Research Article | Vol. 29, No. 24 / 22 Nov 2021 / Optics Express 40462
Optics EXPRESS

Stealth and secured optical coherent transmission using a gain switched frequency comb and multi-homodyne coherent detection

EYAL WOHLGEMUTH,[1,*] YARON YOFFE,[1] PANTEA NADIMI GOKI,[2] MUHAMMAD IMRAN,[2] FRANCESCO FRESI,[3] PRAJWAL DODDABALLAPURA LAKSHMIJAYASIMHA,[4] ROI COHEN,[1] PRINCE ANANDARAJAH,[4] LUCA POTÌ,[3,5] AND DAN SADOT[1]

[1]*Department of Electrical and Computer Engineering, Ben-Gurion University of the Negev, Beer Sheva, Israel*
[2]*Scuola Superiore Sant'Anna, Via Moruzzi 1, 56124 Pisa, Italy*
[3]*Photonic Networks and Technologies National Laboratory - CNIT, Via Moruzzi 1, 54124 Pisa, Italy*
[4]*Photonics Systems and Sensing Lab., School of Electronic Engineering, Dublin City University, Glasnevin, Dublin 9, Ireland*
[5]*Universitas Mercatorum, Rome, Italy*
[*]*wohlgemu@post.bgu.ac.il*

Abstract: A novel all-optical stealth and secured transmission is proposed and demonstrated. Spectral replicas of the covert signal are carried by multiple tones of a gain switched optical frequency comb, optically coded with spectral phase mask, and concealed below EDFA's noise. The secured signal's spectrum is spread far beyond the bandwidth of a coherent receiver, thus forcing real time all-optical processing. An unauthorized user, who does not possess knowledge on the phase mask, can only obtain a noisy and distorted signal, that cannot be improved by post-processing. On the other hand, the authorized user decodes the signal using an inverse spectral phase mask and achieves a substantial optical processing gain via multi-homodyne coherent detection. A transmission of 20 Gbps under negative −7.5 dB OSNR is demonstrated here, yielding error-free detection by the eligible user.

© 2021 Optical Society of America under the terms of the OSA Open Access Publishing Agreement

1. Introduction

As the demand for bandwidth is scaling up to unprecedented levels, information confidentiality, integrity and availability are becoming increasingly important, particularly in sensitive applications such as financial transactions, military, medical records, and private information sharing. The optical infrastructure is prone to a major data breach, as it is exposed to various attacks such as fiber tapping, false data injection and jamming [1–3]. To cope with these considerable security threats, common encryption protocols are implemented in all seven layers of the open systems interconnection (OSI) model. Such protocols often rely on prime factorization and high computational complexity algorithms. However, in the era of supercomputing and quantum computing [4], any digital encryption scheme can be decrypted in theory, as the valuable raw data can be recorded and processed offline. Moreover, in upper layers standard encryption techniques, metadata remains unencrypted, as well as the existence of the transaction itself, and might be used by an adversary for eliciting sensitive information on the users by data mining techniques.

To overcome this challenge, security schemes by all-optical means, also known as optical layer security or photonic layer security, have been proposed and demonstrated [5]. Such a strategy augments the security performances of the entire communication network, as it offers many unique advantages over digital security protocols. In particular, it enables real-time, low-latency, low-power operation, which cannot be provided by conventional security algorithms

#431070 https://doi.org/10.1364/OE.431070
Journal © 2021 Received 10 May 2021; revised 26 Jul 2021; accepted 12 Aug 2021; published 19 Nov 2021

Optics EXPRESS

at today's line rates, exceeding 1.3 Tbps per single wavelength [6]. Additionally, side-channel attacks can be prevented since all-optical processing does not generate electromagnetic radio frequency signatures. Several approaches for optical layer security have been widely investigated, including quantum communication, chaos-based communication, all-optical XOR gates, and spread spectrum (SS) techniques in particular, optical code division multiple access (OCDMA) [7–11].

Quantum key distribution (QKD) [12,13] is considered unconditionally secured, i.e. completely resilient against cryptanalytic attacks. However, its performances still remains incomparable with the other security approaches, as bitrate-distance ($B \cdot L$) product is limited to several Mbits / second × km [13]. Consequently, QKD is mainly considered for key exchange protocols, rather than for encrypting the data in a full line-rate. In chaos-based communications, the user message is transmitted using a chaotic signal carrier, which is very sensitive to initial hardware conditions, and is generated by a laser diode that contains optoelectronic feedback or optical feedback [14]. Using different chaos synchronization scheme and using optical coherent masking and detection, the speed to tens of Gbit/s can be achieved [15]. In addition, OEO-based chaos system recorded 30 Gbps transmission over 100 km distance [16]. All-optical processing techniques such as optical XOR gates have also been suggested for replacing electronic logic circuits with photonic alternatives, utilizing nonlinearity phenomena such as four-wave mixing (FWM) in a saturated semiconductor optical amplifier (SOA) [17].

OCDMA has been mainly proposed for passive optical networks (OCDMA-PONs) [18] applications. In turn, OCDMA has been suggested for security purposes as well [7–11] since eliminating the multi-user interference (MUI) provides a certain level of authentication. The generation of the optical code (OC) is provided by spectral phase encoding, also known as spectral phase encoded time spreading (SPECTS-OCDMA), or by a multiplication with direct sequences (DS-OCDMA) in the time domain. In spectral phase encoding, the OC can be inscribed by either a fiber Bragg grating (FBG) or obtained by a dynamic spatial light modulator (SLM) [19]. FBG implementation, however, is passive and cannot meet security needs, where dynamic key changing is required. Therefore, for security applications, a dynamic, short settling time optical engine should be provided such as SLM based-devices or phase shifters array in between DWDM demultiplexer and multiplexer.

The gap between the data security requirements and the available security techniques calls for a new security approach that is immune to traffic analysis and provides a stealth transmission. The envisaged system enables scalable and high key change rates, compatibility with today's flex grid DWDM networks, low-cost implementation, based on off-the-shelf components, and can be accommodated in highly integrated technologies such as silicon photonics. Here, we propose and demonstrate a novel all-optical SS technique in which digital post-processing and traffic analysis cannot be applied by the eavesdropper, and enhanced immunity to man-in-the-middle attacks as well as jamming is provided. On top of that, our proposed system can provide a stealth transmission (steganography) [20,21], whilst the data resembles a noise-like waveform, and it can be concealed below the noise level in both time and frequency domains.

Under proper design considerations, the proposed system requires an all-optical real-time decoding that can be performed by the eligible user exclusively, using the correct OC. Otherwise, a distorted low level of SNR is determined during the optical detection process, with no possible improvement. Thus, such system forces the eavesdropper to decode the encrypted data "on the fly", or alternatively to record a complex optical signal of multi-THz bandwidth under extremely low received power conditions, which is considered of high complexity, and potentially unrealistic. Unlike OCMDA, the proposed system is protected from an unauthorized baseband recording. This solves the major drawback of both coherent and incoherent OCDMA from being an encryption system.

Optics EXPRESS

The proposed method is based on the concept of multi-homodyne coherent detection, enabled by optical frequency combs, that serve as both the signal's carrier and LO. The low phase-noise and the high correlation degree between the comb's tones allow a detection mechanism that incorporates the entire emission spectrum of the optical frequency comb. This scheme enables the authorized user to achieve an optical processing gain, therefore a legitimate detection is possible under extremely low OSNR conditions. In addition, the reported technique is agnostic to modulation type or rate, thus allows coherent high order modulation (HOM) schemes, operation at high symbol rates, as well as polarization diversity transmission.

In this work, the concept of multi-homodyne coherent detection is analytically explained, and its security performance is analyzed for both the authorized and unauthorized users, and verified by numerical simulations. Furthermore, an experimental validation is performed by demonstrating authorized error-free recovery of a 10 Gbuad QPSK stealth signal with negative optical signal-to-noise ratio (OSNR) of −7.5 dB and extremely weak received signal power as low as −49 dBm. In addition, we measured the reception performance of the unauthorized user showing that the intercepted signal is bounded to a very low SNR, regardless of the post digital processing that is being applied. In other words, for the eavesdropper, some of the data is permanently lost.

2. Stealth and secured optical coherent transmission system

The proposed system (depicted in Fig. 1) is based on an optical frequency comb as a multi-carrier source, which is used to generate the E-field $E_{\mathrm{s}}(t)$, a sum of the various spectral replicas of the modulated complex baseband signal, $b(t)$. Such scheme allows the signal's energy to be spread over an ultra-wide, potentially multi-THz bandwidth. Subsequently, the signal is optically encoded with a spectral phase mask, denoted by $\Psi(f)$, which can be regarded as the secret private key. The broadband encoded signal is then concealed below the noise level of a pre-amp EDFA, represented by the analytic E-field $E_{\mathrm{tx}}(t)$.

In order to properly detect the signal, two-fold operation must be applied all-optically. First, the spectral phase mask should be eliminated by implementing the inverse mask , $\Psi^{-1}(f)$. Second, the received decoded E-field, $E_{\mathrm{rx}}(t)$, is mixed with a synchronized optical frequency comb LO, evoking multi-homodyne coherent detection. It is assumed that the receiver possess the knowledge of the encryption key. This can be provided with out-of-band authenticated key-exchange protocols, that are widely available.

Subjected to an appropriate synchronization between the transmitter's and the receiver's combs, the coherent optical-to-electrical photodetection folds all the transmitted passband replicas into the baseband. Due to the high phase correlation, the interference terms are added constructively, in a coherent addition manner. This coherent addition effectively forms an optical processing gain which is proportional to the number of overlapping tones of the two combs.

