



atoms



Review

Quantum Encryption in Phase Space

Randy Kuang

Special Issue

Quantum Optics and Quantum Information

Edited by

Dr. Apurba De and Dr. Tasnim Ahmed



<https://doi.org/10.3390/atoms14030023>

Review

Quantum Encryption in Phase Space

Randy Kuang 

Quantropi Inc., 1545 Carling Av., Suite 620, Ottawa, ON K1Z 8P9, Canada; randy.kuang@quantropi.com

Abstract

Quantum Encryption in Phase Space (QEPS) is a physical-layer encryption framework that harnesses the quantum-mechanical properties of coherent states to secure optical communications against both classical and quantum computational threats. By applying randomized phase shifts, displacements, or their dynamic combinations—implemented as unitary transformations in phase space—QEPS disrupts the phase reference essential for coherent detection, establishing a phase synchronization barrier. This review synthesizes the theoretical foundations, security mechanisms, and experimental progress of the QEPS framework, encompassing its three principal variants: the round-trip Quantum Public Key Envelope (QPKE) protocol—a public-key-like scheme built upon phase randomization (QEPS-p), the symmetric phase-only QEPS-p, and the displacement-based QEPS-d. Experimental validations demonstrate that authorized users achieve bit-error rates (BERs) below the forward-error-correction threshold, whereas eavesdroppers are confined to BERs near 50%, equivalent to random guessing—all while utilizing standard coherent optical transceivers at data rates up to 200 Gb/s over 80 km of fiber. We further examine QEPS's robustness to channel impairments, its seamless compatibility with existing digital signal processing (DSP) pipelines, and its distinctive position within the post-quantum cryptography landscape. Finally, we outline key challenges and future research directions toward deploying QEPS as a practical, quantum-resistant security layer for next-generation optical networks.

Keywords: quantum encryption; physical-layer security; coherent optical communications; phase-space encryption; coherent states; Basis randomization; quantum public key encryption; phase synchronization barrier; post-quantum cryptography; digital signal processing; optical fiber security

1. Introduction

The advent of large-scale quantum computing represents a paradigm shift in computational capabilities with profound and urgent implications for cryptographic security. Shor's algorithm [1], which efficiently factors large integers and computes discrete logarithms on a quantum computer, directly threatens the foundational hardness assumptions of widely deployed public-key cryptosystems such as RSA, Diffie–Hellman, and elliptic curve cryptography. This impending vulnerability has spurred global efforts in post-quantum cryptography (PQC) [2], aiming to develop classical algorithms resistant to quantum attacks. A complementary approach emerges from the quantum domain itself: constructing cryptographic schemes whose security is rooted in fundamental quantum laws, rather than computational complexity assumptions.



Academic Editor: Pascal Quinet

Received: 5 January 2026

Revised: 27 February 2026

Accepted: 6 March 2026

Published: 11 March 2026

Copyright: © 2026 by the author.

Licensee MDPI, Basel, Switzerland.

This article is an open access article distributed under the terms and

conditions of the [Creative Commons](https://creativecommons.org/licenses/by/4.0/)

[Attribution \(CC BY\)](https://creativecommons.org/licenses/by/4.0/) license.

1.1. Quantum Encryption Paradigms: From Key Distribution to Direct Encryption

Quantum cryptographic strategies can be broadly classified into three categories based on operational modality and physical scale: quantum key distribution (QKD), quantum secure direct communication (QSDC), and quantum direct encryption schemes such as Quantum Encryption in Phase Space (QEPS)—encompassing both symmetric and public-key variants.

Quantum Key Distribution (QKD) is a micro-scale approach operating in the deep quantum regime using single photons or weak coherent pulses. The seminal BB84 protocol [3] established the foundational paradigm for quantum-secure key exchange, with security rooted in the no-cloning theorem [4,5] and the disturbance induced by measurements in incompatible bases. Subsequent security proofs formalized its information-theoretic guarantees under realistic assumptions [6,7].

Continuous-variable (CV) extensions further generalized QKD using coherent states and homodyne detection [8,9], enabling compatibility with standard telecom components. Comprehensive theoretical treatments of QKD security and implementation challenges are provided in [10,11].

In practice, real-world QKD systems are hybrid quantum–classical architectures. Quantum channels generate correlated raw keys, while classical post-processing—including sifting, error correction, privacy amplification, and authentication—is essential to establish the final shared secret [10]. Authentication of the classical channel, typically via a short pre-shared secret or computationally secure digital signatures, is mandatory; without it, QKD alone cannot guarantee secure key establishment.

Deployment considerations for QKD include dedicated fiber links or coexistence engineering with classical traffic, along with specialized hardware such as single-photon detectors and precise timing electronics. Experimental demonstrations over metropolitan and long-distance fiber links highlight both feasibility and rate–distance trade-offs [11,12]. Key rates decrease with channel loss, limiting distance without trusted relay nodes or quantum repeaters. Consequently, many practical deployments use QKD-generated keys primarily to refresh symmetric encryption systems (e.g., AES) rather than replacing symmetric encryption entirely. Industry-oriented perspectives emphasize hybrid integration strategies that combine quantum entropy sources with conventional symmetric cryptography for operational scalability [9,11].

