High-security 2.5 Gbps, polarization multiplexed 256-ary OCDM using a single multi-port encoder/decoder

Takahiro Kodama,[1,*] Nobuyuki Kataoka,[2] Naoya Wada,[2] Gabriella Cincotti,[3] Xu Wang,[4] Tetsuya Miyazaki,[2] and Ken-ichi Kitayama[1]

[1]*Department of Electrical Electronic, and Information Engineering, Osaka University, 565-0871 Osaka, Japan*
[2]*Ultrafast Photonic Network Group, National Institute of Information and Communication Technology, 184-8795 Tokyo, Japan*
[3]*Department of Applied Electronics, University Roma Tre, via della Vasca Navale 84, I-00146 Rome, Italy*
[4]*School of Engineering and Physical Sciences, Heriot-Watt University, Riccarton, EH14 4AS, Edinburgh, U. K.*
**kodama@pn.comm.eng.osaka-u.ac.jp*

Abstract: A block-ciphered (M-ary) optical code division multiplexing (OCDM) can provide larger security than a conventional OCDM system based on bit ciphering. We propose a polarization multiplexed (POL-MUX) M-ary OCDM system and demonstrated 2.5 Gbps, POL-MUX 256 (= 16X16)-ary OCDM transmission using a single multi-port optical encoder/decoder (E/D). We show that this architecture reduces the number of required optical codes and enhances the system confidentiality.

OCIS codes: (060.4230) Multiplexing; (060.4510) Optical communications; (060.4785) Optical security and encryption; (080.1238) Array waveguide devices.

References and links

1. 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 Photon. Technol. Lett. **19**(8), 559–561 (2007).
2. 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," *ECOC2006*, 2006.
3. T. H. Shake, "Security performance of optical CDMA against eavesdropping," J. Lightwave Technol. **23**(2), 655–670 (2005).
4. T. H. Shake, "Confidentiality performance of spectral-phase-encoded optical CDMA," J. Lightwave Technol. **23**(4), 1652–1663 (2005).
5. D. E. Leaird, Z. Jiang, and A. M. Weiner, "Experimental investigation of security issues OCDMA: a code-swiching sheme," Electron. Lett. **41**(14), 817–819 (2005).
6. X. Wang, N. Wada, T. Miyazaki, G. Cincotti, and K. Kitayama, "Asynchronous Multiuser Coherent OCDMA System With Code-Shift-Keying and Balanced Detection," IEEE J. Sel. Top. Quantum Electron. **13**(5), 1463–1470 (2007).
7. G. Cincotti, N. Wada, and K. Kitayama, "Secure optical bit- and block-cipher transmission using a single multiport encoder/decoder," *in Proc. Optical Fiber Communication Conference and National Fiber Optic Engineers Conference (OFC/NFOFC 2008)*, JThA93, 2008.
8. E. Narimanov, and B. Wu, "Advanced Coding Techniques for Asynchronous Fiber-Optical CDMA," *2005 Quantum Electronics and Laser Science Conference (QELS)*., JThE70, 2005.
9. S. Galli, R. Menendez, R. Fischer, and R. J. Runser, "A Novel Method for Increasing the Spectral Eficiency of Optical CDMA," IEEE Globecom. **4**, 2009–2013 (2005).
10. R. Menendez, A. Agarwal, P. Toliver, J. Jackel, and S. Etemad, "Direct optical processing of M-ary code-shift keyed spectral phase encoded OCDMA," J. Optical Netw. **6**(5 Issue 5), 442–450 (2007).
11. T. Kodama, N. Nakagawa, N. Kataoka, N. Wada, G. Cincotti, X. Wang, T. Miyazaki, and K. Kitayama, "Secure 2.5Gbit/s,16-ary OCDM block-ciphering with XOR using a single multi-port en/decoder," J. Lightwave Technol. **28**(1), 181–187 (2010).
12. N. Kataoka, T. Kodama, N. Wada, G. Cincotti, X. Wang, T. Miyazaki, and K. Kitayama, "Demonstration of Secure 2.5Gbps, 256ary Polarization-Multiplexed OCDM transmission using Single Multi-port Encoder/Decoder," *Proc. CLEO 2009, CTuJ3*, Baltimore, Maryland, USA, Jun. 2009.
13. 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," J. Lightwave Technol. **24**(1), 103–112 (2006).

