Experimental Investigation of Security Issues in O-CDMA

Zhi Jiang, *Student Member, IEEE*, Daniel E. Leaird, *Senior Member, IEEE*, and
Andrew M. Weiner, *Fellow, IEEE, Fellow, OSA*

***Abstract*—In this paper, two vulnerabilities that allow an eavesdropper to extract data from an isolated user in a two-code-keying spectrally phase-coded optical-code-division-multiple-access (O-CDMA) system are experimentally demonstrated. One of these vulnerabilities stems from spectral dips that result from phase-to-amplitude conversion in the encoding process, which allows eavesdropping by using a narrowband tunable optical filter and a simple energy detector. A modified O-CDMA transmitter scheme that masks this vulnerability is demonstrated. A second, especially serious, vulnerability allows eavesdropping by using a differential-phase-shift-keying receiver. Both of these vulnerabilities arise from a structure in the coding and signaling schemes that allow an eavesdropper to recover data, with relatively simple hardware and without attempting to learn the codes.**

***Index Terms*—Differential phase shift keying (DPSK), fiber optics communications, optical code-division multiple access (O-CDMA), security.**

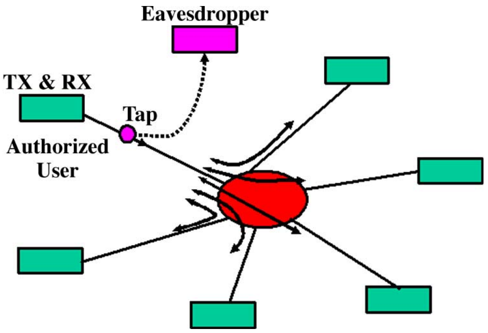

Fig. 1. Vulnerability illustration in the upstream traffic in a star network. (Color version available online at http://www.ieeexplore.ieee.org.)

I. Introduction

TIME-DIVISION multiplexing and wavelength-division multiplexing have been extensively explored and utilized in optical communication systems. Alternatively, optical code-division multiple access (O-CDMA) is receiving increased attention recently. In O-CDMA, different users whose signals may be overlapped both in time and frequency share a common communications medium; multiple access is achieved by assigning different minimally interfering code sequences to different O-CDMA transmitters. In many O-CDMA approaches, input ultrashort pulses are time-spread during the encoding process into lower intensity noiselike signals. In the receiver, data corresponding to a desired user is separated from multiaccess interference (MAI) via a matched filtering (decoding) operation, in which properly decoded signals are converted back to the original pulselike signals, while improperly decoded signals remain low-intensity noiselike temporally broadened waveforms. Multiuser ~Gb/s O-CDMA systems have been demonstrated by several groups [1]–[8], including our own previous demonstrations of O-CDMA systems utilizing reconfigurable spectral phase coding and low-power nonlinear waveform discrimination [1], [2].

The potential provided by O-CDMA for enhanced information security is frequently mentioned in addition to other possible advantages such as simplified and decentralized network control, improved spectral efficiency, and increased flexibility in the granularity of bandwidth that can be provisioned. This is plausible at first glance considering that, frequently, the O-CDMA encoded signal manifests itself as a noiselike waveform that may not be accessible to an eavesdropper without knowledge of the applied code. Therefore, for a properly configured system, an eavesdropper may potentially experience a significant disadvantage in signal to noise ratio compared to the authorized O-CDMA receiver. However, this argument is worth deeper consideration. It has been noted [9] and experimentally demonstrated [1] that there is no security at all in spectrally phase-coded O-CDMA for a single-user system employing ON–OFF keying (OOK). This is due to the fact that, for an OOK system, although the encoded waveform is noiselike 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 noiselike waveforms, but integrates the energy in a bit period. As a result, although on an ultrafast time scale the noiselike coded waveform is very different from the properly decoded short pulses, it still shows a clear eye diagram, which could be detected by an eavesdropper with no knowledge of the code. Therefore, there is no security at all for such OOK single-user O-CDMA systems. On the other hand, even in a multiuser network environment, typically, there are still fiber links where only a single user exists (for example, the upstream traffic in a star network, as shown in Fig. 1), as pointed out by a recent systematic theoretical study on security issues in O-CDMA [10], [11]. In this case, eavesdropping can be easily accomplished using a simple energy detector if an OOK data-modulation

Manuscript received February 4, 2006; revised July 10, 2006. This work was supported by the Defense Advanced Research Projects Agency under Grants MDA972-03-1-0014 and W911NF-05-1-0237.

The authors are with the School of Electrical and Computer Engineering, Purdue University, West Lafayette, IN 47907 USA (e-mail: zjiang@purdue.edu; leaird@purdue.edu; amw@purdue.edu).