Quantum Secure Direct Communication (QSDC) represents an alternative micro-scale paradigm enabling direct transmission of secret messages without prior key establishment [13–15]. QSDC protocols employ single photons or entangled photon pairs, leveraging entanglement-based encoding or quantum one-time-pad principles [16–18]. Unlike QKD, QSDC transmits information directly, avoiding separate key distribution [19,20].

Real-world demonstrations confirm that QSDC can achieve fully quantum communication over short distances, albeit with practical limitations: sensitivity to channel loss, reliance on precise quantum-state preparation and detection, and hardware requirements for entanglement generation and measurement [14,15]. These constraints currently restrict high data-rate, long-distance deployment, but QSDC provides a crucial proof-of-concept for end-to-end quantum messaging without classical key dependence [18,19].

Quantum Encryption in Phase Space (QEPS) is a macro-scale approach operating at the quantum–classical boundary using bright coherent states—the same carriers used in modern coherent optical communications. QEPS performs direct physical-layer encryption of modulated data signals compatible with standard telecom infrastructure.

QEPS exploits the number–phase uncertainty relation for coherent states, $\Delta n \cdot \Delta \phi \geq 1/2$, together with the operational necessity of a phase-synchronized local oscillator (LO) for coherent detection. Security arises from cryptographically controlling the communication

basis in phase space: without knowledge of the secret transformation applied to the modulation constellation (e.g., QPSK, K-QAM), an interceptor cannot establish the correct phase reference, rendering conventional coherent demodulation ineffective. The encrypted information remains embedded in quadrature relationships accessible only to receivers with the shared key.

Unlike QKD, QEPS does not claim unconditional, information-theoretic security. Instead, it relies on a physical-layer adversarial model in which security derives from quantum-limited measurement constraints and the infeasibility of reconstructing the encrypted phase reference without the secret key. Thus, QEPS complements QKD: while QKD secures key establishment via disturbance detection, QEPS secures high-speed data transmission by cryptographically controlling phase synchronization within existing coherent optical systems.

This tripartite classification highlights a central distinction: QKD and QSDC operate in the deep quantum regime with specialized hardware and hybrid quantum-classical workflows, whereas QEPS leverages bright coherent states and standard coherent transceivers to provide quantum-enhanced physical-layer encryption compatible with high-capacity optical networks.

1.2. Phase Space: The Arena for Optical Quantum Encryption

Phase space provides the natural framework for describing quantum states of light used in optical communications, particularly coherent states $|\alpha\rangle = \hat{D}(\alpha)|0\rangle$. These quasi-classical states exhibit robust, laser-like properties while retaining intrinsic quantum noise. The phase-space formalism, visualized via Wigner functions or constellation diagrams, enables intuitive design of encryption protocols as geometric transformations—rotations, displacements, and dynamic combinations—applied directly to the optical field.

The evolution of QEPS has progressed through three generations of unitary operators:

1. Phase Operators ($\hat{\phi}(\phi)$): Randomize the phase of a coherent state. Effective for PSK but partially exposes amplitude information in QAM formats [21].
2. Displacement Operators ($\hat{d}(\alpha)$): Translate coherent states across phase space, randomizing both quadratures and enabling secure QAM encryption [22,23].
3. Dynamic Displacement Operators (DDOs): Combine time-varying phase and displacement operations, creating a highly randomized cipher space and improving robustness against advanced attacks [24].

Experimental demonstrations confirm QEPS-d can operate at up to 560 Gb/s over standard fiber with unauthorized decryption yielding near 50% bit error rate [23].

1.3. Quantum Public-Key Encryption in Phase Space

Quantum Public Key Envelope (QPKE) implements public-key functionality using coherent states [25]. A recipient's public key is a coherent state randomized by a secret phase ϕ_r ; the sender encodes a message phase ϕ_k and returns it. Without knowledge of ϕ_r , an eavesdropper cannot reliably extract ϕ_k , as measurement requires access to the appropriate phase reference. Alternative chip-scale implementations achieve related objectives using partially coherent light and integrated interferometers [26].

Conceptually, QPKE relies on physical measurement constraints in phase space rather than computational hardness assumptions. Unlike QKD, it does not claim unconditional information-theoretic security but instead leverages limitations in phase reference recovery within coherent detection systems.

As summarized in Table 1, QEPS operates as a constellation-level coherent-state encryption framework. A key-dependent phase-space transformation is applied to the communication basis of modulated coherent states. Authorized receivers perform deterministic

inversion of this transformation within the digital signal processing (DSP) chain prior to carrier phase recovery, restoring the correct basis for coherent demodulation. Receivers lacking the transformation cannot establish a valid phase reference and therefore observe outcomes effectively randomized by intrinsic coherent-state quantum noise.

Table 1. Comparison of QKD, QSDC, and QEPS paradigms.

