Khalil et al. *EPJ Quantum Technology* (2024) 11:49
https://doi.org/10.1140/epjqt/s40507-024-00260-y

EPJ Quantum Technology
a SpringerOpen Journal

RESEARCH Open Access

Experimental demonstration of quantum encryption in phase space with displacement operator in coherent optical communications

Mostafa Khalil[1*], Adrian Chan[2], David V. Plant[1*], Lawrence R. Chen[1*] and Randy Kuang[3*]

*Correspondence:
mostafa.khalil2@mail.mcgill.ca;
david.plant@mcgill.ca;
lawrence.chen@mcgill.ca;
randy.kuang@quantropi.com
[1]Department of Electrical and Computer Engineering, McGill University, Montreal, QC, Canada
[3]Quantropi Inc., Ottawa, ON, Canada
Full list of author information is available at the end of the article

Abstract

We provide experimental validation of quantum encryption in phase space using displacement operators in coherent states (DOCS) in a conventional coherent optical communication system. The proposed encryption technique is based on displacing the information symbols in the phase space using random phases and amplitudes to achieve encryption randomly and provide security at the physical layer. We also introduce a dual polarization encryption approach where we use two different and random DOCS to encrypt the X and Y polarizations separately. The experimental results show that only authorized users can decrypt the signal correctly, and any mismatch in the displacement operator coefficients, amplitudes, or phases will lead to a bit error ratio (BER) of approximately 50%. We also compare the performance of the system with and without encryption over 80 km of standard-single mode fiber (SSMF) transmission to assess the added penalty of such encryption. The achieved net bit rates are 224, 448, and 560 Gb/s for QPSK, 16QAM, and 32QAM modulation formats, respectively. The experimental results showcase the efficacy of the DOCS encryption technique in resisting various decryption attempts, demonstrating its effectiveness in ensuring the security and confidentiality of transmitted data in a real-world transmission scenario.

Keywords: Displacement operator; Encryption in phase space; Coherent optical communications; Key distribution; Data confidentiality

1 Introduction

To satisfy the increasing demand for data confidentiality and authenticity, it is important to ensure that communications are being properly secured. Since optical communication links have evolved from conventional applications in telecommunications to become the preferred infrastructure for transmitting substantial amounts of information, extensive research has been investigated to improve the optical networks' performance. These improvements include spectral efficiency, data rate, and DSP speed [1, 2]. In long-haul optical fiber transmission, eavesdropping attacks are more likely to occur, wherein an eavesdropper can steal optical signals by tapping into the physical transmission links [3–5]. Various encryption techniques have been proposed and investigated to enhance the secrecy of in-

formation in fiber networks including QKD [6], optical chaos-based communication [7], optical steganography [8, 9], and XOR encryption [10, 11].

QKD can be achieved by encrypting the key information in the quantum states of a single photon, this is now known as the BB84 protocol [12]. QKD has the advantage of indicating whether an eavesdropper is trying to get the key information or not. However, QKD requires specialized infrastructure, including a single photon transmitter, detector, and quantum communication channels. QKD also has limited communication distance and low data rates [13].

Optical chaos-based communication can be seen as a jamming signal over an information signal. On the transmitter side, the information signal is coupled into a fiber loop and amplified by an EDFA, while on the receiver side, the chaotic signal is split and one of the taps goes through an open loop to regenerate the chaos, and the other tap is launched into a photodetector. To decrypt the signal correctly, the EDFA on the receiver side must match with the one on the transmitter side [14–16]. The chaotic signals generated by such systems are not truly random, which can make them more susceptible to eavesdropping attacks by adversaries who can predict the behavior of the system.

Optical steganography is based on hiding the information signal in public channels, preventing eavesdroppers from detecting the stealth signal [8, 17]. One of the optical steganography techniques is done by using a temporal phase mask to encode the information signal by spreading the signal through CD, and only the right dispersion compensation receiver can decode the stealth signal correctly. However, data rates beyond 10 Gb/s remain a challenge in optical steganography [18].

Optical XOR gates have been recently investigated due to their high-speed encryption and electromagnetic wave immunity. However, the implementation of XOR gates requires special infrastructure and is limited in terms of transmission distance [11, 19].

In [20], Kuang and Bettenburg proposed a novel QKD-inspired approach using randomized Glauber states based on a round-trip mechanism for coherent optical communications. The roundtrip mechanism prevents sharing the secret key with any other entities. First, a user, Bob, creates a Glauber state as a quantum public key envelope by randomly modulating a secret phase that is known only to him and transmits the signal to another user, Alice, who modulates the information signal with no knowledge about the signal that Bob sent. Alice then transmits the signal back to Bob who is now able to use his secret key to read Alice's information signal. In [21–24], we have demonstrated extensive theoretical analysis of the latter approach through simulation using commercial software, Optisystem, and MATLAB, and in [25, 26], we experimentally validate our simulation results. In [27], we proposed a new encryption approach that is based on displacement operators in coherent optical communications and demonstrated theoretical proofs and preliminary simulation results. The DOCS is a generalized form of EPS [27]. Briefly, the EPS technique is based on creating a series of random phases that act like an envelope for the information signal and change its phases randomly. Only authorized users with the same random phase series can remove the envelope and detect the information signal. The generation of the encryption key can be done in the physical layer by employing a phase modulator before or after data modulation, and it can also be done in DSP for coherent optical communications. On the receiver side, the physical layer decryption can be done either by employing another phase modulator to reverse the phases by sharing the same series of random phases as a secret key, or in the DSP for a less complex system. The DOCS en-

cryption approach creates a series of random phases with random amplitudes to encrypt the signal, making optical fiber links more secure against eavesdropping attacks.