Digital Object Identifier 10.1109/JLT.2006.883661

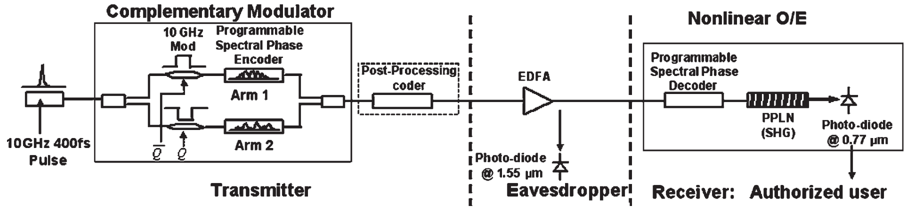

Fig. 2. Experimental setup to investigate vulnerability from coding-induced spectral dips.

format is used, as pointed out above. The study in [10] and [11] suggests that the vulnerability to eavesdropping can be reduced for a data-modulation format based on switching between two-code words (in the following, we refer to this as code switching or two-code keying). It is also suggested that spectral phase coding is one of the more promising approaches for O-CDMA from a security perspective, due to the large code space.

The theoretical study in [10] and [11] concentrates on paths with isolated single users, which are the most vulnerable, and analyzes the probability that the eavesdropper can fully and precisely determine the O-CDMA code. Specific eavesdropping detector structures are presented to illustrate the possibility of the eavesdropper breaking the security of spectral phase-coded signals by directly measuring the code words. The proposed hardware approach for eavesdropping is more complex from the practical implementation perspective but, in principle, should be possible. The analysis shows that the probability of full code determination depends on the signal-to-noise ratio, considering the energy at the eavesdropper per chip (as opposed to the full energy integrated over the spectral code). The study in [10] and [11] also shows that the probability of full code interception increases rapidly if the eavesdropper is able to integrate measurement results over multiple repetitions of the code word (i.e., over multiple data bits) but point out that such integration will likely be precluded for a two-code-keying spectrally phase-coded O-CDMA system.

In our laboratory, we have recently implemented a code-switching scheme for spectrally phase-coded O-CDMA experimentally [12]. Our experiments demonstrate that the code-switching data-modulation format enhances security compared to OOK by eliminating the vulnerability to eavesdropping based on a simple energy detector, as suggested in [10] and [11]. We noted, however, that our work in [12] did not preclude the possibility of vulnerability to eavesdropping strategies that exploit the other structure in the coding and signaling scheme. In this paper, we investigate and experimentally demonstrate simple vulnerabilities not previously reported that allow eavesdropping of data from an isolated user on a two-code-keying spectrally phase-coded O-CDMA system. These vulnerabilities allow data recovery with simple hardware and without the need for any attempt to learn the code.

Before going into experimental details, we would like to clarify the meaning of security in O-CDMA within the general framework of security study in the literature. Although there are unconditionally secure systems (e.g., quantum key distribution systems), no classical communication system will ever be unconditionally secure. Most practical systems fall into the category of computationally secure, which is defined as requiring a sufficiently large amount of computation time and resources to break it [10]. The theoretical security study in [10] and [11], focusing on determining the O-CDMA code, is considered as a study of computational security in O-CDMA systems. In this paper, we investigate simple vulnerabilities even without searching the code space, implying that O-CDMA may not even be computationally secure.

In Section II of this paper, we demonstrate a vulnerability arising from coding-induced spectral dips (phase-to-amplitude conversion) that allow eavesdropping with a receiver consisting only of a tunable optical filter and a simple energy detector. We also demonstrate a modified phase-coding scheme that can successfully mask this vulnerability. In Section III, we demonstrate a vulnerability to an eavesdropper equipped with a differential phase shift keying (DPSK) demodulator. This vulnerability is particularly serious because the eavesdropper can exploit the full energy of the tapped signal integrated over the entire spectral range, even without any knowledge of the code, in order to obtain high signal-to-noise ratio. In Section IV, we conclude.

II. Vulnerability From Coding-Induced Spectral Dips

A schematic diagram of the code-switching scheme is shown in Fig. 2. An actively mode-locked fiber laser ($\sim$3 ps), followed by a dispersion decreasing fiber soliton compressor producing nearly transform-limited $\sim$0.4 ps pulses at 10 GHz repetition rate centered 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-Gb/s pseudo random bit sequence (PRBS) $2^{31} - 1$ data stream, but data and data bar are assigned to the two arms, respectively. The data-modulated ultrashort pulses are input into fiber-coupled Fourier-transform pulse shapers [13] 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 realize code switching. In order to achieve high-quality code switching, care is taken to match the average power and fiber length in each arm. After combining the two arms, bits “1” and “0” are occupied by two distinct but equal energy noiselike waveforms encoded according to codes 1 and 2, respectively. An additional pulse shaper can be used as a postprocessing coder to enhance the security, as will be discussed later. The receiver consists of a pulse shaper used to decode the authorized user, a highly sensitive fiber pigtailed periodically poled lithium niobate (PPLN) waveguide chip [14] used to perform the second harmonic

