Secure Optical Communication Based on Optical Code Reconfiguration Scheme

Xu Wang*[a], Zhensen Gao[a], Bo Dai[a], Nobuyuki Kataoka[b] and Naoya Wada[b]

[a]School of Engineering and Physical Sciences, Heriot-Watt University, Edinburgh, UK, EH14 4AS, *Email: x.wang@hw.ac.uk
[b]Photonic Network Group, National Institute of Information and Communications Technology (NICT), Tokyo, Japan, 184-8795

ABSTRACT

In this paper, we review the advances of using bit-by-bit optical code scrambling and rapid reconfigurable/code-length variable technologies for security improvement in optical communication systems.

Keywords: Fiber optics and optical communications, phase modulation, encoding/decoding, optical code division multiple access, secure optical communication

1. INTRODUCTION

With the explosive growth of optical network resources, secure optical communication is becoming increasingly important and has recently attracted great research interest. To meet the military or commercial requirement of private data exchange, it is crucial to protect certain confidential data from malicious eavesdropping by an unauthorized party, and therefore, special attention should be paid on the security in the deployment of next generation optical network. Various approaches for secure optical communication have been proposed over the past years, such as quantum key distribution [1], chaotic communication [2] and so on [3-4]. In addition to them, the optical code (OC) based en/decoding that has been widely exploited in optical code division multiple access (OCDM) system is considered as another promising candidate for secure optical communication [5-6], because the encoded signal by the OC manifests itself like a noise, making the eavesdropper rather hard to intercept the data.

Although the OC processing can intuitively prevent the eavesdropper from accessing the privacy data, security vulnerabilities have been revealed in OCDMA systems [7-8]. It has been demonstrated that the eavesdropper can extract the OC by analyzing the coding induced dips of the encoded spectrum [7] or waveform [8] in either the time spreading encoding or spectral phase encoding system. The security of OCDMA systems is also closely related to the data modulation formats [5, 7]. It has been demonstrated that in an OOK-OCDMA system, an eavesdropper can tap the individual user's signal and recover the data by using a simple power detector without the need of knowing the exact OC [5, 7]. Advanced optical modulation formats such as differential-phase-shift-keying (DPSK) and code-shift-keying (CSK) can overcome this vulnerability since the data bit 0 and bit 1 have identical intensity for these modulation formats. However, as demonstrated later, an eavesdropper can use a DPSK demodulator rather than a power detector to directly recover the data from the encoded noise-like signals because the interference of the adjacent bit with identical coded waveform generates high level output while the interference is nearly zero if the adjacent bits are from different codes [7]. Careful analysis reveals that the conventional approaches by assigning a fixed OC for all the bits is not resistant to eavesdropping with an appropriate detector whatever en/decoding and modulation formats are used. By assigning different code for each bit and rapidly reconfiguring the OC, the data confidentiality could be significantly improved in the OCDMA system.

Recently, we have proposed a time domain spectral phase en/decoding (SPE/D) scheme utilizing two opposite dispersive elements and a high speed phase modulator place between them for OCDMA application [9]. This scheme is very flexible in rapidly reconfiguring the optical code and compatible with the fiber-optic systems. We

Photonics and Optoelectronics Meetings (POEM) 2011: Optical Communication Systems and Networking, edited by Zisen Zhao, Richard Penty, Chester Shu, Tao Jiang, Proc. of SPIE Vol. 8331, 83310F · © 2012 SPIE · CCC code: 0277-786X/12/$18 · doi: 10.1117/12.924049

further proposed to use this optical code reconfigurable scheme for secure optical communications. In this paper, the recent advances of bit-by-bit optical code scrambling and rapid reconfigurable/code-length-variable optical code shifting technologies for security improvement in optical communication systems based on the time domain SPE/D scheme are reviewed [10-12].

2. BIT-BY-BIT OPTICAL CODE SCRAMBLING TECHNIQUE FOR SECURE OPTICAL COMMUNICATION

2.1 Principle of Bit-by-Bit Optical Code Scrambling Technique

Fig. 1 shows the proposed bit-by-bit optical code scrambling technique based on the time domain SPE/D scheme using a single phase modulator for simultaneous optical encoding and DPSK data modulation [10]. In this scheme, an ultra-short optical pulse train with a broadband spectrum (λ_1, λ_2, λ_3, λ_4…) is used as the laser source. The time domain SPE section is composed of a pair of dispersive devices with opposite dispersion (–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 $\overline{\text{OC}}$. 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, $\overline{\text{OC2}}$, $\overline{\text{OC4}}$, OC6, $\overline{\text{OC1}}$, 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 OC4: 00π0π00π… and OC6:π0πππ0ππ…, respectively).