On the other hand, broadband optical noise, $N(f)$, which attains random phase across the optical spectrum, e.g., amplified spontaneous emission (ASE), is folded in an incoherent addition manner following the optical mixing with the LO comb. Under optimal conditions, the signal energy is reinforced in a quadratic ratio versus the number of tones, while the noise energy is reinforced linearly. Hence, this multi-homodyne detection scheme generates an optical processing gain, equals to the number of signal's spectral replicas (the number of comb's tones) that are participating in the multi-homodyne coherent detection. The rest of this section is organized as follows. Subsection 2.1 analytically presents the signal's generation. The modeling of the spectral phase mask for spectral phase encoding and the optical noise loading are provided in Subsections 2.2 and 2.3, respectively. Follows, in section 3., the system's performance for the authorized user as well as the statistical detection performance of the unauthorized user are derived.

Optics EXPRESS

2.1. Optical frequency comb as multi-signal carrier

Let us assume that a continuous time baseband symbols stream of N symbols length, $b(t) = \sum_{n=1}^{N-1} d_n\, p(t - nT_s)$, is modulating the output of an optical frequency comb laser source, where T_s is the symbol duration time, $p(t)$ is the pulse shaping function, and $\{d_n\}_{n=1}^{N}$ is an i.i.d. complex symbol sequence. Consequently, the entire comb spectrum is modulated at once, replicating the baseband PSD L times, corresponding to the number of the comb's tones. The modulated field of the replicated baseband signal is therefore given in the time domain as follows:

$$E_s(t) = \begin{cases} \sqrt{P_s} \sum_{l=\frac{1-L}{2}}^{\frac{L-1}{2}} e^{j2\pi\left(f_c + l\delta_f\right)t} \sum_{n=1}^{N} d_n\, p\left(t - n\frac{1}{\delta_f}\right) & \text{if } L \text{ odd,} \\ \sqrt{P_s} \sum_{l=-\frac{L}{2}+1}^{\frac{L}{2}} e^{j2\pi\left(f_c + \left(l-\frac{1}{2}\right)\delta_f\right)t} \sum_{n=1}^{N} d_n\, p\left(t - n\frac{1}{\delta_f}\right) & \text{if } L \text{ even.} \end{cases} \tag{1}$$

f_c and δ_f denote the center frequency and free-spectral range (FSR) of the optical frequency comb, respectively. In addition, it is assumed that the comb has a flat spectrum, thus the amplitude of each tone, $\sqrt{P_s}$, is constant for its L tones. This can be achieved by optical equalization of the comb's tones. Without loss of generality, and to ease the notations, it is assumed henceforth that the comb generates an odd number of tones. In order to prevent overlapping between two adjacent replicas, synchronization between the comb's FSR and the Baud is required such that $(T_s = 1/\delta_f)$. In addition, the digital baseband signal is ensured to be band-limited by applying a square-root-raised-cosine filter (SRRC) digital pulse shaping. Following the generation of the replicated modulated signal, the two security steps are carried out: spectral phase encoding and optical noise loading for steganography.

2.2. Spectral phase encoding

The spectral phase mask is used to encode the replicated signal by assigning each of its spectral replicas a one or more random phase terms, equivalent to a random time delay. The resulting time-domain signal, previously a train of ultra-short pulses, is smeared according to the pattern of the mask, to gain stealthiness in the time domain. In the model we have presented here, the spectral phase mask is comprised of $\mathcal{B}$ spectral bins, each of Δf bandwidth, and the entire mask is centered around the emission center frequency of the optical frequency comb (f_c). The number of bins satisfies $\mathcal{B} = \lceil * \frac{\mathrm{BW}}{\Delta_f} \rceil$, where the total bandwidth of the mask, $\mathrm{BW} = L \cdot \delta_f$, is designed to cover the L spectral replicas and the "tails" of the two marginal replicas as well. A ceiling function, $\lceil * \cdot \rceil$, is used above, to return the smallest integer that is greater than or equal to its argument. The key is a set of pseudorandom variables $\left\{\phi_\beta\right\}_{\beta=1}^{\mathcal{B}}$, where ϕ_β is the spectral phase term associated with the β-th spectral bin of the mask, uniformly distributed within the range $[0, 2\pi]$, i.e. $\phi_\beta \sim U(0, 2\pi)$. Considering that, the inclusive transfer function of the SLM device, for a complex amplitude, is described as follows:

$$\Psi(f) = \begin{cases} \sum_{\beta=\frac{1-\mathcal{B}}{2}}^{\frac{\mathcal{B}-1}{2}} e^{j\phi_\beta}\, \Pi\left(\frac{f - f_c + \beta\Delta_f}{\Delta_f}\right) * \left(\frac{1}{\sqrt{2\pi}\sigma_f}\, e^{-\frac{1}{2}\left(f/\sigma_f\right)^2}\right) & \text{if } \mathcal{B} \text{ odd,} \\ \sum_{\beta=-\frac{\mathcal{B}}{2}}^{\frac{\mathcal{B}}{2}-1} e^{j\phi_\beta}\, \Pi\left(\frac{f - f_c + \left(\beta+\frac{1}{2}\right)\Delta_f}{\Delta_f}\right) * \left(\frac{1}{\sqrt{2\pi}\sigma_f}\, e^{-\frac{1}{2}\left(f/\sigma_f\right)^2}\right) & \text{if } \mathcal{B} \text{ even.} \end{cases} \tag{2}$$

In the expression above, the spectral phase mask is modeled as a rectangular pattern convoluted with the optical transfer function (OTF) of the SLM device [22]. We used $*$ symbol to denotes the convolution operator. The rectangular pattern stems from the SLM's pixels array structure, expressed by a sum of shifted rectangular functions $\Pi(\cdot)$. For the OTF, a spectral Gaussian is considered, with standard deviation σ_f, a scalar quantity constant over the operation frequency range of the device. σ_f is related to the full width at half maximum (FWHM) bandwidth of the

Optics EXPRESS

OTF by $\sigma_f = \mathrm{BW_{OTF}}/2\sqrt{2\ln 2}$. As a result of applying the spectral phase mask, the secured transmitted field takes the analytic form $E_{\mathrm{tx}}(t)$, with a Fourier transform:

$$S_{\mathrm{tx}}(f) = \Psi(f)\sqrt{P_s}\sum_{l=\frac{1-L}{2}}^{\frac{L-1}{2}} B\left(f - f_c - l\delta_f\right) + N(f), \tag{3}$$

where $B(f)$ is the Fourier transform of the baseband symbol stream $b(t)$, and $N(f)$ represents an optical wideband noise, as specified later in subsection 2.3.

Addressing the security strength of the proposed system, two factors should be considered: first, the resolution of the spectral phase mask, and second, the number of spectral replicas. While the former sets a computational complexity for the unauthorized user, the latter bounds the unauthorized user's detection to a certain level of electrical SNR which cannot be further improved after photoelectric conversion. In case that several phases are applied on each replica, the unauthorized detected baseband signal will suffer from a random ISI. Therefore, the unauthorized user is forced to mitigate the ISI with a linear equalizer. Furthermore, the SNR will still be limited to a degraded value which was determined while the photoelectric conversion had been performed. The resolution of the mask, and the amount of possible permutations define the computational resources required for this task. The ISI, measured in unit intervals (UIs), corresponds the ratio between the signal's Baud and the spectral phase mask's resolution as follows:

$$\mathrm{ISI} = (T_s\Delta f)^{-1}. \tag{4}$$

In the simulations presented in this paper, two cases were considered: a single mask's bin per replica, and several bins per replica, while in the experiment described in Section 4. only the single bin case was tested due to the hardware limitations. The two masks used for these simulations are depicted in Fig. 2. In practice, modern SLMs, based on a liquid crystal on silicon (LCoS), have optical transfer function $\mathrm{BW_{OTF}} \approx 10.7$ GHz, with a deviation of ±0.2 GHz over the C-band [22]. Such SLMs enable a temporal spreading of one symbol period or one unit interval (UI), for 10 GBaud signal, as shown in Figs. 2(a) and 2(c). For higher resolution SLMs, a spectral resolution of 6.25 GHz is considered [23], which may increase the ISI to 4 UIs for 25 GBaud signal, as shown in Figs. 2(b) and 2(d). Some proposed photonic processors introduces spectral resolution below 100 MHz [24], enabling ultra-high security level by stretching each 10 GBaud symbol over 100 UIs, forcing the unauthorized user enormous amount of computational resources for the digital bits recovery.

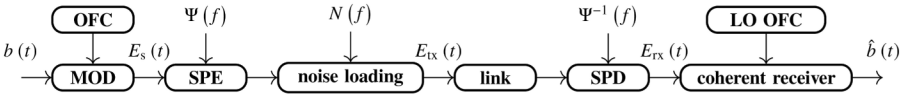


Fig. 1. The proposed security system block diagram with the notations of: baseband signal $b(t)$, replicated baseband signal's E-field $E_{\mathrm{s}}(t)$, transmitted secured field $E_{\mathrm{tx}}(t)$, received decoded field $E_{\mathrm{rx}}(t)$, and the recovered baseband signal $\hat{b}(t)$. The following abbreviation were used: OFC - optical frequency comb, MOD - modulator, SPE - spectral phase encoding, SPD - spectral phase decoding, LO - local oscillator.