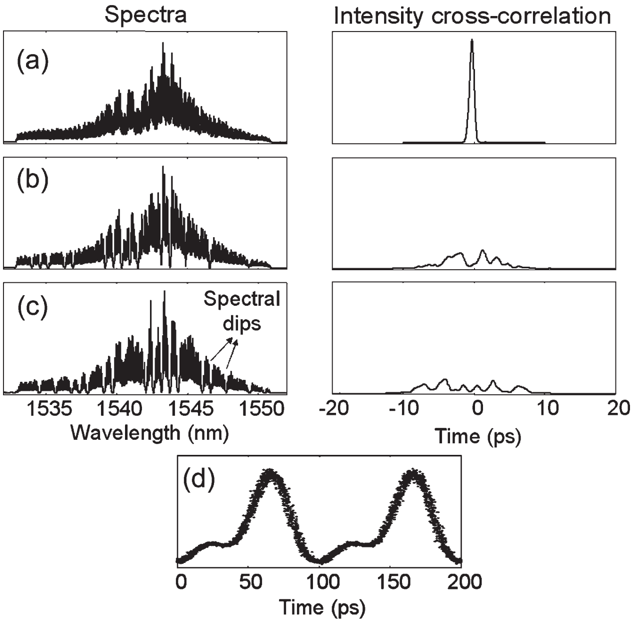

Fig. 3. Spectra and corresponding intensity cross correlation of (a) uncoded; (b) coded arm 1; and (c) coded arm 2. (d) Waveform of the combined signals measured by photodetector and sampling scope.

generation (SHG) nonlinear discrimination function [1], [2], and a photo-diode operating at the SHG wavelength of 0.77 μm adapted from 10-Gb/s Ethernet. This is the same receiver structure we used in our previous O-CDMA studies employing OOK. For two-code-keying operation, this ideally converts one of the desired transmitter codes to a high output level, while converting the second code from the desired transmitter, as well as any O-CDMA MAI signals, to a low output level. In principle, a two-code-keying receiver consisting of a splitter and a pair of parallel decoders (matched to the two respective transmit waveforms) and SHG chips, followed by a differencing operation, might offer more optimal performance, but this was not implemented in our experiments. For the purposes of this demonstration, it is assumed that an eavesdropper could tap into the fiber link somewhere after the complementary modulator (and postprocessing coder) but before the decoder.

For an eavesdropper using an energy detector (here a 20-GHz bandwidth photo-diode at 1.5 μm), the eye diagram is clear for a single arm (traditional single-user O-CDMA), and as discussed, there is no security at all [1], [12], but for the code-switching scheme, there is no eye diagram at all with such a simple energy detector since both bits "1" and "0" are occupied by encoded waveforms [12]. In this sense, the security is enhanced since the information is concealed by the code-switching scheme to resist simple interception from a malicious eavesdropper. Fig. 3(a) shows the uncoded spectrum and corresponding intensity cross-correlation measurement, which is ~400-fs short pulse. Fig. 3(b) and (c) shows the coded spectra of the two arms in the code-switching scheme, which are measured individually by blocking the opposite arm. The short pulses are broadened to noiselike waveforms after encoding. Although noiselike waveforms are distinct from each other between two arms on an ultrafast time scale due to different codes, an energy detector, which could be a standard receiver bandwidth-limited to the bit rate, is unable to resolve the fine structure of the noiselike waveforms but integrates the energy in a bit period. As a result, bits "1" and "0," represented by these two waveforms from two arms, cannot be distinguished using such a detector. Fig. 3(d) shows the time-domain waveform of the combined signals detected by the photo-diode and measured by a sampling scope, which confirms that there is no eye diagram in the code-switching scheme.

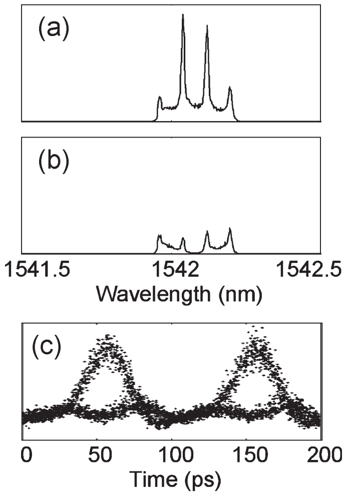

Fig. 4. Spectra of (a) arm 1 without a dip and (b) arm 2 with a dip filtered by a narrow-bandpass filter in the vicinity of 1542 nm. (c) Waveforms.

However, for the spectrally phase-coded O-CDMA investigated by several groups, including our own [1]–[4], [11], the coding process will generate spectral dips, as shown in Fig. 3(a) and (b). This phenomenon results from diffraction effects experienced by frequency components falling at transitions in the spectral phase code [15]. This effect is not due to practical imperfections; it is expected for fundamental reasons and has been explained quantitatively in [15]. In the spectral phase-coding process, the frequency components of each chip are phase shifted by zero or π according to the length-31 M-sequence codes. Therefore, each spectral dip marks a phase transition. From the measured spectral data, one can easily recover the codes according to this principle. Other (relatively complicated) methods have also been proposed for an eavesdropper to measure the code [10], [11]. Here, we show that the spectral dips lead to structure in the signals that can be exploited directly for eavesdropping in a simple way. For the code-switching scheme, clear spectral measurements for individual arms become somewhat difficult since two differently coded spectra are combined together. However, one can recover the data by simply scanning a narrow-bandpass optical filter across the combined spectra, even without measuring the code. At the spectral positions where one arm has a dip while the other arm does not, there is a power difference between them. Such power difference will generate eye diagrams, which are similar to an OOK signal from a single arm. Fig. 4 shows such an example. In the vicinity of 1542 nm, there is no dip for arm 1 but a dip for arm 2 on the coded spectra, as shown in Fig. 4(a) and (b). We use a high-resolution pulse shaper [16] as a tunable narrow-bandpass filter to achieve this discrimination, where four spectral lines (separated at 10 GHz—the repetition rate) are filtered out. As expected, an eye diagram, shown