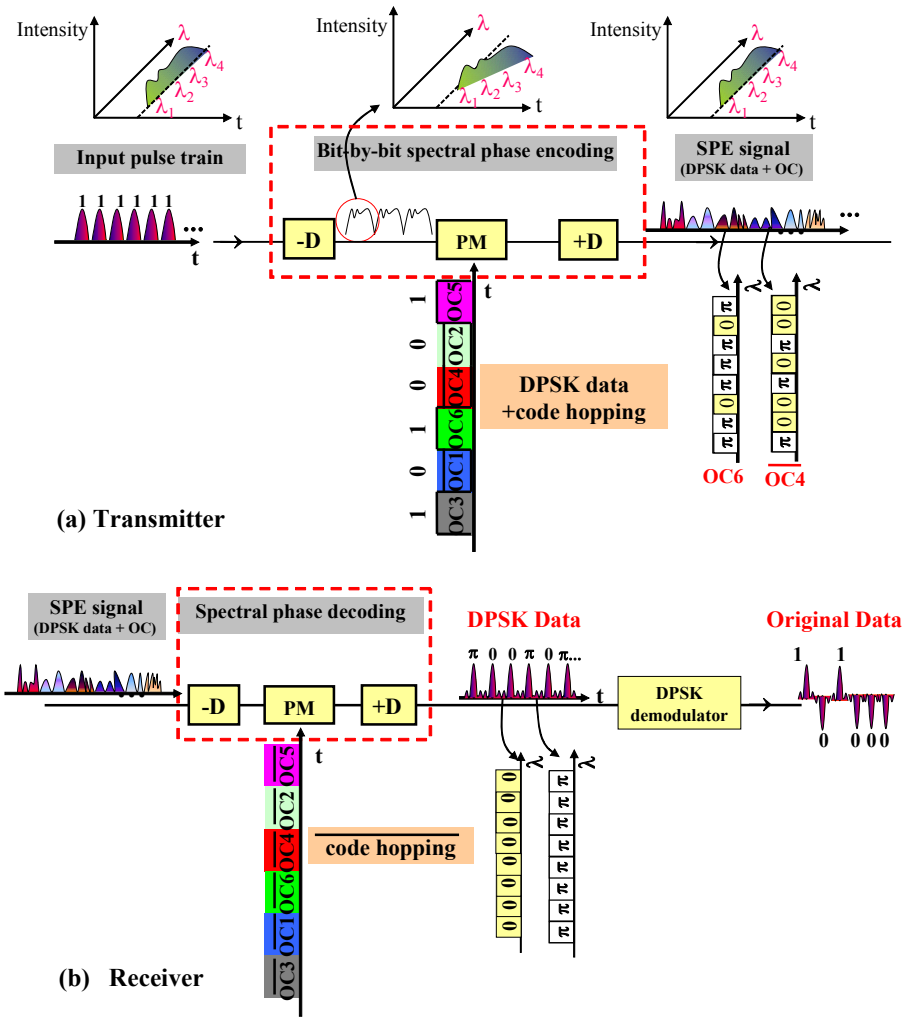

Fig.1 Principle of the proposed scheme (a) transmitter for bit-by-bit code scrambling and DPSK data modulation; (b) receiver for SPD and DPSK data demodulation.

At 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 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 "$\overline{OC4}$+$\overline{OC4}$=π", while for symbol "0", the total phase is "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, which can enable the rapid bit-by-bit code reconfigurable capability to significantly improve the data confidentiality for secure optical communication application.

2.2 Experimental demonstrations of the Bit-by-Bit Optical Code Scrambling

Fig.2 shows the experimental setup. At the transmitter, 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

spectrum is broadened by super-continuum (SC) generation. The source repetition rate is converted to 2.5GHz. 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. Different spectral components spread into different positions in time domain. 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. 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 OC. The correctly decoded signal is launched into a 2.5GHz DPSK demodulator followed by a balanced detector to extract the original DPSK data. The security of our system relies on both the optical codes (physical layer security) and the code hopping pattern (electrical layer security). 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.

