Experimental investigation of security issues in OCDMA: a code-switching scheme

D.E. Leaird, Z. Jiang and A.M. Weiner

Spectrally phase coded OCDMA with a modulation format based on switching between two codes is demonstrated. The code switching data modulation format enhances security compared to on-off keying by eliminating a vulnerability to eavesdropping based on a simple energy detector.

Introduction: Optical code-division multiple-access (OCDMA) is receiving increasing attention with several groups pushing to realise ~Gbit/s multi-user demonstrations [1–8]. Among other possible advantages provided by OCDMA, its potential for enhanced information security is frequently mentioned. This is plausible at first glance considering the OCDMA encoded signal manifests itself as noise-like waveforms that may not be accessible to an eavesdropper without knowledge of the applied code; however, this argument is worth deeper thought. Our group has previously demonstrated there is no security at all in OCDMA for a single-user system employing on-off keying (OOK) [1]. This is due to the fact that, for an OOK system, although the encoded waveform is noise-like on an ultrafast time scale, it can be detected using a simple energy detector without any knowledge of the spectral code. For example, the energy detector could be a standard receiver bandwidth limited to the bit rate which is unable to resolve the fine structure of the noise-like waveforms but integrates the energy in a bit period. Fig. 1 confirms this argument in a 10 Gbit/s spectrally phase coded system. Fig. 1*a* shows the properly decoded waveforms seen by an authorised user, which are recovered back to a short pulse as desired (intensity cross-correlation). When detected by a 20 GHz photodiode, a clear eye diagram is observed as expected. Fig. 1*b* shows the encoded noise-like waveform (intensity cross-correlation), which is distinct from a short pulse on an ultrafast time scale. However, using the 20 GHz photodiode, a similarly clear eye diagram is still observed, which could be detected by an eavesdropper with no knowledge of the code. This clearly shows that there is no security at all for such OOK single-user OCDMA systems. On the other hand, even in a multi-user network environment, there are typically still fibre links where only a single user exists and which are therefore vulnerable as pointed out by a recent systematic theoretical study on security issues in OCDMA [9, 10]. In [9, 10], a code-switching scheme is proposed, which may provide enhanced security in OCDMA. In this Letter, we experimentally demonstrate for the first time to our knowledge this code-switching scheme for spectrally phase coded OCDMA.

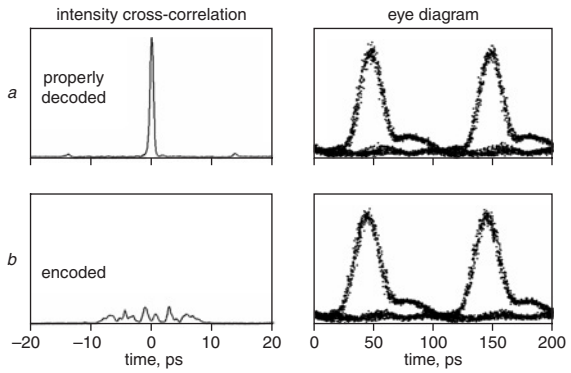

Fig. 1 *Vulnerability illustration for OCDMA system*

a For authorised user, properly decoded short pulse shows clear eye diagram
b For malicious eavesdropper, encoded noise-like waveform still shows clear eye diagram
Pulses measured by intensity cross-correlation. Eye diagrams measured using 20 GHz bandwidth photodiode at 1.5 μm and sampling scope

Experiments and results: A schematic diagram of the code-switching scheme is shown in Fig. 2. An actively modelocked fibre laser followed by a dispersion decreasing fibre soliton compressor producing nearly transform-limited ~0.4 ps pulses at ~10 GHz centred near 1542 nm is used as the pulse source. A coupler is used to generate two arms in a complementary modulator geometry to achieve code-switching. Each arm is equipped with an intensity modulator employing OOK and driven by the same 10 Gbit/s PRBS $2^{31} - 1$ data stream, but data and data bar are assigned to the two arms, respectively. The data-modulated ultra-short pulses are input into fibre coupled Fourier transform pulse shapers [11] which incorporate 128 element liquid crystal modulator arrays to spectrally phase code the spectrum of the source laser. Two different codes (here length 31 *M*-sequence codes) are applied to the two arms to realise code switching. To achieve high quality code-switching, care is taken to match the average power and fibre length in each arm. After combining the two arms, bits '1' and '0' are occupied by two distinct but equal energy noise-like waveforms encoded according to code 1 and code 2, respectively. The receiver consists of a fibre coupled Fourier transform pulse shaper used to decode the authorised user, a highly sensitive fibre pigtailed periodically-poled lithium niobate (PPLN) waveguide chip to perform the second-harmonic generation (SHG) nonlinear discrimination function [1, 2, 12], and a photodiode operating at the SHG wavelength of 0.77 μm adapted from 10 Gbit/s Ethernet. The measured SHG efficiency of PPLN is 3.1%/mW for continuous wave (CW) and 170%/pJ for ultra-short pulses. Dispersion compensating fibre is used to compensate for the dispersion of the fibre link. For the purposes of this demonstration it is assumed that an eavesdropper could tap into the fibre link somewhere after the complementary modulator but before the decoder.