Aspect	Comparison
Primary Function	QKD: Key establishment QSDC: Direct message transmission without prior key QEPS: Physical-layer encryption of modulated data
Quantum Regime	QKD/QSDC: Single photons or entangled states QEPS: Bright coherent states (e.g., QPSK, K-QAM)
Security Basis	QKD: Disturbance detection (information-theoretic with classical authentication) QSDC: Quantum state integrity and eavesdropping detection QEPS: Key-dependent phase-space transformation with DSP inversion, preventing unauthorized phase-reference recovery
Classical Dependence	QKD/QSDC: Require authenticated classical channel and post-processing QEPS: Uses standard coherent DSP; no disturbance-based key sifting
Hardware	QKD/QSDC: Dedicated quantum hardware modules QEPS: Compatible with standard coherent optical transceivers
Deployment Considerations	QKD: Per-link devices, distance–loss tradeoff QSDC: Short-distance operation; specialized quantum hardware required QEPS: Inline encryption compatible with existing telecom fiber
Typical Usage	QKD: AES key refresh in deployed systems QSDC: Fully quantum communication demonstrated in real-world settings QEPS: High-speed optical link encryption

Note: Unlike QKD, whose security is information-theoretic, QEPS security derives from physical-layer constraints and quantum-limited measurements of coherent states. QSDC demonstrates practical operation over short distances, although specialized hardware is required. The table highlights practical and operational distinctions rather than absolute security guarantees.

From this comparison, a practical question arises: can physical-layer security be introduced into high-speed coherent optical systems without relying on single-photon hardware or separate key-distribution infrastructure? QEPS is proposed in this context. It operates in the bright coherent-state regime already used in standard telecom networks, preserving compatibility with existing coherent transceiver architectures while introducing a distinct physical-layer encryption mechanism.

Unlike conventional symmetric encryption schemes such as AES-256, where ciphertext can be perfectly copied, stored, and subjected to offline cryptanalysis, QEPS operates directly at the physical transmission layer. In classical encryption, the adversary may record the full digital ciphertext without degradation and attempt decryption at a later time under evolving computational capabilities.

In contrast, QEPS encodes information in coherent optical fields whose recovery requires phase-consistent coherent detection. While optical tapping of a fiber link remains physically possible, successful reconstruction of the transmitted communication basis requires knowledge of the secret phase-space transformation and proper convergence

within the DSP chain. In the absence of this transformation, intercepted measurements may fail to establish a valid phase reference, leading to outcomes effectively randomized by intrinsic coherent-state quantum noise.

This distinction reflects a difference in security model rather than a claim of unconditional secrecy: QEPS introduces measurement-dependent physical constraints at the signal acquisition stage, whereas conventional encryption relies purely on computational hardness at the digital layer.

1.4. Experimental vs. Theoretical Security Claims in QEPS

To clarify the scope of what has been experimentally demonstrated versus what remains theoretically proposed, we categorize QEPS security claims as follows in Table 2.

Table 2. Experimental vs. Theoretical Security Claims in QEPS.

Claim/Feature	Experimental Demonstration	Theoretical/Heuristic
Physical-layer encryption of modulated data	Demonstrated on standard coherent transceivers at up to 560 Gb/s over fiber [23]	Not applicable
Key-dependent phase-space transformations	Implemented experimentally for phase-only and displacement-based schemes [22]	Dynamic displacement operator (DDO) fully generalized design remains theoretical [24]
Phase-synchronization barrier against unauthorized receivers	Near-random BER ($\approx 50\%$) for unauthorized receivers observed experimentally [23]	Security proofs against arbitrary quantum attacks remain heuristic
Constellation-level encryption for QAM formats	Demonstrated experimentally for 16-QAM and 64-QAM formats [23]	Generalization to higher-order QAM is theoretical
Public-key implementation (QPKE)	Chip-scale proof-of-concept using integrated interferometers [26]	Security against adaptive attackers based on measurement constraints remains heuristic
Resistance to advanced attacks (machine learning, coherent eavesdropping)	Not yet experimentally validated	Security arguments are currently based on phase-space uncertainty principles and practical DSP inversion constraints; a full composable security proof remains an open research problem

Note: This table explicitly separates experimentally verified capabilities of QEPS from features that remain theoretically proposed or heuristic.

In addition to Table 2, we explicitly label security claims in the text as either experimentally demonstrated or theoretically proposed/heuristic to ensure clarity for readers. For example:

- Experimentally demonstrated: Phase-space encryption of 16-/64-QAM coherent states with deterministic key-based inversion, yielding near-50% BER for unauthorized receivers [23].

- Theoretically proposed/heuristic: Full security proofs for arbitrary quantum or machine-learning-based attacks on dynamic displacement operator schemes [24].

This distinction ensures that readers can immediately assess the practical scope of QEPS security versus features currently supported by theory and design principles.

1.5. The Broader Landscape of Optical Physical-Layer Security

QEPS exists within a rich ecosystem of optical encryption techniques, each with distinct mechanisms. Polarization-based schemes rapidly scramble the state of polarization using digital scramblers [27]. Other approaches include cross-phase encoding with all-optical gates [28], electro-optic phase feedback systems [29], quantum homomorphic encryption [30], and encryption exploiting spatial coherence properties [31]. These strategies offer varied trade-offs between security, data rate, complexity, and compatibility with existing network infrastructure.

Integrated photonic approaches represent another promising direction. Wu et al. [26] demonstrated public-key encryption using a lithium niobate photonic chip with a Mach-Zehnder interferometer mesh, encoding keys in the incoherent optical transmission matrix. This highlights the potential for chip-scale integration of quantum-inspired encryption protocols, offering advantages in compactness, power efficiency, and compatibility with emerging photonic systems.