#128889 - $15.00 USD Received 26 May 2010; revised 9 Jul 2010; accepted 26 Aug 2010; published 23 Sep 2010

1. Introduction

Time division multiplexing (TDM) uses a time slot as a communication channel, while, wavelength division multiplexing (WDM) uses a wavelength. On the other hand, optical code division multiplexing (OCDM) is based on spectrally or time-domain encoded waveforms. One of the main advantages of OCDM systems is their intrinsic data confidentiality, because messages are encoded at the transmitter and can be recovered only by an authorized user, who knows the optical code (OC). On-off keying (OOK)-differential-phase-shift-keying (DPSK)-modulated and code-shift-keying (CSK)-OCDM systems have been investigated and experimentally demonstrated during the past decade [1,2]. 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 security by simple data-rate power detection without any information about the OC [3–5]. In DPSK-modulated OCDM architectures, an eavesdropper could decipher the transmitted data, without any knowledge about the OC, using a commercial DPSK decoder and a data-rate power detector [6]. On the other hand, in CSK-modulated OCDM transmission, an eavesdropper that 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 [7]. A more secure encoding method is the block-ciphering approach, that transforms a sequence of $\log_2 M$ bits into an OC [8,9]. Block-ciphering is also known as M-ary OCDM and the corresponding operation principle is shown in Fig. 1(a), in this case a set of M codewords is assigned to each user, and different sequences of $\log_2 M$ bits of a message are mapped onto different OCs [10]. This scheme presents two levels of confidentiality: physical-layer security, because an adversary should be able to correctly detect the OC, and computational security, since he or she does not know which sequence of bits corresponds to a given OC, and the number of possible combinations equates M!. Recently, 2.5Gbit/s, 16-ary OCDM transmission over a 50 km link has been experimentally demonstrated, using a single multi-port arrayed waveguide grating (AWG)-based E/D, that can simultaneously generate and decode as many codes as the number of its ports [11]. However, the number of OCs is limited by the port count, and it would be desirable

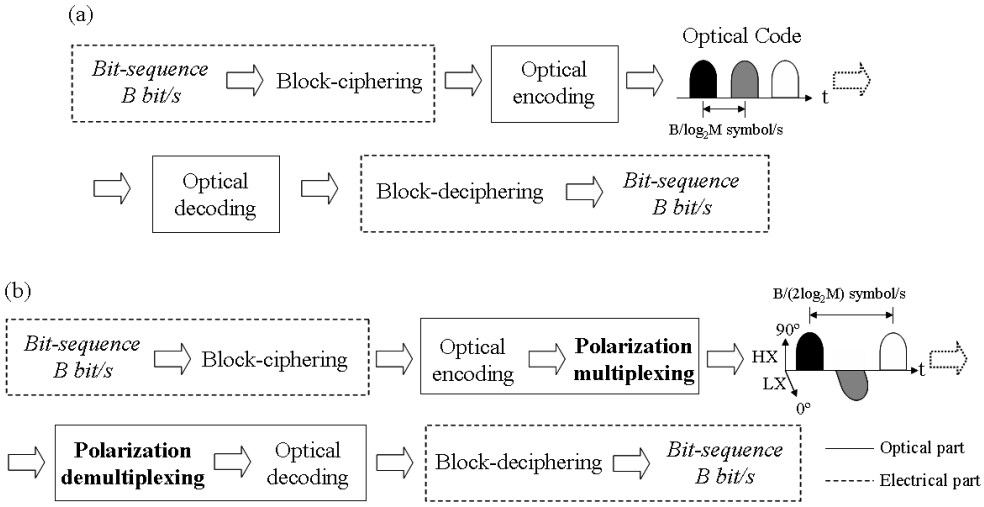

Fig. 1. Scheme of M-ary OCDM (a) Conventional system (b) Polarization multiplexed system.

if the M-ary number can be increased without increasing the number of OCs. To overcome this limitation, more recently we have proposed a novel POL-MUX M-ary OCDM system that is shown Fig. 1(b) and largely reduces the number of codes needed [12]. In the present paper, we demonstrate a POL-MUX 2.5 Gbps, 32 (= 16 + 16)-ary OCDM transmission using 16

#128889 - $15.00 USD Received 26 May 2010; revised 9 Jul 2010; accepted 26 Aug 2010; published 23 Sep 2010

OCs generated by a multi-port optical E/D, we remark that in a conventional M-ary system, the number of OCs requested would be 256, that is beyond the capability of the current OCDM technology. We also discuss and analyze the corresponding data security in terms of data confidentiality against cipher-text only attack (COA) and chosen plaintext attacks (CPA), and show that POL-MUX OCDM doubles the spectral efficiency and enhances the data confidentiality.

