Bit-by-bit optical code scrambling technique for secure optical communication

Xu Wang[1*], Zhensen Gao[1], Xuhua Wang[1], Nobuyuki Kataoka[2] and Naoya Wada[2]

[1]*Joint Research Institute for Integrated Systems, Sch. of Engineering and Physical Sciences, Heriot-Watt University, Riccarton, Edinburgh, EH14 4AS, UK*

[2]*Photonic 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*

** x.wang@hw.ac.uk*

Abstract: We propose and demonstrate a novel bit-by-bit code scrambling technique based on time domain spectral phase encoding/decoding (SPE/SPD) scheme using only a single phase modulator to simultaneously generate and decode the code hopping sequence and DPSK data for secure optical communication application. In the experiment, 2.5-Gb/s DPSK data has been generated, decoded and securely transmitted over 34km by scrambling five 8-chip, 20-Gchip/s Gold codes with prime-hop patterns. The proposed scheme can rapidly reconfigure the optical code hopping sequence bit-by-bit with the DPSK data, and thus it is very robust to conventional data rate energy detection and DPSK demodulation attack, exhibiting the potential to provide unconditional transmission security and realize even one-time pad.

OCIS codes: (060.0600) Fiber optics and optical communications; (060.5060) Phase modulation; (999.999) Encoding/decoding; (9999.999) Optical code division multiple access; (999.999) secure optical communication.

References and links

1. K. Kitayama, and M. Murata, "Versatile Optical Code-Based MPLS for Circuit, Burst, and Packet Switchings," J. Lightwave Technol. **21**(11), 2753–2764 (2003).
2. N. Wada, H. Furukawa, and T. Miyazaki, "Prototype 160Gbit/s/port optical packet switch based on optical code label processing," IEEE J. Sel. Top. Quantum Electron. **13**(5), 1551–1559 (2007).
3. X. Wang, K. Matsushima, K. Kitayama, A. Nishiki, N. Wada, and F. Kubota, "High-performance optical code generation and recognition by use of a 511-chip, 640-Gchip/s phase-shifted superstructured fiber Bragg grating," Opt. Lett. **30**(4), 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 Commun. Mag. **40**(9), 83–87 (2002).
6. J. P. Heritage, and A. 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. **43**(25), 1449 (2007).
9. S. Etemad, A. Agarwal, T. Banwell, J. Jackel, R. Menendez, and P. Toliver, "OCDM-based photonic layer "security" scalable to 100 Gbit/s for existing WDM networks," J. Opt. Netw. **6**(7), 948–967 (2007).
10. I. Glesk, Y.-K. Huang, C.-S. Brès, and P. R. Prucnal, "OCDMA platform for avionics applications," Electron. Lett. **42**(19), 1115–1116 (2006).
11. I. Glesk, M. Sorel, A. E. Kelly, and P. R. Prucnal, "Enhancing Performance of Optical Communication Systems with advanced Optical Signal Processing," J. Opt. Netw. **5**(11), 1328–1334 (2010).
12. T. H. Shake, "Confidentiality performance of spectral-phase-encoded optical CDMA," J. Lightwave Technol. **23**(4), 1652–1663 (2005).
13. T. H. Shake, "Security performance of optical CDMA against eavesdropping," J. Lightwave Technol. **23**(2), 655–670 (2005).

#138763 - $15.00 USD Received 29 Nov 2010; revised 30 Jan 2011; accepted 30 Jan 2011; published 8 Feb 2011