Comparison with QAM-based Noise Randomization: Conventional QAM-based noise randomization perturbs individual constellation symbols using quantum or classical noise. In contrast, QEPS applies a key-dependent phase-space transformation to the communication basis. Authorized receivers perform deterministic inversion of the transformation within the DSP chain, restoring the original basis prior to coherent detection. Unauthorized receivers, lacking the secret phase reference, cannot reconstruct the basis and observe outcomes effectively randomized by intrinsic coherent-state quantum noise. This basis-level transformation distinguishes QEPS from simple symbol-level noise masking.

1.6. Chaos-Based Optical Encryption: A Comparative Perspective

Before discussing nonlinear masking approaches such as optical chaos encryption, it is important to distinguish constellation-level coherent-state encryption from waveform-level analog masking. As described above, QEPS operates by applying a key-dependent phase-space transformation to the communication basis. By contrast, chaos-based encryption embeds information within nonlinear carrier dynamics at the analog waveform level.

Optical chaos encryption leverages nonlinear dynamics and sensitivity to initial conditions [32,33]. Chaos-based schemes typically employ synchronized chaotic carriers—generated via optical feedback, injection, or electro-optic loops—to mask or modulate information-bearing signals [34,35]. Security relies primarily on the computational difficulty of reconstructing nonlinear dynamics and the practical challenge of achieving precise synchronization without knowledge of system parameters [36,37]. Recent advances have enhanced bandwidth and transmission distance [34,38], with DSP and machine learning improving synchronization performance [35,39]. However, chaos encryption typically operates at the analog waveform level, often requiring active synchronization and, in some implementations, multiple signal paths.

In contrast, QEPS exploits the quantum-mechanical uncertainty of coherent states together with the operational necessity of phase synchronization in coherent detection. Rather than embedding data in a complex waveform, QEPS cryptographically transforms the phase-space basis itself, creating a phase-synchronization barrier: without the secret transformation, coherent demodulation fails and the observed constellation appears randomized.

Summary Perspective:

- QAM-based noise masking: Obscures symbols via stochastic perturbation.
- Chaos encryption: Masks information within nonlinear carrier dynamics.
- QEPS: Encrypts the communication basis in phase space through deterministic, key-controlled transformations compatible with standard coherent transceivers.

This harmonized terminology clarifies that QEPS is a constellation-level coherent-state encryption framework designed for high-speed optical systems, while chaos-based approaches operate at the analog waveform level with different security assumptions and implementation trade-offs.

1.7. Scope and Contribution of This Review

This comprehensive review synthesizes the theoretical foundations, security analyses, experimental progress, and future trajectories of Quantum Encryption in Phase Space. We provide a unified perspective on the QEPS framework, tracing its evolution from phase-based to dynamic displacement operator approaches. We elucidate its core security principle—exploiting the number-phase uncertainty and LO-synchronization requirement to render eavesdropping futile—and contrast this with the disturbance-detection basis of QKD, the single-photon direct transmission of QSDC, and the synchronization-dependent paradigm of chaos-based encryption. By examining both theoretical models and experimental demonstrations, we assess the practical viability of QEPS for securing high-speed optical networks against both classical and quantum computational threats. Furthermore, we situate QEPS within the broader context of optical physical-layer security, highlighting its unique advantages as a protocol capable of leveraging standard telecom hardware to provide quantum-enhanced security. Through this synthesis, we aim to provide researchers and practitioners with a clear understanding of the potential, challenges, and future directions of phase-space encryption in building the quantum-resilient communication infrastructure of tomorrow.

2. Theoretical Foundations: Coherent States and Phase-Space Dynamics

2.1. Coherent States: Bridging Classical and Quantum Optics

The coherent state $|\alpha\rangle$, first formalized by Glauber [40], represents a fundamental cornerstone of quantum optics and serves as the primary information carrier in modern coherent optical communications. Generated by displacing the vacuum state, $|\alpha\rangle = \hat{D}(\alpha)|0\rangle$, where $\alpha = |\alpha|e^{i\phi} \in \mathbb{C}$ encodes both amplitude and phase information, coherent states uniquely bridge the classical and quantum domains. They are quasi-classical, exhibiting laser-like properties while retaining intrinsic quantum noise. This duality makes them ideally suited for high-speed communications and, as we will show, for quantum-inspired encryption. Their defining properties include:

- Minimum Uncertainty: Coherent states saturate the Heisenberg uncertainty principle with equal uncertainties in the two field quadratures ($\Delta X = \Delta P = 1/2$ in appropriate units). This makes them the closest quantum mechanical analogue to a stable classical electromagnetic wave.
- Poissonian Photon Statistics: The photon number distribution is Poissonian, $\mathcal{P}(n) = e^{-|\alpha|^2} |\alpha|^{2n} / n!$, with mean photon number $\bar{n} = |\alpha|^2$. This matches the statistical behavior of an ideal laser operating well above threshold and underpins the signal-to-noise characteristics in coherent optical systems.
- Overcompleteness: Coherent states form an overcomplete basis, satisfying the resolution of identity $\frac{1}{\pi} \int |\alpha\rangle\langle\alpha| d^2\alpha = \mathbb{I}$. This property allows any optical quantum state to be expressed as a superposition of coherent states, providing a powerful representation for calculations.

