DSP-Based Physical Layer Security for Coherent Optical Communication Systems

Giddings, Roger; He, Jiaxiang; Tang, Jianming; Jin, Wei

IEEE Photonics Journal

DOI:
10.1109/JPHOT.2022.3202433

Published: 01/10/2022

Peer reviewed version

DSP-Based Physical Layer Security for Coherent Optical Communication Systems

Jiaxiang He, Roger Giddings, Wei Jin and Jianming Tang

***Abstract*—A novel digital signal processing (DSP)-based scheme for physical layer security in coherent optical communication systems is proposed and numerically investigated. The optical layer signal encryption is accomplished by two dispersive elements and one phase modulator (PM) driven by a DSP-generated encryption key, whilst signal decryption uses similar components but with inverted dispersion values and security keys. A critical aspect of the DSP-based physical layer security is that the security keys, driving the PMs to hide/recover the data signals, must be highly unpredictable and noise-like, thus orthogonal frequency division multiplexing (OFDM) signals are employed as they possess these characteristics, they can also be easily generated and cover a suitably wide range of unique keys. Numerical simulations are conducted to determine optimum system parameters for achieving a high level of security, the key parameters requiring optimization are the dispersion of the dispersive elements and the bandwidth of the security keys. Using these determined optimum parameters, in-depth investigations are undertaken of encryption/decryption induced transmission performance penalties, sensitives to various parameter offsets and operation over various transmission distances. To observe any data signal dependencies, various performance metrics are investigated for different combinations of modulation formats (DQPSK and 16QAM) and baud rates (40Gbaud and 100Gbaud) for the transmitted data signals. The proposed DSP-based physical layer security scheme is shown to have the potential to achieve, in a low-cost and highly effective manner, a high level of physical layer security with acceptable performance penalties for existing coherent optical communication systems.**

***Index Terms*— secure optical communications, optical layer encryption, coherent optical communications**

I. Introduction

Along with the well-known increasing demands on capacity and reach performance in long-haul, high speed optical fibre communications, improving data security has also attracted a lot of attention recently, especially as cybercrime activities are increasing [1]. The conventional way to realize secure communications is to apply complex digital cryptographic algorithms in the upper network layers [2]. However, securing information by software encryption is rapidly becoming an ineffective method to achieve secure optical communications networks, due to the rapid development in the power of quantum computers, this is allowing brute-force decryption methods to decrypt information within acceptable time frames. Lately, a lot of research work is being focused on physical-layer security methods which are not susceptible to the rapidly escalating computational power of quantum computers [3]. Some popular physical layer security methods currently of great interest include optical code multiplexing techniques, quantum communications and chaotic optical communications.

Optical code division multiple access (OCDMA) secures the optical system through encoding message signals from multiple users with orthogonal codes in the time or frequency domain [4], [5], but due to some vulnerabilities, such as standardized orthogonal codes, eavesdroppers may be able to extract data from the system [6]. Quantum key distribution (QKD) is a well-known and increasingly popular technique in quantum secure communications, it provides security for communication systems by sharing secret keys generated by quantum algorithms between the transmitter end and the receiver end [7]–[9]. The major advantage of QKD is that any third-party intercepting the key is always detectable, thus achieving ultra-high security. However, strong disparity exists between the maximum communication data rates in classical and QKD-based communications because of limitations on the rate of quantum key distribution and the fact that the typically adopted uncrackable encryption algorithms require the key to be at least as long as the corresponding data. The current maturity of the required quantum technology is also such that it is still relatively expensive. Thus, the mass market uptake of quantum secure communications relies on further technological developments and significant reductions in implementation costs [8]. In chaotic secure optical communications, information is masked and unmasked by synchronized chaotic optical signals in the encryption and decryption sides [10]–[13]. Chaotic secure systems benefit from applying readily available and simple laser devices, but synchronizing the chaotic optical carriers and achieving data transmission speeds above several 10s Gb/s [14], [15], are both ongoing challenges [16]. Techniques in [17], [18] provide different encoding methods combined with chaos encryption, both techniques have a large key space for physical layer security and so provide high security levels. However, these two techniques are only

This work was supported by The DSP Centre and has been part-funded by the European Regional Development Fund through the Welsh Government and by the North Wales Growth Deal through Ambition North Wales, Welsh Government and UK Government *(Corresponding author: R. P. Giddings).*

J. X. He, R. P. Giddings, W. Jin and J. M. Tang are with the School of Computer Science and Electronic Engineering, Bangor University, Bangor, LL57 1UT, U. K. (e-mail: eeu970@bangor.ac.uk; r.p.giddings@bangor.ac.uk; w.jin@bangor.ac.uk; j.tang@bangor.ac.uk).

applicable to OFDM-PONs and so do not support long-haul networks.

Many physically secure structures based on chaotic systems have also been proposed and investigated [19]–[23]. [19] provides a method to apply chaotic optical carriers into a system to achieve signal encryption, however, an eavesdropper may simply use a direct detection-based receiver and a filter with a suitable cut-off frequency to recover the data. While [20] employs a chaotic optical carrier with an extra encryption module, which includes a PM and a dispersion component to enhance the security by using phase-to-intensity conversion to further hide the information, but the benefits of the extra module might be easily removed by a tunable dispersion compensation element as the PMs do not cause any intensity changes for cases where the dispersion effect is negligible. [21] realizes encryption by applying a dispersive element to firstly temporally distort the transmitted signal, then, a chaos-based key driven PM applies optical phases changes, which are then converted to intensity changes by another dispersive element. The decryption side is an identical but inverse version of the encryption side. This scheme gets rid of the limitation on transmission bandwidths of the chaotic signals to enable high speed data transmissions. This scheme also offers a cost-effective physical structure which employs low cost, commercially available components. However, the way of generating the chaos-based security keys is still very complex and it also has the drawback of requiring a separate wavelength to transmit the security keys. Furthermore the basic technique for physical layer security in [21] is investigated in intensity modulation and direct detection (IMDD) transmission systems only, thus the suitability of the security technique to coherent systems is also an important factor to consider as coherent optical systems are employed for high speed, long-reach optical communications where security is also vital. A technique for physical layer security in coherent optical systems is proposed in [23], however this technique has the major disadvantage that it cannot be retrofitted to existing coherent transmission systems, because the secure system is realized by introducing a cipher-based algorithm at the bit level.

Inspired by previous work on IMDD based optical links, we apply a similar physical secure structure as in [21], to a coherent optical communication system, however to avoid the complexity of chaos-based security key generation, we propose a novel DSP-based approach to generate security keys for driving the PMs. The full structure of the newly proposed scheme is shown in Fig. 1. The proposed system uses real-time digitally generated OFDM signals as the security keys, thus removing the challenges of applying chaotic signals as keys and removes the stringent requirements of chaotic optical carrier synchronization. The DSP generated OFDM signal-based keys used to drive the PMs in the new scheme are noise-like signals in the time domain and are produced based on a unique and private set of parameters which are preprogramed into a security module pair before installation, thus transmitting the key together with the data is not necessary. The proposed key generation method requires the two transceivers to be physically connected, before deployment, they then negotiate and agree on the secret key's parameters, and so the selected key parameters are unknown to the operator for increased security. It would also potentially be feasible to employ secure key distribution techniques [24], [25] to establish the key, however the possibility of incorporating dynamic secure key distribution in this work would need further consideration.