14. 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 Photon. Technol. Lett. **17**(3), 705–707 (2005).
15. X. Wang, N. Wada, T. Miyazaki, and K. Kitayama, "Coherent OCDMA System Using DPSK Data Format With Balanced Detection," IEEE Photon. Technol. Lett. **18**(7), 826–828 (2006).
16. D. E. Leaird, Z. Jiang, and A. M. Weiner, "Experimental investigation of security issues in OCDMA: a code-switching scheme," Electron. Lett. **41**(14), 817–819 (2005).
17. Z. Jiang, D. E. Leaird, and A. M. Weiner, "Experimental investigation of security issues in O-CDMA," J. Lightwave Technol. **24**(11), 4228–4234 (2006).
18. X. Wang, and N. Wada, "Spectral phase encoding of ultra-short optical pulse in time domain for OCDMA application," Opt. Express **15**(12), 7319–7326 (2007).
19. Z. Gao, X. Wang, N. Kataoka, and N. Wada, "Demonstration of time-domain spectral phase encoding/DPSK data modulation using single phase modulator", IEEE LEOS Summer Topical 2009, New port, CA, USA, Paper TuA3.1.
20. X. Wang, Z. Gao, N. Kataoka, and N. Wada, "Time domain spectral phase encoding/DPSK data modulation using single phase modulator for OCDMA application," Opt. Express **18**(10), 9879–9890 (2010).
21. B. Schneier, *Applied cryptography*, Second edition, (John Wiley & Sons, 1996), Chapter 7.
22. Z. Wang, A. Chowdhury, and P. R. Prucnal, "Optical CDMA Code Wavelength Conversion Using PPLN to Improve Transmission Security," IEEE Photon. Technol. Lett. **21**(6), 383–385 (2009).
23. C. E. Shannon, "Communication theory on secrecy systems," J. Bell Syst. Tech. **28**(4), 656–715 (1949).

1. Introduction

Optical code (OC) generation and recognition are one of the key techniques in future photonic networks such as optical-packet-switching (OPS), optical-burst-switching (OBS) and especially optical-code-division-multiple-access (OCDMA) system [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, according to which different user can be distinguished by the proper optical decoder at the receiver [4, 5]. Due to the all-optical processing based optical code generation and recognition, the OCDMA exhibits the unique features of allowing fully asynchronous transmission, low-latency access which is desirable for burst traffic environment, protocol transparency, high network flexibility, simplified network management and so on [6,7]. Among all the other potential advantages, providing the information security is generally considered as an inherent benefit of OCDMA system [5, 7–9]. Security reinforcement in incoherent OCDMA system has been achieved previously by using wavelength-hopping time-spreading and optical XOR techniques [10, 11].

In coherent OCDMA system, one may intuitively think that the eavesdropper cannot intercept the data without knowledge of the applied code because the optical pulse encoded by the optical encoder manifests itself as a noise-like waveform. However, *Shake* [12, 13] pointed out that a simple power detector can easily makes the eavesdropper access to the data in a single user OCDMA system employing on-off keying (OOK) modulation format. *Jiang et al* [14] has also experimentally demonstrated the security vulnerability of a spectrally phase encoded OOK-OCDMA system. This is mainly due to the fact of data-rate detection by the standard energy detector to perform the integration of the whole energy in one bit period, so a clear eye-diagram can still be obtained for the cross-correlation signals. Various approaches have been proposed to overcome the vulnerabilities in single user OCDMA system. Advanced optical modulation formats have been adopted in OCDMA system to address this issue. In [15], 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, in this DPSK-OCDMA system, the eavesdropper can still decipher the data using a common DPSK demodulator without any information of the code. A code switching data modulation format for enhancing the security was also investigated in [16]. 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 demonstrated later [17], 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

#138763 - $15.00 USD Received 29 Nov 2010; revised 30 Jan 2011; accepted 30 Jan 2011; published 8 Feb 2011

from different codes. 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 has also been discussed in [16]. It has been suggested that the data confidentiality could be significantly improved in an OCDMA system by rapidly reconfiguring the optical codes [12, 13], but this concept has not been demonstrated yet because most of the conventional optical coding schemes cannot offer 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 [18]. 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. Moreover, it exhibits the potential to perform the optical code generation and DPSK data modulation simultaneously using single phase modulator [19, 20].