2. System architecture and operation principle

Figure 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 bit/s is segmented every 8 bits by a serial-to-parallel (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 1. We remark that the segmentation in the

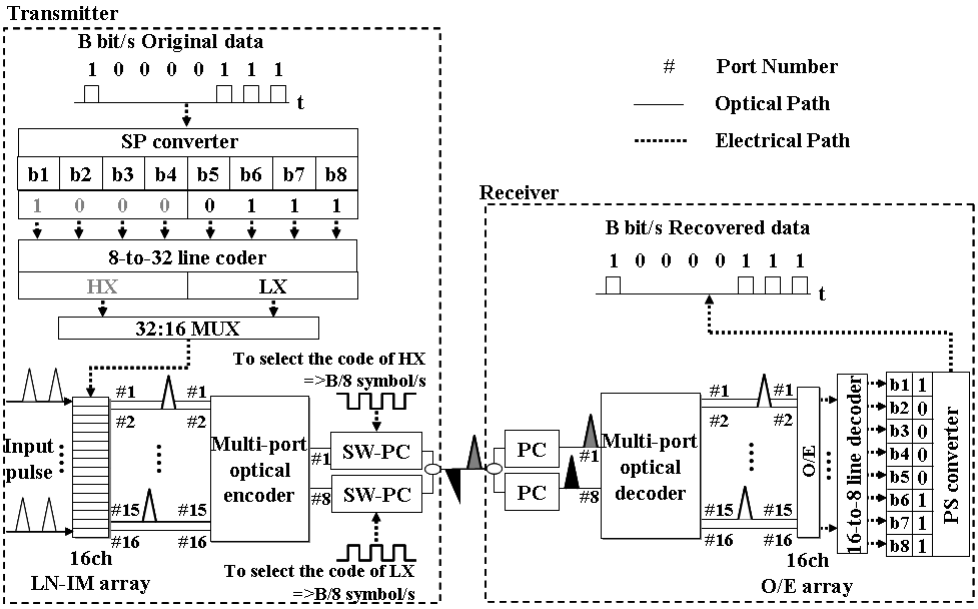

Fig. 2. Architecture of polarization-multiplexed 256-ary OCDM system.

Table 1. Code Lookup Table

	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

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.

#128889 - $15.00 USD Received 26 May 2010; revised 9 Jul 2010; accepted 26 Aug 2010; published 23 Sep 2010

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 $LiNbO_3$ intensity modulator (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 multiport E/D. Therefore, the transmission system of Fig. 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), because in this case we can avoid expensive time-gating devices.

In the optical domain, the optical seed pulses at B/4 bit/s 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 [13]. 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 C2 and C15 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 switch (SW) at this two outputs selects the HX and LX codes and the polarization controller (PC) rotates their polarization of 90° and 0°, 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 unequivocally 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) array, and it is launched into the 16-to-8 line decoder, so that the original 8 bit data sequence is recovered via the parallel-to-serial (PS) converter, using the same code lookup table (Table 1).

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, maximum interface frequency: 622.08 MHz).

3. Experimental results

Figure 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 Gbit/s 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. 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 super continuum (SC) light source, which consists 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 (iii). The spectrum of the SC signal is shown in inset (iv). The SC signal is fed into an optical

#128889 - $15.00 USD Received 26 May 2010; revised 9 Jul 2010; accepted 26 Aug 2010; published 23 Sep 2010