OFDM signals are ideal for security key generation as a large key space can be easily produced by i) manipulating a set of different modulation parameters, including subcarrier count, subcarrier modulation formats, bit/power loading, clipping ratio and cyclic prefix length, ii) dynamically changing the OFDM modulation parameters from symbol to symbol, iii) the OFDM input bit sequence can be generated in numerous different ways to ensure a high entropy level, such as using a common stream cipher directly, such as RC4 [26] or combining a conventional PRBS sequence with a cipher stream and iv) the generated OFDM symbol samples can be further manipulated and combined using numerous different mathematical operations, all these factors being uniquely defined by the security key. This way of generating the noise-like waveform for encryption, can result in a theoretically unlimited number of security keys, thus achieving an excellent level of security. It should be noted that the key uniqueness will have varying sensitivity to the different OFDM modulation parameters, so this must be taken into account when determining the parameter selection rules for key generation, as an example, the required discrete levels for power loading must be predetermined. It is also important to highlighted that the proposed technique is transparent to the data transmission signals' format, data rate and bandwidth, thus breaking the limitations on signal transmission speed whilst still satisfying the demand of high-level physical layer security.

In this paper, the detailed operational performance of the DSP-based physical layer security system is numerically verified, and thus the proposed technique is shown to be valid for physical layer security in coherent optical communications. Firstly, the required optimum dispersion values and bandwidth of the security keys are determined to minimize implementation

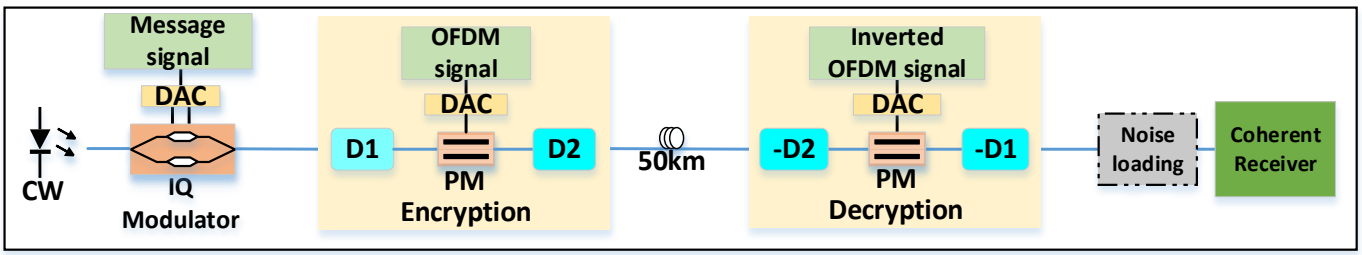

Fig. 1. Physical layer secure coherent optical communication system

costs whilst still achieving the required level of security. It is shown that, to achieve suitably high security, data signals with higher order modulation formats and higher baud rates require lower dispersion levels. However, higher baud rates require higher security key bandwidth. Optimum dispersion values and key bandwidth are determined to cover the considered range of data signals. Next, it is shown that there is a minimal performance penalty when the encryption and decryption elements employ identical parameters. Importantly, the system provides a high security level, even if an eavesdropper taps off some optical power and employs a tunable dispersive element to attempt steal the data. Then, to consider practical implementation issues, the sensitivity of the system to different encryption/decryption parameter offsets is explored in detail thus providing a clear understanding of the design and implementation tolerance aspects. Such technical robustness explorations are valuable but were excluded in [21]. It is revealed that the system is most sensitive to the dispersion offsets between the two dispersive elements placed adjacent to the transmission fibre and the timing offset (relative to the ideal timing) of the decryption keys. Also, transmitted signals with higher modulation formats and higher baud rates show more sensitivity to these offsets. Finally, the operation of the physical layer secure coherent optical system is also investigated over various transmission distances, i.e., multiple 80km amplified spans, it is shown that, without any parameter offsets, the performance is virtually identical to conventional long-haul coherent optical links with dispersion compensating fibres (DCFs).

II. Fundamental Operating Principle and System Architecture

The physical layer secure coherent system structure is shown in Fig. 1, where the system security is achieved by a transmitter-located physical layer encryption element and a receiver located physical layer decryption element. The encryption element consists of three optical components namely a dispersive element D1, a PM and a dispersive element D2. The transmitted data signal is first distorted by D1 due to the chromatic dispersion-induced temporal broadening effect on each data symbol, this also leads to further distortion due to the associated inter-symbol interference (ISI) effect. Then, the PM driven by a security key-based driving voltage, subsequently introduces a security key dependent dynamic phase change to the signal, which expands the optical signal bandwidth due to the non-linear characteristic of the PM modulation process, the PM thus introduces encryption within the signal's phase information. Next, to further enhance the security level, the dispersive element D2 then performs further distortion by chromatic dispersion-induced phase to amplitude conversions, thus introducing encryption within the signal's amplitude information. Accordingly, some of the secure phase encryption has also been transferred to secure amplitude encryption, which is dependent on the level of dispersion in D2. Finally, the data within the transmitted optical signals are completely masked in both the time and frequency domains by security key-controlled phase and amplitude distortions.

TABLE I
LIST OF PARAMETERS

Parameter	Value
Baud Rate for Transmitted Signal	40/100 Gbaud
Modulation Format	DQPSK/16QAM
Launch Power for Transmitted Signal	-10 dBm
Received Optical Power for Received Signal	-13 dBm
Optical Power for LO Laser at Coherent Receiver	13 dBm
IFFT Size for OFDM Key	32
Modulation Format for OFDM key subcarriers	16QAM
Power Loading for OFDM key subcarriers	uniform
Clipping Ratio for OFDM Key	14 dB
Modulation Index for PM	1.2
SSMF Transmission Distance	50 km
SSMF dispersion	16 ps/nm/km
SSMF Dispersion Slope	0.08 ps/nm^2/km
Fibre Attenuation	0.2 dB/km
Fibre Nonlinear Index	2.6e-20 m^2/W

For simplicity, the transfer functions of dispersive elements considered in this paper are modelled as:

$$H(\omega)_D = e^{-jD\frac{\lambda^2}{4\pi c}\omega^2} \quad (1)$$

where D is the dispersion introduced by the dispersive element, ω is the angular frequency offset from the optical carrier frequency, c is the speed of light in a vacuum and λ is the optical wavelength. Taking the inverse Fourier transform of $H(\omega)_D$, the impulse response of the dispersive element is $h(t)_D$. Assuming the unencrypted optical signal is $s(t)$, the encrypted optical signal, $s(t)_{En}$, can be expressed as:

$$s(t)_{En} = \{[s(t) \otimes h(t)_{D1}] e^{j\pi\frac{s(t)_{key}}{V_\pi}}\} \otimes h(t)_{D2} \quad (2)$$

where $h(t)_{D1}$ and $h(t)_{D2}$represent the impulse responses of the two dispersive elements D1 and D2, $s(t)_{key}$ is the OFDM-based security key, V_π is the half-wave volatge for the PM. The modualtion index m, of the PMs, is defined as $\left|s(t)_{key}\right|_{MAX} / V_\pi$. Assuming the impulse response of a standard single mode fiber (SSMF) is $h(t)_{fibre}$, the received encrypted signal after fiber transmission is:

$$s(t)_{Rx} = s(t)_{En} \otimes h(t)_{fibre} \quad (3)$$

The structure of the decryption element is the exact mirror opposite structure to the encryption element with inverse signs for the dispersive elements and the PM driving signal, the decrypted signal is therefore:

$$s(t)_{De} = \{[s(t)_{Rx} \otimes h(t)_{-D2}] e^{j\pi\frac{-s(t)_{key}}{V_\pi}}\} \otimes h(t)_{-D1} \quad (4)$$

To achieve the best decryption performance, the dispersive element -D2, in the decryption element, will compensate for the dispersion associated with both the optical fibre link and the dispersive element D2 in the encryption element. Comparing Eq. (2) and Eq. (4), we can see that the components in the decryption side remove all the distortions introduced by the encryption element by following an exact reverse order process

