DPSK optical code hopping scheme using single phase modulator for secure optical communication

Xu Wang*[1], *Senior Member, IEEE,* Zhensen Gao[1], Nobuyuki Kataoka[2] and Naoya Wada[2]

1Joint Research Institute for Integrated Systems, Sch. of Engineering and Physical Sciences, Heriot-Watt University, Riccarton, Edinburgh, EH14 4AS, UK,
2Photonic Network Group, New Generation Network Research Center, National Institute of Information and Communications Technology (NICT), 4-2-1, Nukui-Kitamachi, Koganei-shi, Tokyo 184-8795, Japan,
** Tel: (44) 131 451 3775, Fax: (44)131 451 , e-mail: X. Wang@hw.ac.uk*

ABSTRACT

A novel bit-by-bit code hopping scheme using single phase modulator is proposed and demonstrated for secure optical communication application. In the experiment, 2.5Gbps DPSK data has been generated and securely transmitted over 34km by scrambling five 8-chip, 20Gchip/s Gold codes with prime-hop patterns.

Keywords: Fiber optics and optical communications, Phase modulation, Encoding/decoding, Optical code division multiple access, Secure optical communication.

1. INTRODUCTION

Optical code (OC) generation and recognition are the key techniques in future photonic network such as optical-code-division-multiple-access (OCDMA), optical packet switching (OPS) and optical burst switching (OBS) [1-3]. In a typical OCDMA system, all the users can share the same transmission media (time, wavelength) but each of them is assigned a unique optical code. At the receiver, different users are discriminated by its corresponding optical code [4-5]. Due to the all-optical processing of optical code generation and recognition, the OCDMA exhibits the unique features of allowing fully asynchronous transmission without the requirement of complex and expensive electronic equipment, low-latency access which is desirable for burst traffic environment and so on [6-7]. Among the other potential advantages of OCDMA, the information security in the physical layer is generally considered as an inherent benefit of OCDMA system [5, 8-9] owing to the optical code based encoding that makes the OCDMA encoded signal manifest itself as a noise-like waveform, so the eavesdropper can not intercept the data without knowledge of the applied code.

However, *Shake* [10-11] pointed out that a simple power detector can easily break the data confidentiality for single user OCDMA system employing on-off keying (OOK) modulation format. *Jiang* [12] experimentally demonstrated the vulnerability of a spectrally phase encoded OOK OCDMA system. Various approaches have been proposed to overcome the vulnerabilities in single user OCDMA system. Among them, advanced modulation formats have been adopted in OCDMA system to address this issue. In [13], the differential-phase-shift-keying (DPSK) data modulation format and balanced detection have been proposed to combat the noise as well as enhancing the security. However, the eavesdropper can still decipher the data using a common DPSK demodulator without any information of the code for the DSPK-OCDMA. A code switching data modulation format for enhancing the security was investigated in [14]. In this scheme, bit '1' and '0' are encoded into two noise-like waveforms with equal energy according to two different codes, so it can eliminate the vulnerability of eavesdropping based on a simple power detector. However, as *Jiang* demonstrated later [15-16], a simple DPSK demodulator can also be used to recover the data from the code switching scheme because the interference of the adjacent bit with identical coded waveform generate high level output while the interference is nearly zero if the adjacent bits are from different codes. He also investigated another kind of vulnerability arising from coding induced spectral dips in the spectral phase encoded OCDMA system that will allow the eavesdropper to extract the code by analyzing the fine structure of the spectra [15]. It has been suggested that the data confidentiality could be significantly improved in an OCDMA system by rapidly reconfiguring the optical codes [10-11], but this concept has not been demonstrated yet because the conventional optical coding schemes do not have the fast reconfigurable capability.

Recently, we proposed a novel time domain spectral phase en/decoding (SPED) scheme, utilizing two opposite dispersive fibers and a high speed phase modulator for OCDMA application [17]. This scheme is very flexible in reconfiguring the optical codes and compatible with the fiber optical system. It is also very robust to the wavelength drift of the laser source. By using a linearly chirped fiber Bragg grating (LCFBG) to serve as the dispersive device, this system is more compact, stable and has lower latency [18]. Moreover, it exhibits the potential to perform the optical code generation and DPSK data modulation simultaneously using single phase modulator [19].