2.3. Noise loading

The deliberate noise loading is designed to ensure an insufficient SNR for the unauthorized user, on one hand. On the other hand, the authorized user can reacquire a detectable SNR via multi-homodyne coherent detection, but only after decoding the spectral phase mask. Furthermore, it is possible to set a negative OSNR to achieve steganography, i.e. stealth transmission. The

Optics EXPRESS

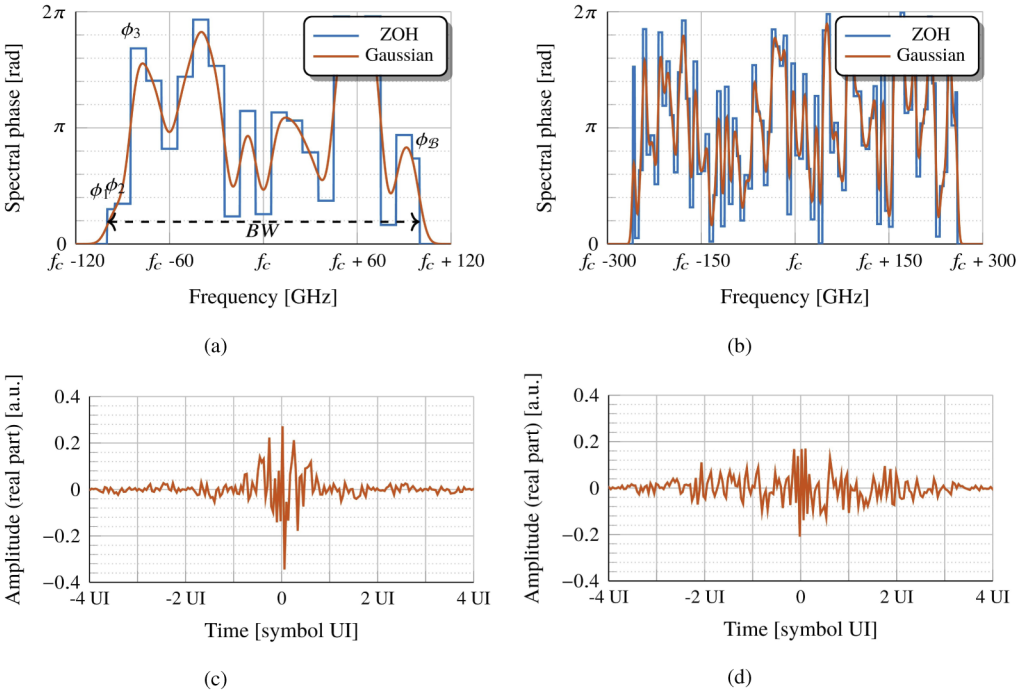


Fig. 2. An example of two spectral phase masks with BW = 210 GHz and BW = 525 GHz, corresponding to twenty 10 GHz replicas, and twenty 25 GHz replicas, respectively, filtered with SRRC, $\beta = 0.2$. The transfer function is plotted on top, and its associated impulse response below. The transfer function is given as a theoretical zero-order hold (ZOH) in blue and as practical Gaussian-shaped in red. For both masks it is considered that the OTF FWHM is equal to the bin width ($\mathrm{BW_{OTF}} = \Delta_f$). In (a) and (c), the Baud is equal to the bin width ($\mathrm{BW_{OTF}} = \Delta_f = \delta_f = 10$ GHz), so that each symbols extends over 1 unit interval (UI), corresponding to a 'conventional' LCoS SLM device. In (b) and (d), a high resolution mask with 4 bins per replica ($\mathrm{BW_{OTF}} = \Delta_f = \frac{1}{4}\delta_f = 6.25$ GHz), where the symbols extends over 4 UIs.

initial OSNR level is set at the transmitter, by loading the encoded signal with ASE noise. This is readily done by amplifying the encoded signal with EDFA before transmitting it to the line. The ASE power spectral density (PSD) can be expressed as follows:

$$S_{\mathrm{sp}}(f) = n_{\mathrm{sp}}(f)\, h\nu\, [G(f) - 1], \tag{5}$$

where $G(f)$ is the gain of the medium, and h is Plank's constant. $n_{\mathrm{sp}}(f) > 1$ is a dimensionless spontaneous emission factor of the gain medium. In general, $G(f)$ and $n_{\mathrm{sp}}(f)$ weakly dependent on the frequency over 200 GHz bandwidth, thus the ASE PSD can be labeled as $N_0/2$ and measured in units of W/Hz.

Regarding the OSNR calculation, the convention where the ASE PSD is integrated over 12.5 GHz (or 0.1 nm) band, while the bandwidth of the signal is not considered, does not make sense for steganography applications. Especially because of spreading the signal's energy over extremely wide bandwidth determines the stealthiness level. Here we defined OSNR as the power ratio of the signal PSD over the noise PSD, per the same bandwidth, namely

$$\mathrm{OSNR} = \frac{\int_{f_c-\mathrm{BW}/2}^{f_c+\mathrm{BW}/2} S_{\mathrm{tx}}(f)\, df}{\int_{f_c-\mathrm{BW}/2}^{f_c+\mathrm{BW}/2} S_{\mathrm{sp}}(f)\, df}. \tag{6}$$

Optics EXPRESS

In addition, we define the spectral prominence of signal over the noise level as a merit for the stealthiness level. For instance, 0 dB OSNR (equal PSDs of noise and signal) yields 3 dB spectral prominence, and −16 dB OSNR yields 0.1 dB spectral prominence.

$$P\,[\mathrm{dB}] = 10\log_{10}\left(1 + 10^{-\mathrm{OSNR}\,[\mathrm{dB}]/10}\right). \tag{7}$$

Prominence of less than 0.1 dB can be considered a stealth transmission. Although some optical spectrum analyzers can achieve higher amplitude resolution than 0.1 dB, in such prominence the secured signal can hardly be distinguished among existing spectral features in the fiber, such as side modes of public channels.

3. System performance

In the analysis performed here, two cases are considered: In Subsection 3.1, the authorized user which is assumed to perfectly decode the mask and performs multi-homodyne coherent addition [25,26]. In Subsection 3.2, the unauthorized user, who employs the appropriate optical hardware, however does not possess knowledge of the encoding phase mask, carries a brute force attack over the encoded signal. For both cases, the detection figure of merits, such SNR and BER are computed and corresponding numerical simulations are presented as well.

3.1. Authorized user detection performance

For the detection performance, the model of amplified homodyne coherent detection is used. The generated currents represent real and imaginary parts of the beating amplified signal and LO fileds. The output current, $i_{\mathrm{x}}^{\mathrm{in}}(t)$ of the X state of polarization (SOP) of the in-phase component, at the output of polarization diversity coherent balanced receiver, is given as [27]:

$$i_{\mathrm{x}}^{\mathrm{in}}(t) = \underbrace{2R\,\mathrm{Re}\left\{E_{\mathrm{S}}(t)\,E_{\mathrm{LO}}^{*}(t)\right\}}_{\text{signal-LO beating}} + \underbrace{2R\,\mathrm{Re}\left\{E_{\mathrm{ASE}}(t)\,E_{\mathrm{LO}}^{*}(t)\right\}}_{\text{LO-ASE beating noise}} + \underbrace{i_{\mathrm{sh}}^{\mathrm{in}}(t)}_{\text{shot noise}} + \underbrace{i_{\mathrm{TIA}}^{\mathrm{in}}(t)}_{\text{thermal noise}}, \tag{8}$$

where R is the photodiode responsivity, assuming equal responsivities for the signal and the LO branches, $i_{\mathrm{sh}}^{\mathrm{in}}(t)$ is the shot noise with a two-sided psd of $S_{i_{\mathrm{sh}}}(f) = qRP_{LO}\ [\mathrm{A}^2/\mathrm{Hz}]$, and $i_{\mathrm{TIA}}^{\mathrm{in}}(t)$ is the input-referred noise current density. Similarly, the quadrature current of the X SOP, $i_{\mathrm{x}}^{\mathrm{quad}}(t)$, can be extracted, to generate the complex recovered baseband signal $\hat{b}(t) = i_{\mathrm{x}}^{\mathrm{in}}(t) + j\cdot i_{\mathrm{x}}^{\mathrm{quad}}(t)$.

For ASE limited systems, such as steganography applications, the SNR is dominated by contribution of the ASE noise, rather than shot or thermal noises, therefore the two last terms of Eq. (8) are negligible. The ASE field can be described by the following autocorrelation function and the (two-sided) power spectral density:

$$\mathrm{E}\left[E_{\mathrm{ASE}}(t)\,E_{\mathrm{ASE}}^{*}(t-\tau)\right] = \delta(\tau)\,n_{\mathrm{sp}}(G-1)\,h\nu \text{ and } S_{E_{\mathrm{ASE}}} = n_{\mathrm{sp}}(G-1)\,h\nu, \tag{9}$$

respectively.

The suggested model assumes an ideal detection where the signal is matched-filtered and sampled at maximum correlation points. The variance of the complex recovered baseband signal $\hat{b}(t)$ can be computed using Eq. (1), at the ideal sampling points, mT, as follows:

$$\begin{aligned}\mathcal{E}_{\hat{b}} &= \mathrm{var}\left\{p(-mT) * 2RE_{\mathrm{S}}(mT)\,E_{\mathrm{LO}}^{*}(mT)\right\}\\ &= 4R^2P_{LO}P_S\,\mathrm{E}\left[\left|p(-mT) * \sum_{l=\frac{1-L}{2}}^{\frac{L-1}{2}} e^{j2\pi\left(f_c+l\delta_f\right)mT}\sum_{n=1}^{N} d_n p\left((n-m)\,T\right)\sum_{l'=\frac{1-L}{2}}^{\frac{L-1}{2}} e^{-j2\pi\left(f_c+l'\delta_f\right)mT}\right|^2\right].\end{aligned} \tag{10}$$

Optics EXPRESS

Rearranging Eq. (10) yields:

$$\mathcal{E}_{\hat{b}} = 4R^2 P_{LO} P_S \, \mathrm{E}\Big[\Big| \sum_{l=\frac{1-L}{2}}^{\frac{L-1}{2}} \sum_{l'=\frac{1-L}{2}}^{\frac{L-1}{2}} e^{j2\pi\left((l-l')\delta_f\right)mT} \sum_{n=1}^{N} d_n p(-mT) * p\left((n-m)\,T\right)\Big|^2\Big]. \tag{11}$$

