ACADEMIA QUANTUM

Research article
Published: 2025-01-06
https://doi.org/10.20935/AcadQuant7462

Quantum encryption in phase space with dynamic displacement operators and quantum permutation pad

Randy Kuang[1,*]

Academic Editors: Guilherme Temporao, Steven K. Lamoreaux

Abstract

We propose the Dynamic Displacement Operator (DDO) as part of Quantum Encryption in Phase Space (QEPS-dd), a novel scheme for securing coherent optical communications using Quadrature Amplitude Modulation (QAM). In this framework, the K-QAM encoding is modeled as a quantum operator, with its constellation points forming the eigenbasis. The encoding and decoding processes are treated as operations of this quantum operator on its eigenstates, ensuring coherent communication via digital signal processing at both the transmission and reception sides. The DDO combines a displacement operator and a phase-shift operator, producing dynamic effects that enhance the randomization of the cipher constellation, thus significantly improving communication security. To further strengthen encryption, we introduce the Quantum Permutation Pad (QPP), which randomizes the DDO basis. Together, these components offer robust protection against both classical and quantum attacks. Our security analysis shows that the most effective attack is a brute-force search for the secret DDO pad, with a computational complexity of $\mathcal{O}(2^{\ell}!)$, where ℓ represents the bit length of the DDO pad. As ℓ increases, the factorial growth in complexity makes the system resistant to classical methods and quantum algorithms such as Grover's search. Building on prior experimental results with phase- shift (QEPS-p) and displacement (QEPS-d) operators, we propose that QEPS-dd can be implemented for high-speed quantum-secure communication over existing optical networks, offering a practical solution for enhancing communication security.

Keywords: *phase space, phase-shift operator, displacement operator, quantum encryption, quantum permutation pad (QPP), quadrature amplitude modulation (QAM)*

Citation: Kuang R. Quantum encryption in phase space with dynamic displacement operators and quantum permutation pad. *Academia Quantum* 2025;2. https://doi.org/10.20935/AcadQuant7462

1. Introduction

Quantum Key Distribution (QKD) has emerged as a leading cryptographic technology, leveraging quantum mechanics to secure communication against the growing threat of quantum computing [1–4]. Unlike classical encryption methods, which rely on the computational complexity of mathematical algorithms [5–7], QKD exploits the unique properties of quantum states—particularly superposition and entanglement—to establish cryptographic keys. QKD enables secure key exchange by encoding information in the quantum states of photons, where any eavesdropping attempt inevitably disturbs the system, thereby alerting the communicating parties. This intrinsic reliance on quantum indeterminacy offers unparalleled security, positioning QKD as a promising solution for safeguarding communications in the quantum era.

While QKD has made significant advancements, particularly with the development of Twin-Field QKD (TF-QKD) [8–11], which extends the distribution range beyond 800 km, most protocols remain focused on using single photons as qubits. The concept of high-dimensional QKD was introduced by Buttler, Lamoreaux, and Torgerson in 2012 [12], proposing a four-dimensional (D = 4) QKD protocol that combines polarization, phase, and time-bin encoding to generate up to 20 distinct quantum states. Unlike traditional two-dimensional protocols such as BB84, this high-dimensional approach enhances both security and transmission efficiency. Designed for practical implementation with existing time- and polarization-encoded technologies, the protocol is error-tolerant and robust for real-world applications, achieving a raw bit rate of two bits per detection and, under ideal conditions, a qubit rate of one per transmission.

Since its inception, high-dimensional QKD has seen further theoretical and experimental advancements [13–17]. Some QKD protocols have also integrated coherent detection techniques [2, 18, 19], similar to those used in optical communication systems. However, it is important to note that QKD is designed primarily for establishing shared secret keys and does not directly encrypt data.

Coherent optical communications have become a cornerstone of modern optical infrastructure, driving high-speed data transmission systems since their early development [20–22]. These advancements have been particularly propelled by the adoption

[1]Research, Quantropi Inc., Ottawa, ON K1Z 8P9, Canada.
[*]email: randy.kuang@quantropi.com

of coherent detection technologies, which enhance signal detection efficiency in optical networks [23–25]. Coherent detection allows the extraction of both amplitude and phase information from modulated optical signals, improving data rates, spectral efficiency, and long-distance signal resilience.

As coherent optical communication continues to advance, the need for robust physical-layer security has become increasingly important. Various encryption schemes have been proposed to address these concerns. In 2021, Peng et al. introduced a method based on Structured Random Light, which uses light-field manipulation to secure optical channels [26], making it difficult for unauthorized parties to decode the transmitted data. In 2022, Wu et al. proposed a hybrid chaotic encryption scheme utilizing a dual-polarization IQ modulator to enhance security [27]. In 2023, Zhao et al. developed a traceless encryption approach that transforms a standard QPSK scheme into more complex modulation formats [28], further enhancing signal obfuscation.

These advances mark important progress in securing coherent optical communications at the physical layer. However, challenges remain in achieving scalable and practical encryption schemes that can operate seamlessly with the existing infrastructure.

Building on these developments, Quantum Encryption in Phase Space (QEPS) was first proposed by Kuang and Bettenburg in 2020 [29]. Unlike QKD, which relies on single photons and dual quantum and classical communication channels, QEPS uses coherent states of quantum harmonic oscillators [30] and operates entirely within the optical domain. This makes QEPS highly compatible with existing coherent optical communication infrastructures, leveraging well-established technologies for signal generation, modulation, and detection. QEPS requires only a single optical channel for key distribution and symmetric encrypted data communications, with successfully demonstrated early implementations of phase shift–based QEPS (QEPS-p) [31].

In 2023, Kuang and Chan extended the QEPS framework by introducing displacement operators (QEPS-d), offering a new level of security through randomized displacements in phase space [32]. This approach was experimentally validated by Khalil et al. in 2024 [33].

This article further advances QEPS encryption by introducing Dynamic Displacement Operators (DDOs). DDOs combine static displacement and phase-shift operators to generate dynamic randomization effects on coherent states, enhancing security. In our model, Quadrature Amplitude Modulation (QAM) is treated as a quantum mechanical system, where a K-QAM encoding operator, denoted as $\hat{Q}_K$, acts on a set of K constellation points or basis states, $|\beta_1\rangle, \ldots, |\beta_K\rangle$. This enables the treatment of QEPS-p, QEPS-d, and QEPS-dd as quantum operators acting on the K-QAM basis, resulting in randomized cipher constellations. To decrypt these constellations and restore the original K-QAM basis with minimal Bit Error Rate (BER), shared secret operators are required.

The detailed structure and operation of QEPS encryption are explored in Section 2, followed by an analysis of its security. We conclude with a discussion of future directions in Section 3.

