Wavelength-division multiplexing Fresnel transform encoding of time-varying signals

Christian Cuadrado-Laborde
Ricardo Duchowicz
CONICET-CIC
Centro de Investigaciones Ópticas
P.O. Box 124 (1900)
La Plata, Argentina
E-mail: claborde@ciop.unlp.edu.ar

Enrique E. Sicre
UADE
Facultad de Ingeniería y Ciencias Exactas
Lima 717 (1073)
Buenos Aires, Argentina

Abstract. We study the wavelength-division multiplexing implementation of the recently proposed temporal Fresnel transform encoding technique, in order to evaluate its potential application for secure data transmission in short-haul fiber optic links. The different signal broadenings produced by each stage of the encoding process are analyzed in a dual time-frequency domain by using the Wigner distribution function. Furthermore, the robustness of the proposed method is illustrated by comparing the signal-to-noise ratio between the input and the decrypted signals obtained by varying typical parameters of the encryption-decryption setup. Numerical simulations revealed good system performance. Finally, we consider experimental feasibility with current photonic technology.
 [DOI: 10.1117/1.2968216]

Subject terms: fiber optics; time-domain encryption; Wigner distribution function.

Paper 070902R received Nov. 9, 2007; revised manuscript received Jun. 2, 2008; accepted for publication Jun. 2, 2008; published online Aug. 11, 2008.

1 Introduction

Information security is a subject of ever increasing importance. Optical techniques have shown great potential for information security applications in the spatial domain, especially since the middle 1990s, when Réfrégier and Javidi proposed a double random phase encoding technique (DRPE) to encrypt high-security images.[1] This technique involves the multiplication of the input image by two random phase masks (RPMs) located in the input and the Fourier planes of a 4f system, respectively. It can be shown that if these RPMs are statistically independent white noises, then the encrypted image is also a complex white noise signal. Because detectors are phase-insensitive, the RPM located at the Fourier plane serves as the only key in this encryption scheme.[1] Enlarging the key space is a well-known approach to increase the security level.[2] One way to achieve it is by encrypting images through the fractional Fourier transform DRPE; as a result, the scale factors and the transform orders offer additional keys.[3–5] Moreover, a phase-encoding version of the DRPE setup was also proposed,[6] and a slight improvement in robustness to additive noise was numerically demonstrated in that case.[7] Another approach closely related to these techniques (and somewhat simpler) is the lensless DRPE.[8,9] It replaces the 4f systems by simple free-space propagation of the light amplitude between RPMs. From a mathematical point of view, the Fresnel transform serves here as the basic operating principle. We refer to this encryption setup from now on merely by the acronym for Fresnel transform encoding (FTE).

The development of low-loss, dispersion-optimized transmission optical fibers has revolutionized telecommunications by its unprecedented possibilities.[10] Signal multiplexing is a standard way of increasing the bit-rate requirements, for fully exploiting their inherent transmission capacity within networks. A variety of multiplexing schemes can be implemented in order to increase the system capacity. As an example, wavelength-division multiplexing (WDM) is a technology that multiplexes several optical carrier signals on a single optical fiber by using different wavelengths.[10] It has two distinct advantages: (i) time-varying data streams can be sent in parallel, and (ii) time-costly operations can be carried out at great speeds. As a result, it has found growing importance in data transmission.

Very recently, Cuadrado-Laborde proposed a temporal Fresnel transform encoding technique.[11] Our purpose here is extending that approach to encrypt and efficiently transmit time-varying optical data streams by using several channels, mainly for secure short-haul telecommunication applications (e.g., for metropolitan networks). Most encryption techniques in the spatial domain use Fourier lenses[1,3–6]; however, in the time domain, the implementation of Fourier lenses based on electro-optic phase modulation (by far the most common available technology in this field) sometimes becomes cumbersome or even impossible, because the time aperture and the phase factor are inversely related (i.e., the longer the time aperture, the smaller the phase factor).[12] For this reason it becomes even more important than in the spatial case to make a time-domain analysis of a lensless encryption approach and its WDM possibilities.

The paper is organized as follows. In Sec. 2.1 we present the encryption and decryption stages of the WDM FTE plus the single-channel FTE operation. The different broadenings produced at each stage of the encoding process, in both time and frequency domains, are reviewed in Sec. 2.2. Computer simulations supporting the theoretical findings are presented in Sec. 3. In Sec. 4 we discuss some practical

0091-3286/2008/$25.00 © 2008 SPIE

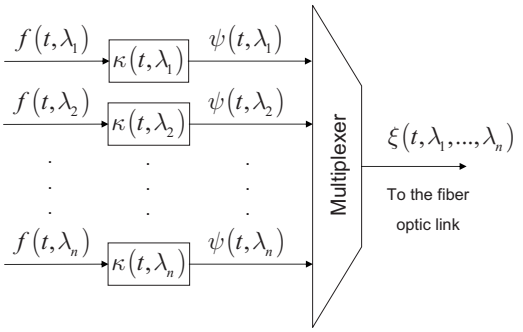

Fig. 1 WDM-FTE setup for encryption. Here $f(t,\lambda_i)$ is an optical input signal, $\psi(t,\lambda_i)$ its encrypted counterpart, $\kappa(t,\lambda_i)$ the impulse response of a single-channel encryption stage, and $\xi(t,\lambda_1,\ldots,\lambda_n)$ the WDM-encrypted signal at the input of the fiber optic link.

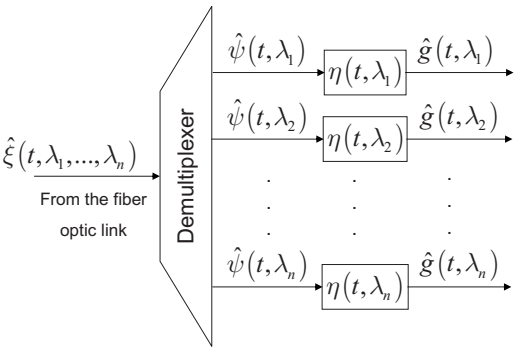

Fig. 2 WDM-FTE setup for decryption. Here $\hat{\xi}(t,\lambda_1,\ldots,\lambda_n)$ is the WDM-encrypted signal at the output of the fiber optic link, $\hat{\psi}(t,\lambda_i)$ a single-channel encrypted signal, $\hat{g}(t,\lambda_i)$ its decrypted counterpart, and $\eta(t,\lambda_i)$ the impulse response of a single-channel decryption stage.

features of the experimental implementation of the proposed setup. Finally, our conclusions are presented in Sec. 5.