Previously, we demonstrated simulation results of the security analysis of the proposed technique in [27]. In this paper, we experimentally validate the DOCS encryption approach in coherent optical communication systems over 80 km of SSMF. Employing the DOCS encryption approach, we achieve net data rates of 224, 448, and 560 Gb/s using dual-polarization QPSK, 16-QAM, and 32 QAM, respectively, and the measured BERs are below the FEC levels. We also investigate the challenges in coherent transmissions against eavesdropping attacks. Taken together, the experimental results indicate that the DOCS encryption technique has the potential to achieve a high level of physical layer security with acceptable performance at such high data rates and enhance data confidentiality in existing coherent optical communication systems. Compared to AES and RSA which have significant computational overhead due to the complexity of their algorithms [28], the computational overhead of the DOCS encryption relies mainly on the synchronization process for decryption. The throughput of the DOCS encryption is very high, as it does not significantly impact the data transmission rates. AES offers relatively high throughput but is still lower than DOCS due to its computational nature, and RSA has the lowest throughput among the three. One of the disadvantages of the DOCS encryption in practical deployment is that the codeword still needs to be shared with other parties for decryption.

2 Operating principles

An example of a geometric representation based on the DOCS encryption technique for coherent optical transmission is shown in Fig. 1. Assume we have typical QPSK modulation format symbols defined in the phase space as illustrated in red dots. After applying the displacement operator, $\hat{D}(\alpha)$, the symbols are displaced to another location in the phase space as illustrated in blue dots. In general, the $\hat{D}(\alpha)$ displaces any input state $|\alpha\rangle$ to any other state $|\beta\rangle$ in the phase space [29]. A phase shift operator $\hat{D}(\alpha = |\beta|e^{j\varphi})$ is a special case of a displacement operator, where symbols are displaced with a fixed amplitude and random phases in the phase space. In [27], we proved that the displacement operator is a unitary reversible operator. Therefore, applying the displacement operator to a coherent state, and then applying the inverse of the displacement operator returns the coherent

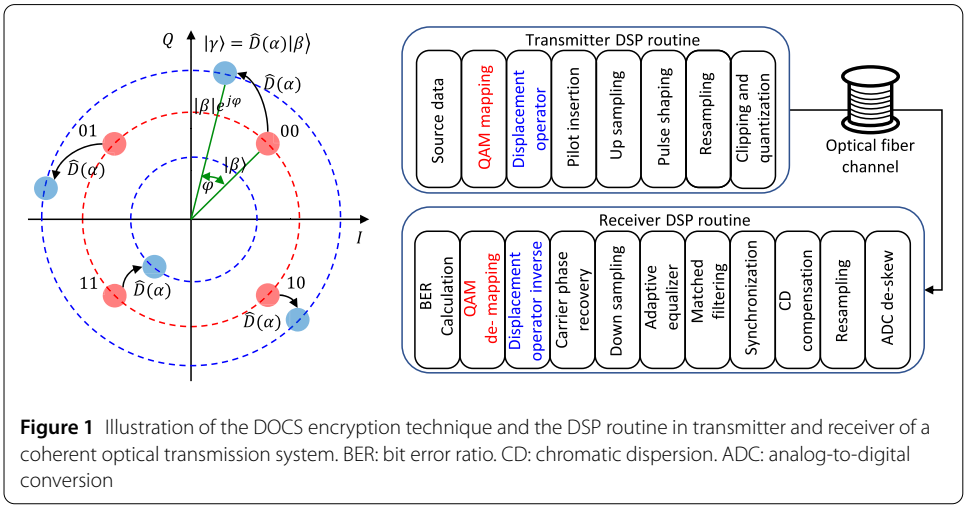

Figure 1 Illustration of the DOCS encryption technique and the DSP routine in transmitter and receiver of a coherent optical transmission system. BER: bit error ratio. CD: chromatic dispersion. ADC: analog-to-digital conversion

state to its original geometry in phase space. The displacements applied to the information symbols can be completely random in phase space, namely, phases are not just restricted to 0 and π, nor amplitudes are restricted to certain values. Therefore, the number of possible random displacement masks can be vast. For example, if the phase mask has $N = 30$ values, and the phase shifts $\varphi = \pi \times m$, where $m \in (0, 1, 2, \ldots, 6)$, then there are 7^{30} possibilities in the random phase mask. The same formula can be used to determine the possibilities in the amplitude variation mask. The total number of possibilities is the summation of the phase and amplitude masks.

The displacement operator in a coherent state can be expressed as follows:

$$\hat{D}(t) = \left|\beta(t)\right| e^{j(\varphi(t)+\delta\varphi)} \tag{1}$$

where $\beta(t)$ and $\varphi(t)$ are the amplitude variation and the phase deviation applied to the information signal, respectively, and $\delta\varphi$ is an initial random phase of the displacement operator. Let us assume an information signal, $s(t)$, then, the encrypted information signal can be expressed as follows:

$$s(t)_{En} = s(t) \otimes \left|\beta(t)\right| e^{j(\varphi(t)+\delta\varphi)} \hat{e} \tag{2}$$

where, $\hat{e}$ is the polarization unit vector. The information signal, $s(t)$, can be modulated using any modulation format. In our demonstration, we focus on QPSK and QAM modulation formats. After transmitting the encrypted signal over optical fiber, and assuming the impulse response of the fiber channel is $f(t)_{\text{fiber}}$, the received signal can be expressed as follows:

