Novel Super Structured Bragg Gratings for Optical Encryption

Jose M. Castro, Ivan B. Djordjevic, *Member, IEEE*, and David F. Geraghty, *Member, IEEE*

***Abstract*—A new type of optical encryption based on superstructured Bragg gratings is proposed. Security is provided by the transformation of the signal to noiselike patterns in the optical domain, which hides any structure to nonauthorized users. Encryption at speeds of several gigabits per second with low bit error rates is simulated.**

***Index Terms*—Code-division multiple access (CDMA), communication system security, gratings, optical communication, optical pulse shaping.**

I. Introduction

DURING the last decade, techniques such as quantum cryptography and chaotic encryption systems have been proposed to enhance the security of optical systems. These techniques use different approaches to provide security. In quantum cryptography, the eavesdropper detection is based on Heisenberg's uncertainty principle, which states that the observation of a quantum system unavoidably disturbs its state [1]. In chaotic cryptography, the dynamics of lasers in the chaotic regime are made to follow prescribed trajectories depending on the information to be transmitted [2]. For decoding chaotic trajectories, the synchronization between transmitter and receiver is necessary. While quantum cryptography has the potential to solve the problem of key distribution at moderate transmission rates, the encryption based on chaotic carriers can provide privacy at high transmission rates. However, the complexity level of both systems is still high.

Simpler approaches to improve security have been proposed using fiber Bragg gratings (FBGs) [3] and optical code-division multiplexing-access OCDMA systems [4]–[6]. Those schemes generate well-defined pulse sequences (chips) at selected wavelengths, which can be easily observed by an eavesdropper. Therefore, the security of these systems depends on the dimensionality of the code, which is very low in most of the cases. Recent analysis has shown that conventional cryptography provides a much greater degree of confidentiality than OCDMA encoding [7], [8].

In this paper, we propose and model a novel scheme to enhance security in optical systems using super structured Bragg gratings (SSBGs) with pseudorandom modulation. This type of SSBG is designed using couple mode theory and transfer matrix methods to produce noiselike impulse responses. The encryption process is performed in two steps: encoding and masking.

During the encoding process, the data is transformed into an optical noiselike pattern by the use of the pseudorandom SSBG (PR-SSBG). This step has similarities with spectral-phase-encoding OCDMA [6], [8]. However, there is an important difference. Spectral phase encoding produces either a noisy spectrum or a noisy temporal response but not both. A well-defined structure in the spectrum or temporal response provides ways to break the security using techniques previously reported [7], [8]. Our approach, using the proposed PR-SSBG, produces noiselike spectrum and noiselike impulse response since the amplitude and the phase are changed pseudorandomly.

In the masking process, the encoded signal is combined with a quasi-orthogonal noise generated by another set of PR-SSBG. This second step resembles the process of combining multiple CDMA channels [7]. The key difference is that noiselike sequences (no chips) are combined in an asynchronous way, producing a high variety of noisy patterns. The resultant signal to be transmitted is a noiselike sequence in which the structure of the bits in frequency and temporal domain is lost for an eavesdropper.

The advantages of our scheme are numerous. The encryption is performed in the optical domain simply using the PR-SSBG as a hardware key. There is no need to synchronize the noisy lasers. There is large time spreading (TS) produced by the PR-SSBG. Therefore, the average transmitted power can be reduced without reducing the energy per bit. The reduced transmitted power, the high optical bandwidth, and the pseudoorthogonal noise make the correct sampling and signal recovery for intruders challenging. When similar power is used for the information and pseudoorthogonal noise, the best signal-to-noise ratio (SNR) the eavesdropper can obtain is ~ 1. The noise in the eavesdropper's detector and the losses due to tapping would reduce his/her SNR even more. Conversely, low bit error rates (BER) for authorized users are easily attained through decryption, and a moderate power penalty can be achieved using the bandwidth similar to a standard wavelength-division-multiplexing (WDM) channel separation.

The remainder of this paper is organized as follows. In Section II, the structure, spectrum, and temporal response of the PR-SSBG are analyzed. Additionally, the algorithm to find a set of PR-SSBG with pseudoorthogonal impulse response is described. In Section III, the encryption and decryption scheme is explained. A simulation is presented as a demonstration of the concept. Section IV is devoted to the security analysis of the proposed scheme. Finally, Section V briefly presents the main conclusions of our study.

Manuscript received June 28, 2005; revised November 7, 2005. This work was supported by the National Science Foundation under Grant ITR 0325979.

The authors are with the Department of Electrical and Computer Engineering, The University of Arizona, Tucson, AZ 85721-0104 USA (e-mail: jmcastro@email.arizona.edu).

Digital Object Identifier 10.1109/JLT.2006.871028

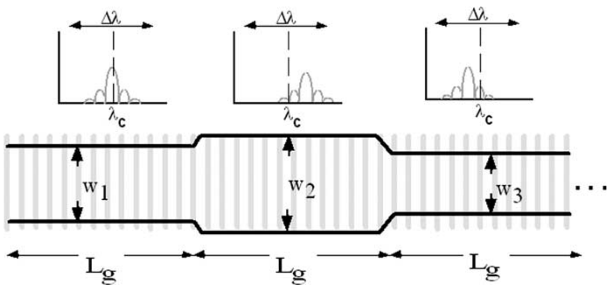

Fig. 1. Basic structure of the super structured random Bragg grating.

II. Pseudorandom Super Structured Bragg Gratings (PR-SSBG)

Bragg gratings have emerged as important components in a variety of optical applications. In their simplest form, BGs consist of a periodic modulation of the refractive index in optical fibers or channel waveguides, which provide reflection at a specific wavelength. Random phase and amplitude errors in the index modulation degrade the grating performance. They reduce the strength of the peak reflection, broaden the spectrum, and produce fluctuations in the phase response [9], [10]. However, for cryptography purposes, these disadvantages can be turned into desired characteristics.

A. Basic Structure and Spectrum

The PR-SSBG consists of a series of uniform gratings, which have similar bandwidths but slightly different Bragg conditions. The Bragg condition can be varied either by changing the grating period or by changing the effective index in the waveguide segment. The latter approach requires simpler fabrication processes, because a grating of fixed periodicity can be used for all grating segments. The effective index can be slightly changed either by UV trimming of photosensitive materials [11] or by small changes in the waveguide width as shown in Fig. 1. Controlling the waveguide width is both accurate and trivial for integrated optic chips, as it is simply defined in the mask layout. For simplicity and without loss of generality, the second approach is assumed. Small width changes $\sim 0.4\ \mu$m require small tapering lengths $(< 10\ \mu\text{m})$ in order to allow adiabatic propagation [12] in the waveguide. These short tapered sections can be ignored in the calculations of reflectivity due to their length.

The grating period is determined by [11] as

$$\Lambda = \frac{\lambda_c}{2n_{\text{eff}}(w_{\text{ave}})} \tag{1}$$

where w_{ave} is the average width, n_{eff} is the effective index of the waveguide as a function of the width, and λ_c is the desired center wavelength.