In this paper, we propose and experimentally demonstrate a novel bit-by-bit code scrambling technique based on our proposed time domain spectral phase en/decoding scheme for secure optical communication.

2. EXPERIMENT

The experimental setup of the proposed bit-by-bit code scrambling and DPSK data modulation scheme is illustrated in Figure 1. At the transmitter, a super-continuum (SC) light source is employed for broadening the spectrum, which is composed of mode-locked laser diode (MLLD), an erbium-doped fiber amplifier (EDFA), and a piece of 2km dispersion- flattened-fiber (DFF). The mode-locked laser diode (MLLD) produces nearly transform- limited ~4ps (FWHM) Gaussian-like pulses with a repetition rate of 10GHz, spectrally centers at 1550.28nm. The source repetition rate is down converted to 2.5GHz by using a Mach-Zehnder intensity modulator (IM) and pulse pattern generator (PPG). The whole setup includes two main sections: bit-by-bit spectral phase encoding using the mixed DPSK data and scrambled code hopping sequence, and bit-by-bit code

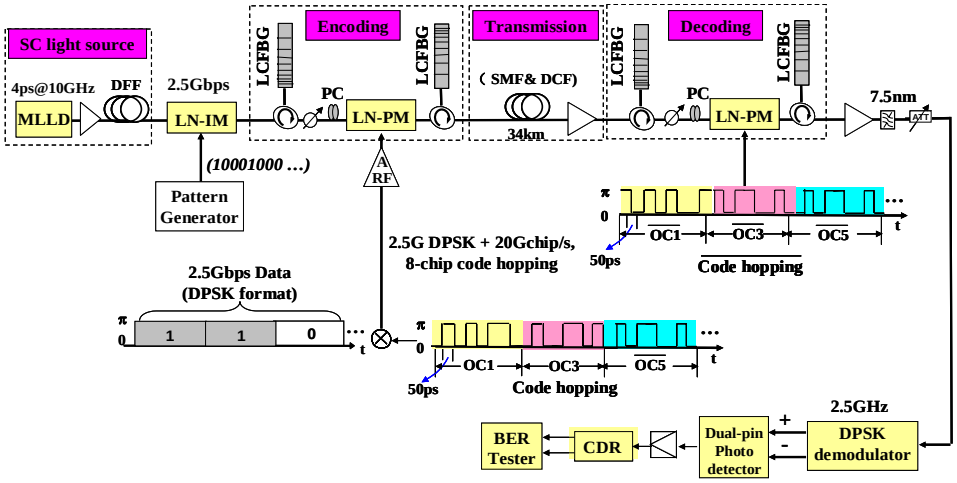

Fig.1 Experimental setup of bit-by-bit code scrambling based on time domain SPE/SPD scheme

recognition using only the complementary code hopping sequence. In the encoding section, a LCFBG with 3dB bandwidth of ~4.5nm and dispersion slope of about -80ps/nm is used to stretch the 2.5GHz optical pulse into 360ps time duration for one bit. In the experiment, the LCFBG functions not only as a dispersive device but also as an optical band-pass filter (BPF) to cutoff the residual input spectrum to avoid the overlap between two adjacent stretched pulses, since obvious overlap will degrade the decoding and transmission performance [18]. Different spectral components spread into different position in time domain. The dispersed pulse is then temporally modulated by a phase modulator driven by the combination of 2.5Gbps DPSK data and scrambled code hopping sequence, which contains five 8-chip, 20Gchip/s(corresponding to 8-chip, 78GHz/chip spectral code pattern) Gold codes with 7 chips plus a zero. The five Gold codes are: OC1: 10010110, OC2:11100010, OC3:10101010, OC4:10101100 and OC5:00001010, respectively. The correlation property of the Gold codes is of vital importance to guarantee the security of the proposed code scrambling scheme, because the eavesdropper can still decipher the DPSK data using a wrong code hopping sequence if the cross-correlation is rather high.