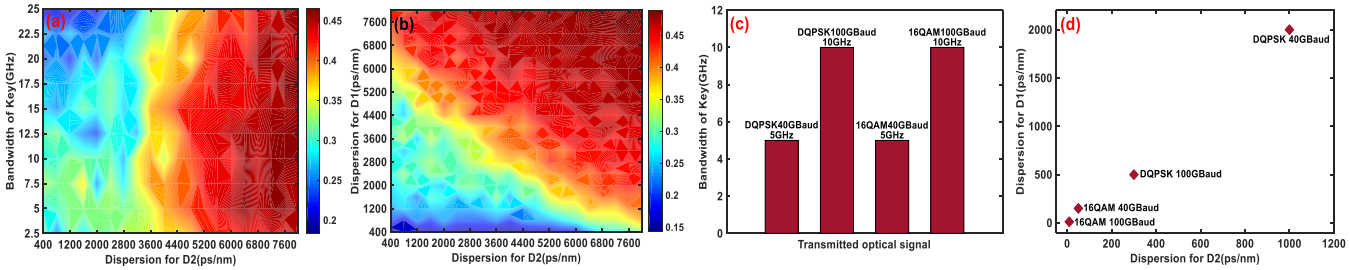

Fig. 2. (a) The influence of bandwidth of security keys on BER for DQPSK signals with 40Gbaud, fixing D1 to 3000ps/nm, and determining stable settings for bandwidth of the key; (b) The influence of value of D1 and D2 on BER for DQPSK with 40GBaud, fixing bandwidth of key to 5GHz, and determining suitable values for D1 and D2; (c) Optimum bandwidth of keys for different transmitted message signals under different suitable D1 and D2 values to reach BER=0.3; (d) Optimum dispersion values for D1 and D2 for different transmitted signals with a security key bandwidth of 10GHz to reach BER=0.3.

and so it recovers the transmitted optical data signal.

The proposed physical layer security technique thus has the major advantages that it employs a simple physical structure based on relatively low-cost optical components but provides a high security level. It is transparent to the signal modulation format, can operate at extremely high signal baud rates and can be retrofitted to an existing coherent optical link. Furthermore, it utilizes a unique DSP-based technique to dynamically generate the security keys in real-time using reconfigurable DSP hardware, the adopted security key controlling the particular hardware configuration, the reconfigurable DSP approach has the advantage of minimising the required overall DSP complexity. Other benefits of the technique are that transmitting the security key along with the data in a separate channel is not necessary, thus leading to improved spectral utilization efficiency, it also greatly simplifies the task of generating identical security keys at the encryption and decryption elements, enables simple control of the key selection, offers the potential for a vast key space, is capable of exploiting the low-cost associated with the volume production of digital integrated circuits (ICs) and can have high reliability due to the use of highly mature technologies.

Furthermore, operation at the physical layer provides excellent robustness to brute force attacks based on powerful quantum computers, as eavesdroppers must record the transmitted high-speed waveform samples, requiring vast memory. The attacker would not only need to determine the key by brute force but also apply a brute force approach to model the correct structure of the decryption element.

In this paper, numerical simulations are performed using MATLAB and VPItransmission Maker. The employed system parameters for the considered coherent optical system are listed in Table I.

III. Determination of Optimum System Parameters

A. Optimization of dispersive elements' values and bandwidth of secure system keys

Based on the operating principle outlined in section II, the security level of the coherent optical secure communication system is clearly dependent on the parameters of D1, D2 and the bandwidth of the security key signals driving the PMs. It is thus vital to select suitable values for these parameters to ensure the secure coherent optical system can adequately hide the transmitted data. From a practical implementation and cost perspective, it is also desirable to minimize the dispersion values for D1 and D2, and the bandwidth of the security keys whilst achieving a desired high level of security, therefore this section determines suitable optimum values for the aforementioned parameters. Here, a sufficiently high level of security is considered to be achieved when an illegally implemented receiver observes a BER≥0.3. An initial modulation index of 1.2 is adopted for the PMs.

To check the security level of the encrypted signals, the encrypted signal is fed directly to the coherent receiver after noise loading. At the receiver, appropriate digital algorithms are applied to perform coherent signal recovery, including a least mean square (LMS) equalizer (with a fixed number of taps and step size optimized according to the received signals). Firstly, a 40Gbaud, differential quadrature phase shift keying (DQPSK) modulated data signal is generated, and suitable contour plots are then produced to observe how the BER changes with variations in dispersive values D1 and D2 and the bandwidth of the security keys. Attention is first paid to the selection of the bandwidth of the security keys. The encryption element has a fixed D1 dispersion value of 3000ps/nm, with the D2 value and the bandwidth of the security key being varied. It is shown in Fig. 2 (a), that a suitable bandwidth for the security key is 5GHz as a higher bandwidth does not considerably increase the BERs, which, however, start to reduce as the key bandwidth increases significantly. The existence of an optimum key bandwidth can be explained by the fact that for a given dispersion value, a sufficient key bandwidth is required to cause a suitably high level of phase change-induced signal distortions. The reason why, as the key bandwidth continues to increase further, the BERs start to decrease, as shown in Fig.2 (a), is that the faster phase changes in the frequency domain, in combination with D2, produce faster amplitude changes in the time domain, which exceed the data signal's bandwidth so are less effective at encryption. Thus, due to the limited power of the PM driving signal less power is available in the more effective encryption frequency bands of the key.

Next, attention is paid to the selection of the values for the two dispersive components with the bandwidth of the security key set to 5GHz. Fig. 2(b) clearly illustrates the growth in the BER follows the increase of both D1 and D2 dispersion values, this is due to the increasing temporal signal distortion associated with higher dispersion. Furthermore, the encryption capability is seen to be influenced more by the dispersion value

of D1 when both dispersive elements have relatively small dispersion values, this can be explained by the fact that the D1-induced distortion are then effectively amplified by the subsequent encryption element distortions, whereas this effect does not apply to D2-induced distortions. There are shown to be multiple suitable combinations of the D1 and D2 values for achieving a BER of ~0.3, thus, the encryption/decryption device pairs could be manufactured with varying D1/D2 combinations to reduce the vulnerability to an attacker identifying the D1/D2 values. The selected combination of D1 and D2 are 2000ps/nm and 1000ps/nm respectively.

To encrypt transmitted coherent optical data signals with different bandwidth and formats, the DSP-based physical layer encryption system will have different demands on D1, D2 and the security key bandwidth. Simulations are therefore also performed, using the system employed in calculating Fig. 2(a) and (b), to determine the optimum values for D1, D2 and key bandwidth, when transmitting three other data signals of DQPSK at 100GBaud and 16QAM at 40GBaud and 100GBaud. As shown in Fig. 2(c), with the different optimum dispersion parameters for D1 and D2 used in each case, it is shown that the optimum bandwidth of the key is related to the baud rate of the transmitted data signals. To enable the system to be transparent to different transmitted data signals up to 16-QAM at 100GBaud, the optimum bandwidth of the key is determined to be 10GHz. By applying this optimum bandwidth for the security key, the optimum dispersion values for different transmitted data signals are shown in Fig. 2(d). Signals with higher order modulation formats and higher baud rates can be seen to require lower dispersion values for D1 and D2, as signals with higher order modulation formats are more sensitive to any distortions in both amplitude and phase changes, and signals with higher baud rate are more susceptible to the ISI introduced by the dispersion elements. Based on the above results, adopting D1 = 2000ps/nm, D2 = 1000ps/nm and a security key bandwidth of 10GHz will enable a secure system to be achieved for all the different combinations of transmitted data signals considered in this paper. These parameter values are thus considered as the default values applied in further simulations unless stated otherwise. Fig. 3(a-f) shows the