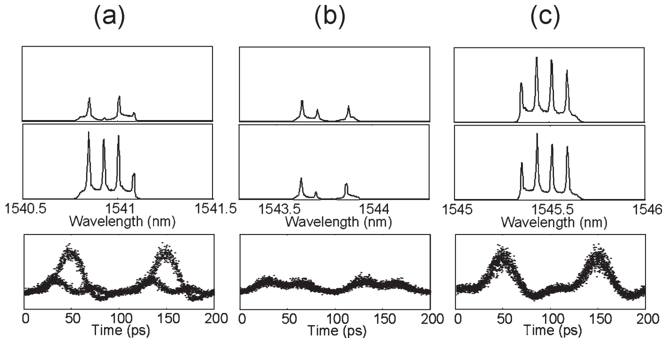

Fig. 5. Spectra and waveforms measurement. (a) Arm 1 with a dip and arm 2 without a dip. (b) Both with a dip. (c) Both without a dip.

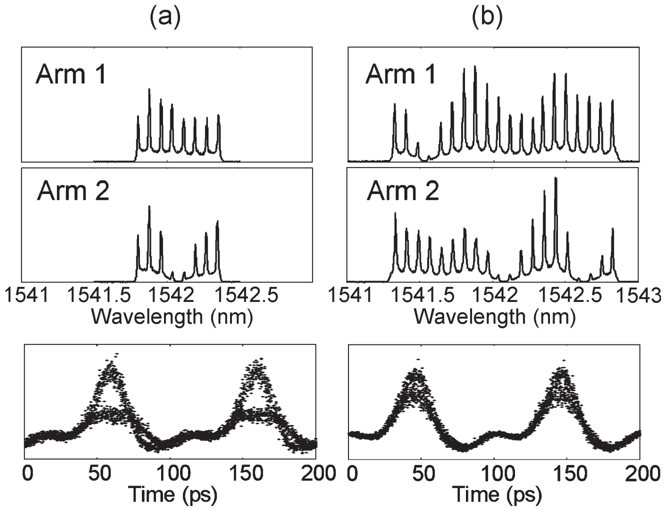

Fig. 6. Spectra and waveforms measurement using optical filters with different passband bandwidths for (a) arm 1 without a dip and (b) arm 2 with a dip.

in Fig. 4(c), is observed, which demonstrates a very clear vulnerability to eavesdropping.

Since there are multiple spectral dips in the spectra, the eavesdropper may scan the narrow-bandpass optical filter across the spectra to locate the position to detect the data. Fig. 5 shows such typical measurements at those possible positions of spectral dips (at the edge of each code chip), where: 1) there is a dip for arm 1 but no dip for arm 2; 2) there are dips for both arms; and 3) there is no dips for both arms, respectively. Similar to Fig. 4, Fig. 5(a) shows an eye diagram demonstrating a clear vulnerability. As expected, there are no eye diagrams for 2) and 3). For an eavesdropper without knowledge of the code, generally, there are many locations across the spectra to detect the data. For example, assuming the phase shift (zero or π) for each code chip is randomly assigned, there is 50% probability to detect data with clear eye diagram for each possible position of spectral dips. As a result, half of those positions are vulnerable to eavesdropping.

The bandwidth of the narrow-bandpass optical filter also plays an important role in the eavesdropping capability. In this particular example, a bandwidth allowing four spectral lines to pass through is appropriate to measure a clear eye diagram. For comparison, we change the bandwidth to allow eight and 20 spectral lines pass through, as shown in Fig. 6. The power difference between the two arms within the bandwidth, corresponding to eight spectral lines, still permits measuring an eye diagram in Fig. 6(a). However, the power difference between two arms becomes smaller relative to the total power as the bandwidth increases, showing almost no eye diagram for the 20 spectral line case [Fig. 6(b)]. This illustrates that the optimal parameters for the eavesdropper depend highly on the details of O-CDMA system configuration. The performance of the eavesdropper will depend on the received energy per spectral chip relative to the noise level, which also depends on the O-CDMA system parameters. It should also be noted that one can easily envision strategies that will improve eavesdropping performance by combining the energy from multiple spectral dip locations.

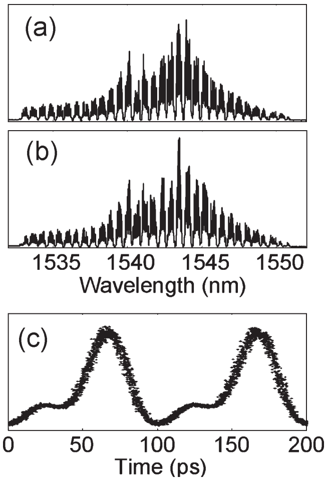

Fig. 7. Spectra of (a) arm 1 and (b) arm 2 after postprocessing. (c) Waveforms.