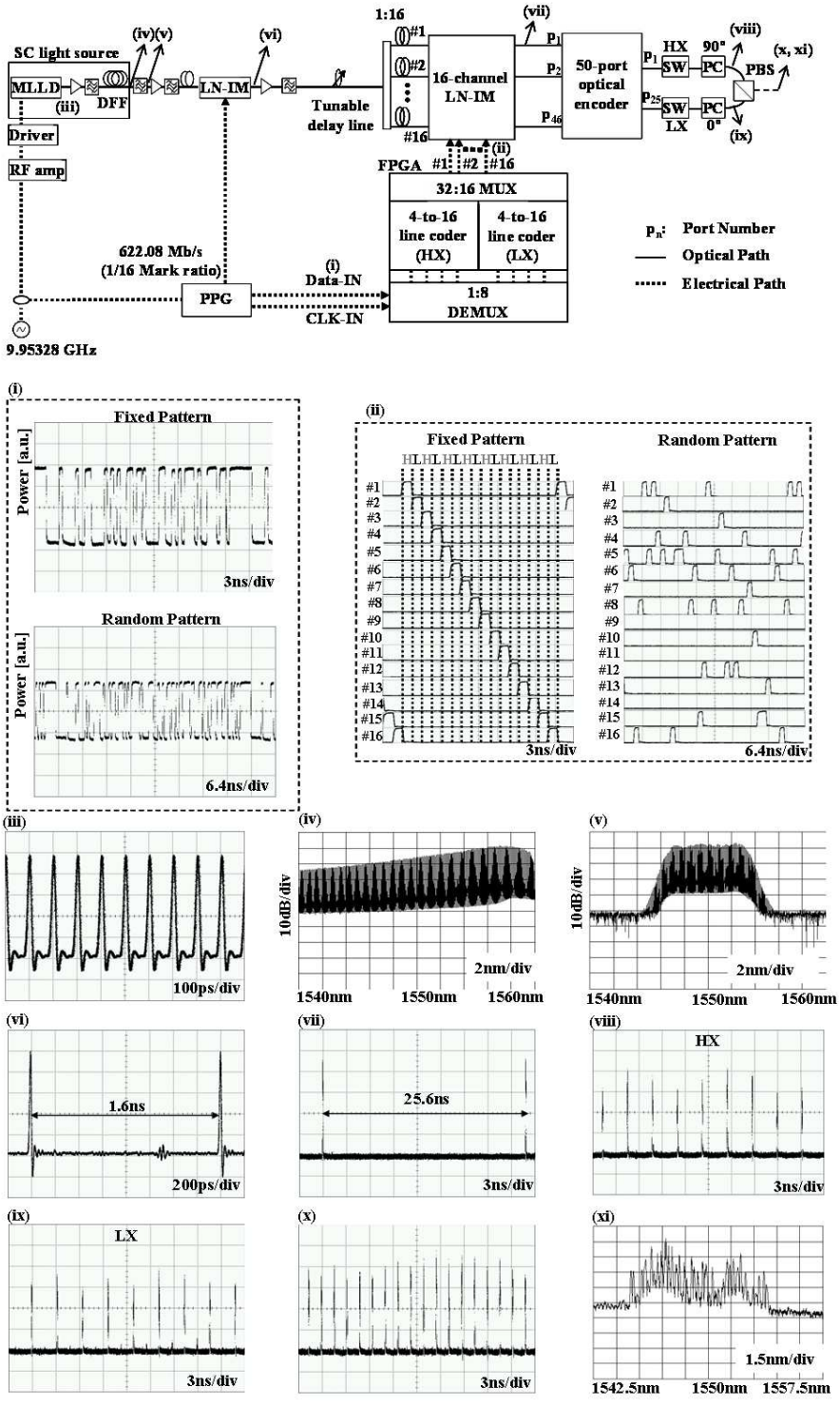

Fig. 3. Experimental setup of polarization-multiplexed 256-ary OCDM transmission system.

band-pass filter (OBPF) with 7.5 nm bandwidth at the center wavelength of 1550 nm (as shown in inset (v)). The pulse streams generated by the pulse pattern generator (PPG) are

#128889 - $15.00 USD Received 26 May 2010; revised 9 Jul 2010; accepted 26 Aug 2010; published 23 Sep 2010

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. 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 ($p_i = 1 + 3i$ (i = 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. 3. The PC rotates their polarization of 90° and 0°, 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.

Figure 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 lines by a 10 dB coupler. The main line (90%-branch) and sub line (10%-branch) are directed to the optical decoder and clock recovery (CR) circuit, respectively. The inset (i) in Fig. 4 shows the recovery clock extracted from the 256-ary OCDM signal using the CR circuit. In the main line, 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 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 (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 Gbit/s serial data sequence by the PS converter. Inset (vi) in Figs. 4 show the waveform of the recovered serial data in case of the fixed and random patterns, respectively.