$$s(t)_{Rx} = s(t)_{En} \otimes f(t)_{\text{fiber}} \tag{3}$$

To decrypt the signal, we apply the inverse of the displacement operator to the received signal as follows:

$$s(t)_{De} = \left\{ s(t)_{Rx} \otimes \left|\beta'(t)\right| e^{-j(\varphi(t)+\delta\varphi)} \right\} \otimes f'(t)_{\text{fiber}} \tag{4}$$

where $f'(t)_{\text{fiber}}$ is the CD compensation element corresponding to the fiber channel. The amplitude variation codeword, $\beta(t)$, should be chosen carefully to satisfy the power constraint of the system. Symbols with a high PAPR introduce a larger nonlinear phenomenon and limit the system's performance [30]. The DAC and ADC operate with a finite ENoB, which adds quantization noise to the information signal [31]. The phase deviation codeword, $\varphi(t)$, can be chosen randomly as we mentioned earlier. We emphasize this point because such encryption is novel and represents one of our main contributions. In general, high-order modulation formats tend to have a lower tolerance to noise due to the reduction in the Euclidean distance between constellation points. In higher-order modulation formats, more bits are transmitted per symbol, resulting in a denser constellation diagram. Thus, the DOCS encryption technique affects higher-order modulation formats than lower-order ones.

The baseline DSP flow is also shown in Fig. 1. On the transmitter side, the data source is obtained by generating a PRBS, which is then mapped into QAM symbols. Then, the gen-

erated symbols are processed by the displacement operator encryption scheme. Pilot symbols are appended to the symbols for synchronization. The encrypted symbol sequence is up-sampled to 2 SPS, shaped by a RRC pulse filter, and resampled to match the DAC sampling rate. On the receiver side, a series of signal processing techniques are applied to ensure accurate reception of the signal before decryption. These techniques include ADC de-skew, resampling, CD compensation, synchronization, matched filtering, adaptive equalization, down-sampling to 1 SPS, and carrier phase recovery which is based on the BPS algorithm [32]. Then, the inverse of the displacement operator is applied to decrypt the signal, and symbols are de-mapped into QAM symbols and then bits for BER calculations.

3 Experimental results and discussion

The experimental setup of a secure coherent optical transmission system using the DOCS encryption technique is shown in Fig. 2. The transmitter side comprises a μITLA, a DAC, a dual-polarization DP-IQM, and an EDFA. The μITLA generates light at a wavelength of 1550 nm, and the DP-IQM modulates the optical signal with the encrypted mapped and pre-emphasized data sequence. Both polarizations are encrypted using the same displacement operator. The sampling rate of the DAC and ADC is the same and approximately 70 GSa/s with 8-bit resolution. The DP-IQM has 4 channels representing IQ and dual polarization status and are organized in order as XI, XQ, YI, and YQ, respectively. Then, the optical signal is amplified with an EDFA before it is launched into the 80-km of SSMF. On the receiver side, a typical coherent detection system is used. A μITLA is used as a LO and mixed with the encrypted signal through a 90^o optical hybrid. The beating signal is detected by BPDs, and the electrical signal is captured for signal processing. The transmitter and receiver DSP steps to employ the DOCS encryption and decryption technique are illustrated in Fig. 1. We conducted our experiment using a commercial coherent transceiver modem. The integrated laser within the coherent transceiver modem boasts a linewidth below 100 kHz, which indicates low phase noise, thereby ensuring high coherence and stability in our optical signal. The coherent transciever modem can operate stably over a range of operating conditions. The experiments were conducted in a lab, and the devices were in a quasi-stable environment (temperature fluctuations and vibrations are slow varying). As we repeated the experiments multiple times on different dates, we

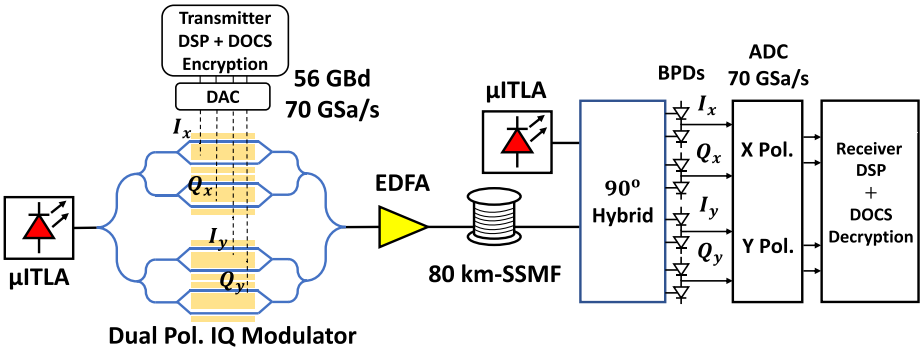

Figure 2 The experimental setup of the DOCS encryption technique in a typical coherent optical transmission. μITLA: micro-integrable tunable laser assembly. EDFA: erbium-doped fiber amplifier. BPDs: balanced photodetectors

obtained very similar performance when reproducing the experiments so that these slow fluctuations did not seem to have an impact. The receiver sensitivity could detect signals below −30 dBm.

To assess the performance of the DOCS encryption technique, first, spectra, and histograms are calculated at the transmitter side with and without the DOCS encryption technique. Then, BER analyses are presented for each case at different codeword symbol shifts, phase deviations, and ROP over 80-km SSMF transmission. We also investigate the performance of the system when two random displacement operators are applied to the two polarization states, X and Y, separately.

