Zhang et al. *EPJ Quantum Technology* (2026) 13:41
https://doi.org/10.1140/epjqt/s40507-026-00480-4

EPJ.org

EPJ Quantum Technology

RESEARCH Open Access

Toward practical quantum encryption in phase space: simulated QPSK and 16-QAM with dynamic displacement operators

Chenyu Zhang[1,2*], Randy Kuang[3*], Jian Xu[1,2], Kai Wen[1,2], Tianyi Wu[1], Zhenrong Zhang[2] and Chen Dong[1]

*Correspondence:
zxkcy0212@gmail.com;
randy.kuang@quantropi.com
[1]Information Support Force Engineering University, Wuhan, 450007, China
[3]Research, Quantropi Inc., 1545 Carling Av, Suite 620, Ottawa, K1Z 8P9, ON, Canada
Full list of author information is available at the end of the article

Abstract

Building upon the theoretical framework of Dynamic Displacement Operators (DDO) introduced in Ref. (Kuang, in Acad Quantum 2, 2025, https://doi.org/10.20935/AcadQuant7462), we present a simulation validation of a quantum-enhanced encryption scheme for coherent optical communication systems in phase space. The method integrates random phase shift operators (PSOs) and displacement operators (DOs) to dynamically manipulate information symbols on a symbol-by-symbol basis, enabling secure physical-layer encryption. Simulation results confirm that accurate decryption is only possible with the correct operator pair; any mismatch in displacement or phase parameters leads to bit error rates approaching 50%, effectively blocking unauthorized access. We further compare the performance of unencrypted transmission with various quantum-enhanced physical-layer security (QEPS) configurations over different fiber lengths, and explicitly validate the scalability of the proposed scheme by simulating a higher-order Quantum Permutation Pad (QPP) with a depth of $m = 2$ for 16-QAM. The results validate the robustness of the proposed DDO-based scheme against partial or incorrect decryption attempts, underscoring its potential for securing data transmission in classical optical networks.

Keywords: Quantum encryption; Coherent optical communication; Dynamic displacement operator (DDO); Physical-layer security; Phase space modulation; Bit error rate (BER); Quantum-enhanced physical security (QEPS); Displacement operator; Phase shift operator; Quantum Permutation Pad (QPP)

1 Introduction

As the backbone of modern data transmission, optical communication technology has rapidly evolved to support high-speed and high-capacity demands. Current research heavily focuses on optimizing network performance, primarily through enhanced bandwidth utilization, boosted data throughput, and accelerated digital signal processing (DSP) [2, 3].

As concerns over data privacy and integrity grow, building secure and reliable communication systems has become paramount. The inherent openness of long-distance optical fiber communication links makes them particularly vulnerable to eavesdropping, as adversaries can readily intercept optical signals by physically accessing the transmission

Springer

medium [4–6]. To address this threat, various encryption schemes have been proposed and extensively studied to enhance the security of fiber-optic networks. Among these, Quantum Key Distribution (QKD) has emerged as a leading cryptographic technology [7].

QKD leverages the principles of quantum mechanics to enable secure key exchange, particularly in the face of growing quantum computing threats [8–10]. Unlike classical encryption methods, which depend on computational hardness assumptions such as integer factorization [11] or discrete logarithms [12, 13], QKD employs quantum superposition and entanglement to establish cryptographic keys that are information-theoretically secure, meaning their security relies on the fundamental laws of physics rather than computational complexity assumptions [8, 10]. QKD encodes information in the quantum states of individual photons, ensuring that any eavesdropping attempt disturbs the system and alerts the communicating parties. This inherent sensitivity to observation provides unparalleled cryptographic security, positioning QKD as a promising solution for quantum-era communications. While QKD is typically associated with single-photon detection, some advanced QKD protocols also employ coherent detection techniques [14, 15], aligning more closely with the infrastructure of classical coherent optical systems. However, QKD is primarily designed for key establishment rather than direct data encryption.

To secure the optical infrastructure itself, various physical-layer encryption (PLE) methods have been explored. These include optical XOR using dual-drive Mach–Zehnder modulators (DD-MZM) [16], spectral phase encoding combined with QKD [17], polarization-state rotation [18], chaotic phase encryption [19, 20], and mode-dependent loss manipulation in multimode fibers [21]. These analog PLE methods differ fundamentally from digital encryption embedded in higher-layer physical modules (e.g., those implementing AES). Analog PLE aims to prevent *any* intelligible ciphertext extraction at the optical layer, whereas digital modules, even if encrypted, can still be tapped to retrieve the ciphertext for subsequent off-line decryption.

Comparison with Existing Schemes To contextualize the advantages of the proposed QEPS-dd framework Table 1, we compare it with two prominent physical-layer encryption strategies: Chaos-based encryption and XOR-based scrambling.

Chaos-based optical encryption relies on nonlinear feedback dynamics to generate pseudo-random carriers. While these systems achieve high unpredictability, they often suffer from sensitivity to synchronization errors, noise accumulation, and hardware parameter mismatch, which limit their scalability in high-speed coherent systems. Conversely, XOR-based methods offer implementation simplicity and low cost. However, they typically operate in the discrete digital domain. This discrete nature makes them inherently less compatible with analog coherent modulation formats like QPSK and 16-QAM, as they lack the continuous-state obfuscation required to resist sophisticated phase inference attacks.

In contrast, QEPS-dd utilizes non-commutative quantum operators—specifically displacement and phase-shift operators—applied directly in the continuous quantum phase space. This approach ensures that both amplitude and phase are jointly randomized in a physically meaningful manner, providing full compatibility with standard coherent optical infrastructure. Although QEPS-dd introduces moderate complexity regarding operator computation and key management (as discussed in Sect. 3.7), it offers a deterministic and mathematically rigorous encryption model.

Table 1 Comparison of Physical Layer Encryption Schemes

Comparison Dimension	Chaos-based Encryption	XoR-based Encryption	QEPS-dd
Modulation Compatibility	High sensitivity often degrades constellation quality; supporting high-order QAM requires complex compensation algorithms.	Typically optimized for binary formats (BPSK/OOK); direct optical mapping to high-order QAM is architecturally challenging.	Linearly operates in phase space; natively supports QPSK, 16-QAM, and higher-order formats without structural changes.
Implementation Complexity	Requires chaotic lasers, feedback loops, and strict hardware synchronization; hard to integrate.	Requires dual stable carriers and precise optical path alignment for interference-based logic.	Uses standard commercial IQ modulators; implemented via DSP algorithms.
Noise Tolerance(SNR Robustness)	Highly sensitive to laser linewidth and phase noise; synchronization is unstable under realistic channel impairments.	Performance degrades significantly with spatial misalignment or phase jitter.	Robust against phase drift and noise; stable performance validated at 28 Gbaud over 80 + km.
Security Mechanism and Analyzability	Relies on dynamics unpredictability; lacks a rigorous mathematical proof of security.	Security relies on physical uniqueness; hard to quantify information leakage analytically.	Based on phase-space indistinguishability; provides a theoretically analyzable key space ($H \approx 508$ m).

In 2020, Kuang and Bettenburg introduced *Quantum Encryption in Phase Space* (QEPS), a novel optical-layer encryption scheme leveraging randomized phase modulation within a round-trip public key distribution paradigm, thereby mimicking public-key cryptography [22]. Unlike QKD, which relies on single photons and separate quantum channels, QEPS uses coherent states of quantum harmonic oscillators and operates entirely within the optical domain. This makes QEPS highly compatible with existing coherent optical communication infrastructure, utilizing standard components for signal generation, modulation, and detection. QEPS achieves both key distribution and symmetric data encryption over a single optical channel. The initial version, known as QEPS-p, was validated experimentally using phase-only encryption [23–28].

In 2023, Kuang and Chan extended the framework by introducing displacement operators, leading to QEPS-d [29]. This enhancement introduced additional encryption strength via randomized displacements in phase space. The QEPS-d approach was experimentally demonstrated in 2024 by Khalil et al. [30]. While both QEPS-p and QEPS-d significantly increased the bit error rate (BER), approaching 0.5 for unauthorized receivers, they still suffered from key limitations. QEPS-p revealed partial amplitude information due to ring-like constellation patterns, while QEPS-d lacked sufficient randomization due to its static displacement, leaving it susceptible to certain predictive attacks.

To overcome these challenges, Kuang proposed a further enhancement: *QEPS with Dynamic Displacement Operators* (QEPS-dd) [1]. This latest iteration introduces dynamic displacement operators (DDOs) that combine phase-shifting and displacement operations in a time-varying and signal-state-dependent manner. The resulting encryption mechanism injects temporal and spatial randomness, greatly increasing resistance against both classical and quantum attacks. As a scalable and future-proof solution, QEPS-dd represents a significant advancement in quantum-secure optical encryption.

Building upon the theoretical framework introduced by Kuang, which formally defined the Quantum Encryption in Phase Space with Dynamic Displacement Operators (QEPS-dd), this study focuses on the first simulation-based implementation and verification of that framework within a classical coherent optical communication environment.

Unlike [1], which primarily established the mathematical formulation and operator structure of QEPS-dd, the present work aims to validate its feasibility, correctness, and DSP compatibility through system-level simulation using OptiSystem.