The Bragg wavelength in each segment of length L_g can be obtained as

$$\lambda_i = \lambda_c \frac{n_{\text{eff}}(w_i)}{n_{\text{eff}}(w_{\text{ave}})} \tag{2}$$

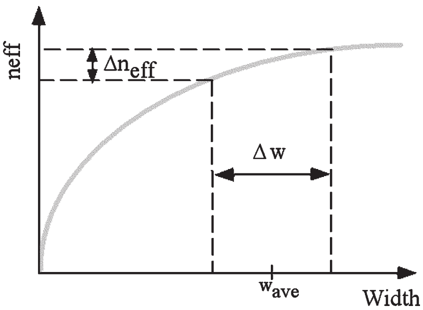

Fig. 2. Effective index as a function of the width in each grating segment.

where w_i is the width of the ith segment. The range of required segment widths to produce the desired changes in the effective index is shown in Fig. 2. The width is changed in discrete steps determined by waveguide fabrication resolution.

The spectrum of PR-SSBG is computed using the transfer matrix method [11]. This method is in excellent agreement with experimental results not only for standard apodized gratings but for random grating arrays [13]–[15] as well. The basic procedure is described here. The parameters of each segment are related to the matrix

$$T(w_i,\lambda) = \begin{vmatrix} T_{11}(w_i,\lambda) & T_{12}(w_i,\lambda) \\ T_{21}(w_i,\lambda) & T_{22}(w_i,\lambda) \end{vmatrix} \tag{3}$$

where λ is the wavelength of the incoming signal, and the elements of the matrix are defined as

$$\begin{aligned} T_{11}(w_i,\lambda) &= \cosh\left(\sqrt{Kac^2-\delta^2(w_i,\lambda)}L_g\right) \\ &\quad - \frac{j\delta(w_i,\lambda)\sinh\left(\sqrt{Kac^2-\delta^2(w_i,\lambda)}L_g\right)}{\sqrt{Kac^2-\delta^2(w_i,\lambda)}} \end{aligned} \tag{4}$$

$$T_{12} = -\frac{jKac\,\sinh\left(\sqrt{Kac^2-\delta^2(w_i,\lambda)}L_g\right)}{\sqrt{Kac^2-\delta^2(w_i,\lambda)}} \tag{5}$$

$$T_{22} = T_{11}^* \qquad T_{21} = -T_{12}. \tag{6}$$

The detuning and coupling coefficients can be determined by

$$\delta(w_i,\lambda) = \frac{2\pi}{\lambda}n_{\text{eff}}(w_i) - \frac{\pi}{\Lambda} \tag{7}$$

$$Kac = \frac{\pi}{\lambda}\Delta n\eta \tag{8}$$

where Δn is the index modulation, and η is the overlap integral between mode profiles of the incoming and reflected signals. The detuning parameter δ describes the shift from the Bragg condition in each grating segment. For a specific wavelength, δ changes as a function of the segment width. On the other hand, the coupling strength of every grating segment is kept constant, as shown in (8).

The matrix resultant of the interaction $T(\lambda)$ of M consecutive grating segments is given by

$$T(\lambda) = \prod_{i=1}^{M} T(w_i,\lambda). \tag{9}$$

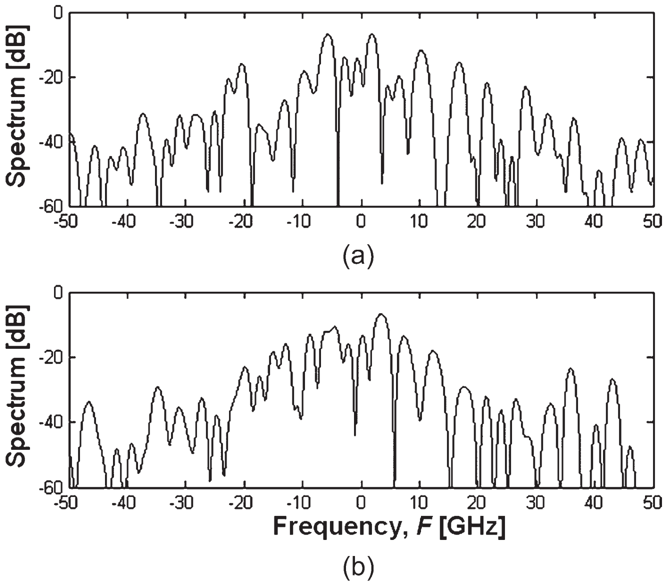

Fig. 3. Spectrum of two PR-SSBGs generated using the parameters from Table I. Relative frequency centered at 193.548 THz.

TABLE I
PARAMETERS OF PR-SSBG USED IN THE SIMULATION

Parameter	Symbol	units	Value
Total Length	L_t	cm	5
Segment Length	L_g	µm	200
Index modulation	Δn		4x10^{-5}
Neff span	Δn_{eff}		8x10^{-4}
# Neff levels	L		4
Normalized maximum cross-correlation peak	ρ		0.25

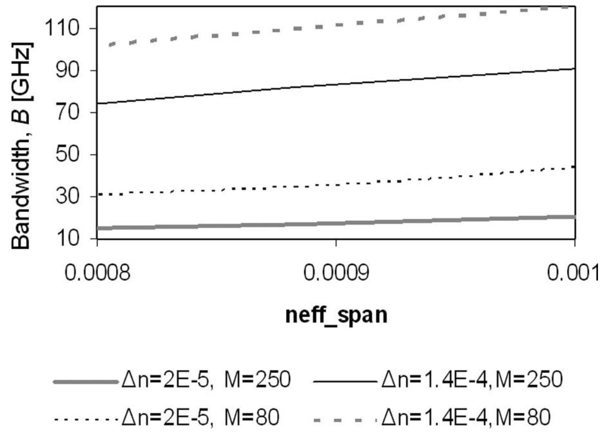

Fig. 4. 10-dB bandwidth for a system with $L_t = 50mm$, different segment lengths L_g, and modulation indices Δn as a function of the span effective index.

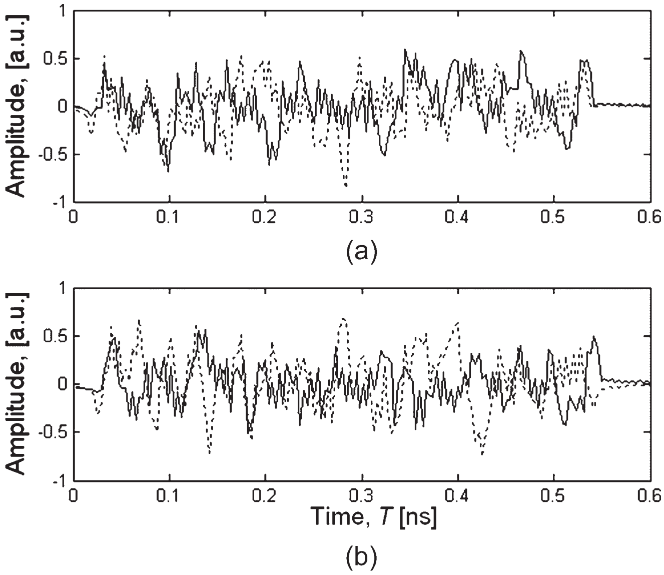

Fig. 5. Responses of two PR-SSBGs to a Gaussian pulse with 10 ps of duration. Real and imaginary terms are represented as solid and dashed lines, respectively.

From this matrix, the reflection can be obtained as

$$r(\nu) = \frac{T_{21}\left(\lambda = \frac{c}{v}\right)}{T_{11}\left(\lambda = \frac{c}{v}\right)}. \tag{10}$$

As opposed to typical Bragg gratings, the reflection spectrum (both the amplitude and the phase) of the PR-SSBG is not necessarily symmetric with respect to the center frequency. Fig. 3 shows the reflection spectrum for two different PR-SSBGs, with parameters described in Table I. The spectrum asymmetry introduces both amplitude and frequency modulations of the optical carrier.