Considering the pulse shaping orthogonality, as well as the normalization of the symbols' energy $\mathrm{E}\left[\left|\sum_{n=1}^{N} d_n\right|^2\right] = 1$, Eq. (11) can be further simplified to:

$$\mathcal{E}_{\hat{b}} = 4L^2 R^2 P_{LO} P_S. \tag{12}$$

Addressing the noise term, the detected noise current variance, at sampling points $t = mT$, is given by:

$$\begin{aligned} \mathcal{E}_n &= \mathrm{var}\left\{E_{\mathrm{ASE}}(t)\, E^*_{\mathrm{LO}}(t)\right\} \quad = \\ &= 4R^2\, \mathrm{E}\Big[\sum_{l'=\frac{1-L}{2}}^{\frac{L-1}{2}} \sum_{l'=\frac{1-L}{2}}^{\frac{L-1}{2}} \int_{-\infty}^{\infty} P^*(f')\, S_{ASE}\left(f' - \left(f_c + l'\delta_f\right)\right) e^{j2\pi f' t} df' \\ &\quad \cdot \int_{-\infty}^{\infty} P(f'')\, S^*_{ASE}\left(f'' - \left(f_c + l''\delta_f\right)\right) e^{-j2\pi f'' t} df'' \Big]. \end{aligned} \tag{13}$$

Using the ASE field autocorrelation given in Eq. (9), last expression can be rewritten as follows:

$$\mathcal{E}_n = 4R^2 \frac{N_0}{2} \sum_{l'=\frac{1-L}{2}}^{\frac{L-1}{2}} \sum_{l''=\frac{1-L}{2}}^{\frac{L-1}{2}} \int_{-\infty}^{\infty} P^*\left(f'' - (l''-l')\,\delta_f\right) P(f'') e^{-2j\pi(l''-l')\delta_f t} df''. \tag{14}$$

Considering the orthogonality of the pulse shaping: $\int_{-\infty}^{\infty} P^*(f - l\delta_f)P(f)df = 0 \;\forall\, l \neq 0$, the noise variance is:

$$\mathcal{E}_n = 4LR^2 \frac{N_0}{2} \int_{-\infty}^{\infty} |P(f)|^2 df. \tag{15}$$

Finally, the SNR for the authorized user is computed as the ratio $\frac{\mathcal{E}_{\hat{b}}}{\mathcal{E}_n}$ of Eqs. 12) and 15):

$$\mathrm{SNR}_{authorized} \quad = \quad L \frac{P_{LO} P_S}{\frac{N_0}{2} \int_{-\infty}^{\infty} |P(f)|^2 df}. \tag{16}$$

For reference, a conventional scenario where a continuous wave (CW) laser source with energy P_S is used as the signal carrier. For this case, the detected SNR is:

$$\mathrm{SNR}_{CW} = \frac{P_{LO} P_S}{\frac{N_0}{2} \int_{-\infty}^{\infty} |P(f)|^2 df}. \tag{17}$$

A factor of L is introduced at the SNR expression of the authorized user, compared to a single carrier transmission. The reinforcement of the SNR by the optical processing gain, is due to the coherent addition of L signal's replicas.

$$\mathrm{OPG}_{authorized} = \frac{\mathrm{SNR}_{authorized}}{\mathrm{SNR}_{CW}} = L. \tag{18}$$

Simulation results for the authorized user EVM and BER are given in Figs. 3(a) and 3(b), respectively, for the case of 10 GBaud QPSK with 10 GHz phase mask resolution. Various number of spectral replicas are considered (5, 20 and 80), and different levels of OSNR.

Optics EXPRESS

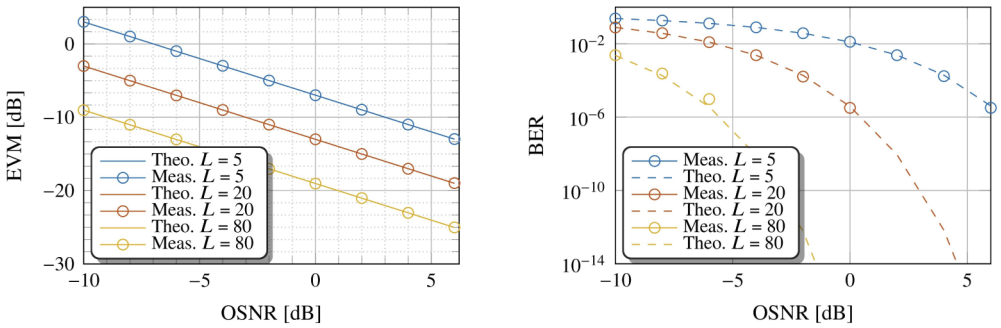


Fig. 3. (a) EVM vs. OSNR. and (b) BER vs. OSNR. In both plots, continuous line represents the theoretical computation based of the proposed model (Eq. (16)). Numerical simulation results are shown in round markers.

3.2. *Unauthorized user detection performances*

The detection performance of the unauthorized user may be divided into two cases, derived from the optical hardware that applies the spectral phase mask. In the first case, one spectral phase term per signal's replica is assumed. Therefore, the FSR of the comb equals to the mask's resolution ($\delta_f = \Delta_f$), and the number of spectral replicas equals to the number of the mask's bins ($L = \mathcal{B}$), such scenario is depicted in Fig. 2(a). When the decoding mask does not match the encoding one, incoherent summation of the spectral replicas limits the SNR of the detected baseband signal. As a result, a SNR gap between the authorized user and the unauthorized user is achieved. This SNR gap, also referred in this paper as optical processing gain, grows linearly with the number of the signal's spectral replicas. In turn, the optical processing gain can determines the secrecy capacity [28,29], a measure for the security level of the system.

The second case, which is depicted in Fig. 2(b), several spectral phase terms are applied for each replica. This effectively forms additional dispersive spectral distortion, which leads to a random intersymbol interference (ISI), as shown in Eq. (4). This is particularly challenging for coherent receivers, as fundamental tasks, such as synchronization, channel estimation and equalization are inherently limited due to the severe SNR conditions. Yet, despite the added complexity, an "unlimited resources" receiver may attain the SNR limit of the first case by recording the signal and offline processing.

We analyze here the statistical performances of the authorized user versus the unauthorized user, in terms of optical processing gain, which were derived in Eq. (18). For the sake of simplicity, the derivation below addresses the first case of single phase term per replica. Let us recall that an unauthorized user decodes the signal using an unmatched spectral phase mask, followed by multi-homodyne coherent detection. Consequently, the detected baseband signal can be written as:

$$\begin{aligned}\hat{B}_{unauthorized}(f) =& P^*(f) R E_s E_{\mathrm{LO}} \left(\sum_{l=\frac{1-L}{2}}^{\frac{L-1}{2}} e^{j\theta_l} B\left(f - f_c - l\delta_f\right) + N'(f) \right) \\ & * \sum_{l=-\frac{L}{2}+1}^{\frac{L}{2}} \delta\left(f - f_c - l\delta_f\right),\end{aligned} \tag{19}$$

where θ_l in a random variable $\theta_l \sim U(0, 2\pi)$, represents the phase differences between the encoding spectral phase mask and decoding one, for the l-th replica. Reproducing the same

Optics EXPRESS

derivation of the authorized user SNR, the resulting SNR of the unauthorized user is given by:

$$\mathrm{SNR}_{unauthorized} = \frac{|\sum_{l=\frac{1-L}{2}}^{\frac{L-1}{2}} e^{j\theta_l}|^2}{L} \frac{\mathcal{E}_{\hat{b}}}{\mathcal{E}_n}, \tag{20}$$

with the corresponding optical processing gain of:

$$\mathrm{OPG}_{unauthorized} = \frac{\mathrm{SNR}_{unauthorized}}{\mathrm{SNR}_{CW}} = \frac{|\sum_{l=\frac{1-L}{2}}^{\frac{L-1}{2}} e^{j\theta_l}|^2}{L}. \tag{21}$$

The summation of Eq. (21) is a complex random variable with random amplitude (A) and random phase (ϕ), i,e., $\mathcal{E}$ is trivially written as:

$$\mathcal{E} = \sum_{l=\frac{1-L}{2}}^{\frac{L-1}{2}} e^{J\theta_l} = Ae^{j\phi}. \tag{22}$$

It is shown [30] that the amplitude A satisfies Rayleigh distribution, (Rayleigh $\left(\sqrt{L/2}\right)$). In addition, its amplitude's absolute value square ($|A|^2$) is an Exponential R.V. satisfying $|A|^2 \sim$ Exponential$(1/L)$ [31]. To ease the notation, let us denote $\mathrm{OPG}_{unauthorized} = O = \frac{\mathcal{E}}{L}$. Considering that scaling an Exponential R.V. by a factor of $1/L$ scales the distribution parameter by the reciprocal factor. Therefore, $O \sim$ Exponential(1) with probability density function (PDF) and cumulative distribution function (CDF):

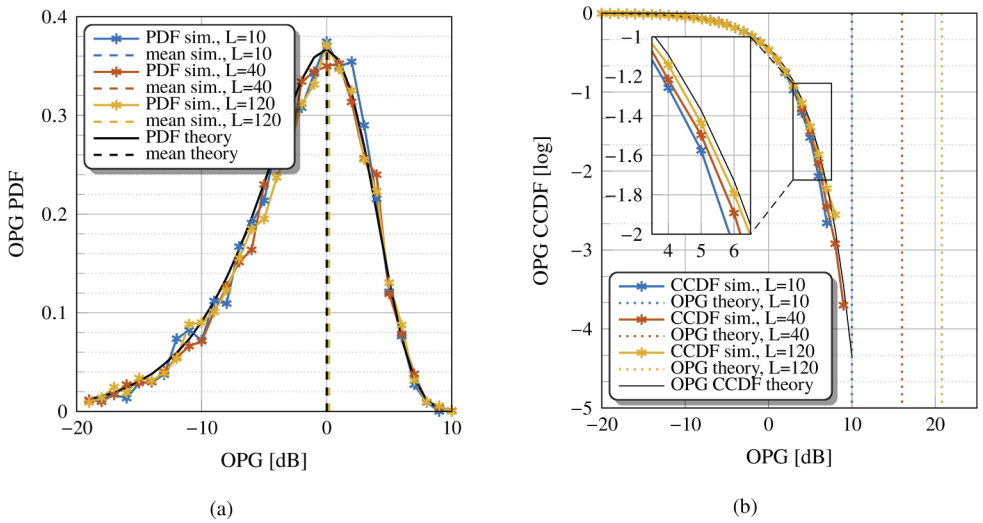
$$f_O(o) = e^{-o}, \quad F_O(o) = 1 - e^{-o}, \tag{23}$$

and the following statistics: $\mathrm{E}[O] = 1$, $\mathrm{var}[O] = 1$. It is therefore shown that for the unauthorized user no processing gain is obtained in average. Moreover, its distribution (PDF and CDF) are independent of the number of spectral replicas L.