In this paper, we propose and experimentally demonstrate for the first time, to the best of our knowledge, a novel bit-by-bit code scrambling technique based on our proposed time domain spectral phase en/decoding scheme for secure optical communication. 2.5-Gb/s DPSK data modulation and five 8-chip, 20-Gchip/s optical Gold codes has been simultaneously generated, and scrambled by Prime-hop patterns bit-by-bit using only a single phase modulator in the experiment. The rapid reconfigurable capability of the combined DPSK data and code hopping sequence makes our system immunity to simple data rate energy detection and DPSK demodulation attack, and therefore, it can significantly improve the transmission security and exhibit the potential to realize even perfect secrecy.

2. Principle of proposed scheme

Figure 1 shows the schematic diagram of the proposed scheme, where the principle of the simultaneous bit-by-bit code scrambling and DPSK data modulation using only a single phase modulator is shown in Fig. 1(a). An ultra-short optical pulse train with a broadband spectrum (λ_1, λ_2, λ_3, λ_4…) is used as the laser source in this scheme. It is injected into the time domain SPE section which is composed of a pair of dispersive devices with opposite dispersion values (–D and + D) and a high speed phase modulator (PM) for bit-by-bit spectral phase encoding. The first dispersive device with dispersion of –D is used for stretching the pulse in time domain, by which the frequency to time mapping can be realized (λ_1, λ_2, λ_3, λ_4…spread in different time positions). The PM is driven by bit-by-bit combining the optical code (OC) patterns and DPSK data which is generated by precoding the original data (101000…) into DPSK data format (100101…) and then combined with the corresponding OC in the following way to modulate the phase of the stretched optical signal: when the DPSK data is symbol "1", the PM is driven by OC, while if symbol is "0", the PM is driven by $\overline{OC4}$. The optical codes can thus be scrambled in this scheme, for example, in the case of Fig. 1(a), the PM can be driven by the combined DPSK data and code sequence as OC5, $\overline{OC2}$, $\overline{OC4}$, OC6, $\overline{OC1}$, OC3. Therefore, the DPSK data can be spectrally phase encoded bit-by-bit by using only one PM. After that, the second dispersive device with opposite dispersion of + D is used for compressing the pulse and generating the DPSK data modulated SPE signal. The spectral phase of each encoded DPSK data is different from the others representing different optical codes (i.e. the phase of the third and fourth data are $\overline{OC4}$: 00π0π00π… and OC6:π0πππ0ππ…, respectively).

In the receiver side, the generated DPSK data modulated SPE signal has to be spectrally phase decoded and then DPSK demodulated to recover the original data. The setup for the SPD is similar to that of the transmitter, as shown in Fig. 1(b) which is also composed of a pair of dispersive devices and a high speed PM. However, the PM is driven only by the complementary scrambled optical code sequences $\overline{OC5}$, $\overline{OC2}$, $\overline{OC4}$, $\overline{OC6}$, $\overline{OC1}$, $\overline{OC3}$, so the spectral

#138763 - $15.00 USD Received 29 Nov 2010; revised 30 Jan 2011; accepted 30 Jan 2011; published 8 Feb 2011

components of each encoded pulse are in phase after the decoder (i.e. For the third data, if the symbol "1", the total phase is "OC4+ $\overline{OC4}$ =π", while for symbol "0", the total phase is "$\overline{OC4}$ + $\overline{OC4}$ =0"). Therefore, the total phase of each decoded pulse becomes (π00π0π…) and the DPSK data is extracted from the SPE signal as (100101…). Finally, a DPSK demodulator with one-bit delay interferometer followed by a balanced detector is used to demodulate the DPSK data and recover the original data as (101000…).

In the proposed scheme, the SPE and SPD utilize similar configuration to perform the optical code generation and recognition, which exhibits the potential to simplify the architecture of both the transmitter and receiver. In addition, only a single phase modulator is used to realize the optical code generation and DPSK data modulation simultaneously, enabling the rapid bit-by-bit code reconfigurable capability to significantly improve the data confidentiality for secure optical communication application.