The bandwidth (B) of PR-SSBG and the time duration of its impulse response (Δt) are important parameters in the design of the proposed security system. The higher the product $B\Delta t$, the higher the number of PR-SSBG with quasi-orthogonal impulse responses. As opposed to typical Bragg gratings, the parameters B and Δt can be controlled independently. The bandwidth depends on Δn, the effective index span Δn_{eff}, and M. The PR-SSBG 10-dB bandwidth for a grating length (L_t) of 5 cm, with different Δn and M, is shown in Fig. 4 as a function of the span effective index. It can be seen that B increases as the effective index span or Δn increases. In addition, B increases as M decreases. The impulse response can be computed from the grating spectrum [15], [16] using the low-pass representation [17]. Most of the impulse response power is within the time slot equal to the forward and backward propagation time through the grating (weak grating condition). Therefore, its time duration can be determined by

$$\Delta t \approx \frac{2n_{\mathrm{eff,ave}}L_t}{c} \tag{11}$$

where c is the speed of light, $n_{\mathrm{eff,ave}}$ is the average effective index of the PR-SSBG, and L_t is the total length of the grating.

For example, in our model, the gratings are interrogated by Gaussian pulses of $\sim$ 10 ps in duration. The impulse responses (low-pass representation) for two different PR-SSBGs (see Fig. 3) are shown in Fig. 5. The complex value of that signal indicates the amplitude and phase modulation. As it is shown, most of the power is contained in a time slot of 500 ns, which corresponds to a length of 5 cm using (11) and Table I parameters. The spreading introduced by the PR-SSBGs reduces the power of the incoming pulses and transforms their patterns. Clearly, the Gaussian pulses has been converted to two noiselike signals, which have low cross correlation, as will be shown in the next section.

B. Code-Set Generation

The previous section shows that the transformation of short pulses (information bits) into noiselike patterns can be performed by PR-SSBGs. Each different PR-SSBG produces a different pattern. The number of possible patterns that can be generated is given by

$$N_g = L^M \tag{12}$$

where L is the number of discrete levels in which the effective index can be changed. For typical parameters as shown in Table I, N_g is extremely high. Nevertheless, not all patterns can be used simultaneously. Only the set of PR-SSBGs with minimum cross correlation can be used to provide security in a communication channel with low BER.

The autocorrelation and cross-correlation responses of a PR-SSBG decryptor is shown in Fig. 6. The PR-SSBG decryptor has the conjugate spectrum of the original grating used to produce the input signal shown in Fig. 5(a). The conjugate pattern, produced simply by reversing the original PR-SSBG, performs as an optical autocorrelator. Fig. 6(b) shows the normalized response of the same PR-SSBG decryptor to a nonmatched signal shown in Fig. 5(b). The normalized cross-correlation coefficient is ~ 0.25.

The maximum number of PR-SSBGs that can generate impulse responses with prespecified maximum cross-correlation peak (ρ), bit rate ($R = 1/\Delta t$), and B defines the cardinality (C) of the codes used for encryption. A set of PR-SSBGs is obtained by random search using the following algorithm.

Step 1) The effective index as a function of the width is obtained from experimental data or by simulations. An average width is computed for a given grating periodicity using (1) to obtain a desired center wavelength. The width span (or effective index span) determines the optical bandwidth used, as shown in Fig. 4.

Step 2) The length of the gratings is computed for a given bit rate. For instance, to obtain $R = 2$ Gb/s, a TS of ~ 500 ps is needed to fill the bit interval. A higher spreading would produce an excessive overlap between adjacent bits and degrade the system performance. For refractive index ~ 1.5 in (11), the length is approximately 5 cm.

Step 3) An initial value for the modulation index $\sim 10^{-4}$ is assumed. The index modulation should be small enough to allow the propagation of the pulse throughout the grating length.

Step 4) The segment widths are expressed as units of the minimum width resolution in a vector (V). The length of this vector is equal to the number of segments M. For example, for a 16-segment PR-SSBG, the four-level vector can be written as $V = (0, 1, 1, 3, 3, 2, 2, 1, 0, 0, 1, 2, 3, 0, 1, 3, 2)$.

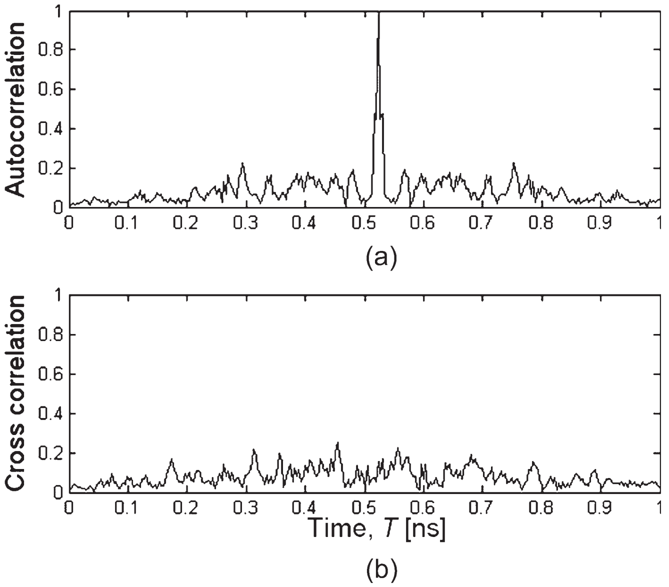

Fig. 6. Normalized autocorrelation and cross-correlation functions for signals shown in Fig. 5.

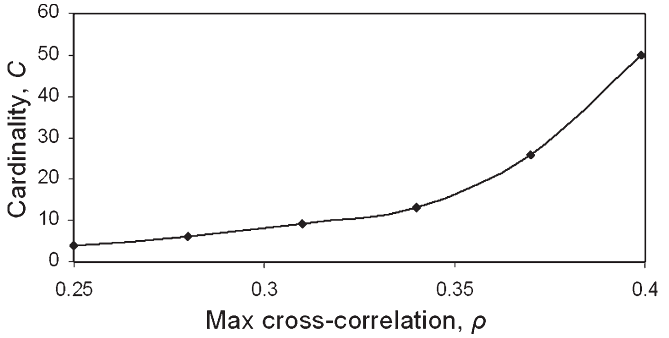

Fig. 7. Cardinality of the set of SSBGs found for 100-GHz bandwidth 2-Gb/s rate as a function of the normalized maximum cross-correlation.

Step 5) An initial V is pseudorandomly generated. The impulse response of the PR-SSBG that has that width profile is computed and stored as a first element of the set. A maximum number of iterations for the random search is defined.

Step 6) Another vector is pseudorandomly generated. The impulse response of the PR-SSBG with that profile is cross correlated with previous impulse responses already in the set. If the absolute value of the cross-correlation peak is lower then the maximum prespecified value, the new profile (grating) is included in the set.

Step 7) Step 6 is repeated until the maximum number of iterations is reached.

Step 8) Steps 5–7 are repeated for different modulation indices. The set that provides the maximum number of PR-SSBGs for a specified bandwidth is selected.