One simple strategy to improve security in terms of concealing the structure of spectral dips is to intentionally generate spectral dips at all possible positions (at the edge of each code chip). For this purpose, an additional pulse shaper is used as a postprocessing coder right after the complementary modulator. Fig. 7(a) and (b) shows the spectra of the individual arms after the postprocessing coder, where spectral dips appear at all possible positions. Fig. 7(c) shows the waveform (no eye diagram), which is similar to Fig. 3(c). The postprocessing coder is operated such that phase shifts of zero and π are applied alternatively to alternating code chips. Such phase transitions generate spectral dips at all spectral positions independent of code. Now, the eye diagram is well concealed, even using a narrow-bandpass filter, as shown in Fig. 8. On the other hand, it is important to show that the code-switching scheme with postprocessing (spectral dips everywhere) still works for the authorized user using conventional O-CDMA detection: decoded by a decoder, discriminated by the PPLN, and detected by the photo-diode at 0.77 μm [1], [2]. Fig. 9 shows the eye diagram for single arm [Fig. 9(a)], for code switching (both arms) [Fig. 9(b)], and for code switching with postprocessing [Fig. 9(c)], where arm 1 is properly decoded. The clear eye diagrams and bit-error-rate (BER) measurement in Fig. 9 demonstrate the code-switching scheme, with postprocessing still working for the authorized user using conventional O-CDMA detection. Note that for the code-switching scheme with postprocessing [Fig. 9(c)], to correctly decode arm 1, the

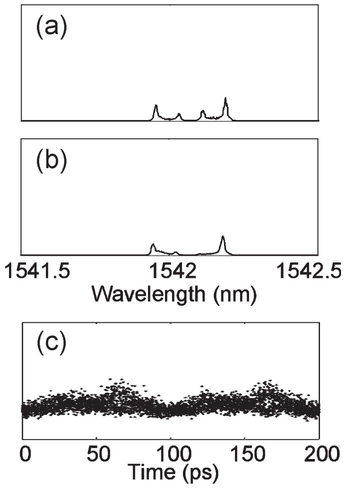

Fig. 8. Spectra of (a) arm 1 and (b) arm 2 in the vicinity of 1542 nm after postprocessing. (c) Waveforms.

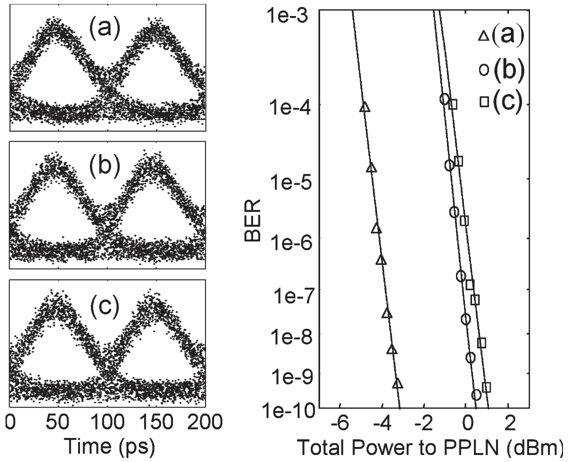

Fig. 9. Eye diagrams and BER measurements for authorized user. (a) Single arm. (b) Code switching. (c) Code switching with postprocessing.

spectral phase of the decoder is set to compensate the sum of the spectral phases from the arm 1 encoder and the postprocessing coder. This is similar to code translation in spectrally phase-coded O-CDMA [17]. The ~3-dB power penalty between BER curves for (a) and (b) is expected, since, ideally, SHG is generated only for code 1, while codes 1 and 2 are both present at the SHG chip at equal power level. The additional small power penalty due to postprocessing, which is around 0.6 dB, is explained on the basis of small changes in the properly decoded pulses as a result of extra spectral dips inserted by the postprocessing coder. Our code-switching scheme also works well with an interference user [12].

III. Vulnerability From a DPSK Demodulator

In the code-switching scheme, bits "1" and "0" are occupied by different spectrally phase-coded waveforms. This is analogous to binary phase shift keying (BPSK), where each bit has a constant energy but is data-coded with zero or π phase shift for bits "0" or "1." Therefore, a simple DPSK demodulator can also be used to recover data from the code-switching scheme. The DPSK format has been intensely investigated in optical fiber communication systems in recent years [18]. Briefly, the DPSK demodulator is a one-bit-delay interferometer, in which the incoming signal is split into two paths and combined again with one-bit difference between the two paths. In conventional BPSK/DPSK, the signals add constructively at the interferometer output for like adjacent bits ("00" or "$\pi\pi$") and destructively for unlike adjacent bits ("0π" or "$\pi 0$"). This converts the phase modulation into an intensity contrast. DPSK demodulation of two-code-keyed O-CDMA signals works in a similar way, provided that the interferometer delay is carefully matched to the data rate with a precision better than the coherence time of the O-CDMA signal (usually this is the duration of the original mode-locked pulse). When adjacent bits are identical (same code waveforms), they can interfere constructively to give a high output. However, when adjacent bits correspond to different code waveforms, their interference is close to zero due to averaging over different spectral chips (assuming the usual case of code pairs with low cross correlation).