Simulation results showing the statistical behaviour of the unauthorized user's optical processing gain obtained by brute force mask trials are presented in Figs. 4(a) and 4(b). The PDF $f_O(o)$ is plotted in Fig. 4(a) in solid lines for 10, 40 and 120 spectral replicas, each curve is generated from 5000 mask trials. The simulation parameters are identical to authorized user's simulation as described in Subsection 3.1, however the encoding mask is assumed to be unknown and the decoding masks are randomly trialed. The theoretical curve plotted in black line, fits the simulated optical processing gain, thus verifies its exponential distribution. In addition, the mean values, plotted in vertical dashed lines, indicates 0 dB optical processing gain. The 0 dB mean optical processing gain implies that the incoherent addition of the signal's spectral replicas increases the baseband signal's energy linearly, in same manner as the ASE noise variance is increased, therefore no optical processing gain is obtained in average. On the opposite, Eq. (18) shows that the authorized user's gains optical processing gain of factor L, as a results of quadratic increase of the signal's baseband energy.

Figure 4(b) plots the complementary CDF (CCDF) in a logarithmic scale, generated from the same data of Fig. 4(a). The vertical dashed lines in this figure represent the optical processing gain of the authorized user according to Eq. (18). Since the optical processing gain distribution is approximately independent of the number of replicas L, the probability of achieving the maximal optical processing gain decreases for all L cases. Unlike the theoretical cure which crosses $o = L$ at finite value, the measured CCDF is expected to asymptotically drops when $o \to L$, since the probability to trial exactly the encoding mask is zero. This contradiction implies that approximating sum of finite phases by Rayleigh distribution is somewhat inaccurate for small

Optics EXPRESS



(a) (b)

Fig. 4. (a) Solid lines denote the probability density function (PDF) of the unauthorized user's optical processing gain (OPG), obtained as a result of brute force phase mask trials, while dashed vertical lines represent the mean values of the OPG. Colored plots are simulation (sim.) results, while black plots (solid and dashed) are theoretical computation, according to Eq. (23). (b) Complementary cumulative distribution function (CCDF) of the OPD, is plotted in logarithmic scale for different number of L. Here also colored plots are simulation results, and black plot is theoretical computation, according to Eq. (23). The dotted lines denote the OPG value of the authorized user, which introduces the asymptotic limit for the unauthorized user OPG. One can observe slight dependency of L, as emphasized by the inset. This dependency is further discussed in the text.

number of L. The inset in Fig. 4(b) highlight the dependency of the CCDF in L. For larger L, the simulation approaches the theoretical model. The reason lies where the assumption of central limit theorem cannot hold for finite number of L. A recursive method to obtain the analytical PDF for finite number of L is provided in [32].

The brute-force analysis assumes the worst-case scenario from a security perspective, i.e. the unauthorized user knows the spectral allocation of the secured stealthy signal and employs the appropriate receiver. If the unauthorized user detects only $l<L$ replicas, the maximal optical processing gain will further decrease by a factor of $\mathrm{OPG}' = (\frac{l}{L}) \cdot \mathrm{OPG}$. Similarly, if the unauthorized user detects $l>L$ replicas, the maximum optical processing gain will decrease in a reciprocal factor of $\mathrm{OPG}' = (\frac{L}{l}) \cdot \mathrm{OPG}$. For $l>L$ case, l valuable replicas are assumed to be folded, however only L of them contain signal's information and the other $l - L$ replicas contain only ASE noise, without information.

4. Experimental method

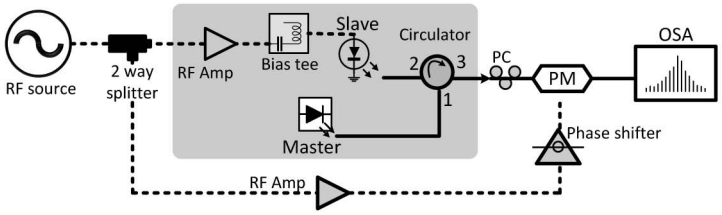
4.1. Frequency comb

The broadband spectrum required for multi-homodyne coherent detection is provided by optical frequency combs which are in general considered highly attractive for next generation optical communications [33,34]. First, they can serve as multi-carrier sources in WDM systems for both the signal's carrier and the local oscillator, replacing tens of tunable continuous-wave lasers by a single source. Secondly, the use of optical frequency comb enables to significantly simplify the coherent receiver by realizing a joint digital signal processing for phase recovery.

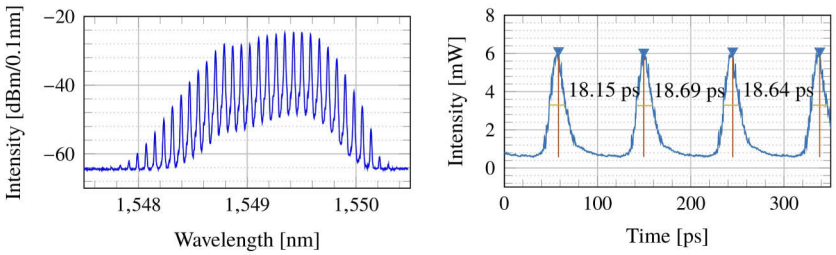
Optics EXPRESS

The optical frequency comb source, used in this work, was based on an externally injected gain switched laser (EI-GSL) [35] . In comparison to other optical frequency combs generation techniques, EI-GSL based on direct modulation is simple, cost efficient and flexible. Some other comb generation techniques, such as Kerr microresonators and electro-optic (EO) modulation [36] can be considered as well. The external injection from a single low linewidth master tunable laser (TL) into the gain switched slave laser enables the EI-GSL source to offer low linewidth [37], tunability of the central emission wavelength [38], a high degree of phase correlation between all of the comb's tones [39], and a tunable and stable free spectral range [40]. It is also important to note that this configuration is suitable for photonic integration [41]. A shortcoming associated with this comb generation technique is the limited number of comb tones generated (directly related to the bandwidth of the laser).

The EI-GSL optical frequency comb generation schematic is shown in Fig. 5(a). A commercially available Fabry-Perot (FP) laser (slave) used in our experiment is a 200 μm long device encased in a high speed butterfly package. The threshold current of the FP was around 8 mA at 25°C and the small signal modulation bandwidth was measured to be around 11 GHz, when biased at 60 mA. Gain switching of this FP laser was achieved by driving the laser diode with a large amplified sinusoidal signal (24 dBm @ 10 GHz) in conjunction with a dc bias current of 60 mA, while the laser was temperature controlled at 25°. A semiconductor based TL, with a linewidth of ~300 kHz and an output power of −4 dBm, was used to inject light via a polarization maintaining circulator into the gain switched laser. However, the number of lines generated (12) was low due to the limited bandwidth of the FP laser used. Hence, the generated comb was expanded by passing it through a 10 Gb/s phase modulator biased at $2.75V_\pi$ and driven by the same RF signal as used for the comb generation. The expanded EI-GSL comb spectrum, as illustrated in Fig. 5(b), yielded 20 clearly resolved phase correlated optical tones, with each of the tones offset by an integer multiple of the drive frequency (10 GHz). The corresponding optical pulse train is shown in Fig. 5(c) with a pulse width of ~ 18.5 ps.



(a)



(b) (c)

Fig. 5. (a) Externally injected gain switched laser (EI-GSL) block diagram. (b) Gain-switched frequency comb with 10 GHz FSR optical spectrum analyzer measurement. (c) Temporal measurement of the frequency comb output with 65 GHz sampling scope.

Optics EXPRESS

4.2. Encryption and steganography system setup

The experimental setup is depicted in Fig. 6. At the transmitter side, the data is mapped to QPSK symbols and digitally shaped using a SRRC filter. This QPSK symbols stream feeds a Mach-Zehnder IQ modulator (I/Q-MZM) that modulates all the optical frequency comb's tones at once, at 10 Gbaud. Synchronization between the comb's FSR and the Baud ($T_s = 1/\delta_f$) is achieved by sharing the same reference clock between the comb device and the DAC. LCoS-based SLM, Finisar WaveShaper, is then used to: a. determine the number of comb tones (L); b. equalize the spectrum; and c. impose the spectral phase mask. Subsequently, a noise loading mechanism, comprised of a variable optical attenuator (VOA) and an Erbium-doped fiber amplifier (EDFA) adjusts various, possibly negative, OSNR levels. The stealth and encrypted signal is transmitted to a short standard single mode fiber (SSMF), forming an optical back-to-back (OBTB) experiment.