3.1 Loaded electrical signals characteristics

The double-sideband spectra of QPSK, 16QAM, and 32QAM before and after pre-emphasizes are shown in Fig. 3 (a) and (b), respectively. The double-sideband spectra are obtained by fast Fourier transform (FFT) of the data sequence of the corresponding modulation format. Figure 3 row (c) represents cumulative distribution histograms of a typical QPSK, a QPSK with the DOCS encryption technique applied to the two polarization states, a QPSK with two random displacement operators each applied to X-Y polarization states and QPSK quantified cumulative distribution histogram, respectively. Figure 3

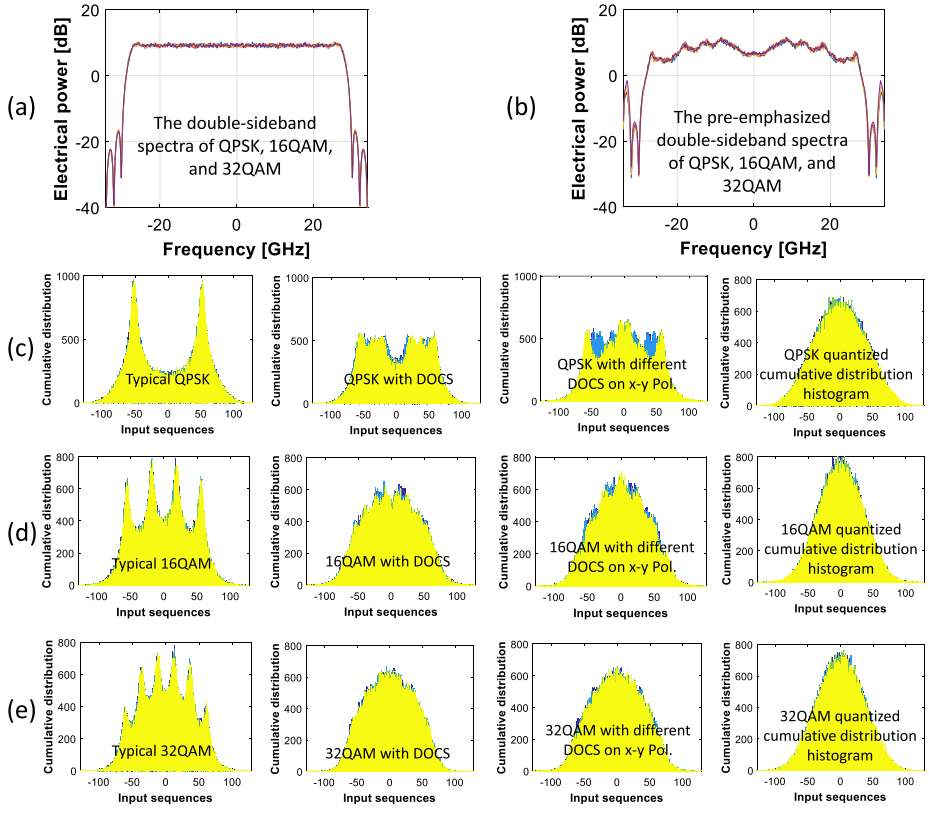

Figure 3 (a) The double-sideband spectra, and (b) the pre-emphasized double-sideband spectra of transmitted QPSK, 16QAM, and 32QAM. Rows (c), (d), and (e) represent the cumulative distribution histogram of a typical QAM modulation format, QAM with DOCS encryption technique, QAM with different DOCS encryption employed on the X and Y polarization states, and the corresponding quantified cumulative distribution for QPSK, 16QAM, and 32QAM, respectively

rows (d) and (e) represent the same thing for 16QAM and 32QAM modulation formats, respectively. These histograms are important to show the penalty of signal qualities with and without the DOCS encryption technique. Reduced signal qualities come as a trade-off for high-level signal encryption.

3.2 Performance evaluation of the DOCS encryption technique

We evaluate the system performance with and without encryption to better assess the penalty of applying the DOCS encryption technique. All experimental results presented in this paper are dual-polarization at 56 GBd after 80-km SSMF transmission. The net bit rates achieved are 224, 448, and 560 Gb/s for QPSK, 16QAM, and 32QAM modulation formats, respectively.

Figure 4 (a) shows the average BER as a function of ROP for QPSK, 16QAM, and 32QAM with (straight lines) and without (dashed lines) employing the DOCS encryption technique. As expected, there is a noticeable degradation in performance compared to the case without encryption. However, most of the points scored BER values below the SD-FEC threshold 2.4×10^{-2}. For ROP > −20 dBm, QPSK and 16QAM scored BER lower than the HD-FEC threshold 3.8×10^{-3}. In general, the trade-off in using higher-order modulation formats like 32QAM is that they offer higher data rates, but they are more sensitive to noise including, but not limited to, DAC, ADC, RF amplifiers, and BPDs. In the ROP