Here, we use a DPSK demodulator scheme which is based on polarization maintaining (PM) fiber [19], as shown in Fig. 10. Light is launched at 45° to the principle axes of the 86.3-m length of PM fiber, which provides a 120.5-ps delay difference for light traveling along the fast and slow axes. To match the bit rate of the DPSK demodulator, the mode-locked laser is set to 8.3-GHz repetition rate. Phase differences between adjacent bits lead to polarization changes at the output of the PM fiber, which are converted to an intensity contrast after the polarizer. In an ideal DPSK receiver, the power of both polarization states separated by the polarizer would be measured and subtracted. For simplicity, in this paper, we measured only the light transmitted through the polarizer, which is already sufficient to demonstrate eavesdropping.

We use 3-ps pulses directly from the mode-locked laser as the input to the code-switching modulator in our DPSK experiment. The O-CDMA code-switching signal processed by the DPSK demodulator and then detected by the photo-diode is shown in Fig. 11(a). An eye diagram is apparent, although it is noisy. The noise comes from frequency fluctuations in the mode-locked laser frequency comb as well as lack of stabilization of the interferometer. We note that the requirement of good frequency stability (narrow linewidth) of the source laser in conventional coherent optical communication is translated into a requirement that the mode-locked laser have a frequency comb with good absolute frequency stability (narrow linewidth) for each of the comb lines. A recent high-resolution pulse-shaping experiment showed that frequency fluctuations in a mode-locked frequency comb lead to intensity fluctuations when the pulse shaper output depends on interferometric addition of contributions from adjacent mode-locked pulses [16]. A similar effect occurs in our DPSK measurement and contributes to the noisy eye. Nevertheless, the presence of an eye immediately demonstrates a clear vulnerability to eavesdropping. Fig. 11(b) selects several scans of the waveforms with clear eyes to emphasize the possibility of such vulnerability.

The DPSK vulnerability identified above is a very serious one for several reasons. First, the eavesdropping scheme does not require any attempt to learn the O-CDMA code. Second, the eavesdropper is unaffected if the code pair used in the code-switching modulator is changed. Third, the eavesdropper is able

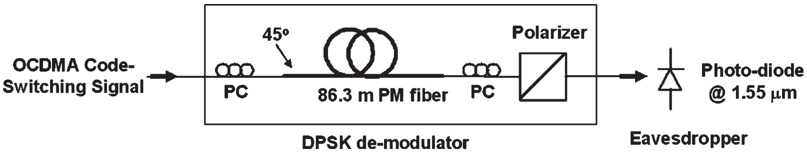

Fig. 10. Experimental setup to investigate vulnerability using a DPSK demodulator. PC: Polarization controller. PM: Polarization maintaining.

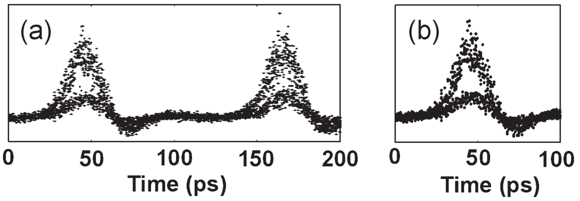

Fig. 11. (a) Waveforms after DPSK demodulator. (b) Picking up several scans of the waveforms with clear eyes to emphasize such possible vulnerabilities.

to exploit the full energy in the intercepted signal, as opposed to other schemes, where only the energy per code chip can be exploited [10], [11]. Given that the eavesdropper is able to use a conventional high-sensitivity detector requiring only a few femtojoules per bit, while the O-CDMA receiver requires nonlinear processing (demonstrated down to 30 fJ per bit [2], which is still an order of magnitude higher than conventional lightwave receivers), there is a significant likelihood that the eavesdropper can attain signal-to-noise ratio comparable to or even better than that of the O-CDMA receiver. Clearly, this fails to fulfill the premise for security in O-CDMA, which is that the eavesdropper without knowledge of the code should be at a signal-to-noise ratio disadvantage. It is important therefore to attempt to identify means by which the transmitter can mask single-user two-code-keyed O-CDMA data from a DPSK receiver. This will be a subject of our future work.

IV. Conclusion

The code-switching data-modulation format enhances security in O-CDMA compared to OOK by eliminating the vulnerability to eavesdropping based on a simple energy detector. Nevertheless, in this paper, we have experimentally demonstrated two vulnerabilities for such a code-switching scheme that allow eavesdropping of data from an isolated user in a two-code-keying spectrally phase-coded O-CDMA system. These vulnerabilities exploit structure in the coding and signaling schemes to recover data, with relatively simple hardware and without requiring knowledge of the codes. We have also demonstrated a modified coding scheme that mitigates one of the eavesdropping vulnerabilities. A key conclusion of this paper is that there may be many opportunities for exploiting structure in coded O-CDMA signals in order to eavesdrop, without the need to measure and determine the code. Although we have focused our investigation on spectral phase coding with an isolated user, it is likely that other O-CDMA schemes suffer from analogous vulnerabilities based on their structure. It may also be possible to extend these ideas to extract data in cases where traffic from multiple O-CDMA users is superimposed. Therefore, one needs to exercise great care in assessing and mitigating such vulnerabilities if the security features of O-CDMA are of interest.

