Rapid programmable/code-length-variable, time-domain bit-by-bit code shifting for high-speed secure optical communication

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

[1]*Joint Research Integrated for Integrated System, Department of Electrical, Electronic & Computer Engineering, Heriot-Watt University, Riccarton, Edinburgh, EH14 4AS, UK*

[2]*Photonic Network Group, National Institute of Information and Communications Technology, Tokyo 184-8795, Japan*

**Corresponding author: x.wang@hw.ac.uk*

Received February 16, 2011; revised March 8, 2011; accepted March 26, 2011;
posted March 30, 2011 (Doc. ID 142578); published April 27, 2011

We propose and experimentally demonstrate a time-domain bit-by-bit code-shifting scheme that can rapidly program ultralong, code-length variable optical code by using only a dispersive element and a high-speed phase modulator for improving information security. The proposed scheme operates in the bit overlap regime and could eliminate the vulnerability of extracting the code by analyzing the fine structure of the time-domain spectral phase encoded signal. It is also intrinsically immune to eavesdropping via conventional power detection and differential-phase-shift-keying (DPSK) demodulation attacks. With this scheme, 10 Gbits/s of return-to-zero-DPSK data secured by bit-by-bit code shifting using up to 1024 chip optical code patterns have been transmitted over 49 km error free. The proposed scheme exhibits the potential for high-data-rate secure optical communication and to realize even one time pad. © 2011 Optical Society of America

OCIS codes: 060.2330, 060.4510, 060.4080, 060.4785, 060.5060.

Information security is an important concern with the increasing use of network resources in modern optical communication systems. In addition to the mathematical algorithm for computational security in a high-level protocol, achieving information security in the optical layer is rather attractive in terms of the hardware-based attacking complexity and the ultrafast all-optical signal-processing-based robustness to electromagnetic signature attacks [1]. Various approaches have been proposed to enhance information security in optical networks [2–4]. Among them, optical-code (OC)-based en/decoding, which has been widely exploited in optical code division multiple access (OCDM) systems is considered a promising technique for providing information security in the optical layer, because the optical pulse exhibits as a noiselike signal after encoding and the eavesdropper cannot recover the original signal and intercept the data without knowledge of the applied OC [5].

Although the OC processing can intuitively prevent the eavesdropper from accessing privacy data, security vulnerability arising from a coding-induced dip in either the time-spreading encoding or spectral phase encoding systems has been reported [6,7]. An eavesdropper can easily extract the OC information by analyzing the fine structure of the encoded spectrum or waveform, and then illegally perform the interception. It has also been pointed out that the security of OC processing is closely related to the data modulation formats [5,6]. The eavesdropper does not need to know the exact OC, but can still access the target data by employing the on–off keying modulation format in simple data-rate power detection [5]. Advanced optical modulation formats, such as differential-phase-shift keying (DPSK) and code-shift keying can overcome this vulnerability since the data bit 0 and bit 1 have identical intensity for these modulation formats. However, as demonstrated in [6], an eavesdropper can use a DPSK demodulator rather than a power detector to directly recover the data from the encoded noiselike signals. Careful analysis reveals that the conventional approach of 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 a different OC for each bit, information security could be dramatically enhanced. An M-ary encoding method that assigns different OCs for different sequences of $\log_2 M$ bits has been demonstrated [8].

Recently, we proposed a time-domain spectral phase en/decoding scheme that utilizes two opposite dispersive elements and a high-speed phase modulator for OCDM applications [9]. This scheme is very flexible in rapidly reconfiguring the optical code and is compatible with fiber-optic systems. We further proposed a simultaneous bit-by-bit OC scrambling and DPSK data modulation technique for secure optical communication based on this scheme [10], in which each bit can be assigned a different OC; thus, the security can be significantly enhanced. However, the data rate and code length are greatly limited by the electronic processing technology, and only a relatively low data rate of 2.5 Gbits/s and an eight-chip code length were demonstrated.

