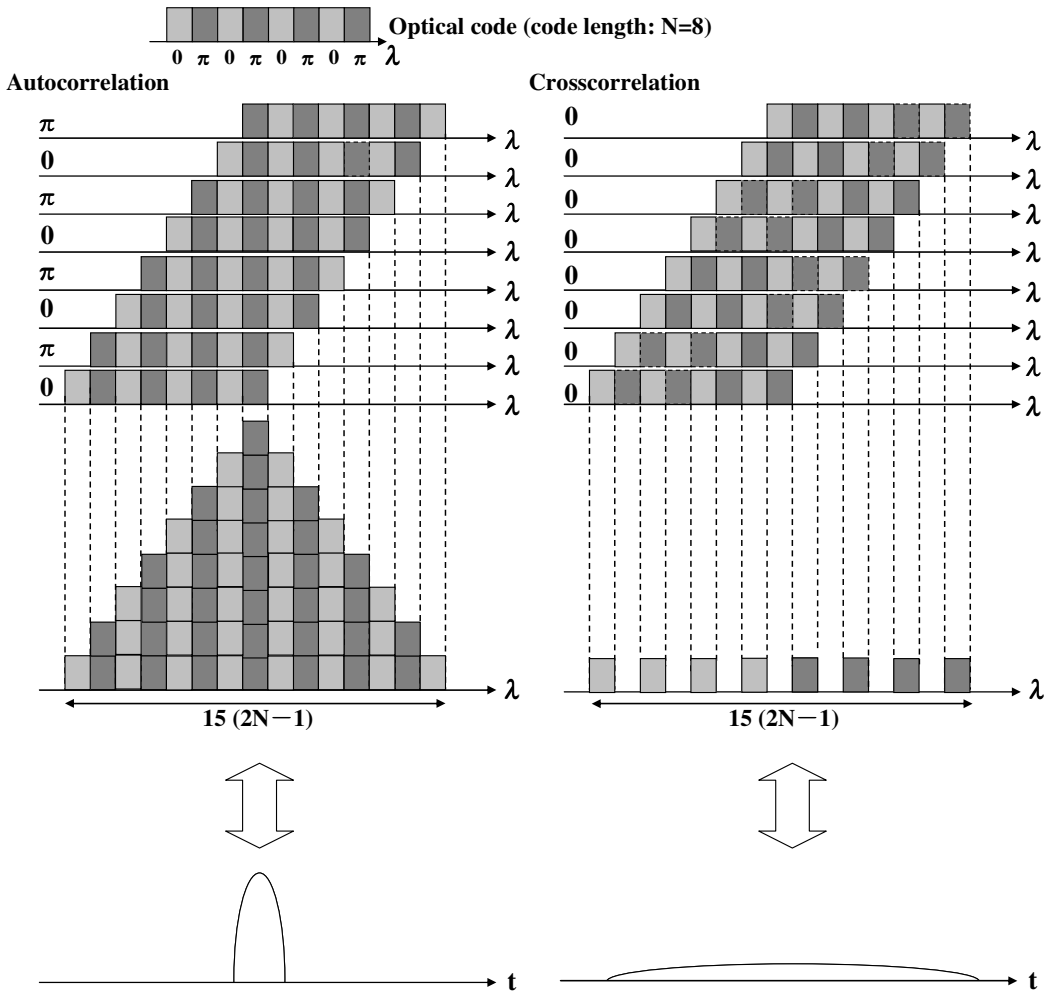



Fig. 2.5: Decoding model of SC-OC.

## 2.3 Bit-ciphered Optical Code Division Multiplexing

A bit-cipher cryptographic system creates a one-to-one correspondence between each bit from each user and an OC. This encryption scheme can be designed to be computationally secure against cipher-text only attacks (COA) by increasing the number of codes, but it is completely vulnerable against some of the cryptographic attacks. Since COA is the simplest attack for the eavesdropper to perform, bit-ciphering schemes present the weakest form of security, even though they are the only kind of confidentiality considered in the literature on OCDM [54].

In conventional bit-ciphering schemes as shown in Fig. 2.6, on-off keying (OOK)-, differential-phase-shift-keying (DPSK)-, and code-shifting-keying (CSK)-OCDM systems have been investigated and experimentally demonstrated during the past decade. However, a careful analysis of the security reveals that the bit-ciphering approach of a conventional OCDM system, where each bit is transformed into an OC, is not resistant against the main confidentiality attacks. In OOK-modulated OCDM systems, an eavesdropper can break the confidentiality by simple data-rate power detection without any information about the OC [54-56]. In DPSK-modulated OCDM architectures [57], an eavesdropper can decipher the transmitted data, without any knowledge about the OC, using a commercial DPSK decoder and a data-rate power detector [58]. On the other hand, in CSK-modulated OCDM transmission [59, 60], an eavesdropper who is able to detect any difference between the two codes (with a time or a spectral analysis) can break the confidentiality, without any optical decoding process. Therefore, a through security analysis has shown that conventional OCDM bit-ciphering schemes, where each bit is transformed into an OC, is not robust against most confidentiality attacks. To overcome these problems, block-ciphering method is proposed [61, 62] and demonstrated [63, 64].

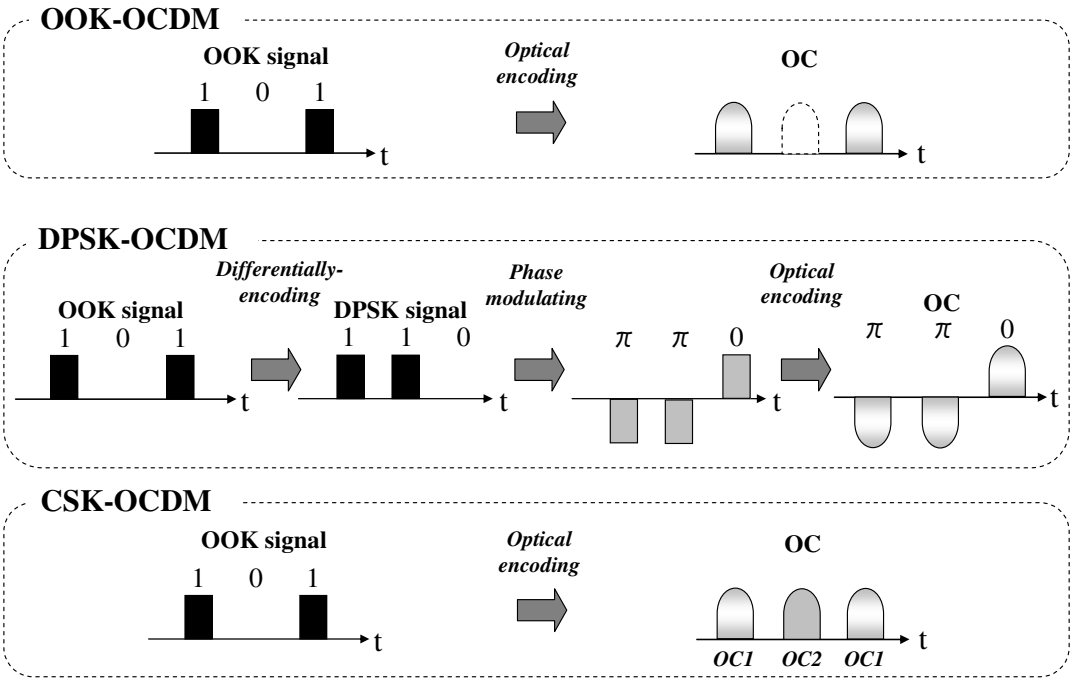



Fig. 2.6: Classification of different bit-ciphered OCDM schemes.

## 2.4 Block-ciphered (M-ary) Optical Code Division Multiplexing

In this scheme, data confidentiality relies on the correspondence of a message block of $m$ bits and a ciphertext with at least $M=2^m$ determinations. Symmetric encryption systems, like data encryption standard (DES) or AES are also used $2^m$-bits block ciphers, designed to generate a one-to-one mapping that looks random, according to the Feistfel method [65].

The simplest block-cipher mode is the ECB encryption as shown in Fig. 2.7, where the message is divided into bit blocks, that are encrypted separately. This ciphering scheme corresponds to M-ary OCDM as shown in Fig. 2.8. In M-ary OCDM, a set of $M$ code words is assigned to each user, and different sequences of $\log_2 M$ bits of a message are mapped onto different OCs. The code lookup table is shown in Table 2.1. This scheme presents two levels of confidentiality: physical-layer confidentiality, because an adversary should be able to correctly detect the OC, and computational confidentiality, since he or she does not know which sequence of bits corresponds to a given OC, and the number of possible combinations equates $M!$. In conventional M-ary OCDM experiments, 4-ary OCDM using integrated passive optical phase decoders have been demonstrated with a set of $\log_2 M$ parallel receivers [64]. However, the number of E/D required for each user is larger. To overcome this limitation, M-ary OCDM system using the unique device, which is a multi-port E/D [66-68] that can simultaneously generate as many codes as the number of its port, has been proposed [69].

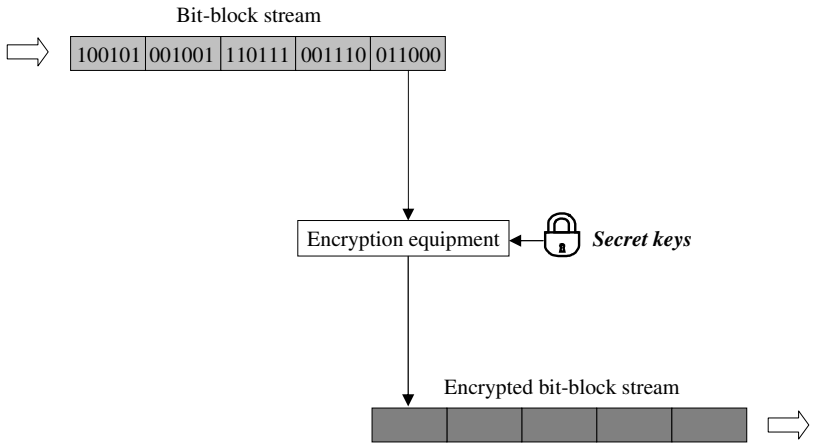



Fig. 2.7: Configuration of ECB mode.

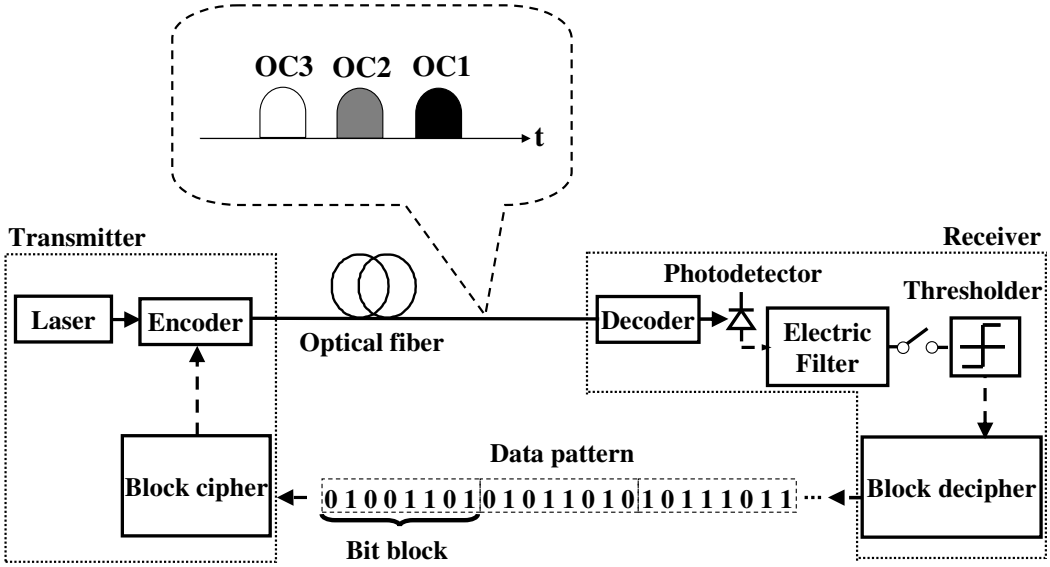



Fig. 2.8: M-ary OCDM architecture.

Table 2.1: Code lookup table.

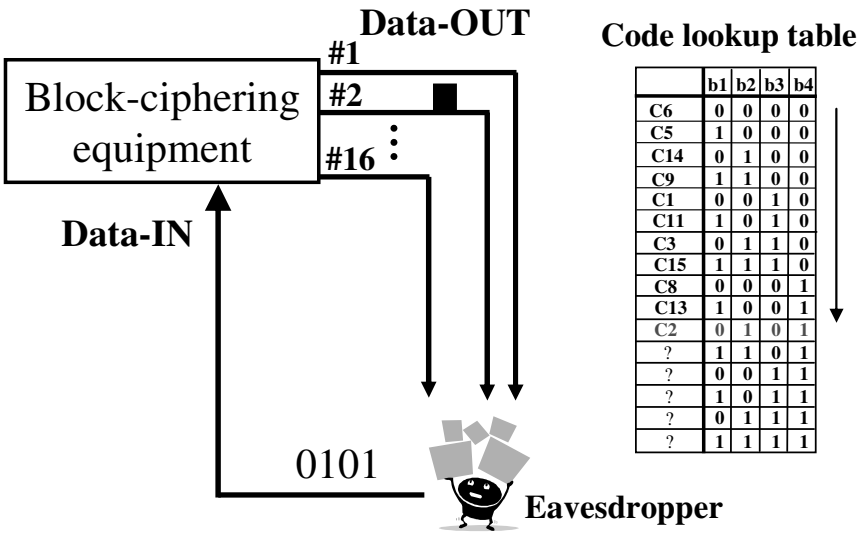
| Bit block | OC |
|---|---|
| 01001101 | OC1 |
| 01011010 | OC2 |
| 10111011 | OC3 |
| ⋮ | ⋮ |

## 2.5 Modeling of Confidentiality Evaluation

As already mentioned, OCDMA systems are often considered potentially secure because multiple users transmit simultaneous encoded signals. However, their vulnerability must be analyzed considering the worst-case condition, assuming that the eavesdropper is able to intercept isolated signal. The analysis is considered that the security performance of a point-to-point (P2P) optically private-key transmission, and, according to the Kerckhoff's principle [70]. Under this principle, the eavesdropper knows the OCDM encoding technique, in terms of data and chip rates, code length,

modulation formats, wavelengths, etc; the only unknown parameter is the particular code of a known code family that the user is employing [71]. Therefore, OCDM confidentiality has been often analyzed as a function of the number of keys, that given device is able to generate. To give a quantitative confidentiality evaluation of OCDM system, we consider two cryptographic attacks, COA and chosen plaintext attacks (CPA) in subsequent chapters. Figure 2.9 shows the simple model of CPA. In CPA, the eavesdropper has access to the encryption function and can encrypt any plaintext message unit of his choice, trying to determine the key. For instance the knowledge that a common message (like a 'Hallo' packet) is transmitted can be used to break the network security within this attack.

To give a quantitative evaluation of the confidentiality of bit- and block-ciphered OCDM schemes, COA is firstly considered as shown in Fig. 2.10. The average number of trials needed to break the confidentiality is $2^m!/2$. Then, the number of bits encoded in a single block is $m=\log_2 M$, and the possible correspondences between a bit sequence and M-ary number. In the case of considering CPA, the average number of trials versus bit block length is shown in Fig. 2.11: in a bit-ciphering scheme, just single attack allows the eavesdropper to intercept the data. In block-ciphered scheme, instead, the number of trials required are $2^m$-1 [72].




| | b1 | b2 | b3 | b4 |
|---|---|---|---|---|
| C6 | 0 | 0 | 0 | 0 |
| C5 | 1 | 0 | 0 | 0 |
| C14 | 0 | 1 | 0 | 0 |
| C9 | 1 | 1 | 0 | 0 |
| C1 | 0 | 0 | 1 | 0 |
| C11 | 1 | 0 | 1 | 0 |
| C3 | 0 | 1 | 1 | 0 |
| C15 | 1 | 1 | 1 | 0 |
| C8 | 0 | 0 | 0 | 1 |
| C13 | 1 | 0 | 0 | 1 |
| C2 | 0 | 1 | 0 | 1 |
| ? | 1 | 1 | 0 | 1 |
| ? | 0 | 0 | 1 | 1 |
| ? | 1 | 0 | 1 | 1 |
| ? | 0 | 1 | 1 | 1 |
| ? | 1 | 1 | 1 | 1 |

Fig. 2.9: CPA model.

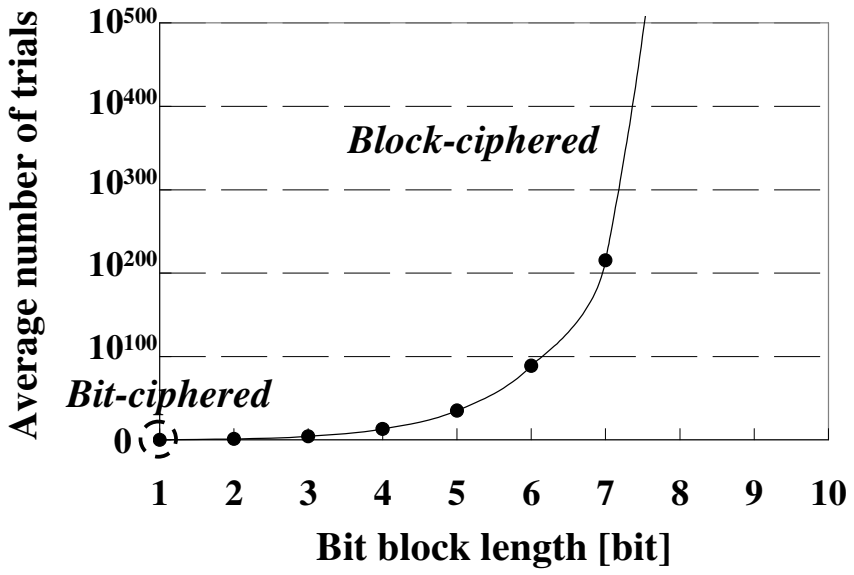



Fig. 2.10: Number of trials to break the confidentiality with COA.

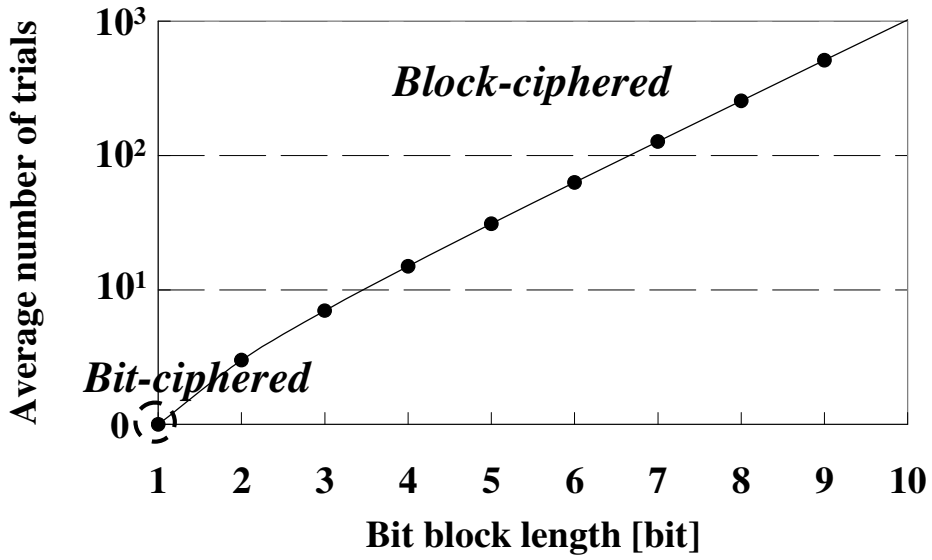



Fig. 2.11: Number of trials to break the confidentiality with CPA.

# 2.6 PSK Optical Code Generated by Multi-port Encoder/Decoder

### 2.6.1 Configuration of Multi-port Encoder/Decoder [67]

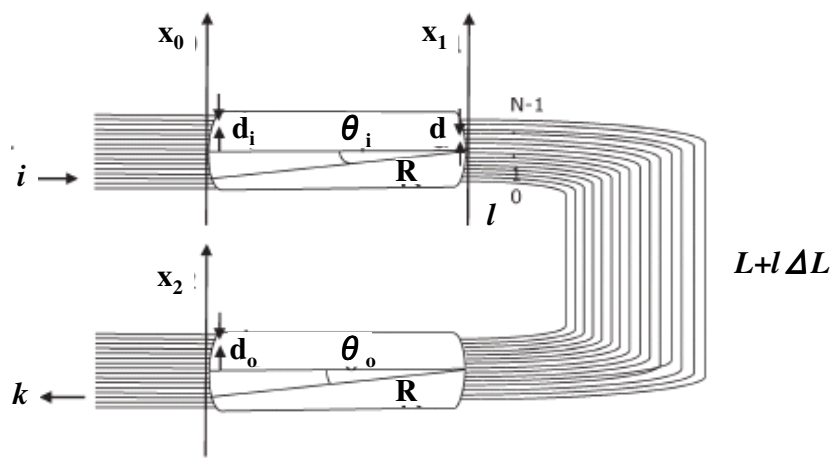



Fig. 2.12: Multi-port E/D configuration.

Table 2.2: Parameters of multi-port E/D

| *Symbol* | *Description* | *Value* |
|---|---|---|
| $\omega_0$ | center angle frequency ( $\lambda$ =1550.984nm) | 193.292 THz |
| $N$ | port count | 16 |
| $R$ | input/output slabs focal length | 20.85 mm |
| $d$ | AWG spacing | 24.6 $\mu$ m |
| $w_g$ | AWG waveguide width | 7 $\mu$ m |
| $d_i$ | waveguide spacing in the input grating | 56.47 $\mu$ m |
| $d_o$ | waveguide spacing in the output grating | 56.47 $\mu$ m |
| $w_{i/o}$ | waveguide width in the input/output grating | 50 $\mu$ m |
| $\triangle L$ | differential path length | 1.0316 mm |
| $n_s$ | effective refractive index | 1.468 |

The mechanism to build a set of OCs can be easily described analyzing the AWG in the time domain: If a short pulse light source is driven into one of the device inputs, *N* copies of the pulse

are generated by the input slab coupler, with phases given by the Rowland circle configuration [66]. The optical pulses travel different paths in the grating and the output slab coupler recombines the pulses to build $N$ codes at the device outputs. Each PSK code is composed of $N$ optical chips, and the differential path delay in the grating is chosen larger than the input pulsewidth, so that the chips in the OC do not overlap. Referring to Fig.2.12 and the parameters listed in Table 2.2, the impulse response between the input $i$ and the output $k$ can be written as

$$h_{ik}(t) = \sum_{l=0}^{N-1} \exp\left[-\mathbf{j}\pi \frac{n_s d}{\lambda}(2l - N + 1)(\sin\theta_i + \sin\theta_o)\right] \times \delta\left(t - n_s \frac{L + l\Delta L}{c}\right) \tag{2.4}$$

$$i, k = 0,1,\ldots,N-1$$

where $\mathbf{j} = \sqrt{-1}$, $\delta(t)$ is the Dirac's delta function, $L$ is the smallest waveguide length, and $\theta_i$, $\theta_o$ are the diffraction angles in the input and output slabs, respectively

$$\sin\theta_i \cong (2i - N + 1)\frac{d_i}{2R}, \qquad \sin\theta_o \cong (2k - N + 1)\frac{d_o}{2R}. \tag{2.5}$$

For the sake of simplicity, the condition is assumed $L = 0$, as its value does not affect the code generation/processing, but it only corresponds to a constant time delay. The chip interval, i.e., the time distance between two consecutive pulses in each code is $\Delta\tau = n_s \Delta L / c$ and it equates with the inverse of the free spectrum range (FSR) of an arrayed waveguide grating (AWG) multiplexer/demultiplexer, and the correlation time is given by $(N-1)\Delta\tau$. From the parameters listed in Table 2.2, it is $\Delta\tau = 5$ ps.

The exponential term in Eq. (2.4) corresponds to the phase of each chip in the code: We set $d_i = d_o$, i.e., identical spacing in the input and output gratings, and then Eq. (2.4) can be reduced

$$h_{ik}(t) = \sum_{l=0}^{N-1} \exp\left[-\mathbf{j}\frac{\pi}{N}(2l - N + 1)(i + k + 1)\right] \times \delta(t - l\Delta\tau). \tag{2.6}$$

$$i, k = 0,1,\ldots N-1$$

The OCs are N-ary PSK codes; in particular, for a given input port $i$, the code generated at the output $k = N - i - 1$ has all the chips with identical phase.