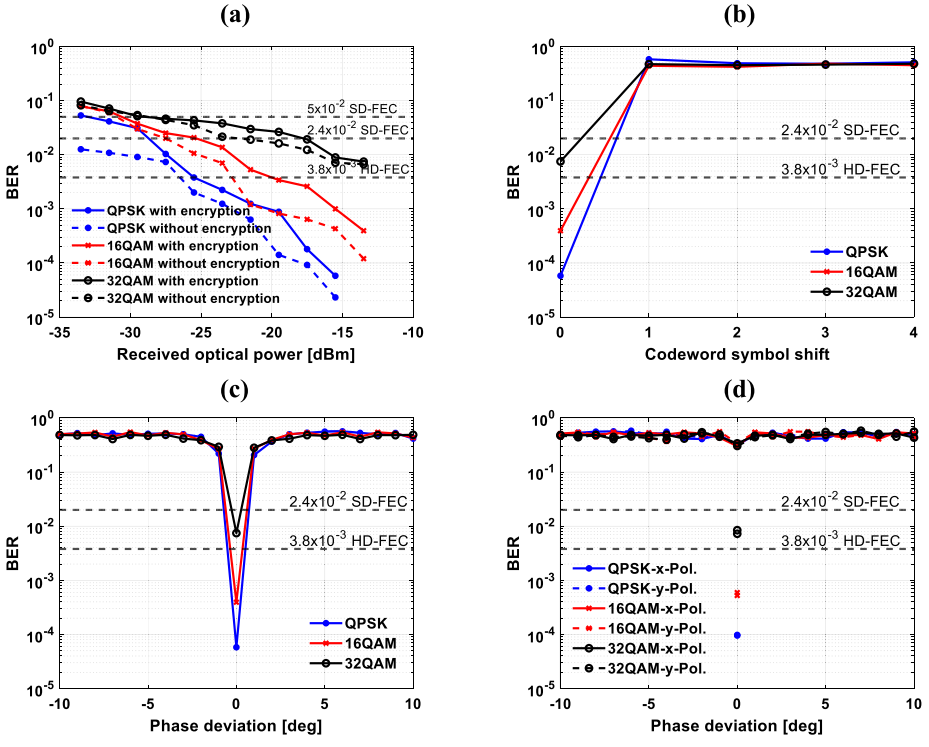

Figure 4 (a) Measured BER as a function of ROP for different modulation formats with and without the DOCS encryption. (b) Measured BER as a function of the shifts in the exact codeword used for encryption and decryption for different modulation formats. (c) Measured BER as a function of the phase deviation of the exact codeword used for encryption and decryption for different modulation formats. (d) Measured BER as a function of phase deviation of two random DOCS codewords used to encrypt the two polarization states to add another layer of security

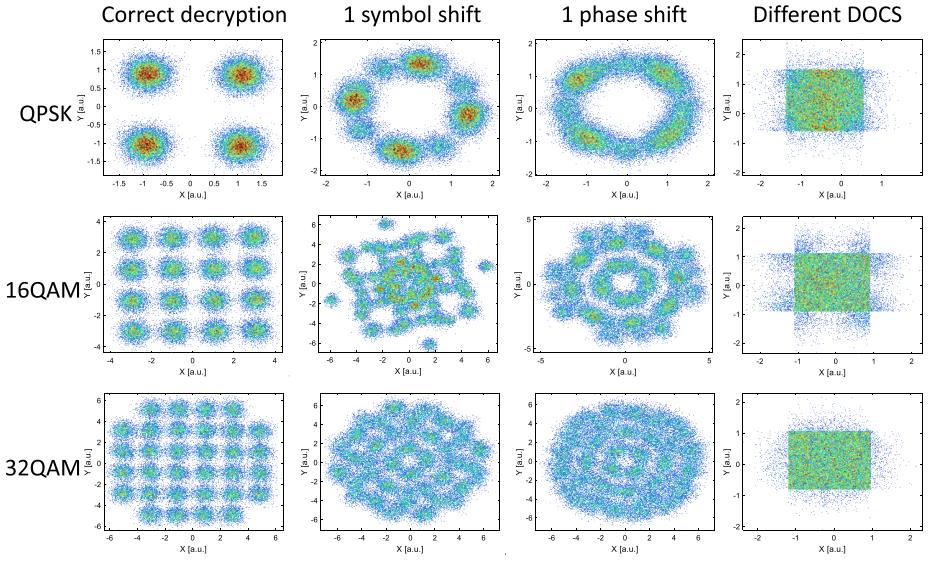

Figure 5 Constellation diagrams of QPSK, 16QAM, and 32QAM when the correct DOCS decryption is used, a single-symbol shift in the correct codeword, a single-phase shift in the correct codeword, and a different DOCS decryption, respectively

analysis, the encryption and decryption are considered to be matched and synchronized. The constellation diagrams of QPSK, 16QAM, and 32QAM are shown in Fig. 5 column 1 (correct decryption). Since we use pilot symbols to help with symbol synchronization, it becomes impractical for the adversary to find the right synchronization between the transmitted and received symbols, assuming the adversary has complete knowledge of the transmitted data and the codeword used for encryption.

For an eavesdropper to decrypt the signal correctly, the exact codeword must be used with the right synchronization, amplitude variations, and phase deviation. Since the DOCS encryption technique is completely random and any values of amplitude variations and phase deviations can be used within the phase space of the QAM symbols, the decryption process using brute force becomes more and more complicated. To begin the eavesdropping analysis against our robust system, we assume that an eavesdropper taps into the fiber link and uses the exact receiver technology as an authenticated receiver without knowledge of the codeword used, this assumption is well-known in cryptography as Kerckhoffs' Principle [33].