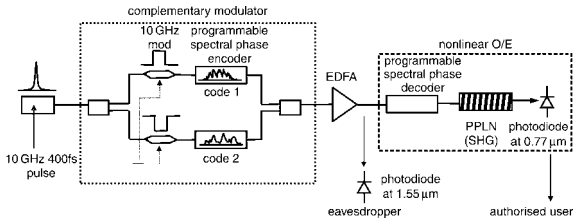

Fig. 2 *Code-switching experimental setup*

For an eavesdropper using an energy detector, here a 20 GHz bandwidth photodiode at 1.5 μm, the eye diagram is clear for single arm (traditional single user OCDMA) and there is no security at all, as shown in Fig. 1*b*. Fig. 3*a* shows the detected waveforms for the code-switching scheme observed by an eavesdropper also using a simple energy detector. There is no eye diagram at all since both bits '1' and '0' are occupied by encoded waveforms, which demonstrates the ability to enhance security through the code-switching scheme. As a result, the information is concealed by the code-switching scheme to resist a simple interception from a malicious eavesdropper.

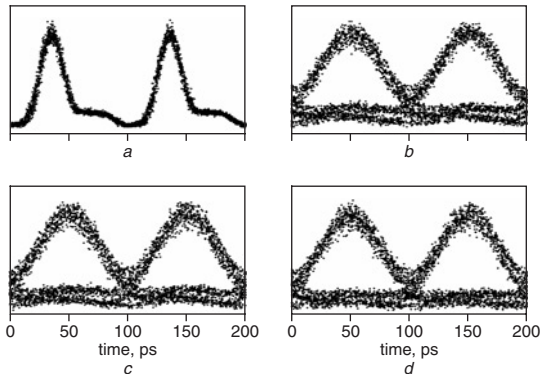

Fig. 3 *Eye diagrams*

a For eavesdropper after complementary modulator (there is no eye)
b For authorised user
c For authorised user with 2.5 Gbit/s modulated interference user using OOK
d For authorised user with unmodulated interference user

On the other hand, it is important to show that the code-switching scheme still works for the authorised user using conventional OCDMA detection: decoded by a decoder, discriminated by the PPLN, and detected by the photodiode at 0.77 μm [1, 2]. For the code-switching scheme, the decoder is set as code 1. After the decoder, bit '1' is properly decoded back to a short pulse to drive the PPLN to high SHG yield; while bit '0' is improperly decoded, remaining a noise-like waveform, and the SHG yield is suppressed. As a result, a clear eye diagram is observed as shown in

Fig. 3*b*. To go one step further, Fig. 3*c* shows the authorised user eye diagram when an interference user modulated at 2.5 Gbit/s with OOK is added after the complementary modulator and prior to the EDFA. Fig. 3*d* shows the authorised user eye diagram when an unmodulated interference user is added – to emulate an interference user also with a code-switching scheme since all bits of the unmodulated interference user are occupied by noise-like waveforms after the decoder. Note that a slot-level timing co-ordination scheme is applied to separate the authorised user and interference user by ~50 ps to avoid beat noise caused by their interaction [1, 2]. The clear eye diagrams in Figs. 3*b–d* demonstrate that the code-switching scheme still works for the authorised user using conventional OCDMA detection and the interference user is well suppressed.

Conclusions: For the first time to our knowledge, we have demonstrated spectrally phase coded O-CDMA with a modulation format based on switching between two codes. As suggested in [9, 10], the code switching data modulation format enhances security compared to on-off keying by eliminating the vulnerability to eavesdropping based on a simple energy detector. We note, however, that our work does not preclude the possibility of vulnerability to eavesdropping strategies that exploit other structures in the coding and signalling scheme. Investigation into other such eavesdropping vulnerabilities is a subject of our ongoing work.