Figure 2 shows the procedure to combine the DPSK data with the code hopping sequence bit-by-bit. First, the DPSK data stream is segmented every five bits into a group and mapped onto an existing prime-hop code pattern H1~H4. i.e. the first five bits (11001…) are mapped onto H2 (OC1, OC3, OC5, OC2, OC4). Each Gold code (OC) in the prime-hop code pattern corresponds to one bit in the DPSK data stream. Then, each DPSK data is mixed with its corresponding OC to drive the PM: when the DPSK data is symbol "1", the PM is driven by OC, while if symbol is "0", the PM is driven by $\overline{OC}$, therefore, the first five bits are driven by OC1, OC3, OC5, $\overline{OC2}$, $\overline{OC4}$ as is shown in Fig.2 (a). The following grouped DPSK data are also driven by corresponding prime-hop code pattern according to a look-up table (i.e. H2, H4, H3, H1, H4, H3, H1, H2…) which is very easy to reconfigure as is shown in Fig. 2 (c). To accurately synchronize the phase code and the stretched pulse, we

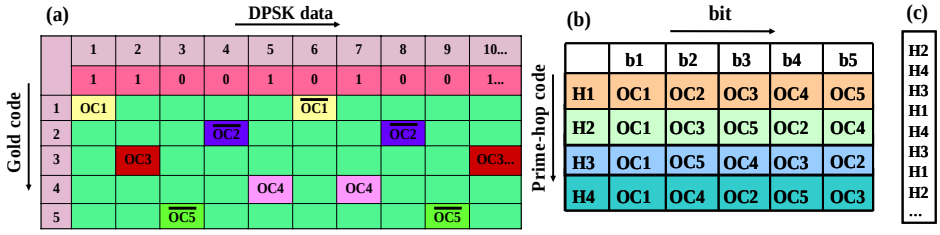

Fig.2 (a) DPSK data and corresponding Gold code; (b) Prime-hop code patterns and (c) Look-up table of prime-hop code pattern

employ an optical delay line before the phase modulator so the code hopping patterns can precisely modulate the phase of the corresponding spectral component for each stretched pulse. After that, another LCFBG with opposite dispersion is used to compress the stretched and phase modulated pulse trains to generate the time domain code hopping sequence encoded SPE signal. A span of single mode fiber (SMF) and dispersion compensation fiber (DCF) with total length of 34km and residual dispersion of ~20ps/nm are used for transmission.

In the decoding section, the identical configuration as the encoding part is used but the PM is driven by the complementary code hopping sequence with all the Gold codes become $\overline{OC}$ (i.e. $\overline{OC1}$, $\overline{OC3}$, $\overline{OC5}$, $\overline{OC2}$, $\overline{OC4}$…). The correctly decoded signal is launched into a 2.5GHz DPSK demodulator followed by a balanced detector to extract the original DPSK data. It is worth noting that the requirement of synchronization between the encoding and decoding stage is very strict in our experiment, making it very difficult for an eavesdropper to correctly decode and recover the DPSK data without accurate chip-level time coordination even if he knows all the code hopping sequences. The security of our system relies on both the optical codes (physical layer security) and the prime-hop pattern look-up table (electrical layer security). An eavesdropper that is able to sift the code hopping sequence encoded signal firstly has to know the number of Gold codes taken from the code space, then he needs to know the correspondence of the Gold codes with the prime-hop code pattern (i.e.H2: OC1, OC3, OC5, OC2, OC4) as well as the scrambling prime-hop code look-up table (i.e. H2, H4, H3, H1, H4, H3…), and eventually he should correctly decode the code hopping sequence. Thus, the proposed bit-by-bit code scrambling scheme can provides higher degree of security and has the potential to realize even one time pad.