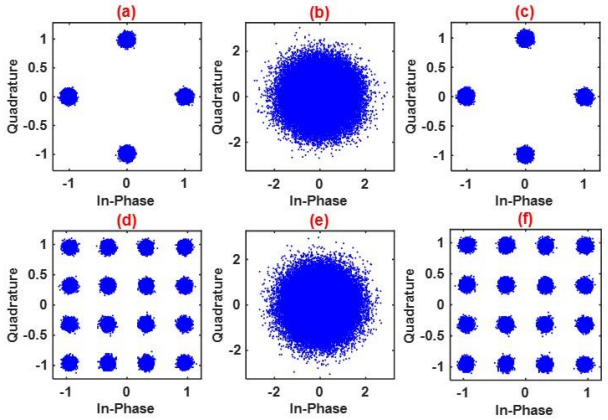

Fig. 3. Transmitted signals are DQPSK and 16QAM at 40Gbaud, and OSNR is set to 30dB. (a) DQPSK signal before encryption; (b) Encrypted signal for DQPSK; (c) Decrypted signal for DQPSK; (d) 16QAM signal before encryption; (e) Encrypted signal for 16QAM; (f) Decrypted signal for 16QAM.

constellations of the received electrical data signals without equalization for DQPSK and 16QAM at 40Gbaud, before and after encryption (BER=0.48) and after decryption respectively. The diagrams clearly prove that the DSP-based physical layer secure system can hide the data signal securely and then decrypt the data correctly. To investigate if the key's subcarrier modulation format has any impact on the security level, OFDM keys with modulation formats of 4QAM, 16QAM, 32QAM and 64QAM are separately employed in a system using the optimum parameters and a DQPSK, 40GBaud data signal. The corresponding BER vs. OSNR performances for a system without decryption is shown in Fig. 4. It can be clearly seen that the encrypted BER performances are virtually identical, and all meet the target BER of ≥~0.3.

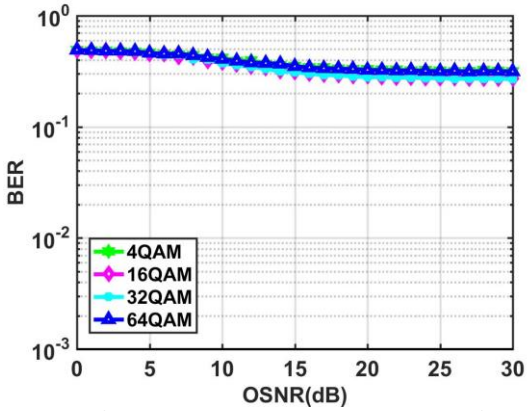

Fig. 4 BER performances with encryption element only for various key subcarrier modulation formats. All subcarriers use the same modulation as indicated in the legend.

In summary, the results obtained in this section indicate that for optimum security module design, i) optimum key bandwidth is dependent on and increases with the data signal baud rate, ii) higher order modulation and higher baud rates require lower dispersion values to achieve the same level of security and the dispersion of D1 should be larger than that of D2. Thus, to make the system transparent to multiple data signals the optimum module parameters should be selected based on the lowest order modulation and lowest baud rate to be encountered in practice.

B. Optimization of modulation index for phase modulators

The modulation index of the PMs will also have a direct impact on the level of data encryption as it influences the bandwidth of the PM modulated optical signals. To identify the optimum PM modulation index, use is made of the system employed in obtaining Fig. 2(a) and the previously identified optimum D1 and D2 parameters. The PM modulation index is varied to determine its impact on the level of encryption, by observing the receiver side BER vs. the received signals' optical signal to noise ratio (OSNR). To ensure the optimum modulation index is applicable to different transmitted data signals, a DQPSK data signal at 40Gbaud is adopted as it is the worst-case scenario, i.e., the signal has more robustness to signal distortions in comparison with other modulation formats and baud rates considered in this paper. The BER vs. OSNR performances for four different values of modulation index are presented in Fig. 5. The PM modulation index must clearly be ≥1.2 to make the physical layer optical secure system achieve

the desired security level of BERs ≥0.3. Therefore, the optimum modulation index for the PMs is identified as 1.2, because using a higher PM modulation index gives very minimal improvement and will also necessitate a higher gain for the linear broadband RF amplifier driving the PMs, which will incur higher cost.

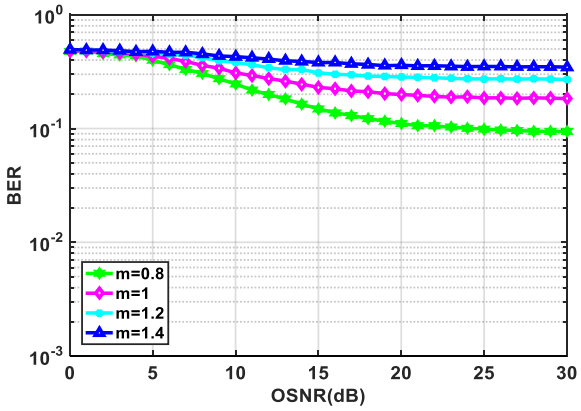

Fig. 5. BER performances with encryption element only for various modulation index values of the PM when transmitting DQPSK at 40Gbaud.

C. Robustness to an illegal decryption attempt using a single dispersive element

As an eavesdropper may attempt to illegally decrypt the signals by applying a single dispersive element at a point along the transmission fibre, this section evaluates the system's robustness to this eavesdropping approach. In the simulation, the encrypted signal is first transmitted over a 50km SSMF, and then passes through a dispersive element of -D2 and is finally coherently detected and demodulated. Firstly, we compare the BER vs. OSNR performances of signals after encryption, using the setup used in calculating Fig. 2(a), and for signals where one dispersive element of -D2 is applied to attempt illegal decryption, the applied dispersive element has a dispersion of -1800ps/nm (i.e., D2 and fibre dispersion are fully compensated). The results in Fig. 6 (a) show there is no difference between the BER vs. OSNR performances of these two setups for the cases of DQPSK at 40GBaud and 100GBaud, thus the system is robust to an eavesdropping attempt that compensates for the dispersion of D2 and the fibre. However, it should be considered that an eavesdropper might apply a tunable dispersive element to attempt decryption, therefore the robustness to an eavesdropping attack using a tunable dispersive element for -D2 is investigated. For the assessment, no optical noise is added as this is the best-case scenario for the eavesdropper. The results show that the BERs are all ~0.3 or above, as shown in Fig. 6 (b). It should be mentioned that lower order modulation and lower baud rate (bandwidth) is less sensitive to the encryption-induced distortion, so the BER performance when transmitting DQPSK at 40GBaud is lower than that for DQSPK at 100GBaud in Fig. 6(b). Thus, DQPSK at 40Gbaud is less robust, so this has been taken into account when selecting the system parameters in section III, so that a sufficient security level is achieved for all adopted signal types. These results confirm that signals after DSP-based physical layer encryption cannot be illegally decrypted by using a single dispersive element, thus the system is robust to this type of eavesdropping attack.