Fig. 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 and clear eye opening of the DPSK data are obtained. 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

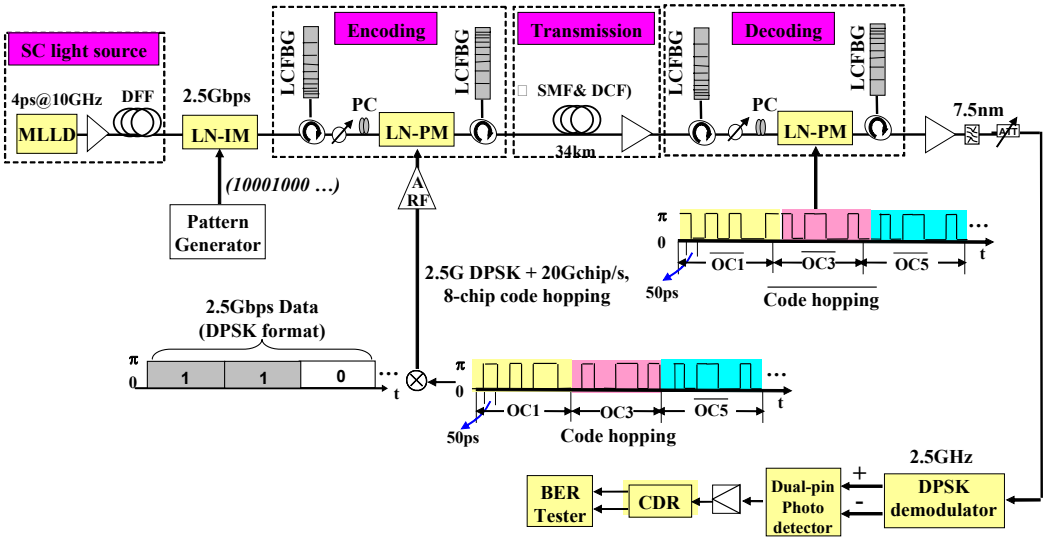

Fig.2 Experimental setup of bit-by-bit code scrambling based on time domain SPE/D scheme.

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. Fig.3 (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 decoding, 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.3 (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.3 (h). As for the cross-correlation signals, no BER can be measured, indicating the security enhancement based on the bit-by-bit code scrambling technique.

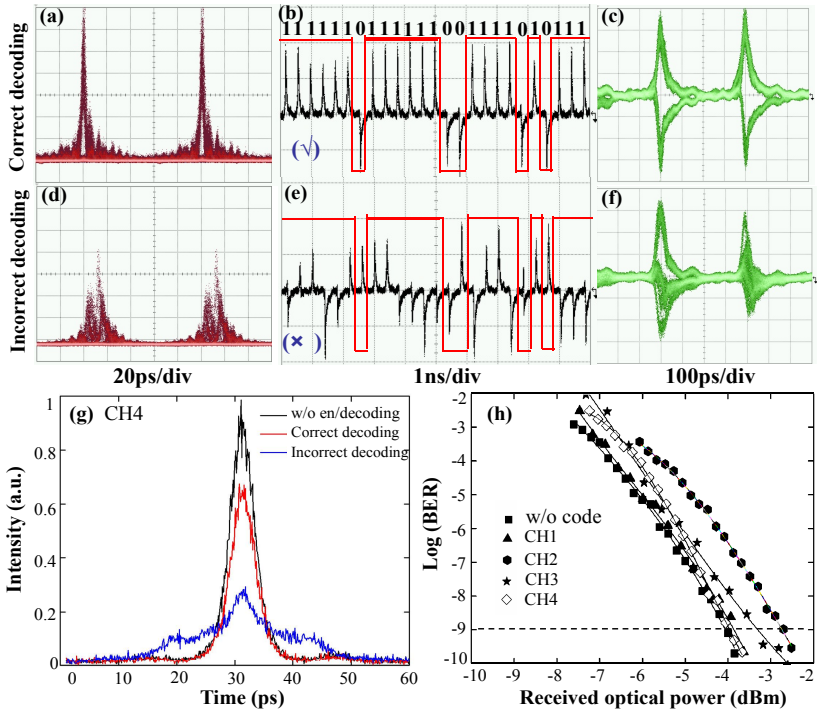

Fig.3 (a) Correctly decoded optical waveform (b) correct electrical pattern and (c) correct eye diagram. The decoded waveform, electrical pattern and eye diagram of the cross-correlation signal are shown in (d) ~ (f), respectively. (g) Auto-/cross-correlation signal measured by an auto-correlator for CH4; (h) BER performances after 34km transmission for the correctly decoded signal.