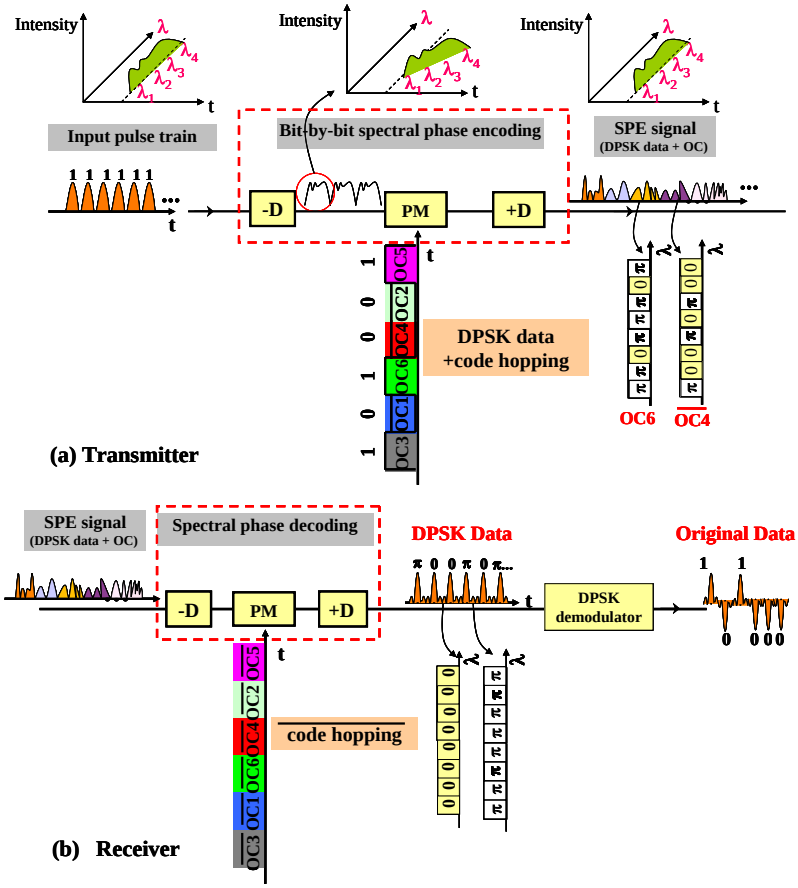

Fig. 1. Principle of the proposed scheme (a) transmitter for bit-by-bit code scrambling and DPSK data modulation; (b) receiver for SPD and DPSK data demodulation

#138763 - $15.00 USD Received 29 Nov 2010; revised 30 Jan 2011; accepted 30 Jan 2011; published 8 Feb 2011

3. Experimental setup

The experimental setup of the proposed bit-by-bit code scrambling and DPSK data modulation scheme is illustrated in Fig. 2. At the transmitter, a super-continuum (SC) light source is

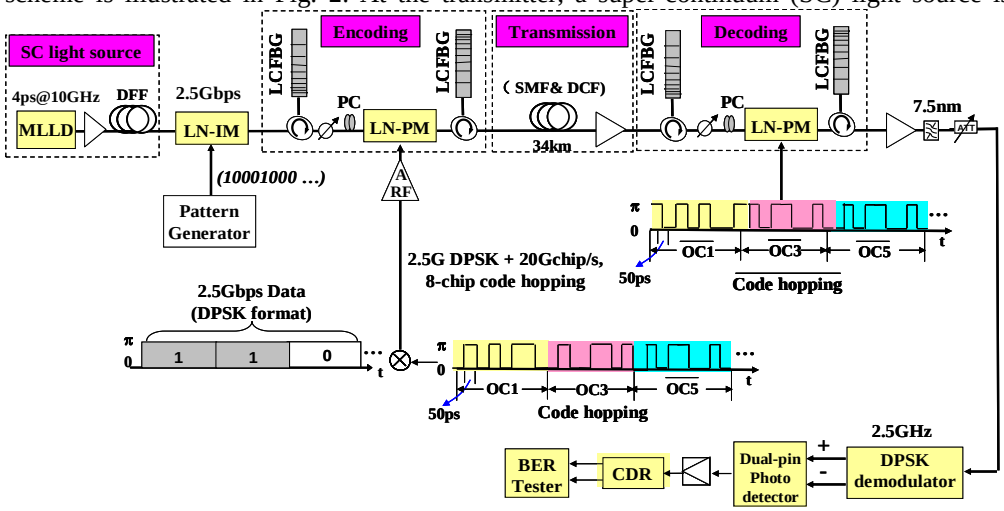

Fig. 2. Experimental setup of bit-by-bit code scrambling based on time domain SPE/SPD scheme.