The maximum number of PR-SSBGs for $B \cong 100$ GHz and $R = 2$ Gb/s is shown in Fig. 7 as a function of ρ. It can be seen that the cardinality increases as the maximum cross-correlation coefficient increases. This increment can be used to generate more noiselike sequences to increase confidentiality. However,

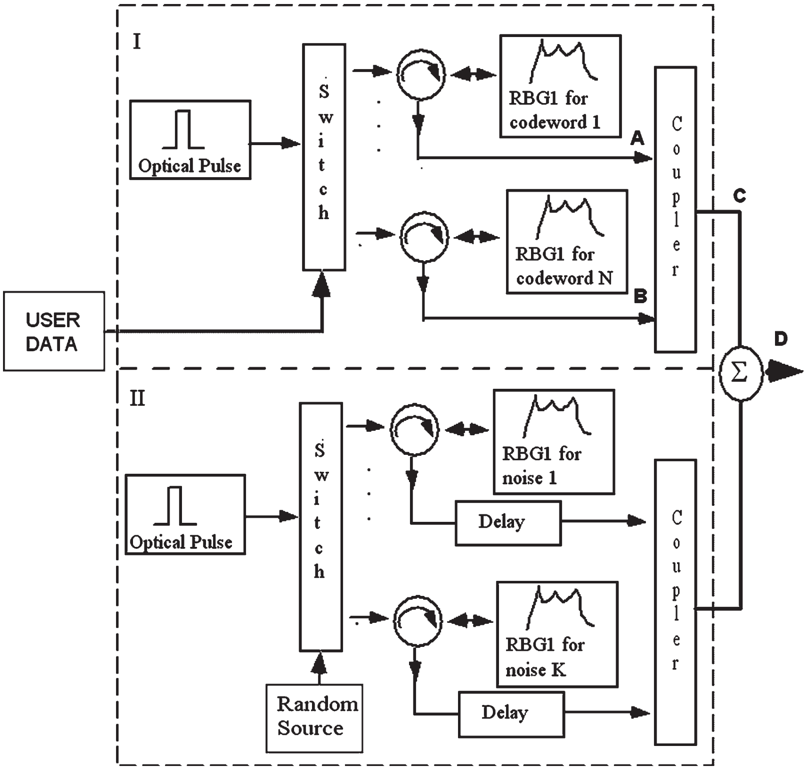

Fig. 8. Transmitter configuration.

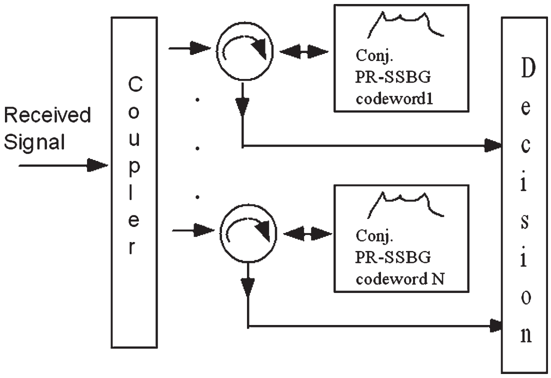

Fig. 9. Receiver configuration.

higher ρ degrades the BER of authorized users. It should be noted that for given parameters (ρ, R, B), several sets of size C can be generated. A pair of PR-SSBGs obtained from different sets would not be quasi-orthogonal. However, these different sets can be used for code reconfiguration.

III. Description of Encryption Scheme

The basic operation of the proposed scheme is explained here. The elements of the system, the transmitter, and the receiver are described first. The performance of the proposed approach is evaluated by simulations.

A. *Transmitter and Receiver Configurations*

The key idea behind the proposed scheme is to transform user codewords into noiselike sequences using PR-SSBGs. These gratings are designed to minimize the cross-correlation peaks between their impulse responses as explained previously. The transmitter, as shown in Fig. 8, consists of two sections. In Section I, user codewords electrically switch the optical pulses among different PR-SSBGs using the data signal. This can be accomplished with a $1 \times N$ LiNbO$_3$ modulator. The output of the gratings is redirected to a common port. In Section II, the pseudorandom codewords switch the optical pulse between different PR-SSBGs. The output of all gratings is again redirected to a common port, and the random delays generated either thermally or electrically are introduced before the outputs merge together. The noise components produced in this section are quasi-orthogonal with respect to the signal resultant from the user (Section I). In the last step of the encoding process, the outputs of both sections are combined. The rate of optical pulses is slightly different for the information and pseudorandom codewords. This rate difference in addition to the random delays increases the resultant pattern diversity.

Fig. 9 shows the configuration of the receiver. It contains the set of conjugate PR-SSBGs to decode the information bits. The sizes of the set and the pseudonoise components determine the degree of security. The higher the cardinality, the more unpredictable the noisy pattern for an eavesdropper; as a consequence, the more secure the channel will be. The cardinality can be increased by increasing L_t and B of the PR-SSBG and by increasing the allowed maximum cross-correlation coefficient ρ between their impulse responses.

However, there are several tradeoffs. From (11), it can be seen that the time duration increases as L_t increases, and the feasible bit rate is reduced. Increasing B reduces the spectral

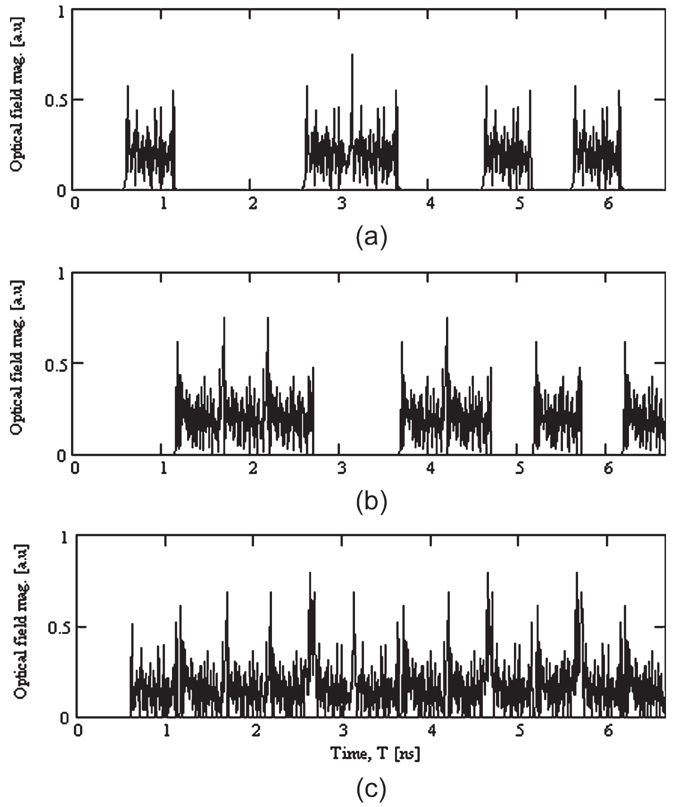

Fig. 10. (a) Signal for ones in the user sequence “100011001010” observed at Point A of the cipher (Fig. 8). (b) Signal for zeroes in the user sequence “100011001010” observed at Point B of the cipher (Fig. 8). (c) Sequence for ones and zeroes at point C of the cipher (Fig. 8).

efficiency of the system working at a given R. The increase of ρ should not degrade the SNR of the user that possesses the complete set of SSBGs (information bits and pseudonoise). At least in theory, that user should be able to reconstruct the noise pattern and subtract it from the signal. However, that would increase the receiver complexity and make the implementation more challenging. In our analysis and simulations, it is assumed that the noise cancellation is not performed. Therefore, there is an effective power penalty due to ρ.