- **Displacement Property and its Simplification:** The action of a displacement operator is given by $\hat{D}(\beta)|\alpha\rangle = e^{i\text{Im}(\alpha\beta^*)}|\alpha + \beta\rangle$. This reveals two distinct effects: a translation in phase space from α to $\alpha + \beta$, and an overall global phase factor. Since global phases are unobservable in physical measurements, the core action can be captured by a reduced displacement operator $\hat{d}(\beta)$ defined by its action:

$$\hat{d}(\beta)|\alpha\rangle \equiv |\alpha + \beta\rangle. \tag{1}$$

This simplified operator retains the additive property $\hat{d}(\beta_1)\hat{d}(\beta_2) = \hat{d}(\beta_1 + \beta_2)$ and, critically, commutes: $[\hat{d}(\beta_1), \hat{d}(\beta_2)] = 0$. As established in QEPS-d [22], this commutativity is a key enabler for practical implementation, allowing encryption and decryption sequences to be applied without concern for operator ordering, thus facilitating direct realization with standard in-phase/quadrature (IQ) modulators.

The combination of robust propagation through optical fiber and inherent quantum-mechanical character makes coherent states a uniquely powerful substrate for physical-layer encryption protocols like QEPS, which harness these properties for security.

2.2. Phase-Space Formalism: Visualizing Quantum Encryption

Phase space provides an elegant and intuitive framework for representing quantum states of light, where each point $(\text{Re}(\alpha), \text{Im}(\alpha))$ corresponds to a coherent state. Unlike discrete variable representations, this continuous phase space allows quantum states to be fully described by quasi-probability distributions that seamlessly blend classical-like features with quantum noise:

$$W(\alpha) = \frac{1}{\pi^2} \int \text{Tr}[\rho \hat{D}(\beta)] e^{\alpha\beta^* - \alpha^*\beta} d^2\beta \tag{Wigner function} \tag{2}$$

$$Q(\alpha) = \frac{1}{\pi} \langle \alpha | \rho | \alpha \rangle \tag{Husimi Q-function} \tag{3}$$

$$P(\alpha) = \text{Glauber-Sudarshan P-representation} \tag{used in optical equivalence theorem}. \tag{4}$$

For a pure coherent state $|\alpha_0\rangle$, the Wigner function is a symmetric Gaussian peak centered at α_0 , while the Q-function represents its overlap with a probe coherent state. The finite width of these distributions is a direct manifestation of the quantum noise inherent to the state. This geometric visualization is particularly powerful for designing and analyzing encryption schemes: rotations and translations in phase space correspond directly to physically implementable unitary operations on the optical field. Moreover, the quantum noise—apparent as the finite breadth of the distributions—provides an innate source of randomness that underpins the cryptographic security of QEPS by obscuring the exact location of the encrypted symbol.

2.3. Key Operator Transformations in Phase Space

The QEPS framework is built upon two fundamental classes of unitary transformations that physically manipulate coherent states in phase space. These operators correspond directly to standard optical components, providing a clear path from theory to experimental implementation.

2.3.1. Phase Operators: Phase-Space Rotations

The phase operator $\hat{\phi}(\phi) = \exp(i\theta a^\dagger a)$ implements rotations in phase space. Acting on a coherent state $|\alpha\rangle$, it produces a rotated coherent state:

$$\hat{\phi}(\phi)|\alpha\rangle = |\alpha e^{i\theta}\rangle. \tag{5}$$

This operation is physically realized by a phase modulator that applies a controllable phase delay θ . For encryption purposes, random phase rotations effectively obscure the original phase information, making this approach particularly suitable for phase-encoded data (e.g., in PSK formats). The original Quantum Public Key Envelope (QPKE) protocol leveraged this transformation, using a secret phase shift as a private key [25]. In a symmetric-key setting, applying a random phase rotation θ_k (determined by a shared secret key) to a data-bearing coherent state $|\alpha_d\rangle$ yields the cipher state:

$$|\psi_{\text{cipher}}\rangle = \hat{\phi}(\theta_k)|\alpha_d\rangle = |\alpha_d e^{i\theta_k}\rangle. \tag{6}$$

2.3.2. Displacement Operators: Phase-Space Translations

The displacement operator $\hat{D}(\alpha) = \exp(\alpha a^\dagger - \alpha^* a)$ implements translations in phase space. Its action on a coherent state is given by:

$$\hat{D}(\beta)|\alpha\rangle = e^{i\text{Im}(\alpha\beta^*)}|\alpha + \beta\rangle. \tag{7}$$

Physically, this corresponds to adding a complex field amplitude β to the optical signal, an operation natively performed by an in-phase/quadrature (IQ) modulator. For cryptographic applications, the global phase factor $e^{i\text{Im}(\alpha\beta^*)}$ is physically irrelevant and can be omitted, leading to the reduced displacement operator $\hat{d}(\beta)$ with the simplified transformation:

$$\hat{d}(\beta)|\alpha\rangle = |\alpha + \beta\rangle. \tag{8}$$

In the QEPS-d encryption scheme [22], a data symbol represented by $|\alpha_d\rangle$ is encrypted by applying a secret displacement β_k :

$$|\psi_{\text{cipher}}\rangle = \hat{d}(\beta_k)|\alpha_d\rangle = |\alpha_d + \beta_k\rangle. \tag{9}$$

The displacement vector β_k , generated from a shared secret key, randomizes the symbol's position across the entire constellation plane.