Figure 4 (b) shows the BER as a function of codeword symbol shift. The results indicate that employing the correct codeword for decryption, but with a single-symbol shift (or more), results in an immediate increase in the BER to approximately 50%. A single-symbol shift in the exact codeword means that information symbols are displaced to new geometry in the phase space, which means every false attempt complicates the decryption process in a real-time scenario. The corresponding constellation diagrams are shown in Fig. 5 column 2 (1 symbol shift) for QPSK, 16QAM, and 32QAM. Next, we assume the correct synchronization and amplitude variations are found but not the correct phase deviation. Figure 4 (c) shows the BER as a function of the phase deviation used to decrypt the signal. A single-phase deviation shift (or more) also leads to an immediate increase in the BER to approximately 50% for the tested modulation formats. Since the received en-

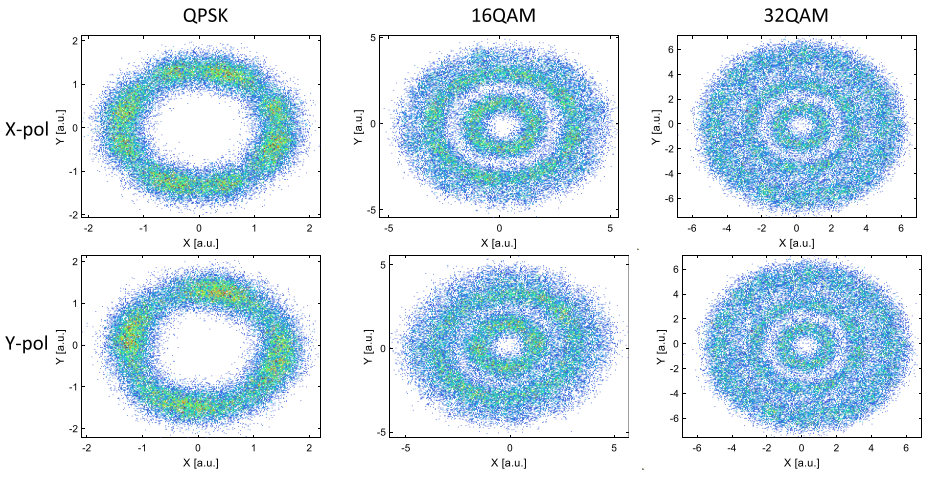

Figure 6 The two polarization states are encrypted with two different displacement operators. Constellation diagrams of QPSK, 16QAM, and 32QAM when the decryption of X-polarized symbols is done using the Y-polarized displacement operator and vice versa

crypted signal has an ambiguous structure, the BPS algorithm failed to compensate for the mismatching of the phase deviation even with the exact codeword and perfect synchronization. It is also important to note that signals using low-order modulation formats, such as QPSK, can tolerate more key noise than signals using high-order modulation formats, such as 32QAM, at the same symbol rate of 56 GBd. The corresponding constellation diagrams are shown in Fig. 5 column 3 (1 phase shift) for QPSK, 16QAM, and 32QAM.

We further explore the performance of the system when each polarization state, X and Y, is encrypted with a random different displacement operator. Equation (2) can be expressed for the two polarization states as follows:

$$\begin{bmatrix} s_{En,x}(t) \\ s_{En,y}(t) \end{bmatrix} = \begin{bmatrix} s_x(t) & 0 \\ 0 & s_y(t) \end{bmatrix} \begin{bmatrix} |\beta_x(t)|e^{j(\varphi_x(t)+\delta\varphi_x)} \\ |\beta_y(t)|e^{j(\varphi_y(t)+\delta\varphi_y)} \end{bmatrix} \tag{5}$$

Figure 4 (d) shows the measured BER as a function of phase deviation for different encryption in the X-Y polarization. Data points below the SD-FEC threshold are with the correct phase deviation and synchronization for each polarization. If the inverse of the X-polarized displacement operator is applied to decrypt the Y-polarized signal, the measured BER is above 30%, and vice versa. The corresponding constellation diagrams are shown in Fig. 6. In general, if a false displacement operator is applied to decrypt the signal, the adversary should not be able to extract any information from the signal. The constellation diagrams in this case are shown in Fig. 5, column 4.

4 Discussion and summary

We have demonstrated experimental validation of quantum encryption in phase space using the displacement operator technique in a conventional coherent optical communication system. Our investigation focused on assessing the system's performance both with and without encryption, allowing us to quantify the impact of the proposed encryption technique. Experimental results indicate the feasibility of implementing the DOCS encryption technique within the existing coherent optical communication infrastructure.

In our demonstration, we intentionally avoided the displacement operator causing destructive interference with the modulated data for simplicity. Specifically, the phases of the displacement operator were selected to ensure they did not align oppositely to those of the symbols across all QAM modulation formats. For instance, in the case of QPSK, where the phases of the modulated data are 45, 135, 225, and 315 degrees, the phases of the displacement operator were carefully chosen not to be opposite to these phases. This constraint restricts the permissible phase choices for the displacement operator, excluding those within ±1 degree of the modulation format phases, as illustrated by our experimental findings in Fig. 4(b). Thus, we avoided scenarios where the signal would fall below the system's detection threshold. In practical applications, once the modulation format is agreed upon between authenticated users, the displacement operator is selected to prevent any destructive interference with the modulated data.

Although we did not have access to directly measure thermal noise and shot noise in the receiver, by comparing results with and without encryption, we aimed to investigate the impact of the displacement operator on the system's overall performance. When performing the comparison, the impact of thermal and shot noise in the receiver are already considered. These noise sources are inherent in any optical communication system. However, distinguishing the exact contribution of thermal noise versus shot noise to the overall system performance is challenging. This difficulty arises because these noise sources interact in complex ways with the signal and with each other, making it impractical to isolate their individual effects explicitly.

The security aspect of DOCS encryption becomes evident when considering potential eavesdropping attempts. If an adversary gains access to the fiber link and detects the encrypted signal, complete knowledge of the DOCS encryption is required for successful decryption. Any false trial by the adversary only introduces additional ambiguity to the received signal, enhancing the security of the communication channel.