B. Numerical Simulation

As the proof of concept, the simplest version of the system is modeled here. In this example, information bits instead of codewords are encoded. PR-SSBGs with parameters listed in Table I and input sources of 10-ps duration are used. The cardinality of the set used for $\rho < 0.25$ is four.

Two PR-SSBGs are used for the information bits and another two are used to produce the quasi-orthogonal noise. Fig. 10(a) and (b) shows the resultant sequence after the pulse is reflected by the gratings for 1 and 0 bits. The user rate is 2 Gb/s. It can be seen that the input pulse is spread from 10 to 500 ps and that it would be relatively easy to simply decrypt the encoded 1s. While the power has been spread into noise, it is still confined to the individual bit periods. This is equivalent to the security provided by two-dimensional wavelength-time OCDMA encryption. This illustrated the need for encrypting 0 bits for additional security.

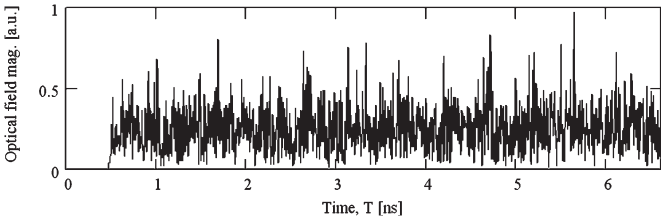

Fig. 11. Signal after noise masking at the output of the encryptor (Point D in Fig. 8).

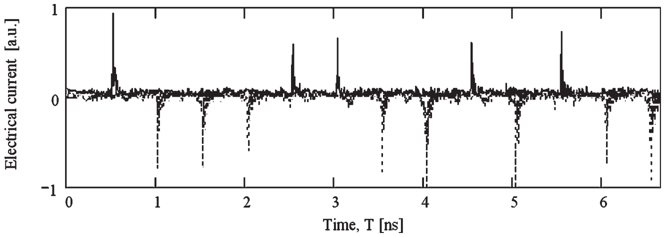

Fig. 12. Signal recovered at the detector of a 40-GHz bandwidth by SSBG operating as a matched filter. The positive peaks (solid line) represent the ones, whereas the negative ones (dashed line) represent the zeroes.

The output of the first section of the cipher (point C in Fig. 8) is shown in Fig. 10(c). Despite the noisy aspect of the individual bits, their patterns could potentially be identified by an eavesdropper capable of sampling at frequencies of 100 GHz with a enough high SNR [8]. However, when the quasi-orthogonal noise is added with different time delays, the noise pattern is difficult to predict. The result of this masking is the hidden structure of the transmitted information as shown in Fig. 11. At the receiver side, using appropriate PR-SSBGs (matched to the transmitter PR-SSBGs), the 0 and 1 bits can be recovered, as shown in Fig. 12. As previously mentioned, the signals from the PR-SSBG are not completely orthogonal; therefore, there is a power penalty due to the nonZERO cross correlation. The BER for the systems both without [Fig. 10(c)] and with the masking noise (Fig. 11) is shown in Fig. 13. After the first step, the Q-factor penalty with respect to a standard WDM channel is small. After the second step, which produces an SNR of ~ 1 for an eavesdropper, the penalty in Q factor is about 4.5 dB for a BER 10^{-8}. The power penalty can be reduced by finding a set with lower ρ or by reducing the power of the pseudonoise. The second approach would increase the SNR of the eavesdropper and reduce the security of the system.

In conventional WDM systems, a Q penalty of 5 dB could be difficult to compensate by increasing the launched power due to nonlinear effects. However, in our scheme, the signal power is 20 dB lower than that in conventional WDM systems due to the spreading of the encrypted signal. Therefore, the transmitted power can be increased by 5 dB without entering into the nonlinear regime. The peak power is recovered in the decryption process at the receiver. Therefore, a low BER is possible while maintaining the eavesdropper SNR below 1.

IV. Security Analysis

Security analysis of optical CDMA systems employing the TS/wavelength hopping (WH) using multiple signal combination is analyzed in [7]. It has been shown that the error-free

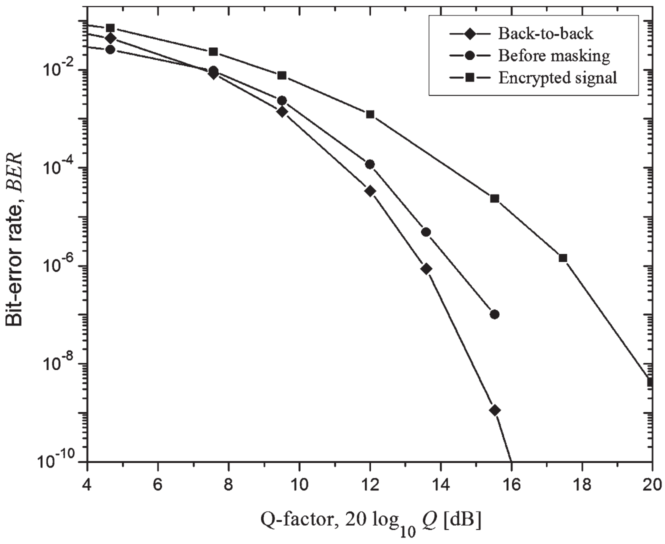

Fig. 13. Limits for a computational secure channel.

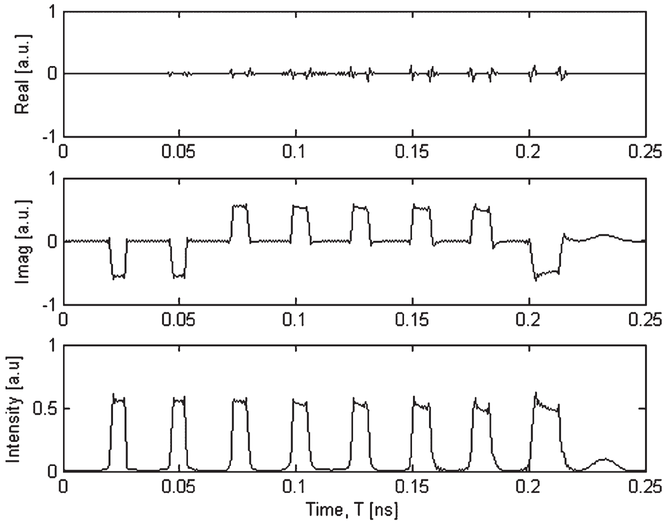

Fig. 14. Temporal phase encoding using a bipolar code of length 8.

code detection is possible for an eavesdropper with an SNR of 12 dB or higher. The reason for this modest performance is the predictability in the patterns that can be generated by the superposition of TS/WH CDMA signals.

Phase-encoding OCDMA can provide a much greater degree of confidentiality [8] than standard TS/WH CDMA systems. However, the security can be broken when the eavesdropper taps the signal either before or at the entry points of the network [7]. Proposed schemes in phase-coding OCDMA [4]–[6] have either a well-structured spectrum or impulse response for an easy implementation of spectrally efficient bipolar codes such as Kasami or Gold sequences [18]. However, a well-defined structure of either frequency bin or time chip is detrimental for security purposes.

Phase encoding using a structured Bragg grating [5] can generate a noisy spectrum. However, it produces a well-structured impulse response as shown in Fig. 14. The limited bandwidth of the detector used in [5] may get impression of having a noiselike temporal profile. However, assuming that the eavesdropper can sample the signal at a proper rate, the chip structure becomes clear (see Fig. 14). The phase can be recovered using standard techniques of coherent communication systems [6], [19].