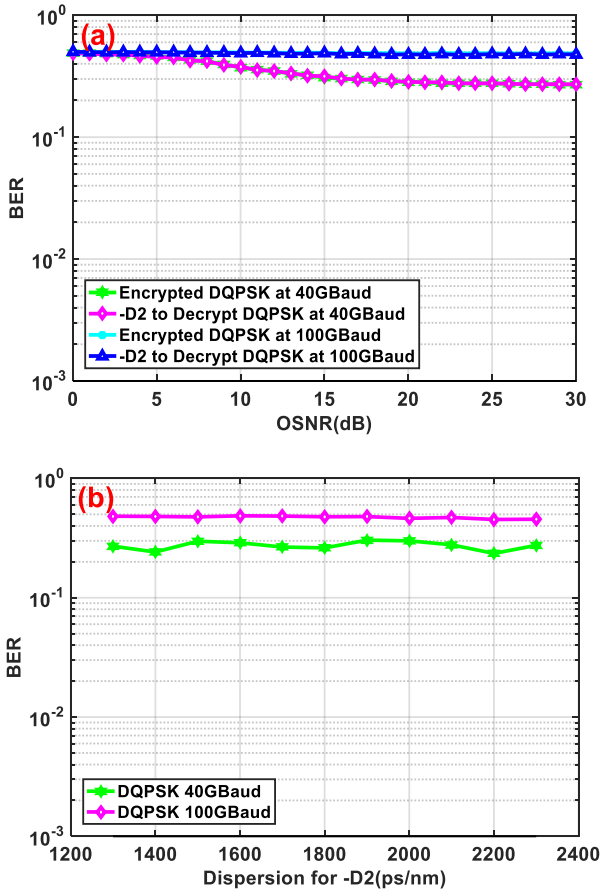

Fig. 6. (a) BER vs. OSNR performances for encryption element and decryption element with -D2 only which has compensated D2 and the fibre dispersion with different transmission baud rates; (b) Measured BER vs. OSNR for applying varying dispersion values for -D2 to do decryption without adding any optical noise.

IV. Analysis of Encryption and Decryption Induced BER Performance Penalty

The DSP-based physical layer secure system is designed to operate as a security system to be retrofitted in existing optical systems, and so should have minimal impact on the performance of the optical systems into which they are deployed. This section investigates the impact of the proposed physical layer secure method on the BER performances of typical coherent optical systems in order to assess any associated performance penalties. The performance penalty is determined by comparing BER vs. OSNR performances of the received data signals in the optical back-to-back (OBTB) system without encryption and decryption elements and in the 50km secure communication system adopting the previously identified optimum secure system parameters. The OBTB system is thus taken as the benchmark. For the secure communication system, the encryption and decryption elements are considered to be perfectly matched, and the dispersion of the transmission fibre is fully compensated by -D2. The results are presented in Fig. 7, where it is shown that the BER penalty

due to the encryption and decryption elements is effectively 0dB, thus the proposed physical layer security technique induces negligible penalty when the encryption and decryption elements are perfectly matched.

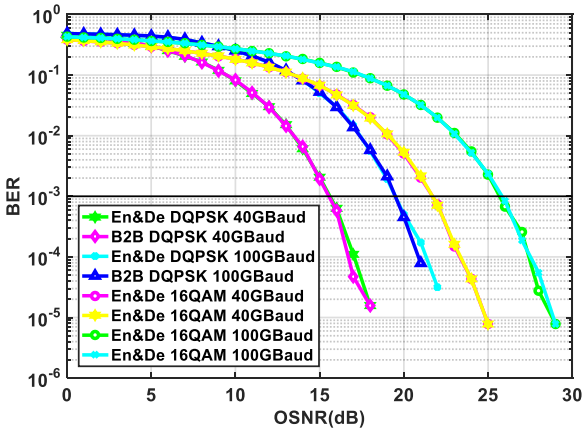

Fig. 7. BER performances of a 50km secure optical system and the optical back-to-back system without encryption and decryption elements for different modulation formats and signal transmission baud rates.

V. System Tolerance to Various Parameter Offsets between Encryption and Decryption Elements

Considering the practical implementation of optical communications systems, offsets in various parameter values between encryption and decryption elements are unavoidable, so it is critical to understand the tolerance of the proposed security technique to these offsets. The parameter offsets to be investigated, to observe their influence on data transmission performance, are: i) the time offset of the decryption security key relative to the ideal timing, ii) variation between D1(D2) and -D1 (-D2) dispersion values, iii) noise content in the encryption and decryption security keys, and iv) offset in the modulation index between the two PMs. This section pays attention to these mismatches between data encryption and decryption elements and investigate the maximum tolerances of the DSP-based physical layer secure systems to these offsets for achieving the BERs of 1×10^{-3}. The encryption part employs the previously identified optimum parameter set for D1, D2, key bandwidth and modulation index for the PM, with the aforementioned offsets applied to the decryption element, simulations are undertaken using the system shown in Fig. 1. Optical noise loading at the receiver before coherent detection is not considered here as it may mask the observed performance degradation trends due to the offsets.

A. Tolerance to offset in security key timing in decryption element

To check the influence of time offset in the security key on the BER performances, a time offset, relative to the ideal timing, is added to the security key feeding the PM in the decryption side. The time offset unit interval is defined as 3.125ps. DQPSK signals are transmitted with baud rates of 40 and 100GBaud through the secure system, the corresponding BER values for different time offsets are shown in Fig. 8(a). Transmitted signals with a higher baud rate are shown to be slightly more sensitive to the time offset in the security key, this is because signals with higher baud rates have wider bandwidths and the associated higher frequency components are more sensitive to the timing offset induced phase distortions. A DQPSK signal at 40Gbaud can tolerate ±4 offset intervals, while at 100Gbaud it can tolerate $< \pm4$ offset intervals. Moreover, as the bandwidth of the security keys and the modulation index of the PMs can potentially impact the system's sensitivity to security key time offset, these two parameters are varied to see their associated impacts on timing offset sensitivity.

As shown in Fig. 8(b) and (c), when transmitting DQPSK with 100Gbaud, the secure optical system with higher security key bandwidth and higher modulation index is more sensitive to the time offset. The underlying physical mechanisms causing these effects can be easily explained: a security key signal with a wider bandwidth suffers a larger change in amplitude for a given timing offset, and a higher modulation index corresponds to a larger absolute signal amplitude, so a larger amplitude signal sees a larger change in amplitude (i.e., a larger decryption phase error) for a given timing offset. Thus, as a larger key amplitude error corresponds to a larger decryption phase error, these effects result in higher sensitivity to timing offset. Based on the above analysis, a key synchronization technique is required to maintain accurate key timing at the decryption unit. The technique should ideally avoid an additional dedicated synchronization wavelength to minimize cost, possible approaches are, embedded synchronization signals within the key and/or timing feedback loops based on received signal characteristics such as peak power, correlation peaks or BER

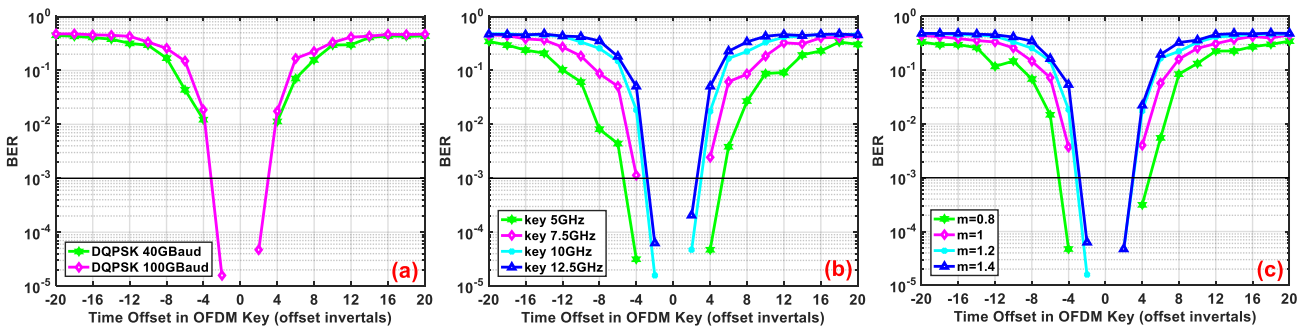

Fig. 8. (a) Measured BER vs. time offset in decryption key when transmitting DQPSK signals with different baud rates; (b) The influence of decryption key time offset and bandwidth on BER performance when m=1.2 and transmitting DQPSK at 100Gbaud; (c) The influence of PM's modulation index on BER performance when key bandwidths equal to 10GHz and transmitting DQPSK signals at 100Gbaud.

minimization.