We measured the bit error rate (BER) of the received data, that are reported in Fig. 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.

#128889 - $15.00 USD Received 26 May 2010; revised 9 Jul 2010; accepted 26 Aug 2010; published 23 Sep 2010

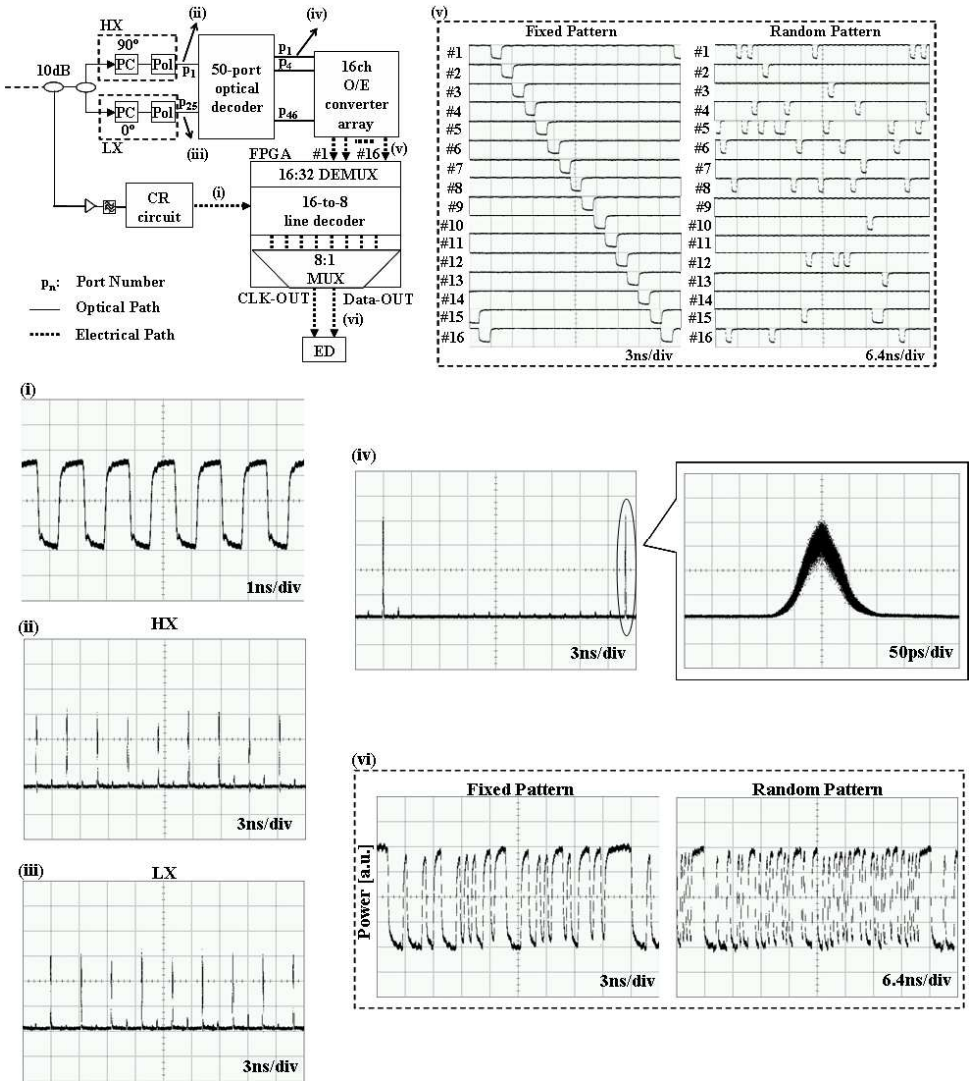

Fig. 4. Experimental setup of polarization-multiplexed 256-ary OCDM receiver system.

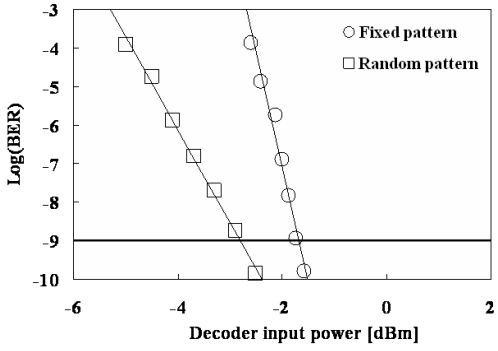

Fig. 5. Measured BERs in case of the fixed and random patterns.