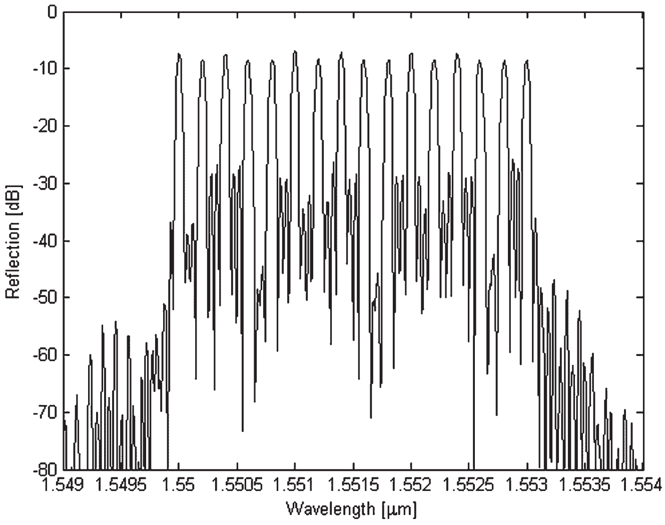

Fig. 15. Spectral-phase encoded using 16 frequency bins.

Spectral phase encoding [4] can produce noiselike impulse responses. However, as shown in Fig. 15, the structure of the spectrum is very well defined. This structure is required to divide the spectrum in the frequency bin in which the phase will be affected by the code. Similarly, the eavesdropper would be able to recover the phase using techniques described in [8].

The encryption scheme presented in this paper produces a noiselike impulse response and a noiselike spectrum profile due to the pseudorandom structure of the grating. There is no structure in the impulse response that can resemble temporal chips. Moreover, the slight variation in the Bragg condition on each segment of the PR-SSBG produces overlaps in the spectrum, which avoids any structure that can be used to identify frequency bins. To further improve the security, this encoded signal is masked using a quasi-orthogonal noise. The combination of two sequences (masking noise and encoded signal) produces a variety of noiselike patterns that hide the user information, as shown in Fig. 11. The security provided for this scheme depends on the capability of generating a high diversity in the noisy patterns.

Under Kerckhoff's principle [20], the eavesdropper knows the encryption algorithm. Only the structure of the PR-SSBGs is kept secret. To uncover the information from the transmitted sequence, an eavesdropper needs to sample the signal at 100 GHz or higher and observe all the possible patterns that can be generated during the encoding process. Sampling rates for signals of 100 GHz or more seem prohibitively fast for eavesdropping. However, a high optical bandwidth can be divided in smaller bins by gratings. The relative phase of each bin can be determined by measuring the beating signal after the detector [8].

If the pseudonoise (Section II of transmitter) and information sequences (Section I of transmitter) were synchronous, the number of possible patterns per bit would be equal to the

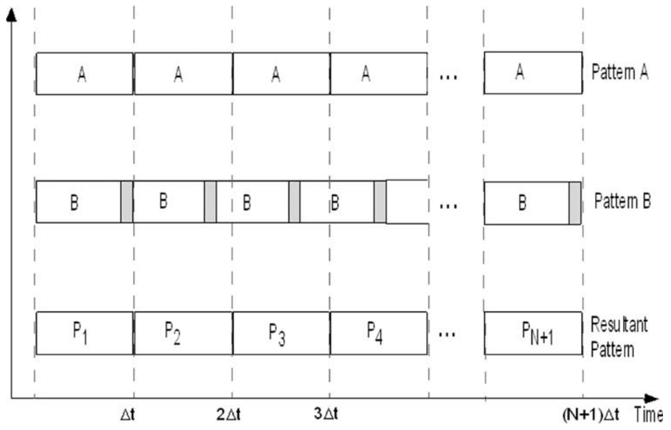

Fig. 16. Combinations of two patterns with slightly different rate. Shadow area indicates the overlap.

number of PR-SSBGs used to encode the noise. In the previous example, only two patterns per bit would be generated. Therefore, the security of the system would depend only on the capability of an eavesdropper to sample weak and high-bandwidth signals. However, the use of different bit rates for masking (R_m) and encoded signals (R_e) produces a diversity of noisy patterns since the masking noise is continuously shifted in time with respect to the encoded signals.

However, the bit rate difference $(R_e - R_m)$ should be kept small in order to avoid excessive overlap between adjacent encoded or masking patterns when similar lengths for PR-SSBG are used. An excessive overlap can provide information to the eavesdropper about the beginning and end of the patterns. The usage of similar lengths for the complete set of PR-SSBG is a desirable property that simplifies the design of codes and gratings with the required correlation properties.

For example, for a PR-SSBG with lengths of $L_t = 5$ cm and $\Delta t = 500$ ps, the rate for the encoding signal is set to 2 Gb/s. The rate of the masking signal to provide less than 10% variation is $R_m < 2.2$ Gb/s and can be determined using the following inequality:

$$\frac{\Delta t - \frac{1}{R_m}}{\Delta t} < 0.1. \tag{13}$$

Fig. 16 shows the process in which different patterns P_i are generated when patterns A (encoded signal) and B (masking signal) are transmitted at slightly different rates. In principle, by making the temporal shifts infinitesimally small, infinite patterns can be generated. However, there is a limitation in generating different patterns. Patterns A and B can be reconstructed using a limited number of points given by the Nyquist–Shannon sampling theorem [17]

$$N_s \approx \left\lfloor \frac{\Delta t}{T_s} \right\rfloor \tag{14}$$

where $T_s = 1/2B$ is the sampling period, and $\lfloor\ \rfloor$ denotes the largest integer less than or equal to the enclosed quantity.

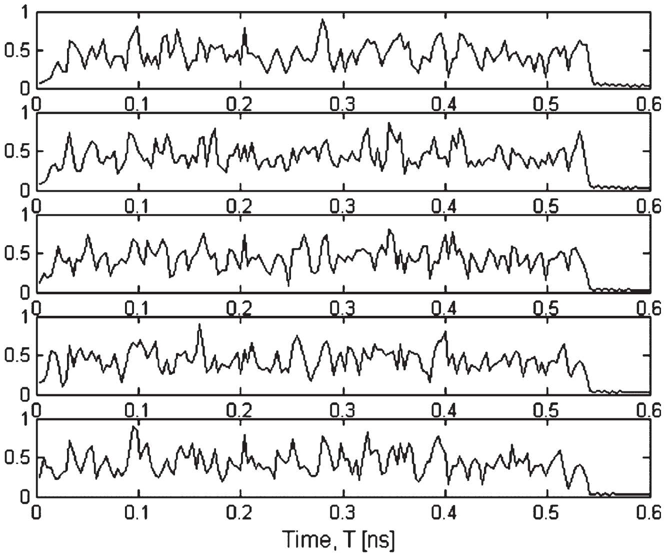

Fig. 17. Normalized power for five consecutive patterns resulting from the asynchronous and incoherent combination of signals shown in Fig. 5.

Since temporal shifts less than T_s would produce essentially similar patterns, the number of different patterns is reduced to at most N_s. For example, using the signals shown in Fig. 5 as A and B ($\Delta t = 500$ ps and $B = 100$ GHz), the maximum number of patterns that can be generated is $N_s = 100$. Five consecutive patterns produced by the combinations of A and B with a temporal shift of 6 ps are shown in Fig. 17.