Acknowledgment

The authors would like to thank R. V. Roussev, C. Langrock, and M. M. Fejer for providing the PPLN device and D. S. Seo for constructing the laser.

References

[1] Z. Jiang, D. S. Seo, S.-D. Yang, D. E. Leaird, R. V. Roussev, C. Langrock, M. M. Fejer, and A. M. Weiner, “Four user, 2.5 Gb/s, spectrally coded O-CDMA system demonstration using low power nonlinear processing,” *J. Lightw. Technol.*, vol. 23, no. 1, pp. 143–158, Jan. 2005.

[2] ——, “Four user, 10 Gb/s spectrally phase coded O-CDMA system operating at ∼30 fJ/bit,” *IEEE Photon. Technol. Lett.*, vol. 17, no. 3, pp. 705–707, Mar. 2005.

[3] S. Etemad, P. Toliver, R. Menendez, J. Young, T. Banwell, S. Galli, J. Jackel, P. Delfyett, C. Price, and T. Turpin, “Spectrally efficient optical CDMA using coherent phase-frequency coding,” *IEEE Photon. Technol. Lett.*, vol. 17, no. 4, pp. 929–931, Apr. 2005.

[4] R. P. Scott, W. Cong, V. J. Hernandez, K. B. Li, B. H. Kolner, J. P. Heritage, and S. J. B. Yoo, “An eight-user time-slotted SPECTS O-CDMA testbed: Demonstration and simulations,” *J. Lightw. Technol.*, vol. 23, no. 10, pp. 3232–3240, Oct. 2005.

[5] P. C. Teh, M. Ibsen, J. H. Lee, P. Petropoulos, and D. J. Richardson, “Demonstration of a four-channel WDM/OCDMA system using 255-chip 320-Gchips/s quaternary phase coding gratings,” *IEEE Photon. Technol. Lett.*, vol. 14, no. 2, pp. 227–229, Feb. 2002.

[6] H. Sotobayashi, W. Chujo, and K. Kitayama, “Highly spectral-efficient optical code-division multiplexing transmission system,” *IEEE J. Sel. Topics Quantum Electron.*, vol. 10, no. 2, pp. 250–258, Mar./Apr. 2004.

[7] X. Wang, N. Wada, T. Hamanaka, K. Kitayama, and A. Nishiki, “10-user, truly-asynchronous OCDMA experiment with 511-chip SSFBG en/decoder and SC-based optical thresholder,” presented at the Optical Fiber Commun. Conf. (OFC), Anaheim, CA, 2005, Paper PDP33.

[8] V. Baby, I. Glesk, R. J. Runser, R. Fischer, Y. K. Huang, C. S. Bres, W. C. Kwong, T. H. Curtis, and P. R. Prucnal, “Experimental demonstration and scalability analysis of a four-node 102-Gchip/s fast frequency-hopping time-spreading optical CDMA network,” *IEEE Photon. Technol. Lett.*, vol. 17, no. 1, pp. 253–255, Jan. 2005.

[9] D. D. Sampson, G. J. Pendock, and R. A. Griffin, “Photonic code-division multiple-access communications,” *Fiber Int. Opt.*, vol. 16, no. 2, pp. 129–157, 1997.

[10] T. H. Shake, “Security performance of optical CDMA against eavesdropping,” *J. Lightw. Technol.*, vol. 23, no. 2, pp. 655–670, Feb. 2005.

[11] ——, “Confidentiality performance of spectral-phase-encoded optical CDMA,” *J. Lightw. Technol.*, vol. 23, no. 4, pp. 1652–1663, Apr. 2005.

[12] D. E. Leaird, Z. Jiang, and A. M. Weiner, “Experimental investigation of security issues in OCDMA: A code-switching scheme,” *Electron. Lett.*, vol. 41, no. 14, pp. 817–819, Jul. 2005.

[13] A. M. Weiner, “Femtosecond pulse shaping using spatial light modulators,” *Rev. Sci. Instrum.*, vol. 71, no. 5, pp. 1929–1960, May 2000.

[14] K. R. Parameswaran, R. K. Route, J. R. Kurz, R. V. Roussev, M. M. Fejer, and M. Fujimura, “Highly efficient second-harmonic generation in buried waveguides formed by annealed and reverse proton exchange in periodically poled lithium niobate,” *Opt. Lett.*, vol. 27, no. 3, pp. 179–181, Feb. 2002.

[15] R. N. Thurston, J. P. Heritage, A. M. Weiner, and W. J. Tomlinson, “Analysis of picosecond pulse shape synthesis by spectral masking in a grating pulse compressor,” *IEEE J. Quantum Electron.*, vol. QE-22, no. 5, pp. 682–696, May 1986.

[16] Z. Jiang, D. S. Seo, D. E. Leaird, and A. M. Weiner, “Spectral line-by-line pulse shaping,” *Opt. Lett.*, vol. 30, no. 12, pp. 1557–1559, Jun. 2005.