### 2.6.2 Correlation Property

The multi-port E/D is able to perform all the correlations, simultaneously. In fact, if an OC is sent to the input port *i*, at all the output ports $l = 0,1,\ldots N-1$, The autocorrelation peak (ACP) detected at one of the device outputs univocally discriminates the incoming OC. According to the Parseval theorem, the correlation function between two OCs generated at the outputs *k* and *k*' can be evaluated in the frequency domain

$$h_{ik}(t) * h_{ik'}(t) = \int_{-\infty}^{\infty} H_{ik}(\omega) H_{ik'}(\omega) \exp(\mathbf{j}\omega t) dt \tag{2.7}$$

$$k, k' = 0,1,\ldots N-1$$

where $*$ denotes the convolution unit and $H_{ik}(f)$ is the transfer function from the input *i* to the output *k*, obtained by Fourier transform of Eq. (2.6)

$$\begin{aligned} H_{ik}(\omega) &= \sum_{l=0}^{N-1} \exp\left[-\mathbf{j}\pi(2l-N+1)\left(\frac{i+k+1}{N}+\frac{\omega\Delta\tau}{2\pi}\right)\right] \\ &= \exp\left[-\frac{\mathbf{j}\omega(N-1)\Delta\tau}{2}\right] \frac{\sin\left[\pi\left(i+k+1+\frac{\omega N\Delta\tau}{2\pi}\right)\right]}{\sin\left[\pi\left(\frac{i+k+1}{N}+\frac{\omega\Delta\tau}{2\pi}\right)\right]} \end{aligned} \tag{2.8}$$

$$i, k = 0,1,\ldots N-1.$$

The power spectra are plotted in Fig. 2.13. Two OCs are orthogonal if the crosscorrelation function of Eq. (2.7) vanishes everywhere, and this happens if the two corresponding transfer functions $H_{ik}(\omega)$ and $H_{ik'}(\omega)$ do not overlap and their product is zero. Therefore, Eq. (2.7) links the code-recognition capability of a full E/D to the spectral response of a multiplexer/demultiplexer, and the lower the crosstalk between two adjacent frequency channels, the "more orthogonal" are the corresponding OCs. The OC generated at two adjacent outputs are "less orthogonal" since the crosstalk between the two adjacent frequency channel is higher; the detection capability of a code set is defined as the ratio between the ACP and the maximum crosscorrelation peak (CCP), and in line with the previous reasoning, we can say that the lower parameter corresponds to the OCs generated at two adjacent outputs.

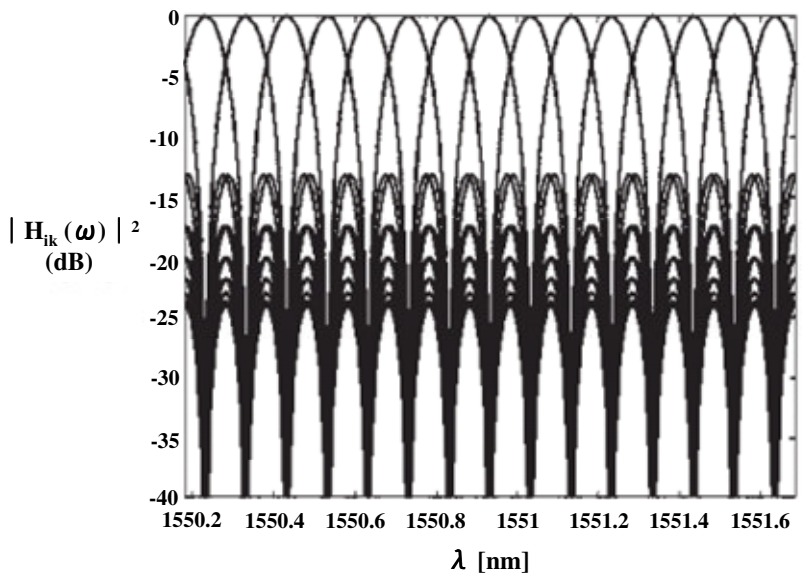



Fig. 2.13: Transfer function at two adjacent output ports.

The correlation signal is computed by substituting Eq. (2.6) into (2.7) and performing simple algebra

$$
\begin{aligned}
h_{ik}(t) * h_{ik'}(t) = & \sum_{l=0}^{N-1}\sum_{l'=0}^{N-1} \exp\left[-\mathbf{j}\frac{\pi}{N}(2l-N+1)(i+k+1)\right] \\
& \times \exp\left[-\mathbf{j}\frac{\pi}{N}(2l'-N+1)(i+k'+1)\right] \\
& \times \delta\left[t-(l+l')\Delta\tau\right] \\
= & \sum_{l=0}^{N-1} \exp\left[-\mathbf{j}\frac{2\pi(l+1)}{N}(i+k+1)\right] \\
& \times \sum_{l'=0}^{l} \exp\left[-\mathbf{j}\frac{2\pi l'}{N}(k'-k)\right]\delta(t-l\Delta\tau) \\
& + \sum_{l=N}^{2N-2} \exp\left[-\mathbf{j}\frac{2\pi(l+1)}{N}(i+k+1)\right] \\
& \times \sum_{l'=l+1}^{2N-1} \exp\left[-\mathbf{j}\frac{2\pi l'}{N}(k'-k)\right]\delta(t-l\Delta\tau) \\
& \qquad\qquad i,k,k' = 0,1,\ldots N-1.
\end{aligned}
\tag{2.9}
$$

To evaluate the autocorrelation function, $k' = k$ is considered in the previous expression

$$h_{ik}(t) * h_{ik'}(t) = \sum_{l'=0}^{N-1} \exp\left[-\mathbf{j}\frac{2\pi l+1}{N}(i+k+1)\right](l+1)\delta(t-l\Delta\tau) + \sum_{l=N}^{2N-2} \exp\left[-\mathbf{j}\frac{2\pi(l+1)}{N}(i+k+1)\right] \times (2N-l-1)\delta(t-l\Delta\tau) \tag{2.10}$$

$$i,k = 0,1,\ldots N-1$$

and the ACP occurs at $t = (N-1)\Delta\tau$ and

$$ACP = \left|h_{ik}(t) * h_{ik}(t)\right|_{t=(N-1)\Delta\tau} = N \tag{2.11}$$

$$i,k = 0,1,\ldots N-1.$$

Furthermore, the maximum sidelobe (MSL) of the autocorrelation function is $MSL = (N-1)$. In the case $k' \neq k$, the crosscorrelation function of Eq. (2.9) becomes

$$h_{ik}(t) * h_{ik'}(t) = \exp\left[-\mathbf{j}\frac{\pi(k-k')}{2N}\right] \times \sum_{l=0}^{2N-2} \exp\left[-\mathbf{j}\frac{2\pi(l+1)}{N}(i+1+\frac{k-k'}{2})\right] \times \frac{\sin\left[\frac{\pi(l+1)(k-k')}{N}\right]}{\sin\left[\frac{\pi(k-k')}{N}\right]}\delta(t-l\Delta\tau) \tag{2.12}$$

$$i,k,k' = 0,1,\ldots N-1$$

and the maximum CCP occurs at $t = \left[(2q+1)/2(k-k')-1\right]\Delta\tau$ with $q = 0,1,\ldots\lfloor 2(2N-1)(k-k')/N \rfloor$, where $\lfloor\ \rfloor$ denotes the integer part, and is

$$CCP = \left|h_{ik}(t) * h_{ik'}(t)\right|_{\left[\frac{N}{2}(k-k')-1\right]\Delta\tau} = \frac{1}{\sin\left[\frac{\pi(k-k')}{N}\right]} \tag{2.13}$$

$$i,k = k' = 0,1,\ldots N-1.$$

Figure 2.14 (a) shows the intensity and the phase of OC generated by a 2 ps width Gaussian-shape

pulse, and the corresponding autocorrelation function is shown in Fig. 2.14 (b). Figure 2.14 (c) and (d) show the crosscorrelation functions between OCs generated at two adjacent output ports and at two far-apart ports, respectively. The code-detection parameter is

$$r = \frac{(ACP)^2}{(CCP)^2} = N^2 \sin^2\left[\frac{\pi(k-k')}{N}\right] \tag{2.14}$$

$$i, k = k' = 0,1,\ldots N-1.$$

The lower value of $r$ corresponds to two OCs generated at two adjacent outputs (i.e., $k = k'+1$).

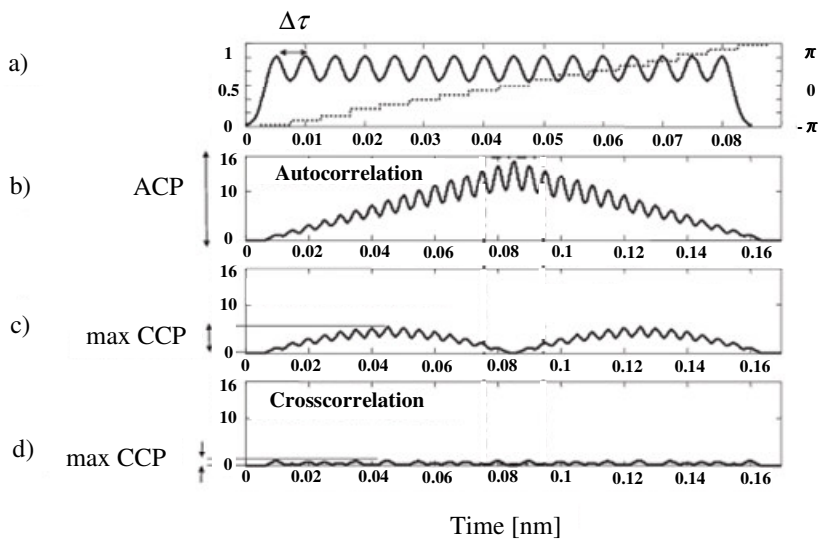



Fig. 2.14: (a) PSK code generated by the device, for an input 2-ps Gaussian-shape pulse. (b) Autocorrelation waveform. (c) Maximum crosscorrelation waveform. (d) Minimum crosscorrelation waveform.

### 2.6.3 Dispersion Effect to Optical Coded Signal

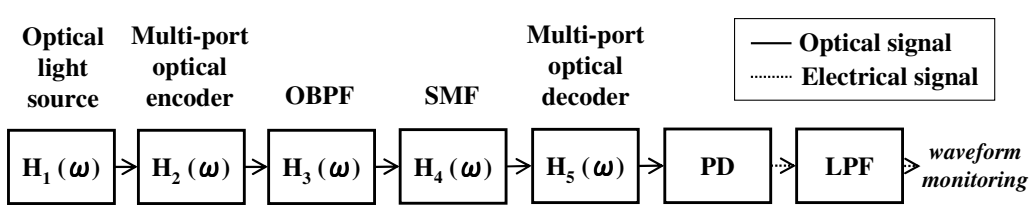



Fig. 2.15: Model of transmission link.

Table 2.3: Parameters used in numerical simulation.

| | |
|---|---|
| Input optical pulse | Pulse shape: Gaussian<br>Center wavelength: 1550 nm<br>Repetition rate: 10 GHz<br>Pulse width: 2 ps |
| OBPF | Filtering shape: Rectangular<br>-3 dB band width: 1.6 nm |
| SMF | Fiber length: 25, 50, 75, 100, 125, 150 km |
| LPF | Filtering shape: Gaussian<br>-3 dB band width: 0.85 nm |

OC transmission system is modeled by the cascaded optical transfer functions of single mode fiber (SMF), multi-port E/D which has port count 16, optical band pass filter (OBPF), followed by the photo-detector, and low pass filter (LPF) as shown in Fig. 2.15. Table 2.3 shows the parameters used in the numerical simulation. Single pulse propagation in SMF can be expressed using nonlinear Schrödinger (NLS) equation [73]. The equation can be written as:

$$\mathbf{j}\frac{\partial U}{\partial z} = -\frac{\mathbf{j}\alpha}{2}U + \frac{\beta_2}{2}\frac{\partial^2 U}{\partial t^2} - \gamma|U|^2 U \tag{2.15}$$

where $U$ ($z$, $t$) represents a complex envelope of electrical field, $\alpha$ is a loss parameter, and $\gamma$ is a nonlinear parameter. Here, transmission distance is considered below 150 km. The simulation is performed in a linear regime by ignoring the fiber nonlinearity. The effects of group velocity dispersion (GVD) on optical pulses propagating in a linear dispersive medium are studied by setting $\gamma$=0 and $\alpha$=0 (loss less) in Eq. (2.15). Then, $U$ satisfies the following linear partial differential equation:

$$\mathbf{j}\frac{\partial U}{\partial z} = \frac{\beta_2}{2}\frac{\partial^2 U}{\partial t^2}. \tag{2.16}$$

Equation (2.16) is readily solved by using the Furier-transform method. If $\tilde{U}$ ($z$, $\omega$) is the Fourier transform of $U$ such that

$$U(z,t) = \frac{1}{2\pi}\int_{-\infty}^{\infty}\tilde{U}(z,\omega)\exp(-\mathbf{j}\omega t)d\omega, \tag{2.17}$$

then $\tilde{U}$ satisfies an ordinary differential equation

$$\mathbf{j}\frac{\partial\tilde{U}}{\partial z} = -\frac{1}{2}\beta_2\omega^2\tilde{U} \tag{2.18}$$

whose solution is given by

$$\tilde{U}(z,\omega) = \tilde{U}(0,\omega)\exp\left(\frac{\mathbf{j}}{2}\beta_2\omega^2 z\right). \tag{2.19}$$

Equation (2.19) shows that GVD changes the phase of each spectral component of the pulse by an amount that depends on both the frequency and the propagation distance. Even though such phase changes do not affect the pulse spectrum, they can modify the pulse shape. By substituting Eq. (2.19) in Eq. (2.17), the general solution of Eq. (2.16) is given by

$$U(z,t) = \frac{1}{2\pi}\int_{-\infty}^{\infty}\tilde{U}(0,\omega)\exp\left(\frac{\mathbf{j}}{2}\beta_2\omega^2 z - \mathbf{j}\omega t\right)d\omega \tag{2.20}$$

where $\tilde{U}(0,\omega)$ is the Fourier transform of the incident field at $z = 0$ and is obtained by

$$\tilde{U}(0,\omega) = \int_{-\infty}^{\infty}U(0,t)\exp(\mathbf{j}\omega t)dt. \tag{2.21}$$

Consider the case of Gaussian-shape OC chip pulse for which the incident field is of the form

$$G(0,t) = \exp(-\frac{t^2}{2T_0^2}) \tag{2.22}$$

where $T_0$ is the half-width (at 1/*e*-intensity point). By substituting Eq. (2.22) in (2.10), autocorrelation waveform after decoding is given by

$$U(0,t)=\sum_{l'=0}^{N-1}\exp\left[-\mathbf{j}\frac{2\pi l+1}{N}(i+k+1)\right](l+1)\exp(-\frac{t^2}{2T_0^2})$$
$$+\sum_{l=N}^{2N-2}\exp\left[-\mathbf{j}\frac{2\pi(l+1)}{N}(i+k+1)\right] \tag{2.23}$$
$$\times(2N-l-1)\exp(-\frac{t^2}{2T_0^2}).$$

By substituting Eqs. (2.21) and (2.23) in (2.20), autocorrelation after transmission can be expressed. In Fig. 2.16, the numerically calculated autocorrelation waveforms after the propagation up to 150 km are shown. As the transmission distance is extended, we can confirm the spread of waveform due to the dispersion effect. Figure 2.17 shows the evolution of autocorrelation train along the fiber length. Here, 10Gbps, OOK-OCDM signal of 7-bit random data pattern is considered to confirm the dispersion effects clearly. As longer the propagation becomes, the inter-symbol interference (ISI) becomes visible as dashed circle part.

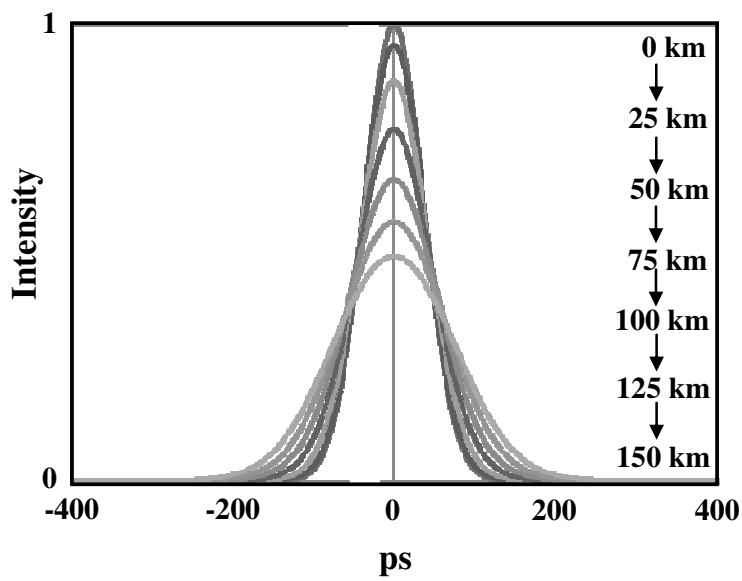



Fig. 2.16: Normalized intensities of autocorrelation waveform.

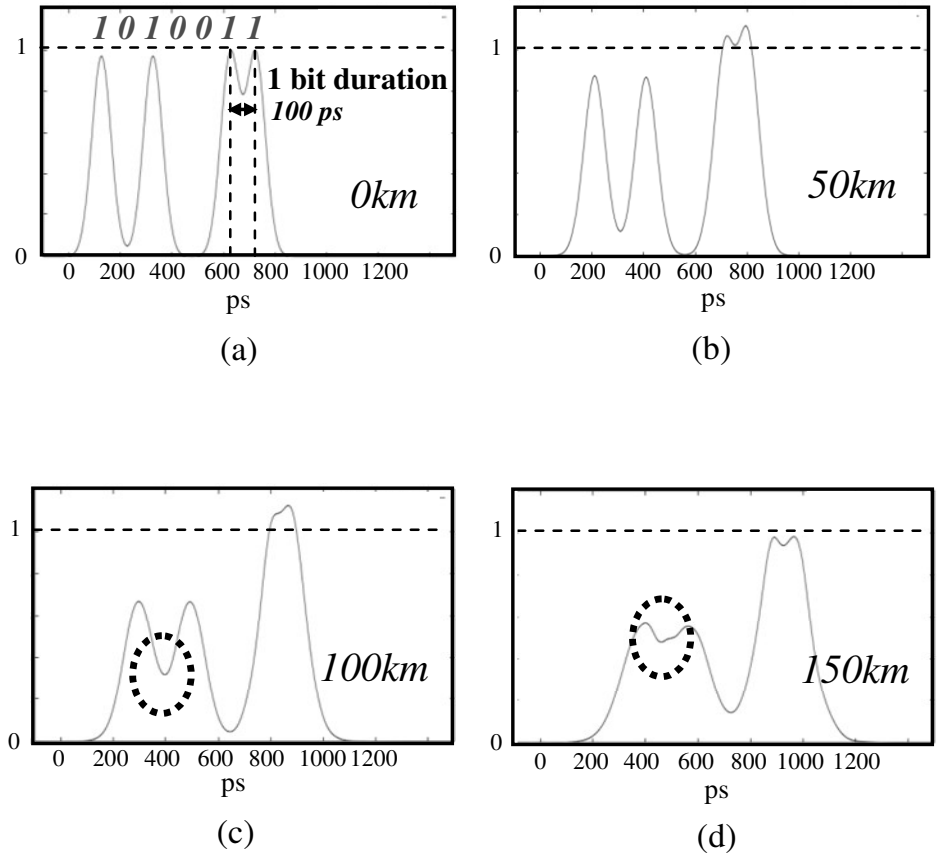



Fig. 2.17: ISI effect of autocorrelation train: (a) 0 km, (b) 50 km, (c) 100 km, (d) 150 km.

## 2.7 Conclusion

In this chapter, the overview of the OCDM has been presented. In Section 2.2, fundamentals of OC encoding and decoding have been described. In Section 2.3, various bit-ciphered OCDM schemes have been introduced and pointed out the vulnerability of the confidentiality. In Section 2.4, block-ciphered OCDM scheme has been introduced. In Section 2.5, these schemes have been compared using the confidential analysis method. In Section 2.6, configuration of multi-port E/D and property of PSK OC have been described. Using these devices and OC techniques forms the basis for the proposed system of the following chapters.

# Chapter 3

# M-ary OCDM System with XOR

## 3.1 Introduction

A block-ciphered M-ary OCDM can provide higher security than a conventional OCDM system based on bit ciphering. In the previous research, M-ary OCDM system, using a single multi-port optical E/D has been described [69]. Recently, 4-ary dual code incoherent OCDM using optical layer exclusive OR (XOR) has been proposed [74, 75], and 16-ary coherent OCDM has been demonstrated [76]. However, M-ary OCDM transmission experiment with true clock data recovery (CDR) has not been demonstrated.

In this chapter, secure 2.5 Gbps, 16-ary coherent OCDM-based block-ciphering with XOR using a single multi-port E/D and its 50 km transmission with true CDR has been experimentally demonstrated.

## 3.2 16-ary OCDM System with XOR

To increase the confidentiality of M-ary OCDM, it is necessary to encrypt many times the message, generating different OCs, by changing the state of the code lookup table. It will be noteworthy that

M-ary OCDM with XOR is the optical implementation of the CBC mode, where the OC depends not only on the bit sequence, but on all the bits of the message processed up to that point. Figure 3.1 illustrates the architecture and the operation principle of a 16-ary OCDM-based block-ciphering system using on-line XOR at the transmitter and receiver.

At the transmitter, a serial data bit stream is segmented every four bits $b_n$ ($n$=1, 2, 3, 4) by the serial-to-parallel (SP) converter. XOR between the 4-bit block data and the previous block data that is stored in the memory is operated on-line and the resultant 4-bit block is mapped onto a code word (as shown in Table 3.1), i.e. an optical code $C_n$ ($n$=1, 2,…, 16) by the 4-to-16 line coder with sixteen output ports, according to the code lookup table. Each output of this line coder generates the corresponding optical code by driving the 16-channel optical gate array that is connected to the 16ch $LiNbO_3$ intensity modulator (LN-IM) array. Only the optical pulse train passing through the optical gate is forwarded to a designated input port of the optical encoder, and one of 16 optical codes is generated. The multi-port E/D has an AWG configuration with $N$ input/output ports. It can generate simultaneously $N$ phase-shifted keyed codes, composed of $N$ chips with equal amplitude and different phases. The device is a direct-sequence spread spectrum (DS-SS) encoder, since the codes are generated and processed in the time domain. The orthogonality of the codes stems from the fact that they occupy different subbands, according to the Parseval's theorem. A detailed description of the coding/decoding features can be found in Ref. [67]. As an example, the incoming block bits (1, 0, 0, 0) is XORed with the initial bit set (initialization vector) (0, 1, 1, 0) stored in the 4-bit memory, resulting in Output1, (1, 1, 1, 0). Output1 is encoded into the optical code $C_8$, according to the code lookup table, and it is also stored in the memory. At the next step, the incoming bit block (0, 1, 1, 1) is XORed with Output1, from the memory, generating Output2, (1, 0, 0, 1), that, in turn, is optically encoded into $C_{10}$.

All the codes are generated at the same output port, so that the selection of the input port of the encoder determines which optical code is generated. Furthermore, the pulse repetition rate equates to the symbol rate, i.e. the bit rate divided by $\log_2 16=4$. At the receiver, the received optical codes are sent to the $16\times16$-port optical decoder, which has the same configuration as the encoder. An auto-correlation waveform appears only at one of the 16 output ports of the optical decoder, and the output port number indicates which is the received OC. The output optical pulse from the decoder is converted into an electrical signal by the 16-channel O/E array. The output signal is launched into the 16-to-4 line decoder. After XOR operation, the original four-bit data sequence is recovered via the parallel-to-serial (PS) converter, using the code lookup table of Table 3.1.

In this system, the SP/PS converters, the code lookup table, and the line coders are fabricated with field programmable gate array (FPGA) (Xilinx Inc., mode number: XC4VLX25SF363, response

time: 10 ns, maximum interface frequency: 622.08 MHz).