Another limitation to produce N_s patterns is the predetermined rate for the masking and encoded signals. Assuming that temporal shifts lower than T_s can be neglected, the maximum period of time before the combination of A and B start repeating is given by

$$T \approx T_s \mathrm{LCM}\left(\left\lfloor \frac{1}{R_e T_s} \right\rfloor, \left\lfloor \frac{1}{R_m T_s} \right\rfloor\right) \tag{15}$$

where LCM denotes the least-common-multiple function. When the rate of the encoding signal (R_e) is fixed to $1/\Delta t$ and the rate difference is small, the maximum number of patterns is

$$N_p \approx \frac{\frac{T}{T_s}}{\left\lfloor \frac{\Delta t}{T_s} \right\rfloor}. \tag{16}$$

For the previous example with $B = 100$ GHz, $R_e = 2$ Gb/s, and $R_m = 2.1$ Gb/s, the maximum number of patterns is 19.

Therefore, due to the fixed rates, not all the delays between A and B are possible. The efficiency for this pattern diversity f is determined by the ratio between the actual number of patterns generated N_p and the maximum number of possible patterns N_s. In the example above, this efficiency is almost 20%. This efficiency can be improved by minimizing the difference $1/R_e - 1/R_m$ while keeping this value higher than T_s.

For the simulation given in previous section, there are two quasi-orthogonal noise patterns C and D combined with each bit pattern A (bit ONE) and B (bit ZERO). In that case, each bit pattern combines randomly with three possible consecutive noise patterns: C–C, C–D, and D–D. This combination, using different time delays, can generate up to 300 patterns/bit.

In general, the maximum number of patterns per codeword is given by

$$N_p \approx f N_s \frac{K(K+1)}{2} \tag{17}$$

where K is the number of gratings used to generate the pseudonoise.

For a system that uses m codewords, an eavesdropper will observe mN_p patterns. However, he/she will not be able to know which pattern corresponds to each codeword. Assuming equiprobable codewords, the number in which the patterns can be arranged can be obtained using the hypergeometric distribution

$$U = \frac{(mN_p)!}{N_p!^m}. \tag{18}$$

For the previous example, assuming a modest efficiency $f = 5\%$, an eavesdropper would observe ~ 30 different sequences. To determine which of them corresponds to bit ONE or ZERO, the number of required combinations is $\sim 10^8$. Therefore, the four PR-SSBGs shown for demonstration would not provide very high security enhancement for an eavesdropper capable of sampling noisy and high-bandwidth signals. However, the level of security increases rapidly by increasing the number PR-SSBGs. For example, using seven PR-SSBGs (four for codewords and three for noise) with the same bandwidth and rate, $U > 10^{60}$. For the present computer speeds, this is an extremely large value. Therefore, longer periods between code reconfiguration can be used.

Since the rates R_e and R_m are fixed, the maximum number of patterns per codeword is limited by (17). The efficiency f can be increased by properly tuning the repetition rates of the encoding and masking signal. Pulse generators can allow tunable repletion rates by changing the cavity length in case of mode locked lasers or by changing the beating frequency in case of dual-wavelength light sources [21]. Careful control is usually required in these types of pulse generators to minimize pulse jitter. For our encryption scheme, the control is not necessary, as a pulse jitter would have the beneficial result of increasing the pattern diversity.

To increase the number of patterns, random delays can be utilized. Random delays also increase the security of the system by erasing traces of periodicity in the spectrum. Peaks that indicate periodicity can appear in the spectrum for long repetitive sequences due to the fixed rates.

To produce noticeable variations in the pattern, the required delay should shift the masking noise by at least the sampling time T_s. Faster scanning rates produce better results. However, for practical purposes, an important increase in U is produced when the scanning rates of the delays can produce changes before the mN_p patterns are seen by the eavesdropper. This means that the minimum scanning rate (SR) is limited to

$$\text{SR} > \frac{|R_m - R_e|}{mN_p}. \tag{19}$$

For the values used in previous examples, $B = 100$ GHz, $R_e = 2$ Gb/s, $R_m = 2.1$ Gb/s, $m = 2$, and $N_p = 30$. The required scanning rate is > 1.7 MHz, and the scan span is > 5 ps.

Several techniques have been proposed to generate delays using scanning mirrors, acoustooptic modulators, or deflectors. A scanning mirror can produce long delays; however, its SR is limited to a few kilohertz. On the other hand, acoustooptic devices can provide scanning rates on the order of 1 MHz [22]. Recently, a technique to provide very fast scanning rates and low distortion using time prism was demonstrated [23]. This technique can produce very high scanning rates (< 500 MHz) with a delay span in the range of 19 ps. Using these demonstrated technologies, the random signal generated at the transmitter can produce the required rates and span for the delays.

A. Code Reconfiguration

As mentioned in Section II, for the given parameters (ρ, R, B), there are many sets of the same cardinality. Therefore, the confidentiality of the proposed scheme can be increased by frequently allowing changes of the code set. The time interval between code reconfigurations would depend on the difficulty to decipher the codes (U). The code reconfiguration can be produced by physically changing the complete set of PR-SSBGs, by optically switching among a set of gratings, or by adding tunability to the gratings. However, the later approach is the most difficult to implement since each small grating section need to be tuned independently.

The simpler approach is switching between PR-SSBG sets. The fabrication of devices that can be used as a core structure for the ciphers was demonstrated using ion-exchange techniques and photosensitive-glass [24] and silica-on-silicon technology [25], [26]. The signal can be encoded and redirected by this compact device [26]. Hundreds of encoders can be placed in a chip using an area as small as 2×5 cm^2 without the need of circulators. A conventional optical switch can be used to change the set of PR-SSBG.

The change of the PR-SSBG set should be performed in an unpredictable way for the eavesdropper. The use of the proposed scheme with traditional cryptography techniques for key generation would enhance the level of security even more. The eavesdropper would need to know the structure of PR-SSBGs and the key that governs the change of their structure.

B. Eavesdropper Detection

To improve his SNR, the eavesdropper would need to take more power from the transmitted signal. A drop in power or an increase in noise due to optical amplification would increase the BER. If the pseudonoise sequence seed is known by the receiver, the BER can be estimated. In the previous example (BER shown in Fig. 13), the drop in Q factor from 11 to 10 would increase the number of bit errors ten times. At 2 Gb/s, these changes can be detected quickly, and a decision can be taken to change the set of PR-SSBGs.

V. Conclusion

A low complexity approach to effectively enhance security in optical channels was presented. Our approach uses PR-SSBGs to produce essentially low-power noisy patterns. This differs from standard FBG encoders, which transform the bit information in well-defined sequences of chips at different wavelengths.

The synthesis of the grating [27] (therefore, the breaking of the key) could be obtained in principle from the observation of the optical pattern as in any linear system. Due to the high optical bandwidth and low power of the signal coming from Section I of cipher, the observation of patterns can be challenging but feasible [6]. However, after the signal is masked by the quasi-orthogonal noise, the observation and grating synthesis becomes extremely difficult. It was demonstrated by simulation that the use of the quasi-orthogonal noise introduces the moderate power penalty for authorized users.