Specifically, we model the dynamic displacement encryption process within practical QPSK and 16-QAM modulation formats, visualize the resulting encrypted constellations, and analyze bit error rate (BER) performance under various transmission conditions. These results demonstrate that QEPS-dd can be successfully operated in coherent optical systems, confirming its practical realizability and robustness against mismatched decryption.

It should be emphasized that although the proposed QEPS-dd scheme is implemented within classical coherent optical communication systems, the encryption operation itself is fundamentally defined in terms of quantum mechanical operators—namely, the displacement operator $\hat{D}(\alpha)$ and the phase-shift operator $\hat{P}(\phi)$—acting on coherent states in phase space.

Therefore, while the physical realization is classical, the encryption process is inherently quantum in its mathematical formalism.

In this sense, the proposed system can be regarded as a quantum-operator-based encryption mechanism, bridging quantum operator theory and classical coherent communication.

2 Quantum encryption in phase space: principles and protocols

2.1 Coherent optical communication and its quantum interpretation

At its core, coherent optical communication leverages advanced modulation formats (e.g., QPSK, QAM) and sophisticated coherent detection techniques to significantly enhance data transmission capacity and efficiency in fiber-optic networks. A typical system comprises two primary components: the transmitter and the receiver. The transmitter includes a laser source and an IQ Mach–Zehnder Modulator (IQ-MZM) for complex modulation, while the receiver features a coherent detector followed by digital signal processing (DSP) modules.

In the QEPS framework, the encryption and decryption processes are parameterized by displacement and phase-shift operators characterized by (α, ϕ), which are pre-synchronized between the transmitter and receiver through a secure initialization procedure. This synchronization ensures that both ends operate with identical operator sequences during data transmission, forming the foundation for reliable decryption in the QEPS-dd system.

Recent advances in Digital Signal Processing (DSP) have dramatically simplified the implementation and improved the performance of coherent optical communication systems. The DSP precisely compensates for various signal impairments, such as chromatic dispersion and phase noise, while also performing crucial synchronization and equalization. This enables the accurate mapping of digital data onto a quadrature amplitude modulation (QAM) basis for transmission. At the receiver, DSP modules meticulously demap the received signal to reliably recover the original bitstream.

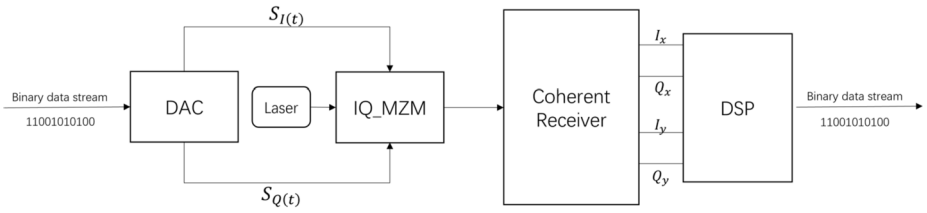


Figure 1 System architecture of coherent optical communication

Figure 2 Displacement operator $\hat{D}(\alpha)$ transforms the vacuum state $|0\rangle$ into a coherent state $|\alpha\rangle$

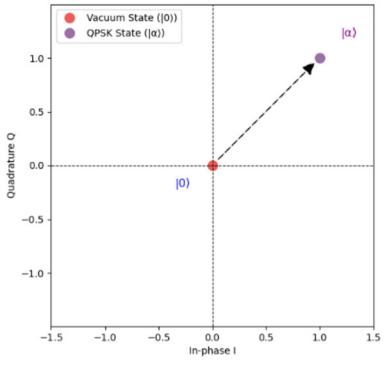


Figure 1 illustrates the modulation and demodulation processes, showing how digital signals are encoded into coherent optical carriers and subsequently recovered using coherent detection.

In quantum terms, a coherent optical signal corresponds to a quantum coherent state $|\alpha\rangle$, which is generated by applying a displacement operator $\hat{D}(\alpha)$ to the vacuum state $|0\rangle$ Figure 2:

$$|\alpha\rangle = \hat{D}(\alpha)|0\rangle, \quad \alpha = re^{-i\phi} \tag{1}$$

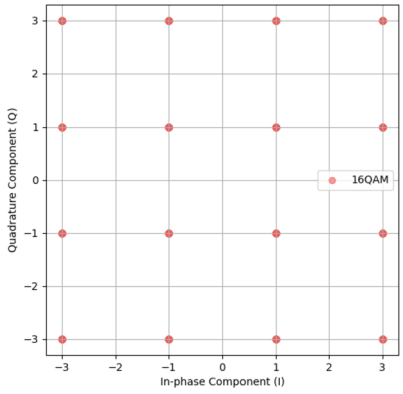
Here, $\alpha = x_I + ix_Q$ represents a complex amplitude, defined by its in-phase (x_I) and quadrature (x_Q) components. This phase-space representation directly mirrors classical modulation formats: the amplitude ($r = |\alpha|$) and phase (ϕ) unambiguously define the signal's position on a constellation diagram. The quadratures x_I and x_Q thus serve as the Cartesian coordinates in phase space, forming the fundamental basis for K-QAM signal constellations. This inherent duality seamlessly bridges classical optical communications and quantum state representations [1].

This correspondence allows K-QAM modulation to be interpreted in quantum mechanics as the action of a discrete encoding operator $\hat{Q}_k$ on a finite set of coherent states $\{|\beta_1\rangle, \ldots, |\beta_K\rangle\}$:

$$\hat{Q}_k|\beta_k\rangle = \beta_k|\beta_k\rangle, \quad k = 1, \ldots, K \tag{2}$$

Each complex value $\beta_k = x_{I,k} + ix_{Q,k}$ precisely defines a constellation point in the optical phase space. For instance, in 16-QAM, $\hat{Q}_{16}$ operates on 16 distinct coherent states, each uniquely mapped to a discrete location. Crucially, unlike the annihilation operator $\hat{a}$ which

Figure 3 Standard 16-QAM signal constellation



possesses a continuous eigenvalue spectrum, the K-QAM operator $\hat{Q}_k$ is characterized by a discrete, finite eigenbasis, which naturally aligns with the principles of classical digital modulation.

This non-commutativity implies a critical consequence: if a signal encoded using $\hat{Q}_{16}$ is subsequently decoded with a mismatched operator, say $\hat{Q}_{32}$, the inherent measurement basis becomes incompatible. This leads to systematic decoding errors, with the resulting bit error rate (BER) approaching 50%, functionally equivalent to random guessing. It is vital to note that this basis mismatch error is operational—stemming from a protocol mismatch—rather than quantum mechanical, thereby distinguishing it from uncertainty-related errors governed by Heisenberg's principle.

2.2 Quantum encryption in phase space: QEPS-dd

To demonstrate the principles of quantum encryption in phase space, we consider a 16-QAM signal constellation. Figure 3 shows the standard 16-QAM constellation used in coherent modulation schemes.

2.2.1 Encryption with phase-shift operators (QEPS-p)

The QEPS-p scheme, proposed by Kuang and Bettenburg [22], introduces phase-space encryption by applying random phase-shift operators $\hat{P}(\phi_j)$ to coherent states. For each coherent symbol $|\beta_k\rangle$, the encryption operation yields:

$$\hat{P}(\phi_j)|\beta_k\rangle = |\beta_k e^{-i\phi_j}\rangle \tag{3}$$

This transformation rotates the signal constellation around the origin by angle ϕ_j. The original constellation (Fig. 4(a)) is randomized into circular rings (Fig. 4(b)).

An eavesdropper using the original K-QAM operator $\hat{Q}_k$ without knowledge of the applied phase shifts experiences a decoding failure:

$$\hat{Q}_k|e^{-i\phi_j}\beta_k\rangle \neq \beta_k|\beta_k\rangle \quad \Rightarrow \text{BER} \approx 50\% \tag{4}$$

A legitimate receiver, however, can undo the encryption by applying the inverse phase shift:

$$\hat{P}^{-1}(\phi_j)|\beta_k e^{-i\phi_j}\rangle = |\beta_k\rangle \tag{5}$$

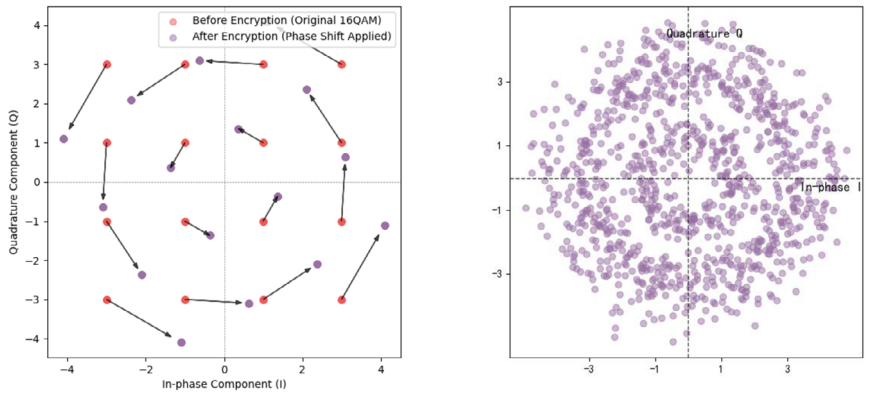


Figure 4 (a) Rotated 16-QAM constellation under phase shift $\hat{P}(\phi)$; (b) Encrypted symbols appear as ring structures

While QEPS-p effectively randomizes the phase information, the resulting ring-like constellation inherently leaks amplitude information. For instance, the radius of each ring remains directly correlated with the original QAM amplitude level, posing a potential vulnerability.