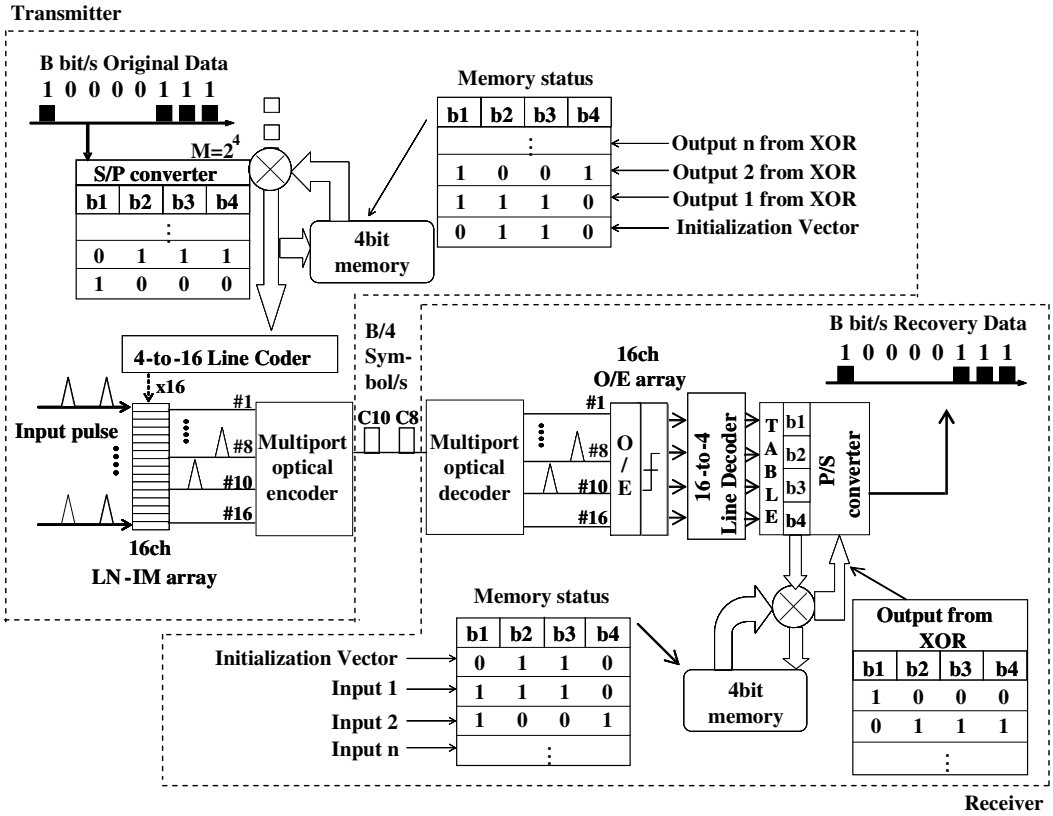



Fig. 3.1: Architecture of 16-ary OCDM block-ciphering system with on-line XOR.

Table 3.1: Code lookup table.

| | b1 | b2 | b3 | b4 | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| C1 | 0 | 0 | 0 | 0 | C9 | 0 | 0 | 0 | 1 |
| C2 | 1 | 0 | 0 | 0 | C10 | 1 | 0 | 0 | 1 |
| C3 | 0 | 1 | 0 | 0 | C11 | 0 | 1 | 0 | 1 |
| C4 | 1 | 1 | 0 | 0 | C12 | 1 | 1 | 0 | 1 |
| C5 | 0 | 0 | 1 | 0 | C13 | 0 | 0 | 1 | 1 |
| C6 | 1 | 0 | 1 | 0 | C14 | 1 | 0 | 1 | 1 |
| C7 | 0 | 1 | 1 | 0 | C15 | 0 | 1 | 1 | 1 |
| C8 | 1 | 1 | 1 | 0 | C16 | 1 | 1 | 1 | 1 |

# 3.3 Experiments

## 3.3.1 Experiment without XOR

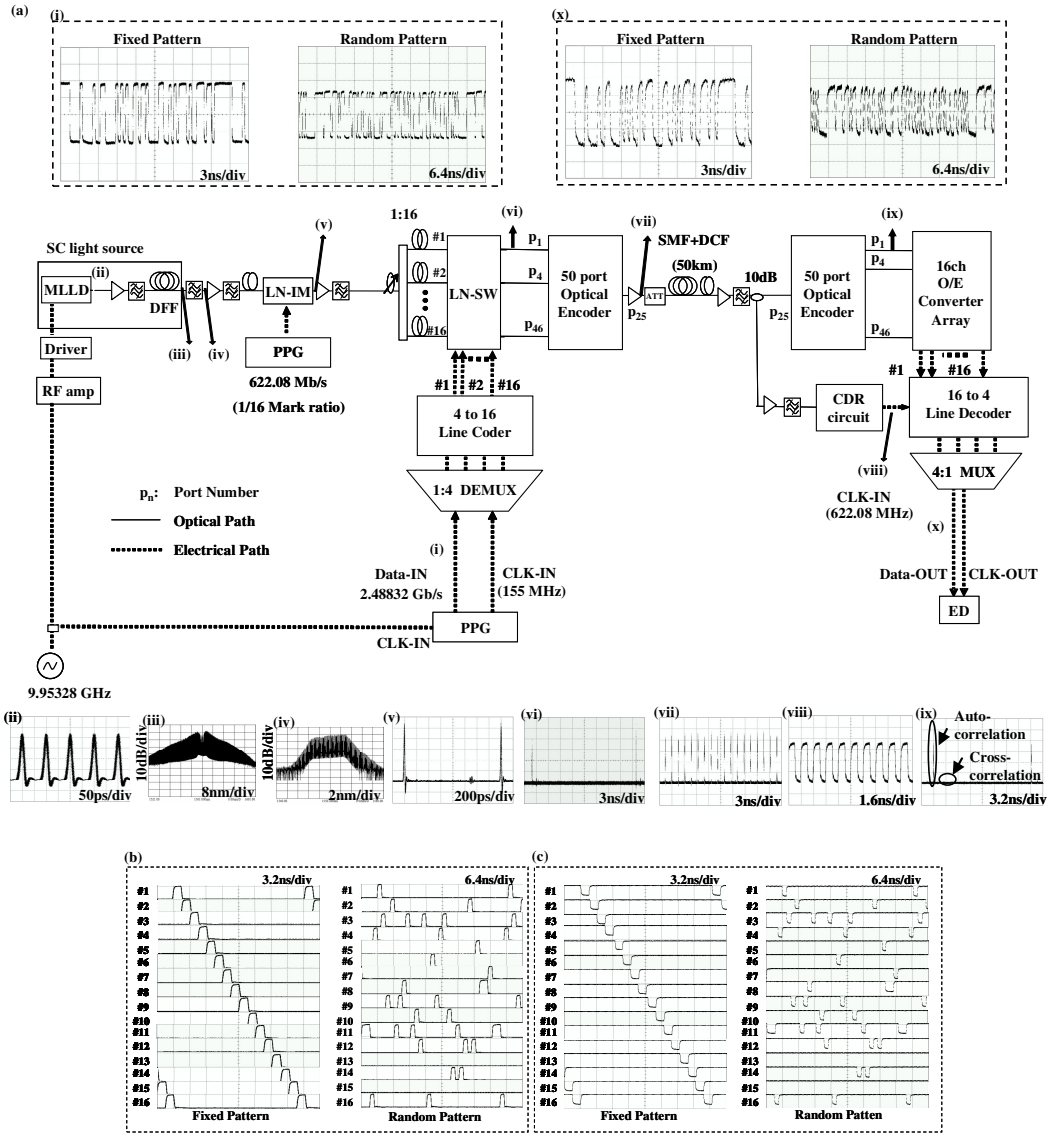



Fig. 3.2 (a) Experimental setup of 16-ary OCDM using single multi-port E/D. (b) Electric gate signals at each output of the 4-to-16 line coder for fixed and random patterns. (c) Electric gate signals at each output of the 16-to-4 line decoder for fixed and random patterns.

Figure 3.2 shows the experimental setup and results of 16-ary OCDM using 50×50-port optical en/decoder. Total of 16 ports are used with 2 ports spacing in the 50x50-port optical en/decoder. At the transmitter, a pulse pattern generator (PPG) generates a fixed pattern data, which includes all the code words in order, or a random pattern data, which consists of 128-bit long pseudo random bit sequence, at 2.48832 Gbps (as shown in inset (i)). Each group of four bits in the data sequence is mapped onto a code word according to the code lookup table by the FPGA-based 16-ary line coder. Depending on the code word, the gate signal is sent into the corresponding $LiNbO_3$ switch (LN-SW) of the 16-channel LN-SW array. A super-continuum (SC) light source is employed, which is composed of a mode-locked laser diode (MLLD), an erbium-doped fiber amplifier (EDFA), and a 2-km dispersion-flattened fiber (DFF). The MLLD at 1565 nm is driven at 9.95328 GHz (as shown in inset (ii)). The spectrum of the SC signal is shown in inset (iii). The SC signal is fed into an OBPF with 7.5 nm bandwidth at the center wavelength of 1550 nm (as shown in inset (iv)). These pulse streams are down-converted to 622.08 MHz by the LN-IM (as shown in inset (v)) and split into sixteen arms by optical couplers. Each arm is connected to an LN-SW, respectively. In each LN-SW, only when the pulse arrival timing corresponds to the gate signal from the line coder, the optical pulse is sent through. Fig. 3.2 (b) shows the gate signals at each output of the 4-to-16 line coder for the fixed and random patterns, respectively. Inset (vi) of Fig. 3.2 shows the output pulse of an LN-SW. Each output of LN-SWs is connected to a different input port of the multi-port optical encoder, which generates 500 Gchip/s, 50-chip PSK optical codes. Phase information patterns of chip in 16 OCs which are used in this demonstration are shown in Fig. 3.3. Inset (vii) in Fig. 3.2 shows the waveform of the multi-port optical encoder output. Therefore, the multi-port optical encoder generates a 16-ary, 622.08 MSymbol/s OCDM signal with a single code word in each symbol time interval. This 622.08 MSymbol/s OCDM signal is amplified and launched into the 50-km transmission fiber, which is composed of a SMF and a dispersion compensation fiber (DCF).

In an M-ary OCDM transmission experiment, to recover the original data from the transmitted 16-ary OCDM signal, we newly develop the instantaneous-response-type CDR circuit to recover the 622.08 MHz clock. Figure 3.4 shows the configuration of the developed CDR circuit. It is composed of some logic devices and two capacitors. The operational principle is that input signal is converted to 622.08 MHz clock by the loop circuit. At the receiver, the transmitted signal is divided into two lines by a 10 dB coupler. The main line (90 %-branch) and sub line (10 %-branch) are directed to the optical decoder and the CDR. Inset (viii) in Fig. 3.2 shows the recovered clock data that can be extracted from the 16-ary coding signal using the developed CDR circuit. In the optical decoder, each output port generates the auto-correlation waveform corresponding to each optical code. Inset (ix) in Fig. 3.2 shows one of the auto-correlation waveforms. These auto-correlation pulses are

launched into sixteen photo detector (PD) array, respectively. The received signals are converted to electric gate signals by a 16-ch O/E converter array and the recovered clock (as shown in Fig. 3.2 (c)) and then converted to four parallel bits according to the input port by the FPGA-based 16-to-4 line decoder. Each four parallel bits is converted into the 2.48832 Gbps serial data by the PS converter. Inset (x) in Fig. 3.2 shows the waveform of the recovered serial data, which corresponds to original serial data.

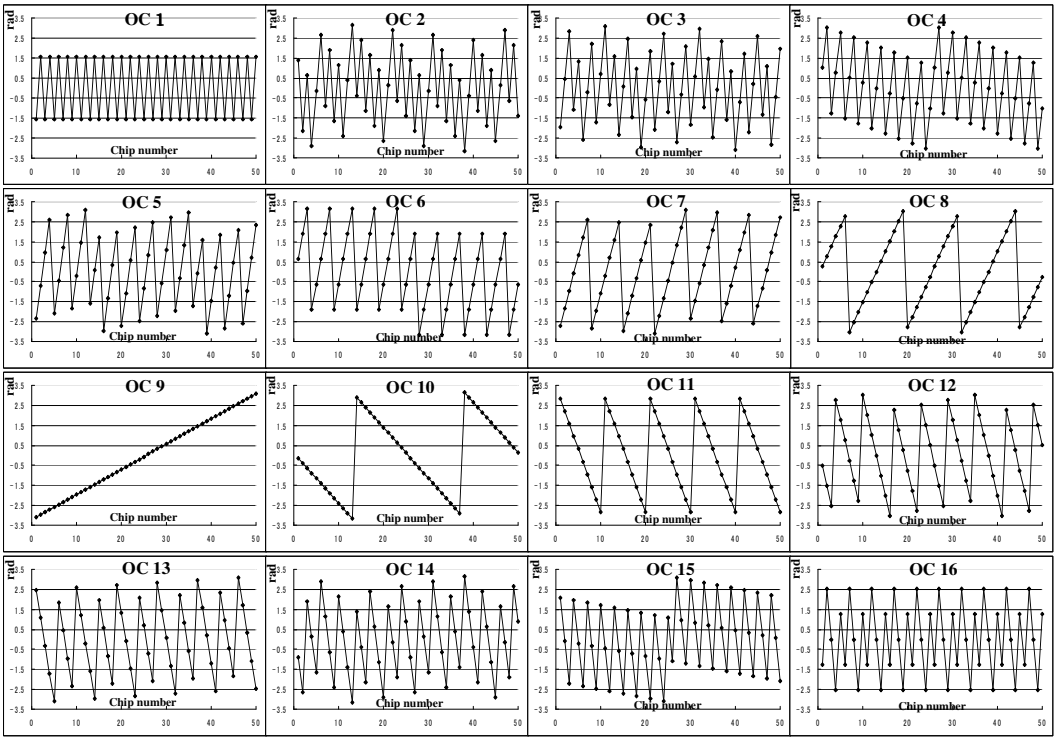



Fig. 3.3: Phase patterns of chip pulse in 16 OCs

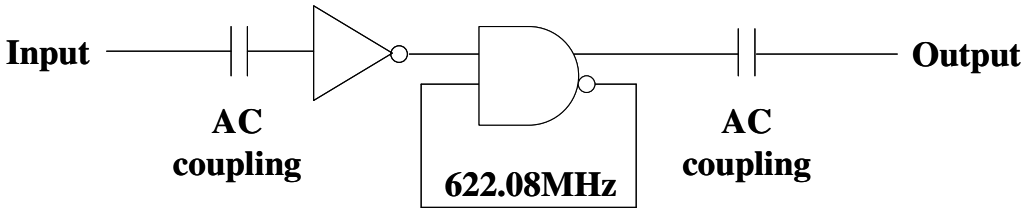



Fig. 3.4: Structure of instantaneous-response-type CDR circuit.

## 3.3.2 Experiment with XOR

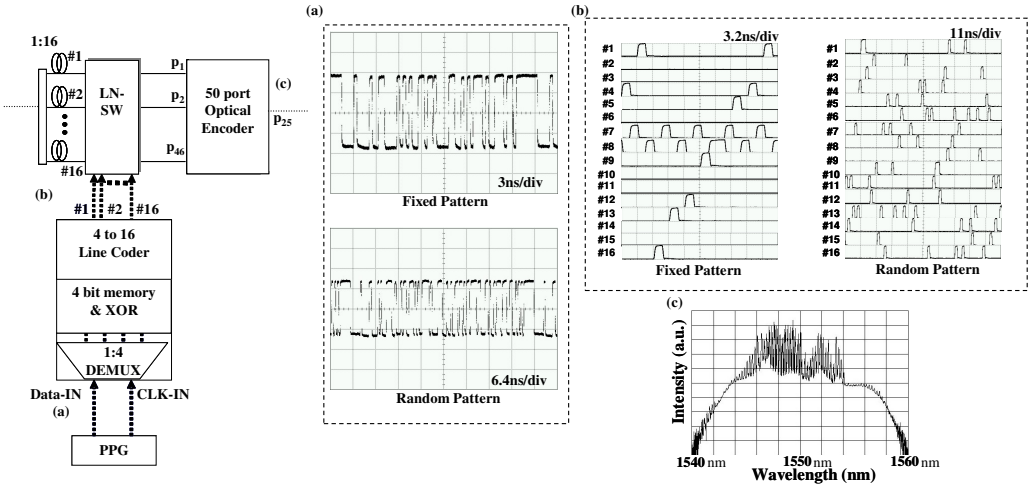



Fig. 3.5: Experimental setup of 16-ary OCDM transmission system with on-line XOR. (a) A PPG generates a fixed pattern data sequence and random pattern sequence. (b) Electric gate signals at each output of the 4-to-16 line coder for fixed and random patterns. (c) Power spectrum after 50×50-port optical encoder.

Figure 3.5 shows the experimental setup of 16-ary OCDM-based block-ciphering transmitter with on-line XOR using single multi-port optical encoder. Compared with Fig. 3.2 (a), the only difference is that a 4-bit memory and a XOR have been added before the 4-to-16 line coder. The PPG generates a fixed pattern, or a random pattern data sequence (as shown in Figs. 3.5 (a)). Figures 3.5 (b) shows the waveforms at each output of the 4-to-16 line coder for both cases, respectively. The power spectrum after 50×50-port optical encoder is shown in Fig. 3.5 (c). The central wavelength is about 1550 nm.

A close-up look at the 16-ary OCDM-based block-ciphering receiver is shown in Figure 3.6. Figures 3.6 (a) show the gate signals before the 16-to-4 line decoder. Figures 3.6 (b) show the waveform of the recovered serial data that coincides with the original transmitted serial data. Figures 3.7 show the power spectra for each output port of the multi-port optical decoder. The two peaks of each spectrum in Fig. 3.7 are used to retain the information at 500 Gchip/s. It should be mentioned that the theoretical power spectrum has sidelobes with the frequency interval of 500 GHz on both side of the central peak [67], and the measured spectrum shows a sidelobe along with the central peak. Each output signal has a wavelength shift of 0.24 nm with respect to the signal generated at the

adjacent output port; as an example, the peak spectrum at output port 4 is shifted of 0.24 nm with respect to the spectrum at output port 1. Figures 3.8 show the auto-correlation waveforms generated at each output port of the multi-port optical decoder.

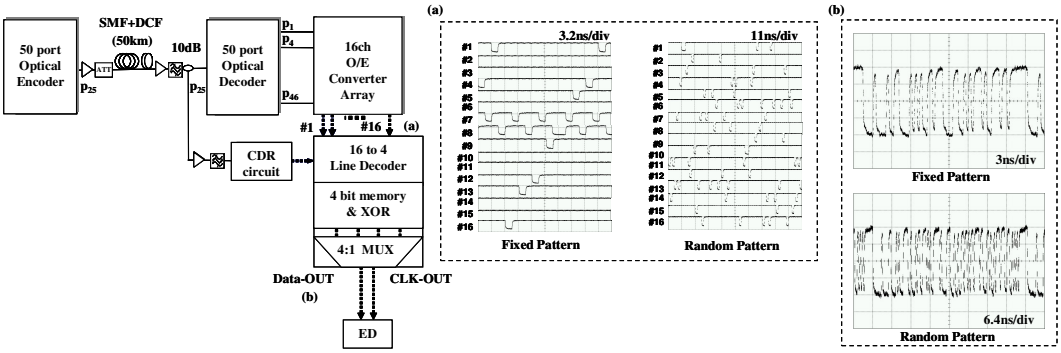



Fig. 3.6 Experimental setup of 16-ary OCDM receiver system with on-line XOR. (a) Electric gate signals at each output of the 4-to-16 line coder for fixed and random patterns. (b) Waveforms of the regenerated serial data.

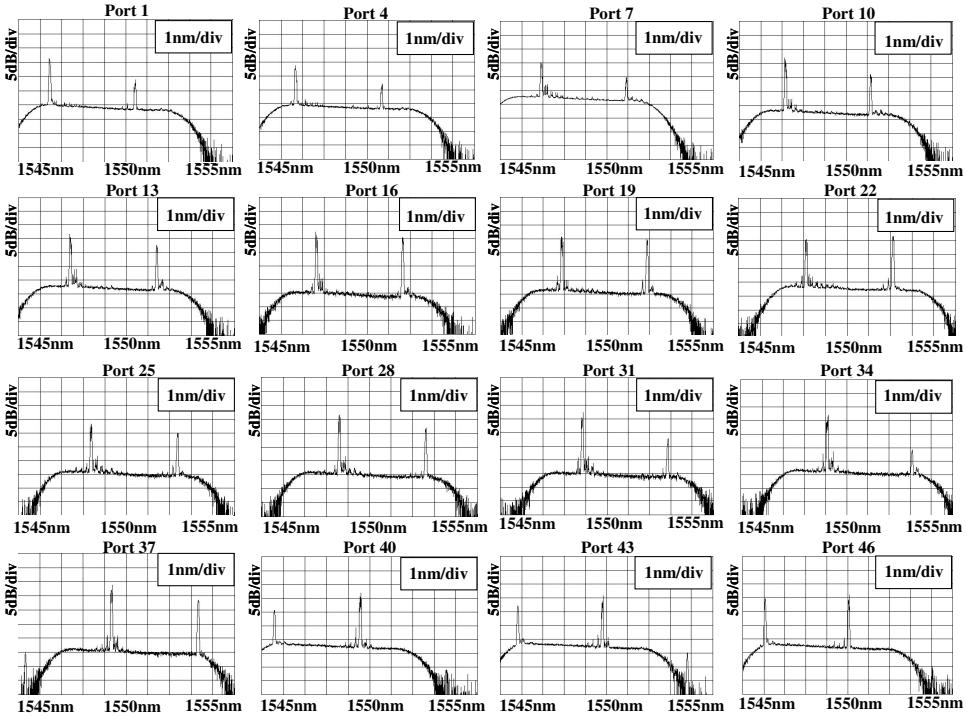



Fig. 3.7: Spectra generated at each output port of the multi-port optical decoder.

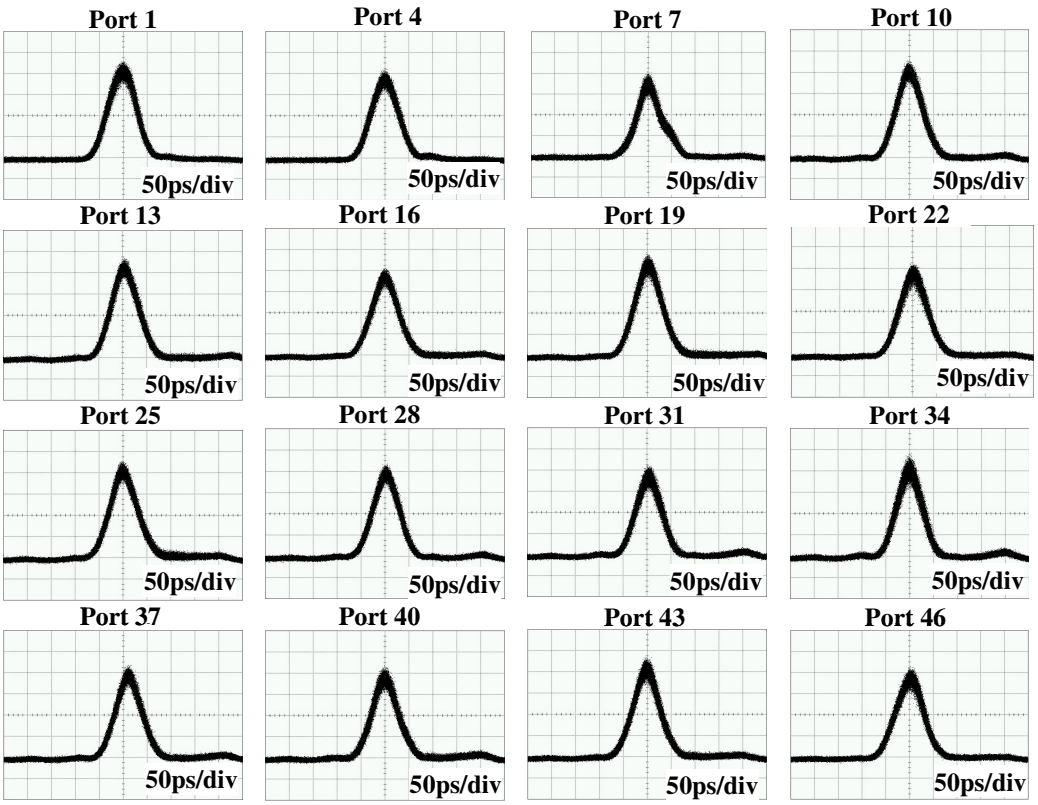



Fig. 3.8: Autocorrelation waveforms generated from each output port of the multi-port optical decoder.

Finally, we measured the bit error rates (BERs) of the received serial data in eight cases. Figure 3.9 shows the measured BERs: the fixed and random patterns without/with on-line XOR in case of back-to-back (B-to-B) and after 50 km transmission. In all cases, error free transmission (BER < $10^{-9}$) has been achieved. We define the power penalty as the receiver sensitivity difference at BER = $10^{-9}$. The power penalties between B-to-B and after 50 km transmission in original random and fixed pattern are about 1.2 and 0.4 dB, respectively. On the other hand, in XORed case, the power penalties between B-to-B and after 50 km transmission in random and fixed pattern are about 0.6 and 1.2 dB, respectively. Therefore, the power penalty of the original fixed pattern case is the lowest.