2. Quantum encryption in phase space

In this section, we begin by introducing the quantum interpretation of coherent communications using QAM encoding operators (Section 2.1). We then explore QEPS encryption based on phase-shift and displacement operators (Section 2.2). The focus then shifts to QEPS encryption with DDOs and Quantum Permutation Pad (QPP) (Section 2.3), where we delve into the novel mechanism behind DDO together with QPP. Lastly, we present a comprehensive security analysis (Section 2.5), evaluating the robustness of the proposed encryption schemes against both classical and quantum attacks.

2.1. Quantum interpretation of coherent optical communications

An optical coherent state is a quantum state associated with the Quantum Harmonic Oscillator (QHO) [30]. It can be described using the displacement operator $\hat{D}(\alpha)$, which shifts the vacuum state $|0\rangle$ to a coherent state $|\alpha\rangle$:

$$|\alpha\rangle = \hat{D}(\alpha)|0\rangle. \tag{1}$$

In this expression, α is a complex number that encodes both the amplitude and phase information of the coherent state. Specifically, $\alpha = re^{i\phi}$, where $r = |\alpha|$ represents the amplitude and ϕ is the phase.

This coherent state can also be represented as a complex modulation, $\alpha = x_I + ix_Q$, where x_I and x_Q are the in-phase and quadrature components, respectively, in the phase space. This representation is fundamental to coherent optical communications, where modulation and demodulation are performed based on these components.

The advancements in digital signal processing (DSP) modules have simplified the implementation of coherent optical communication systems, as shown in **Figure 1**. The DSP handles signal compensations and corrections, enabling the mapping of digital data onto a QAM basis for transmission. At the receiver, the data are demapped to retrieve the transmitted digital information.

Figure 1 illustrates a 16-QAM constellation, where 16 coherent states $\{|\beta_1\rangle, \ldots, |\beta_{16}\rangle\}$ are used for both transmission and reception. These states represent a set of points in the phase space, each corresponding to a unique combination of amplitude and phase.

In quantum mechanics, K-QAM encoding and decoding can be viewed as the action of a K-QAM encoding operator $\hat{Q}_K$ on an eigenbasis $\{|\beta_1\rangle, \ldots, |\beta_K\rangle\}$:

$$\hat{Q}_K|\beta_k\rangle = \beta_k|\beta_k\rangle, \quad k \in [1, K]. \tag{2}$$

Thus, operators like $\hat{Q}_{16}$, $\hat{Q}_{32}$, $\hat{Q}_{64}$, etc. correspond to different K-QAM communication schemes (16-QAM, 32-QAM, 64-QAM, etc.). Equation (2) implies that an eavesdropper could potentially intercept the communication and measure it using the same standard eigenbasis. While an eavesdropper may not know the specific basis used, they can attempt different bases and disregard those that yield a high BER.

It is important to distinguish between the K-QAM encoding operator $\hat{Q}_K$ and the annihilation operator $\hat{a}$, which also acts on coherent states. Coherent states are eigenstates of the annihilation operator, i.e., $\hat{a}|\beta\rangle = \beta|\beta\rangle$, but the K-QAM encoding operator $\hat{Q}_K$ has

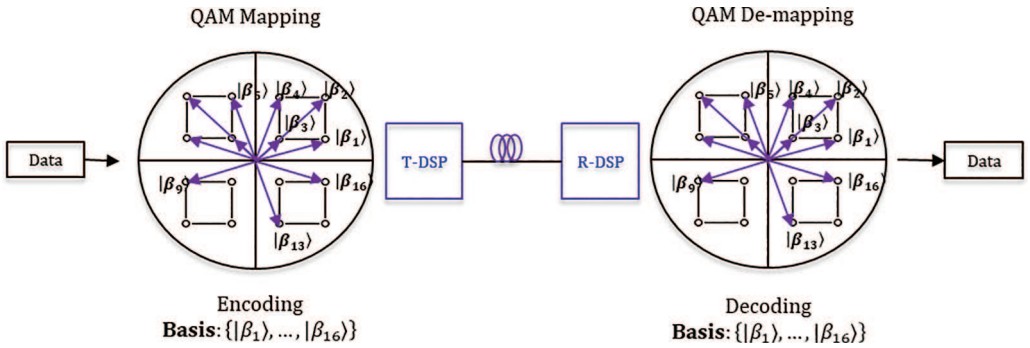

Figure 1 • Coherent optical communication illustrated using 16-QAM modulation. Digital data are first mapped onto a constellation diagram for transmission. In 16-QAM, there are 16 dots distributed across four quadrants, each representing a coherent state $|\beta_i\rangle$, where $i = 1, \ldots, 16$. The digital signal processing (DSP) on both the transmission side (T-DSP) and the receiving side (R-DSP) works together to maintain an acceptable bit error rate (BER) and recover digital data based on the received constellation diagram.

only K specific eigenstates as its basis. This difference is crucial for understanding the unique behavior of K-QAM communication.

Moreover, different K-QAM operators do not commute:

$$\hat{Q}_K \hat{Q}_{K'} \neq \hat{Q}_{K'} \hat{Q}_K. \tag{3}$$

This non-commutability is significant because it implies that coherent QAM communication must occur within the same eigenbasis. Using a different basis for reception, such as a 32-QAM operator when a 16-QAM operator was used for transmission, can result in a maximum 50% BER. This non-commutativity can be interpreted as a generalized uncertainty principle for coherent communications, distinguishing it from the uncertainty principle that governs QKD with single-photon qubits.

2.2. Quantum encryption in phase space with phase-shift and displacement operators

Kuang and Bettenburg introduced the concept of using random phase-shift operators to encrypt coherent states in phase space in 2020, called QEPS-p [29]. Since its proposal, simulations and experiments validating QEPS-p have been published [31,34]. The encryption process involves selecting a set of random phases $\{\phi_1, \ldots, \phi_n\}$, which form corresponding phase-shift operators $\{\hat{\varphi}(\phi_1), \ldots, \hat{\varphi}(\phi_n)\}$. The QEPS-p encryption for a coherent state can be mathematically expressed as follows:

$$\hat{\varphi}(\phi_j)|\beta_k\rangle = |e^{-i\phi_j}\beta_k\rangle. \tag{4}$$

which results in the rotation of the complex vector β_k by a phase angle ϕ_j around the origin in the phase space.

In the context of a 16-QAM basis, as shown in **Figure 2**, the encryption with QEPS-p is illustrated. In **Figure 2a**, two phase-shift operators, $\hat{\varphi}(\phi_1)$ and $\hat{\varphi}(\phi_2)$, are used to randomly rotate the constellation points around the origin. **Figure 2b** depicts the effect of applying a set of random phase shifts, resulting in a randomized constellation where the basis coherent states form rings around the origin, with the radii corresponding to the amplitudes.