Based on Fig. 8(a-c), the tolerance for DQPSK at 100GBaud, with m=1.2 and security key bandwidth=10GHz is approximately ±3 offset intervals. It is shown that reducing the sensitivity to timing offset can be achieved by choosing lower security key bandwidth and/or lower modulation index for the PMs. However, these parameters also have an impact on security level as determined in section III, so there is a trade-off between the tolerance to secure key time offsets and the level of security.

B. Impact of offsets in -D1 and -D2 dispersion values and impact of modulation index on sensitivity to -D1 and -D2 offsets

With the values of D1 and D2 in the encryption side and the bandwidth of the security keys set to the previously determined optimum values, dispersion offsets are separately added to -D1 and -D2 in the decryption side, to observe the impact on system BER performances for the secure system illustrated in in Fig. 1. As shown in Fig. 9(a), for an offset in -D1, DQPSK with 40Gbaud (100Gbaud) can tolerate $> \pm 1500$ ps/nm (± 1000ps/nm). Transmitted signals with a lower baud rate can thus tolerate more offset, this can be explained by the fact that signals with lower baud rates (i.e., longer symbol periods) have stronger tolerances to the dispersion induced ISI effect. To determine if the PM modulation index impacts the sensitivity to offset in -D1, the BER versus -D1 dispersion offset for DQPSK at 100Gbaud is plotted in Fig. 9(b), for different values of modulation index in both PMs. Fig. 9(b) shows that the PM modulation index variations have negligible impact on the system's sensitivity to dispersion offset in -D1 when transmitting DQPSK at 100GBaud. This is because the modulation index of PM only influences the amplitude of the phase changes from the security key, which are then completely removed in the decryption side. The received signal after decryption is thus only affected by the dispersion offset between D1 and -D1, which is subsequently compensated by the LMS equalizer in the coherent receiver.

Fig. 9(c) and (d) show the corresponding results for an offset in -D2. For a modulation index of 1.2, DQPSK with 40Gbaud and 100Gbaud can tolerate approximately ± 120 ps/nm and ± 30ps/nm respectively. The signals with higher baud rates are again more sensitive to the dispersion offsets between D2 and -D2, as they are more susceptible to the dispersion induced ISI effects. In contrast to the dispersion offset in -D1, when transmitting DQPSK with 100Gbaud, the modulation index variations of the PMs have an influence on the system's sensitivity to dispersion offset in -D2. A higher PM modulation index makes the system slightly more sensitive to the dispersion offset in -D2, as shown in Fig. 9(d). The secure system can tolerant less than about ± 30 ps/nm for DQPSK with 100Gbaud when the PM modulation index is 1.2. The offset tolerance range is increased when the PM modulation index is reduced. This can be explained by the fact that the larger the -D2 offset the larger the dispersion offset-induced signal distortions, which makes it harder to correct the PM induced phase changes. Thus, the smaller phase changes, associated with a lower PM modulation index, are able to tolerate the residual distortions better, and so allow a larger -D2 offset range. However, reducing the PM modulation index does not give a significant reduction in the -D2 dispersion offset range, and for practical applications, low PM modulation indexes are not desirable because of the associated reduction in the system security level. The physical mechanisms behind the high sensitivity of the proposed technique to the dispersion offset in -D2 is that the dispersion offsets in -D2 cannot be effectively removed by the PM and -D1 in the decryption element.

These results indicate the level of manufacturing tolerances required for the D2 and -D2 dispersive elements, alternatively a tunable dispersive element could be used in practice for D2 or -D2, in order to achieve the required low dispersion offset.

C. Impact of noise in the security keys

In practical applications, the encryption and decryption OFDM security keys, although identical in the digital domain, are produced using different analogue hardware, thus the produced encryption and decryption keys have different noise content but can have similar signal-to-noise ratio (SNR) values. In this section, to represent the practical generation of security keys, independent additive white Gaussian noise (AWGN) is added to each of the electrical analogue security keys feeding the PMs in the encryption and decryption sides, thus the required security key fidelity is determined in order to minimize the impact on the BER performance of the secure system. In the investigations, the same SNR is adopted for the two keys, however the noise signals are independent. The system BER vs. SNR of the keys is shown in Fig. 10, for different modulation formats and baud rates. The results show that the secure optical system requires SNRs of the security keys to be >18dB to achieve a BER of >1E-3 in all cases. In practice, OFDM signals can be easily generated with SNRs > 25dB. Furthermore,

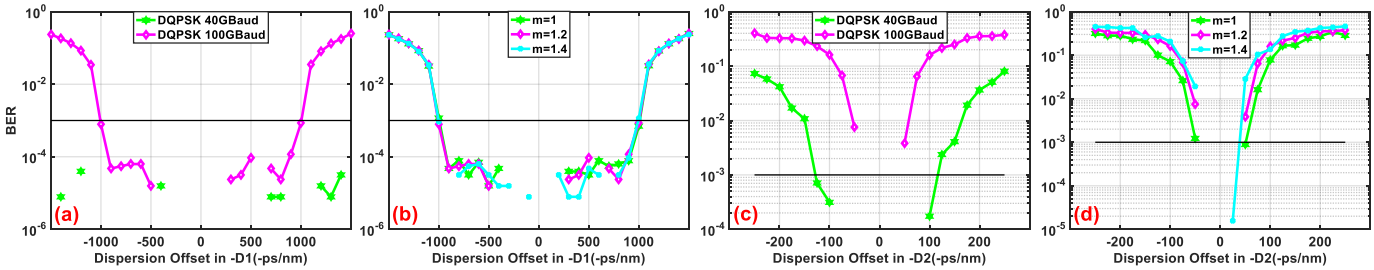

Fig. 9. (a) The influence of dispersion offset in -D1 (relative to optimum value) on BER when transmitting DQPSK signals with different baud rates; (b) The influence of dispersion offset in -D1 on BER with different PM modulation index when transmitting DQPSK signals with 100Gbaud; (c) The influence of dispersion offset in -D2 (relative to optimum value) on BER when transmitting DQPSK signals with different baud rates; (d) The influence of dispersion offset in -D2 on BER with different PM modulation indexes when transmitting DQPSK signals with 100Gbaud.

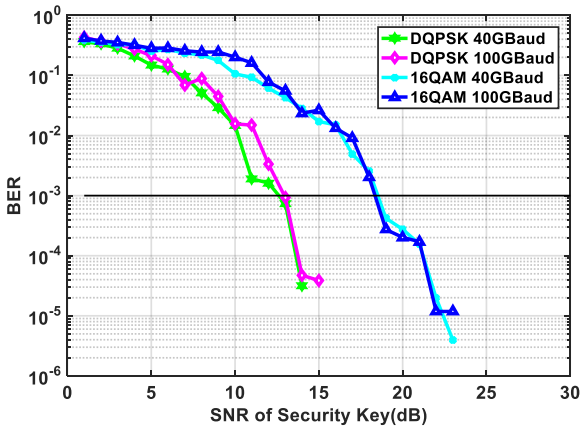

Fig. 10. The influence of noises in security keys on BER performances when message signals are with different modulation formats and transmission baud rates.

transmitted signals using low order modulation formats can tolerate more key noise than signals using high order modulation formats of the same baud rates. This is because signals with low order modulation formats have relatively strong tolerances to the phase noise caused by the security key noise. It is also observed here that baud rate has very minimal influence on BER performances. This can be attributed to the fact that, when considering one symbol, the data signal's power spectral density (PSD) and its noise PSD (induced by the key noise) both vary in proportion to the symbol period. Thus, changing the symbol period (baud rate) will not change the data signal's key noise related SNR, and so there is no significant impact on BER performance.