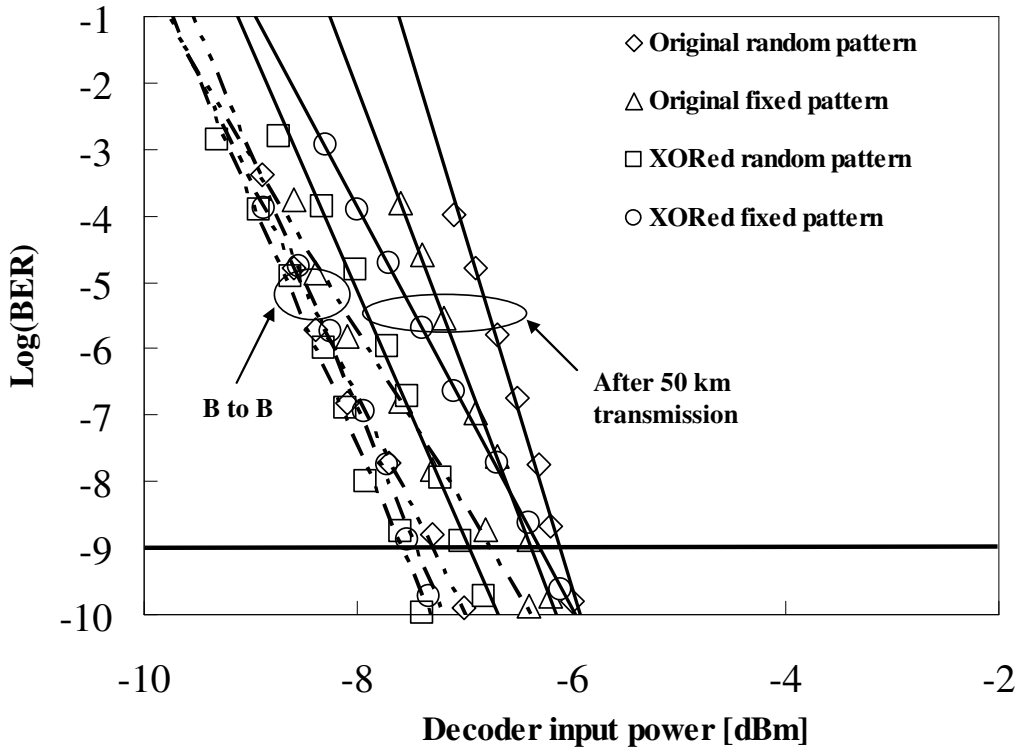



Fig. 3.9: Measured BERs of back-to-back and 50-km transmission.

## 3.4 Conclusion

Secure 16-ary, 622 MSymbol/s coherent OCDM-based block ciphering with online XOR and its 50-km transmission have been experimentally demonstrated. The newly developed instantaneous-response-type CDR circuit is a key enabler for the transmission to recover the clock data from 16-ary OCDM signal, and the use of a single multi-port E/D has simplified the optical implementation. The proposed scheme guarantees enhanced both physical and computational data confidentiality. Finally, we have observed that this point-to-point transmission can be extended to multiple users, realizing a secure OCDM-based access network.

# Chapter 4

# M-ary OCDM System Using Polarization Multiplexing

## 4.1 Introduction

In conventional M-ary OCDM, the number of OCs is limited by the port count, and it would be desirable if the M-ary number can be increased without increasing the number of OCs. To overcome this limitation, a novel POL-MUX M-ary OCDM system is proposed, as shown in Fig. 4.1. The code lookup table is shown in Table 4.1. This method can largely reduce the number of codes needed. In this chapter, we demonstrate a POL-MUX 2.5 Gbps, 256 (= 16 × 16)-ary OCDM transmission using 16 OCs generated by a multi-port optical E/D, we remark that in a conventional M-ary system, the number of OCs required would be 256, that is beyond the capability of the current OCDM technology. We also analyze the corresponding data security in terms of data confidentiality against COA and CPA, and show that POL-MUX OCDM doubles the spectral efficiency and enhances the data confidentiality.

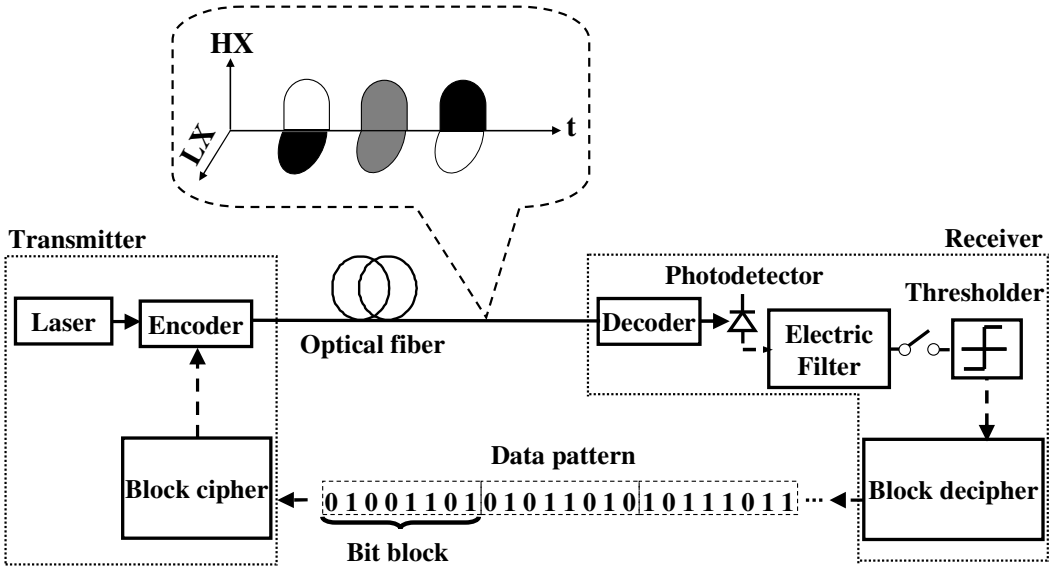



Fig. 4.1: Scheme of polarization-multiplexed M-ary OCDM.

Table 4.1 Code lookup table

| Bit block | OC | |
|---|---|---|
| | HX | LX |
| 01001101 | ● | ○ |
| 01011010 | ◐ | ◐ |
| 10111011 | ○ | ● |
| ⋮ | ⋮ | ⋮ |

## 4.2 256-ary OCDM System Using Polarization Multiplexing

Figure 4.2 shows the architecture and the operation principle of a POL-MUX 256-ary OCDM system. At the transmitter, a serial data bit stream at $B$ bps is segmented every 8 bits by a SP converter and each 8-bit block is sent to a 8-to-32 line coder. The former 4-bit block (higher-order

bits: HX) and the latter 4-bit block (lower-order bits: LX) are mapped onto two codewords, according to Table 4.2. We remark that the segmentation in the HX and LX blocks is used only for sake of clearness, and that in a secure POL-MUX OCDM system, a message of 8 bits can be decomposed in two parts of 4 bits each in a complete arbitrary way.

The 32 outputs of the line coder are time-interleaved into 16 lines by an electronic 32:16 multiplexer (MUX) and each output is connected to one of 16 ports of a LN-IM array, to generate a gate signal that selects an optical seed pulse corresponding to the OC. We observe it would be possible to encode the LX and HX blocks onto two orthogonal polarizations using two identical E/Ds, and that the proposed configuration requires only a single multi-port E/D. Therefore, the transmission system of Fig. 4.3 presents the same performance of a OCDM system, where the LX and HX codes are time interleaved; however, the use of two orthogonal polarizations allows us to simplify the receiver (see Fig. 4.4), because in this case we can avoid expensive time-gating devices.

In the optical domain, the optical seed pulses at $B/4$ bps are launched into 16 port LN-IM array, and only the optical pulses passing through the optical gate are forwarded to a designated input port of the multi-port optical encoder. The multi-port optical E/D has an AWG configuration with $N$ input/output ports and it can generate simultaneously $N$ phase-shifted keyed codes, composed of $N$ chips with equal amplitude and different phases [67]. As an example of operation, the incoming block bits (1, 0, 0, 0, 0, 1, 1, 1) is divided into the HX 4-bit block (1, 0, 0, 0) and the LX 4-bit block (0, 1, 1, 1), that are encoded into the $C_2$ and $C_{15}$ codes, respectively. All the 16 codes are generated at the same output port, and the selection of the input port of the multi-port optical encoder determines which OC is generated. However, in the proposed system, we use two different output ports (#1 and #25) of the multi-port optical encoder for the HX and LX blocks, respectively. The switches (SWs) at these two outputs select the HX and LX codes and the polarization controllers (PCs) rotate their polarization of 90º and 0º, respectively. Therefore, the code repetition rate at each polarization state is equal to the symbol rate at $B/8$ Symbol/s.

At the receiver, the 256-ary OCDM signal is split into two encoded signals with orthogonal polarization states by the PCs, and each code is processed by the multi-port optical decoder, which has the same configuration as the encoder. An auto-correlation waveform appears only at one of the 16 output ports of the optical decoder, and the output port number clearly identifies the received OC. The output optical pulse from the decoder is converted into an electrical signal by the 16-channel optical-to-electrical (O/E) converter array, and it is launched into the 16-to-8 line

decoder, so that the original 8 bit data sequence is recovered via the PS converter, using the same code lookup table (Table 4.2).

The SP/PS converters, the code lookup table, and the line coders are fabricated with FPGA (Xilinx Inc., mode number: XC4VLX25SF363, response time: 10 ns, maximum interface frequency: 622.08 MHz).

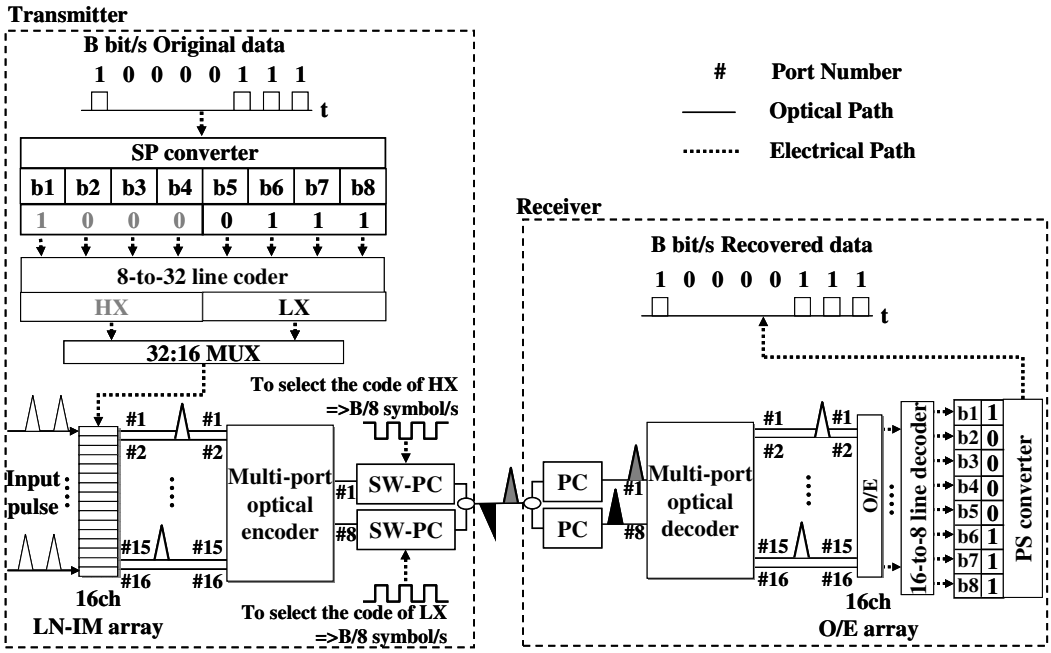



Fig. 4.2: Architecture of polarization-multiplexed 256-ary OCDM system.

Table 4.2: Code lookup table.

| HX \ LX | C1 | C2 | C3 | C4 | ····· | C15 | C16 |
|---|---|---|---|---|---|---|---|
| C1 | 00000000 | 00001000 | 00000100 | 00001100 | ····· | 00000111 | 00001111 |
| C2 | 10000000 | 10001000 | 10000100 | 10001100 | ····· | 10000111 | 10001111 |
| C3 | 01000000 | 01001000 | 01000100 | 01001100 | ····· | 01000111 | 01001111 |
| C4 | 11000000 | 11001000 | 11000100 | 11001100 | ····· | 11000111 | 11001111 |
| ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋱ | ⋮ | ⋮ |
| C15 | 01110000 | 01111000 | 01110100 | 01111100 | ····· | 01110111 | 01111111 |
| C16 | 11110000 | 11111000 | 11110100 | 11111100 | ····· | 11110111 | 11111111 |

# 4.3 Experiments

Figure 4.3 shows the experimental setup of the 256-ary OCDM transmitter, where two data patterns (shown in the inset (i)) have been used: a fixed pattern and a $2^7$-1 pseudo-random bit sequence (PRBS)). In the first case, the sequence of input bits is such that all the codes are generated in an ordered sequence (see inset (ii)), where the PRBS emulates a standard communication signal. At the transmitter, the serial data bit stream at 2.48832 Gbps is segmented every 8 bits by the SP converter; the 8-bit sequence is then halved to generate the HX and LX 4-bit blocks, that are separately mapped onto one of the 16 OCs, according to the code lookup table. The outputs of the line coder are time interleaved by a 32:16 electronic MUX and, as a result, a gate signal for HX and LX is alternately generated at the 16 outputs of the FPGA-based line coder to drive the 16-channel LN-IM array. Inset (ii) of Fig. 4.3 shows the gate signals at each output of the 4-to-16 line coder for the fixed and the random patterns, respectively. We used a SC light source, which consists of a MLLD, an EDFA, and a 2-km DFF. The MLLD at the wavelength of 1565 nm is driven at 9.95328 GHz, as shown in inset (iii). The spectrum of the SC signal is shown in inset (iv). The SC signal is fed into an OBPF with 7.5 nm bandwidth at the center wavelength of 1550 nm (as shown in inset (v)). The pulse streams generated by the PPG are down-converted to 622.08 MHz by a LN-IM, as shown in inset (vi), and split into 16 arms by optical couplers.

Each arm is connected to the 16-channel LN-IM array: the pulse passes through only if its arrival time corresponds to the gate signal from the line coder; we used a tunable delay line to synchronize the optical and electrical pulses. Inset (vii) of Fig. 4.3 shows the output pulse from one channel of the LN-IM array. Each output of the LN-IM arrays is connected to a different input port of the multi-port encoder, which generates 16 different OCs composed of 50 chip at 500 Gchip/s; the phase shift keying OC that is generated depends on which input and output ports have been used. In this experiment, only 16-input ports ($p_n$=1+3$n$ ($n$=0, 1, 2,…, 15)) have been used, i.e. a port every three of the 50-port optical encoder. On the other hand, the ports $p_1$ and $p_{25}$ have been used as outputs, each of them generates a 16-ary, 622.08 MSymbol/s OCDM signal with a single codeword in each symbol time interval. The codes of HX and LX are time interleaved, and they are shown in the insets (viii) and (ix) of Fig. 4.3. The PC rotates their polarization of 90º and 0º, respectively, and finally the HX and LX encoded signals are combined together by a polarization beam splitter (PBS), as shown in the inset (x); the inset (xi) shows the spectrum of 256-ary OCDM signal.

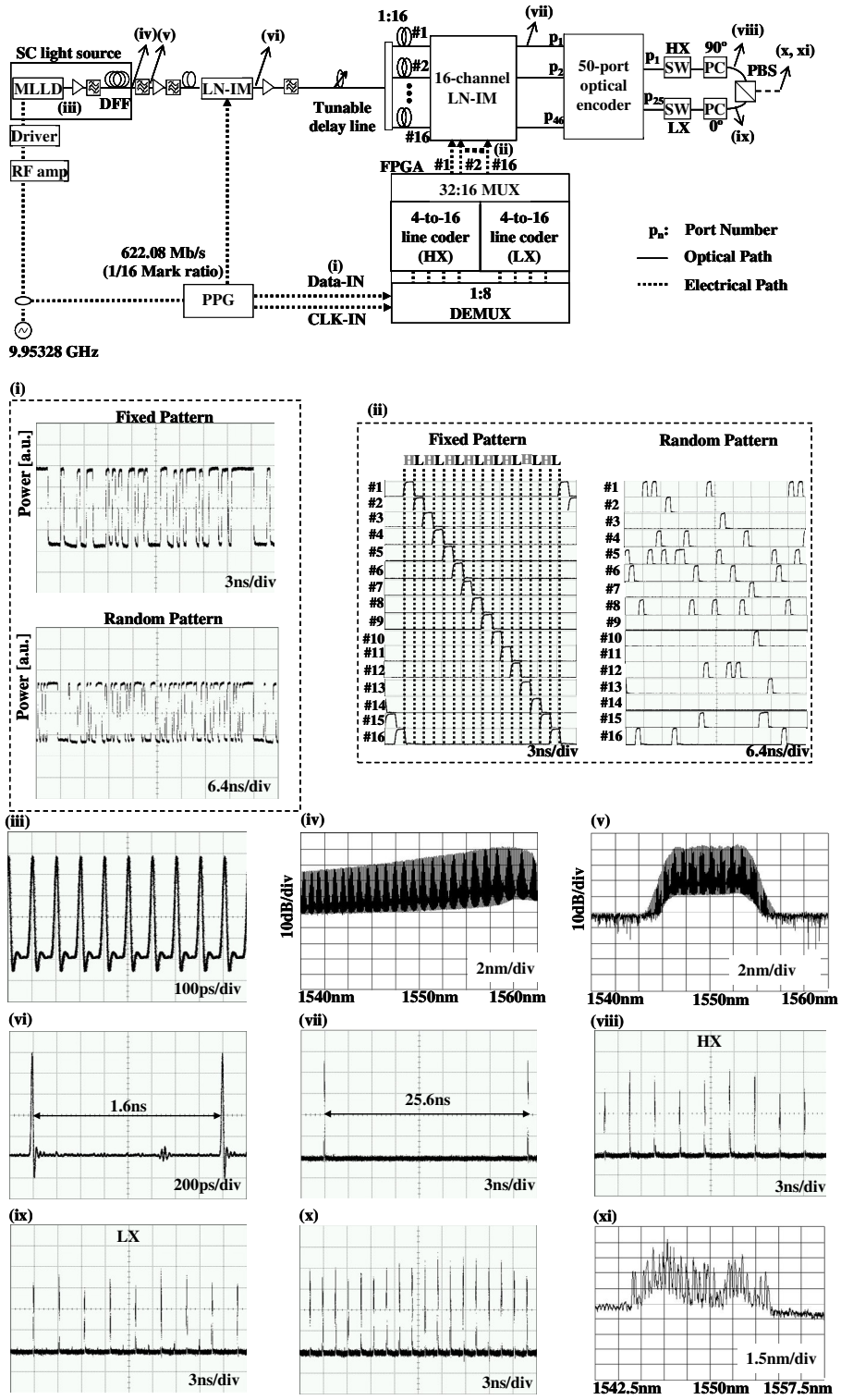



Fig. 4.3: Experimental setup of POL-MUX 256-ary OCDM transmission system.

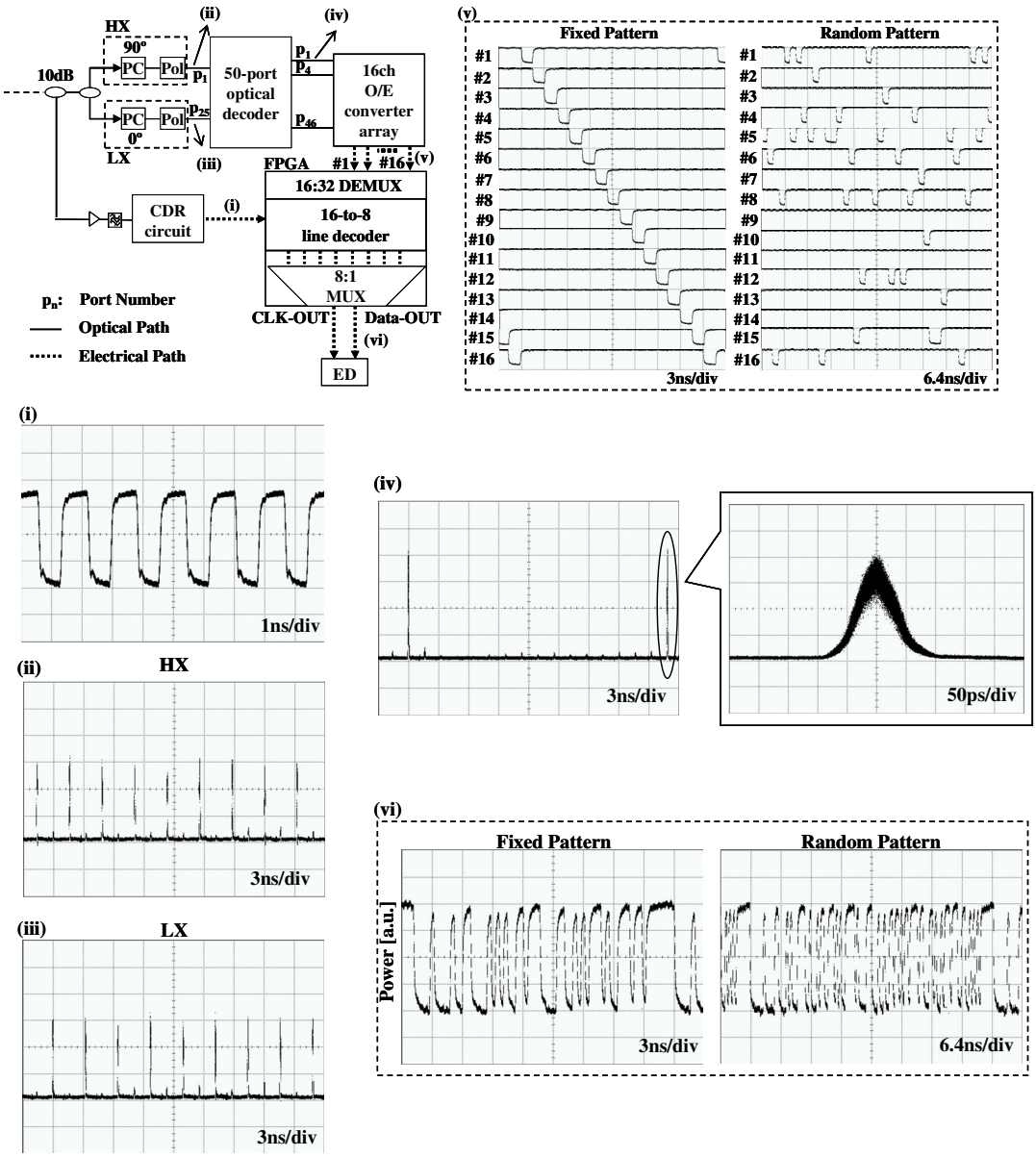



Fig. 4.4: Experimental setup of polarization-multiplexed 256-ary OCDM receiver system.

Figure 4.4 shows the experimental setup and the outputs of the POL-MUX 256-ary OCDM receiver. At the receiver, the transmitted signal is divided into two branches by a 10 dB coupler. The main branch (90 %) and sub branch (10 %) are directed to the optical decoder and clock data recovery (CDR) circuit, respectively. The inset (i) in Fig. 4.4 shows the recoveryed clock from the 256-ary OCDM signal using the CDR circuit. In the main branch, the received OCs are split into two arms to be polarization-demultiplexed by using a PC and a polarizer (Pol). The insets (ii) and (iii) of Fig. 4.4 show waveforms of polarization-demultiplexed HX and LX signals, respectively,

that are sent to different input port of the multi-port optical decoder, which has the same configuration as the encoder. An auto-correlation waveform appears only at one of the 16 output ports of the optical decoder, and the output port number indicates the received optical code, as shown in the inset (iv).

The output optical pulse from the decoder is converted into an electrical signal by a 16-channel O/E converter array (as shown in Fig. 4.4 (v)) and then converted into 8-parallel bits by the FPGA-based 16-to-8 line coder. Finally, the 8 parallel bits are converted into the 2.48832 Gbps serial data sequence by the PS converter. Inset (vi) in Figs. 4.4 show the waveform of the recovered serial data in case of the fixed and random patterns, respectively.

We measured the BER of the received data, that are reported in Fig. 4.5, for fixed and random patterns, respectively. In both cases, error free operation has been achieved. The power penalty between the fixed and random cases in case of BER=$10^{-9}$ is 1.1 dB, and it is presumable due to the fact that the random pattern does not include all the code words.