2.3.3. Dynamic Displacement Operators: Combined Transformations

The most general encryption transformation within the QEPS framework combines both displacement and phase operations, often in a time-dependent sequence. A dynamic displacement operator (DDO) can be defined as:

$$\hat{U}_{\text{DDO}}(t) = \hat{d}(\beta(t))\hat{\phi}(\theta(t)) = \hat{d}(\beta(t))\hat{\phi}(\theta(t)), \tag{10}$$

where $\beta(t)$ and $\theta(t)$ evolve according to a cryptographically secure algorithm driven by the secret key. Applying this operator to a data state yields the cipher state:

$$|\psi_{\text{cipher}}(t)\rangle = \hat{U}_{\text{DDO}}(t)|\alpha_d\rangle = |\alpha_d e^{i\theta(t)} + \beta(t)\rangle. \tag{11}$$

This approach, formalized in QEPS-dd [24,41], creates a cipher space with enhanced dimensionality and temporal variability, significantly increasing the difficulty of cryptanalysis.

2.3.4. Non-Commutativity: The Quantum Mechanical Heart of Security

The mathematical bedrock of QEPS security is the fundamental non-commutativity of the displacement and phase operators. For the full operators, this is expressed as:

$$[\hat{D}(\beta), \hat{\phi}(\phi)] \neq 0, \tag{12}$$

which follows from the canonical commutation relation $[a, a^\dagger] = 1$. This algebraic property is a direct consequence of the Heisenberg uncertainty principle applied to the conjugate observables of quadrature amplitude and phase. Cryptographically, it ensures that an eavesdropper lacking the secret key sequence cannot determine or invert the composite encryption transformation—even with perfect measurement equipment. Applying decryption operations in the wrong order (due to an incorrect key guess) yields a result quantum-mechanically distinct from the original message. This intrinsic quantum property, augmented by the practical necessity of a phase-synchronized local oscillator for coherent detection, establishes a multi-layered security barrier fundamentally different from classical computational encryption.

These theoretical pillars—coherent states as robust, quantum-encoded information carriers; phase space as an intuitive encryption design arena; explicit transformation equations for encryption operations; and non-commuting operators as enforcers of cryptographic secrecy—collectively form the essential mathematical foundation for the Quantum Encryption in Phase Space framework detailed in the following sections.

3. The QEPS Framework: Principles and Mechanisms

Building upon the theoretical foundations of coherent states and phase-space transformations, we now present the Quantum Encryption in Phase Space (QEPS) framework as a systematic approach to physical-layer encryption for coherent optical communications [22,23,25,41,42]. The framework leverages the quantum mechanical properties of coherent states and unitary operators to achieve secure, high-speed data transmission over existing optical infrastructure.

It is noteworthy that the QPKE protocol represents a specific application architecture (a round-trip, public-key-like protocol) that implements the phase randomization principle of QEPS-p. In contrast, QEPS-p, QEPS-d, and QEPS-dd are defined primarily by their encryption operators and are typically deployed in symmetric-key configurations.

3.1. Core Encryption Protocol Architecture

The QEPS encryption process employs phase shift operator $\hat{\phi}(\phi)$ and displacement operator $\hat{D}(\alpha)$ to transform data-bearing coherent states. Each modulated symbol in a coherent optical communication system is represented by a single coherent state $|\beta\rangle$ drawn from a K -QAM constellation. The encryption transformation for each symbol is expressed as:

$$|\psi_{\text{enc}}\rangle = \hat{U}_{\text{key}}|\beta\rangle, \tag{13}$$

where \hat{U}_{key} represents a unitary transformation parameterized by a shared secret key. This formulation encompasses three main variants, each characterized by the specific form of \hat{U}_{key} :

- QEPS-p (Phase-based): Uses only phase shift operators, rotating constellation points around the origin:

$$|\psi_{\text{enc}}\rangle = \hat{\phi}(\phi)|\beta\rangle = |e^{-i\phi}\beta\rangle,$$

where $\phi \in [0, 2\pi)$ is derived from the secret key.

- QEPS-d (Displacement-based): Uses only displacement operators, shifting the entire constellation in phase space:

$$|\psi_{\text{enc}}\rangle = \hat{D}(\alpha)|\beta\rangle = |\alpha + \beta\rangle,$$

where $\alpha \in \mathbb{C}$ is derived from the secret key.

- QEPS-dd (Dual Displacement Operator): Combines both operators in sequence:

$$|\psi_{\text{enc}}\rangle = \hat{D}(\alpha)\hat{\phi}(\phi)|\beta\rangle = |\alpha + e^{-i\phi}\beta\rangle,$$

where both $\alpha \in \mathbb{C}$ and $\phi \in [0, 2\pi)$ are derived from the secret key. The dynamic nature arises because the combined transformation creates an effective displacement $\alpha + (e^{-i\phi} - 1)\beta$ that depends on $|\beta\rangle$, making the encryption state-dependent and enhancing security.