Acknowledgments: This material is based upon work supported by DARPA under grant MDA972-03-1-0014. The authors acknowledge R. V. Roussev, C. Langrock and M. M. Fejer for providing the PPLN device and D. S. Seo's work in constructing the laser.

 19 May 2005
Electronics Letters online no: 20051830
doi: 10.1049/el:20051830

D.E. Leaird, Z. Jiang and A.M. Weiner (*Purdue University, 465 Northwestern Ave., West Lafayette, IN 47907-2035, USA*)

E-mail: zjiang@purdue.edu

References

1 Jiang, Z., Seo, D.S., Yang, S.-D., Leaird, D.E., Roussev, R.V., Langrock, C., Fejer, M.M., and Weiner, A.M.: 'Four user, 2.5 Gb/s, spectrally coded O-CDMA system demonstration using low power nonlinear processing', *J. Lightwave Technol.*, 2005, **23**, (1), pp. 143–158
2 Jiang, Z., Seo, D.S., Yang, S.-D., Leaird, D.E., Roussev, R.V., Langrock, C., Fejer, M.M., and Weiner, A.M.: 'Four user, 10 Gb/s spectrally phase coded O-CDMA system operating at ~30 fJ/bit', *IEEE Photonics Technol. Lett.*, 2005, **17**, (3), pp. 705–707
3 Etemad, S., Toliver, P., Menendez, R., Young, J., Banwell, T., Galli, S., Jackel, J., Delfyett, P., Price, C., and Turpin, T.: 'Spectrally efficient optical CDMA using coherent phase-frequency coding', *IEEE Photonics Technol. Lett.*, 2005, **17**, (4), pp. 929–931
4 Cong, W., Scott, R.P., Hernandez, V.J., Li, K., Heritage, J.P., Kolner, B.H., and Yoo, S.J.B.: 'High performance 70 Gbit/s SPECTS optical-CDMA network testbed', *Electron. Lett.*, 2004, **40**, (22), pp. 1439–1440
5 Teh, P.C., Ibsen, M., Lee, J.H., Petropoulos, P., and Richardson, D.J.: 'Demonstration of a four-channel WDM/OCDMA system using 255-chip 320-Gchips/s quaternary phase coding gratings', *IEEE Photonics Technol. Lett.*, 2002, **14**, (2), pp. 227–229
6 Sotobayashi, H., Chujo, W., and Kitayama, K.: 'Highly spectral-efficient optical code-division multiplexing transmission system', *IEEE J. Sel. Top. Quantum Electron.*, 2004, **10**, (2), pp. 250–258
7 Wang, X., Wada, N., Hamanaka, T., Kitayama, K., and Nishiki, A.: '10-user, truly-asynchronous OCDMA experiment with 511-chip SSFBG en/decoder and SC-based optical thresholder'. 2005 Optical Fiber Communication Conf. (OFC'05), Anaheim, CA, 2005, Paper PDP33
8 Baby, V., Glesk, I., Runser, R.J., Fischer, R., Huang, Y.K., Bres, C.S., Kwong, W.C., Curtis, T.H., and Prucnal, P.R.: 'Experimental demonstration and scalability analysis of a four-node 102-Gchip/s fast frequency-hopping time-spreading optical CDMA network', *IEEE Photonics Technol. Lett.*, 2005, **17**, (1), pp. 253–255
9 Shake, T.H.: 'Security performance of optical CDMA against eavesdropping', *J. Lightwave Technol.*, 2005, **23**, (2), pp. 655–670
10 Shake, T.H.: 'Confidentiality performance of spectral-phase-encoded optical CDMA', *J. Lightwave Technol.*, 2005, **23**, (4), pp. 1652–1663
11 Weiner, A.M.: 'Femtosecond pulse shaping using spatial light modulators', *Rev. Sci. Instrum.*, 2000, **71**, (5), pp. 1929–1960
12 Roussev, R.V., Langrock, C., Kurz, J.R., and Fejer, M.M.: 'Periodically poled lithium niobate waveguide sum-frequency generator for efficient single-photon detection at communication wavelengths', *Opt. Lett.*, 2004, **29**, (13), pp. 1518–1520