2.2.2 *Encryption with displacement operators* (*QEPS-d*)

To obscure both phase and amplitude, QEPS-d [29] uses random displacement operators $\hat{d}(\alpha_i)$ to shift coherent states:

$$\hat{d}(\alpha_i)|\beta_j\rangle = |\alpha_i + \beta_j\rangle \tag{6}$$

These operators are commutative under composition:

$$\hat{d}(\alpha)\hat{d}(\beta) = \hat{d}(\beta)\hat{d}(\alpha) \tag{7}$$

The resulting state is no longer an eigenstate of the original K-QAM operator:

$$\hat{Q}_k|\alpha_i + \beta_j\rangle \neq (\alpha_i + \beta_j)|\alpha_i + \beta_j\rangle \tag{8}$$

This misalignment leads to decoding failure by unauthorized parties. A legitimate receiver, knowing α_i, applies the inverse displacement to recover the plaintext state:

$$\hat{d}^{-1}(\alpha_i)|\alpha_i + \beta_j\rangle = |\beta_j\rangle \tag{9}$$

Figure 5 shows the operation of QEPS-d on signals. While QEPS-d offers enhanced concealment compared to QEPS-p, its reliance on static displacement operations, applied uniformly regardless of the input signal's properties, remains a limitation. This static nature could potentially be exploited by powerful analysis tools or through the collection of sufficient data, making it susceptible to certain advanced attacks.

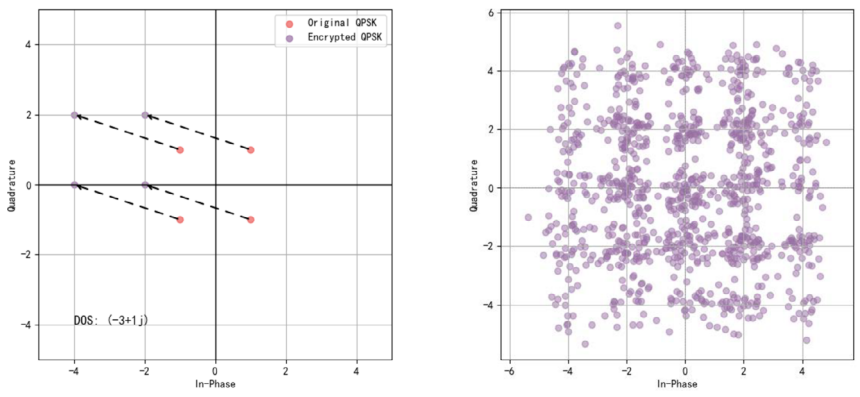


Figure 5 (a) QPSK signals displaced into the 16-QAM domain; (b) Encrypted constellation with randomized positions

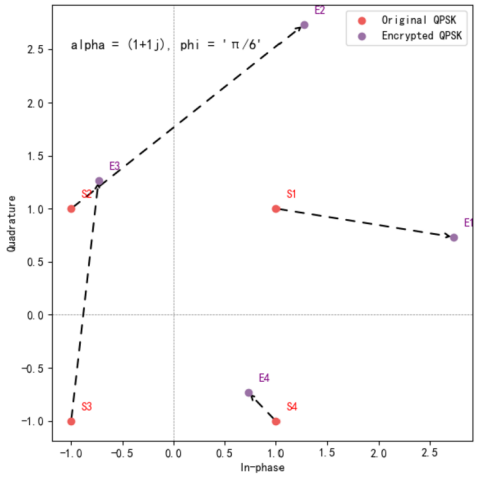


Figure 6 DDO-induced displacement varies with both the operator and the input state, producing non-uniform encryption

2.2.3 Encryption with dynamic displacement operators (*QEPS-dd*)

To overcome limitations of static encryption, QEPS-dd introduces the Dynamic Displacement Operator (DDO), defined as:

$$\hat{d}(\alpha, \phi) = \hat{d}(\alpha)\hat{P}(\phi) \tag{10}$$

When applied to a coherent state $|\beta\rangle$, this operator produces a state-dependent transformation:

$$\hat{d}(\alpha, \phi)|\beta\rangle = |\alpha + e^{-i\phi}\beta\rangle \tag{11}$$

This operation is equivalent to a dynamic displacement $\hat{d}(\alpha')$ where $\alpha' = \alpha + (e^{-i\phi} - 1)\beta$, explicitly associating the displacement with the target state β as shown in Fig. 6.

Unlike previous schemes, DDOs exhibit non-commutative behavior, crucial for enhanced security:

$$\hat{d}(\alpha,\phi)\hat{d}^{-1}(\alpha',\phi') \neq \hat{I} \quad \text{unless } \alpha = \alpha',\ \phi = \phi' \tag{12}$$

This means the inverse operation is precise. More importantly, their non-commutativity extends to sequences of operations:

$$\hat{d}(\alpha,\phi)\hat{d}(\alpha',\phi')|\beta\rangle \neq \hat{d}(\alpha',\phi')\hat{d}(\alpha,\phi)|\beta\rangle \tag{13}$$

The inverse transformation is defined as:

$$\hat{d}^{-1}(\alpha,\phi)|\alpha + e^{-i\phi}\beta\rangle = \hat{P}^{-1}(\phi)\hat{d}^{-1}(\alpha)|\alpha + e^{-i\phi}\beta\rangle = |\beta\rangle \tag{14}$$

The entropy of a key space defined by $\{\alpha,\phi\}$ and size $N = N_d N_p$ is:

$$H = -\sum_{i=1}^{N} p_i \log_2 p_i \tag{15}$$

where N_d and N_p represent the number of possible values in the displacement space and phase shift space, respectively. This doubling of the key space entropy makes QEPS-dd significantly more resistant to brute-force attacks. Furthermore, its dynamic and non-commutative nature ensures that encrypted states are unique and vary not only with the cryptographic keys but also intrinsically with the input signals. This produces a cipher space of exceptionally high complexity and unpredictability. Consequently, QEPS-dd establishes an advanced and robust framework for phase-space quantum encryption, designed to be resilient against both classical and nascent quantum adversaries.

3 Simulation results and analysis

This section presents the detailed simulation results, meticulously validating the performance of the proposed Quantum Encryption in Phase Space using Dynamic Displacement Operators (QEPS-dd).

3.1 System architecture and simulation setup

The overall encrypted communication architecture is comprehensively illustrated in Fig. 7. At the transmitter, the quantum encryption module seamlessly integrates the dynamic displacement operator (DDO) $\hat{d}(\alpha,\phi)$ into a standard coherent optical transmitter. The encrypted optical waveform then propagates through a single-mode optical fiber. At the receiver, heterodyne coherent detection is employed, combining a local oscillator (LO) laser with a balanced photodetector to precisely extract the in-phase (I) and quadrature (Q) components of the signal. Crucially, the receiver applies the inverse DDO $\hat{d}^{-1}(\alpha,\phi)$, synchronized with the transmitter, to accurately recover the plaintext signal.

At the transmitter, the DDO encryption operates directly in the IQ modulation stage—before optical transmission—by applying the composite displacement and phase-shift operators to the modulated symbols in phase space. This operation is equivalent to a controlled, time-varying adjustment of amplitude and phase on the optical field and therefore does not interfere with downstream transmission or channel compensation.

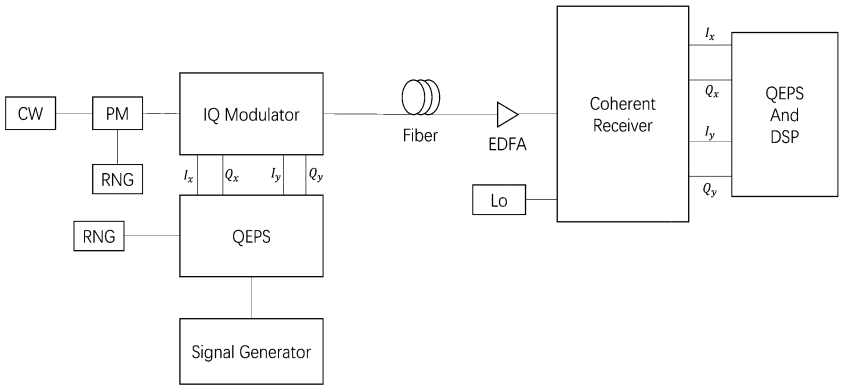


Figure 7 Overall simulation diagram of QEPS-dd

Table 2 Simulation parameters

Layout Parameter	Sequence length	65,536 bits
	Baud rate	28 Gbaud
	PM period	1024
CW Laser and LO Laser	Center wavelength	1550 nm
	Power	5 dBm
	Linewidth	0.1 MHz
	Azimuth	45 deg
IQ Modulator	Extinction ratio	20 dB
	Switching bias	3 V
	Insertion loss	5 dB
EDFA	Forward pump power	13-14 mW
	Forward pump wavelength	980 nm
	Loss at 1550 nm	0.1 dB/m
	Loss at 980 nm	0.15 dB/m
Optical Fiber	Length	80 km
	Attenuation	0.2 dB/km
	Dispersion	16.75 ps/nm/km
	Dispersion slope	0.075 ps/nm^2/km
	Differential group delay	0.2 ps/km
	Effective area	80 μm^2

At the receiver, the signal first undergoes all standard DSP procedures required for coherent detection, including chromatic dispersion (CD) compensation, polarization demultiplexing, and carrier phase/frequency recovery. Only after these conventional DSP steps are completed and the coherent field is properly reconstructed in the digital domain, the inverse DDO operation (decryption) is applied in the IQ plane. This ensures that decryption operates on a correctly phase-aligned signal, avoiding interference with adaptive DSP algorithms.