In this Letter, we propose and demonstrate a rapid programmable and code-length variable bit-by-bit code-shifting technique operated in the bit overlap regime with the capability of supporting a high data rate of 10 Gbits/s and code length of up to 1024 for enhancing information security. Figure 1 illustrates the principle of the proposed technique. A phase-shift-keying modulation format is employed in this scheme, as shown in Fig. 1(a), with a return-to-zero (RZ)-DPSK data format. The ultrashort data pulse is stretched by a highly dispersive element in the time domain and each bit of the stretched pulse occupies T_s time duration as a result of 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, ultralong code-length-variable OC with chip duration of T_c

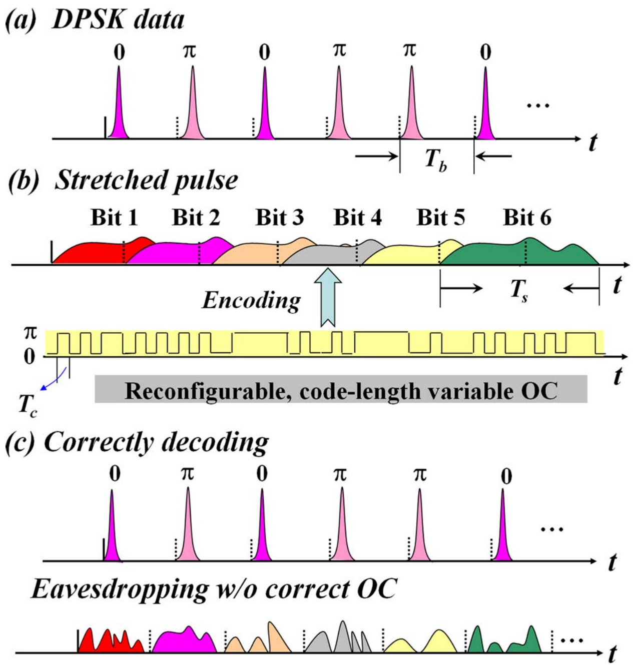

Fig. 1. (Color online) Principle of the proposed bit-by-bit code-shifting scheme. (a) Original DPSK data, (b) bit-by-bit code-shifting after pulse stretching, and (c) correctly decoded signal and eavesdropper-intercepted signal without correct OC.

is applied onto the overlapped pulses to perform time-domain spectral phase encoding, as shown in Fig. 1(b). By using a long pseudorandom OC, each stretched pulse can experience a 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 as bit-by-bit code shifting. In this scheme, the OC could have an unprecedented code length and thus a large code space. Note that the encoding process is completely data-rate independent and there is no specific requirement for the dispersion value as long as the $T_s > T_b$ is satisfied. For achieving a 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 an autocorrelation signal with high peak power, as shown in Fig. 1(c). An eavesdropper that is able to intercept the DPSK data would have to know both the chromatic dispersion and the applied ultralong 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 noiselike 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.

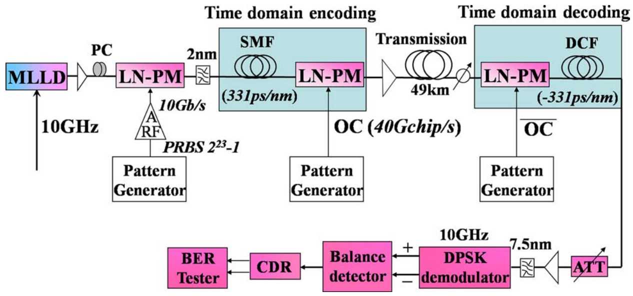

Fig. 2. (Color online) Experimental setup of the proposed time-domain bit-by-bit code-shifting scheme.

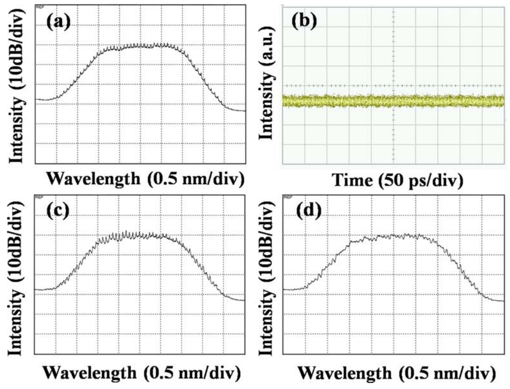

Fig. 3. (Color online) (a) Spectrum and (b) waveform of the stretched pulse after the dispersive SMF; (c) and (d) are the spectra of the correct and incorrect decoded signals, respectively.