2 Wavelength-Division Multiplexing Fresnel Transform Encoding for Time-Varying Signals

2.1 *WDM and Single-Channel FTE: Encryption-Decryption Setups*

We start by briefly reviewing the FTE, as it was originally proposed in the space domain.[8,9] Two RPMs are employed, the first placed at the input plane, and the second located at a distance z_1 away. The output plane is defined at a distance z_2 from the second RPM. When the system is perpendicularly illuminated with a plane wave of wavelength λ, the encrypted image is obtained at the output. In this method, the second RPM, z_1, z_2, and even λ act as keys. Since the inverse Fresnel transform cannot be realized optically, the complex conjugation of the encrypted image should be taken as input for decryption. The decryption setup is the same as that for encryption, but in the reverse direction. Later, Chen and Zhao upgraded the FTE setup for realizing the possibility of optical color image encryption by wavelength multiplexing.[13] Recently Peng et al. showed that the FTE scheme is vulnerable to chosen-plaintext attack (CPA).[14] They showed how an opponent can access random phase keys in either the input or the Fresnel domain, if the wavelength and the propagation distances are known, with the impulse functions as chosen plaintexts. However, it should be remembered that CPA becomes important in other contexts, in particular in public-key cryptography, where the encryption key is public and attackers can encrypt any plaintext they choose. Besides, it is not a trivial task for an eavesdropper to get the knowledge of both propagation distances and the mean wavelength. Anyway, we proceed as in Ref. 13, enlarging the key space, in order to improve the security performance, consecutively employing the Fresnel transform several times, as is later shown in the description of single-channel FTE.

First we discuss the photonic implementation of the multiple-channel encryption setups, postponing until later the detailed discussion of the single-channel FTE setup. Figure 1 shows the WDM-FTE setup for time-varying signal encryption. The transmission of each optical data stream $f(t,\lambda_i)$ through a single-channel encryption stage [with temporal impulse response $\kappa(t,\lambda_i)$] produces at the output the encrypted signal $\psi(t,\lambda_i)$. This signal represents the encryption of each input time-varying optical data stream at a specific wavelength λ_i. The wavelength dependence within the argument of functions is expressed only when strictly necessary within this article, because in WDM it is clear that each communication channel is characterized by its wavelength. The several encrypted signals are transmitted together by the same fiber optic link by recombining them through a multiplexer; i.e., $\xi(t,\lambda_1,\ldots,\lambda_n)=\Sigma_n\psi(t,\lambda_i)$, where n represents the total number of channels.

Figure 2 shows the WDM-FTE setup for decryption. The circumflex accent over the signals stands for those changes introduced by the transmission through the fiber optic link; in this way the multiplexed signal is represented by $\hat{\xi}(t,\lambda_1,\ldots,\lambda_n)$. After demultiplexing, each signal component [e.g., $\hat{\psi}(t,\lambda_i)$] is decrypted by passaging it through its corresponding single-channel decryption stage, with temporal impulse response $\eta(t,\lambda_i)$. The output $\hat{g}(t,\lambda_i)$ represents the decryption result of each input optical data stream $f(t,\lambda_i)$.

Now we discuss in more detail the time-domain single-channel FTE encryption and decryption setups. Because the single-channel setups are essentially the same for every channel, for the sake of clarity we omit within this discussion subscripts or arguments denoting wavelength dependence. For transferring the FTE setups to the time domain, we make use of the space-time duality, which expresses the resemblance between the equations that describe the paraxial diffraction of beams in space and the temporal dispersion of narrowband pulses in a dielectric medium (first-order dispersion).[12,15–17] Basically, the distortion of a pulse in a dispersive medium because of first-order chromatic dispersion is mathematically identical to Fresnel diffraction; i.e., they have the same impulse response provided a change of variables is made. In this way it is possible to transfer the FTE setup to the time domain.[11]

Figure 3 shows the proposed single-channel FTE encryption setup. The RPMs have been replaced by phase

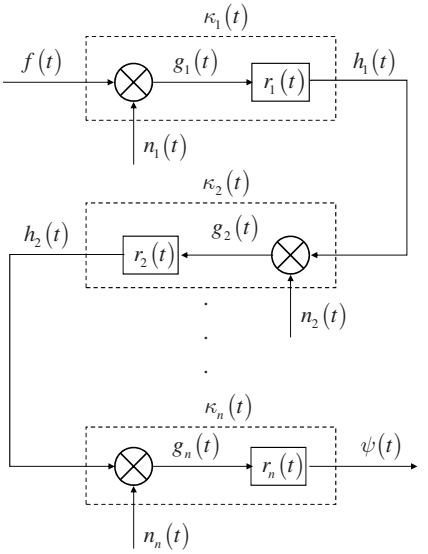

Fig. 3 Single-channel FTE setup for encryption. Here $f(t)$ is an optical input signal, and $\psi(t)$ its encrypted counterpart; $\kappa_k(t)$ is the impulse response of each encryption stage, which is composed of a phase modulator fed with a quasi-white-noise signal $n_k(t)$ plus a dispersive stage represented by its temporal impulse response $r_k(t)$.

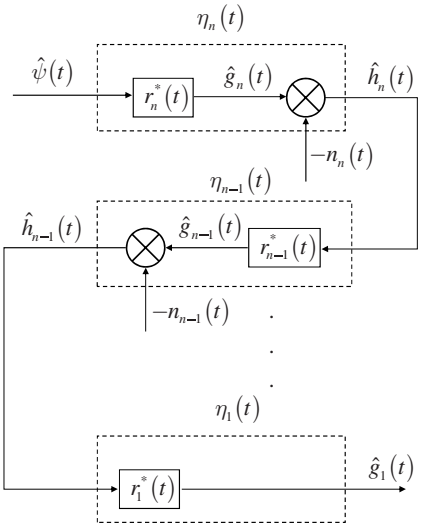

Fig. 4 Single-channel FTE setup for decryption. The asterisk $(^*)$ stands for the complex conjugate, and the signals and systems are the same as in Figs. 2 and 3.

modulators (PMs); i.e., $p_k(t)=\exp[j2\pi n_k(t)]$, where $n_k(t)$ denotes an independent electrical white noise sequence uniformly distributed in $[0, 1]$ at the k'th encryption stage of the corresponding channel. The pulse propagation through a first-order dispersive medium [represented in Fig. 3 through its temporal impulse response $r_k(t)$] replaces the free-space propagation through a distance z_k. This can be treated as a conventional phase-only filter, providing a quadratic spectral phase response (linear group delay). Thus, its frequency response can be expressed as $R_k(\omega)=\exp[j\omega^2\Phi_{20}^{(k)}/2]$, where $R_k(\cdot)=\Im[r_k(\cdot)]$ is the Fourier transform of $r_k(\cdot)$, ω is the angular frequency in baseband, and $\Phi_{20}^{(k)}$ is the first-order dispersion coefficient of the k'th encryption stage of the channel.[12,18] By using the relationship $(1/\sqrt{2\alpha})\exp(-\omega^2/4\alpha)=\Im[\exp(-\alpha t^2)]$, the temporal impulse response results as $r_k(t)=\exp[-(j/2\Phi_{20}^{(k)})t^2]$,[12] where the constant factor has been discarded.