The simulation was rigorously conducted using OptiSystem software, adhering strictly to the architecture depicted in Fig. 7. We configured the simulation parameters to closely mirror those used in prior QEPS-d experimental studies [29], with detailed specifications conveniently summarized in Table 2.

3.2 QPSK with QEPS-dd encryption

3.2.1 Back-to-back (B2B) encryption-decryption simulations

In the back-to-back (B2B) simulation configuration, the optical signal is transmitted directly from the transmitter to the receiver, bypassing fiber propagation. This setup allows us to isolate and precisely evaluate the encryption-decryption performance without the influence of channel-induced impairments.

For encryption, we constructed the dynamic displacement operator (DDO) from a composition of two distinct operator sets:

- **Displacement Operators (DOs):** These correspond to the 16 constellation points of a standard 16-QAM modulation format, providing the spatial shifts in phase space.
- **Phase Shift Operators (PSOs):** These apply phase angles $\phi_j \in \{0°, 24°, 48°, 72°, 96°, 120°\}$, yielding 6 distinct PSOs for rotational transformations.

The combined DDO encryption space thus comprises a total of $16 \times 6 = 96$ unique operator pairs. In our simulation, to faithfully implement the time-varying QPP protocol, a pseudo-random sequence was employed to dynamically select a specific operator pair (α_k, ϕ_k) from this 96-element set for each transmitted symbol. This symbol-by-symbol dynamic selection ensures that the encryption is time-varying and state-dependent, resulting in the diffuse, cloud-like constellation distribution observed in the undecrypted results, rather than a static displacement. According to Kuang's Quantum Permutation Pad (QPP) framework [1], one can construct a set of m permutations of this 96-element operator space, forming a robust QPP. The entropy of this QPP is then given by:

$$H = m \cdot \log_2(96!) \approx 508 \cdot m \text{ bits}$$

This represents a vastly larger keyspace than traditional symmetric-key encryption methods such as AES-256, offering an exceptionally high degree of quantum-resistant security—even when using only a single permuted DDO space ($m = 1$).

Figure 8 illustrates the simulation results under B2B conditions for four critical decryption scenarios:

- **Fig. 8(a): No Decryption (Eavesdropping Scenario)** In this scenario, a QPSK-modulated signal is encrypted using a randomly selected DDO at the transmitter, but no decryption is performed at the receiver. This directly simulates an adversary intercepting the ciphertext without possession of the proper key. The resulting constellation appears completely scrambled and diffuse, with no discernible structure. The observed bit error rate (BER) is approximately 48%, remarkably close to the theoretical limit for random binary data (50%), effectively concealing the original information content from an unauthorized party.
- **Fig. 8(b): PSO-Only Decryption (Correct PSOs)** Here, the receiver attempts decryption using only the correct phase shift operator (PSO) $\hat{P}^{-1}(\phi)$, without applying the corresponding displacement inversion. Due to the inherent non-commutative nature of DDOs, this partial decryption operation actually acts as a further, unintended transformation rather than an inverse. This produces an even more randomized and diffused constellation compared to the no-decryption case (Fig. 8(a)), pushing the BER even closer to 50%. This case powerfully demonstrates the robustness of DDO's structure: even with one correct component (PSO), the absence of full inversion leads to complete failure in signal recovery.

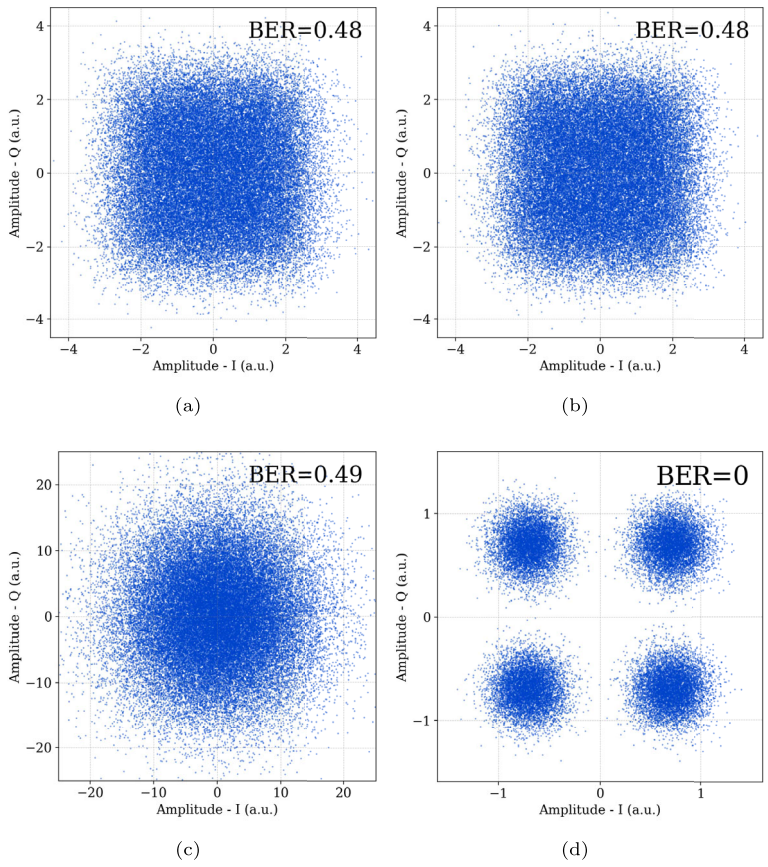


Figure 8 Constellation diagrams under B2B conditions with DDO encryption and varying decryption strategies: (a) no decryption, (b) PSO-only decryption, (c) DO-only decryption, and (d) full DDO decryption

- **Fig. 8(c): DO-Only Decryption (Correct Displacements)** In this setup, the receiver applies only the correct displacement operator $\hat{d}^{-1}(\alpha)$, successfully canceling the translational shifts introduced during the encryption process. Consequently, the displacement-induced shifts are removed, but the uncorrected phase rotations from the PSOs remain. This results in a circular or disk-like constellation, primarily centered at the origin, with a BER of 48%. This visually represents the residual phase encryption, confirming that displacement-only decryption is insufficient.
- **Fig. 8(d): Full DDO Decryption** In this critical scenario, the legitimate receiver applies the exact inverse DDO $\hat{d}^{-1}(\alpha, \phi)$, perfectly matching both the displacement and phase shift parameters used at the transmitter. The original QPSK constellation is then perfectly restored, exhibiting a measured BER of 0%. This unequivocally confirms the correctness and full reversibility of the proposed encryption scheme, demonstrating that successful, error-free decryption is only possible when both displacement and phase components of the key are accurately recovered. This scenario robustly validates the precision and security of the QEPS-dd encryption framework.

These B2B simulations conclusively show that the DDO-based encryption scheme achieves a high level of cryptographic strength. Unauthorized access or attempts at partial decryption consistently fail to reveal the original information, while only full and accurate decryption enables error-free communication, underscoring the scheme's robust security.

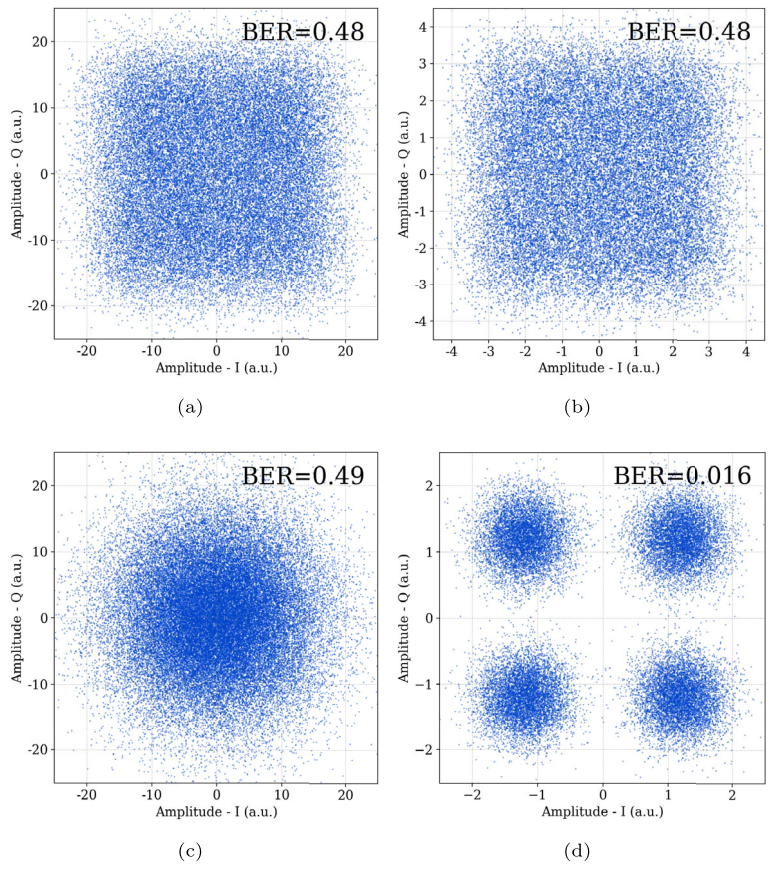


Figure 9 Constellation recovery after 89 km fiber transmission using different decryption strategies: (a) no decryption, (b) PSO-only decryption, (c) DO-only decryption, and (d) full DDO decryption

3.2.2 Fiber transmission results (89 *km*)

Figure 9 presents the constellation diagrams after 89 km of single-mode optical fiber transmission, employing the identical encryption-decryption configurations used in the back-to-back (B2B) simulations shown in Fig. 8. This expanded scenario deliberately introduces realistic fiber impairments—such as chromatic dispersion, signal attenuation, and accumulated phase noise—into the encrypted QPSK signal transmission. This rigorous test evaluates the resilience and practical performance of the QEPS-dd scheme under more realistic fiber channel conditions.