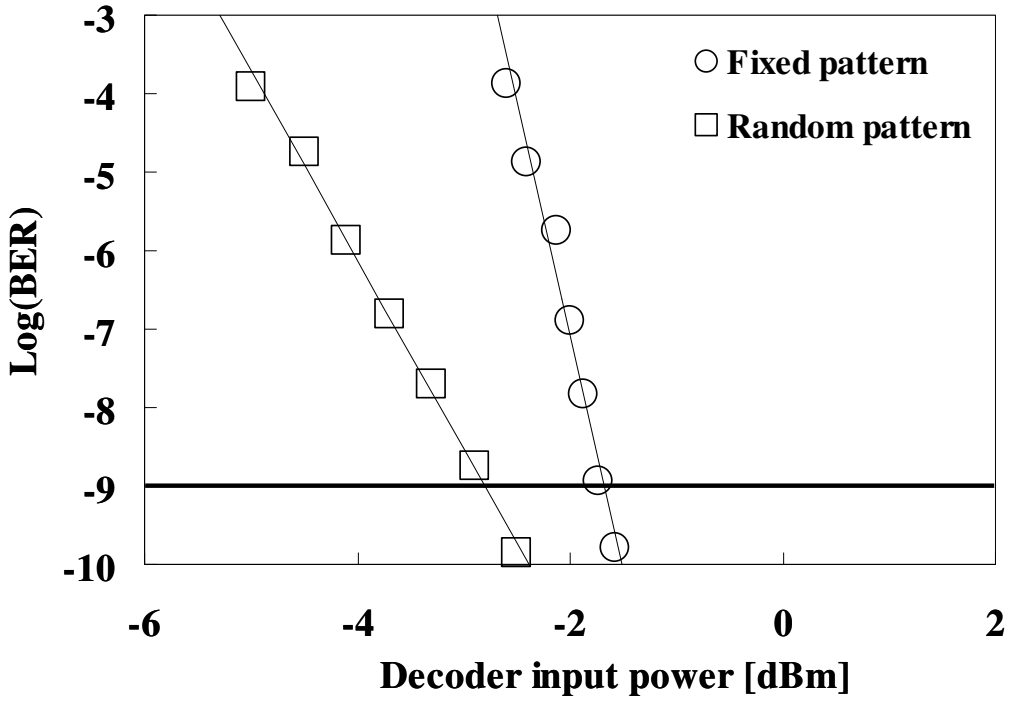



Fig. 4.5: Measured BERs in case of the fixed and random patterns.

# 4.4 Data Confidentiality Analysis

In this section, we analyze the confidentiality of a POL-MUX M-ary OCDM system, making a comparison with a conventional M-ary OCDM system. In both cases, a stream of $m$ bits from a single user is encoded into different codewords: in a conventional OCDM transmission, $M=2^m$ OCs are necessary, whereas in POL-MUX M-ary OCDM, each block of data is split in the HX and LX parts, that are converted into OCs, with the same $2^{m/2}$ determinations. Therefore, the number of different OCs is reduced from $M$ to $\sqrt{M}$, and we have demonstrated a 256 (=16×16)-ary POL-MUX OCDM, using only 16 OCs; we remark that standard 256-ary OCDM transmission would be very difficult to experimentally demonstrate. POL-MUX OCDM system presents the following additional advantages, to conventional OCDM.

1) reduced complexity of the electrical block-ciphering components;
2) the symbol rate at each polarization state is reduced and therefore fast response receivers are not required;
3) the spectral efficiency is doubled;

We observe that both conventional M-ary and POL-MUX M-ary OCDM systems furnish both 'optical' and 'electrical' confidentiality, since an eavesdropper has first to decrypt the optical code, and later he or she has to find the correspondence with a sequence of bits. The 'optical' confidentiality of the two systems is identical, since they use the same number of optical codes. Therefore, to analyze the system security, we considered only the 'electrical' confidentiality evaluating the average number of trials that adversary has to make to decrypt a message. To give a quantitative evaluation of the confidentiality of conventional and POL-MUX systems, we consider COA. In a conventional M-ary system, $M$ equates the number of OCs, and the average number of trials needed to break the system security equates the half of all the possible combinations, that is $M!/2$ [72]. In a POL-MUX OCDM, only $\sqrt{M}$ OCs are used, and the confidentiality can be evaluated in the following way: first of all, the message of $m$ bits is split in two parts, that can be chosen in a complete arbitrary way. Since the eavesdropper cannot know which $m/2$ bits have been selected to be encoded on the same polarization, he or she has to make some guesses and the only way to tell if his/her guess is right is looking at the deciphered output to see if it is meaningful. The number of possible $m/2$-combinations of $m$ elements, i.e. the number of sequences of $m/2$ bits taken over a set of $m$ is $m(m-1) \ldots (m-m/2+1)/(m/2)! = m!/[(m/2)!]^2$ and it is $8!/(4!)^2=70$ in our case. The

two groups of $m/2$ bits are separately encoded onto $\sqrt{M}$ OCs, using two independent lookup tables for the two polarizations, and the total number of possible choices is$\cdot(\sqrt{M})!\times(\sqrt{M})!$. Therefore, the average number of trials that the eavesdropper has to make is $[(\sqrt{M})!]^2 m!/\{2*[(m/2)!]^2\}$ and it is plotted in Fig. 4.6 (a), as a function of the number of OCs. We observe that the 'electrical' confidentiality of a POL-MUX M-ary system is enhanced with respect to that one corresponding of a conventional system with the same number of OCs.

Using 16 OCs, the system confidentiality against a COA in a POL-MUX M-ary OCDM system is more than $10^{28}$, if two different lookup tables have been used for the two polarizations and the eavesdropper does not know how the 8-bit sequence has been split in the LX and HX blocks; on the other hand, $10^{13}$ trials are needed to break the confidentiality of a conventional M-ary system that uses 16 OCs.

The lowerbound security parameter of modern cryptanalysis is the number of plaintexts that an eavesdropper needs to know in a CPA, to break the system confidentiality. In a conventional M-ary system, a CPA could reveal the cryptographic secret key, i.e. the scheme that has been used to couple each sequence of $m$ bits with one of the $M$ OCs. We assume that the lookup is completely arbitrary (i.e. no recursive scheme for the secret key has been used), so that the adversary has to be able to encrypt all the codewords, except one, i.e. $M$-1 codewords to intercept the data. As an example, considering $m$=8 bits, the eavesdropper should encode all the sequences 00000000, 00000001,…, 11111111 minus one to find all the information, and this operation requires $M$-1=255 trials. In a POL-MUX M-ary OCDM system, the eavesdropper can easily reveal how the message is split into the HX and LX blocks, just encoding a single message. For each polarization, the adversary has to find all the correspondences (minus one) between the sequences of $m/2$ bits and the $\sqrt{M}$ OCs, making $\sqrt{M}$ -1 attempts. If we assume that the lookup tables of the two polarizations are independent, the total number of trials required to decrypt all the codewords in a POL-MUX M-ary OCDM system is $2(\sqrt{M}-1)$, and it is 30 in our case. Figure 4.6 (b) shows the confidentiality against CPAs for a conventional and a POL-MUX M-ary OCDM system, using the same number of OCs from an inspection of this figure, we observe that the POL-MUX technique doubles the 'electrical' confidentiality against CPA, with respect of a system that uses the same number of OCs, if two different look up tables have been used for the two polarizations.

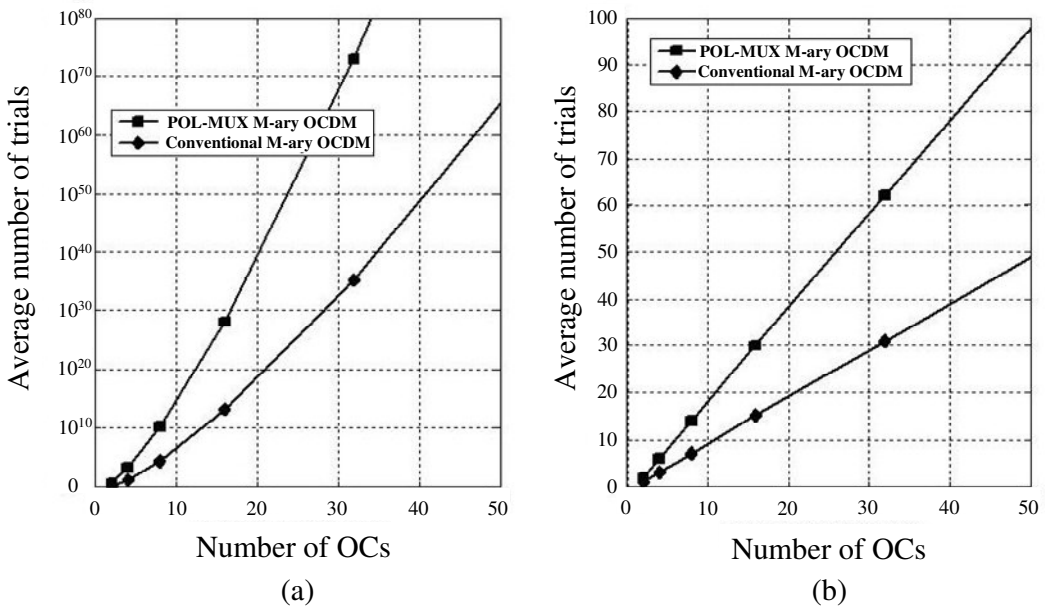



Fig. 4.6: (a) Number of trials to break the confidentiality with a COA, (b) Number of trials necessary to break the confidentiality with a CPA.

## 4.5 Conclusion

In this chapter, we propose a novel M-ary OCDM system using polarization multiplexing technique and a single multi-port optical E/D. We show that POL-MUX M-ary OCDM system can reduce the number of OCs requested and doubles the spectral efficiency, compared with a conventional system. We have demonstrated a 2.5 Gbps, 256-ary POL-MUX OCDM system using a single multi-port E/D and analyzed the corresponding confidentiality.

# Chapter 5

# M-ary OCDM System Using Multidimensional Optical Codes

## 5.1 Introduction

To make M-ary OCDM scalable with respect to *M* count, the M-ary OCDM scheme shown in Fig. 5.1 has been proposed, based on multidimensional PSK OCs [69], [77]. The code lookup table is shown in Table 5.1. To the best of our knowledge, however, this technique has been not experimentally demonstrated yet, and its implementation is one of the main achievements of the present research.

The remainder of this chapter is structured as follows. Section 5.2 describes the principle of multidimensional PSK OCs.

In Section 5.3, we propose and describe the principle of 4096-ary OCDM system using multidimensional PSK OCs generated by a single multi-port optical E/D.

In Section 5.4, we experimentally demonstrate the 4096-ary (=16 × 16 × 16)-ary OCDM at 2.5 Gbps for the first time. The number 4096 of different OCs that have been experimentally generated/processed by a single device is a world record for fiber optics system.

In section 5.5, we show that the impairment due to multiple interference affects the system performance more than other kind of noises (e.g., thermal, shot, phase induced intensity noise (PIIN)).

Section 5.6 analyzes the data confidentiality against COA and CPA.

Section 5.7 proposes a 10 Gbps, 4096-ary OCDMA-based PON, that uses a multi-port E/D in the central office and in the users premises. We also analyze the influence of the MAI.

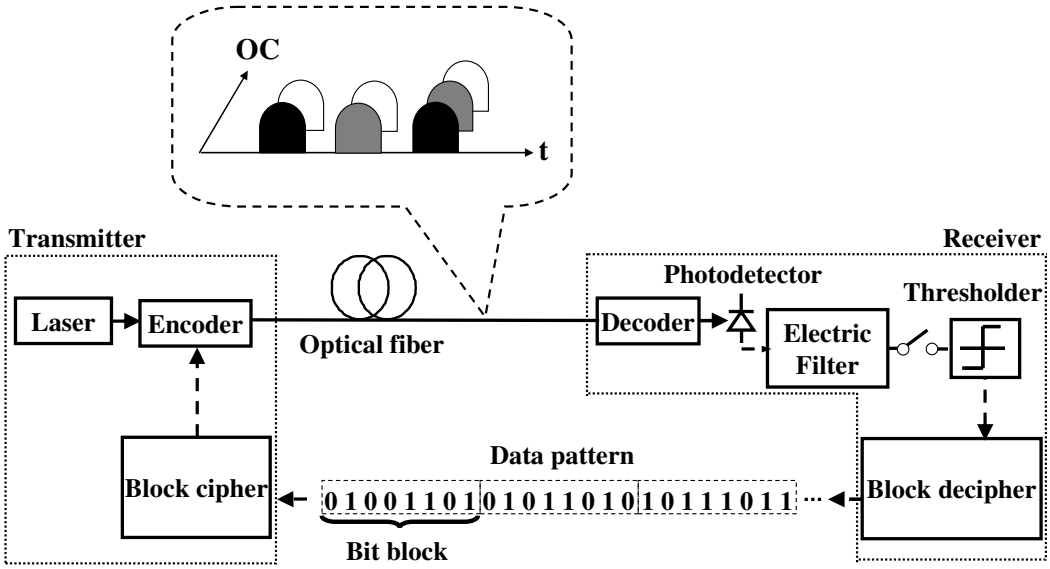



Fig. 5.1: Scheme of M-ary OCDM using multidimensional OC.

Table 5.1: Code lookup table.

| Bit block | OCs |
|---|---|
| 01001101 | |
| 01011010 | |
| 10111011 | |
| ⋮ | ⋮ |

## 5.2 Multidimensional Optical Code Processing

Figure 5.2 show the concept of proposed multidimensional OC processing. In the proposed multidimensional OC processing, some OCs are assigned to one bit-block. In the multi-port optical decoder, multidimensional OCs are launched into and correlated. An autocorrelation waveform emerges only when the code matches, while in contrast, all the other correlations show crosscorrelation outputs. As a result, we can recognize the desired OC.

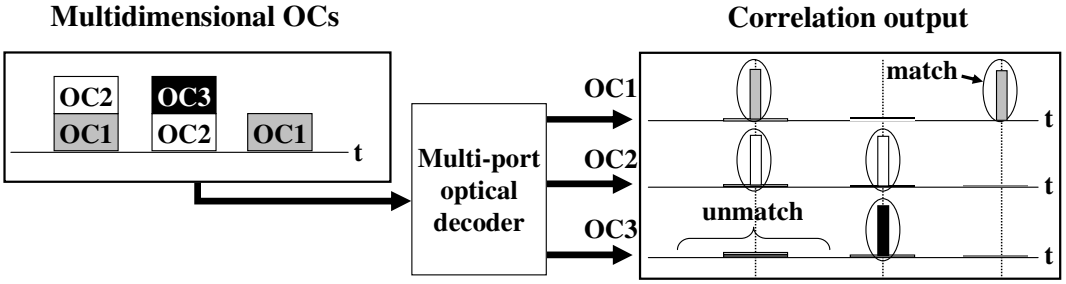



Fig. 5.2: Multidimensional OC processing.

## 5.3 4096-ary OCDM System Using Multidimensional PSK Optical Codes

A multi-port E/D is a planar device with an AWG configuration that is able to generate/process as many PSK OCs as the number $N$ of its ports. If a short laser pulse is sent into one of its input ports, a set of $N$ OCs are simultaneously generated at the E/D outputs. Furthermore, forwarding an OC into one of the E/D input ports, at the output ports we obtain all the crosscorrelation signals, and the ACP detected at the matched port, clearly identifies the OC.

To increase the number of OCs, without increasing the number of the device ports, we can refer to a multidimensional configuration. In this case, $1 \leq n \leq N$ short laser pulses (even at the same wavelength) are forwarded into $n$ input ports, and a set of $N$ multidimensional OCs are generated at the device outputs; each multidimensional OC is the superposition of $n$ PSK OCs, and it is detected by the same E/D measuring $n$ ACPs at the matched ports [69]. The total number of different multidimensional OCs that can be generated/processed by a single E/D is $2^N-1$ (considering that at least $n$=1 laser pulse must be sent to the E/D inputs), and thus the case with $n$=0 is eliminated.

A block-ciphering (or M-ary system) is a transmission scheme where the stream of bits is segmented into blocks (sequences of $m=\log_2 M$ bits), that are encoded into OCs. Therefore, to transmit all the data, $M$ different OCs are necessary, and if we use the multi-port E/D in the multidimensional configuration, we need a device with $N>m$ ports. The code lookup table that transforms a sequence of $m$=12 bits into $M$=4096 multidimensional OCs is shown in Table 5.2 (a): The columns represent the input ports of an E/D with $N$=13 ports and the circles mean that a short laser pulse is sent into that port. In this demonstration, for sake of simplicity, we used a very basic code assignment method and the OC combinations are sequentially assigned to bit blocks, following the lookup tables of Table 5.2. For instance, for the case $d$=3, the bit blocks 0000(=0), 0001=(1), 0010=(2), 0011(=3), 0100(=4), 0101(=5) correspond to $C_1$, $C_2$, $C_3$, $C_4$, $C_5$ and $C_6$, respectively. Then, the bit block 0110(=6) corresponds to the combination of $C_1$ and $C_2$, whereas 0111(=7) is the combination of $C_1$ and $C_3$ and so on…

To simplify the encoding process, we can further split the block of $m$ bits into $d$ groups, and separately encode the sequences of $m/d$ bits into different OCs. For each group, we use $m/d$+1 different ports of the E/D and Tables 5.2 (b)-(d) shows the correspondence between the data sequences (segmented in $d$=2, 3 and 4 parts, respectively) and the multidimensional OCs.

Table 5.2: Code lookup table (a) $d$=1, (b) $d$=2, (c) $d$=3, (d) $d$=4.

**(a)**

| X | #1 | #2 | #3 | #4 | #5 | #6 | #7 | #8 | #9 | #10 | #11 | #12 | #13 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 000000000000 | ○ | | | | | | | | | | | | |
| 000000000001 | | ○ | | | | | | | | | | | |
| 000000000010 | | | ○ | | | | | | | | | | |
| 000000000011 | | | | ○ | | | | | | | | | |
| 000000000100 | | | | | ○ | | | | | | | | |
| 000000000101 | | | | | | ○ | | | | | | | |
| 000000000110 | | | | | | | ○ | | | | | | |
| 000000000111 | | | | | | | | ○ | | | | | |
| ⋮ | | | | | | | | | | | | | |
| 111111111100 | | | | | | ○ | | | ○ | ○ | ○ | ○ | ○ |
| 111111111101 | | | | | | | ○ | | ○ | ○ | ○ | ○ | ○ |
| 111111111110 | | | | | | | | ○ | ○ | ○ | ○ | ○ | ○ |
| 111111111111 | ○ | | ○ | | ○ | | ○ | | ○ | | ○ | | ○ |

**(b)**

| LX | #1 | #2 | #3 | #4 | #5 | #6 | #7 | HX | #8 | #9 | #10 | #11 | #12 | #13 | #14 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 000000 | ○ | | | | | | | 000000 | ○ | | | | | | |
| 000001 | | ○ | | | | | | 000001 | | ○ | | | | | |
| 000010 | | | ○ | | | | | 000010 | | | ○ | | | | |
| 000011 | | | | ○ | | | | 000011 | | | | ○ | | | |
| 000100 | | | | | ○ | | | 000100 | | | | | ○ | | |
| 000101 | | | | | | ○ | | 000101 | | | | | | ○ | |
| 000110 | | | | | | | ○ | 000110 | | | | | | | ○ |
| 000111 | ○ | ○ | | | | | | 000111 | ○ | ○ | | | | | |
| ⋮ | | | | | | | | ⋮ | | | | | | | |
| 111100 | | | | ○ | ○ | | ○ | 111100 | | | | ○ | ○ | | ○ |
| 111101 | | | | ○ | | ○ | ○ | 111101 | | | | ○ | | ○ | ○ |
| 111110 | | | | | ○ | ○ | ○ | 111110 | | | | | ○ | ○ | ○ |
| 111111 | ○ | | ○ | | ○ | | ○ | 111111 | ○ | | ○ | | ○ | | ○ |

**(c)**

| LX | #1 | #2 | #3 | #4 | #5 | MX | #6 | #7 | #8 | #9 | #10 | HX | #11 | #12 | #13 | #14 | #15 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0000 | ○ | | | | | 0000 | ○ | | | | | 0000 | ○ | | | | |
| 0001 | | ○ | | | | 0001 | | ○ | | | | 0001 | | ○ | | | |
| 0010 | | | ○ | | | 0010 | | | ○ | | | 0010 | | | ○ | | |
| 0011 | | | | ○ | | 0011 | | | | ○ | | 0011 | | | | ○ | |
| 0100 | | | | | ○ | 0100 | | | | | ○ | 0100 | | | | | ○ |
| 0101 | ○ | ○ | | | | 0101 | ○ | ○ | | | | 0101 | ○ | ○ | | | |
| 0110 | ○ | | ○ | | | 0110 | ○ | | ○ | | | 0110 | ○ | | ○ | | |
| 0111 | ○ | | | ○ | | 0111 | ○ | | | ○ | | 0111 | ○ | | | ○ | |
| 1000 | ○ | | | | ○ | 1000 | ○ | | | | ○ | 1000 | ○ | | | | ○ |
| 1001 | | ○ | ○ | | | 1001 | | ○ | ○ | | | 1001 | | ○ | ○ | | |
| 1010 | | ○ | | ○ | | 1010 | | ○ | | ○ | | 1010 | | ○ | | ○ | |
| 1011 | | ○ | | | ○ | 1011 | | ○ | | | ○ | 1011 | | ○ | | | ○ |
| 1100 | | | ○ | ○ | | 1100 | | | ○ | ○ | | 1100 | | | ○ | ○ | |
| 1101 | | | ○ | | ○ | 1101 | | | ○ | | ○ | 1101 | | | ○ | | ○ |
| 1110 | | | | ○ | ○ | 1110 | | | | ○ | ○ | 1110 | | | | ○ | ○ |
| 1111 | ○ | | ○ | | ○ | 1111 | ○ | | ○ | | ○ | 1111 | ○ | | ○ | | ○ |

**(d)**

| LX | #1 | #2 | #3 | #4 | MLX | #5 | #6 | #7 | #8 | MHX | #9 | #10 | #11 | #12 | HX | #13 | #14 | #15 | #16 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 000 | ○ | | | | 000 | ○ | | | | 000 | ○ | | | | 000 | ○ | | | |
| 001 | | ○ | | | 001 | | ○ | | | 001 | | ○ | | | 001 | | ○ | | |
| 010 | | | ○ | | 010 | | | ○ | | 010 | | | ○ | | 010 | | | ○ | |
| 011 | | | | ○ | 011 | | | | ○ | 011 | | | | ○ | 011 | | | | ○ |
| 100 | ○ | ○ | | | 100 | ○ | ○ | | | 100 | ○ | ○ | | | 100 | ○ | ○ | | |
| 101 | | ○ | ○ | | 101 | | ○ | ○ | | 101 | | ○ | ○ | | 101 | | ○ | ○ | |
| 110 | | | ○ | ○ | 110 | | | ○ | ○ | 110 | | | ○ | ○ | 110 | | | ○ | ○ |
| 111 | ○ | | | ○ | 111 | ○ | | | ○ | 111 | ○ | | | ○ | 111 | ○ | | | ○ |

The implementation of electric code lookup table is based on a memory device, whose memory size $S$ [bit] equates the number of its elements. It is easy to verify that the number of elements of the lookup tables shown in Table 5.2 is

$$S = d \times 2^{\frac{\log_2 M}{d}} \times \left( \frac{\log_2 M}{d} + 1 \right) \tag{5.1}$$

The numerical $S$ is plotted as a function of $d$ in Fig. 5.3 for $M$=4096. It is evident that a large value of $d$ reduces the required memory size and simplifies the electronic circuit. Therefore, in our implementation, we have chosen $d$=3, so that the memory size is $S$=240 bit.

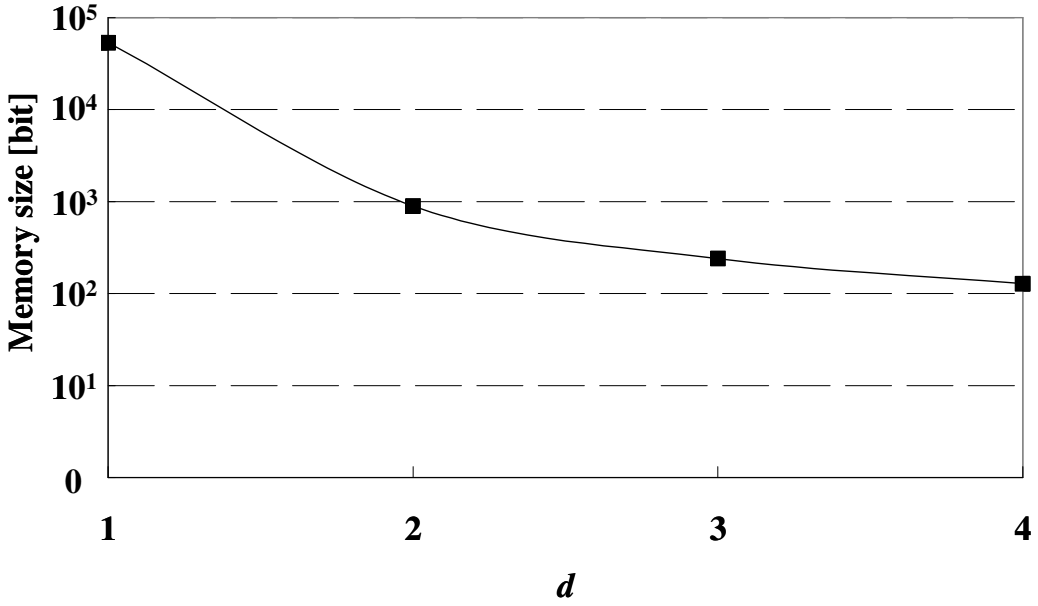



Fig. 5.3: Memory size $S$ against $d$ parameter.