The integration of the DOCS encryption/decryption technique with coherent DSP at the transmitter/receiver ends establishes a robust foundation for secure data transmission. The proposed encryption technique is tested over 80 km-SSMF transmissions using dual polarization at 56 GBd. The net bit rates achieved are 224, 448, and 560 Gb/s for QPSK, 16QAM, and 32QAM modulation formats, respectively. Our experimental results demonstrate that attempting to decrypt the signal with any symbol shift, phase deviation shift, or a different codeword results in a BER of approximately 50%. This highlights the resilience of DOCS encryption against eavesdropping attacks, showcasing its effectiveness in ensuring the confidentiality of the transmitted data. Future investigations include assessments of how the proposed encryption technique performs under common optical communication interference such as cross-talk or multipath interference.

Acknowledgements
This research was supported in part by the Natural Sciences and Engineering Research Council (Canada) and the MITACS Accelerate program. The authors thank Ciena for the use of a Wavelogic modem in their experiments.

Author contributions
M.K. conducted the experiments, proposed the dual-polarization encryption, analyzed the results, and wrote the manuscript. A. C. performed the simulation analysis. D. V. P. and L. R. C. revised the manuscript and supervised the experiments. R. K. proposed the displacement operator encryption. All authors reviewed the manuscript.

Funding
This research was supported in part by the Natural Sciences and Engineering Research Council (Canada) and the MITACS Accelerate program.

Data Availability
No datasets were generated or analysed during the current study.

Declarations

Ethics approval and consent to participate
Not applicable.

Consent for publication
The authors have consented to the submission to the journal.

Competing interests
The authors declare no competing interests.

Author details
[1]Department of Electrical and Computer Engineering, McGill University, Montreal, QC, Canada. [2]Synopsys Inc., Ottawa, ON, Canada. [3]Quantropi Inc., Ottawa, ON, Canada.

Received: 7 March 2024 Accepted: 22 July 2024 Published online: 31 July 2024

References

1. Yu J, Zhang J. Recent progress on high-speed optical transmission. Digital Commun Networks. 2016;2(2):65–76. https://doi.org/10.1016/j.dcan.2016.03.002.
2. He J, Norwood RA, Brandt-Pearce M, Djordjevic IB, Cvijetic M, Subramaniam S, Himmelhuber R, Reynolds C, Blanche P, Lynn B, Peyghambarian N. A survey on recent advances in optical communications. Comput Electr Eng. 2014;40(1):216–40. https://doi.org/10.1016/j.compeleceng.2013.11.017. 40th-year commemorative issue.
3. Fok MP, Wang Z, Deng Y, Prucnal PR. Optical layer security in fiber-optic networks. IEEE Trans Inf Forensics Secur. 2011;6(3):725–36. https://doi.org/10.1109/TIFS.2011.2141990.
4. Skorin-Kapov N, Furdek M, Zsigmond S, Wosinska L. Physical-layer security in evolving optical networks. IEEE Commun Mag. 2016;54(8):110–7. https://doi.org/10.1109/MCOM.2016.7537185.
5. Zhu Q, Yu X, Zhao Y, Nag A, Zhang J. Resource allocation in quantum-key-distribution- secured datacenter networks with cloud–edge collaboration. IEEE Int Things J. 2023;10(12):10916–32. https://doi.org/10.1109/JIOT.2023.3242725.
6. Rosenberg D, Harrington JW, Rice PR, Hiskett PA, Peterson CG, Hughes RJ, Lita AE, Nam SW, Nordholt JE. Long-distance decoy-state quantum key distribution in optical fiber. Phys Rev Lett. 2007;98:010503. https://doi.org/10.1103/PhysRevLett.98.010503.
7. Argyris A, Syvridis D, Larger L, Annovazzi-Lodi V, Colet P, Fischer I, García-Ojalvo J, Mirasso CR, Pesquera L, Shore KA. Chaos-based communications at high bit rates using commercial fibre-optic links. Nature. 2005;438(7066):343–6. https://doi.org/10.1038/nature04275.
8. Wu B, Wang Z, Tian Y, Fok MP, Shastri BJ, Kanoff DR, Prucnal PR. Optical steganography based on amplified spontaneous emission noise. Opt Express. 2013;21(2):2065–71. https://doi.org/10.1364/OE.21.002065.
9. Huang C, Ma PY, Shastri BJ, Mittal P, Prucnal PR. Robustness of optical steganographic communication under coherent detection attack. IEEE Photonics Technol Lett. 2019;31(4):327–30. https://doi.org/10.1109/LPT.2019.2891955.
10. Li Z, Li G. Ultrahigh-speed reconfigurable logic gates based on four-wave mixing in a semiconductor optical amplifier. IEEE Photonics Technol Lett. 2006;18(12):1341–3. https://doi.org/10.1109/LPT.2006.877008.
11. Chan K, Chan C-K, Chen LK, Tong F. Demonstration of 20-gb/s all-optical xor gate by four-wave mixing in semiconductor optical amplifier with rz-dpsk modulated inputs. IEEE Photonics Technol Lett. 2004;16(3):897–9. https://doi.org/10.1109/LPT.2004.823750.
12. Bennett CH, Brassard G. Quantum cryptography: public key distribution and coin tossing. Theor Comput Sci. 2014;560:7–11.
13. Wang H, Pi Y, Huang W, Li Y, Shao Y, Yang J, Liu J, Zhang C, Zhang Y, Xu B. High-speed Gaussian-modulated continuous-variable quantum key distribution with a local local oscillator based on pilot-tone-assisted phase compensation. Opt Express. 2020;28(22):32882–93. https://doi.org/10.1364/OE.404611.
14. Yang L, Zhang L, Yang R, Yang L, Yue B, Yang P. Chaotic dynamics of erbium-doped fiber laser with nonlinear optical loop mirror. Opt Commun. 2012;285(2):143–8. https://doi.org/10.1016/j.optcom.2011.09.029.
15. Xue C, Jiang N, Lv Y, Wang C, Li G, Lin S, Qiu K. Security-enhanced chaos communication with time-delay signature suppression and phase encryption. Opt Lett. 2016;41(16):3690–3. https://doi.org/10.1364/OL.41.003690.
16. Jiang N, Zhao A, Xue C, Tang J, Qiu K. Physical secure optical communication based on private chaotic spectral phase encryption/decryption. Opt Lett. 2019;44(7):1536–9. https://doi.org/10.1364/OL.44.001536.
17. Wang Z, Prucnal PR. Optical steganography over a public dpsk channel with asynchronous detection. IEEE Photonics Technol Lett. 2011;23(1):48–50. https://doi.org/10.1109/LPT.2010.2090516.
18. Lavrov R, Jacquot M, Larger L. Nonlocal nonlinear electro-optic phase dynamics demonstrating 10 gb/s chaos communications. IEEE J Quantum Electron. 2010;46(10):1430–5. https://doi.org/10.1109/JQE.2010.2049987.
19. Jinno M, Matsumoto T. Ultrafast all-optical logic operations in a nonlinear Sagnac interferometer with two control beams. Opt Lett. 1991;16(4):220–2. https://doi.org/10.1364/OL.16.000220.
20. Kuang R, Bettenburg N. Quantum public key distribution using randomized Glauber states. In: 2020 IEEE international conference on Quantum Computing and Engineering (QCE). 2020. p. 191–6. https://doi.org/10.1109/QCE49297.2020.00032.
21. Chan A, Khalil M, Shahriar KA, Plant DV, Chen LR, Kuang R. Encryption in phase space for classical coherent optical communications. Sci Rep. 2023;13(1):12965. https://doi.org/10.1038/s41598-023-39621-5.
22. Chan A, Khalil M, Shahriar KA, Chen LR, Plant DV, Kuang R. On the security of an optical layer encryption using coherent-based tf-qkd in classical optical fiber links. In: 2022 4th International Conference on Computer Communication and the Internet (ICCCI). 2022. p. 105–10. https://doi.org/10.1109/ICCCI55554.2022.9850244.