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 Gaussian-like pulses with a repetition rate of 10GHz, spectrally centered at 1550.28nm. The source repetition rate is converted to 2.5GHz by using a Mach-Zehnder intensity modulator (IM) and pulse pattern generator (PPG). The following setup includes two main sections: bit-by-bit spectral phase encoding using the mixed DPSK data and scrambled code sequence, and bit-by-bit code recognition using only the complementary code hopping sequence.

In the encoding section, a LCFBG with 10-dB bandwidth of ~4.7nm and dispersion slope of about −80ps/nm is used to stretch the 2.5GHz optical pulse into 376ps 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, between obvious overlap can degrade the decoding and transmission performance [18]. Different spectral components spread into different positions in time domain as a result of the chromatic dispersion. The dispersed pulse is then temporally phase modulated by a PM driven by the combination of 2.5-Gb/s DPSK data and scrambled code hopping sequence, which contains five 8-chip, 20-Gchip/s (corresponding to 8-chip, 78-GHz/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 peak power ratio (P/C) between the auto-/cross-correlations is very low. Figure 3 (a)~(c) shows the measured encoded waveform (upper row), encoded spectrum (middle row) for the five Gold codes and the auto/cross-correlation signals (lower row) for OC2, respectively. All the five codes have been successfully decoded in the experiment and the decoded pulses exhibit well-defined auto-correlation peak. An identical phase modulator in the encoding and decoding side, and less than 20ps/nm residual dispersion of the SMF & DCF are essential to reduce the sidelobes and improve the decoding performance of the auto-correlation signal. As shown in Fig. 3 (c), the average P/C for the 8-chip, 20-Gchip/s codes can reach to ~2, which is sufficient to

#138763 - $15.00 USD Received 29 Nov 2010; revised 30 Jan 2011; accepted 30 Jan 2011; published 8 Feb 2011

discriminate different codes and perform the DPSK code hopping experiment. By increasing the chip number and chip rate of the optical code, the P/C can be further improved to enhance the security.

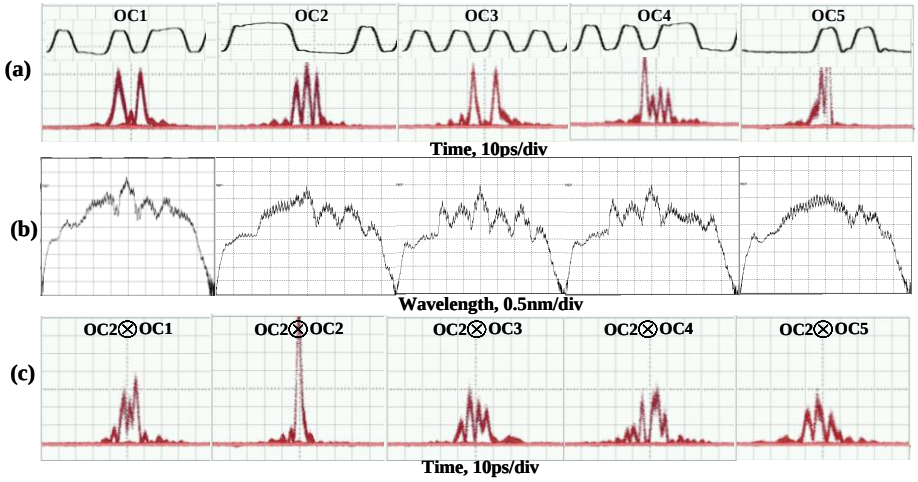

Fig. 3. (a) Encoded waveform (upper row) and (b) encoded spectrum (middle row) for the five codes; (c) Auto-/cross- correlation signals for OC2 (lower row).