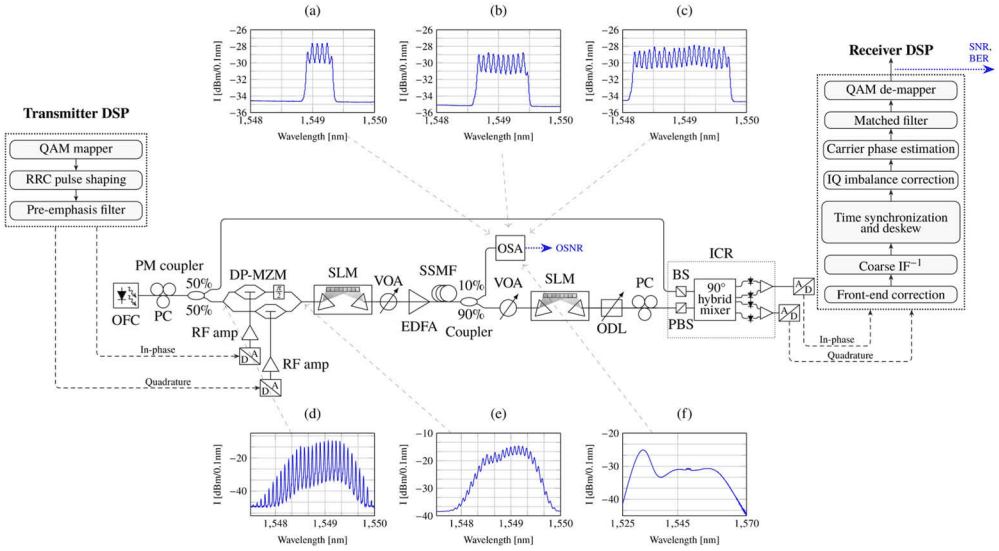


Fig. 6. Setup for encrypted and stealth coherent optical system. OFC – externally injected gain-switched optical frequency comb laser; DP-MZM – dual parallel Mach-Zehnder modulator; PC – polarization controller; SLM – spatial light modulator; VOA – variable optical attenuator; EDFA - Erbium-doped fiber amplifier; SSMF – standard single mode fiber; OSA – optical spectrum analyzer; ODL – optical delay line; ICR – integrated coherent receiver. Blue text indicated where OSNR, SNR and BER are measured. Insets (a), (b) and (c) represent the modulated, flattened and encoded spectrum at 7 dB OSNR for 5, 10, and 20 tones, respectively. In insets (d) and (e), raw and modulated spectrum are shown. Inset (f) represents a full C-band OSA trace, with 20 tones signal of total 200 GHz bandwidth at −10 dB OSNR.

Insets (a), (b) and (c) of Fig. 6 represent optical spectrum analyzer (OSA) traces of modulated, flattened and encoded spectrum at 7 dB OSNR for 5, 10, and 20 tones, respectively. In insets (d) and (e), raw and modulated spectrum are shown. Inset (f) represents a full C-band OSA trace, with 20 tones signal of total 200 GHz bandwidth at −10 dB OSNR.

At the receiver, a branch of the unmodulated optical frequency comb is used as the LO for multi-homodyne coherent detection. In practical implementations, some techniques may be used to regenerate a synchronized LO, for example, transmitting the LO on orthogonal polarization or transmitting a pilot tone [42]. To maximize the temporal overlapping, an optical delay line (ODL) is used. A polarization controller (PC) is used to align the signal and the LO before they are mixed together at the coherent receiver, and the product of the multi-homodyne coherent

Optics EXPRESS

detection results in a baseband signal that is being digitized. Follows, the Rx DSP is applied: first, filtering the baseband term (to eliminate high-order interference terms), second, running a conventional coherent detection chain, in a similar fashion to [26].

5. Results and discussion

The security scheme is evaluated by by numerical simulation and by experiment. Based on the experimental scheme described above, the system's performance was assessed for both the authorized and unauthorized users. A thorough quantitative analysis was performed on the following parameters: 1) SNR versus OSNR for the authorized user, and for the unauthorized user while applying a typical (unmatched) phase mask. 2) The optical processing gain, obtained by the multi-homodyne coherent detection, vs. the optical frequency comb's number of tones. 3) The stealthiness level by measuring the signal's prominence in the optical spectrum domain. 4) BER versus OSNR for the authorized and unauthorized users. Throughout this experimental session, a secured 10 Gbaud single-polarization QPSK signal is transmitted.

5.1. Experimental results

The optical processing gain enables the authorized user to achieve a considerable improvement in the SNR, which is proportional to the optical frequency comb's number of tones participating in the multi-homodyne coherent detection, as shown in Eq. (16). The relation between the SNR and the OSNR is given as follows:

$$\mathrm{SNR} = \mathrm{OSNR} + \mathrm{PG} + \mathrm{PER}, \tag{24}$$

where $\mathrm{PG} = 10\log_{10}(L)$, and the polarization extinction ratio (PER) term is related to the defined polarization of the signal carrier versus the unpolarized nature of the ASE noise. While the two ASE polarization states contribute to the measured ASE, the coherent receiver tracks the polarization of the received signal, thus effectively discriminates the orthogonal polarization component of the ASE. Therefore, a theoretical 3 dB polarization extinction ratio should be considered in favour of the received SNR. In practice, the coherent receiver is not perfectly aligned with the polarization of the received signal, and the polarization extinction ratio is calculated according to:

$$\mathrm{PER} = 10\log_{10}\left(2 \cdot \frac{\text{Detected signal power}}{\text{Total signal power}}\right). \tag{25}$$

Figure 7(a) represents the authorized user's SNR (blue curves) vs. OSNR, obtained for 5, 10 and 20 comb's tones. For instance, in case of −1 dB OSNR, and a signal carried by 20 tones, a detected SNR of 15 dB is expected to be achieved by the authorized user, attributed by 13 dB optical processing gain and another 3 dB polarization extinction ratio. In practice, a SNR of 9 dB was obtained, validating the predicted high optical processing gain, nevertheless limited by the system's noise floor that restrains the linear SNR-OSNR relation at high SNR.

The system's noise floor is comprised of various noise and distortion sources such as MZM and RF drivers nonlinearty, DAC and ADC impairments, laser phase noise, etc. Such noises are originated at the baseband and therefore affect each of the passband replicas in the same manner. The optical processing gain which diminishes the broadband ASE noise cannot resort to baseband-related noises thus bounds the detected SNR to roughly 12 dB in an OBTB measurements, in the described experiment. Hence, in order to extract the optical processing gain out of the detected SNR, the latter should be de-embedded off the system's noise floor. The system noise floor can be readily measured by detecting a signal with a high OSNR (of more than 30 dB). Figure 7(b) depicts two SNR curves, recovered from a 20 tones carrier, before and after noise de-embedding. Using the de-embedded SNR, a clear optical processing gain chart can be generated. It is further

Optics EXPRESS

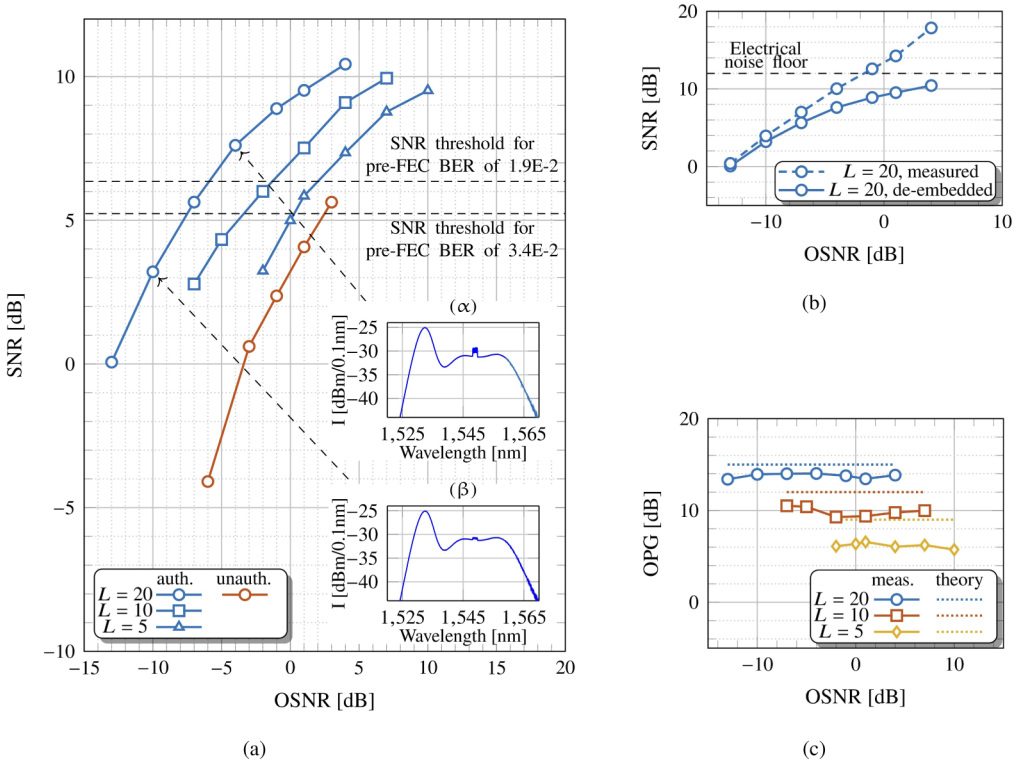


Fig. 7. (a) The SNR vs. OSNR of a 10 Gbaud single-polarization QPSK signal detected by the authorized user (blue) for 5, 10 and 20 comb's tones, and the SNR detected by the unauthorized user for 20 tones. Insets: an optical spectrum of 20 tones at −4 dB OSNR (α) and at −10 dB OSNR (β). Two types of pre-FEC BER thresholds are indicated by dashed horizontal lines. (b) Measured SNR curve (solid line), and post-processed SNR curve (dashed line) after de-embedding the system's noise floor which limits the SNR to a maximal value of 12 dB (dashed horizontal line). (c) Optical processing gain (OPG) of the authorized user for different number of tones. The theoretical values are given in dashed lines.

worth noting that the OSNR is defined here as the ratio of the optical signal's total power to the noise power in the same optical bandwidth (200 GHz in case of 20 tones), in units of [dB]. In addition, the SNR refers to the averaged symbol's energy divided by the noise power spectral density (E_s/N_0).