Figure 2 shows the schematic diagram of the proof-of-principle experimental setup. A 10 GHz mode-locked laser diode (MLLD) producing ~2.8 ps pulses at 1550.75 nm is modulated at 10 Gbits/s by a lithium niobate phase modulator (LN-PM) driven by a $2^{23} - 1$ pseudorandom bit sequence. A span of single-mode fiber (SMF) with dispersion of ~331 ps/nm is used to significantly broaden the pulse train. To reduce the dispersion mismatch caused by the nonideal dispersion compensation in the receiver, an optical bandpass filter with 3 dB bandwidth of ~2 nm is employed before the SMF. Because of the high chromatic dispersion, each bit of the original pulse is stretched into an ~662 ps time duration and, thus, the adjacent consecutive pulses significantly overlap each other. After the temporal stretching, a 40 GHz LN-PM driven by the reconfigurable 40 Gchip/s, code-length variable OC is used to perform the time-domain spectral phase encoding. Different stretched pulses will thus experience an effective ~26 chip spectral phase pattern according to the T_s/T_c. Four different kinds of OC, each with two gold codes, with code lengths of 64 chips, 128 chips, 512 chips, and 1024 chips are used in the demonstration. A piece of ~49 km dispersion-compensated fiber (DCF) is used for transmission. For time-domain spectral phase decoding, a configuration

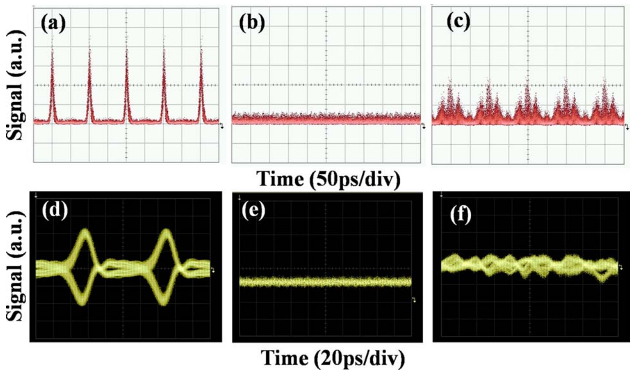

Fig. 4. (Color online) Waveforms of the decoded signals (a) with proper dispersion and OC, (b) without proper dispersion, and (c) without proper OC. (d)–(f) are the corresponding eye diagrams after the DPSK demodulator for (a)–(c).

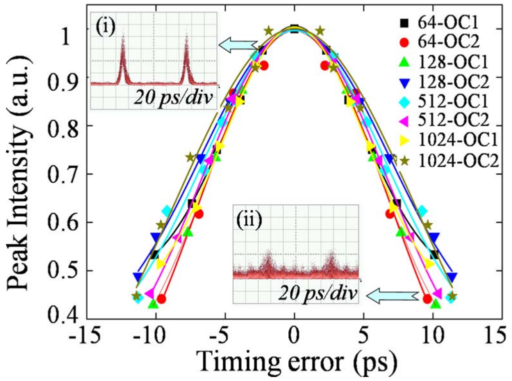

Fig. 5. (Color online) Peak intensity of the decoded pulse versus timing error for different kinds of OC.

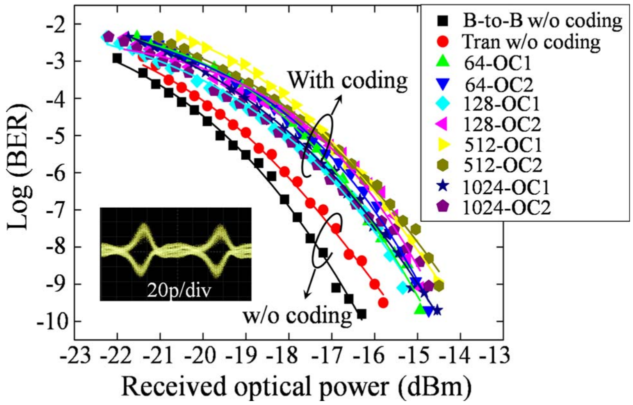

Fig. 6. (Color online) BER curves of the secure DPSK data with various OCs.

similar to that of the encoding is utilized, but the PM is driven by the complementary OC, and a span of DCF with opposite dispersion of approximately −331 ps/nm is used to compress the spectral phase decoded signal in order to retrieve the original pulse. The correctly decoded pulses are finally directed into a DPSK demodulator with a one-bit delay ($\sim$100 ps) interferometer followed by a balanced detector to recover the DPSK data for bit-error-rate (BER) measurement.