Based on the results, the DSP-based secure optical system does not have particularly challenging requirements for noise content in the security keys as practically achievable key SNR levels have minimal impact on data signal BER performance.

D. Modulation index offset in PMs

To evaluate the influence of offsets in the modulation index of the PMs in the encryption and decryption side, for simplicity, the modulation index of the encryption PM is fixed at the optimum value, while the modulation index of the decryption PM is varied. The variations in BER performances of the secure optical system for different modulation formats and baud rates are observed. Fig. 11 shows that transmitted signals coded with DQPSK (16-QAM) can tolerate a PM modulation index offset of approximately ±33% (±16%). A higher modulation index offset introduces more phase errors and as described above, signals with high order modulation formats are relatively more sensitive to the phase error. The baud rates of the transmitted signals have very minimal influence on the sensitivity to the PM modulation index offsets, this is again due to the aforementioned reasons for the minimal influence of baud rate observed in Fig. 11. Thus, the DSP-based secure optical system can tolerate relatively large offsets in the modulation index of the PMs.

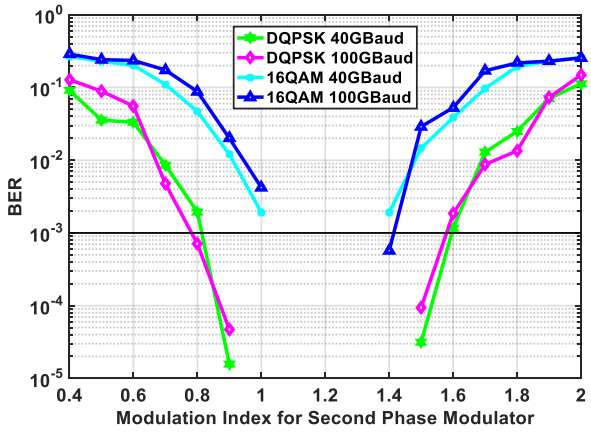

Fig. 11. The influence of modulation index offset between encryption and decryption PMs on BER performance when the data signals have different modulation format and baud rates.

E. Performance with combined encryption and decryption parameter offsets

After discussing the influences of each individual parameter's offset on the secure system's performances, it is essential to consider the case where all parameter offsets exist at the same time to evaluate the overall system performances in a practical application scenario. Here the encryption side employs the identified optimum values of dispersion D1 and D2, bandwidth of the security keys and PM modulation index, while the decryption element is implemented with various decryption parameter offsets separately and in combination. Decryption parameter offsets considered include dispersion offset in -D1 and -D2, noise added to the keys, modulation index offset in the decryption PM and time offset in the decryption key.

Based on the observed maximum individual offsets and the corresponding system sensitivities, an example combination of practical decryption parameter offsets is given in Table. II. Fig.

TABLE II
PARAMETER SETTINGS AND OFFSET SETTINGS

Parameter	Encryption	Decryption	Offset
D1	2000ps/nm	2100ps/nm	100ps/nm (5%)
D2	1000ps/nm	1015ps/nm	15ps/nm (1.5%)
Noise in key (SNR)	20dB	20dB	
Modulation index offset	1.2	1.26	0.06 (5%)
Time offset		2 offset intervals	6.25ps

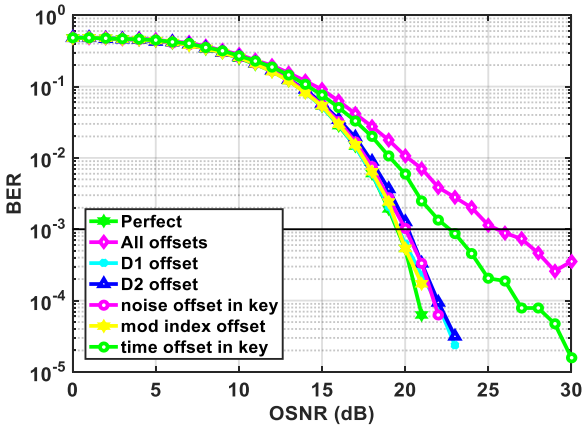

Fig.12 The influence of adding different offsets in system separately and together on BER performances for DQPSK with 100Gbaud.

12 shows the BER vs. OSNR curves for the ideal case (no decryption parameter offsets) and for the individual and combined offset cases using the values in Table II. When all the decryption parameter offsets occur, there is a 5dB OSNR penalty compared to the ideal case. Therefore, it is easy to understand that if encryption and decryption parameter offsets are maintained within the levels suggested in Table II, the DSP-based physical layer secure communication system has a practical OSNR penalty.

VI. Analysis of System Performances for Different Transmission Distances

For differnet application scenarios, the fiber transmission distances are variable, and thus it is essential to investigate the transmission performances of the proposed secure optical communication systems for different transmission distances. To further explore the encyption and decrytion elements' impacts on system transmission performances, transmission performance comparisons between the proposed secure systems and conventional coherent transmission systems are also of great importance. The identified optimum values for the encryption and decryption elements are employed with no parameter offsets. Furthermore, an Erbium doped fibre amplifier (EDFA) (gain: 16dB; noise figure: 4 dB) is inserted after every 80km fibre span. For the proposed secure systems, as the fibre length is varied, -D2 in the decryption element is adaptively adjusted to compensate for the fibre dispersions for all fiber spans in addition to D2. The received optical power and LO power are as defined in Table I. For fair comparisons, the coherent optical systems without security, employ suitable DCF to reduce fiber dispersion-induced signal distortions. The BER vs. distance performances of signals with different modulation formats and baud rates are shown in Fig. 13. It can be observed that the sercure optical system has similar transmisison performances to the conventional coherent system without incorporting the proposed secure techniques [26], [27]. For the case of transmitting 16QAM with 100Gbaud (40GBaud), i.e. 400Gb/s (160Gb/s), the proposed secure system can operate at up to 250 km (650km) transmission distances and still achieves

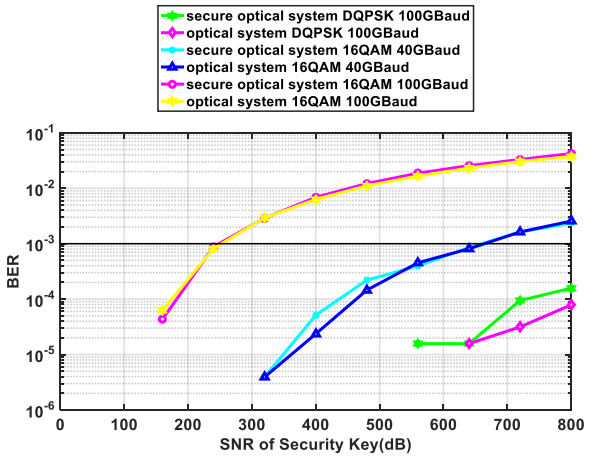

Fig. 13. Transmission performances of the proposed secure optical system and conventional coherent optical system (without security) for different fibre transmission distances.

BERs≤1E-3. This demonstrates that the DSP-based physical layer secure optical communicaiton system can have great potential for supporting long-haul applications.

VII. Conclusions

A novel and cost-effective DSP-based physical layer security technique for coherent optical communications has been proposed, where noise-like OFDM signals are utilized as highly effective private security keys to significantly enhance the security levels.

Detailed and comprehensive simulations have been undertaken to: i) identify the optimum parameters for the encryption and decryption elements to achieve a high level of security, ii) explore, by using the identified optimum encryption and decryption parameters, the performances of the proposed physical layer secure communication system. The results show that when the encryption and decryption elements' parameters are matched, the proposed secure systems can deliver similar performances to the convention coherent transmission systems, and iii) investigate the proposed secure system's sensitivity to various encryption/decryption parameter offsets and security key's SNRs. It is shown that the proposed secure systems are relatively more sensitive to the key timing offset and D2/-D2 offsets in comparison with other encryption and decryption parameter offsets, thus providing critical information relating to practical implementation aspects.