On the other hand, the fact that positive or negative dispersion can be obtained adds an extra degree of versatility in the time domain, something that is not present in the spatial case, where the complex conjugate of the encrypted signals has to be taken for decoding.[8,11] In turn, this introduces the following change in the decryption setup, as compared with Refs. 8 and 9: $r_k(\cdot)\Rightarrow r_k(\cdot)^*$ (see Fig. 4).

The amount of dispersion between the last PM at the encryption stage $p_n(t)$ and the first at the decryption stage $p_n^*(t)$ should be reduced to zero for a successful decryption. For mathematical simplicity, and without losing generality, we assume that all dispersive effects of the fiber optic link are already included at the last dispersive stage $r_n(t)$ of the encryption. Under this assumption the fiber optic link behaves as an ideal transmission medium with unity transfer function, and therefore $\psi(t)=\hat{\psi}(t)$.[11] Then, through a simple Fourier-transform-based analysis it can be easily demonstrated that $|\hat{g}_n(t)|=|f(t)|$. Therefore, the following keys are necessary for decoding each transmitted channel at the decryption stage:

$$\text{keys:}\quad \{n_2(t),\ldots,n_{n-1}(t),n_n(t);\Phi_{20}^{(1)},\ldots,\Phi_{20}^{(n-1)},\Phi_{20}^{(n)};\lambda\}. \tag{1}$$

Because detectors are not phase-sensitive, the final phase correction through $p_1^*(t)$ is not generally needed; hence $n_1(t)$ was removed from the keys list and the last decryption stage (see Fig. 4). In Sec. 3 we analyze how sensitive the decryption stage is against a detuning of these parameters.

In this way, $\kappa_k(t)$ $[\eta_k(t)]$ becomes the impulse response of the k'th encryption [decryption] stage; see Figs. 3 and 4. It can also be observed that we have extended each encryption stage to the n'th degree to increase its security strength.[13]

Finally, the following relationships exist between the WDM FTE and single-channel FTE (see Figs. 1–4):

$$\kappa(t)=\prod_{k=1}^{n}\kappa_k(t), \tag{2a}$$

$$\eta(t)=\prod_{k=1}^{n}\eta_k(t), \tag{2b}$$

where n represents the total number of encryption stages. It should be kept in mind that as the data propagate through the encryption process, the signal temporally broadens. Therefore, the time aperture of the $(k+1)$'th PM of the encryption stage should be slightly larger than that of the k'th PM, in order to phase-modulate the partially encrypted signal completely and correctly.

2.2 *Signal-Spreading Analysis in Time and Frequency Domains*

Quantifying the spreading in both time (t) and frequency (ν) domains as the signal is encrypted becomes a requisite for analyzing the multiplexing performance of the proposed setup. In what follows we assume that signals [e.g., $f(t)$] are bounded within some finite region in the time-frequency phase-space domain. Of course, this really means that we only take into account (for analysis purposes) the part of the time-frequency phase-space domain (t,ν) where both the optical power of the signal itself and its spectrum are significantly nonzero functions This means that the following relation should be satisfied:

$$\{f(t),F(\nu)\}\approx 0 \qquad \forall\,\{|t|,|\nu|\}>\{\Delta t_f/2,\Delta\nu_f/2\}, \tag{3}$$

where—and from now on—a capital letter stands for the Fourier transform of the signal denoted by the corresponding lowercase letter: $F(\nu)=\Im[f(t)]$; and where Δt_f and $\Delta\nu_f$ are the total temporal and frequency extents, respectively. Arguments or subscripts denoting wavelength dependence are omitted in this subsection, since the results to be derived are equally applicable to any wavelength. The Wigner distribution function (WDF) is specially appropriate for performing this analysis in that it gives, roughly speaking, the distribution of the signal energy over time and frequency.[19,20] The WDF of a one-dimensional signal $f(t)$ is given by

$$W_f(t,\nu)=\int f(t+t'/2)f^*(t-t'/2)\exp(-i2\pi\nu t')\,\mathrm{d}t'. \tag{4}$$

There are two processes involved as the input signal is progressively encrypted, namely, phase modulation with a random signal, and subsequent propagation through a first-order dispersive medium; see Fig. 3. In the time domain, from a mathematical point of view, the first process is a product of the signal and the complex exponential associated with the phase modulation, while the second is a convolution between the output of the first process and the temporal impulse response of the dispersive medium.[16] Regarding the first process, there is a property of the WDF that is especially useful: the multiplication of two functions in the time domain [e.g., $g_1(t)=f(t)p_1(t)$; see Fig. 3] implies a frequency-domain convolution of their corresponding WDFs[19,21]:

$$W_g(t,\nu)=\int W_f(t,\nu-\nu')W_p(t,\nu')\,\mathrm{d}\nu'. \tag{5}$$

From Eq. (5) the product signal $g_1(t)$ with time width $\Delta t_g^{(1)}$ becomes the temporal overlapping of the individual signals (having time widths Δt_f and $\Delta t_p^{(1)}$), which can be expressed as $\Delta t_g^{(1)}=\min\{\Delta t_f,\Delta t_p^{(1)}\}$, where $\min\{,\}$ stands for the lesser quantity between the braces. On the other hand, following Eq. (5), the bandwidth of the product signal is the sum of the bandwidths of the individual signals.[11,19,21] Both effects are summarized below

$$\Delta t_g^{(1)}=\Delta t_f, \tag{6a}$$

$$\Delta\nu_g^{(1)}=\Delta\nu_f+\Delta\nu_p^{(1)}, \tag{6b}$$

where in Eq. (6a), it is considered than the time aperture of the PM should be large enough to phase-modulate the whole input signal, so that, as a consequence, $\min\{\Delta t_f,\Delta t_p^{(1)}\}=\Delta t_f$.[11]