Figures 3(a) and 3(b) show the spectrum and the waveform of the stretched 10 Gbits/s RZ-DPSK pulse train after the dispersive SMF. It can be seen that the data pulse has been significantly stretched in the time domain and the adjacent pulses overlap each other, so the waveform exhibits as system noise. Figure 3(c) shows the spectrum of the correctly decoded signal, which has a profile similar to that of the original DPSK data modulated spectrum, which indicates the phase has been successfully retrieved after the decoding. However, for the incorrectly decoded signal, as shown in Fig. 3(d), the spectrum is quite different from Figs. 3(a) and 3(c), showing that the phase information is lost. There are no coding-induced dips in the encoded spectra or waveform that exist in conventional encoding approaches, so it can eliminate the vulnerability to attack by analyzing the dips.

Figures 4(a) and 4(d) show the correctly decoded waveform and the corresponding eye diagram after applying the correct OC, both of which have clear eye openings. In contrast, it is impossible for an eavesdropper to sift the DPSK data by using a simple power detector or DPSK demodulator without the proper chromatic dispersion compensation and OC. As shown in Figs. 4(b) and 4(e) without proper dispersion, the eavesdropper can get only a noiselike signal. As for Fig. 4(c), without the proper OC, although the stretched pulses have been compressed, the phase relationship has not been preserved and only noiselike eye diagrams have been achieved, as shown in Fig. 4(f). By using higher dispersive elements, the compressed pulses in Fig. 4(c) can also be overlapped with each other, indicating potential security enhancement based on the proposed time-domain bit-by-bit code-shifting technique. Synchronization between the optical encoding and decoding sides is quite essential to recover the original data pulses and improve security. Figure 5 shows the measured peak intensity reduction of the decoded pulses versus the timing error between the en/decoding sides for different OCs, from which one can see that, as the timing error increases to approximately ±10 ps, the normalized peak intensity degrades from 1 to 0.4, as shown in insets (i) and (ii) of Fig. 5, in which case, the decoded pulses gradually submerge in the noiselike background and no BER can be measured. A tunable optical delay line with a resolution of 0.2 ps is employed before the PM in the decoding side to temporally align the complementary spectral phase pattern with the encoding OC to guarantee the decoding performance. Synchronization is much easier to achieve than in the previously proposed bit-by-bit OC scrambling scheme in the experiment [10]. Figure 6 shows the measured BER for the four types of OC with different code lengths. Compared with the back-to-back case, the transmission and optical en/decoding induce a power penalty within $\sim$2 dB (evaluated at BER $= 10^{-9}$), partially due to imperfect dispersion compensation and decoding. Error-free transmission over 49 km has been achieved for all the OCs.

We have proposed and experimentally demonstrated a time-domain bit-by-bit code-shifting scheme that allows us to rapidly program a code-length-variable ultralong OC for enhancing information security. This scheme requires only conventional dispersive elements and PMs and exhibits the potential to operate at higher data rates and to realize even one time pad by increasing the code length for secure optical communication.

References

1. P. R. Prucnal, M. P. Fok, Y. Deng, and Z. Wang, Proc. SPIE **7632**, 76321M (2009).
2. A. Argyris, D. Syvridis, L. Larger, V. Annovazzi-Lodi, P. Colet, I. Fisher, J. Garcia-Ojalvo, C. R. Mirasso, L. Pesquera, and K. A. Shore, Nature **438**, 343 (2005).
3. J. M. Castro, I. B. Djordjevic, and D. F. Geraghty, J. Lightwave Technol. **24**, 1875 (2006).
4. Y. Du, F. Xue, S. J. B. Yoo, and Z. Ding, J. Lightwave Technol. **25**, 2799 (2007).
5. T. H. Shake, J. Lightwave Technol. **23**, 655 (2005).
6. Z. Jiang, D. E. Leaird, and A. M. Weiner, J. Lightwave Technol. **24**, 4228 (2006).
7. Z. Si, F. Yin, M. Xin, H. Chen, M. Chen, and S. Xie, Opt. Lett. **35**, 229 (2010).
8. T. Kodama, N. Nakagawa, N. Kataoka, N. Wada, G. Cincotti, X. Wang, T. Miyazaki, and K. Kitayama, J. Lightwave Technol. **28**, 181 (2010).
9. X. Wang and N. Wada, Opt. Express **15**, 7319 (2007).
10. X. Wang, Z. Gao, X. H. Wang, N. Kataoka, and N. Wada, Opt. Express **19**, 3503 (2011).