The encryption parameters (α, ϕ) can vary dynamically from symbol to symbol according to a predetermined sequence generated from the shared secret key, forming what is termed a Dynamic Displacement Operator Pad (DDOP) [41], using Quantum Permutation Pad or QPP [43]. This time-varying encryption ensures that each symbol undergoes a unique transformation, preventing pattern recognition by unauthorized receivers.

The physical implementation typically employs a single IQ-MZM modulator that applies the combined transformation $\hat{D}(\alpha)\hat{\phi}(\phi)$ in a single step, with the complex driving signals (I, Q) calculated from both the data symbol β and the encryption parameters (α, ϕ) . This approach maintains compatibility with standard coherent optical transceivers while introducing the quantum encryption layer.

3.2. Channel Normalization via Digital Signal Processing

A critical enabling technology for QEPS is modern Digital Signal Processing (DSP) [44–46] in coherent optical systems. The DSP integration framework, illustrated in Figure 1 [47] for the QEPS-d variant, applies equivalently to all QEPS variants (p, d, and dd) with appropriate substitutions of the encryption/decryption operators. For authorized parties, this DSP performs the dual function of decrypting the signal and normalizing channel impairments, creating an effective DSP-trusted channel.

The complete transmitter processing chain operates as follows:

1. Source data undergoes QAM mapping to generate complex symbols β , which correspond mathematically to coherent states $|\beta\rangle$.
2. The Encryption Operator \hat{U}_{key} (specific to the QEPS variant) applies the encryption. For QEPS-d: $|y\rangle = \hat{D}(\alpha)|\beta\rangle$; for QEPS-p: $|y\rangle = \hat{\phi}(\phi)|\beta\rangle$; for QEPS-dd: $|y\rangle = \hat{D}(\alpha)\hat{\phi}(\phi)|\beta\rangle$.
3. The encrypted complex waveform $|y\rangle$ then enters the standard transmitter DSP routine: pilot symbols are inserted for synchronization, the signal is up-sampled, pulse-shaped, re-sampled to the DAC rate, and finally undergoes clipping and quantization before optical modulation.

After propagation through the optical fiber channel and coherent detection with ADC de-skew correction, the receiver DSP chain executes:

1. Synchronization aligns the signal using inserted pilots.
2. Matched filtering optimizes the signal-to-noise ratio.
3. The Adaptive equalizer compensates for linear channel impairments (e.g., chromatic and polarization-mode dispersion).
4. Down-sampling reduces the data to one sample per symbol.
5. Carrier phase recovery corrects for laser phase noise and frequency offset.
6. The Inverse Encryption Operator $\hat{U}_{\text{key}}^{-1}$ is applied using the shared key. This crucial decryption step restores the original constellation point β .
7. Finally, QAM de-mapping recovers the bit stream for BER calculation.

This sequence embodies channel normalization for the authorized user: standard DSP algorithms first condition the signal, then decryption restores its structure, enabling

accurate demapping. The entire chain compensates for physical channel effects, resulting in a low-BER link—the DSP-trusted channel.

Conversely, for an eavesdropper lacking the secret key, step 6 (Inverse Encryption Operator) cannot be performed. Without the correct inverse transformation, the signal constellation remains scrambled in the optical field domain. Importantly, this is not merely a digital encryption layer like AES, which operates on bits and is independent of the transmission channel. Rather, QEPS fundamentally alters the physical waveform such that the transmitted symbols are no longer standard QAM symbols recognizable to a classical coherent receiver.

This physical transformation has profound implications for the eavesdropper’s recovery attempt. While an eavesdropper can execute the initial DSP steps (1–5) on the encrypted waveform $|y\rangle$ —as these algorithms operate on signal statistics and pilots rather than specific constellation geometry—the process breaks down at the critical decryption step:

- Without the secret key, the Inverse Encryption Operator cannot be applied correctly. Any attempt at inversion (including skipping it entirely) leaves the signal in a scrambled state.
- When this scrambled signal reaches QAM de-mapping, it no longer corresponds to valid constellation points, preventing meaningful data recovery.
- The encryption’s effect is thus not to prevent initial DSP convergence, but to ensure that the signal presented to the decision circuitry remains indistinguishable from noise after all channel compensation has been applied.
- Even with brute-force key search, each trial would require complete QAM demapping and error evaluation, as the DSP chain up to carrier recovery may still execute on incorrectly decrypted signals without obvious failure cues.

Thus, while AES provides digital security by scrambling bits, QEPS provides physical-layer security by ensuring that only the legitimate receiver can transform the compensated signal into a decodable constellation. The security manifests not in early DSP failure, but in the final impossibility of mapping the processed signal to valid data symbols without the precise inverse transformation.