Now we turn our attention to the second process, the propagation of a signal through a first-order dispersive medium. This can be mathematically expressed as a Fresnel transform, which is a member of the three-parameter class of linear integral transforms, widely known as linear canonical transforms (LCTs), defined as[19,22]

$$f_{\alpha,\beta,\gamma}(t')=\exp(-j\pi/4)\sqrt{\beta}\times\int f(t)\exp[j\pi(\alpha t^2-2\beta tt'+\gamma t'^2)]\,\mathrm{d}t, \tag{7}$$

where α, β, and γ are real constant parameters. It can be recognized that Eq. (7) also describes the Fourier transform and the fractional Fourier transform as special cases. The effect of a LCT on the WDF can be represented in the following matrix notation in the time-frequency phase space[19,22]:

$$\begin{pmatrix}t'\\ \nu'\end{pmatrix}=\begin{pmatrix}\gamma/\beta & 1/\beta\\ -\beta+\alpha\gamma/\beta & \alpha/\beta\end{pmatrix}\begin{pmatrix}t\\ \nu\end{pmatrix}, \tag{8}$$

where (t',ν') and (t,ν) denote the transformed and initial points in the time-frequency phase space, respectively. Using the introduced formulation, we can calculate the signal at the output of the dispersive medium $h_1(t)$ as the convolution between $g_1(t)$ and the impulse response of the dispersive medium $r_1(t)$ (see Fig. 3), as follows:

$$h_1(t')=g_1(t)*r_1(t)=\int g_1(t)r_1(t'-t)\,\mathrm{d}t=\int g_1(t)\exp\left(-j\frac{1}{2\Phi_{20}^{(1)}}(t'-t)^2\right)\mathrm{d}t, \tag{9}$$

where $*$ stands for the convolution operation, and the previously derived impulse response of the dispersive medium was used. Equations (7) and (9) reduce to the same expression (except for a constant factor) provided the following relationships are fulfilled: $\alpha=\beta=\gamma=-1/(2\pi\Phi_{20}^{(1)})$. Next, by substituting these values in Eq. (8), the following transformation operates in the time-frequency phase space:

$$\begin{pmatrix}t'\\ \nu'\end{pmatrix}=\begin{pmatrix}1 & -2\pi\Phi_{20}^{(1)}\\ 0 & 1\end{pmatrix}\begin{pmatrix}t\\ \nu\end{pmatrix}. \tag{10}$$

This relationship is fulfilled for every point in the time-frequency phase space. However, because we are analyzing the signal spreading, we introduce in Eq. (10) the temporal and frequency extents; i.e., $\{t,\nu\}\Rightarrow\{\Delta t_g^{(1)},\Delta\nu_g^{(1)}\}$ and $\{t',\nu'\}\Rightarrow\{\Delta t_h^{(1)},\Delta\nu_h^{(1)}\}$. Therefore, the following equalities are obtained:

$$\Delta t_h^{(1)}=\Delta t_g^{(1)}-2\pi\Phi_{20}^{(1)}\,\Delta\nu_g^{(1)}, \tag{11a}$$

$$\Delta\nu_h^{(1)} = \Delta\nu_g^{(1)}. \tag{11b}$$

The final broadenings that are obtained when the input signal passages through the tandem PM dispersive medium can be derived by substituting Eq. (6) in Eq. (11), and so

$$\Delta t_h^{(1)} = \Delta t_f - 2\pi\Phi_{20}^{(1)}(\Delta\nu_f + \Delta\nu_p^{(1)}), \tag{12a}$$

$$\Delta\nu_h^{(1)} = \Delta\nu_f + \Delta\nu_p^{(1)}. \tag{12b}$$

These results can be easily extended to n encryption stages. In the following section we numerically illustrate the WDM-FTE performance by using two encryption stages, so we rewrite Eq. (12) to include $n=2$ stages:

$$\Delta t_\psi = \Delta t_f - 2\pi\Phi_{20}^{(T)}(\Delta\nu_f + \Delta\nu_p^{(1)}) - 2\pi\Phi_{20}^{(2)}\,\Delta\nu_p^{(2)}, \tag{13a}$$

$$\Delta\nu_\psi = \Delta\nu_f + \Delta\nu_p^{(1)} + \Delta\nu_p^{(2)}, \tag{13b}$$

where $\Phi_{20}^{(T)} \equiv \Phi_{20}^{(1)} + \Phi_{20}^{(2)}$. Equation (13a) states that the encoded signal transmitted by the fiber optic link has a time width Δt_ψ that depends directly on both the time width of the input signal and the dispersion parameters of the encoding setups (through $\Phi_{20}^{(1)}$ and $\Phi_{20}^{(2)}$). Regarding with the bandwidth of the encoded signal $\Delta\nu_\psi$, like Δt_ψ, it depends on the input signal's spectral characteristics (through $\Delta\nu_f$), and the phase modulators' spectral contents $\Delta\nu_p^{(1)}$ and $\Delta\nu_p^{(2)}$, which in turn are determined by $n_1(t)$ and $n_2(t)$.[11]

3 Numerical Results

Certainly, the technique fails if we have to transmit time-unlimited, as well as bandwidth-unlimited, signals. In fact, if white noise is used for encryption, the time width of the encoded signal broadens excessively, thereby slowing the data transmission speed. This fact can be further corroborated by analyzing Eq. (13a), if we wish to exploit the fiber optic multiplexing capabilities. Thus, it becomes evident that true white noise cannot be employed, because both Δt_ψ and $\Delta\nu_\psi$ directly depend on $\Delta\nu_p^{(1)}$ and $\Delta\nu_p^{(2)}$, which in turn are determined by the spectral content of the electrical signals used for the two PMs, viz., $n_1(t)$ and $n_2(t)$; see Fig. 3. Therefore, in order to get a noise signal that accomplishes both requirements—secure encoding and bandwidth limitation—we propose using a quasi-white-noise signal with a well-defined bandwidth that is obtained by applying an iterative procedure to limit the spectral content of $P(\nu)$ below a certain threshold value $\Delta\nu_p$, where we have omitted the use of indices for $\Delta\nu_p$, because this procedure should be performed in the same way for every PM, independently of encryption stage or channel wavelength.

Very recently one of us described the procedure in detail[11]; therefore we just summarize its main features here. The input to the process is a true random PM function described by $p_0(t)$, and its spectral content is iteratively reduced to the desired value, $\Delta\nu_p$. The procedure is stopped after the j'th iteration when the error given by $e = \int_{|\nu|>\Delta\nu_p/2} |P_j(\nu)|^2\,d\nu$ becomes small enough. For computational purposes, we have used random PMs having a spectral content limited below $\Delta\nu_p \approx 45$ GHz, obtained with 15 iterations, after which e is below 1%.