- **Fig. 9(a): No Decryption** The QPSK signal, encrypted with DDO at the transmitter, is transmitted over 89 km without any decryption at the receiver, directly simulating a passive eavesdropping attempt over a significant distance. The resulting constellation is thoroughly randomized and dispersed, showing no recoverable structure, with a bit error rate (BER) of approximately 48%, effectively equivalent to random guessing. This robustly confirms that DDO encryption maintains strong confidentiality even across practical 89 km fiber links.
- **Fig. 9(b): PSO-Only Decryption (Correct PSOs)** Only the phase shift operator (PSO) $\hat{P}^{-1}(\phi)$ is applied at the receiver, while the displacement operator is intentionally omitted. As observed in the B2B case, the constellation becomes even more randomized and spread out than in the undecrypted scenario (Fig. 9(a)). This

persistent scrambling is attributable to the non-commutative nature of the DDO, where applying only the PSO effectively introduces further, detrimental misalignment. The BER remains prohibitively high at 48%, emphatically highlighting the encryption's formidable resistance to partial-key attacks.

- **Fig. 9(c): DO-Only Decryption (Correct Displacements)** Applying only the displacement operator $\hat{d}^{-1}(\alpha)$ successfully cancels the translational shifts from the encryption, yet the phase rotation component remains uncorrected. The resulting constellation distinctly exhibits a circular, disk-like distribution centered at the origin, unequivocally reflecting the residual PSO encryption. While visually distinct from Fig. 9(a), the BER still measures a high 48%, conclusively demonstrating that correct displacement alone is fundamentally insufficient for intelligible signal recovery.
- **Fig. 9(d): Full DDO Decryption** When the receiver applies the complete and correct inverse dynamic displacement operator $\hat{d}^{-1}(\alpha, \phi)$, the QPSK signal is successfully decrypted and coherently demodulated. The recovered constellation pattern closely resembles the ideal QPSK structure, albeit with slight, expected fiber-induced distortion due to channel impairments. Crucially, the BER drops significantly to 1.6%, indicating nearly error-free recovery and confirming that the full DDO decryption operator is absolutely essential for maintaining signal integrity over realistic fiber transmission distances.

In summary, the 89 km fiber transmission results decisively reaffirm the conclusions drawn from the B2B simulations. Unauthorized or incomplete decryption consistently yields near-random output with a BER of approximately 48%, while complete and correct DDO decryption achieves robust signal recovery with a remarkably low BER. These findings strongly validate both the quantum-resistant security and the practical performance viability of QEPS-dd in real-world optical network deployments.

3.3 16-QAM and 64-QAM DDO encryption

To comprehensively evaluate the scalability and versatility of the proposed encryption framework, the modulation format was upgraded from QPSK to 16-QAM. This higher-order modulation introduces a greater number of constellation points with increased complexity in both amplitude and phase, inherently boosting spectral efficiency while simultaneously presenting a more significant challenge for accurate decryption. Figure 10 presents the simulated constellation diagrams for 16-QAM signals under various decryption scenarios, utilizing the identical DDO encryption process as in the preceding QPSK tests.

- **Fig. 10(a): No Decryption** The 16-QAM signal is encrypted with DDO at the transmitter but remains undecrypted at the receiver, precisely emulating an eavesdropping scenario for a higher-order modulation. The resulting constellation appears completely randomized and diffused, exhibiting no visible structure or symbol grouping whatsoever. The bit error rate (BER) reaches approximately 49%, virtually the theoretical maximum for random guessing of 16-QAM data, conclusively confirming that the DDO effectively conceals the transmitted information even for complex modulation formats.
- **Fig. 10(b): PSO-Only Decryption** In this case, only the phase shift operator (PSO) is applied at the receiver. The constellation remains highly scattered and disordered, offering absolutely no recognizable pattern of the original 16-QAM structure. While

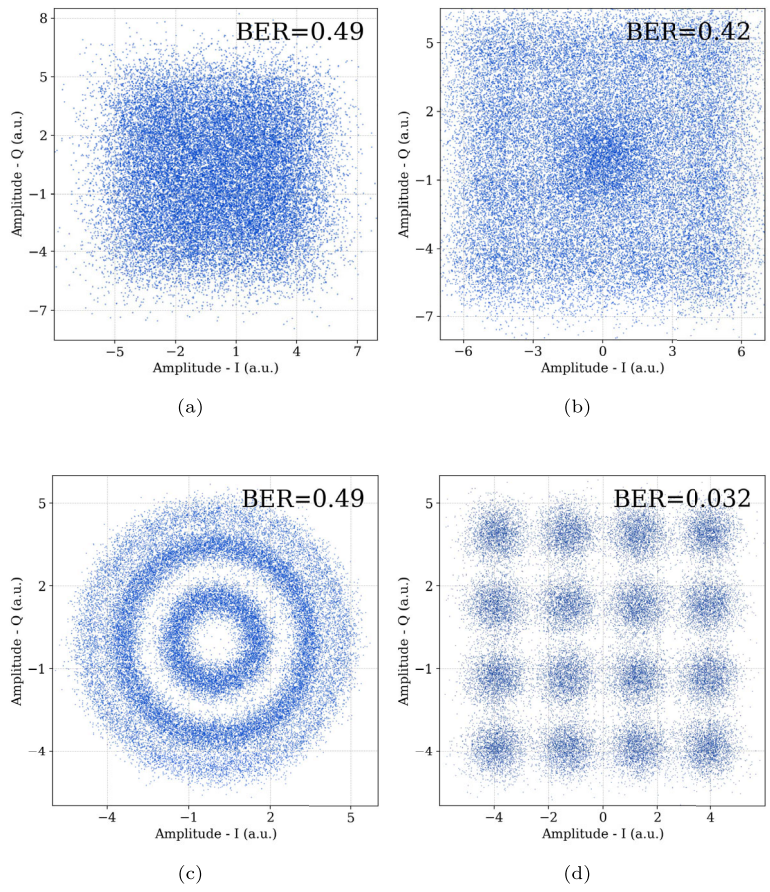


Figure 10 16-QAM constellation recovery under different decryption strategies: (a) no decryption, (b) PSO-only decryption, (c) DO-only decryption, (d) full DDO decryption

the BER is slightly reduced to 42%, this still unequivocally indicates complete decryption failure. This outcome once again strikingly reflects the non-commutative behavior of the DDO, where applying only a partial component of the operator further distorts the signal rather than recovering it.

- **Fig. 10(c): DO-Only Decryption** When only the displacement operator (DO) is utilized at the receiver, the amplitude shifts introduced during encryption are effectively removed. However, the residual, uncorrected PSO encryption causes the constellation points to form four distinct concentric ring-like structures, each corresponding to one of the four amplitude levels inherent in 16-QAM. Although some underlying structure is partially revealed, symbol discrimination remains utterly infeasible, consistently resulting in a BER of 49%. This demonstrates that even with higher-order modulations, partial decryption is inadequate.
- **Fig. 10(d): Full DDO Decryption** When the legitimate receiver applies the correct inverse DDO, incorporating both displacement and phase shift components, the 16-QAM constellation is successfully recovered. Distinct symbol clusters are clearly visible at their expected locations. Due to inherent fiber impairments and system noise, some constellation points exhibit minor distortion, but overall demodulation is highly accurate, achieving an impressive BER of 3.2%. This compelling result