3. RESULTS AND DISCUSSION

We have tried four different code hopping sequences for 2^7-1 pseudo random bit sequence (PRBS) DPSK data in the experiment:CH1~CH4. An auto-correlation high peak pulse stream will be generated if the code hopping sequence for decoding matches with that in the encoding, and the two code hopping sequences are accurately synchronized by adjusting the optical delay line before the PM, otherwise a cross-correlation low peak power signal will be produced. Figure 3 (a) shows the correctly decoded optical waveform which exhibit clear eye opening. The electrical pattern and corresponding eye diagram are shown in Fig.3 (b) and (c), respectively. Correct pattern (010010000100…) and clear eye opening of the DPSK data are obtained as expected. The dense sidelobes in the decoded optical waveform and the asymmetry of the two DPSK eye diagrams can be attributed to the different decoding performance of the five Gold codes. For comparison, the decoded optical waveform, electrical pattern and eye diagram of the cross-correlation signal are illustrated in Fig. 3 (d) ~ (f). In contrast, the incorrectly decoded optical waveform behaviors like a noise representing the cross-correlations among all the Gold codes. The electrical pattern is evidently wrong and its corresponding eye diagram was closed which clearly shows that an eavesdropper can not break the security of our system without the knowledge of the code hopping sequence. Even though he may get an obscure eye diagram due to the limited code length in the experiment as is shown in Fig 3. (f), he still can not recover the original DPSK data.

The measured bit-error-rate (BER) performance after 34km transmission for the correctly decoded signal is shown in Fig. 3(g). Error-free transmission has been achieved for all the four code hopping sequences. We should note that in the absence of optical en/decoding, an eavesdropper could easily break the network security by simply using a 2.5GHz DPSK demodulator and its measured BER is also shown in Fig.3 (g). Compared to the case of without en/decoding, the average power penalty for the four code hopping sequences is about 0.6dB due to the non-ideal decoding. As for the cross-correlation signal, no BER can be measured indicating the security enhancement based on the bit-by-bit code scrambling technique.

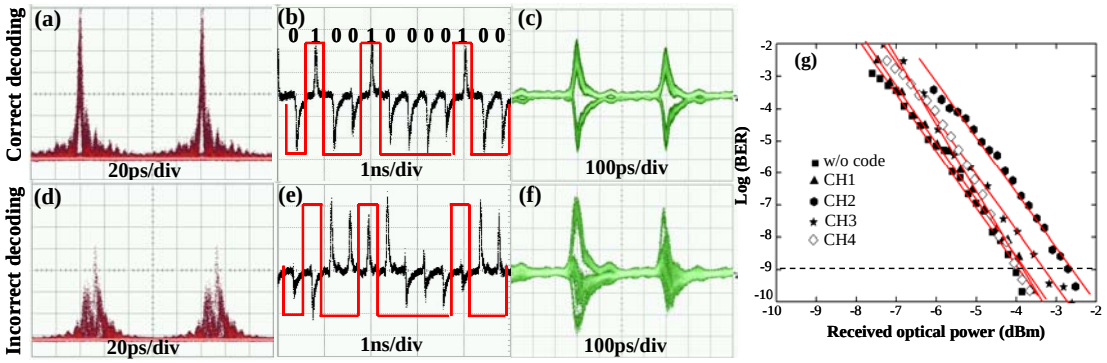

Fig.3 (a) Correctly decoded optical waveform (b) correct electrical pattern and (c) correct eye diagram. The decoded waveform, electrical pattern and eye diagram of the cross-correlation signal are shown in (d) ~ (f), respectively. (g) BER performance after 34km transmission for correctly decoded signal

4. CONCLUSIONS

We have proposed and demonstrated a reconfigurable bit-by-bit code scrambling technique based on time domain spectral phase en/decoding scheme for secure optical communication. 2.5Gbps DPSK data and four code hopping sequences scrambled by five 8-chip, 20Gchip/s Gold codes using prime-hop patterns have been simultaneously generated using single phase modulator. The scrambled code hopping sequences have been successfully decoded and BER<10^{-9} has been achieved for the 2.5Gbps DPSK data after 34km transmission. The proposed bit-by-bit code scrambling scheme can significantly enhance the transmission security in physical layer and exhibit the potential to realize one time pad.

REFERENCES

[1] K. Kitayama and M. Murata, "Versatile Optical Code-Based MPLS for Circuit, Burst, and Packe Switchings", J. Lightwave Technol. 21 (11), 2753-2764, (2003)

[2] N. Wada, H. Furukawa, T. Miyazaki: Prototype 160Gbit/s/port optical packet switch based on optical code label processing, IEEE Journal of Selected Topics in Quantum Electronics, vol. 13, no. 5, pp. 1551-1559, 2007.