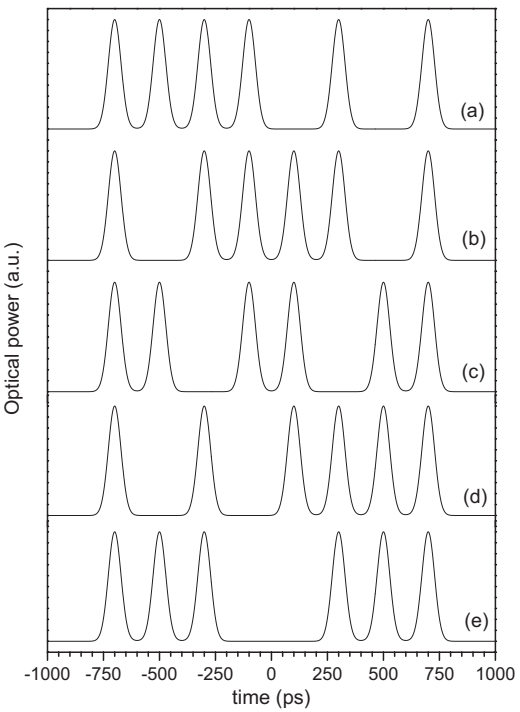

Fig. 5 Input signal intensities of (a) $f(t,\lambda_1 \approx 1548.51$ nm), (b) $f(t,\lambda_2 \approx 1549.31$ nm), (c) $f(t,\lambda_3 \approx 1550.12$ nm), (d) $f(t,\lambda_4 \approx 1550.92$ nm), and (e) $f(t,\lambda_5 \approx 1551.72$ nm). The data stream is composed of eight time slots of 200 ps each, and a 1 data bit is represented by a Gaussian optical pulse of 40-ps mean width at $1/e$ intensity.

Numerical calculations were performed in a time window of ≈137 ns with 2^{17} equally spaced points (time discretization). These values are large enough to correctly visualize both the signals in the time domain and their Fourier spectra.

Figure 5 shows the binary optical input signals to the FTE setup sketched in Fig. 1. Each input is composed of eight slots, each one having a time width of $T_1 = 200$ ps, so becoming the temporal extension of one data stream with $\Delta t_f = 1.6$ ns. Inside each slot, a 1 data bit is represented by an optical Gaussian pulse of unit intensity and mean width $T_0 = 40$ ps at $1/e$ intensity; whereas an empty slot represents a 0 bit. The interference effects between adjacent channels are illustrated by using the following five input signals (in order of increasing wavelength): (a) $f(t,\lambda_1 \approx 1548.51$ nm), (b) $f(t,\lambda_2 \approx 1549.31$ nm), (c) $f(t,\lambda_3 \approx 1550.12$ nm), (d) $f(t,\lambda_4 \approx 1550.92$ nm), and (e) $f(t,\lambda_5 \approx 1551.72$ nm), which are sufficiently representative of a narrow band in a WDM transmission at 100-GHz spacing.* The same total dispersion was selected for every channel: $\Phi_{20}^{(T)} = \Phi_{20}^{(1)} + \Phi_{20}^{(2)} = -4 \times 10^3$ ps^2/rad. However, in order to use different keys for each channel, the dispersion distribution between encryption stages was varied, between $\Phi_{20}^{(1,i)}$ and $\Phi_{20}^{(2,i)}$. In this way, the selected keys for $f(t,\lambda_1)$ to $f(t,\lambda_5)$ become (relative to $\Phi_{20}^{(T)}$): {0.5,0.5}, {0.55,0.45}, {0.45,0.55}, {0.4,0.6}, and finally {0.6,0.4}.

*All wavelengths were selected according to ITU-T Recommendation G.694.1 (06/2002), "Spectral grids for WDM applications: DWDM frequency grid."

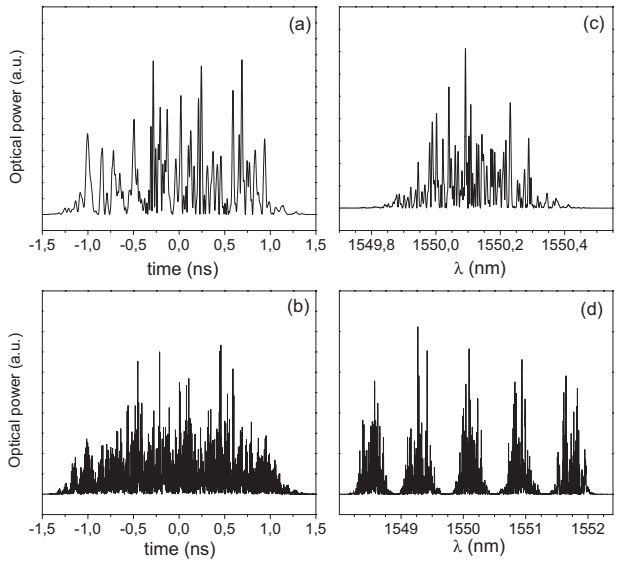

Fig. 6 (a) Encrypted signal intensity corresponding to a single channel, viz., $\psi(t,\lambda_3)$. (b) Encrypted signal intensity corresponding to the WDM transmission of the five data streams shown in Fig. 5; i.e., $\xi(t,\lambda_1,\ldots,\lambda_5)$. (c) and (d): spectral powers $\Psi(\nu,\lambda_3)$ and $\Xi(\nu,\lambda_1,\ldots,\lambda_5)$ of the signals shown in (a) and (b), respectively. All wavelengths are the same as in Fig. 5.

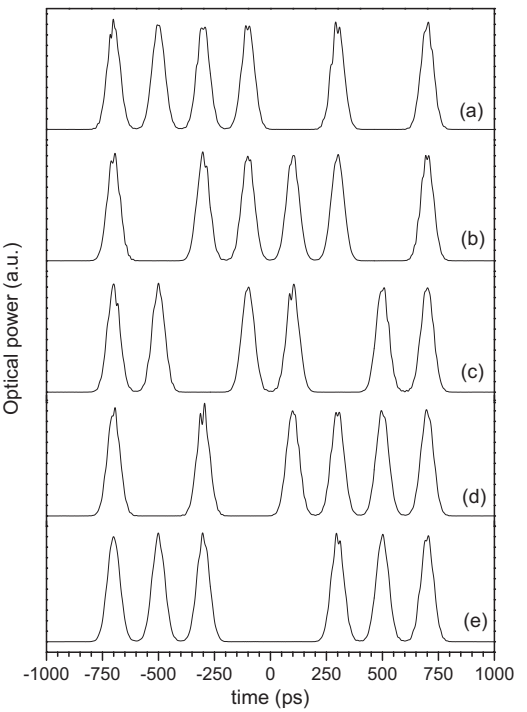

Fig. 7 Decrypted signal intensities corresponding to the inputs shown in Fig. 5: (a) $\hat{g}(t,\lambda_1)$, (b) $\hat{g}(t,\lambda_2)$, (c) $\hat{g}(t,\lambda_3)$, (d) $\hat{g}(t,\lambda_4)$, and (e) $\hat{g}(t,\lambda_5)$. All wavelengths are the same as in Fig. 5.