Figure 4 shows the procedure to combine the DPSK data with the code hopping sequence bit-by-bit. Firstly, 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 $\overline{\text{OC}}$, therefore, the first five bits are encoded by OC1, OC3, $\overline{\text{OC5}}$, $\overline{\text{OC2}}$, OC4 as shown in Fig. 4(a). Similarly, the following grouped DPSK data is also encoded by the corresponding prime-hop code pattern (see Fig. 4(b)) that is very flexible to reconfigure according to a look-up table (i.e. H2, H4, H3, H1, H4, H3, H1, H2…) shown in Fig. 4(c). To accurately synchronize the phase code and the stretched pulse, an optical delay line is employed 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.

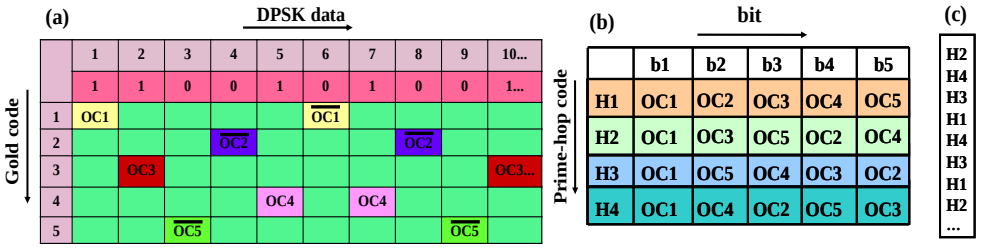

Fig. 4. (a) DPSK data and corresponding Gold code; (b) Prime-hop code patterns and (c) Look-up table of prime-hop code pattern

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 $\overline{\text{OC}}$ (i.e. $\overline{\text{OC1}}$, $\overline{\text{OC3}}$, $\overline{\text{OC5}}$, $\overline{\text{OC2}}$, $\overline{\text{OC4}}$ …). The correctly decoded signal is launched into a

#138763 - $15.00 USD Received 29 Nov 2010; revised 30 Jan 2011; accepted 30 Jan 2011; published 8 Feb 2011

2.5GHz DPSK demodulator followed by a balanced detector to extract the original DPSK data. It is worthy to note that the requirement of synchronization between the encoding and decoding stage is rather strict in this experiment, making it very difficult for an eavesdropper to correctly decode and recover the DPSK data without accurate chip-level time coordination even if she 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 by proper time coordination. 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.

4. Bit-by-bit code scrambling/DPSK data modulation using single PM

We have carried out a proof-of-principle experiment using four different code hopping sequences CH1~CH4 using 2^7-1 pseudo-random-bit-sequence (PRBS) RZ-DPSK data. 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 5(a) shows the correctly decoded optical waveform for CH4 (H3 H4 H1 H2 H2 H4 H1 H3 H2 H3 H1 H4 H4 H3 H2 H1…) measured by a 10GHz optical sampling oscilloscope which exhibit clear eye opening. The electrical pattern and corresponding eye diagram are shown in Fig. 5(b) and (c), respectively. Correct