Figure 5.4 shows the configuration of the FPGA (Xilinx Inc., mode number: XC4VLX25SF363, response time: 10 ns, maximum interface frequency: 622.08 MHz), that consists of $d$=3 sets of the 4-to-5 line coders and 1:$n$ ($n$=1, 2, 3) demultiplexer (DEMUX), so that each one of the three parts of the lookup table is implemented by a different 4-to-5 line coder. This scheme presents the additional advantage of large flexibility, because the M-ary number can be easily changed, according to the status of the electrical SW, as shown in Table 5.3.

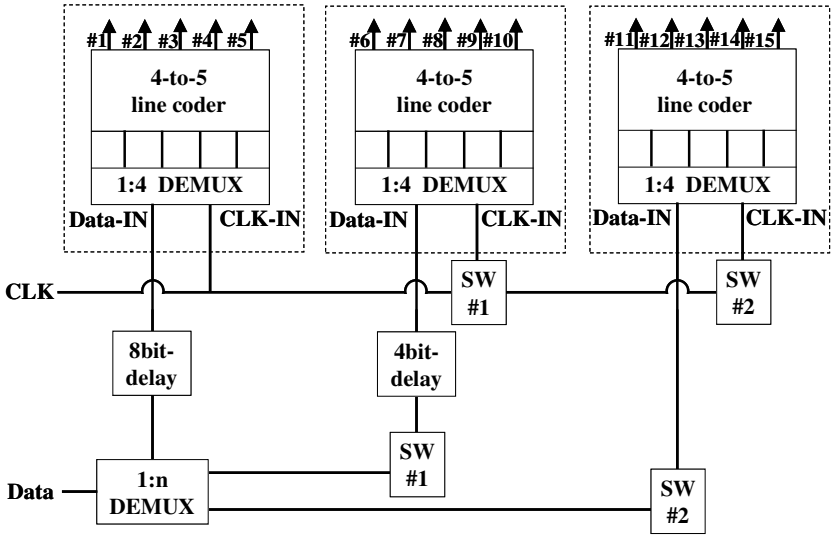



Fig. 5.4: Detailed structures of FPGA (1:12 DEMUX and 12-to-15 line coder ).

Table 5.3: Correspondence table of SW and *M*.

| SW #1 | SW #2 | M |
|---|---|---|
| OFF | OFF | 16 |
| OFF | ON | 256 |
| ON | OFF | 256 |
| ON | ON | 4096 |

We have implemented the 4096-ary OCDM architecture shown in Fig. 5.5. At the transmitter, a serial data bit stream at *B* bps is segmented every *m*=12 bits by a SP converter and each 12-bit block is sent to the line coder. The sequences of 12 bits are mapped into OCs, according to the code lookup table shown in Table 5.2 (c). Each output of line coder is connected to one of the *m*=12 ports of a multi-channel LN-IM gate switch array, that selects optical seed pulses corresponding to the OC. In the optical domain, the optical seed pulses at *B*/12 Hz are launched into the multi-channel LN-IM array, and only the pulses passing through the optical gate are forwarded to a designated input port of the multi-port E/D. Note that the selection of the input ports of the multi-port optical E/D determines which multidimensional OC is generated and that the code repetition rate equates to the symbol rate *B*/12 Hz.

At the receiver, the 4096-ary OCDM signal is processed by a multi-port optical E/D, that is identical to the one used at the transmitter. The autocorrelation waveforms detected at the matched output ports identify the multidimensional OC and are converted into an electrical signal by the multi-channel O/E converter array, and then launched into the line decoder, so that the 12-bit data sequence is recovered via the PS converter, using the same code lookup table of Table 5.2 (c).

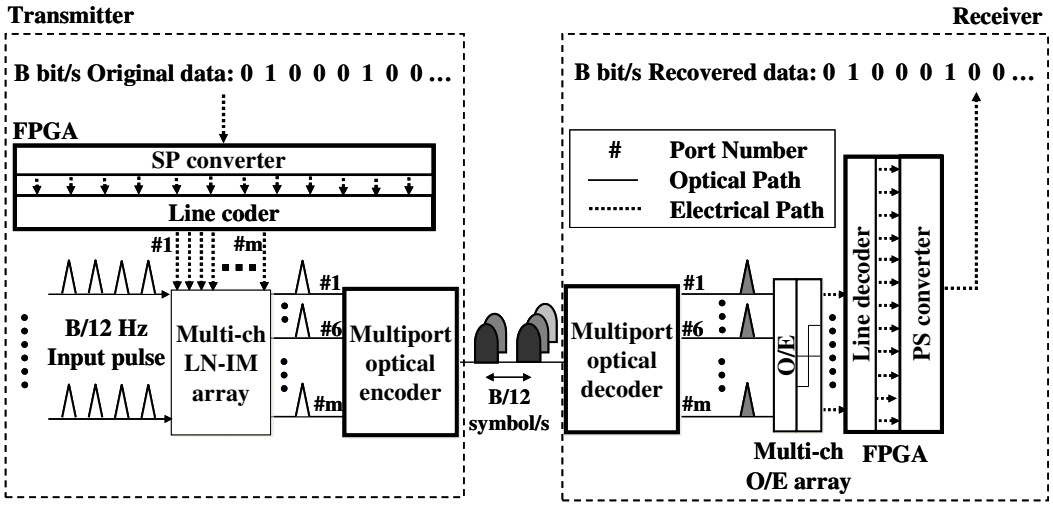



Fig. 5.5: Architecture of the 4096-ary OCDM system.

# 5.4 Experiments

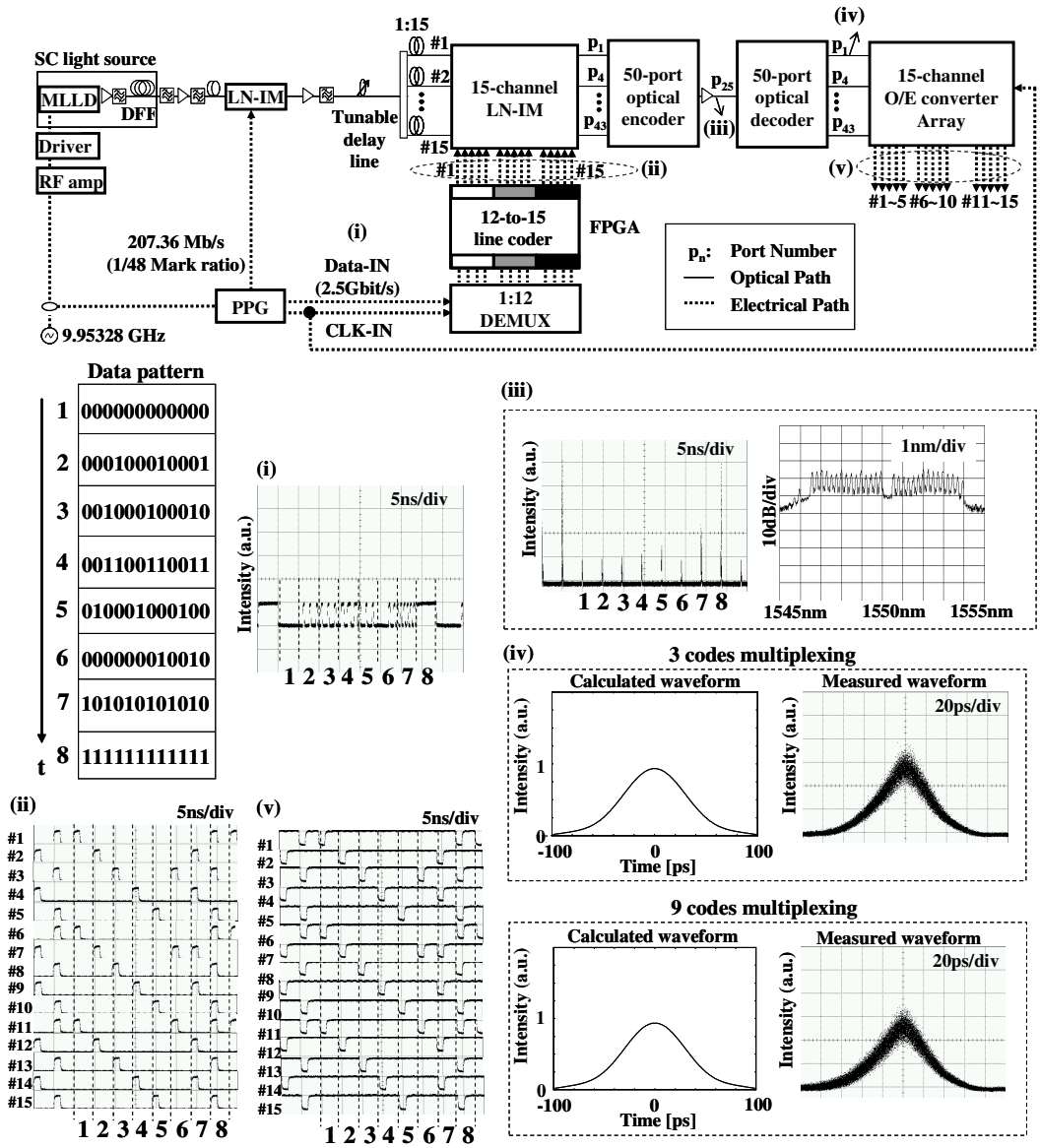



Fig. 5.6: Experimental setup of 4096-ary OCDM system ($d$=3).

Figure 5.6 shows the experimental setup of the 4096-ary OCDM transmitter; the serial data bit stream at $B$=2.48832 Gbps is segmented every 12 bits by the 1:12 DEMUX. We have further split the 12-bit sequence into $d$=3 blocks, and each 4-bit block is separately encoded using 5 inputs of the E/D. Therefore, in total we used $m$=15 E/D input ports and 15-dimensional OCs. The gate signals generated at the outputs of the 12-to-15 line coder (shown in Inset (ii)) are used to drive the 15-channel LN-IM array. We transmitted a fixed 96-bit data pattern, which includes all the codes in a period (shown in the Inset (i)).

A SC light source has been used at the transmitter, which consists of a MLLD, an EDFA, and a 2-km DFF. The MLLD at the wavelength of 1565 nm is driven at 9.95328 GHz and the SC signal is fed into an OBPF with 7.5 nm bandwidth at the center wavelength of 1550 nm. The pulse streams are down-converted to $B/12$=207.36 MHz by a LN-IM, and split into 15 arms by optical couplers. Each arm is connected to a LN-IM: the pulses pass through only if their arrival time coincides with the gate signal pattern from the line coder. Each output of the LN-SWs is connected to a different input port of the multi-port E/D; we used 15 input ports (every 3 port) of a 50×50 multi-port E/D. Please note that 16 ports out of 50 ports are used by selecting every 3 ports. The multidimensional OCs are the superposition of 15 PSK OCs, each of them is composed of 50 chips at 500 Gchip/s chip rate. Inset (iii) of Fig. 5.6 shows the waveform and spectrum of the 4096-ary OCDM signal. The output power of the encoder and input power of the decoder are -18.5 and -10.2 dBm.

At the receiver side, the 4096-ary OCDM signal is sent to the multi-port optical E/D and the autocorrelation waveforms are detected at the matched output ports. Inset (iv) show the calculated (left trace) and measured (right trace) autocorrelation waveforms of a multidimensional OC composed by 3 and 9 PSK OCs, respectively. We observe that experimental data are in good agreement with the theoretical model.

The output optical pulses from the multi-port optical E/D are converted into an electrical signal by the 15-channel O/E converter array (as shown in Inset (v)). All the electrical gate signal patterns show a clear opening and there is a perfect correspondence with the gate signals at the transmitter (Inset (ii)). We used a CDR circuit for data synchronization at the receiver, which has been described in Ref. [78].

The BER of an M-ary OCDM system was measured in Ref. [78], using a FPGA at the receiver. In this Chapter, we were not able to measure the BER, but the performance of the system is deducted from an inspection of the eye opening. Therefore, we can claim that the operation principle of a 4096-ary system has been successfully demonstrated.

50 km transmission of 16-ary OCDM signal through a SMF and DCF has been demonstrated in Chapter 3, showing that the M-ary signal can be transmitted over long link, if chromatic dispersion is properly compensated for. In addition, the transmission of multiplexed OCs has been demonstrated over 40 km fiber in Ref [77].

## 5.5 System Performance Analysis

In the analysis of the performance of multidimensional OCs, there are two main noise sources that we have to take into account: the cross correlation signals arising from unmatched PSK OCs and the beat noise at the detector. Figure 5.7 shows the model for the receiver that we have used for the numerical simulations: the received M-ary OCDM signal is correlated by the multi-port optical E/D with $N$ input/output ports and transformed into electrical signals by the O/E converters. The bandwidth of the O/E converters for 10 Gbps data rate is limited to 8.5 GHz. The electrical signals are then integrated over the time and dumped to a threshold circuit in order to determine the received signal. The time interval of the integrated-and-dumped circuit is the symbol duration $T_s$ i.e. the inverse of the symbol rate.

We assume that the multidimensional OC is composed of $m$ PSK OCs, so that the received optical field at the matched output $i$ can be written as [67]:

$$
\begin{aligned}
E(t) = & \sum_{l=0}^{N-1}(l+1)\exp\left[-\mathbf{j}\frac{2\pi(l+1)}{N}(i+k'+1)\right]\exp\left[-\frac{(t-l\Delta\tau)^2}{2T_0^2}\right] \\
& + \sum_{l=N}^{2N-2}(2N-l-1)\exp\left[-\mathbf{j}\frac{2\pi(l+1)}{N}(i+k'+1)\right]\exp\left[-\frac{(t-l\Delta\tau)^2}{2T_0^2}\right] \quad \textbf{Autocorrelation} \\
& + \sum_{k=1}^{m}\exp\left[-\mathbf{j}\frac{\pi(k'-k)}{N}\right]\sum_{l=0}^{2N-2}\exp\left[-\mathbf{j}\frac{2\pi(l+1)}{N}\left(i+1+\frac{k'-k}{2}\right)\right] \\
& \times \frac{\sin\left[\frac{\pi(l+1)(k'-k)}{N}\right]}{\sin\left[\frac{\pi(k'-k)}{N}\right]}\exp\left[-\frac{(t-l\Delta\tau)^2}{2T_0^2}\right] \quad \textbf{Crosscorrelation}
\end{aligned}
\qquad (5.2)
$$

$\Delta\tau$ is the time spacing between two consecutive chip pulses in each code (i.e. $1/\Delta\tau$ is the chip rate), whereas $k$ ($k=k'$) is the matched input port and $k$ ($k\neq k'$) are the input ports of the encoder where pulses are sent to generate multidimensional codes. The chip pulse waveforms are assumed to be Gaussian and $T_0$ is their full width half maximum (FWHM) of the input pulse. We assume that consecutive chips (with different $l$) partly interfere with each other, according to the experimental setup described in Section 5.4.

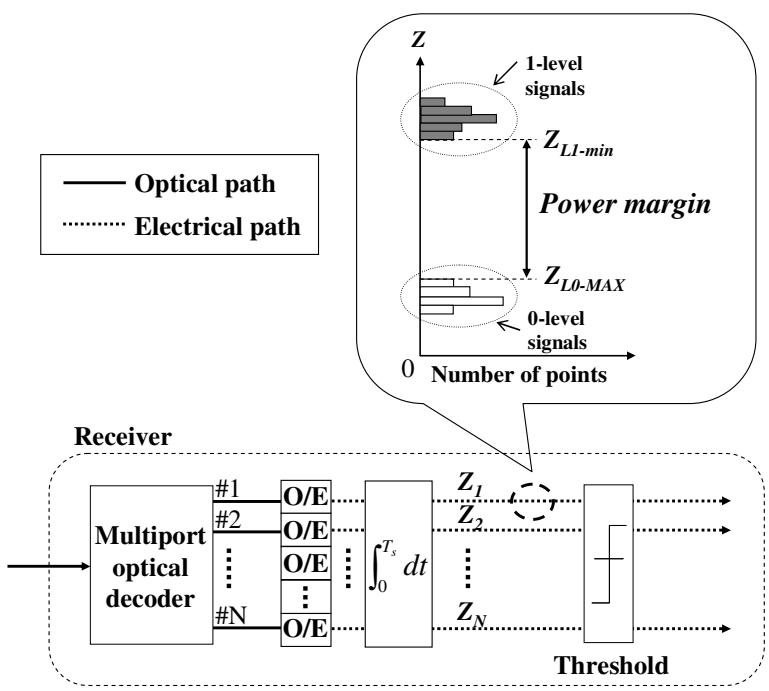



Fig. 5.7: System evaluation model of the receiver.

We calculate the signal $Z$ detected at the outputs of the O/E converter array as [30]:

$$
\begin{aligned}
Z &= \Re \int_0^{T_s} E(t)\cdot E^*(t)\,dt \\
&= \Re \int_0^{T_s} \left\{ \sum_{l=0}^{N-1} (l+1)^2 \exp\left[\frac{(t-l\Delta\tau)^2}{T_0^2}\right] + \sum_{l=N}^{2N-2} (2N-l-1)^2 \exp\left[\frac{(t-l\Delta\tau)^2}{T_0^2}\right] \right\} dt \\
&\quad + \Re \int_0^{T_s} \sum_{k=1}^{m} \sum_{l=0}^{2N-2} \frac{\sin\left[\frac{\pi(l+1)(k-k')}{N}\right]}{\sin\left[\frac{\pi(k-k')}{N}\right]} \exp\left[-\frac{(t-l\Delta\tau)^2}{T_0^2}\right] dt \\
&\quad + 2\Re \int_0^{T_s} \sum_{k=1}^{m} \sum_{l=0}^{N-1} \frac{\sin\left[\frac{\pi(l+1)(k-k')}{N}\right]}{\sin\left[\frac{\pi(k-k')}{N}\right]} \\
&\quad \times \cos\left[\frac{\pi(l+1)(k+k')}{N} - \frac{\pi(k-k')}{2N}\right] \exp\left[-\frac{(t-l\Delta\tau)^2}{T_0^2}\right] dt \\
&\quad + 2\Re \int_0^{T_s} \sum_{k=1}^{m} \sum_{l=N}^{2N-2} (2N-l-1) \frac{\sin\left[\frac{\pi(l+1)(k-k')}{N}\right]}{\sin\left[\frac{\pi(k-k')}{N}\right]} \\
&\quad \times \cos\left[\frac{\pi(l+1)(k+k')}{N} - \frac{\pi(k-k')}{2N}\right] \exp\left[-\frac{(t-l\Delta\tau)^2}{T_0^2}\right] dt \\
&\quad + 2\Re \int_0^{T_s} \sum_{k=1}^{m} \sum_{k''=1}^{m} \sum_{l=0}^{2N-2} \frac{\sin\left[\frac{\pi(l+1)(k-k')}{N}\right]}{\sin\left[\frac{\pi(k-k')}{N}\right]} \\
&\quad \times \frac{\sin\left[\frac{\pi(l+1)(k''-k')}{N}\right]}{\sin\left[\frac{\pi(k''-k')}{N}\right]} \cos\left[\frac{\pi(k''-k)}{2N} + \frac{\pi(l+1)(k-k'')}{N}\right] \exp\left[-\frac{(t-l\Delta\tau)^2}{T_0^2}\right] dt
\end{aligned}
\tag{5.3}
$$

**Autocorrelation**

**Crosscorrelation**

**Autocorrelation-crosscorrelation beat noise**

**Crosscorrelation-crosscorrelation beat noise**

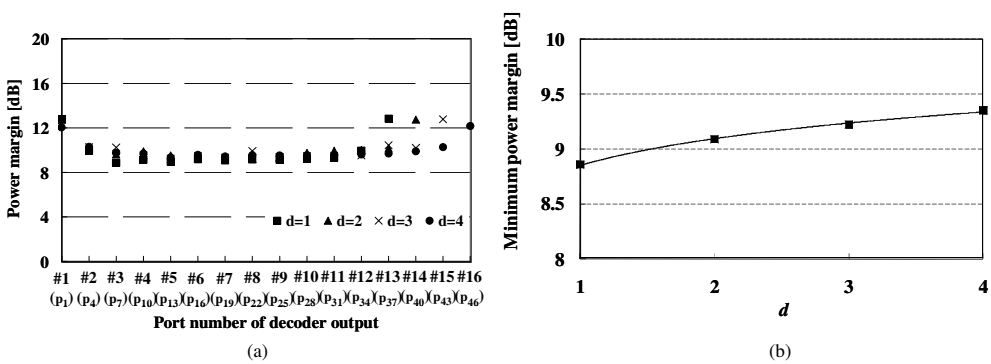
where $\Re$ is the responsibility of the photodetector. In this expression, the first and second terms are the intensities of the autocorrelation and the crosscorrelation signals, respectively. The third and fourth terms are the beat noise between the autocorrelation and the crosscorrelation. For the PSK OCs, we have to take into account the beat noise as we use a coherent source with coherent time $\tau_c$ much longer than the chip duration $\Delta\tau$ since all chips of OC are generated by a passive device, the phase relation between two different interfering signal is kept during the integration time $T_s$. Therefore, we cannot neglect the last terms in Eq. (5.3) which represents the beat noise between the $m$ crosscorrelation signals. It is noteworthy that we assume that all the input signals have the same polarization in the worst-case scenario. We exploit the key property of the PSK OCs of Eq. (5.3), i.e. the fact that the crosscorrelation signals detected at non-adjacent ports are very small and can be neglected [67], [68].

In our numerical simulations, we consider a multi-port E/D with $N$=50 input/output ports and a

Gaussian input pulse with $T_0$=2.2 ps. The integration time is $T_s$ =12/$B$ =4.8 ns and the chip interval is $\Delta\tau$=2 ps. The results from our numerical simulations, for all values of $d$ ($d$=1, 2, 3 and 4), confirm a clear separation between 0-level signal (related to the crosscorrelations) and 1-level signal (related to the autocorrelation) at every E/D output port. The power margin is defined as the difference between the minimum power of 1-level signal $Z_{L1\text{-}min}$ and the maximum power of 0-level signal $Z_{L0\text{-}MAX}$ as shown in Fig. 5.7.

$$\textbf{Power margin}\,[\textbf{dB}] = 10\log_{10}\frac{Z_{L1-\min}}{Z_{L0-MAX}} \tag{5.4}$$

Figure 5.8 (a) shows the power margin evaluated at each port of the E/D, for various values of the parameter $d$. The values obtained at the first and the last ports are higher with respect to the values corresponding to the other ports, because the effect of multiple interferences is smaller. The minimum power margin is slightly enhanced by increasing the value of $d$, as it is evident by an inspection of Fig. 5.8 (b) and it assumes the values of 8.9, 9.1, 9.2 and 9.4 dB, respectively. These results will confirm the decoding in the experiment with a good margin of the thresholding.




(a) (b)

Fig. 5.8: (a) Power margin at each port against $d$. (b) Minimum power margin versus number of $d$.

# 5.6 Data Confidentiality Analysis

An M-ary OCDM system that uses multidimensional OCs presents the following advantages, over conventional OCDM:

1) Increased code cardinality;
2) Reduced response speed of the electrical device at the receiver;
3) Enhanced data confidentiality [69];

In this section, we analyze the data confidentiality and we observe that M-ary systems that use conventional and multidimensional OCs provide both ‘optical’ and ‘electrical’ confidentiality, since an eavesdropper has first to decrypt the OC, and then he or she has to find the correspondence with the

sequence of bits. The 'optical' confidentiality of the M-ary system that uses multidimensional codes is *m* times larger than the one corresponding to a conventional system. In fact, in a multidimensional system, *m* PSK OCs are transmitted simultaneously and an eavesdropper must detect all of them correctly in order to decrypt the message. However, to analyze the system security, we considered only the 'electrical' confidentiality, evaluating the average number of trials that adversary has to make to decrypt a message. To give a quantitative evaluation of the system confidentiality, we first consider an exhaustive key search attack, or brute force attack, that is the simplest cryptanalysis attack; in this case, the eavesdropper is able to intercept only the ciphertext, i.e. the multidimensional OCs, and he or she has to guess which lookup table that has been used, i.e., the correspondence between the multidimensional OCs and the sequence of *m* bits.