Figure 6(a) shows the intensity of an encrypted signal, viz., $\psi(t,\lambda_3)$, whereas Fig. 6(b) shows the total intensity of the simultaneous transmission of the five encrypted data streams, i.e., $\xi(t,\lambda_1,\ldots,\lambda_5)$. Their corresponding spectral powers are shown in Fig. 6(c) and 6(d); they are denoted by $\Psi(\nu,\lambda_3)$ and $\Xi(\nu,\lambda_1,\ldots,\lambda_5)$, respectively. It can be observed, by comparing Figs. 5(c) and 6(a), that the encrypted signal has temporally broadened, from $\Delta t_f^{(3)}=1.6$ ns to $\Delta t_\psi^{(3)}\approx 2.6$ ns. This last value compares reasonably well with the predicted value obtained by applying Eq. (13a), $\Delta t_\psi^{(3)}\approx 2.8$ ns, where the spectral extent of the input signal $\Delta\nu_f^{(3)}\approx 5$ GHz (i.e., $\Delta\lambda_f^{(3)}\approx 0.1$ nm) was directly obtained from the calculated spectra (not shown). Regarding the spectral extent, Fig. 6(c) shows that, as a consequence of the encryption process, it has increased to $\Delta\nu_\psi^{(3)}\approx 90$ GHz (i.e., $\Delta\lambda_\psi^{(3)}\approx 0.8$ nm), which also compares reasonably well with the value predicted by Eq. (13b), viz., $\Delta\nu_\psi^{(3)}\approx 99$ GHz. Finally, it should be taken into account that Eqs. (13a) and (13b) are approximate, in that they were obtained by assuming that signals are bounded in both time and frequency [see Eq. (3), where the time-frequency uncertainty principle is relaxed]. This is the main reason for the difference between obtained and calculated values.

After passaging through the multiplexer, all the encrypted signals are recombined, thereby sharing the same time window, which is a distinctive feature of WDM transmission.[10] For this reason the five channels together have the same total temporal extension as one single encrypted signal [see Fig. 6(b) as compared with Fig. 6(a)]. Finally, in Fig. 6(d) the whole five-encrypted-signal spectrum is shown, where it can be seen that there is no appreciable overlap between single-channel spectra.

Figure 7 shows the decrypted signals corresponding to the FTE encryption of the signals showed in Fig. 5. One can clearly observe the close resemblance between the inputs and decrypted signals. The small ripple present in the decrypted signal diminishes as the separation between channels enlarges; in this way, a compromise between noise and channel capacity must be reached. The separation between channels, $\Delta\nu^{(c)}$, depends on the frequency extent of the encrypted signal, see Eq. (13b). Until now, it has remained constant and equal to $\Delta\nu^{(c)}=100$ GHz, a value that is large enough to prevent severe crosstalk between channels [see Fig. 6(a)]. Figure 8 shows the behavior of a typical decrypted signal [viz., $\hat{g}(t,\lambda_2)$] when the separation between channels, $\Delta\nu^{(c)}$, is varied. In (a), $\Delta\nu^{(c)}=200$ GHz ($\lambda_2\approx 1548.51$ nm and $\lambda_3\approx 1550.12$ nm), yielding a better signal decryption than that shown in Fig. 7(b). In (b), $\Delta\nu^{(c)}=50$ GHz ($\lambda_2\approx 1549.72$ nm and $\lambda_3\approx 1550.12$ nm), and a worse decrypted signal is clearly observed. For both cases, the spectral powers are also shown in order to better illustrate the crosstalk effects [see Fig. 8(c) and 8(d)]. When $\Delta\nu^{(c)}\approx 50$ GHz, the decrypted signal presents a strong degradation because the selected separation between channels is smaller than the spectral extent of the encrypted signal, as can be easily observed in Fig. 8(d) and further checked with Eq. (13b).

As it was mentioned in Sec. 2.1, it is important to analyze the method's sensitivity to variation of its key parameters. We qualify the resemblance degree between the original signal and its decrypted counterpart with the signal-to-noise ratio (SNR) defined by

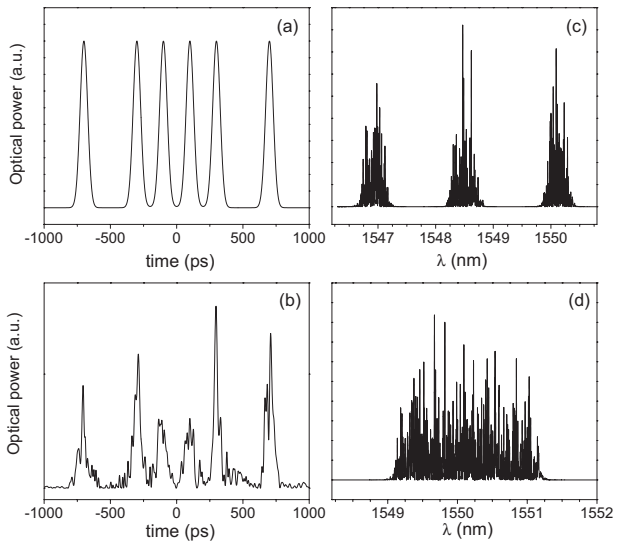

Fig. 8 Behavior of the intensity of a typical decrypted signal, $\hat{g}(t,\lambda_2)$, when the separation between channels, $\Delta\nu^{(c)}$, is varied: (a) $\Delta\nu^{(c)}\approx 200$ GHz ($\lambda_2\approx 1548.51$ nm and $\lambda_3\approx 1550.12$ nm), and (b) $\Delta\nu^{(c)}\approx 50$ GHz ($\lambda_2\approx 1549.72$ nm and $\lambda_3\approx 1550.12$ nm). The spectral power is also shown in both cases—(c) $\hat{G}(\nu,\lambda_2\approx 1548.51$ nm) and (d) $\hat{G}(\nu,\lambda_2\approx 1549.72$ nm)—between adjacent-channel power spectra, viz., $\hat{G}(\nu,\lambda_1)$ and $\hat{G}(\nu,\lambda_3)$, to better illustrate the crosstalk increment.

$$\mathrm{SNR}=10\log\left\{\frac{\int|f(t,\lambda_i)|^2\,\mathrm{d}t}{\int[f(t,\lambda_i)-|\hat{g}(t,\lambda_i)|]^2\,\mathrm{d}t}\right\}. \tag{14}$$

Figure 9 shows the SNR of a decrypted signal, viz., $\hat{g}(t,\lambda_3)$, as a function of the relative variation of the first dispersion coefficient (i.e., $\Delta\Phi_{20}^{(1,3)}/\Phi_{20}^{(T,3)}$) of the decryption stage $[r_1^*(t,\lambda_3)]$. From a cryptoanalysis point of view it is desirable to have a strong degradation of the decrypted signal as one, or several, key parameters change even slightly. However, this feature also makes difficult a practical implementation of any encryption setup. The behavior of this encryption setup shown in Fig. 9 is a compromise between these two considerations and can be considered acceptable performance.