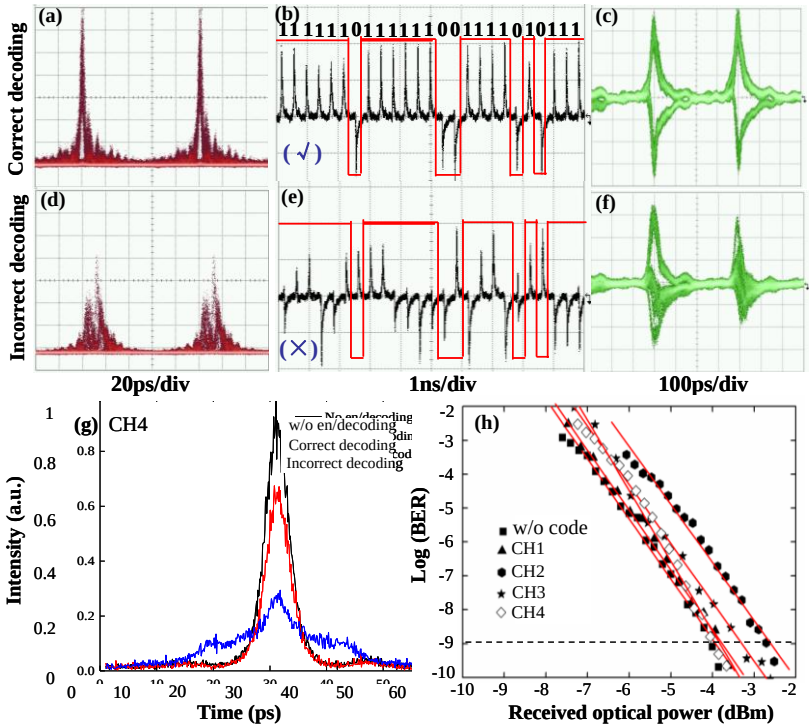

Fig. 5. (a) Correctly decoded optical waveform, (b) correct electrical pattern and (c) correct eye diagram. The decoded waveform, electrical pattern and eye diagram of the cross-correlation signal are shown in (d) ~(f), respectively. (g) Auto-/cross-correlation signal measured by an auto-correlator for CH4; (h) BER performance after 34km transmission for the correctly decoded signal.

#138763 - $15.00 USD Received 29 Nov 2010; revised 30 Jan 2011; accepted 30 Jan 2011; published 8 Feb 2011

pattern (1111110111111001111010111…) 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. 5 (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 is closed, which clearly shows that an eavesdropper cannot break the security of this 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. 5(f), he still cannot recover the original data pattern. Figure 5(g) shows the auto-/cross-correlation trace measured by an auto-correlator with a maximum scan range of 60ps, from which one can see that the peak intensity of the correctly decoded signal is slightly lower than that of no en/decoding due to non-ideal transmission dispersion compensation, discrepancy of the code transition generated from the two PPGs, but it is twice higher than that of the incorrectly decoded signals.

The measured bit-error-rate (BER) performance after 34km transmission for the correctly decoded signal is shown in Fig. 5(h). Error-free transmission has been achieved for all the four code hopping sequences. 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. 5(h). 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 signals, no BER can be measured, indicating the security enhancement based on the bit-by-bit code scrambling technique.

5. Security analysis

In this section, we analyze the data confidentiality of the proposed bit-by-bit code scrambling/DPSK data modulation OCDM system. Let's define **Key Length** (*L*), is the length of the hopping pattern, and **Code Number** (*n*), is the number of optical codes used in the hopping pattern. In the example shown in Fig. 6, *L*=12, *n*=6.

User Data	1	0	1	0	1	1	0	0	1	0	1	1	1	0	1	……
Hopping Pattern	OC1	$\overline{\text{OC3}}$	OC4	$\overline{\text{OC1}}$	OC6	OC5	$\overline{\text{OC2}}$	$\overline{\text{OC4}}$	OC6	$\overline{\text{OC5}}$	OC3	OC2	OC1	$\overline{\text{OC3}}$	OC4	……

Key Length: 12 Code Number: 6

Fig. 6. An example for definition of Key Length and Code Number

Assuming that a sophisticated eavesdropper knows the *n* in the system, thus the confidentiality of user data is mainly guaranteed by the *L*.

The cardinality of the hopping patterns is *C*:

$$C = P_L^n \bullet n^{L-n} \quad (L \geq n) \tag{1}$$

Here $P_L^n = L!/(L-n)!$ denotes the permutation of *L* with *n* elements.

The average number of trials to break the hopping pattern by brute-force attack is *C*/2.

To compare with the traditional symmetric encryption system [21], we adopt the term **effective key length** (L_{eff}), which is defined as $L_{eff}=\log_2 C$ [22]. The effective key length of the proposed scheme is given by

$$L_{eff} = Log_2(P_L^n \bullet n^{L-n}) \quad (L \geq n) \tag{2}$$

In practical, a system encrypted by 128-bit symmetric key is nearly unbreakable by brute-force attack, which is considered from time, cost and thermodynamic limitations [21]. Currently, both Advanced Encryption Standard (AES) and Route Coloniale 4 (RC4), which are

#138763 - $15.00 USD Received 29 Nov 2010; revised 30 Jan 2011; accepted 30 Jan 2011; published 8 Feb 2011

widely used in Secure Sockets Layer (SSL) and Wired Equivalent Privacy (WEP), adopted 128-bit key as a standard. So here we take the 128-bit symmetric key as a reference to compare the level of computational security of the proposed scheme.