Attempting to decode the encrypted coherent states with a standard K-QAM basis would lead to a BER close to 50% due to the relationship:

$$\hat{Q}_K|e^{-i\phi_j}\beta_k\rangle \neq \beta_k|\beta_k\rangle, k \in [1, K], j \in [1, n], \tag{5}$$

because the cipher coherent state $|e^{-i\phi_j}\beta_k\rangle$ is no longer a basis eigenstate of $\hat{Q}_K$. However, a receiver that possesses the shared secret of the phase-shift operators can correctly restore the original K-QAM constellation with an acceptable BER:

$$\hat{\varphi}^{-1}(\phi_j)|e^{-i\phi_j}\beta_k\rangle = |e^{i\phi_j}e^{-i\phi_j}\beta_k\rangle = |\beta_k\rangle, k \in [1, K], j \in [1, n], \tag{6}$$

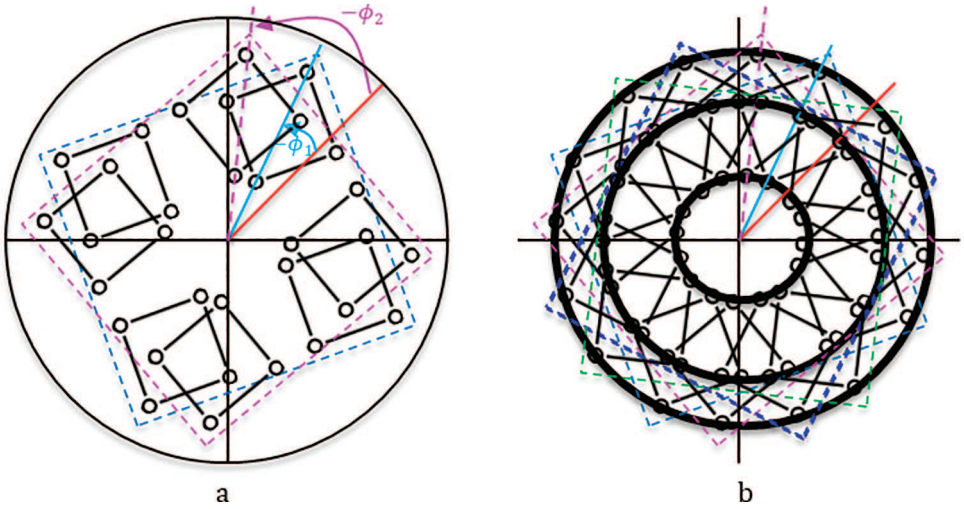

Figure 2 • QEPS-p encryption illustrated with a 16-QAM modulation scheme. (a) A typical 16-QAM basis randomly rotated around the origin by two phase-shift operators, $\hat{\varphi}(\phi_1)$ and $\hat{\varphi}(\phi_2)$. (b) A random constellation resulting from QEPS-p encryption with a set of random phase-shift operators, where the three rings indicate the three amplitudes in the 16-QAM.

indicating that the phase-shift operator is unitary and reversible. Originally, Kuang and Bettenburg proposed QEPS-p as a public key scheme with a self-shared secret for round-trip coherent communication [29], using the Phase-Shift Keying scheme then for symmetric encryption with QPSK [34]. Tapping optical signals from QEPS-p-encrypted communications would only reveal the data modulation scheme from the number of rings, as shown in **Figure 2**, where three rings represent three amplitudes in 16-QAM. This makes it impossible for an attacker to extract the digital data except for knowing that the data modulation scheme is 16-QAM.

In 2023, Kuang and Chan introduced a reduced displacement operator, denoted as $\hat{d}(\alpha)$, by omitting the global phase factor, which has no effect on the measurements of coherent states, when a displacement operator acts on a coherent state [32]. This operator is defined as follows:

$$\begin{aligned} \hat{d}(\alpha)|\beta\rangle &= |\alpha+\beta\rangle, \\ \hat{d}(\beta)|\alpha\rangle &= |\alpha+\beta\rangle, \\ \rightarrow \hat{d}(\alpha)\hat{d}(\beta) &= \hat{d}(\beta)\hat{d}(\alpha). \end{aligned} \tag{7}$$

Kuang and Chan proposed using a set of random displacement operators $\hat{d}(\alpha_i)$, where $i \in [1, m]$, for the encryption of a K-QAM basis $\{|\beta_1\rangle, \ldots, |\beta_K\rangle\}$, resulting in a random cipher basis:

$$\hat{d}(\alpha_i)|\beta_j\rangle = |\alpha_i+\beta_j\rangle. \tag{8}$$

This cipher basis is no longer an eigenbasis of the K-QAM encoding operator $\hat{Q}_K$:

$$\hat{Q}_K|\alpha_i+\beta_j\rangle \neq (\alpha_i+\beta_j)|\alpha_i+\beta_j\rangle. \tag{9}$$

From a quantum mechanical perspective, any attempt to receive the ciphered coherent states, encrypted with QEPS-d, using a K-QAM basis would result in a BER close to 50%, making it impossible to extract any digital data.

However, the original K-QAM eigenbasis can be restored once the set of encryption operators is shared with the receiver, allowing for QEPS decryption:

$$\hat{d}^{-1}(\alpha_i)|\alpha_i+\beta_j\rangle = |-\alpha_i+\alpha_i+\beta_j\rangle = |\beta_j\rangle, \quad j \in [1, K]. \tag{10}$$

This means that a scheme of QEPS with random displacement operators, or QEPS-d, can be established between peers with a secretly shared set of displacement operators. The experimental implementation of the QEPS-d scheme has been recently reported by Khalil et al. [33], achieving line speeds of 224 Gbps, 448 Gbps, and 560 Gbps for QPSK, 16-QAM, and 32-QAM, respectively.