The proposed scheme can operate at bit rates of several gigabits per second in standard fibers. The encryption/decryption process is performed in the optical domain. It has a scalable structure that allows increments in security by simply employing more wavelengths and/or a larger bandwidth. Improvements in the versatility and security can be obtained by increasing the number of gratings, by increasing the used bandwidth, and by adding tunability to the PR-SSBGs.

References

[1] C. Elliott, "Quantum cryptography," *IEEE Security Privacy*, vol. 2, no. 4, pp. 57–61, Jul./Aug. 2004.

[2] V. Annovazzi-Lodi and A. Scire, "Synchronization of chaotic injected-laser systems and its application to optical cryptography," *IEEE J. Quantum Electron.*, vol. 32, no. 6, pp. 953–959, Jun. 1996.

[3] P. Torres, L. C. G Valente, and M. C. R Carvalho, "Security system for optical communication signals with fiber Bragg gratings," *IEEE Trans. Microw. Theory Tech.*, vol. 50, no. 1, pp. 13–16, Jan. 2002.

[4] 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.

[5] P. C. Teh, P. Petropoulos, M. Ibsen, and D. Richardson, "A comparative study of the performance of seven and 63 chip optical code-division multiple access encoders based on superstructured fiber Bragg gratings," *J. Lightw. Technol.*, vol. 19, no. 9, pp. 1352–1364, Sep. 2001.

[6] H. Sotobayashi, W. Chujo, and K.-I. 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] T. H. Shake, "Security performance of optical CDMA against eavesdropping," *J. Lightw. Technol.*, vol. 23, no. 2, pp. 655–670, Feb. 2005.

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

[9] R. Feced and M. N. Zervas, "Effects of random phase and amplitude error in optical fiber Bragg gratings," *J. Lightw. Technol.*, vol. 18, no. 1, pp. 90–101, Jan. 2000.

[10] G. Coppola, A. Irace, A. Cutolo, and M. Iodice, "Effect of fabrication errors in channel waveguide Bragg gratings," *Appl. Opt.*, vol. 38, no. 9, pp. 1752–1758, Mar. 1999.

[11] R. Kashyap, *Fiber Bragg Grating*. San Diego, CA: Academic, 1999.

[12] A. Fenner Milton and W. K. Burns, "Mode coupling in optical waveguide horns," *IEEE J. Quantum Electron.*, vol. QE-13, no. 10, pp. 828–835, Oct. 1977.

[13] B. Fisher and O. Shapira, "Localization of light in a random grating array in a single mode fiber," presented at the Conf. Lasers and Electro-Optics (CLEO), Baltimore, MD, 2001.

[14] M. V. Berry and S. Klein, "Transparent mirrors: Rays waves and localization," *Eur. J. Phys.*, vol. 18, no. 3, pp. 222–228, May 1997.

[15] H. Ghafouri-Shiraz and M. Tang, "Interaction between ultrashort optical pulse and fiber gratings with random profile noise," *Proc. Inst. Elect. Eng.—Optoelectron.*, vol. 151, no. 1, pp. 16–26, Feb. 2004.

[16] J. Azaña, "Study of optical pulses–fiber grating interaction by means of joint time-frequency signals representation," *J. Lightw. Technol.*, vol. 21, no. 11, pp. 2931–2941, Nov. 2003.

[17] J. G. Proakis, *Digital Communications*. New York: McGraw-Hill, 2001.

[18] M. P. Lotter and L. P. Linde, "A comparison of three families of spreading sequences for CDMA applications," in *Proc. IEEE South African Symp. Commun. Signal Process.*, 1994, pp. 68–75.

[19] G. P. Agrawal, *Fiber-Optic Communication Systems*, 3rd ed. New York: Wiley, 2002.

[20] A. S. Tanenbamum, *Computer Networks*. Upper Saddle River, NJ: Prentice-Hall, 2003.

[21] R. Hui, B. Zhu, K. Demarest, C. Allen, and J. Hong, "Generation of ultrahigh-speed tunable-rate optical pulses using strongly gain-coupled dual-wavelength DFB laser diodes," *IEEE Photon. Technol. Lett.*, vol. 11, no. 5, pp. 518–520, May 1999.

[22] R. Piyaket, S. Hunter, J. E. Ford, and S. Esener, "Programmable ultrashort optical pulse delay using an acousto-optic deflector," *Appl. Opt.*, vol. 34, no. 8, pp. 1445–1453, Mar. 1995.

[23] J. van Howe and C. Xu, "Ultrafast optical delay line by use of a time-prism pair," *Opt. Lett.*, vol. 30, no. 1, pp. 99–101, Jan. 2005.

[24] J. M. Castro, D. F. Geraghty, B. West, and S. Honkanen, "Fabrication and comprehensive modeling of ion-exchanged Bragg optical add/drop multiplexers," *Appl. Opt.*, vol. 43, no. 33, pp. 6166–6173, Nov. 2004.

[25] J. M. Castro, D. F Geragthy, S. Honkanen, C. Greiner, D. Iazikov, and T. W. Mossberg, "Demonstration of mode conversion using anti-symmetric waveguide Bragg gratings," *Opt. Express*, vol. 13, no. 11, pp. 4180–4184, Jun. 2005.

[26] ——, "Optical add–drop multiplexers based on the anti-symmetric waveguide Bragg grating," *Appl. Opt.*, vol. 45, no. 6, pp. 1236–1243, Feb. 2006.

[27] J. Skaar and R. Feced, "Reconstruction of gratings from noisy reflection data," *J. Opt. Soc. Amer. A, Opt. Image Sci.*, vol. 19, no. 11, pp. 2229–2237, Nov. 2002.

Jose M. Castro received the M.Sc. and Ph.D. degrees from the University of Arizona, Tucson, AZ, in 2003 and 2006, respectively, all in electrical engineering.

He was trained in wire and cable technologies at Pirelli, Sao Paolo, Brazil, and in quality management at the Kensai Kenshu Center, Japan. He is the author of more than 20 international journal articles and international conference papers. His research interests include fiber and integrated optics, dense wavelength division multiplexing, optical code-division multiple-access systems, and optical cryptography.

Ivan B. Djordjevic (M'04) received the B.Sc., M.Sc., and Ph.D. degrees from the University of Nis, Nis, Serbia, in 1994, 1997, and 1999, respectively, all in electrical engineering.

Prior to joining the University of Arizona, Tucson, in 2004, he was with the University of the West of England, Bristol, U.K.; the University of Bristol, Bristol, U.K.; Tyco Telecommunications, Eatontown, NJ; the National Technical University of Athens, Athens, Greece; the State Telecommunications Company (Telecom Serbia), Nis, Serbia; and the University of Nis, Nis, Serbia. He is currently an Assistant Research Professor of electrical and computer engineering at the University of Arizona. His research interests include dense wavelength division multiplexing fiber-optic communication systems and networks, error control coding, orthogonal frequency division multiplexing, code division multiple access, optical packet switching, free-space optics, communication theory, satellite communications, wireless communications, and coherent communications. He is author of more than 100 international publications.

David F. Geraghty (S'94–M'97) received the B.S. degree (with honors) in engineering and applied science, the M.S., and Ph.D. degrees both in applied physics from the California Institute of Technology, Pasadena, in 1991, 1994, and 1997, respectively. His thesis work investigated wavelength conversion by four-wave mixing in semiconductor optical amplifiers.

He is currently an Assistant Professor at the Department of Electrical and Computer Engineering, University of Arizona, Tucson. His research focuses on fiber and integrated optics, primarily for telecommunications applications.