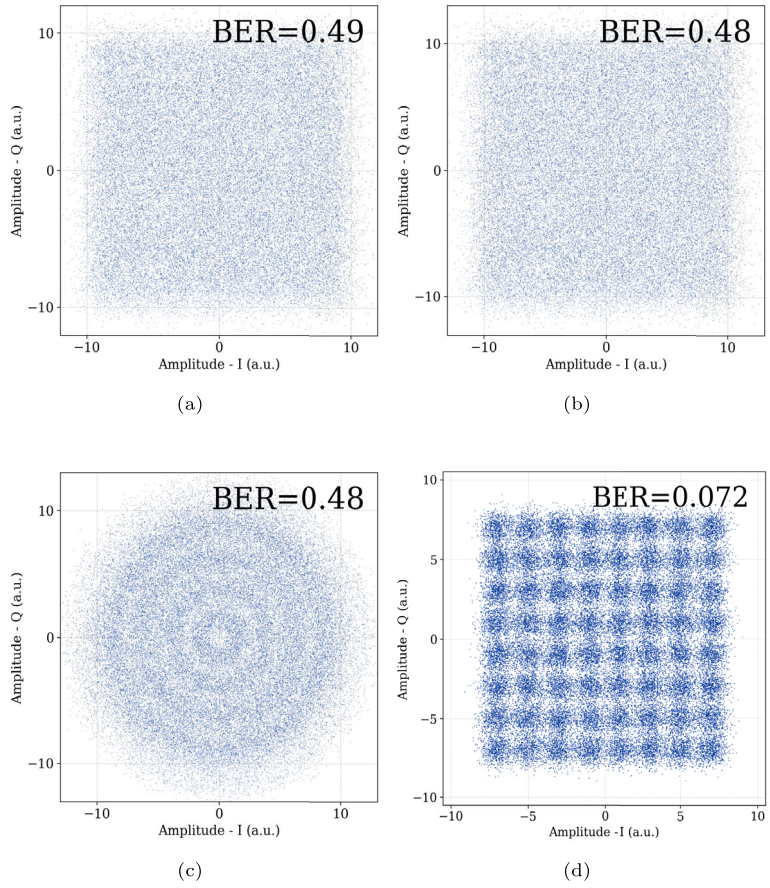


Figure 11 64-QAM constellation recovery under different decryption strategies: (a) no decryption, (b) PSO-only decryption, (c) DO-only decryption, (d) full DDO decryption

definitively validates that the QEPS-dd scheme remains highly effective and robustly secure even when applied to higher-order modulation formats like 16-QAM.

- **Fig. 11(a): No Decryption** For the 64-QAM scenario shown in Fig. 11(a) (No Decryption), the encryption effect is even more pronounced due to the higher symbol density. The undecrypted signal manifests as a dense, cloud-like distribution with high entropy, completely obscuring the 64 distinct constellation points. The measured Bit Error Rate (BER) hovers around the theoretical limit for random guessing, confirming that the DDO encryption scales effectively to conceal information even in high-order, spectrally efficient formats.
- **Fig. 11(b): PSO-Only Decryption** Moving to the PSO-Only Decryption in Fig. 11(b), applying the phase shift operator in isolation fails to recover any meaningful structure. Unlike the lower-order case, the dense packing of 64-QAM means that phase rotation without displacement correction results in significant symbol overlap and chaos. The constellation remains statistically indistinguishable from noise, and the BER stays prohibitively high, reinforcing the fact that security relies on the joint operation of the operator pair rather than individual components.
- **Fig. 11(c): DO-Only Decryption** In the DO-Only Decryption case (Fig. 11(c)), removing the displacement component reveals the amplitude characteristics of the

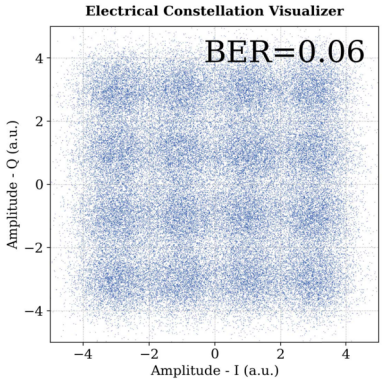


Figure 12 Simulation results for QPP depth $m = 2$

signal but leaves the phase scrambled. Consequently, the constellation collapses into a complex series of concentric rings—more numerous than in the 16-QAM case—corresponding to the multiple amplitude levels inherent to 64-QAM. While this reveals a partial geometric structure, the lack of phase alignment renders symbol discrimination impossible, yielding a BER that is practically equivalent to the fully encrypted state.

- **Fig. 11(d): Full DDO Decryption** Finally, Fig. 11(d) (Full DDO Decryption) demonstrates the successful restoration of the 64-QAM constellation upon applying the correct inverse operators. All 64 symbol clusters are clearly distinct and mapped to their expected grid positions. Although the reduced Euclidean distance between symbols in 64-QAM makes the signal naturally more sensitive to residual noise compared to 16-QAM, the demodulation remains robust. The system achieves a BER well below the FEC threshold, definitively validating the scheme's capability to handle high-order modulations without compromising signal integrity.

These comprehensive results emphatically confirm that the QEPS-dd encryption scheme can be reliably extended beyond QPSK to support more complex constellations such as 16-QAM and 64-QAM. This versatility allows for maintaining both robust data confidentiality and high decryption fidelity in authorized communication systems, even with increased spectral efficiency.

To further validate the scalability of the security framework and address the theoretical model of the Quantum Permutation Pad (QPP)1, we extended the simulation to include a Level-2 QPP ($m = 2$) configuration. In this scenario, the encryption uses a composite of two dynamic displacement operators determined by a permuted index sequence.

The result of the $m = 2$configuration is shown in Figure 12. The authorized receiver, synchronized with the $m = 2$ permutation key, successfully recovers the 16-QAM constellation, albeit with a slightly higher BER compared to the $m = 1$ case. But, the encrypted signal exhibits a higher degree of entropy. This experiment confirms that the simulation platform supports the full QPP protocol, bridging the gap between the physical-layer transmission and the information-theoretic security analysis.

3.4 Key synchronization and pre-shared key distribution

A critical requirement for any practical implementation of QEPS-dd lies in the secure synchronization of the dynamic displacement operator (DDO) parameters—namely, the

displacement amplitude (α) and the phase rotation (ϕ)—between the transmitter and receiver. In this work, the key distribution is realized through a pre-shared key (PSK) mechanism, which represents a mature and fully compatible approach within classical coherent optical communication frameworks.

In the proposed architecture, the transmitter (Alice) and the receiver (Bob) initially establish a shared key table containing ordered pairs of DDO parameters (α_i, ϕ_i), each corresponding to one operator element within the Quantum Permutation Pad (QPP) space. This pre-shared table functions as the fundamental synchronization reference, from which both parties select the identical operator pair during data transmission. A synchronization clock or frame-aligned header signal determines the active index k_t at time t, ensuring deterministic alignment such that both ends apply the corresponding operators:

$$Encryption : \hat{d}(\alpha_{k_t}, \phi_{k_t}), \quad Decryption : \hat{d}^{-1}(\alpha_{k_t}, \phi_{k_t}) \tag{16}$$

This synchronization procedure enables precise temporal matching of encryption and decryption operations without requiring any quantum channel or additional optical hardware. The key index evolution may follow a pre-defined pseudo-random sequence derived from the QPP permutation map, thus introducing time-varying operator dynamics while preserving deterministic reproducibility for legitimate users.

To ensure low implementation overhead and seamless integration with existing infrastructure, the management of the DDO key space follows a two-phase lifecycle compatible with standard secure optical networks:

Phase 1: Physical Initialization (PSK Foundation). Adopting the Pre-Shared Key (PSK) mechanism standard in classical coherent optical networks, the fundamental Look-Up Table (LUT) containing the 96 DDO operator pairs is loaded into the transceiver's secure memory during the physical link establishment phase. This utilizes standard secure provisioning interfaces (e.g., offline key loading), creating a robust "Root of Trust" without requiring the real-time transmission of the full operator coefficients. Given the small size of the operator set (approximately 1 KB), the storage overhead is negligible for modern DSP chips.

Phase 2: Dynamic Runtime Updates. While the foundation is a static PSK, to ensure dynamic security, the selection sequence of these operators is refreshed periodically. This requires only the distribution of a lightweight PRNG seed or Permutation Index to maintain Forward Secrecy. This low-bandwidth update traffic involves negligible data overhead (hundreds of bits) and can be seamlessly supported by an auxiliary management channel, such as a low-rate QKD link, without affecting the high-speed data transmission.

3.5 Error sensitivity analysis

Figure 13 vividly illustrates the bit error rate (BER) as a function of two critical types of decryption errors: displacement operator (DO) mismatches and phase shift operator (PSO) angle deviations. When the decryption operator perfectly matches the encryption operator, the BER remains near zero, unequivocally confirming accurate signal recovery. However, even minor discrepancies in the decryption parameters result in a rapid and severe degradation of performance.