Figure 3 illustrates a typical 16-QAM constellation displaced by two displacement operators $\hat{d}(\alpha_1)$ and $\hat{d}(\alpha_2)$. The figure clearly shows that a displacement operator $\hat{d}(\alpha_i)$ displaces the entire constellation by a complex vector α_i in phase space. A set of randomly selected displacement operators would produce a random constellation diagram, making it impossible to restore the K-QAM basis

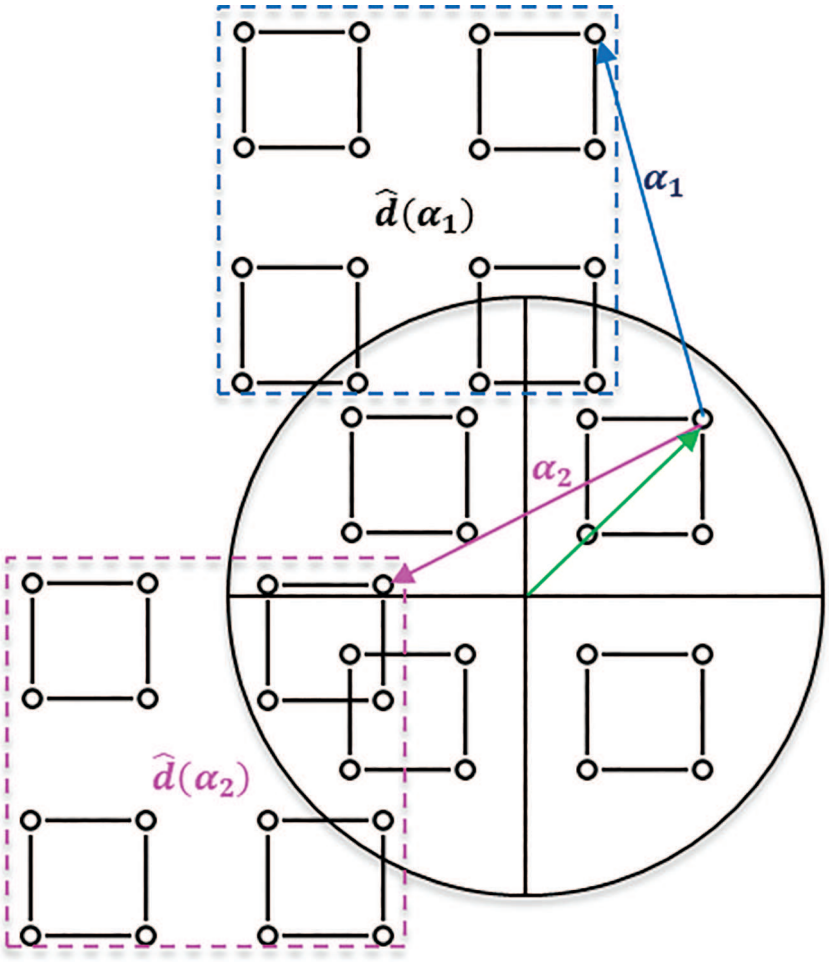

Figure 3 • QEPS-d encryption illustrated with a 16-QAM modulation scheme. The diagram shows a typical 16-QAM basis displaced upward by a displacement operator $\hat{d}(\alpha_1)$ and downward to the lower left by a displacement operator $\hat{d}(\alpha_2)$.

constellation without knowing the secret displacement operators used in transmission. Unlike QEPS-p, QEPS-d encryption does not produce any rings in the cipher constellation, meaning that tapping the communication channel would not reveal the type of K-QAM modulation used in transmission.

2.3. Quantum encryption in phase space with dynamic displacement operators and quantum permutation pad

Both the phase-shift $\hat{\varphi}(\phi)$ and displacement $\hat{d}(\alpha)$ operators are considered static operators in the context of quantum mechanics. When applied to different coherent states, these operators have predictable, consistent effects: the phase-shift operator $\hat{\varphi}(\phi)$ changes the phase of any coherent state $|\beta\rangle$ by a fixed phase angle ϕ, while the displacement operator $\hat{d}(\alpha)$ performs a complex vector addition between the displacement α and the target coherent state β.

However, a more versatile operator can be created by combining the displacement and phase-shift operators into a single entity:

$$\hat{d}(\alpha,\phi) = \hat{d}(\alpha)\hat{\varphi}(\phi). \tag{11}$$

When this joint operator $\hat{d}(\alpha,\phi)$ acts on a coherent state $|\beta\rangle$, the resulting state is given by

$$\begin{aligned}\hat{d}(\alpha,\phi)|\beta\rangle &= \hat{d}(\alpha)|e^{-i\phi}\beta\rangle = |\alpha + e^{-i\phi}\beta\rangle \\ &= \hat{d}(\alpha + (e^{-i\phi}-1)\beta)|\beta\rangle.\end{aligned} \tag{12}$$

Equation (12) shows that the joint operation or encryption by $\hat{d}(\alpha,\phi)$ is effectively equivalent to a new displacement operator $\hat{d}(\alpha + (e^{-i\phi}-1)\beta)$, which depends on the target coherent state $|\beta\rangle$. In other words, the displacement performed by $\hat{d}(\alpha,\phi)$ is not fixed but dynamically varies based on the specific coherent state it is applied to:

$$\hat{d}(\alpha,\phi) \to \hat{d}(\alpha + (e^{-i\phi}-1)\beta). \tag{13}$$

This is why we refer to $\hat{d}(\alpha,\phi)$ as a DDO—its outcome is contingent upon the target coherent state. The dynamic nature of this operator introduces an additional layer of complexity and randomness to the cipher constellation, thereby enhancing the security of the QEPS encryption scheme.

To decrypt a received cipher coherent state that has been encrypted using the DDO $\hat{d}(\alpha,\phi)$, the receiver must apply the inverse of the DDO, defined as $\hat{d}^{-1}(\alpha,\phi) = \hat{\varphi}^{-1}(\phi)\hat{d}^{-1}(\alpha)$. The decryption process is given by

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

demonstrating that the original coherent state is fully recovered.

Figure 4 illustrates the effect of the DDO $\hat{d}(\alpha,\phi)$. The diagram shows two different target coherent states $|\beta\rangle$ and $|\beta'\rangle$ subjected to the same DDO $\hat{d}(\alpha,\phi)$. The resultant equivalent displacement operators, as depicted in the figure by brown solid and dashed lines, are different from the target states $|\beta\rangle$ to $|\beta'\rangle$, highlighting the dynamic nature of the displacement operation. This dynamic feature of $\hat{d}(\alpha,\phi)$ further randomizes the cipher constellation and significantly boosts the security of the QEPS encryption scheme.