3. RAPID RECONFIGURABLE/CODE-LENGTH VARIABLE BIT-BY-BIT CODE SHIFTING TECHNIQUE FOR HIGH SPEED SECURE OPTICAL COMMUNICATION

3.1 Principle of Bit-by-Bit Optical Code Shifting Technique

In the bit-by-bit code scrambling scheme, although each bit can be assigned a different OC to enhance the security, the data rate mainly depends on the code length and chip rate, which are mainly limited by the electronic processing technology. We further proposed a rapid programmable/code length variable bit-by-bit code shifting technique with the capability of high speed secure optical communication [11].

Fig.4 illustrates the principle of the proposed technique. Phase-shift-keying modulation format is employed in this scheme, as shown in Fig.4 (a) with DPSK data format. The ultra-short data pulse is stretched by a highly dispersive element in time domain and each bit of the stretched pulse occupies T_s time duration as a result of the chromatic dispersion. As the T_s is greater than the data pulse period T_b, the adjacent pulses are temporally overlapped with each other. After the pulse stretching, a rapid reconfigurable, ultra-long code length variable OC with chip duration of T_c is applied onto the overlapped pulses to perform time domain spectral phase encoding, as shown in Fig.4 (b). By using a long pseudo random OC, each stretched pulse can experience different OC section with an effective code length of T_s/T_c and these sections are shifted by T_b/T_c chips bit-by-bit, which can be referred to bit-by-bit code

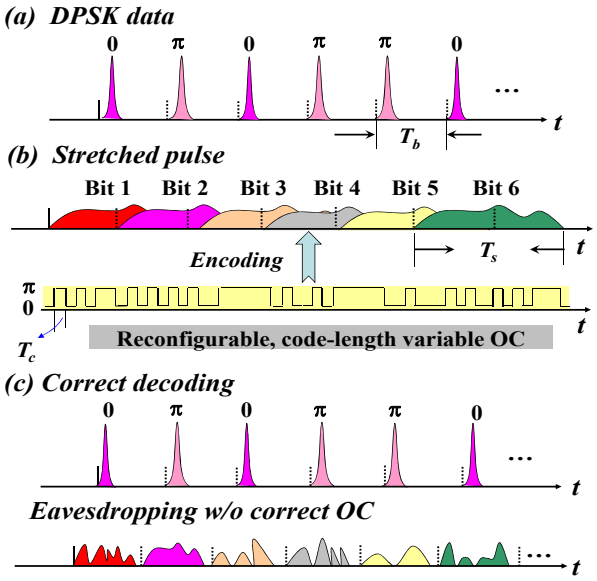

Fig.4 Principle of bit-by-bit code shifting technique for security enhancement.

shifting. In this scheme, the OC could have an unprecedented code length and thus a large code space. Notice that the encoding process is data rate independent and there is no specific requirement of the dispersion value as long as the $T_s > T_b$ is satisfied. For achieving long effective code length, high dispersion is desirable. To decode the overlapped spectral phase encoded signal, the inverse process with complementary OC and opposite dispersion should be conducted to reconstruct the original-like auto-correlation signal with high peak power, as shown in Fig.4 (c). An eavesdropper that is able to intercept the DPSK data should be able to know both the chromatic dispersion and the applied ultra-long OC. Even if he knows the dispersion value for pulse compressing, it is still impossible for him to extract the DPSK data without the correct OC, because only a noise-like cross-correlation signal with random phase for each bit is obtained in this case and the phase shift between different bits is no longer 0, π or any constant value.