[3] X. Wang, K. Matsushima, K. Kitayama, A. Nishiki, N. Wada, F. Kubota, "High performance optical code generation and recognition by use of 511-chip, 640-Gchip/s phase shifted superstructured fiber Bragg grating", Opt. Lett., vol.30, no.4, pp,355-357, 2005.

[4] P. R. Prucnal, M. A. Santoro and T. R. Fan, "Spread spectrum fiber-optic local area network using optical processing", J. Lightwave. Technol. 4 (5), 547-554 (1986).

[5] A. Stock and E. H. Sargent, "The role of optical CDMA in access networks," IEEE Communication Magazine 40, 83-87 (2002).

[6] Jonathan P. Heritage and Andrew M. Weiner, "Advances in Spectral Optical Code-Division Multiple-Access", IEEE J. Quantum Electron. 13(5), 1351-1369 (2007)

[7] X. Wang and K. Kitayama, "Analysis of beat noise in coherent and incoherent time-spreading OCDMA," J. Lightwave Technol. 22 (10), 2226-2235 (2004).

[8] Y.-K. Huang, B. Wu, I. Glesk, E. E. Narimanov, T. Wang and P. R. Prucnal, "Combining cryptographic and steganographic security with self-wrapped optical code division multiplexing techniques", Electron. Lett., vol.43, no.25, 2007.

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

[10] T. H. Shake, "Confidentiality performance of spectral-phase-encoded optical CDMA," J. Lightwave Technol. 23 (4), 1652-1663, (2005)

[11] T. Shake: Security performance of optical CDMA against eavesdropping, J. Lightwave Technol., vol. 23. pp. 655-670, Feb. 2005.

[12] Z. Jiang, D. Seo, S. Yang, D. E. Leaird, R. V. Roussev, C. Langrock, M. M. Fejer, and A. M. Weiner, "Four-user 10-Gb/s spectrally phase-coded O-CDMA system operating at ~ 30 fJ/bit," IEEE Photonics Technol. Lett. 17 (3), 705-707 (2005)

[13] X. Wang, N. Wada, T. Miyazaki, K. Kitayama, "Coherent OCDMA System Using DPSK Data Format With Balanced Detection", IEEE Photonics Technol. Lett. 18 (7), 826-828 (2006)

[14] D. E. Leaird, Z. Jiang, and A. M. Weiner, "Experimental investigation of security issues in OCDMA: a code-switching scheme," Electron. Lett. 41, 817–819 (2005).

[15] Z. Jiang, D. E. Leaird and A. M. Weiner, "Experimental investigation of security issues in O-CDMA", J. Lightwave Technol., vol. 24. pp. 4228-4334, Nov. 2006.

[16] A. M. Weiner, Z. Jiang, and D. E. Leaird, "Spectrally phase-coded O-CDMA", Journal of optical networking, 6 (6), 728-755 (2007)

[17] X. Wang and N. Wada, "Spectral phase encoding of ultra-short optical pulse in time domain for OCDMA application", Optics Exp. 15(12), 7319-7326 (2007).

[18] X. Wang and N. Wada, "Reconfigurable Time Domain Spectral Phase Encoding/Decoding Scheme Using Fibre Bragg Gratings for Two-dimensional Coherent OCDMA", European Conference on Optical Communication (ECOC'08), P.3.11, September, Brussels, Belgium, 2008.

[19] Z. Gao, X. Wang, N. Kataoka and N. Wada "Demonstration of time-domain spectral phase encoding/ DPSK data modulation using single phase modulator", LEOS Summer Topical 2009, TuA3.1, New port, A, USA, 2009.

[20] B. Wu, I. Glesk, P. R. Prucnal, and E. Narimanov, "Security analysis of stealth transmission over a public fiber-optical network," in Conf. Lasers and Electro-Optics, May 2007, pp. 1–2.

[21] Z. Wang, A. Chowdhury and P. R. Prucnal, "Optical CDMA Code Wavelength Conversion Using PPLN to Improve Transmission Security", IEEE Photonics Technol. Lett. 21 (6), 383-385 (2009).