Figure 7(a) shows the dependence of L_{eff} with the code number n and the key length L. The plane of L_{eff}=128 is shown here as a reference level. By increasing the key length L and code number n, L_{eff} can be greater than the reference level, showing significant security improvement based on the proposed scheme. Figure 7(b) shows the conditions when L_{eff}=128 (which means that the security level equals to 128-bit symmetric key system). We can see that the shortest key length L is 26 that can achieve the reference security level.

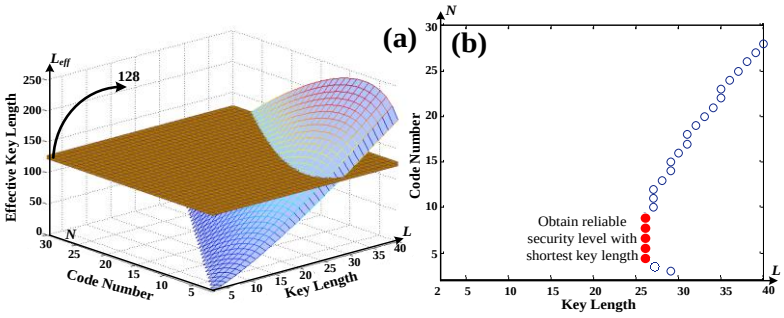

Fig. 7. (a) The increasing trend of Effective key length (*KL*) versus code number (*N*) and the key length (*L*); (b) Region of the *n* and *L* for higher security level than 128-bit symmetric key.

Compared with the traditional symmetric-key encryption, the proposed scheme is in the physical (optical) layer and is totally transparent to upper-layer protocol/contents in the communication system. The optical buffer and optical signal processing techniques is still a huge barrier against the eavesdropper to apply any traditional cryptanalysis method to break the security of the proposed scheme. The eavesdropper must take much more time than doing the same processes in electrical domain even when performing the simplest brute-force attack.

With the great flexibility provided by the proposed scheme, we can rapidly reconfigure the code to enable L to a magnitude as same as the data length. Note that if the L equals to the data length, we could achieve the so-called "perfect secrecy" [23] (the same security level as "one time pad"). Therefore, compared to the traditional OOK- [14], DPSK- [15] and CSK-OCDM [16] systems using only one or two fixed codes, the proposed bit-by-bit code scrambling/DPSK data modulation technique can provide significantly higher security level, and exhibits the potential to provide unconditional transmission security and realize even the perfect secrecy.

6. Conclusion

We have proposed and experimentally demonstrated, for the first time, a rapidly reconfigurable bit-by-bit code scrambling technique based on time domain spectral phase en/decoding scheme for secure optical communication. 2.5-Gb/s DPSK data and four code hopping sequences scrambled by five 8-chip, 20-Gchip/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 2.5-Gb/s DPSK data after 34km transmission. The proposed bit-by-bit code scrambling scheme can significantly enhance the data confidentiality in optical layer, exhibiting the potential to realize one time pad in optical communication system.

#138763 - $15.00 USD Received 29 Nov 2010; revised 30 Jan 2011; accepted 30 Jan 2011; published 8 Feb 2011

Acknowledgements

This work is partly supported by the Royal Society international joint project. Zhensen Gao would like to thank the Royal Academy of Engineering for the international travel grant to enable him to carry out this experiment. The authors also acknowledge Mr. Sumimoto and Y. Tomiyama of NICT for their technical supports in this experiment.

#138763 - $15.00 USD Received 29 Nov 2010; revised 30 Jan 2011; accepted 30 Jan 2011; published 8 Feb 2011