3.2 Demonstration of Bit-by-Bit Optical Code Shifting Technique

Fig.5 shows the experimental setup to demonstrate the bit-by-bit code shifting technique. A 10 GHz MLLD is modulated at 10-Gb/s by a LN-PM driven by 2^{23}-1 PRBS sequence. A span of SMF with dispersion of ~ 331 ps/nm is used to significantly broaden the pulse train. Because of the high chromatic dispersion, each bit of the original pulse is stretched into ~662 ps time duration and thus the adjacent consecutive pulses are significantly overlapped with each other. After the temporal stretching, a 40-GHz LN-phase modulator driven by the reconfigurable 40-Gchip/s, code-length variable OC is used to perform bit-by-bit time domain spectral phase encoding. Gold codes with code length of 64-chip, 128-chip, 512-chip and 1024-chip are used in the demonstration. For the time domain spectral phase decoding, similar configuration as the encoding is utilized but the PM is driven by the complementary OC, and a span of dispersion compensation fiber (DCF) with opposite dispersion of ~ -331 ps/nm is used to compress the spectral phase decoded signal in order to retrieve the original pulse. The correctly decoded pulses are

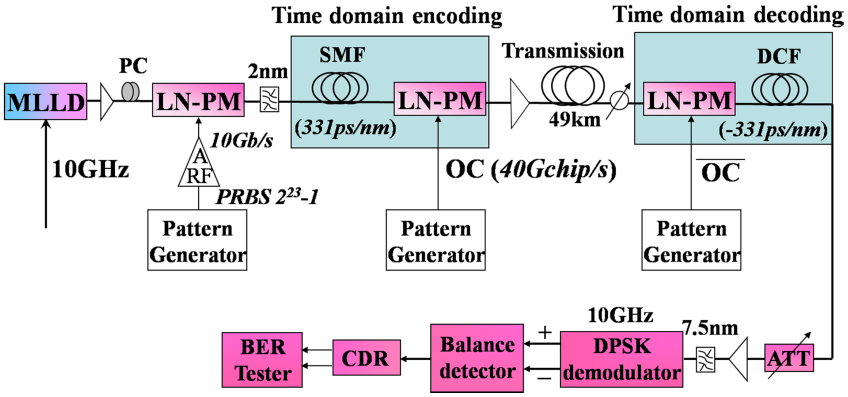

Fig.5 Experimental setup of the proposed time domain bit-by-bit code shifting scheme.

finally directed into a DPSK demodulator followed by a balanced detector to recover the DPSK data for BER measurement. Figs.6 (a) and 3(b) show spectrum and waveform of the stretched 10-Gb/s DPSK pulse train after the dispersive SMF. It can be seen that the data pulse has been significantly stretched in time domain and the adjacent pulses overlap with each other, so the waveform exhibits as a system noise. Fig.6 (c) shows the spectrum of the correctly decoded signal, from which one find that it has similar profile as the original DPSK modulated pulse spectra, which indicates the phase has been successfully retrieved after the decoding. Whereas for the incorrectly decoded signal, as shown in Fig.6 (d), the spectrum is quite different from Fig. 6(a) and 6(c), showing that the phase information is lost. There are no coding induced dips in the encoded spectra or waveform that exists in conventional encoding approaches, so it can eliminate the vulnerability of attacking by analyzing the dips.

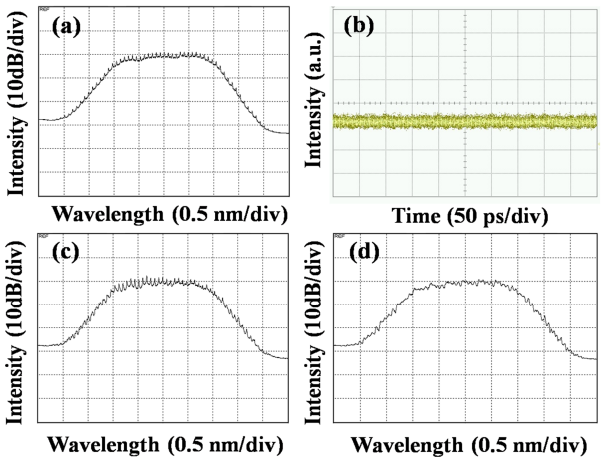

Fig.6 Spectrum (a) and waveform (b) of the stretched pulse; (c) and (d) are the spectrum of the correctly and incorrectly decoded signal, respectively

Fig.7 (a) and 7(d) show the correctly decoded waveform and the corresponding eye diagram after applying the correct OC, both of which have clear eye opening. In contrast, it is impossible for an eavesdropper to sift the DPSK data by using a simple power detector or DPSK demodulator without proper chromatic dispersion compensation and OC. As shown in Fig. 7(b) and 7(e) without proper dispersion, the eavesdropper can only get a noise-like signal. As for Fig.7(c) without proper OC, although the stretched pulses have been compressed, the phase relationship has not been preserved and only noise-like eye diagrams have been achieved, as shown in Fig.7 (f). By using higher dispersive elements, the compressed pulses in Fig.7 (c) can also be overlapped with each other, indicating potential security enhancement based on the time domain bit-by-bit code shifting technique. Fig. 7(g) shows the measured BER for the four types of OCs with different code lengths. Compared with the back-to-back, the transmission and optical en/decoding induce a power penalty within ~2 dB (evaluated at BER=10^{-9}), partially due to the non perfect dispersion compensation and decoding. Error-free transmission over 49km has been achieved for all the OCs.