#128889 - $15.00 USD Received 26 May 2010; revised 9 Jul 2010; accepted 26 Aug 2010; published 23 Sep 2010

4. Security 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 requested, 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 √M, and we have demonstrated a 256 (= 16X16)-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, with respect to conventional OCDM.

1) reduced complexity of the electrical block-ciphering components;

2) the code rate at each polarization state is reduced and therefore fast response receivers are not required;

3) the spectral efficiency is doubled;

4) the data confidentiality is enhanced;

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 an exhaustive key search attack, or brute force attack, that is the simplest COA attack; in this case, the eavesdropper is able to intercept only the cipher-text, i.e. the OCs, and to break the system security, an eavesdropper has to determine the correspondence between the OC and the sequence of m bits. 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 [7]. In a POL-MUX OCDM, only √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

#128889 - $15.00 USD Received 26 May 2010; revised 9 Jul 2010; accepted 26 Aug 2010; published 23 Sep 2010

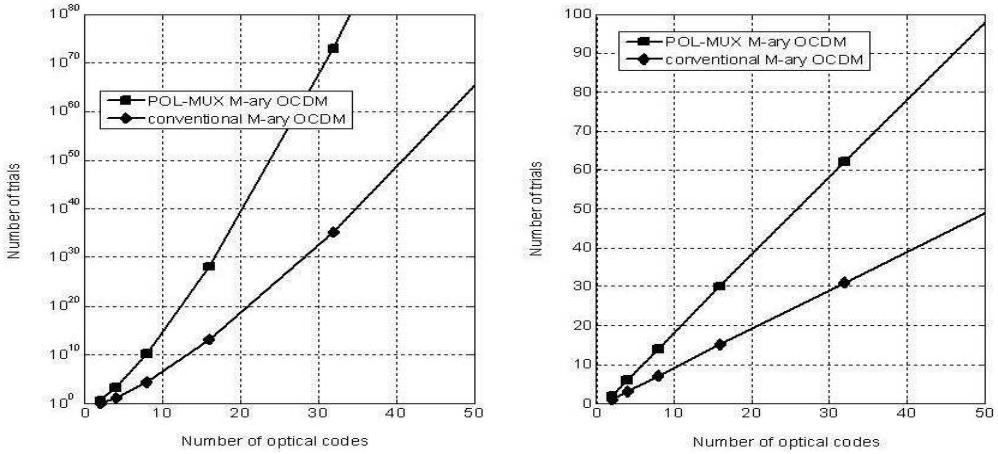

Fig. 6. (a) Number of trials to break the confidentiality with a COA (b) Number of trials necessary to break the confidentiality with a CPA.

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. Later, 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 $\cdot(\sqrt{M})!*(\sqrt{M})!$. 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. 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: this attack assumes that the eavesdropper has the capability to choose arbitrary plaintexts to be encrypted to obtain the corresponding ciphertexts, i.e. the OCs. 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 30 in our case. Figure 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,

#128889 - $15.00 USD Received 26 May 2010; revised 9 Jul 2010; accepted 26 Aug 2010; published 23 Sep 2010

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.

5. Conclusion

In this paper, we propose a novel M-ary OCDM system using polarization multiplexing technique and a single multi-port optical en/decoder. 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 2.5Gbps, 256-ary POL-MUX OCDM system using a single multi-port en/decoder and analyzed the corresponding security.

Acknowledgement

The authors would like to thank Y. Tomiyama and H. Sumimoto of the National Institute of Information and Communications Technology (NICT) for their supports in the experiment. The authors would also like to thank H. Fujinuma of NTT Electronics Corporation (NEL) for his cooperation in the experiment. X. Wang acknowledges the support of Royal Society International Joint Project. The work described in this paper was carried out with the support of the BONE-project ("Building the Future Optical Network in Europe"), a Network of Excellence funded by the European Commission through the 7th ICT-Framework Program. The authors are thankful to an anonymous Reviewer, whose comments have enhanced the technical quality of the paper.

#128889 - $15.00 USD Received 26 May 2010; revised 9 Jul 2010; accepted 26 Aug 2010; published 23 Sep 2010