[17] Z. Jiang, D. S. Seo, D. E. Leaird, A. M. Weiner, R. V. Roussev, C. Langrock, and M. M. Fejer, “Reconfigurable all-optical code translation in spectrally phase coded O-CDMA,” *J. Lightw. Technol.*, vol. 23, no. 6, pp. 1979–1990, Jun. 2005.

[18] A. H. Gnauck and P. J. Winzer, "Optical phase-shift-keyed transmission," *J. Lightw. Technol.*, vol. 23, no. 1, pp. 115–130, Jan. 2005.

[19] E. Ciaramella, G. Contestabile, and A. D'Errico, "A novel scheme to detect optical DPSK signals," *IEEE Photon. Technol. Lett.*, vol. 16, no. 9, pp. 2138–2140, Sep. 2004.

Zhi Jiang (S'03) received the B.S. (*with highest honors*) and M.S. degrees in electronics engineering from Tsinghua University, Beijing, China, in 1999 and 2002, respectively, and the Ph.D. degree in electrical and computer engineering from Purdue University, West Lafayette, IN, in 2006.

His research focuses on the areas of ultrafast technology, optical pulse shaping, optical fiber communication, and fiber nonlinearity.

Dr. Jiang received the Ross and Mary I. Williams Fellowship, Purdue University, in 2002–2003. He was selected as a finalist for the 2005 OSA New Focus/Bookham Student Award. He was one of the recipients of the 2005 IEEE/LEOS Graduate Student Fellowships.

Daniel E. Leaird (M'01–SM'05) was born in Muncie, IN, in 1964. He received the B.S. degree in physics from Ball State University, Muncie, in 1987 and the M.S. and Ph.D. degrees in electrical and computer engineering from Purdue, Purdue University, West Lafayette, IN, in 1996 and 2000, respectively.

In 1987, he joined the Bell Communications Research (Bellcore), Red Bank, NJ, as a Senior Staff Technologist and later advanced as a member of the technical staff. From 1987 to 1994, he worked with the Ultrafast Optics and Optical Signal Processing Research Group, where he was a key team member in research projects, in ultrafast optics, such as shaping of short optical pulses using liquid crystal modulator arrays, investigation of dark soliton propagation in optical fibers, impulsive stimulated Raman scattering in molecular crystals, and all-optical switching. Since 1994, he has been with the Ultrafast Optics and Optical Fiber Communications Laboratory School of Electrical and Computer Engineering, Purdue University, where he is currently a Senior Research Scientist and Laboratory Manager. He has coauthored approximately 60 journal articles, 80 conference proceedings. He holds two U.S. patents.

Dr. Leaird is active in the optics community and professional organizations, including the Optical Society of America and the IEEE Lasers and Electro-Optics Society (LEOS), where he is a member of the Ultrafast Technical Committee as well as serving as a Consultant to venture capitalists by performing technical due diligence. He also serves as a frequent reviewer for *Optics Letters, Optics Express, Photonics Technology Letters, Applied Optics,* and *Journal of the Optical Society of America B*, in addition to serving on National Science Foundation review panels in the SBIR program. He has received several awards for his work in the ultrafast optics field including a Bellcore "Award of Excellence," a Magoon Award for outstanding teaching, and an Optical Society of America/New Focus Student Award.

Andrew M. Weiner (S'84–M'84–SM'91–F'95) received the Sc.D. degree in electrical engineering from the Massachusetts Institute of Technology (MIT), Cambridge, in 1984.

From 1979 to 1984, he was a Fannie and John Hertz Foundation Graduate Fellow at MIT. Upon graduation, he joined Bellcore, first as member of the technical staff and later as a Manager of Ultrafast Optics and Optical Signal Processing Research. He moved to Purdue University, West Lafayette, IN, in 1992 and is currently the Scifres Distinguished Professor of Electrical and Computer Engineering. From 1997 to 2003, he served as the ECE Director of Graduate Admissions. He has published five book chapters and over 175 journal articles. He has been an author or coauthor of over 300 conference papers, including approximately 80 conference invited talks, and has presented over 70 additional invited seminars at university, industry, and government organizations. He holds eight U.S. patents. His research focuses on ultrafast optical signal processing and high-speed optical communications. He is especially well known for pioneering the field of femtosecond pulse shaping, which enables generation of nearly arbitrary ultrafast optical waveforms according to user specification.

Prof. Weiner has received numerous awards for his research, including the Hertz Foundation Doctoral Thesis Prize (1984), the Adolph Lomb Medal of the Optical Society of America (1990), the Curtis McGraw Research Award of the American Society of Engineering Education (1997), the International Commission on Optics Prize (1997), the IEEE LEOS William Streifer Scientific Achievement Award (1999), the Alexander von Humboldt Foundation Research Award for Senior U.S. Scientists (2000), and the inaugural Research Excellence Award from the College of Engineering at Purdue (2003). He is a Fellow of the Optical Society of America. He has served as Cochair of the Conference on Lasers and Electro-optics and the International Conference on Ultrafast Phenomena and as an Associate Editor of several journals. He has also served as Secretary/Treasurer of IEEE LEOS and as a Vice President of the International Commission on Optics (ICO).