The most significant characteristic of DDOs is their inherent non-commutativity, which is crucial in understanding their behavior and implications. This non-commutativity can be mathematically expressed as follows:

$$\begin{aligned}&\hat{d}(\alpha',\phi')\hat{d}(\alpha,\phi)|\beta\rangle = \hat{d}(\alpha',\phi')|\alpha + e^{-i\phi}\beta\rangle \\ &= |\alpha' + e^{-i\phi'}[\alpha + e^{-i\phi}\beta]\rangle, \\ &\hat{d}(\alpha,\phi)\hat{d}(\alpha',\phi')|\beta\rangle = \hat{d}(\alpha,\phi)|\alpha' + e^{-i\phi'}\beta\rangle \\ &= |\alpha + e^{-i\phi}[\alpha' + e^{-i\phi'}\beta]\rangle.\end{aligned} \tag{15}$$

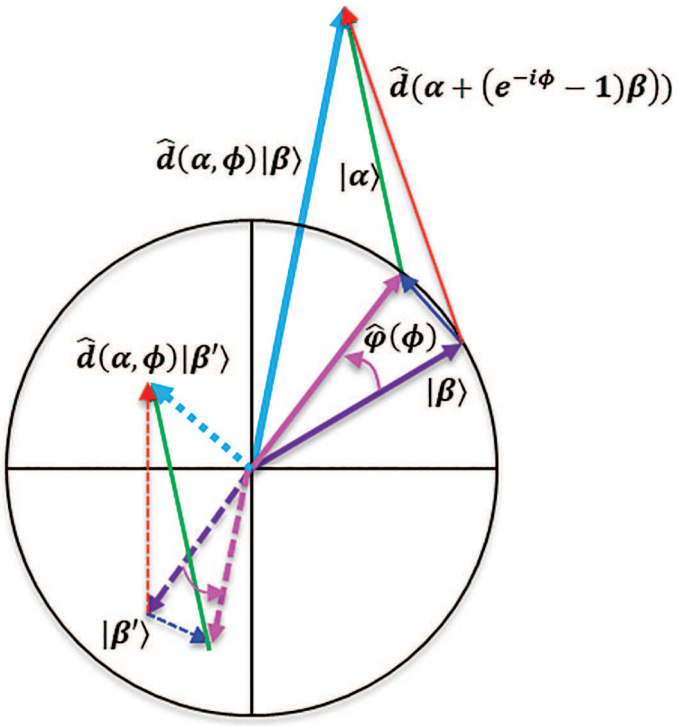

Figure 4 • QEPS-dd encryption illustrated with two coherent states $|\beta\rangle$ and $|\beta'\rangle$. The diagram shows that a dynamic displacement operator $\hat{d}(\alpha,\phi)$ is applied to a target coherent state $|\beta\rangle$ (top right) and then to a different target coherent state $|\beta'\rangle$ (lower left). The different resultant coherent states underscore the dynamic nature of the operator.

This shows that the order in which the DDOs are applied affects the outcome, leading to different resultant states. Such non-commutativity is not a trivial feature; rather, it implies a fundamental limitation on the simultaneous knowledge or precise control of the parameters α and ϕ. This can be formally represented as follows:

$$[\hat{d}(\alpha,\phi),\hat{d}(\alpha',\phi')] \neq 0, \tag{16}$$

indicating that the operators do not commute unless $\alpha = \alpha'$ and $\phi = \phi'$. This non-commutativity introduces a generalized uncertainty principle in the context of DDOs, which has significant implications for the security of the QEPS-dd encryption scheme.

In practical terms, this uncertainty principle enhances the security of the QEPS-dd encryption. An attacker attempting to intercept or decode the encrypted cipher coherent states would face the challenge of dealing with the non-commutative nature of the operators. This would necessitate a brute-force search over the entire space of α and ϕ parameters for acceptable BER, exponentially increasing the difficulty of breaking the encryption. Thus, the non-commutativity of DDOs plays a crucial role in reinforcing the robustness and security of the QEPS-dd encryption scheme.

The DDO effectively addresses the limitations associated with traditional phase-shift and displacement operators. Specifically, while phase-shift operators may unintentionally reveal information about the encoding of QAM schemes such as the amplitudes of coherent states and static displacements applied by displacement operators, DDOs offer a more secure alternative. In scenarios where only a single displacement operator is used, the encryption provided by QEPS can often be reversed or corrected using DSP modules.

However, the introduction of DDOs, even in configurations with just a single static displacement operator paired with multiple phase-shift operators, significantly enhances the robustness of QEPS encryption. This increased security arises from the dynamic nature of the DDOs, which vary the displacements in a way that makes it impossible for DSP modules to decode or correct the encrypted signal, thus maintaining the confidentiality of the QAM scheme and protecting it against potential attacks.

By incorporating DDOs into the encryption process, the complexity is greatly increased, making it much more challenging for an adversary to reverse-engineer or bypass the QEPS encryption, even in cases where a combination of static displacements and phase shifts is used.

To maximize security, a selected set of DDOs, known as the DDO Pad (DDOP), can be optimized using the QPP [35, 36], which is a method proposed by Kuang and his colleagues for both classical and quantum computing implementations. The DDOP can be constructed using a publicly known m-QAM scheme and n-PSK as follows:

$$\begin{aligned}&\{\hat{d}(\alpha_1,\phi_1),\ldots,\hat{d}(\alpha_m,\phi_1),\ldots,\hat{d}(\alpha_1,\phi_n),\ldots,\hat{d}(\alpha_m,\phi_n)\} \rightarrow \\ &\{DD[0],\ldots,DD[r=m*(j-1)+i-1]=\hat{d}(\alpha_i,\phi_j),\ldots,DD[R]\},\end{aligned} \tag{17}$$

where $R = m \times n - 1$ is the total number of DDO operators. For example, a DDO base might contain 64, 128, or 256 DDO operators for $m = n = 8$, $m = 16$ and $n = 8$, and $m = n = 16$, respectively. To maximize the number of constellation points, it is recommended to adjust the phase angle ϕ_j with a random phase shift: $\phi_j = \frac{2\pi}{n}j + \delta_j$, where $j \in [1, n]$ and $\delta_j < \frac{2\pi}{n}$. Under this configuration, QEPS encryption using the entire set of DDO base operators transforms a standard K-QAM constellation into a random constellation with a maximum of $m \times n \times K$ constellation points. However, using a publicly known DDO base for encryption would allow an attacker to decrypt the QEPS using the same DDO base.

To enhance security, a shared random secret s can be employed to select DDO operators from the DDO base. Assuming $m \times n = 2^\ell$, the secret can be segmented into portions $\{s_i\}$ of ℓ bits, with each s_i representing the decimal value of the i-th segment. This effectively converts the secret s into a DDOP $\{DD[s_i]\}$. The length of the secret is determined by the required level of security. The DDOP generated in this manner may have some DDO operators appearing multiple times, while others may not be selected at all, resulting in a cipher constellation with fewer points than $m \times n \times K$ for the K-QAM scheme.