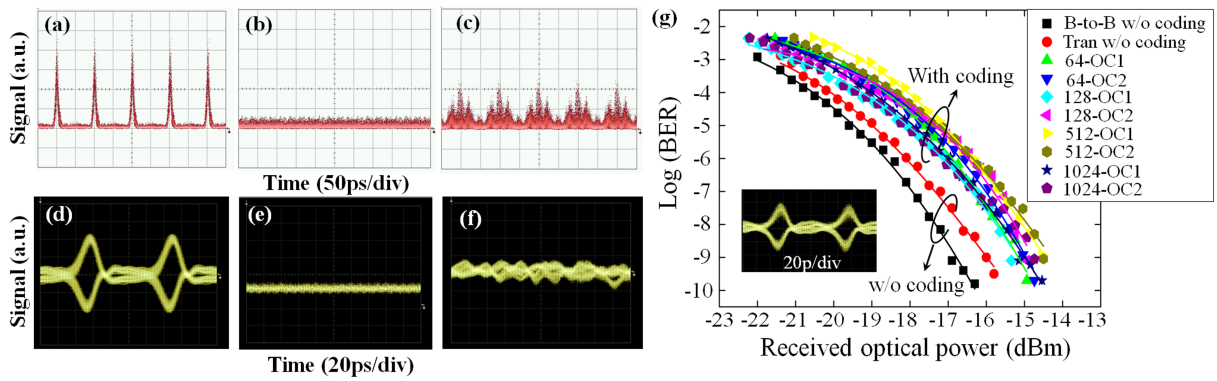

Fig. 7. Waveforms of the decoded signals for (a) with proper dispersion and OC, (b) without proper dispersion and (c) without proper OC. (d)-(f) are the corresponding eye diagrams after DPSK demodulator. (g) BER curves of various OCs.

3.3 Security Improvement of High Speed OOK Data Using Bit-by-Bit Optical Code Shifting Technique

As conventional optical code processing systems employing OOK data modulation is vulnerable to the power detection attack, we further proposed to use the bit-by-bit code shifting technique to enhance OOK data security by introducing significant symbol overlapping for both the encoded and incorrectly decoded noise-like signals. Fig. 8 illustrates the experimental setup [12]. To investigate the security for different bit rates, both 10 Gb/s and 40 Gb/s OOK data are used in the experiment. The 40 GHz pulse train is generated by multiplexing the 10GHz pulses using a four-stage planar lightwave circuit (PLC)-based optical time division multiplexer (OTDM). To generate the 10 Gb/s and 40 Gb/s OOK data, the original pulse train is intensity modulated by a lithium-niobate (LN) intensity modulator driven by 10 Gb/s or 40 Gb/s pseudo-random-bit-sequence (PRBS) of length 2^{11}-1. Then after that, three identical cascaded linearly chirped fiber Bragg gratings (LCFBGs) (each has a 10-dB bandwidth of ~4.7 nm and dispersion slope of ~80ps/nm) are used to significantly broaden the pulse train. Each bit of the original pulse with a bit period of T_b is broadened within the time duration T_s of ~1128ps and hence the adjacent consecutive stretched pulses are significantly overlapped with each other. After the temporal stretching, a 40GHz LN-phase modulator driven by a 40Gchip/s, fast reconfigurable and code-length variable pseudo-random OC with chip duration of T_c is used to perform phase modulation on the stretched pulses which can be regarded as time domain spectral phase encoding. Each stretched pulse will experience a different section of the OC and has a 45-chip spectral phase pattern according to T_s/T_c. At the receiver side, similar configuration as the encoding part is utilized but the phase modulator is driven by the complementary code patterns for spectral phase decoding. The synchronization between the optical encoding and decoding sides is essential for decoding the stretched pulse train. A global clock is used throughout the system and a tunable optical delay line is also employed before the phase modulator to temporally align the complementary spectral phase pattern and the applied OC in the encoding side. After that, another series of LCFBGs with opposite dispersion are used to compress the stretched and spectral phase decoded signal to recover the original pulse. The correctly decoded signal is finally launched into a 10Gb/s or 40Gb/s packet receiver for O-E conversion.).