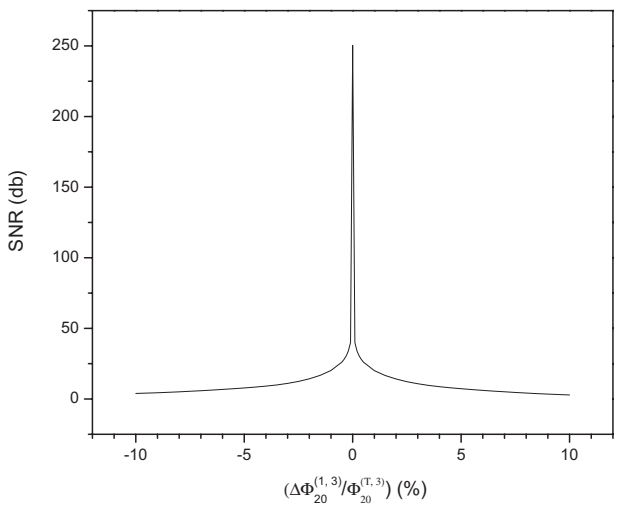

Fig. 9 Signal-to-noise ratio of the decrypted signal $\hat{g}(t,\lambda_3)$ as a function of the relative variation $\Delta\Phi_{20}^{(1,3)}/\Phi_{20}^{(T,3)}$ of the first dispersion coefficient of the decryption stage, $r_1^*(t,\lambda_3)$.

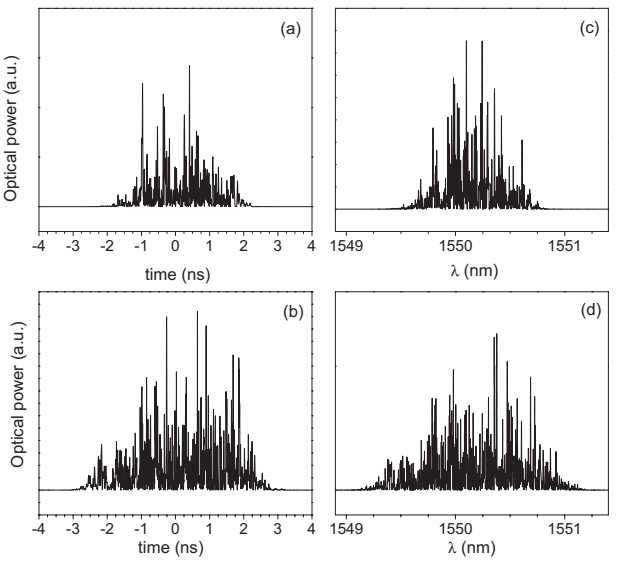

Fig. 10 Spreading behavior of the intensity of a typical encrypted signal [viz., $\psi(t,\lambda_3)$] as a function of the spectral extent $\Delta\nu_p$ of two different quasi-white noises: (a) $\Delta\nu_p\approx 90$ GHz, and (b) $\Delta\nu_p\approx 135$ GHz. The spectral power is also shown in both cases, in (c) and (d), respectively.

Finally, we study the behavior of an encrypted signal [viz., $\psi(t,\lambda_3)$] as a function of the spectral extent of three different quasi-white noises: (i) $\Delta\nu_p\approx 45$ GHz, (ii) $\Delta\nu_p\approx 90$ GHz, and (iii) $\Delta\nu_p\approx 135$ GHz. Case (i) was studied before and is repeated here only for comparison [see Fig. 6(a) and 6(c)]. Figure 10(a) and 10(c) and Fig. 10(b) and 10(d) show the encrypted signal and its corresponding spectra for cases (ii) and (iii), respectively. The temporal and frequency extents of the encrypted signal for the second and third cases, observed from Fig. 10, are: (ii) $\Delta t_\psi^{(3)}\approx 4.2$ ns and $\Delta\nu_\psi^{(3)}\approx 180$ GHz (i.e., $\Delta\lambda_\psi^{(3)}\approx 1.4$ nm), and (iii) $\Delta t_\psi^{(3)}\approx 5$ ns and $\Delta\nu_\psi^{(3)}\approx 220$ GHz (i.e., $\Delta\lambda_\psi^{(3)}\approx 2$ nm). These values compare reasonably well with those predicted from Eq. (13): (ii) $\Delta t_\psi^{(3)}\approx 4$ ns and $\Delta\nu_\psi^{(3)}\approx 190$ GHz, and (iii) $\Delta t_\psi^{(3)}\approx 5.1$ ns and $\Delta\nu_\psi^{(3)}\approx 270$ GHz.

4 Feasibility Considerations

Now we consider the experimental implementation feasibility of the proposed setup. The example studied throughout this work, as regards with the separation between channels, belongs to dense WDM (DWDM). In the case of applications using the entire frequency band between second and third transmission windows (between 1310 and 1550 nm), OH-free silica fibers could be used in order to fully exploit the WDM capacity of this encryption setup. These fibers nearly eliminate the OH attenuation peak, as well as establishing performance requirements in the L band, spanning the communication wavelength range from $\approx$1310 nm to $\approx$1625 nm, and allowing for full-spectrum operation. For instance, a full-spectrum single-mode fiber has typical dispersion values ranging from zero at $\lambda_0\approx 1317$ nm to D

≈ 20 ps/(nm km) (i.e., $\beta_2 \approx -28.5$ ps^2/km) at $\lambda \approx 1625$ nm.[†] By employing this fiber, and by considering the frequency spacing mainly used throughout this work (i.e., $\Delta\nu^{(c)} = 100$ GHz), ≈430 channels could be assigned for secure data transmission. Otherwise, with an ordinary single-mode fiber, ≈213 channels could be transmitted in both windows (≈170 and ≈43 channels in the second and the third window, respectively). Moreover, the wavelength dependence of the dispersion of the fiber optic link should be carefully considered in the experimental implementation.

Polarization-mode dispersion (PMD) induced by random birefringence in single-mode optical fibers can be the dominant source of pulse distortion in high-bit-rate transmission systems at great distances.[10] However, PMD coefficients of contemporary fibers can be as low as 0.02 ps/km$^{1/2}$. For the aforementioned full-spectrum fiber, the typical PMD value is lower than 0.06 ps/km$^{1/2}$. Because this encryption method was intended mainly for short-haul fiber optic links (e.g., metropolitan distances), PMD does not constitute a major problem in a WDM context.

5 Conclusions

The implementation of the WDM FTE technique in the temporal domain was studied to evaluate its potential application for secure data transmission in metropolitan fiber optic links. Decryption by an eavesdropper becomes impossible because of the large number of degrees of freedom involved and the vast number of possible permutations of parameter keys. Special emphasis was placed on analyzing the optical fiber multiplexing capabilities. We have found general expressions relating the temporal and frequency extents of the encrypted signal transmitted through the fiber optic link to the input signal and key parameters. As a result, a quasi-white-noise signal with a well-defined bandwidth is used to enhance the channel-number capacity in WDM.