We advocate using quantum permutation to transform the DDO base into a DDOP. For an ℓ-bit quantum computing base $\{|0\rangle, |1\rangle, \ldots, |2^\ell - 1\rangle\}$, there are $2^\ell!$ possible quantum permutations $\hat{p}_i$. Each permutation $\hat{p}_i$ can uniformly randomize the order of the base states:

$$\hat{p}\{|0\rangle, |1\rangle, \ldots, |2^\ell - 1\rangle\} = \{|p(0)\rangle, |p(1)\rangle, \ldots, |p(2^\ell - 1)\rangle\}.$$

This implies that each base state appears with equal probability. By treating the DDO base indexes as an ℓ-bit computing base, we obtain

$$\begin{aligned}&\hat{p}\{|0\rangle,\ldots,|R\rangle\} = \{|p(0)\rangle,\ldots,|p(R)\rangle\} \\ &\{DD[0],\ldots,DD[R]\} \longrightarrow \{DD[p(0)],\ldots,DD[p(R)]\}.\end{aligned} \tag{18}$$

The DDOP derived from this quantum permutation maximizes the cipher constellation points for any K-QAM scheme and ensures the highest level of security for QEPS encryption. A shared secret s should be of sufficient length to satisfy the security requirements. The maximum secret length for a quantum permutation is $\ell \times 2^\ell$ bits, with an effective entropy of $\log_2(2^\ell!)$ bits. For example, when $\ell = 8$, the maximum secret length is 2048 bits for a single quantum permutation, with an effective entropy of 1864 bits. In specific implementations, such as the one described in QEPS-d [33], a DDOP can be treated as a codeword. Repeating the process described in Eq. (18) allows for the creation of multiple DDOPs, thereby enhancing security.

2.4. Possible implementation

An example implementation using QEPS-dd encryption is illustrated in **Figure 5**, with further technical and experimental validation details provided by Khalil et al.[33]. This implementation demonstrates the integration of QEPS-dd into an optical communication system, emphasizing its feasibility in real-world conditions. The DSP modules on both the transmission and receiving sides, enclosed in dashed rectangles, ensure the correct transmission and reception of coherent states. Source digital data are first processed with QAM mapping (constellation) and then encrypted with QEPS-dd before being transmitted over fiber via DSP-T. On the receiving side, DSP-R modules handle compensations and corrections before QEPS-dd decryption restores the correct QAM base for QAM de-mapping. The experimental results show that the system consistently achieves acceptable BER thresholds, confirming reliable data recovery. The data analysis, which includes BER measurements and QAM constellation assessments, validates the

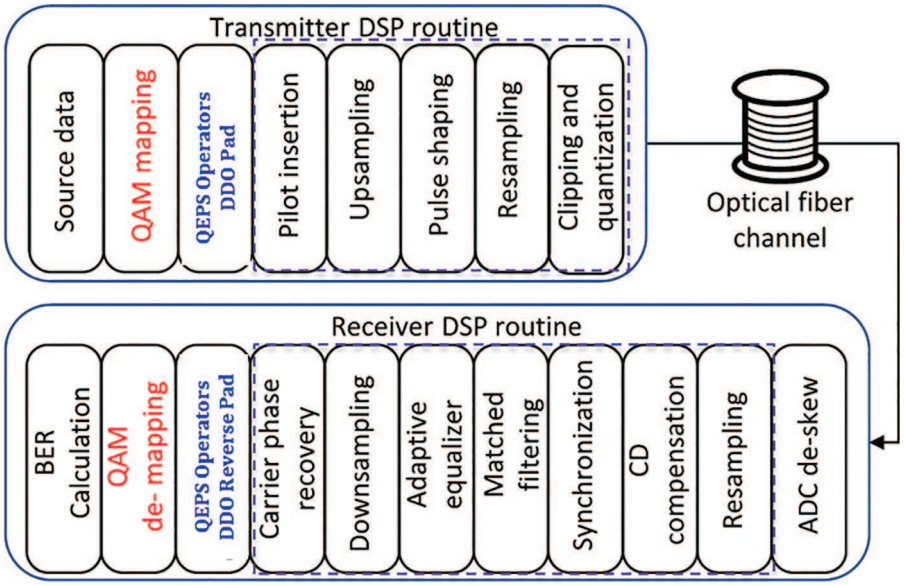

Figure 5 • An implementation using QEPS-dd encryption is illustrated based on [33]. DSP, digital signal processing; QAM, quadrature amplitude modulation; QEPS, quantum encryption in phase space; DDO, dynamic displacement operator; BER, bit error rate; CD, chromatic dispersion; ADC, analog-to-digital conversion.

robustness of the proposed scheme. Additionally, ongoing research aims to address practical implementation challenges such as synchronization, noise resilience, and hardware optimization, ensuring scalability and applicability in broader optical network environments.

2.5. Security of QEPS-dd encryption

The DDO, a key component in QEPS-dd encryption, does not commute with the K-QAM encoding operator $\hat{Q}_K$, as described in Eq. (2). This can be expressed as follows:

$$\hat{d}(\alpha_i, \phi_j)\hat{Q}_K \neq \hat{Q}_K\hat{d}(\alpha_i, \phi_j),$$

where $\hat{d}(\alpha_i, \phi_j)$ represents the DDO with parameters α_i and ϕ_j. The non-commutativity between these operators means that they do not share the same eigenbasis. From a quantum mechanical perspective, this implies that when an adversary attempts to measure the cipher coherent states in the K-QAM basis $\{|\beta_1\rangle, \ldots, |\beta_K\rangle\}$, the measurement results will be random. The resulting BER would be close to 50%, making it practically impossible for an eavesdropper to extract meaningful digital information or ciphertext from the intercepted coherent states.

The analog nature of the cipher coherent states in QEPS-dd further complicates potential attacks. Unlike classical cryptosystems where the ciphertext is typically digital, QEPS-dd operates in a continuous, analog domain. The coherent states used in the encryption process are continuous-valued signals rather than discrete digital ciphertexts, making it far more challenging to recover the original K-QAM basis or digital information without the correct DDOP. Even advanced cryptographic methods such as algorithm reductions, parallel computing, and quantum computing approaches like Grover's algorithm [37] are largely ineffective against the analog nature of QEPS-dd encryption, as these techniques rely on digital structures absent in continuous-valued coherent states.

For an attacker, the most viable strategy is a brute-force search for the correct DDOP. The randomization introduced by the DDO and quantum permutation gates ensures that no analytical or computational shortcuts exist to bypass the encryption. The correct DDOP is essential to decrypt the cipher coherent states and restore the K-QAM constellation with an acceptable BER.

The complexity of a brute-force attack on QEPS-dd encryption scales factorially with the length of the DDOP. If the secret DDOP is ℓ bits long, the computational complexity of discovering the correct pad is given by $\mathcal{O}(2^\ell!)$ for a single value ϕ_j or a publicly known value of each ϕ_j, a factorial growth that quickly becomes infeasible as ℓ increases. This scaling arises from the quantum permutation gates, which randomize the DDOP, making the search space exponentially large and resistant even to quantum computing techniques [36].

Table 1 illustrates the complexity of brute-force searching for a DDOP of varying lengths and their equivalent Shannon entropy [36]. For instance, with $\ell = 5$, the brute-force search complexity is equivalent to searching a space of 117 bits. As ℓ increases beyond 5, even a single DDOP provides security exceeding NIST's level V, with search complexity growing to levels that make a brute-force attack virtually impossible.