Figure 7(c) depicts the optical processing gain calculated from the same data of Fig. 7(a). As predicted by the analytical model (Eq. (24)), the optical processing gain is independent of the initial OSNR condition. In addition, the optical processing gain stands in a good agreement with respect to the theory, as it is fairly equal to the number of the comb's tones participating in the multi-homodyne coherent detection. The agreement is up to a penalty of 1.5 dB (at 20 tones), 2.5 dB (at 10 tones) and 3 dB (at 5 tones) between the theoretical and the measured PG, as indicated by the vertical gaps between solid and dashed lines of Fig. 7(c). This optical processing gain penalty can be explained by several factors, including the polarization misalignment between the received signal and the detector (unideal polarization extinction ratio), some imperfections that are not fully compensated by the receiver DSP, and the limited ability to equalize the various comb's tones at the transmitter. Specifically, the marginal tones are rather attenuated by the SLM, as shown in Fig. 6, insets (a)–(c). Therefore measurements with a low number of tones (5)

Optics EXPRESS

introduce a larger optical processing gain penalty relative to measurements with a high number of tones (20).

To demonstrate the stealthiness/steganography level of the secured signal, the optical spectrum is plotted as insets (α) and (β) in Fig. 7(a). Inset (α) represents a signal with OSNR of −4 dB, which produces a PSD prominence of 1.4 dB, while the inset (β) indicates a signal of −10 dB OSNR, with 0.4 dB PSD prominence. Such small spectral features can be concealed within a public network, loaded with public WDM channels [43]. The ability to produce a stealth signal with sufficient bit error-rate performance, is therefore a function of the comb number of tones, the OSNR and the pre-FEC BER threshold that should be attained for error-free detection.

In Fig. 8 the measured BER is plotted for the authorized user and for the unauthorized user at a constant $L = 20$ number of tones. Two error-free detection thresholds are shown in this figure. A 3rd generation FEC with a SNR threshold of 9.35 dB, assuming 15% overhead and net-coding gain (NCG) of 11 dB, designed to convert a 1.9E-2 pre-FEC BER to less than 1E-15 [44,45]. An advanced 4th generation FEC with a SNR threshold of 8.25 dB assuming NCG of 11.5 dB for QPSK, which is designed for a pre-FEC BER of 3.4E-2 [46]. The BER of Fig. 8 stands in a good agreement with respect to the known relation of BER in additive white Gaussian noise channel $P_{err} = \mathrm{Q}\left(\sqrt{\mathrm{SNR}}\right)$ [47]. This result validates the analytical model, as the ASE noise undergoes an incoherent addition, remains a white Gaussian noise.

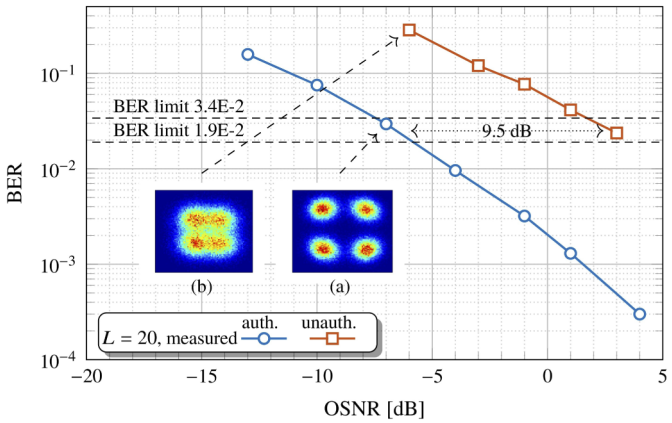


Fig. 8. BER vs. OSNR for authorized and unauthorized users at constant number of 20 tones. Insets: constellations received at almost equal OSNR points for authorized user (a) and Eve (b).

A single-polarization 20 Gbps line-rate error-free operation at −7.5 dB OSNR is demonstrated, with respect to the 3.4% pre-FEC BER. The BER chart indicates that a potential improvement of 4 dB in the optical processing gain will allow a stealth operation at −11.5 dB OSNR, corresponding to the use of 50 comb's tones. While 100 spectral tones (1 THz total bandwidth) will allow operation at −14.5 dB OSNR, with a minor spectral prominence of 0.15 dB. It is worth noting that chromatic dispersion may be a limiting factor in $B \cdot L$ product, and proper dispersion compensation should be implemented in the optical domain. Since the carrier wavelength is far away from the zero-dispersion wavelength, β_3 has a negligible contribution to the pulse broadening, that is therefore dominated by the residual (uncompensated) β_2 [47]. Consequently, for the case of residual dispersion of less than 100 m, and overall bandwidth of 1 THz, it can be shown that the optical processing gain penalty is less than 1 dB.

Increasing the number of comb's tones will improve the optical processing gain and therefore the steganography level of the encryption system as well. For addressing deployment of the proposed system in a real-world network, it is imperative to discuss steganography in cascaded

Optics EXPRESS

amplifiers networks. In such links, each amplifier stage degrades the OSNR, thus the received OSNR is inevitably lower than the line OSNR. To ensure steganography through the entire optical link, the network architect should consider the OSNR penalty introduced by the cascaded amplifiers. The expression for OSNR after cascade of N_{amp} amplifiers is given as follows [47]:

$$\text{OSNR [dB]} = 58 + P_{in} - \text{NF} - \Gamma - 10\log_{10}\left(N_{\text{amp}}\right), \tag{26}$$

while assuming that each amplifier compensates for the loss of the previous span (Γ dB). In data center interconnections (DCI), which are typically sub-100 km, one can consider two amplifiers: Tx booster and Rx pre-amp. Therefore DCI scenario adds a 3 dB OSNR penalty.

The performance of the unauthorized user was evaluated, and presented in Fig. 7(a) and Fig. 8, by the red lines. For a decent comparison, the polarization and the delay line were optimized for both the authorized and for the unauthorized users. A random mask at the unauthorized receiver was selected, which invoked an incoherent addition process of the various spectral replicas of the signal. An absolute incoherent addition will result in SNR degradation that is equals to the number of tones. In case of $L = 20$ and an equal number of mask's spectral bins, a 13 dB SNR degradation is expected for the unauthorized user. The red curve of Fig. 7(a) shows a constant 9.5 dB SNR degradation, relative to the authorized user (blue line) with 20 tones operation. For example, at −7 dB OSNR, the authorized user obtains the pre-FEC BER of 2E-2, while the unauthorized user approaches 2E-1 of error rate at higher OSNR conditions of −6 dB. Constellation diagrams of these two points are shown in insets (a) and (b) of Fig. 8, respectively.

Evidently, the chosen random phase mask has generated a SNR degradation of 9.5 dB where 13 dB of SNR degradation was expected for an absolute incoherent addition case of the unauthorized user. This gap is explained by the limited flatness of the frequency comb, and due to the modeling of the SLM phase response as rectangles, rather than its practical shape. Yet, it is shown that the unauthorized user achieves significantly poorer detection performance, even when only 20 tones are used. Upon increasing the number of tones, the encryption strength will be dramatically improved.

6. Conclusions

We have proposed and experimentally validated a novel concept of multi-homodyne coherent detection enabled by an optical frequency comb source. We utilize this scheme for stealth optical encryption by applying optical spectral phase encoding to the modulated EI-GSL output. The demonstrated scheme achieves all-optical encryption and steganography transmission with error-free operation over extremely low link budget conditions, such as 40 Gbps transmission under negative −7.5 dB OSNR. Decoding the secured signal requires real-time broadband manipulation by all-optical means, else the signal is permanently destroyed.

Funding. Ministero degli Affari Esteri e della Cooperazione Internazionale; Science Foundation Ireland (15/CDA/3640).

Disclosures. The authors declare no conflicts of interest.

Data availability. Data underlying the results presented in this paper are not publicly available at this time but may be obtained from the authors upon reasonable request.

References

1. M. Zafar Iqbal, H. Fathallah, and N. Belhadj, "Optical fiber tapping: Methods and precautions," in *8th International Conference on High-capacity Optical Networks and Emerging Technologies*, (2011), pp. 164–168.
2. K. Shaneman and S. Gray, "Optical network security: technical analysis of fiber tapping mechanisms and methods for detection prevention," in *IEEE MILCOM 2004. Military Communications Conference, 2004.*, vol. 2 (2004), pp. 711–716 Vol. 2.
3. R. Rejeb, M. S. Leeson, and R. J. Green, "Fault and attack management in all-optical networks," IEEE Commun. Mag. **44**(11), 79–86 (2006).
4. F. Arute, K. Arya, R. Babbush, D. Bacon, J. Bardin, R. Barends, R. Biswas, S. Boixo, F. Brandao, D. Buell, B. Burkett, Y. Chen, Z. Chen, B. Chiaro, R. Collins, W. Courtney, A. Dunsworth, E. Farhi, B. Foxen, and J. Martinis, "Quantum supremacy using a programmable superconducting processor," Nature **574**(7779), 505–510 (2019).