23. Khalil M, Chan A, Shahriar KA, Chen LR, Plant DV, Kuang R. Security performance of public key distribution in coherent optical communications links. In: 2021 3rd International Conference on Computer Communication and the Internet (ICCCI). 2021. p. 123–9. https://doi.org/10.1109/ICCCI51764.2021.9486822.
24. Chan A, Khalil M, Shahriar KA, Chen LR, Plant DV, Kuang R. Security analysis of a next generation tf-qkd for secure public key distribution with coherent detection over classical optical fiber networks. In: 2021 7th International Conference on Computer and Communications (ICCC). 2021. p. 416–20. https://doi.org/10.1109/ICCC54389.2021.9674320.
25. Shahriar KA, Khalil M, Chan A, Chen LR, Kuang R, Plant DV. Enhancing data security in optical fiber communication through dual layer encryption with randomized phases. In: Frontiers in optics + laser science 2022 (FIO, LS). Technical digest series. Rochester: Optica Pub. Group; 2022. p. 5–80. https://doi.org/10.1364/FIO.2022.JW5A.80.
26. Shahriar KA, Khalil M, Chan A, Chen LR, Kuang R, Plant DV. Physical-layer secure optical communication based on randomized phase space in pseudo-3-party infrastructure. In: Conference on lasers and electro-optics. Technical digest series. San Jose: Optica Pub. Group; 2022. p. 4–3. https://doi.org/10.1364/CLEO_SI.2022.SF4L.3.
27. Kuang R, Chan A. Quantum encryption in phase space with displacement operators. EPJ Quantum Technol. 2023;10(1):26. https://doi.org/10.1140/epjqt/s40507-023-00183-0.
28. Hasib AA, Haque AAMM. A comparative study of the performance and security issues of aes and rsa cryptography. In: 2008 third international conference on convergence and hybrid information technology. vol. 2. 2008. p. 505–10. https://doi.org/10.1109/ICCIT.2008.179.
29. Paris MGA. Displacement operator by beam splitter. Phys Lett A. 1996;217(2):78–80. https://doi.org/10.1016/0375-9601(96)00339-8.
30. Schindler PC, Schmogrow R, Dreschmann M, Meyer J, Tomkos I, Prat J, Krimmel H-G, Pfeiffer T, Kourtessis P, Ludwig A, Karnick D, Hillerkuss D, Becker J, Koos C, Freude W, Leuthold J. Colorless fdma-pon with flexible bandwidth allocation and colorless, low-speed onus [invited]. J Opt Commun Netw. 2013;5(10):204–12. https://doi.org/10.1364/JOCN.5.00A204.
31. Varughese S, Lippiatt D, Tibuleac S, Ralph SE. Frequency dependent enob requirements for 400g/600g/800g optical links. J Lightwave Technol. 2020;38(18):5008–16. https://doi.org/10.1109/JLT.2020.3000177.
32. Pfau T, Hoffmann S, Noe R. Hardware-efficient coherent digital receiver concept with feedforward carrier recovery for *m* -qam constellations. J Lightwave Technol. 2009;27(8):989–99. https://doi.org/10.1109/JLT.2008.2010511.
33. Mrdovic S, Perunicic B. Kerckhoffs' principle for intrusion detection. In: Networks 2008 - the 13th international telecommunications network strategy and planning symposium, vol. Supplement. 2008. p. 1–8. https://doi.org/10.1109/NETWKS.2008.6231360.

Publisher's Note