Specifically, PSO angle errors exceeding 5° or incorrect DO index selections cause the BER to escalate sharply, often approaching the random guessing limit of 50%. This steep

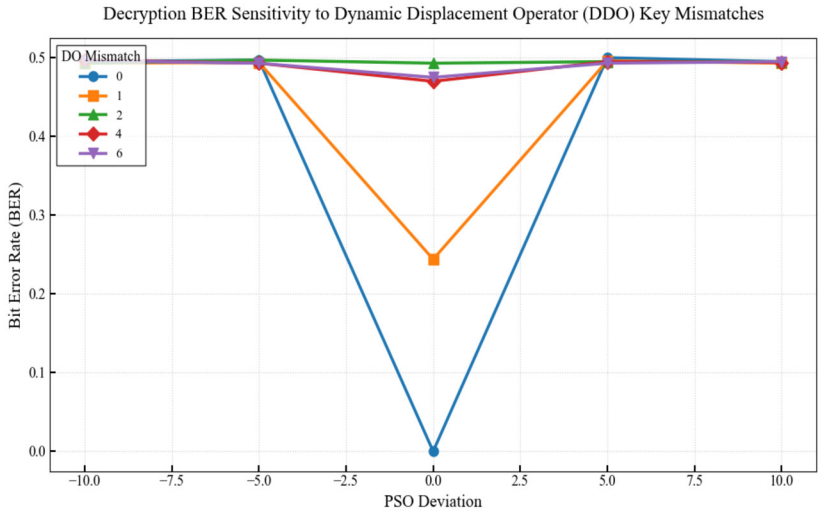


Figure 13 BER as a function of displacement operator (DO) mismatches and phase shift operator (PSO) angle errors. Precise alignment between encryption and decryption parameters is required for reliable communication

rise compellingly indicates that partial or incorrect decryption not only fails to recover the signal but actively increases the randomness and diffusion of the received constellation, rendering unauthorized decryption efforts indistinguishable from noise.

This pronounced sensitivity fundamentally stems from the non-linear and intricate structure of phase-space transformations uniquely introduced by the DDO. Each encrypted symbol is uniquely altered in both amplitude and phase, and only the exact, precise inverse operation can effectively undo the transformation. The results unequivocally emphasize the absolute necessity of strict key synchronization between sender and receiver in practical deployments, further reinforcing the inherent security strength of the QEPS-dd encryption framework.

3.6 BER performance vs. fiber length

Figure 14 comprehensively illustrates the variation of $\log_{10}$(BER) as a function of fiber length, ranging from 50 km to 100 km, under four distinct encryption configurations: no encryption (baseline), phase shift operator (PSO) only, displacement operator (DO) only, and full dynamic displacement operator (DDO) encryption. This analysis provides crucial insights into the scheme's performance over varying transmission distances.

- **No encryption / PSO-only encryption:** These two curves consistently exhibit the lowest BER values across all tested distances. The $\log_{10}$(BER) gradually increases from approximately −5.8 at 50 km to −4.2 at 70 km. Crucially, the BER remains below the industry-standard soft-decision forward error correction (SD-FEC) threshold up to around 85 km, indicating highly reliable communication over medium distances with minimal performance degradation for these less complex scenarios.
- **DO-only encryption:** For this configuration, the BER degradation occurs more rapidly compared to the phase-only or no-encryption cases. The SD-FEC threshold is crossed at approximately 65 km. This reflects the added complexity and increased sensitivity introduced by amplitude (displacement) modulation, which makes the

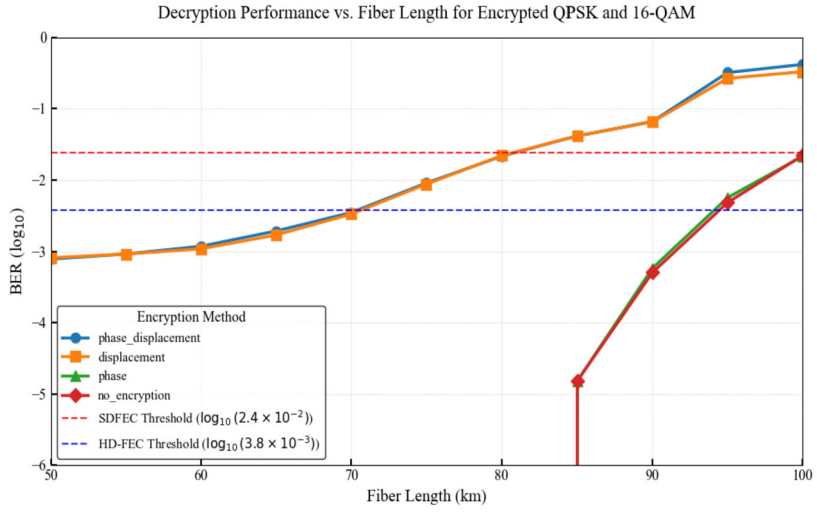


Figure 14 Impact of fiber length and encryption scheme on $\log_{10}$(BER). SD-FEC and HD-FEC thresholds indicate practical performance limits

signal more vulnerable to fiber-induced impairments such as dispersion and attenuation.

- **DDO encryption (phase + displacement):** As anticipated, this comprehensive encryption configuration yields the highest BER among the four schemes. The DDO encryption (phase + displacement) exhibits the highest BER degradation among the tested configurations. Physically, this penalty arises from the expansion of the signal constellation in phase space. Unlike phase-only encryption, which preserves the modulus of the coherent states, the displacement operator shifts symbols to arbitrary positions, often increasing the effective radius (r) of the constellation points. In coherent detection, the impact of phase noise is multiplicative with amplitude; a phase deviation $\Delta\phi$ results in a Euclidean error distance of $\Delta E \approx r \cdot \Delta\phi$. Consequently, displaced symbols with larger radii become significantly more sensitive to laser linewidth and accumulated phase noise during fiber transmission. Furthermore, the expanded constellation requires a higher Optical Signal-to-Noise Ratio (OSNR) to distinguish adjacent symbols after fiber attenuation.regarding the practical transmission limit, the DDO scheme maintains a BER below the Hard-Decision FEC (HD-FEC) threshold (3.8×10^{-3}) up to approximately 70 km. Beyond this distance, the compounded effects of attenuation and phase noise on the expanded constellation cause the BER to exceed correctable limits, necessitating intermediate amplification (EDFA) or advanced carrier phase recovery algorithms for longer reach.

While the DDO scheme inherently exhibits a slightly higher BER under long-distance fiber transmission due to its complex transformations, it simultaneously offers superior encryption strength due to its dual-layer, dynamic transformation of the signal constellation. These results strongly suggest that with further strategic improvements, such as adaptive dispersion compensation, optimized forward error correction, or sophisticated transmitter-side pre-compensation, the effective range of secure communication using DDO-based encryption could be significantly extended, paving the way for its wider practical adoption.

3.7 Security considerations and resistance to cryptanalytic attacks

While the preceding BER analysis empirically demonstrates the encryption robustness of QEPS-dd, a comprehensive evaluation must further examine its resistance to standard cryptanalytic attack models, including known-plaintext and chosen-plaintext attacks. The security of the proposed system originates not merely from statistical obfuscation, but from the non-commutative, state-dependent, and time-varying structure of the Dynamic Displacement Operator (DDO).

In a known-plaintext attack (KPA), an adversary attempts to infer the secret parameters (α, ϕ) by analyzing a large number of plaintext–ciphertext pairs.

Crucially, this mapping is non-linear and jointly dependent on both the encryption operators and the quantum state being encrypted.

Because the displacement and phase-shift operators are non-commutative, the final encrypted state depends not only on the operator parameters $(\alpha_{k_t}, \phi_{k_t})$ but also on the temporal order in which they are applied, as determined by the Quantum Permutation Pad (QPP).Simultaneously, the transformation outcome intrinsically depends on the amplitude and phase of the input coherent state itself.

This dual dependence—on both operator dynamics and signal properties—creates a non-linear, state-dependent mapping in phase space that cannot be expressed as a fixed or invertible analytical function.

As a result, even with extensive collections of known plaintext–ciphertext pairs, an adversary cannot construct a deterministic inverse to recover the underlying operator parameters or predict future ciphertexts. Each symbol is encrypted by a unique, context-dependent transformation jointly defined by the time-varying operators and the signal state, ensuring an exponentially large and dynamically evolving cipher space.

In a chosen-plaintext attack (CPA), the adversary deliberately selects test inputs in an attempt to probe the encryption mechanism. However, the composite operator $\hat{d}(\alpha_{k_t}, \phi_{k_t}) = \hat{d}(\alpha_{k_t})\hat{P}(\phi_{k_t})$ produces ciphertexts whose positions in phase space depend not only on the chosen input but also on the instantaneous values of α_{k_t} and ϕ_{k_t}, which vary pseudo-randomly according to the QPP permutation. Consequently, two identical plaintext states injected at different time indices generate uncorrelated ciphertexts. The resulting ciphertext distribution in the (x_I, x_Q) domain is statistically indistinguishable from a Gaussian noise background, ensuring that plaintext inference via CPA or correlation analysis is infeasible.

From an information-theoretic standpoint, the entropy of the composite operator space scales factorially with the number of available operator pairs. Specifically, for a QPP sequence of length m, the total entropy is approximately $H \approx m \cdot log_2(N!)$. Our new simulation results in Sect. 3.3 (for the $m = 2$ configuration) empirically validate this capability, demonstrating that the system can support these high-entropy states.

This confirms that the computational complexity for an attacker increases exponentially with m, while the physical layer integrity for the legitimate user is maintained. This combination explosion, coupled with the non commutative algebraic structure of DDO, ensures that any incorrect parameter selection will result in cracking failure, thereby eliminating brute force or differential attack attempts.