Table 1 • The complexity of an ℓ-bit dynamic displacement operator pad and its equivalent Shannon entropy. The equivalent Shannon entropy is tabulated for two δ_j cases: $N = 1$ (single value) and $N = 3$ (three values)

ℓ	$\mathcal{O}(2^\ell!)$	**Entropy (bits):** $N = 1$	**Entropy (bits):** $N = 3$
5	2.63×10^{35}	117	351
6	1.28×10^{89}	295	885
7	3.85×10^{215}	716	2,148
8	8.57×10^{506}	1,684	5,052

To further enhance QEPS-dd encryption, we could adjust the phase-shift operators $\hat{\varphi}(\phi_j)$, where $\phi_j = (j-1)\frac{2\pi}{n} + \delta_j$, with $\delta_j \in \{\Delta_1, \ldots, \Delta_N :\in (0, \frac{2\pi}{n})\}$. This modification increases the complexity from $\mathcal{O}(2^\ell!)$ to $\mathcal{O}((2^\ell!)^N)$ and the equivalent entropy from $\log_2(2^\ell!)$ to $N\log_2(2^\ell!)$. **Table 1** also shows the equivalent

entropy for $N = 3$. If δ_j can take one from a set of three values $\{\Delta_1, \Delta_2, \Delta_3\}$ for a given ϕ_j, the entropy for $\ell = 5$ would provide higher security than NIST level V, with 351 bits of entropy.

Moreover, completely concealing the values of ϕ_j so that they are known only to trusted communication peers would significantly increase the difficulty for attackers, as they would no longer be selecting a value for δ_j from a predefined set of N options, but instead would be forced to guess its exact value.

2.6. Distinction between QEPS-dd, QEPS-p, and QEPS-d

In this subsection, we outline the key distinctions between the DDO and two variations of QEPS, namely QEPS-p and QEPS-d. While all three approaches operate within the framework of phase-space encryption, their methodologies and security mechanisms differ significantly.

QEPS-p employs the random *phase-shift operator* to perform QEPS. By introducing random phase shifts to the coherent states, QEPS-p introduces a controlled random variation in the states' phase, making the communication basis random and difficult for eavesdroppers to extract information without knowing how to convert the random communication basis to the standard basis. This approach ensures that even if an adversary attempts to measure the quantum state, they would encounter a close 50% BER, so no digital data can be extracted.

QEPS-d employs the random *displacement operator* in phase space to encode quantum information. The displacement operator acts on the coherent state by shifting it in phase space, thus modifying both its amplitude and its phase, and randomizing the communication basis. Without knowing the shared secret, an adversary cannot convert the randomized basis back to the regular communication basis, and any measurements would lead to a BER close to 50%, making it impossible to extract digital data.

QEPS-dd integrates both phase-shift and displacement operators into DDOs, demonstrating the dynamic effects on resultant coherent states after operating on different coherent states, which provides better security. QEPS DDO refers to the QEPS-dd pad by applying QPP to further enhance encryption security. In this case, a fixed set of displacement operators and a fixed set of phase-shift operators can be publicly selected, but a DDOP will be randomly chosen through a shared secret, leveraging the extremely high Shannon entropy in QPP. Based on this, QEPS DDO would be much easier to standardize the QEPS.

3. Conclusions

In this article, we have proposed a novel quantum encryption scheme in phase space, which introduces DDOs combined with the QPP to address the security challenges faced by conventional phase-shift and displacement operators. The DDO-based approach enhances encryption by utilizing dynamic, no-commutative transformations, significantly bolstering the system's resilience against attacks that may compromise static or predictable configurations.

The addition of the QPP further strengthens security by incorporating nonlinear and unpredictable encryption processes. By dynamically permuting the DDO base set, QPP maximizes cipher constellation points and fortifies the encryption of QEPS-dd, ensuring that the system is highly resistant to digital interception. This level of complexity provides a robust defense, particularly against attacks that exploit vulnerabilities in traditional optical communications systems, where communication data can be extracted from the fibers. QEPS-dd encryption thwarts such attacks unless the shared secret is compromised.

While the theoretical foundation of this scheme has been established, the next phase will involve experimental implementation. Leveraging prior experimental reports on QEPS-p and QEPS-d encryption, we plan to collaborate with McGill University to conduct further research and test the practical aspects of the proposal. This future work will focus on evaluating the performance, security, and practical deployment of the system in real-world quantum communication networks.

In conclusion, this proposal sets forth a promising direction for quantum encryption, integrating dynamic displacement and permutation techniques to elevate the security framework of quantum cryptographic systems. We expect that this approach will not only contribute to advancements in quantum cryptography but also facilitate the development of more secure and scalable quantum communication protocols over the exisiting infrastructure.

Acknowledgments

The author would like to express sincere gratitude to Dr. Khalil for his valuable discussions and insights regarding the experimental details of QEPS-d encryption [33]. His expertise and guidance have significantly helped to the development and refinement of QEPS-dd encryption, helping to bridge the gap between theoretical concepts and practical implementation.

Funding

The author declares no direct financial support was received for the research, authorship, or publication of this article. This work was conducted as part of the author's role at Quantropi Inc.

Author contributions

The author confirms sole responsibility for this work. The author approves of this work and takes responsibility for its integrity.

Conflict of interest

The author declare no conflict of interest.

Competing interest

The author declare that they have no competing interests.

Data availability statement

Data supporting these findings are available within the article, at https://doi.org/10.20935/AcadQuant7462, or upon request.

Institutional review board statement

Not applicable.

Informed consent statement

Not applicable.

Additional information

Received: 2024-09-09

Accepted: 2024-12-11

Published: 2025-01-06

Academia Quantum papers should be cited as *Academia Quantum 2025*, ISSN 3064-979X, https://doi.org/10.20935/AcadQuant7462. The journal's official abbreviation is *Acad. Quant.*