According to the Kerckhoffs' principle, we assume that the eavesdropper knows everything about the OCDM encoding technique, in terms of data and chip rates, code length, modulation formats, wavelengths, and so on. In addition, if the message of *m* bits is split into *d* parts, the adversary knows also the segmentation rule. The *d* groups of *m*/*d* bits are separately encoded onto *m*/*d*+1 OCs, using *d* independent lookup tables, so that the total number of possible choices is $d\left(2^{\frac{m}{d}}!\right) = d(\sqrt[d]{M}!)$. Figure 5.9 (a) shows the number of trials necessary to break the system confidentiality in a 4096-ary system, as a function of *d*. In our demonstration, the 12-bit message is split in *d*=3 parts, and the number of COA necessary is $3\times(16!) = 7\times10^{13}$.

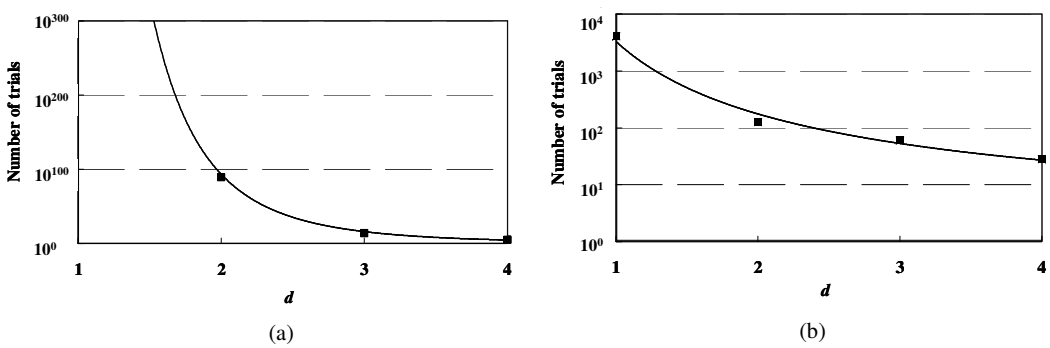



Fig. 5.9: (a) Number of trials to break the confidentiality with COA, (b) Number of trials necessary to break the confidentiality with a CPA.

The lowerbound security parameter of modern cryptanalysis is the number of plaintexts that an eavesdropper needs to know in a CPA, to break the system confidentiality: this attack assumes that the eavesdropper has the capability to choose arbitrary plaintexts and he or she can encrypt them to obtain the corresponding ciphertexts, i.e., the OCs. In M-ary OCDM that uses multidimensional PSK OCs, the eavesdropper can easily reveal how the message is split into the *d* blocks, just encoding a single

message. For each block, the adversary has to find all the correspondences (minus one) between the sequences of *m*/*d* bits and the OCs, making $\sqrt[d]{M}-1$ attempts. If we assume that the lookup tables of the *d* blocks are independent, the total number of trials required to decrypt all the codewords in a multidimensional M-ary OCDM system is $d(\sqrt[d]{M}-1)$. Figure 5.9 (b) shows the confidentiality against CPAs for 4096-ary, as a function of *d*; in our implementation, for *d*=3, the number of attempts required is 45. The confidentiality comparison of three M-ary OCDM systems is shown in Table 5.4.

Table 5.4: Confidentiality comparison of M-ary OCDM systems.

| | Conventional | POL-MUX | Multidimensional |
|---|---|---|---|
| Number of trials against COA | $M!/2$ | $\left[\left(\sqrt{M}\right)!\right]^2 m!/\left\{2\times\left[(m/2)!\right]^2\right\}$ | $d\left(\sqrt[d]{M}!\right)$ |
| Number of trials against CPA | $(M-1)\log_2 M$ | $2\left(\sqrt{M}-1\right)$ | $d\left(\sqrt[d]{M}-1\right)$ |

# 5.7 Extension of Multiple Access: M-ary OCDMA System

10 Gbps TDM-PON is the most promising candidate for the next generation access networks and the corresponding standardization activities have been already completed in IEEE802.3av [18] and ITU-T G.984.5. OCDMA is considered as one of the candidate systems for NG-PON2. Recently, 10 Gbps OCDMA-based PONs have been experimentally demonstrated [79-81], and it has been shown that these systems are a reliable alternative to standard TDM-PON [19], with a larger data confidentiality and bandwidth efficiency, they also allow asynchronous transmission, soft capacity on demand, protocol transparency, simplified network control and flexibility in the QoS management.

In a conventional OCDMA-based PON, each user receives a different OC and can access the network in an asynchronous way, however, the corresponding data confidentiality is quite limited, since an eavesdropper can sift data transmitted to or by another user is he or she possesses the matched decoder. Therefore, to increase the data confidentiality in access networks, we propose a new 10 Gbps 4096-ary OCDMA-based PON system, where each user transmits and receives multidimensional PSK OCs, i.e. a different set of PSK OCs.

## 5.7.1 System Configuration

Figure 5.10 shows the system architecture: a multi-port E/D is located in each ONU and in the OLT.

In the downlink transmission, the central office encodes the signal using the combination of the OCs assigned to the different ONUs. At the receiver side, each ONU decodes only the matched set of OCs. In the uplink, all ONUs can simultaneously transmit signals to the central office in an asynchronous way because each ONU uses a different combination of OCs. This is so-called *tell-and-go* access protocol.

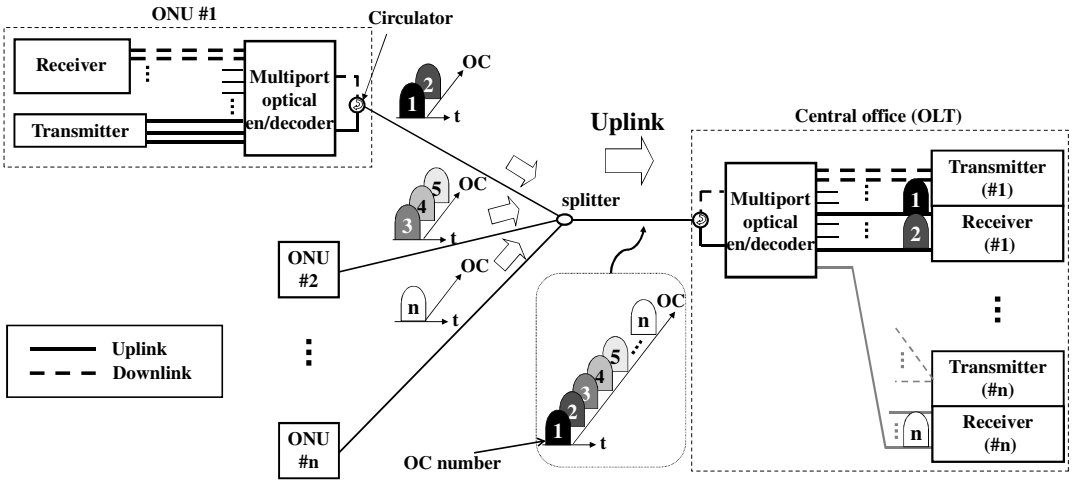



Fig. 5.10: Architecture of a 4096-ary OCDMA-PON.

## 5.7.2 Performance Analysis of 4096-ary OCDMA System

In the case of a $B$=10 Gbps, $2^m$=4096-ary OCDMA system, the symbol interval is $T_s=m/B$=1.2 ns. To increase the overall number of user, we increase the number of chip pulses (that equates the number $N$ of the ports of the E/D) in each OC duration $T_{code}$ must satisfy the condition $2T_{code} \leq T_s$ to avoid inter-symbol overlapping, because the autocorrelation and crosscorrelation signals extend over the double of the code duration.

We consider three multi-port E/Ds with $N$=100, 200 and 300 ports, so that the OC duration is 200 ps, 400 ps and 600 ps, respectively. However, to generate codes that are orthogonal (low crosscorrelation), we use only the odd ports, so the total number of OCs available are 50, 100, and 150, respectively. Please note that an AWG with 400 ports has been already fabricated [82]. Therefore, a multi-port E/D with up to 400 ports would be realistic.

We assume that there are $n$ active ONUs in the network and 15 different OCs codes are assigned to each ONU. The system performance are evaluated when the MAI noise is maximum, i.e., all ONUs access synchronously to the network, with the same symbol rate. Moreover, we assume that all OCs of all ONUs except for ONU #1 are used in the case of 2 or more ONUs. In the following, the condition is assumed as a worst case (as shown in Fig. 5.11).

In the case of 100-chip OCs, ONU #$n$ transmits/receives OCs generated/processed at the 15 ports $p_r=2n+6r-1$ ($n$=1, 2,…, 3, $r$=0, 1,…, 14) of the E/D. With an E/D of 200 ports (200-chip OCs), the 15 ports $p_r=2n+12r-1$ ($n$=1, 2,…, 6, $r$=0, 1,…, 14) are assigned to ONU #$n$. Finally, ONU #$n$ is assigned

to the 15 ports $p_r$=2$n$+20$r$-1 ($n$=1, 2,…, 10, $r$=0, 1,…, 14), for 300-chip OCs. In Fig. 5.12, the minimum power margin at the output ports of ONU #1 is plotted for different numbers of simultaneous ONUs, and we observe that it decreases with the number of ONUs. Although the number of users that can be accommodated in the M-ary OCDMA is not impressive, it may find a niche application such as mission-critical access.

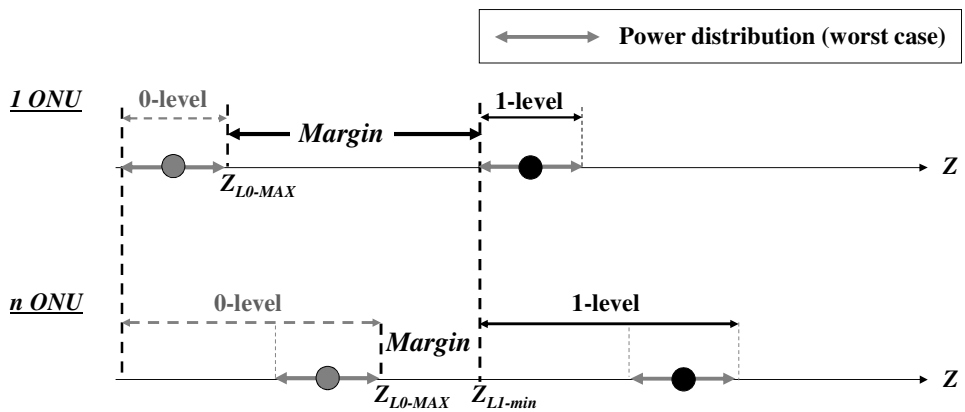



Fig. 5.11: A model of power margin at multi-ONU.

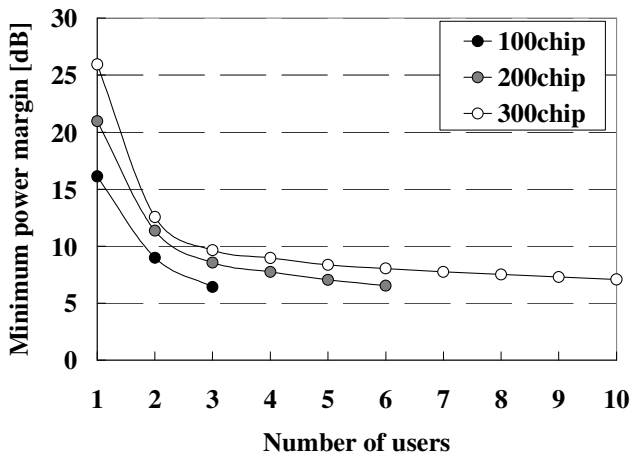



Fig. 5.12: Minimum power margin versus number of ONUs.

## 5.8 Conclusion

We have proposed and experimentally demonstrated M-ary OCDM system based on multidimensional PSK OCs generated by multi-port E/D. The input bit sequence is segmented into *d* blocks, which are separately encoded into OCs. We have experimentally demonstrated the proof-of-concept of a 4096-ary, 207.36 MSymbol/s, coherent OCDM system and we have based numerically evaluated the corresponding confidentiality, that decreases with the parameter *d*. The numerical simulations show that the power margin between the 0 and 1-level at each port of the E/D is quite high, and it increases with *d*, so that there is a trade-off between the power margin and the data confidentiality. Finally, a new 10 Gbps, OCDM-based access network has been proposed and numerically analyzed, based on a 10 Gbps, 4096-ary OCDMA system using a multi-port E/D.

# Chapter 6

# Conclusions

This dissertation has been devoted to present a study on secure M-ary OCDM using a single multi-port E/D for the purpose of achieving high-security P2P transmission which another multiplexing technique can not reach. In addition, the system is also applied to high transmission rate system since the symbol rate can be lowered by increasing the number of *M*. This scheme allows to be reduced the effect of ISI by improving the dispersion tolerance. The main results obtained in this dissertation can be summarized as follows:

In Chapter 3, secure 16-ary, 622 MSymbol/s coherent OCDM-based block ciphering with online XOR and its 50-km transmission have been experimentally demonstrated. The newly developed instantaneous-response-type CDR circuit is a key enabler for the transmission to recover the clock data from 16-ary OCDM signal, and the use of a single multi-port E/D has simplified the optical implementation. The proposed scheme guarantees enhancement of both physical and computational data confidentiality.

In Chapter 4, we have proposed a novel M-ary OCDM system using polarization multiplexing technique and a single multi-port optical E/D. We showed that POL-MUX M-ary OCDM system can reduce the number of necessary OCs and doubles the spectral efficiency, compared with a conventional system. We have demonstrated a 2.5 Gbps, 256-ary POL-MUX OCDM system using a single multi-port E/D and analyzed the corresponding confidentiality.

In Chapter 5, we have proposed and experimentally demonstrated M-ary OCDM system based on multidimensional PSK OCs generated by multi-port E/D. The input bit sequence is segmented into *d* blocks, which are separately encoded into OCs. We have experimentally demonstrated the proof-of-concept of a 4096-ary, 207.36 MSymbol/s, coherent OCDM system and we have numerically evaluated the corresponding confidentiality, that decreases with the parameter *d*. The numerical simulations show that the power margin between the 0 and 1-level at each port of the E/D is quite high, and it increases with *d*, so that there is a trade-off between the power margin and the data confidentiality. Finally, a new 10 Gbps, OCDM-based access network has been proposed and numerically analyzed, based on a 10 Gbps, 4096-ary OCDMA system using a multi-port E/D.

All the results have been shown in Chapter 3, 4, and 5 prove highly reliable feasibility of the proposed M-ary OCDM systems. M-ary OCDM system with XOR can be realized by use of the

optical implementation of the CBC mode. By combining the techniques of Chapter 3 and 4, M-ary OCDM system can also be closer to the bit block length of the current encryption standard algorithm AES that every user can choice the bit block length in three patterns (128, 192 or 256). The method of selecting bit block length is considered applying the introduced the electrical circuit in Chapter 5.

In the future development of the system, fine processing technology against optical waveguide is also important issue. With the development of multi-port E/D that can generate a large number of OC by microfabrication technology, a large number M-ary system can be constructed.

From the all obtained results and findings, each proposed techniques are expected to support M-ary OCDM/OCDMA system for advanced secure optical access networks in future photonic networks.

# Acronyms

| | |
|---|---|
| ACP | autocorrelation peak |
| AES | advanced encryption standard |
| AWG | arrayed waveguide grating |
| BER | bit error rate |
| bps | bit per second |
| B-to-B | back-to-back |
| CBC | cipher block chaining |
| CCP | crosscorrelation peak |
| CDR | clock data recovery |
| CIA | confidentiality, integrity and availability |
| COA | cipher-text only attacks |
| CPA | chosen plaintext attacks |
| CR | clock recovery |
| CSK | code-shifting-keying |
| DCF | dispersion compensation fiber |
| DEMUX | demultiplexer |
| DES | data encryption standard |
| DFF | dispersion-flattened fiber |
| DPSK | differential-phase-shift-keying |
| DS-SS | direct-sequence spread spectrum |
| DWDMA | dense wavelength division multiple access |
| ECB | electronic codebook |
| E/D | encoder/decoder |
| EDFA | erbium-doped fiber amplifier |

| | |
|---|---|
| FPGA | field programmable gate array |
| FSR | free spectral range |
| FTTH | fiber-to-the-home |
| FWHM | full width half maximum |
| GMPLS | generalized multiprotocol label switching |
| GVD | group velocity dispersion |
| IP | Internet protocol |
| IPsec | Internet protocol security |
| ISI | inter-symbol interference |
| ISO | international organization for standardization |
| LN-IM | $LiNbO_3$ intensity modulator |
| LN-SW | $LiNbO_3$ switch |
| LPF | low pass filter |
| MLLD | mode-locked laser diode |
| MSL | maximum sidelobe |
| MUX | multiplexer |
| NG | next-generation |
| NLS | nonlinear Schrödinger |
| OBPF | optical band pass filter |
| OC | optical code |
| OCDM | optical code division multiplexing |
| OCDMA | optical code division multiple access |
| ODN | optical distribution network |
| O/E | optical-to-electrical |
| OFDMA | orthogonal frequency division multiple access |
| OLT | optical line terminal |
| ONU | optical network unit |
| OOK | on-off keying |
| PBS | polarization beam splitter |
| PC | polarization controller |
| PD | photo detector |
| PIIN | phase induced intensity noise |
| PL1sec | photonic layer 1 security technology |
| POL-MUX | polarization multiplexed |
| PON | passive optical networks |
| PPG | pulse pattern generator |

| | |
|---|---|
| PRBS | pseudo-random bit sequence |
| PS | parallel-to-serial |
| PSK | phase-shift keying |
| P2P | point-to-point |
| QKD | quantum key distribution |
| QNRC | quantum noise randomized cipher |
| QoS | quality of service |
| RSA | Rivest, Shamir, and Adleman |
| SC | spectral coding |
| SC | super-continuum |
| SCOC | secure communications using optical chaos |
| SHA-1 | secure Hash algorithm 1 |
| SMF | single mode fiber |
| SP | serial-to-parallel |
| SSL | secure socket layer |
| SW | switch |
| TDM | time division multiplexing |
| TDMA | time division multiple access |
| TS | time-spreading |
| VPN | virtual private network |
| WDM | wavelength division multiplexing |
| WDMA | wavelength division multiple access |
| XOR | exclusive OR |
| 1-D | one-dimensional |
| 2-D | two-dimensional |

# List of Symbols

| Symbol | Description |
|---|---|
| $\omega$ | angular frequency |
| $\lambda$ | wavelength |
| $h_d(t)$ | function of decoder |
| $H_d(\omega)$ | Fourier spectrum of decoder |
| $h_e(t)$ | function of OC |
| $H_e(\omega)$ | Fourier spectrum of OC |
| **j** | imaginary unit |
| $u_0(t)$ | output of matched filter |
| $\psi(t)$ | auto-correlation function of the input OC |
| $\omega_0$ | center frequency ($\lambda$=1550.984 nm) |
| $N$ | port or chip number |
| $R$ | input/output slabs focal length |
| $d$ | AWG spacing |
| $w_g$ | AWG waveguide width |
| $d_i$ | waveguide spacing in the input grating |
| $d_o$ | waveguide spacing in the output grating |
| $w_{i/o}$ | waveguide width in the input/output grating |
| $\Delta L$ | differential path length |
| $n_s$ | effective reflactive index |
| $\delta(t)$ | Dirac delta |
| $L$ | smallest waveguide length |
| $\theta_i$ | diffraction angles in the input slab |
| $\theta_o$ | diffraction angles in the output slab |
| $\Delta\tau$ | time distance between two consecutive pulses in each code |
| $i$ | input/output port number of multi-port E/D |
| $l$ | chip pulse number |
| $k$ | input/output port number of multi-port E/D |
| $*$ | convolution unit |
| $H_{ik}(\omega)$ | transfer function from the input $i$ to the output $k$ |
| $MSL$ | maximum sidelobe |

| | |
|---|---|
| $U$ | normalized amplitude |
| $\gamma$ | nonlinear parameter |
| $\tilde{U}$ | Fourier transform of the incident field |
| $T_0$ | half-width (at $1/e$ -intensity point) |
| $b_n$ | serial data bit stream is segmented every four bits |
| $C_n$ | optical code number |
| $B$ | serial data bit stream |
| $S$ | memory size |
| $k'$ | output port number of multi-port decoder |
| $T_s$ | integration time |
| $Z_{L1\text{-}min}$ | minimum power of 1-level signal |
| $Z_{L0\text{-}MAX}$ | maximum power of 0-level |
| $T_{code}$ | each OC duration |

# Bibliography


[1] G. S. Kanter, D. Reilly, and N. Smith, "Practical physical-layer encryption: The marriage of optical noise with traditional cryptography," *IEEE Communications Magazine*, vol. 47, no. 11, pp. 74-81, November 2009.

[2] M. Medard, D. Marquis, R. A. Barry, and S. G. Finn, "Security issues of all-optical networks," *IEEE Network*, vol. 11, no. 3, pp. 42-48, May/June 1997.

[3] T. Wu and A. K. Somani, "Cross-talk attack monitoring and localization in all-optical networks," *IEEE/ACM Transactions on Networking*, vol. 13, no. 6, pp. 1390-1401, December 2005.

[4] R. Rejeb, M. S. Leeson, and R. J. Green, "Fault and attack management in all-optical networks," *IEEE Communications Magazine*, vol. 44, no. 11, pp. 79-86, November 2006.

[5] T. Deng and S. Subramaniam, "Analysis of optical amplifier gain competition attack in a point-to-point WDM link," in *Proc. International Society for Optics and Photonics (SPIE)*, vol. 4874, no. 249, pp. 249-261, Boston, MA, USA, July 2002.

[6] T. Deng and S. Subramaniam, "Covert low-power QoS attack in all-optical wavelength routed networks," in *Proc. Global Telecommunications Conference (GLOBECOM 2004)*, vol. 3, pp. 1948-1952, Dallas, Texas, USA, November 2004.

[7] S. V. Kartalopolos, "Security in advanced optical communication networks," in *Proc. IEEE International Conference on Communications (ICC 2009)*, pp. 1-5, Dresden, Germany, June 2009.

[8] The Wolf Report (in German) [Online]. Available: http://www.youtube.com/watch?v=2DvaubDDbss see also

[9] M. Fujiwara, S. Miki, T. Yamashita, Z. Wang, and M. Sasaki, "Photon level crosstalk between parallel fibers installed in urban area," *Optics Express*, vol. 18, no. 21, pp. 22199-22207,

October 2010.

[10] T. Kleinjung, K. Aoki, J. Franke, A. K. Lenstra1, E. Thomél, J. W. Bos, P. Gaudry, A. Kruppa, P. L. Montgomery, D. A. Osvik, H. te Riele, A. Timofeev, and P. Zimmermann, "Factorization of a 768-bit RSA modulus," *Cryptology ePrint Archive: Report 2010/006*, February 2010.

[11] C. H. Bennett and G. Brassard, "Quantum cryptography: public key distribution and coin tossing," in *Proc. IEEE International Conference on Signal Processing (ICSPCC 1984)*, pp. 175-179, Bangalore, India, December 1984.

[12] A. Argyris, D. Syvridis, L. Larger, V. Annovazzi-Lodi, P. Colet, I. Fischer, J. Garcia-Ojalvo, C.Mirasso, L. Pesquera, and K. Shore, "Chaos-based communications at high bit rates using commercial fiber-optic links," *Nature*, vol. 438, no. 17, pp. 343-346, November 2006.

[13] H. P. Yuen, "A new quantum cryptography," *Report in Northwestern University: DARPA Proposed paper*, 2000.

[14] J. P. Heritage and A. M. Weiner, "Advances in spectral optical code-division multiple-access communications," *IEEE Journal of Selected Topics in Quantum Electronics*, vol. 13, no. 5, pp. 1351-1369, September/October 2007.

[15] P. R. Prucnal (Ed.), "Optical code division multiple access: fundamentals and applications," *Taylor&Francis*, NewYork, 2006.

[16] T. S. Yum and M. Chen, "A conflict-free protocol for optical WDMA networks," in *Proc. IEEE Global Telecommunications Conference (GLOBECOM 1991)*, vol. 2, pp. 1276-1281, Phoenix, AZ, December 1991.

[17] W. Huang, M. H. M. Nizam, Ivan Andonovic, and M. Tur, "Coherent optical CDMA (OCDMA) systems used for high-capacity optical fiber networks-system description, OTDMA comparison, and OCDMA/WDMA networking," *IEEE/OSA Journal of Lightwave Technol*ogy, vol. 18, no. 6, pp. 765-778, June 2000.

[18] IEEE 802.3av Task Force, http://www.ieee802.org/3/av/.

[19] FSAN NGA, http://www.fsanweb.org/.

[20] K. Kitayama, "OCDMA and OFDMA technologies for NG-PON," in *Proc. Access Networks and In-house Communication (ANIC)*, ATuB4, Toronto, Canada, June 2011.