Security of the Key Infrastructure: To address the security of the Pre-Shared Key (PSK) itself, the QEPS-dd framework employs a layered protection model. The static DDO operator table acts as the system's "Root of Trust" and is stored in tamper-resistant secure

memory within the transceiver hardware. Therefore, physical theft of the key table is equivalent to the physical capture of the communication equipment. Furthermore, the system ensures forward secrecy through the dynamic update of the QPP selection seed. Even if the static table were compromised, an attacker lacking the instantaneous time-varying seed would be unable to reconstruct the correct operator sequence, safeguarding historical and future transmissions.

In summary, the QEPS-dd scheme exhibits multi-layered security:

- **physical concealment through non-commutative phase-space transformations;**
- **algorithmic unpredictability through state-dependent and time-varying encryption;**
- **statistical indistinguishability of ciphertexts under KPA and CPA models.**
- **forward secrecy backed by a hardware-protected root of trust and dynamic seeding.**

Even with complete access to large volumes of plaintext–ciphertext data or partial knowledge of the static infrastructure, an adversary cannot reconstruct the underlying operator parameters or predict future ciphertexts, ensuring a high level of quantum-resilient, physical-layer confidentiality.

Unlike conventional digital encryption, the QEPS-dd framework operates directly in the quantum phase-space formalism, where encryption corresponds to the unitary transformation of coherent states by non-commutative operators. Hence, even though the implementation is classical, the encryption process itself inherits the algebraic properties of quantum mechanics.

4 Conclusion

In this work, we validated a quantum-enhanced physical-layer encryption scheme, termed QEPS-dd, based on the Dynamic Displacement Operator (DDO) [1]. By combining amplitude (displacement) and phase shift transformations in a non-commutative encryption framework, QEPS-dd introduces a novel class of quantum-resistant encryption directly at the physical modulation layer of coherent optical communication systems.

Through comprehensive OptiSystem simulations, we demonstrated the feasibility and robustness of the QEPS-dd architecture under both back-to-back (B2B) and long-distance fiber transmission conditions. The encryption operator space, constructed using 16 displacement levels from 16-QAM and 6 phase angles, forms a 96-element DDO set, which, when permuted into a Quantum Permutation Pad (QPP), enables a cryptographic entropy on the order of $m \cdot \log_2(96!) \approx 508m$ bits—exceeding the security levels of AES-256 even for an $m = 1$ QPP pad. Furthermore, we successfully simulated the QEPS-dd framework with a QPP depth of $m = 2$ for 16-QAM, verifying the scalability of the encryption scheme to higher-complexity key spaces.

Simulation results confirmed that:

- The QEPS-dd scheme successfully obfuscates the signal in both phase and amplitude domains, rendering the constellation patterns indistinguishable without the correct inverse operator.
- Partial decryption using only PSO or DO fails to recover the original signal, and in some cases increases randomness due to the non-commutative structure of the DDO.
- Full decryption using the matching DDO inverse restores the original QPSK or 16-QAM constellation with low BER, confirming the correctness and reversibility of the encryption process.

- BER performance under fiber transmission shows that while DDO encryption incurs slightly higher penalties compared to partial or no encryption, it maintains BER below FEC thresholds up to 70–80 km, validating its viability for secure long-distance communication.
- Sensitivity analysis reveals strong dependence on precise key synchronization, ensuring high resistance to key mismatch and brute-force attacks.

These findings highlight QEPS-dd as a scalable and practical solution for quantum-secure physical-layer encryption in fiber-optic networks. Future work will explore hardware implementation, key management for QPP sequences, and integration with adaptive equalization and FEC schemes to enhance transmission robustness and deployment readiness.

Acknowledgements
The author C. Zhang gratefully acknowledges M. Khalil and A. Chan for generously sharing their MATLAB code used in displacement operator (DO) simulations.

Author contributions
R.K. conceptualized the QEPS DDO protocol and C.Z. performed the simulation implementation. All authors participated in drafting and reviewing the manuscript.

Funding information
This research is supported by the Independent Innovation Science Fund Program of National University of Defense Technology 22-ZZCX-036 and National Youth Science Foundation Project 12204539.

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

Declarations

Ethics approval and consent to participate
Not applicable.

Consent for publication
Not applicable.

Competing interests
The authors declare no competing interests.

Author details
[1]Information Support Force Engineering University, Wuhan, 450007, China. [2]Guangxi Key Laboratory of Multimedia Communications and Network Technology, Guangxi University, Nanning, 530004, China. [3]Research, Quantropi Inc., 1545 Carling Av, Suite 620, Ottawa, K1Z 8P9, ON, Canada.

Received: 11 July 2025 Accepted: 11 February 2026 Published online: 27 February 2026

References

1. Kuang R. Quantum encryption in phase space with dynamic displacement operators and quantum permutation pad. Acad Quantum. 2025;2. https://doi.org/10.20935/AcadQuant7462.
2. Yu J, Zhang J. Recent progress on high-speed optical transmission. Digit Commun Netw. 2016;2(2):65–76. https://doi.org/10.1016/j.dcan.2016.03.002.
3. 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.
4. 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.
5. 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.
6. Zhu Q, Yu X, Zhao Y, Nag A, Zhang J. Resource allocation in quantum-key-distribution- secured datacenter networks with cloud–edge collaboration. IEEE Internet Things J. 2023;10(12):10916–32. https://doi.org/10.1109/JIOT.2023.3242725.
7. Bennett CH, Brassard G. Quantum cryptography: public key distribution and coin tossing. Theor Comput Sci. 2014;560:7–11. https://doi.org/10.1016/j.tcs.2014.05.025. Theoretical Aspects of Quantum Cryptography – celebrating 30 years of BB84.

8. Renner R, Gisin N, Kraus B. Information-theoretic security proof for quantum-key-distribution protocols. Phys Rev A. 2005;72:012332. https://doi.org/10.1103/PhysRevA.72.012332.
9. Djordjevic IB. Physical-layer security and quantum key distribution. 1st ed. Cham: Springer; 2019.
10. Shor PW, Preskill J. Simple proof of security of the bb84 quantum key distribution protocol. Phys Rev Lett. 2000;85:441–4. https://doi.org/10.1103/PhysRevLett.85.441.
11. Rivest RL, Shamir A, Adleman L. A method for obtaining digital signatures and public-key cryptosystems. Commun ACM. 1978;21(2):120–6. https://doi.org/10.1145/359340.359342.
12. Diffie W, Hellman M. New directions in cryptography. IEEE Trans Inf Theory. 1976;22(6):644–54. https://doi.org/10.1109/TIT.1976.1055638.
13. Menezes AJ, Okamoto T, Vanstone SA. Reducing elliptic curve logarithms to logarithms in a finite field. IEEE Trans Inf Theory. 1993;39(5):1639–46. https://doi.org/10.1109/18.259647.
14. Lai J-s, Lin X-y, Qian Y, Liu L, Zhao W-y, Zhang H-y. Deployment-oriented integration of dv-qkd and 100 g optical transmission system. In: Asia communications and photonics conference (ACPC) 2019. Optica Publishing Group; 2019. p. 2–1. https://opg.optica.org/abstract.cfm?URI=ACPC-2019-T2H.1.
15. Qi B. Bennett-brassard 1984 quantum key distribution using conjugate homodyne detection. Phys Rev A. 2021;103:012606. https://doi.org/10.1103/PhysRevA.103.012606.
16. Hui S, Wang D, Wang X, Li Z. Design and implementation of a physical layer optical fiber security communication system based on a zuc stream cipher. Appl Opt. 2024;63(19):5150–8. https://doi.org/10.1364/AO.524900.
17. Shi S, Xiao N. 10-gb/s data transmission using optical physical layer encryption and quantum key distribution. Opt Commun. 2022;507:127603. https://doi.org/10.1016/j.optcom.2021.127603.
18. Gao C, Tang X, Meng Q, Kong W, Chen L, Luan Y, Yang C, Xu H, Cui N, Zhang X. Physical layer encryption for polarization division multiplexing coherent optical communication system based on the rotation of the state of polarization. In: 2021 19th international conference on optical communications and networks (ICOCN). 2021. p. 1–3. https://doi.org/10.1109/ICOCN53177.2021.9563843.
19. Xue C, Xia Y, Chen W, Gu P, Zhang Z. Physical-layer security of optical communication based on chaotic optical encryption without an additional driving signal. Opt Lett. 2023;48(10):2611–4. https://doi.org/10.1364/OL.487627.
20. Zhao A, Jiang N, Liu S, Zhang Y, Qiu K. Physical layer encryption for wdm optical communication systems using private chaotic phase scrambling. J Lightwave Technol. 2021;39(8):2288–95. https://doi.org/10.1109/JLT.2021.3051407.
21. Rothe S, Koukourakis N, Radner H, et al. Physical layer security in multimode fiber optical networks. Sci Rep. 2020;10:2740. https://doi.org/10.1038/s41598-020-59625-9.
22. 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.
23. 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.
24. 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.
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 Publishing 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 Publishing Group; 2022. p. 3–4. https://doi.org/10.1364/CLEO_SI.2022.SF4L.3.
27. 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.
28. 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.
29. 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.
30. Khalil M, Chan A, Plant DV, Chen LR, Kuang R. Experimental demonstration of quantum encryption in phase space with displacement operator in coherent optical communications. EPJ Quantum Technol. 2024;11(1). https://doi.org/10.1140/epjqt/s40507-024-00260-y.

Publisher's note