In the proposed scheme, the OOK data security can be guaranteed by the symbol overlapping of the encoded and incorrectly decoded signal. One may assume that the sophisticated eavesdropper has plenty of resources and knows everything except the OC. However, even if he fabricates identical LCFBGs for temporal compressing the spread pulses, only a cross-correlation signal with significant symbol overlapping can be achieved. If the time duration of the incorrectly decoded signal for each bit is larger than twice the bit period after temporal compressing, the cross-correlation signal may still spread across the time scale with significant symbol overlapping and the bit "0" is filled with the encoded signals from the other bits of "1", so it is difficult for the eavesdropper to discriminate the bit symbol by using a simple power detector. The time duration of the incorrectly decoded signal is mainly determined by the spectral resolution of each chip, which depends on the chromatic dispersion and chip rate R_C.

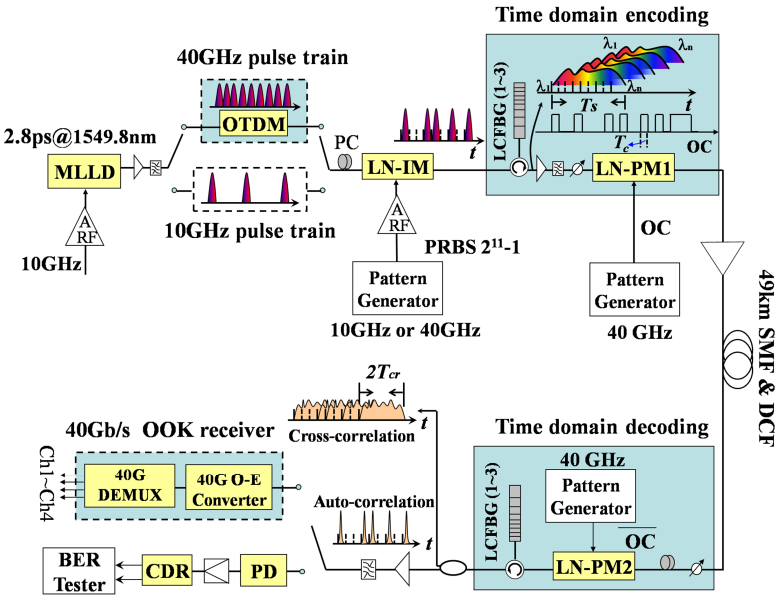

Fig. 8. Experimental setup of the secure OOK optical communication system.

Fig.9 (a)~(b) shows the correctly decoded waveform and corresponding eye diagram for the 40Gb/s OOK pulse train with a 1024-chip OC. Auto-correlation short pulses with high peak power and clear eye opening have been obtained after the correctly decoding. However, as shown in Fig. 9 (c)~(d) using the correct opposite dispersive LCFBGs but incorrect OC, the decoded waveform exhibits as a noise-like signal and no eye opening can be observed in the corresponding eye diagram. It is unable to distinguish the symbol "1" and "0" from the waveform, showing that the eavesdropper cannot easily intercept the data by simple power detection if he has no knowledge of the applied fast reconfigurable, ultra-long OC. Fig.9 (e) ~ (f) show the incorrectly decoded waveform and corresponding eye diagram for R_C of 10Gchip/s. In this case, the symbol "1" and "0" is distinguishable and the eye diagram has opening. This is due to the fact that the time duration for each bit after LCFBGs compressing can generate significant symbol overlapping between the adjacent incorrectly decoded pulses for 40Gchip/s chip rate. While for the R_C of 10Gchip, there is no significant symbol overlapping. Similarly, for the 10Gb/s data rate and 40Gchip/s chip rate, as the time duration for incorrectly decoded signal is smaller than the bit period, it is still possible for the eavesdropper to intercept the data by using power detection even without the OC, as can be seen from the waveform and clear eye diagram shown in Fig. 9 (g)~(h). By further increasing the dispersion and chip rate, security improvement for the 10Gb/s OOK data could also be expected.