[21] P. R. Prucnal, M. A. Santoro, and T. R. Fan, "Spread spectrum fiber-optic local area network using optical processing," *IEEE/OSA Journal of Lightwave Technol*ogy, vol. 4, no. 5, pp. 547-554, May 1986.

[22] J. A. Salehi and C. A. Brackett, "Code division multiple-access technique in optical fiber networks, part I: Fundamental principles and part II: Systems performance analysis," *IEEE. Transactions on Communications*, vol. 37, no. 8, pp. 824-842, August 1989

[23] M. E. Marhic, "Trends in optical CDMA," in *Proc. Multigigabit Fiber Communication (SPIE)*, vol. 1787, no. 80, pp. 80-98, Boston, MA, USA, September 1992.

[24] D. D. Sampson, G. J. Pendock, and R. A. Grifin, "Photonic code-division multiple-access communications," *Taylor & Francis Fiber and Integrated Optics*, vol. 16, no. 2, pp. 129-157, 1997.

[25] K. Kitayama, "Code division multiplexing lightwave networks based upon optical code conversion," *IEEE Journal on Selected Areas in Communications*, vol. 16, no. 7, pp. 1209-1319, September 1998.

[26] K. Kitayama, N. Wada, and H. Sotobayashi, "Architectural considerations of photonic IP router based upon optical code correlation," *IEEE/OSA Journal of Lightwave Technol*ogy, vol. 18, no. 12, pp. 1834-1844, December 2000.

[27] H. Ramanitra, P. Chanclou, Z. Belfqih, M. Moignard, H. Le Bras, and D. Schumacher, "Scalable and multi-service passive optical access infrastructure using variable optical splitters," in *Proc. IEEE/OSA Optical Fiber Communication Conference and the National Fiber Optic Engineers Conference (OFC/NFOEC 2006)*, OFE2, Anaheim, CA, March 2006.

[28] K. Kitayama and M. Murata, "Versatile optical code-based MPLS for circuit, burst, and packet switchings," *IEEE/OSA Journal of Lightwave Technology*, vol. 21, no. 11, pp. 2753-2764, November 2003.

[29] K. Kitayama and N. Wada, "Photonic IP routing," *IEEE Photonics Technology Letters*, vol. 11, no. 12, pp. 1689-1691, December 1999.

[30] X. Wang and K. Kitayama, "Analysis of beat noise in coherent and incoherent time-spreading OCDMA," *IEEE/OSA Journal of Lightwave Technol*ogy, vol. 22, no. 10, pp. 2226-2235, October 2004.

[31] G. E. Town, K. Chan, and G. Yoffe, "Design and performance of high-speed optical pulse-code generators using optical fiber bragg gratings," *IEEE Journal of Selected Topics in Quantum Electronics*, vol. 5, no. 5, pp. 1325-1331, September/October 1999.

[32] H. Tsuda, H. Takenouchi, T. Ishii, K. Okamoto, T. Goh, K. Sato, A. Hirano, T. Kurokawa, and C. Amano, "Spectral encoding and decoding of 10 Gbit/s femtosecond pulses using high resolution arrayed-waveguide grating," *IET Electronics Letters*, vol. 35, no. 14, pp. 1186-1187, July 1999.

[33] Z. Wei, H. M. H. Shalaby, and H. Ghafouri-Shiraz, "Modified quadratic congruence codes for fiber bragg-grating-based spectral-amplitude-coding optical CDMA systems," *IEEE/OSA Journal of Lightwave Technol*ogy, vol. 19, no. 9, pp. 1274-1281, September 2001.

[34] S. Yegnanarayanan, A. S. Bhshan, and B. Jalali, "Fast wavelength-hopping time-spreading

encoding/decoding for optical CDMA," *IEEE Photonics Technology Letters*, vol. 12, no. 5, pp. 573-575, May 2000.

[35] K. Yum, J. Shin, and N. Park, "Wavelength-time spreading optical CDMA system using wavelength multiplexers and mirrors fiber delay lines," *IEEE Photonics Technology Letters*, vol. 12, no. 9, pp. 1278-1280, September 2000.

[36] H. Fathallah, L. A. Rusch, and S. LaRochelle, "Passive optical fast frequency-hop CDMA communications system," *IEEE/OSA Journal of Lightwave Technol*ogy, vol. 17, no. 3, pp. 397-405, March 1999.

[37] X. Wang and K. T. Chan, "A sequentially self-seeded Fabry-Perot laser for two-dimensional encoding/decoding of optical pulses," *IEEE Journal of Selected Topics in Quantum Electronics*, vol. 39, no. 1, pp. 83-90, January 2003.

[38] N. Wada, H. Sotobayashi, and K. Kitayama, "2.5 Gbit/s time-spread/wavelength-hop optical code division multiplexing using fiber bragg grating with super continuum light source," *IET Electronics Letters*, vol. 36, no. 9, pp. 815-817, April 2000.

[39] R. A. Griffin, D. D. Sampson, and D. A. Jackson, "Coherence coding for photonic code-division-multiple access networks," *IEEE/OSA Journal of Lightwave Technol*ogy, vol. 13, no. 9, pp. 1826-1837, September 1995.

[40] M. E. Maric, "Coherent optical CDMA networks," *IEEE/OSA Journal of Lightwave Technol*ogy, vol. 11, no. 5, pp. 854-864, May/June 1993.

[41] N. Wada and K. Kitayama, "A 10 Gb/s optical code division multiplexing using 8-chip optical bipolar code and coherent detection," *IEEE/OSA Journal of Lightwave Technol*ogy, vol. 17, no. 10, pp. 1758-1765, October 1999.

[42] J. A. Salehi, A. M. Weiner, and J. P. Heritage, "Coherent ultrashort light pulse code-division multiple access communication systems," *IEEE/OSA Journal of Lightwave Technol*ogy, vol. 8, no. 3, pp. 478-491, March 1990.

[43] C. C. Chang, H. P. Sardesai, and A. M. Weiner, "Code-division multiple-access encoding and decoding of femtosecond optical pulses over a 2.5 km fiber link," *IEEE Photonics Technology Letters*, vol. 10, no. 1, pp. 171-173, January 1998.

[44] A. Grunnet-Jepsen, A. E. Johnson, E. S. Maniloff, T. W. Mossberg, M. J. Munroe, and J. N. Sweetser, "Fiber bragg grating based spectral encoder/decoder for lightwave CDMA," *IET Electronics Letters*, vol. 35, no. 13, pp. 1096-1097, June 1999.

[45] P. C. Teh, P. Petropoulos, M. Ibsen, and D. J. Richardson, "A comparative study of the performance of seven and 63-chip optical code-division multiple-access encoders and decoders based on superstructured fiber bragg gratings," *IEEE/OSA Journal of Lightwave Technol*ogy,

vol. 19, no. 9, pp. 1352-1365, September 2001.

[46] P. C. Teh, M. Ibsen, J. H. Lee, P. Petropoulos, and D. J. Richardson, "Demonstration of a four-channel WDM/OCDMA system using 255-chip 320-Gchip/s quarternary phase coding grating," *IEEE Photonics Technology Letters*, vol. 14, no. 2, pp. 227-229, February 2002.

[47] K. Matsushima, X. Wang, S. Kutsuzawa, A. Nishiki, S. Oshiba, N. Wada, and K. Kitayama, "Experimental demonstration of performance improvement of 127-Chip SSFBG en/decoder using apodization technique," *IEEE Photonics Technology Letters*, vol. 16, no. 9, pp. 2192-2194, September 2004.

[48] X. Wang, K. Matsushima, A. Nishiki, N. Wada, F. Kubota, and K. Kitayama, " Experimental demonstration of 511-chip 640Gchip/s superstructured FBG for high performance optical code processing," in *Proc. European Cnference of Optical Communication* (*ECOC'04*), Tu1.3.7, Stockholm, Sweden, August 2004.

[49] M. E. Marhic and Y. L. Chang, "Pulse coding and coherent decoding in fiber-optic ladder networks," *IET Electronics Letters*, vol. 25, no. 22, pp. 1535-1536, October 1989.

[50] R. A. Griffin, D. D. Sampson, and D. A. Jackson, "Optical phase coding for code-division multiple access networks," *IEEE Photonics Technology Letters*, vol. 4, no. 12, pp. 1401-1404, December 1992.

[51] N. Wada and K. Kitayama, "Error-free 10 Gb/s transmission of coherent optical code division multiplexing using all-optical encoder and balanced detection with local code," in *Proc. IEEE/OSA Optical Fiber Communication Conference and the National Fiber Optic Engineers Conference (OFC/NFOEC 1998)*, FE7, San Jose, CA, USA, February 1998.

[52] A. M. Weiner, J. P. Heritage, and J. A. Salehi, "Encoding and decoding of femtosecond pulses," *Optics Letters*, vol. 13, no. 4, pp. 300-302, April 1988.

[53] H. Sotobayashi and K. Kitayama, "1.24 Gb/s, optical code division multiplexing transmission over 40km dispersion shifted fiber by bipolar coding using broadband incoherent light source," *IET Electronics Letters*, vol. 35, no. 11, pp. 911-912, May 1999.

[54] T. H. Shake, "Security performance of optical CDMA against eavesdropping," *IEEE/OSA Journal of Lightwave Technol*ogy, vol. 23, no. 2, pp. 655-670, February 2005.

[55] T. H. Shake, "Confidentiality performance of spectral-phase-encoded optical CDMA," *IEEE/OSA Journal of Lightwave Technol*ogy, vol. 23, no. 4, pp. 1652-1663, April 2005.

[56] D. E. Leaird, Z. Jiang, and A. M. Weiner, "Experimental investigation of security issues OCDMA: a code-switching scheme," *IET Electronics Letters*, vol. 41, no. 14, pp. 817-819, July 2005.

[57] X. Wang, N. Wada, T. Miyazaki, and K. Kitayama, "Coherent OCDMA system using DPSK

data format with balanced detection," *IEEE Photonics Technology Letters*, vol. 18, no. 7, pp. 826-828, April 2006.

[58] X. Wang, N. Wada, T. Miyazaki, G. Cincotti, and K. Kitayama, "Asynchronous multiuser coherent OCDMA system with code-shift-keying and balanced detection," *IEEE Joulnal of Selected Topics in Quantum Electronics*, vol. 13, no. 5, pp. 1463-1470, September 2007.

[59] G. Manzacca, X. Wang, N. Wada, G. Cincotti, and K. Kitayama, "Comparative study of multiencoding schemes for OCDM using a single multiport optical encoder/decoder," *IEEE Photonics Technology Letters*, vol. 19, no. 8, pp. 559-561, April 2007.

[60] X. Wang, N. Wada, G. Manzacca, T. Miyazaki, G. Cincotti, and K. Kitayama, "Demonstration of 8 x 10.7 Gbps asynchronous code-shift keying OCDMA with multi-port en/decoder for multidimensional optical code processing," in *Proc. European Cnference of Optical Communication (ECOC2006)*, Th3.6.5, Cannes, France, September 2006.

[61] E. Narimanov and B. Wu, "Advanced coding techniques for asynchronous fiber-optical CDMA," in *Proc. Conference on Lasers and Electro-Optics and The Quantum Electronics and Laser Science Conference (CLEO/QELS 2005)*, JThE70, Baltimore, MD, USA, May 2005.

[62] S. Galli, R. Menendez, R. Fischer, and R. J. Runser, "A novel method for increasing the spectral eficiency of optical CDMA," in *Proc. IEEE Global Telecommunications Conference (GLOBECOM 2005)*, vol. 4, pp. 2009-2013, St. Louis, USA, November 2005.

[63] C. S. Bres, I. Glesk, R. J. Runser, T. Banwell, P. R. Prucnal, and W. C. Kwong, "Nobel M-ary architecture for optical CDMA using pulse position modulation," in *Proc. Lasers and Electro-Optics Society (LEOS 2005)*, ThBB1, Sydney, Australia, October 2005.

[64] R. Menendez, A. Agarwal, P. Toliver, J. Jackel, and S. Etemad, "Direct optical processing of M-ary code-shift keyed spectral phase encoded OCDMA," *Journal of Optical Networking*, vol. 6, no. 5, pp. 442-450, May 2007.

[65] A. J. Menezes, P. C. V. Oorschot, S. A. Vanstone "Handbook of Applied Cryptography," August 2001.

[66] G. Cincotti, "Design of optical full encoders/decoders for code-based photonic routers," *IEEE/OSA Journal of Lightwave Technol*ogy, vol. 22, no. 7, pp. 1642-1650, July 2004.

[67] G. Cincotti, N. Wada, and K. Kitayama, "Characterization of a full encoder/decoder in the AWG configuration for code-based photonic routers-part I: modeling and design," *IEEE/OSA Journal of Lightwave Technol*ogy, vol. 24, no. 1, pp. 103-112, January 2006.

[68] N. Wada, G. Cincotti, S. Yoshima, N. Kataoka, and K. Kitayama, "Characterization of a full encoder/decoder in the AWG configuration for code-based photonic routers-part II: experiments and applications," *IEEE/OSA Journal of Lightwave Technol*ogy, vol. 24, no. 1, pp.

113-121, January 2006.

[69] G. Cincotti, G. Manzacca, V. Sacchieri, X. Wang, N. Wada, and K. Kitayama, "Secure OCDM transmission using a planar multiport encoder/decoder," *IEEE/OSA Journal of Lightwave Technol*ogy, vol. 26, no. 13, pp. 1798-1806, July 2008.

[70] W. C. Perrier, P. A. Perrier, P. R. Prucnal, "Performance comparison of asynchronous and synchronous code-division multiple-access techniques for fiber-optic local area networks," *IEEE Transactions on Communications*, vol. 39, no. 10, pp1625-1634, November 1991.

[71] F. Xue, Y. Du, S. J. Yoo, and Z. Ding, "Security issues on spectral-phase-encoded optical CDMA with phase-masking scheme," in *Proc. IEEE/OSA Optical Fiber Communication Conference and the National Fiber Optic Engineers Conference (OFC/NFOEC 2006)*, OTht3, Anaheim, CA, March 2006.

[72] G. Cincotti, N. Wada, and K. Kitayama, "Secure optical bit- and block-cipher transmission using single multiport encoder/decoder," in *Proc. IEEE/OSA Optical Fiber Communication Conference and the National Fiber Optic Engineers Conference (OFC/NFOEC 2008)*, JThA93, San Diego, CA, February 2008.

[73] G. P. Agrawal, "Nonlinear fiber optics, 3rd ed.," *Academic Press*, San Diego, CA, 2001.

[74] I. Glesk, Y-K. Huang, C.-S. Brès, and P.R. Prucnal, "Improving transmission privacy using optical layer XOR," in *Proc. Conference on Lasers and Electro-Optics and Quantum Electronics and Laser Science Conference (CLEO/QELS 2007)*, CThBB6, Baltimore, MD, USA, May 2007.

[75] I. Glesk, Y-K. Huang, K.S. Kravtsov, and P.R. Prucnal "Increasing optical security with OCDMA using optical XOR," in *Proc. Photonics in Switching (PS 2007)*, WA1.4, San Francisco, CA, USA, August 2007.

[76] N. Nakagawa, N. Kataoka, X. Wang, N. Wada, G. Cincotti, T. Miyazaki, and K. Kitayama, "Experimental demonstration of secure 16-ary, 2.5Gbit/s OCDMA using single multi-port en/decoder," in *Proc. 34th European Conf. Optical Communication (ECOC 2008)*, We.1.F.2, Brussel, Belgium, September 2008.

[77] N. Kataoka, N. Wada, G. Cincotti, K. Kitayama, and T. Miyazaki, "A novel multiplexed optical code label processing with huge number of address entry for scalable optical packet switched network," in *Proc. 33th European Conf. Optical Communication (ECOC 2007)*, Tu.3.2.3, Berlin, Germany, September 2007.

[78] T. Kodama, N. Nakagawa, N. Kataoka, N. Wada, G. Cincotti, X. Wang, T. Miyazaki, and K. Kitayama, "Secure 2.5 Gbit/s, 16-ary OCDM block-ciphering with XOR using a single

multi-port en/decoder," *IEEE/OSA Journal of Lightwave Technology,* vol. 28, no. 1, pp. 181-187, January 2010.

[79] X. Wang, N. Wada, G. Cincotti, T. Miyazaki, and K. Kitayama, "Demonstration of over 128-Gb/s-Capacity (12-Users×10.71-Gb/s/User) Asynchronous OCDMA using FEC and AWG-based multiport optical encoder/decoders," *IEEE Photonics Technology Letters*, vol. 18, no. 15, pp. 1603-1605, August 2006.

[80] N. Kataoka, N. Wada, X. Wang, G. Cincotti, T. Miyazaki, and K. Kitayama, "Full duplex demonstration of asynchronous, 10Gbps x 4-user DPSK-OCDMA system using hybrid multi-port and SSFBG en/decoder," in *Proc. 34th European Conference Optical Communication (ECOC 2008)*, P.6.06, Brussels Expo, Belgium, September 2008.

[81] N. Kataoka, N. Wada, X. Wang, G. Cincotti, and K. Kitayama, "Demonstration of 10Gbps, 4-user, OCDMA transmission over 59km single mode fiber without inline dispersion compensation," in *Proc. IEEE/OSA Optical Fiber Communication Conference and the National Fiber Optic Engineers Conference (OFC/NFOEC 2010)*, OThW1, San Diego, CA, USA, March 2010.

[82] Y. Hida, Y. Hibino, T. Kitoh, Y. Inoue, M. Itoh, T. Shibata, A. Suguta, and A. Himeno, "400-channel 25-GHz spacing arrayed-waveguide grating covering a full range of C-band and L-bands," in *Proc. IEEE/OSA Optical Fiber Communication Conference and the National Fiber Optic Engineers Conference (OFC/NFOEC 2001)*, WB2, Anaheim, CA, USA, March 2001.

# List of Publications

## I. Journals

1. Takahiro Kodama, Naoki Nakagawa, Nobuyuki Kataoka, Naoya Wada, Gabriella Cincotti, Xu Wang, Tetsuya Miyazaki, and Ken-ichi Kitayama, "Secure 2.5Gbit/s, 16-ary OCDM block-ciphering with XOR using a single multi-port en/decoder," *IEEE/OSA Journal of Lightwave Technology,* vol. 28, no. 1, pp. 181-187, January, 2010.
2. Takahiro Kodama, Nobuyuki Kataoka, Naoya Wada, Gabriella Cincotti, Xu Wang, Tetsuya Miyazaki, and Ken-ichi Kitayama, "High-security 2.5Gbit/s, polarization multiplexed 256-ary OCDM using a single multi-port encoder/decoder," *Optics Express,* vol. 18, no. 20, pp. 21376-21385, September 2010.
3. Takahiro Kodama, Nobuyuki Kataoka, Naoya Wada, Gabriella Cincotti, Xu Wang, and Ken-ichi Kitayama, "4096-ary OCDM/OCDMA system using multidimensional PSK codes generated by a single multiport en/decoder," *IEEE/OSA Journal of Lightwave Technology,* vol. 29, no. 22, pp. 3372-3380, November 2011.

## II. International Conferences

1. Takahiro Kodama, Naoki Nakagawa, Nobuyuki Kataoka, Naoya Wada, Gabriella Cincotti, Xu Wang, Tetsuya Miyazaki, and Ken-ichi Kitayama, "Secure 2.5Gbit/s, 16-ary OCDM block-ciphering with XOR using a single multi-port en/decoder and its transmission experiment with true clock recovery," *Proc. Optical Fiber Communication Conference and*

*Explosion National Fiber Optic Engineers Conference (OFC/NFOEC 2009),* OThI3, San-Diego, CA, USA, March 2009 (refereed).

2. Ken-ichi Kitayama, Takahiro Kodama, Nobuyuki Kataoka, Naoya Wada, Xu Wang, and Gabriella Cincotti, "High-security M-ary OCDM block-ciphering: Its en/decoding, transmission, and access," *Proc. 4th International Workshop on OPS& OCDMA*, Session 4, Tokyo, November 2009.
3. Nobuyuki Kataoka, Takahiro Kodama, Naoya Wada, Gabriella Cincotti, Xu Wang, Tetsuya Miyazaki, and Ken-ichi Kitayama, "Demonstration of secure 2.5Gbps, 256ary polarization-multiplexed OCDM transmission using single multi-port encoder/decoder," *Proc. Conference on Lasers and Electro-Optics and The Quantum Electronics and Laser Science Conference (CLEO/QELS 2009),* CTuJ3, Baltimore, Maryland, USA, June 2009 (refereed).
4. Takahiro Kodama, Nobuyuki Kataoka, Naoya Wada, Gabriella Cincotti, Xu Wang, Tetsuya Miyazaki, and Ken-ichi Kitayama, "Demonstration of 16-ary OCDM block-ciphering transmission using a single multi-port en/decoder and true clock recovery," *Proc. Electronic Devices Innovation (EDIS 2009),* WS3-B2, Toyonaka, Osaka, Japan, December 2009.
5. Takahiro Kodama, Naoki Nakagawa, Nobuyuki Kataoka, Naoya Wada, Gabriella Cincotti, Xu Wang, Tetsuya Miyazaki, and Ken-ichi Kitayama, "Secure optical communication: 2.5 Gbps, 16-ary OCDM using a single multi-port encoder/decoder," *Proc. Student Conference on Innovative Electronic Topics (SCIENT 2010),* Po-31, Suita, Osaka, Japan, July 2010.
6. Takahiro Kodama, Nobuyuki Kataoka, Naoya Wada, Gabriella Cincotti, Xu Wang, Tetsuya Miyazaki, and Ken-ichi Kitayama, "High-security 2.5 Gbit/s, block-ciphering M-ary OCDM system," *Proc. Updating Quantum Cryptography and Communications (UQCC 2010),* 139, Minato-ku, Tokyo, Japan, November 2010.
7. Takahiro Kodama, Nobuyuki Kataoka, Naoya Wada, Gabriella Cincotti, Xu Wang, and Ken-ichi Kitayama, "4096-ary OCDM at 2.5 Gbit/s using multidimensional PSK codes with a single multi-port encoder/decoder," *Proc. Optical Fiber Communication Conference and Explosion National Fiber Optic Engineers Conference (OFC/NFOEC 2011),* JWA038, Los Angeles, CA, USA, March 2011 (refereed).
8. Takahiro Kodama, Ken-ichi Kitayama, Nobuyuki Kataoka, Naoya Wada, Gabriella Cincotti, and Xu Wang, "Physical level secure optical communication: M-ary OCDM

using multidimensional PSK codes," *Proc. Electronic Devices Innovation (EDIS 2011),* P-12, Toyonaka, Osaka, Japan, December 2011.

# III. Domestic Conferences

1. Takahiro Kodama, Naoki Nakagawa, Nobuyuki Kataoka, Naoya Wada, Gabriella Cincotti, Xu Wang, Tetsuya Miyazaki, and Ken-ichi Kitayama, "Secure M-ary OCDM block-ciphering using a single multi-port en/decoder," in *IEICE Technical Report*, vol. 108, no. 476, PN2008-95, pp. 65-69, Yonaguni-jima, Okinawa, Japan, March 2009 (in Japanese).
2. Takahiro Kodama, Naoki Nakagawa, Nobuyuki Kataoka, Naoya Wada, Gabriella Cincotti, Xu Wang, Tetsuya Miyazaki, and Ken-ichi Kitayama, "Transmission experiment of secure 16-ary OCDM using a single multi-port en/decoder," in *Proc. IEICE General Conference*, B-10-58, Matsuyama, Ehime, Japan, March 2009 (in Japanese).
3. Takahiro Kodama, Naoki Nakagawa, Nobuyuki Kataoka, Naoya Wada, Gabriella Cincotti, Xu Wang, Tetsuya Miyazaki, and Ken-ichi Kitayama, "Secure M-ary OCDM transmission system: results of transmission experiment and study of high performance," in *IEICE Technical Report*, vol. 109, no. 154, OCS2009-19, pp. 1-6, Yugawara, Shizuoka, Japan, July 2009 (in Japanese).
4. Takahiro Kodama, Nobuyuki Kataoka, Naoya Wada, Gabriella Cincotti, Xu Wang, and Ken-ichi Kitayama, "4096-ary OCDM system using multidimensional PSK optical codes with a single multi-port en/decoder," in *IEICE Technical Report*, vol. 110, no. 431, PN2010-77, pp. 103-107, Kagoshima, Kagoshima, Japan, March 2011 (in Japanese).
5. Takahiro Kodama, Nobuyuki Kataoka, Naoya Wada, Gabriella Cincotti, Xu Wang, and Ken-ichi Kitayama, "High security M-ary OCDMA system: principle demonstration and analysis of performance," in *IEICE Technical Report*, vol. 111, no. 297, OCS2011-98, pp. 33-38, Matsue, Shimane, Japan, November 2011 (in Japanese).