With this proposal, we are introducing a novel alternative approach to the the problem of security by handling multiple data in a temporal dual random phase encoding in fiber optic links, something that has not been deeply explored using these techniques. Thus we present a new point of view with respect to multiplexing transmission mechanisms that expands the possible combinations of encrypted data within a given fiber optic link architecture.

Acknowledgments

This work was supported by the Consejo Nacional de Investigaciones Científicas y Técnicas (CONICET-PIP 6156/05), the Facultad de Ingeniería de la Universidad Nacional de La Plata (UNLP, Project I106), and the Agencia Nacional de Promoción Científica y Tecnológica (ANPCyT, PICT 2005 38289).

References

1. P. Réfrégier and B. Javidi, "Optical image encryption based on input plane and Fourier plane random encoding," *Opt. Lett.* **20**(7), 767–769 (1995).
2. G. Situ and J. Zhang, "A cascaded iterative Fourier transform algorithm for optical security applications," *Optik (Jena)* **114**(10), 473–477 (2003).
3. G. Unnikrishnan, J. Joseph, and K. Singh, "Optical encryption by double-random phase encoding in the fractional Fourier domain," *Opt. Lett.* **25**(12), 887–889 (2000).
4. G. Unnikrishnan and K. Singh, "Double random fractional Fourier-domain encoding for optical security," *Opt. Eng.* **39**(11), 2853–2859 (2000).
5. B. M. Hennelly and J. T. Sheridan, "Image encryption and the fractional Fourier transform," *Optik (Jena)* **114**(6), 251–265 (2003).
6. N. Towghi, B. Javidi, and Z. Luo, "Fully phase encrypted image processor," *J. Opt. Soc. Am. A* **16**(8), 1915–1927 (1999).
7. B. Javidi, N. Towghi, N. Maghzi, and C. Verrall, "Error-reduction techniques and error analysis for fully phase- and amplitude-based encryption," *Appl. Opt.* **39**(23), 4117–4130 (2000).
8. G. Situ and J. Zhang, "Double random-phase encoding in the Fresnel domain," *Opt. Lett.* **29**(14), 1584–1586 (2004).
9. G. Situ and J. Zhang, "A lensless optical security system based on computer generated phase only," *Opt. Commun.* **232**(1), 115–122 (2004).
10. G. Agrawal, *Fiber-Optics Communication Systems*, 3rd ed., John Wiley and Sons, New York (2002).
11. C. Cuadrado-Laborde, "Time-variant signal encryption by lensless dual random phase encoding applied to fiber optic links," *Opt. Lett.* **32**(19), 2867–2869 (2007).
12. J. Azaña and L. R. Chen, "General temporal self-imaging phenomena," *J. Opt. Soc. Am. B* **20**(7), 1447–1458 (2003).
13. L. Chen and D. Zhao, "Optical color image encryption by wavelength multiplexing and lensless Fresnel transform holograms," *Opt. Express* **14**(19), 8552–8560 (2006).
14. X. Peng, H. Wei, and P. Zhang, "Chosen-plaintext attack on lensless double-random phase encoding in the Fresnel domain," *Opt. Lett.* **31**(22), 3261–3263 (2006).
15. B. H. Kolner, "Space-time duality and the theory of temporal imaging," *IEEE J. Quantum Electron.* **30**(8), 1951–1963 (1994).
16. A. Papoulis, "Pulse compression, fiber communications, and diffraction: a unified approach," *J. Opt. Soc. Am. A* **11**(1), 3–13 (1994).
17. J. Azaña, L. R. Chen, M. A. Muriel, and P. W. E. Smith, "Experimental demonstration of real-time Fourier transformation using linearly chirped fibre Bragg gratings," *Electron. Lett.* **35**(25), 2223–2224 (1999).
18. J. van Howe and C. Xu, "Ultrafast optical signal processing based upon space-time dualities," *J. Lightwave Technol.* **24**(7), 2649–2662 (2006).
19. H. M. Ozaktas, Z. Zalevsky, and M. Alper Kutay, *The Fractional Fourier Transform with Applications in Optics and Signal Processing*, John Wiley and Sons, New York (2001).
20. J. Paye, "The chronocyclic representation of ultrashort light pulses," *IEEE J. Quantum Electron.* **28**(10), 2262–2273 (1992).
21. B. M. Hennelly, T. J. Naughton, J. McDonald, J. T. Sheridan, G. Unnikrishnan, D. P. Kelly, and B. Javidi, "Spread-space spread-spectrum technique for secure multiplexing," *Opt. Lett.* **32**(9), 1060–1062 (2007).
22. B. M. Hennely and J. T. Sheridan, "Optical encryption and the space bandwidth product," *Opt. Commun.* **247**,(4–6), 291–305 (2005).

Christian Cuadrado-Laborde received his PhD degree in physics from the National University of La Plata (UNLP, Argentina), and his Electrical and Electronic Engineer degree from the National University of San Luis, in 2005 and 1998, respectively. In 2005, he joined the Optical Research Center (CIOp, Argentina) as a full-time researcher of the National Council for Scientific and Technical Research (CONICET). Since March 2004, he has been an assistant professor of Modern Physics at the Faculty of Engineering of the UNLP. At present, he is a research fellow conducting photonic research at the University of Valencia (Spain). His current research interest includes fiber optics applications and fiber lasers.

[†]Typical values taken from the technical data sheet of the Corning® single-mode full-spectrum optical fiber SMF-28e+™.

Ricardo Duchowicz received his PhD and MS degrees in physics from the National University of La Plata (UNLP, Argentina) in 1981 and 1977, respectively. In 1977 he joined the Optical Research Center (CIOp, Argentina) as a full-time researcher of the National Council for Scientific and Technical Research (CONICET), where he worked on gas laser technology and dye laser physics. In the period 1984 to 1986 he had a fellowship from the Argentine government to conduct molecular laser spectroscopy research at Kaiserslautern University (Germany). His current research interests are in fiber optics studies and applications. He is also professor of physics in the Faculty of Engineering at UNLP. This year he became an OSA member.

Enrique E. Sicre received his PhD and MS degrees in physics from the National University of La Plata, Argentina, in 1981 and 1975, respectively. In the period 1982 to 2000, he worked as a full-time researcher (CONICET) at the Optical Research Center (CIOp, La Plata, Argentina). He was a fellow of the Alexander von Humboldt Foundation (Germany) three times between 1983 and 1994. He currently works at the Universidad Argentina de la Empresa (UADE) as a full professor. He has published extensively on subjects related to optical information processing, optical metrology, and, more recently, pulse transmission in fiber optic links.