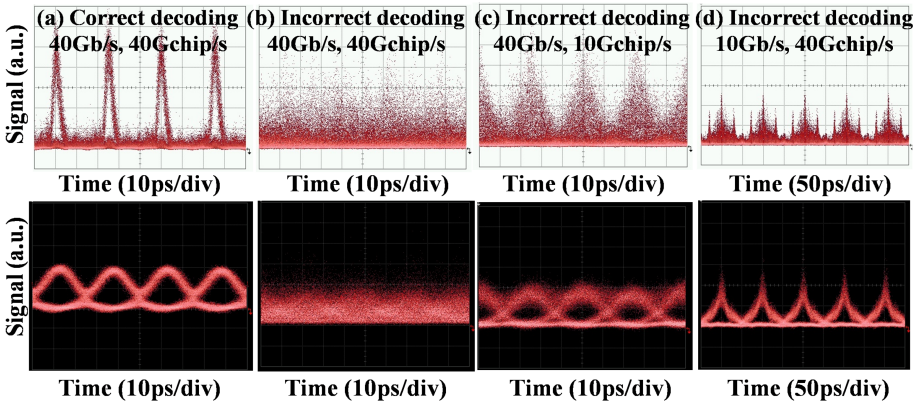

Fig. 9. Waveforms and eye diagrams of (a)~(b) correct and (c)~(d) incorrect decoding for 40Gb/s, 40Gchip/s, and (e)~(f) incorrect decoding for 40-Gb/s, 10-Gchip/s, respectively; (g)~(h) are the incorrectly decoded signals for 10Gb/s, 40Gchip/s.

4. CONCLUSION

In this paper, the advances of using rapid reconfigurable bit-by-bit code scrambling and code shifting technologies for secure optical communication is reviewed. Security improvements for both the OOK and DPSK data modulation formats with various data rates are achieved. The optical code reconfigurable techniques provides an attractive approach for secure optical communication, exhibiting the potential to realize even one time pad.

5. ACKNOWLEDGEMENTS

This work is partly supported by Royal Society International Joint Project. The authors would like to thank H. Sumimoto and Y. Tomiyama of NICT for their technical support in this experiment.

REFERENCES

[1] N. Gisin, and R. Thew, "Quantum Communication," Nature Photon., **1**, 165 (2007).

[2] V. Annovzzi-Lodi, A. Argyris, M. Benedetti, M. Hamacher, S. Merlo, and D. Syvridis, "A chaos-based approach to secure communications," Optics and Photonics News, **19,** 36 (2008).

[3] J. M. Castro, I. B. Djordjevic and D. F. Geraghty, "Novel super structured Bragg gratings for optical encryption," J. lightwave Technol., **24**, 1875 (2006).

[4] M. P. Fok and P. R. Prucnal, "Compact and low-latency scheme for optical steganography using chirped fibre Bragg gratings," Electron. Lett.,**45**, 179 (2009).

[5] Thomas H. Shake, "Security performance of optical CDMA against eavesdropping," J. lightwave Technol., **23**, 655 (2005).

[6] Y. Du, F. Xue, S. J. B. Yoo and Z. Ding, "Security enhancement of SPECTS O-CDMA through concealment against upstream DPSK eavesdropping," J. lightwave Technol., **25**, 2799 (2007).

[7] Z. Jiang, D. E. Leaird and A. M. Weiner, "Experimental investigation of security issues in O-CDMA," J. lightwave Technol., **24**, 4228 (2006).

[8] Z. Si, F. Yin, M. Xin, H. Chen, M. Chen, and S. Xie, "Code extraction from encoded signal in time-spreading optical code division multiple access," Opt. Lett., **35**, 229 (2010).

[9] 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,** 9879 (2010)

[10] X. Wang, Z. Gao, X. H. Wang, N. Kataoka and N. Wada, "Bit-by-bit optical code scrambling technique for secure optical communication," Opt. Express, **19**, 3503 (2011).

[11] Z. Gao, B. Dai, X. Wang, N. Kataoka and N. Wada, "Rapid programmable/code length variable, time domain bit-by-bit code shifting for high speed secure optical communication," Opt. Lett., **36**, 1623 (2011).

[12] Z. Gao, B. Dai, X. Wang, N. Kataoka and N. Wada, "40Gb/s, secure optical communication based upon fast reconfigurable time domain SPE/D with 40Gchip/s optical code and symbol overlapping", Opt. Lett., (to appear)