Publisher's note

Copyright

References

1. Bennett CH, Brassard G. Quantum cryptography: public key distribution and coin tossing. Theor Comput Sci. 2014;560:7–11. doi: 10.1016/j.tcs.2014.05.025
2. Djordjevic IB. Discrete variable (DV) QKD. In: Physical-layer security and quantum key distribution. Springer Cham: Springer Nature Switzerland AG; 2019.
3. Shor PW, Preskill J. Simple proof of security of the BB84 quantum key distribution protocol. Phys Rev Lett. 2000;85(2):441. doi: 10.1103/PhysRevLett.85.441
4. Renner R, Gisin N, Kraus B. Information-theoretic security proof for quantum-key-distribution protocols. Phys Rev A. 2005;72:012332. doi: 10.1103/PhysRevA.72.012332
5. Rivest RL, Shamir A, Adleman L. A method for obtaining digital signatures and public-key cryptosystems. Commun ACM. 1978;21(2):120–6. doi: 10.1145/359340.359342
6. Diffie W, Hellman M. New directions in cryptography. IEEE Trans Inf Theory. 1976;22(6):644–54. doi: 10.1109/TIT.1976.1055638
7. 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. doi: 10.1145/103418.103434
8. Lucamarini M, Yuan ZL, Dynes JF, Shields AJ. Overcoming the rate-distance limit of quantum key distribution without quantum repeaters. Nature. 2018;557(7705):400–3. doi: 10.1038/s41586-018-0066-6
9. Wang R, Yin ZQ, Lu FY, Wang S, Chen W, Zhang CM, et al. Optimized protocol for twin-field quantum key distribution. Commun Phys. 2020;3(1):149. doi: 10.1038/s42005-020-00415-0
10. Chen JP, Zhang C, Liu Y, Jiang C, Zhang WJ, Han ZY, et al. Twin-field quantum key distribution over a 511 km optical fibre linking two distant metropolitan areas. Nat Photon. 2021;15(8):570–5. doi: 10.1038/s41566-021-00828-5
11. Wang S, Yin ZQ, He DY, Chen W, Wang RQ, Ye P, et al. Twin-field quantum key distribution over 830-km fibre. Nat Photon. 2022;16:154–61. doi: 10.1038/s41566-021-00928-2
12. Buttler WT, Lamoreaux SK, Torgerson JR. Practical four-dimensional quantum key distribution without entanglement. Quantum Inf Comput. 2012;12(1–2):1–8. doi: 10.26421/QIC12.1-2-1
13. Dellantonio L, Sørensen AS, Bacco D. High-dimensional measurement-device-independent quantum key distribution on two-dimensional subspaces. Phys Rev A. 2018. doi: 10.1103/PhysRevA.98.062301
14. Bouchard F, Heshami K, England D, Fickler R, Boyd RW, Englert BG, et al. Experimental investigation of high-dimensional quantum key distribution protocols with twisted photons. Quantum. 2018;2:111. doi: 10.22331/q-2018-12-04-111
15. Jo Y, Park HS, Lee SW, Son W. Efficient high-dimensional quantum key distribution with hybrid encoding. Entropy. 2019;21(1):80. doi: 10.3390/e21010080.
16. Li B, Chen C, Yuan B, Zhang X, Dong R, Zhang S, Jin RB. Full characterization of biphotons with a generalized quantum interferometer. Phys Rev A. 2024;109(4):043703. doi: 10.1103/PhysRevA.109.043703
17. Sekga C, Mafu M, Senekane M. High-dimensional quantum key distribution implemented with biphotons. Sci Rep. 2023;13(1):1229. doi: 10.1038/s41598-023-28382-w
18. Lai JS, Lin XY, Qian Y, Liu L, Zhao WY, Zhang HY. Deployment-oriented integration of dv-qkd and 100 g optical transmission system. In: Asia Communications and Photonics Conference (ACPC) 2019. Optical Society of America; 2019; Chengdu. p. T2H.1. Available from: http://opg.optica.org/abstract.cfm?URI=ACPC-2019-T2H.1
19. Qi B. Bennett-brassard 1984 quantum key distribution using conjugate homodyne detection. Phys Rev A. 2021;103:012606. doi: 10.1103/PhysRevA.103.012606
20. Basch E, Brown T. Introduction to coherent optical fiber transmission. IEEE Commun Mag. 1985;23(5):23–30. doi: 10.1109/MCOM.1985.1092572
21. Guifang Li. Recent advances in coherent optical communication. Adv Opt Photon. 2009;1(2):279–307. doi: 10.1364/AOP.1.000279.

22. Kikuchi K. Fundamentals of coherent optical fiber communications. J Lightwave Technol. 2016;34(1):157–79. doi: 10.1109/JLT.2015.2463719

23. Ip E, Lau APT, Barros DJF, Kahn JM. Coherent detection in optical fiber systems. Opt Express. 2008;16(2):753–91. doi: 10.1364/OE.16.000753

24. Li G. Recent advances in coherent optical communication. Adv Opt Photon. 2009;1(2):279–307. doi: 10.1364/AOP.1.000279

25. Puttnam BJ, Luís RS, Mendinueta JMD, Sakaguchi J, Klaus W, Kamio Y, et al. Self-homodyne detection in optical communication systems. Photonics. 2014;1(2):110–30. doi: 10.3390/photonics1020110

26. Peng D, Huang Z, Liu Y, Chen Y, Wang F, Ponomarenko S, et al. Optical coherence encryption with structured random light. PhotoniX. 2021;2:6. doi: 10.21203/rs.3.rs-205624/v1

27. Wu Y, Luo H, Deng L, Yang Q, Dai X, liu D, et al. 60 gb/s coherent optical secure communication over 100 km with hybrid chaotic encryption using one dual-polarization iq modulator. Opt Lett. 2022;47(20):5285–8. doi: 10.1364/OL.470839

28. Zhao ZS, Li PL, Gan WM. Traceless encryption approach for physical layer security in coherent optical communications system. Opt Express. 2023;31(8):12585–96. doi: 10.1364/OE.482135

29. Kuang R, Bettenburg N. Quantum public key distribution using randomized glauber states. In 2020 IEEE International Conference on Quantum Computing and Engineering (QCE); 2020; Denver (CO). p. 191–6. doi: 10.1109/QCE49297.2020.00032

30. Glauber RJ. The quantum theory of optical coherence. Phys Rev. 1963;130:2529–39. doi: 10.1103/PhysRev.130.2529

31. 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. doi: 10.1038/s41598-023-39621-5

32. Kuang R, Chan A. Quantum encryption in phase space with displacement operators. EPJ Quantum Technol. 2023;10(1):26. doi: 10.1140/epjqt/s40507-023-00183-0

33. 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):49. doi: 10.1140/epjqt/s40507-024-00260-y

34. 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, California. Optica Publishing Group; 2022; p. SF4L.3. doi: 10.1364/CLEO_SI.2022.SF4L.3

35. Kuang R, Bettenburg N. Shannon perfect secrecy in a discrete hilbert space. In 2020 IEEE International Conference on Quantum Computing and Engineering (QCE). IEEE; 2020; Denver (CO). p. 249–55.

36. Kuang R, Barbeau M. Quantum permutation pad for universal quantum-safe cryptography. Quantum Inf Process. 2022;21:211. doi: 10.1007/s11128-022-03557-y

37. Grover LK. Quantum mechanics helps in searching for a needle in a haystack. Phys Rev Lett. 1997;79(2):325. doi: 10.1103/PhysRevLett.79.325