Optics EXPRESS

5. M. P. Fok, Z. Wang, Y. Deng, and P. R. Prucnal, "Optical Layer Security in Fiber-Optic Networks," IEEE Trans.Inform.Forensic Secur. **6**(3), 725–736 (2011).
6. P. J. Winzer, D. T. Neilson, and A. R. Chraplyvy, "Fiber-optic transmission and networking: the previous 20 and the next 20 years [invited]," Opt. Express **26**(18), 24190–24239 (2018).
7. T. H. Shake, "Security performance of optical CDMA Against eavesdropping," J. Lightwave Technol. **23**(2), 655–670 (2005).
8. N. Kostinski, K. Kravtsov, and P. R. Prucnal, "Demonstration of an all-optical ocdma encryption and decryption system with variable two-code keying," IEEE Photonics Technol. Lett. **20**(24), 2045–2047 (2008).
9. S. Etemad, A. Agarwal, T. Banwell, J. Jackel, R. Menendez, and P. Toliver, "OCDM-based photonic layer 'security' scalable to 100 Gbits/s for existing WDM networks [Invited]," J. Opt. Netw. **6**(7), 948–967 (2007).
10. S. Etemad, A. Agarwal, T. Banwell, G. D. Crescenzo, J. Jackel, R. Menendez, and P. Toliver, "An Overlay Photonic Layer Security Approach Scalable to 100 Gb/s," IEEE Commun. Mag. **46**(8), 32–39 (2008).
11. B. B. Wu and E. E. Narimanov, "A method for secure communications over a public fiber-optical network," Opt. Express **14**(9), 3738–3751 (2006).
12. H. K. Lo, M. Curty, and K. Tamaki, "Secure quantum key distribution," Nat. Photonics **8**(8), 595–604 (2014).
13. B. Korzh, C. Lim, R. Houlmann, N. Gisin, M.-J. Li, D. Nolan, B. Sanguinetti, R. Thew, and H. Zbinden, "Provably Secure and Practical Quantum Key Distribution over 307 km of Optical Fibre," Nat. Photonics **9**(3), 163–168 (2015).
14. A. Argyris, D. Syvridis, L. Larger, V. Annovazzi-Lodi, P. Colet, I. Fischer, J. Garcia-Ojalvo, C. Mirasso, L. Pesquera, and A. Shore, "Chaos-based communications at high bit rates using commercial fibre-optic links," Nature **438**(7066), 343–346 (2005).
15. L. Wang, X. Mao, A. Wang, Y. Wang, Z. Gao, S. Li, and L. Yan, "Scheme of coherent optical chaos communication," Opt. Lett. **45**(17), 4762–4765 (2020).
16. J. Ke, L. Yi, G. Xia, and W. Hu, "Chaotic optical communications over 100-km fiber transmission at 30-gb/s bit rate," Opt. Lett. **43**(6), 1323–1326 (2018).
17. Y. J. Jung, C. Son, S. Lee, J. Kim, S.-K. Gil, and N. Park, "Demonstration of 10 gbps, all-optical encryption and decryption system utilizing soa xor logic gate," Opt. Quantum Electron. **40**(5-6), 425–430 (2008).
18. K. Kitayama, Xu Wang, and Naoya Wada, "OCDMA over WDM PON-solution path to gigabit-symmetric FTTH," J. Lightwave Technol. **24**(4), 1654–1662 (2006).
19. D. M. Marom, D. T. Neilson, D. S. Greywall, C.-S. Pai, N. R. Basavanhally, V. A. Aksyuk, D. O. López, F. Pardo, M. E. Simon, Y. Low, P. Kolodner, and C. A. Bolle, "Wavelength-Selective 1 x K Switches Using Free-Space Optics and MEMS Micromirrors: Theory, Design, and Implementation," J. Lightwave Technol. **23**(4), 1620–1630 (2005).
20. B. Wu, Z. Wang, Y. Tian, M. P. Fok, B. J. Shastri, D. R. Kanoff, and P. R. Prucnal, "Optical steganography based on amplified spontaneous emission noise," Opt. Express **21**(2), 2065–2071 (2013).
21. B. Wu, A. N. Tait, M. P. Chang, and P. R. Prucnal, "Wdm optical steganography based on amplified spontaneous emission noise," Opt. Lett. **39**(20), 5925–5928 (2014).
22. C. Pulikkaseril, L. A. Stewart, M. A. F. Roelens, G. W. Baxter, S. Poole, and S. Frisken, "Spectral modeling of channel band shapes in wavelength selective switches," Opt. Express **19**(9), 8458–8470 (2011).
23. D. Xie, D. Wang, M. Zhang, Z. Liu, Q. You, Q. Yang, and S. Yu, "Lcos-based wavelength-selective switch for future finer-grid elastic optical networks capable of all-optical wavelength conversion," IEEE Photonics J. **9**(2), 1–12 (2017).
24. S. Asraf, T. Yeminy, D. Sadot, and Z. Zalevsky, "Proof of concept for ultrahigh resolution photonic spectral processor," Opt. Express **26**(19), 25013–25019 (2018).
25. T. Yeminy, D. Sadot, and Z. Zalevsky, "Spectral and temporal stealthy fiber-optic communication using sampling and phase encoding," Opt. Express **19**(21), 20182–20198 (2011).
26. E. Wohlgemuth, Y. Yoffe, T. Yeminy, Z. Zalevsky, and D. Sadot, "Demonstration of coherent stealthy and encrypted transmission for data center interconnection," Opt. Express **26**(6), 7638–7645 (2018).
27. E. Ip, A. P. T. Lau, D. J. F. Barros, and J. M. Kahn, "Coherent detection in optical fiber systems," Opt. Express **16**(2), 753–791 (2008).
28. J. Barros and M. R. D. Rodrigues, "Secrecy capacity of wireless channels," in *2006 IEEE International Symposium on Information Theory*, (2006), pp. 356–360.
29. M. Bloch and J. N. Laneman, "On the secrecy capacity of arbitrary wiretap channels," in *2008 46th Annual Allerton Conference on Communication, Control, and Computing*, (2008), pp. 818–825.
30. P. Beckmann, "Rayleigh distribution and its generalizations," J. Res. NBS **68D**(9), 927–932 (1964).
31. A. Papoulis and S. U. Pillai, *Probability, Random Variables, and Stochastic Processes* (McGraw Hill, Boston, 2002), 4th ed.
32. M. Simon, "On the probability density function of the squared envelope of a sum of random phase vectors," IEEE Trans. Commun. **33**(9), 993–996 (1985).
33. M. Imran, P. M. Anandarajah, A. Kaszubowska-Anandarajah, N. Sambo, and L. Potí, "A survey of optical carrier generation techniques for terabit capacity elastic optical networks," IEEE Commun. Surv. Tutorials **20**(1), 211–263 (2018).
34. V. Torres-Company, J. Schröder, A. Fülöp, M. Mazur, L. Lundberg, O. B. Helgason, M. Karlsson, and P. A. Andrekson, "Laser frequency combs for coherent optical communications," J. Lightwave Technol. **37**(7), 1663–1670 (2019).

Optics EXPRESS

35. P. M. Anandarajah, R. Maher, Y. Q. Xu, S. Latkowski, J. O'Carroll, S. G. Murdoch, R. Phelan, J. O'Gorman, and L. P. Barry, "Generation of coherent multicarrier signals by gain switching of discrete mode lasers," IEEE Photonics J. **3**(1), 112–122 (2011).
36. A. Parriaux, K. Hammani, and G. Millot, "Electro-optic frequency combs," Adv. Opt. Photonics **12**(1), 223–287 (2020).
37. R. Zhou, T. N. Huynh, V. Vujicic, P. M. Anandarajah, and L. P. Barry, "Phase noise analysis of injected gain switched comb source for coherent communications," Opt. Express **22**(7), 8120–8125 (2014).
38. R. Zhou, S. Latkowski, J. O'Carroll, R. Phelan, L. P. Barry, and P. Anandarajah, "40nm wavelength tunable gain-switched optical comb source," Opt. Express **19**(26), B415–B420 (2011).
39. P. D. Lakshmijayasimha, A. Kaszubowska-Anandarajah, E. P. Martin, P. Landais, and P. M. Anandarajah, "Expansion and phase correlation of a wavelength tunable gain-switched optical frequency comb," Opt. Express **27**(12), 16560–16570 (2019).
40. M. D. G. Pascual, R. Zhou, F. Smyth, P. M. Anandarajah, and L. P. Barry, "Software reconfigurable highly flexible gain switched optical frequency comb source," Opt. Express **23**(18), 23225–23235 (2015).
41. M. D. Gutierrez Pascual, V. Vujicic, J. Braddell, F. Smyth, P. Anandarajah, and L. Barry, "Photonic integrated gain switched optical frequency comb for spectrally efficient optical transmission systems," IEEE Photonics J. **9**(3), 1–8 (2017).
42. M. Mazur, A. Lorences-Riesgo, J. Schröder, P. A. Andrekson, and M. Karlsson, "High Spectral Efficiency PM-128QAM Comb-Based Superchannel Transmission Enabled by a Single Shared Optical Pilot Tone," J. Lightwave Technol. **36**(6), 1318–1325 (2018).
43. E. Wohlgemuth, Y. Yoffe, P. Nadimi Goki, M. Imran, F. Fresi, L. Potì, and D. Sadot, "Demonstration of Stealthy and Encrypted Optical Transmission Below Adjacent 50 GHz DWDM Channels," IEEE Photonics Technol. Lett. **32**(10), 581–584 (2020).
44. L. E. Nelson, G. Zhang, M. Birk, C. Skolnick, R. Isaac, Y. Pan, C. Rasmussen, G. Pendock, and B. Mikkelsen, "A robust real-time 100G transceiver with soft-decision forward error correction [Invited]," J. Opt. Commun. Netw. **4**(11), B131–B141 (2012).
45. G. Tzimpragos, C. Kachris, I. B. Djordjevic, M. Cvijetic, D. Soudris, and I. Tomkos, "A Survey on FEC Codes for 100 G and Beyond Optical Networks," IEEE Commun. Surv. Tutorials **18**(1), 209–221 (2016).
46. K. Roberts, Q. Zhuge, I. Monga, S. Gareau, and C. Laperle, "Beyond 100 Gb/s: capacity, flexibility, and network optimization [Invited]," J. Opt. Commun. Netw. **9**(4), C12–C23 (2017).
47. G. P. Agrawal, *Fiber-Optic Communications Systems*, Wiley series in microwave and optical engineering (Wiley, New York, 2002).

93.46.222.216 {ts '2025-02-22 04:56:59'}