It is also shown that the proposed encryption and decryption techniques can introduce an acceptable performance penalty to an existing coherent communication system if the encryption and decryption parameter offsets are kept within specified tolerances. More importantly, the proposed secure optical communication systems are shown to introduce no limitations on transmission distances for different scenarios when negligible encryption and decryption parameter offsets exist. The proposed DSP-based physical layer security technique provides a promising solution for achieving low cost and highly effective network security in coherent optical networks.

References

[1] M. P. Fok, Z. Wang, Y. Deng, and P. R. Prucnal, "Optical Layer Security in Fiber-Optic Networks," *IEEE Trans. Inf. Forensics Secur.*, vol. 6, no. 3, pp. 725–736, Sep. 2011.

[2] H. S. Brar and G. Kumar, "Cybercrimes: A Proposed Taxonomy and Challenges," *J. Comput. Netw. Commun.*, vol. 2018, pp. 1–11, 2018.

[3] V. Mazzone, A. D. Falco, A. Cruz, and A. Fratalocchi, "Photonics based perfect secrecy cryptography: Toward fully classical implementations," *Appl. Phys. Lett.*, vol. 116, no. 26, p. 260502, Jun. 2020.

[4] W. Bernard B. and N. Evgenii E., "A method for secure communications over a public fiber-optical network," *Opt. Express*, vol. 14, no. 9, p. 3738, 2006.

[5] X. Wang, Z. Gao, B. Dai, and G. Buller, "40 Gb/s Secure Optical Communication System Based on Optical Code Technology," in *2018 20th International Conference on Transparent Optical Networks (ICTON)*, Bucharest, Jul. 2018, pp. 1–4.

[6] Z. Jiang, D. E. Leaird, and A. M. Weiner, "Experimental Investigation of Security Issues in O-CDMA," *J. Light. Technol.*, vol. 24, no. 11, pp. 4228–4234, Nov. 2006.

[7] E. Diamanti, H.-K. Lo, B. Qi, and Z. Yuan, "Practical challenges in quantum key distribution," *Npj Quantum Inf.*, vol. 2, no. 1, p. 16025, Nov. 2016.

[8] C. Fabio, P. Enrico, P. Luca, M. Imran, and C. Tommaso, "Secure Quantum Communication Technologies and Systems: From Labs to Markets," *Quantum Rep.*, vol. 2, no. 1, pp. 80–106, Jan. 2020.

[9] F. Xu, M. Curty, B. Qi, and H.-K. Lo, "Measurement-device-independent quantum cryptography," *IEEE J. Sel. Top. Quantum Electron.*, vol. 21, no. 3, pp. 148–158, May 2015.
[10] M. Sciamanna and K. A. Shore, "Physics and applications of laser diode chaos," *Nat. Photonics*, vol. 9, no. 3, pp. 151–162, Mar. 2015.
[11] Y. Huang, P. Zhou, and N. Li, "High-speed secure key distribution based on chaos synchronization in optically pumped QD spin-polarized VCSELs," *Opt. Express*, vol. 29, no. 13, p. 19675, Jun. 2021.
[12] N. Jiang, A. Zhao, S. Liu, C. Xue, and K. Qiu, "Chaos synchronization and communication in closed-loop semiconductor lasers subject to common chaotic phase-modulated feedback," *Opt. Express*, vol. 26, no. 25, pp. 32404–32416, Dec. 2018.
[13] A. Apostolos *et al.*, "Chaos-based communications at high bit rates using commercial fibre-optic links," *Nature*, vol. 438, no. 7066, pp. 343–346, Nov. 2005.
[14] Z. Yang, J. Ke, Q. Zhuge, W. Hu, and L. Yi, "Coherent chaotic optical communication of 30 Gb/s over 340-km fiber transmission via deep learning," *Opt. Lett.*, vol. 47, no. 11, p. 2650, Jun. 2022.
[15] L. Jiang *et al.*, "Chaotic optical communications at 56 Gbit/s over 100-km fiber transmission based on a chaos generation model driven by long short-term memory networks," *Opt. Lett.*, vol. 47, no. 10, p. 2382, May 2022.
[16] R. Lavrov, M. Jacquot, and L. Larger, "Nonlocal Nonlinear Electro-Optic Phase Dynamics Demonstrating 10 Gb/s Chaos Communications," *IEEE J. Quantum Electron.*, vol. 46, no. 10, pp. 1430–1435, Oct. 2010.
[17] X. Huang, L. Zhang, W. Hu, J. P. Turkiewicz, E. Leitgeb, and X. Yang, "Secure OFDM-PON Using Chaotic Constellation Mapping and Probabilistic Shaping," *IEEE Photonics Technol. Lett.*, vol. 33, no. 20, pp. 1139–1142, Oct. 2021.
[18] C. Zhang, W. Zhang, C. Chen, X. He, and K. Qiu, "Physical-Enhanced Secure Strategy for OFDMA-PON Using Chaos and Deoxyribonucleic Acid Encoding," *J. Light. Technol.*, vol. 36, no. 9, pp. 1706–1712, May 2018.
[19] C. Xue *et al.*, "Security-enhanced chaos communication with time-delay signature suppression and phase encryption," *Opt. Lett.*, vol. 41, no. 16, p. 3690, Aug. 2016.
[20] N. Jiang, A. Zhao, Y. Wang, S. Liu, J. Tang, and K. Qiu, "Security-enhanced chaotic communications with optical temporal encryption based on phase modulation and phase-to-intensity conversion," *OSA Contin.*, vol. 2, no. 12, p. 3422, Dec. 2019.
[21] N. Jiang, A. Zhao, C. Xue, J. Tang, and K. Qiu, "Physical secure optical communication based on private chaotic spectral phase encryption/decryption," *Opt. Lett.*, vol. 44, no. 7, p. 1536, Apr. 2019.
[22] Z. Gao *et al.*, "25 Gb/s Physical Secure Communication Based on Temporal Spreading-Then-Random Phase Encryption," *IEEE Photonics Technol. Lett.*, vol. 33, no. 24, pp. 1363–1366, Dec. 2021.
[23] M. Iqbal, L. Velasco, N. Costa, N. A., J. Pedro, and M. Ruiz, "LPsec: a fast and secure cryptographic system for optical connections," *J. Opt. Commun. Netw.*, vol. 14, no. 4, p. 278, Apr. 2022.
[24] X. Liang, C. Zhang, Y. Luo, M. Cui, and K. Qiu, "Secure key distribution and synchronization method in an OFDM-PON based on chaos," *Opt. Express*, vol. 30, no. 11, p. 18310, May 2022.
[25] Z. Zhang, Y. Luo, C. Zhang, X. Liang, M. Cui, and K. Qiu, "Constellation Shaping Chaotic Encryption Scheme With Controllable Statistical Distribution for OFDM-PON," *J. Light. Technol.*, vol. 40, no. 1, pp. 14–23, Jan. 2022.
[26] P. Jindal and B. Singh, "RC4 Encryption-A Literature Survey," in *Procedia Computer Science*, 2015, vol. 46, pp. 697–705.
[27] K. Kazuro, "Analyses of wavelength- and polarization-division multiplexed transmission characteristics of optical quadrature-amplitude-modulation signals," *Opt. Express*, vol. 19, no. 19, p. 17985, Sep. 2011.
[28] J. Lin, H. Sepehrian, L. A. Rusch, and W. Shi, "Single-carrier 72 GBaud 32QAM and 84 GBaud 16QAM transmission using a SiP IQ modulator with joint digital-optical pre-compensation," *Opt. Express*, vol. 27, no. 4, p. 5610, Feb. 2019.