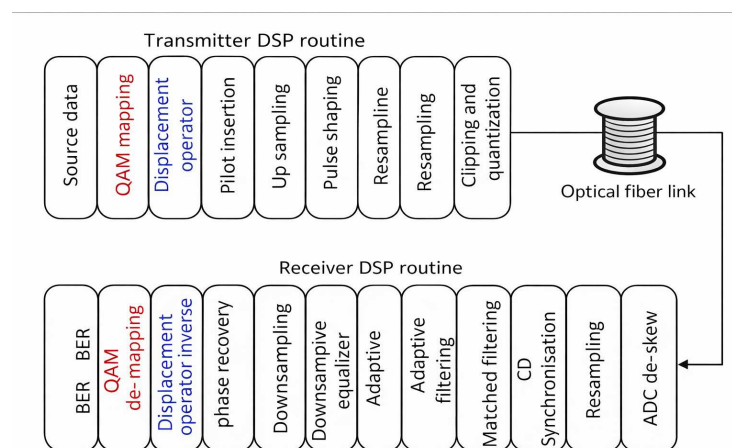


Figure 1. Block diagram of the integrated QEPS DSP system framework, illustrated for the QEPS-d variant [47]. The transmitter path shows QAM mapping followed by the encryption operator (here: Displacement Operator) before standard DSP shaping. The receiver path shows signal conditioning (synchronization, equalization, phase recovery) followed by decryption (here: Displacement Operator Inverse) before final QAM demapping. The framework applies identically to QEPS-p and QEPS-dd with appropriate operator substitutions.

3.3. Cipher Space and Key Space Characterization

The security of QEPS is rooted in the expansion of the original message constellation into a randomized cipher constellation. For a K -QAM constellation $\mathcal{B} = \{|\beta_1\rangle, \dots, |\beta_K\rangle\}$, the cipher space \mathcal{C} is:

$$\mathcal{C} = \{|\psi_{\text{enc}}\rangle : |\psi_{\text{enc}}\rangle = \hat{U}_{\text{key}}|\beta\rangle, |\beta\rangle \in \mathcal{B}, \hat{U}_{\text{key}} \in \mathcal{U}_{\text{key}}\}, \tag{14}$$

where \mathcal{U}_{key} is the set of unitary transformations achievable with valid keys. The cipher expansion ratio:

$$R_{\text{exp}} = \frac{|\mathcal{C}|}{|\mathcal{B}|} \tag{15}$$

is maximized when using a Dynamic Displacement Operator Pad (DDOP) combined with a Quantum Permutation Pad (QPP) [48]. A DDOP is constructed from a publicly known set of $m \times n$ DDOs:

$$\text{DDO Base} = \{\hat{D}(\alpha_i)\hat{\phi}(\phi_j)\}, \quad i = 1, \dots, m, j = 1, \dots, n, \tag{16}$$

which is then permuted via QPP using a shared secret s to produce a random pad:

$$\text{DDOP} = \{\hat{D}(\alpha_{p(1)})\hat{\phi}(\phi_{p(1)}), \dots, \hat{D}(\alpha_{p(R)})\hat{\phi}(\phi_{p(R)})\}, \quad R = m \times n. \tag{17}$$

This process maximizes the cipher constellation points to nearly $m \times n \times K$ and ensures semantic security by making the ciphertext distribution statistically indistinguishable from random noise to an eavesdropper.

3.4. Dynamical Evolution and Security Enhancement

Time-dependent key sequences introduce dynamical evolution into the encryption process, preventing pattern analysis and providing forward secrecy. The encryption parameters can evolve via cryptographically secure pseudorandom number generators (PRNGs) or chaotic maps:

$$\alpha_{n+1} = f_\alpha(\alpha_n, \phi_n, s_n), \tag{18}$$

$$\phi_{n+1} = f_\phi(\alpha_n, \phi_n, s_n), \tag{19}$$

where s_n is the n th state of the master key. This temporal evolution, combined with the non-commutativity of the operators:

$$[\hat{D}(\alpha), \hat{\phi}(\phi)] \neq 0, \tag{20}$$

creates a generalized uncertainty principle that prevents an eavesdropper from simultaneously determining both the displacement and phase parameters. The result is a bit error rate (BER) approaching 50% for any measurement without the correct DDOP.

The security against brute-force attacks is quantified by the effective entropy of the DDOP. For an ℓ -bit secret, the entropy is:

$$H = \log_2(2^\ell!) \quad \text{bits}, \tag{21}$$

which grows factorially with ℓ . For example, with $\ell = 8$, $H \approx 1864$ bits, far exceeding NIST post-quantum security requirements.

3.5. Practical Implementation and Experimental Validation

Practical implementation uses standard coherent optical modules:

- Transmitter: Laser diode, IQ-MZM modulator driven by DACs, DSP for pulse shaping and pilot insertion, with QEPS encryption integrated into the modulation process.
- Receiver: Coherent detector with local oscillator, ADC, QEPS decryption module, followed by standard DSP for channel compensation.

The round-trip QPKE protocol demonstrates how QEPS can emulate public-key functionality: Bob sends an encrypted “envelope” $|\alpha\rangle$ to Alice, who modulates her secret $|\beta\rangle$ and returns $|\alpha + \beta\rangle$. Bob then decrypts with $\hat{D}(-\alpha)$ to recover $|\beta\rangle$. This eliminates the need for pre-shared secrets and enables authentication through self-shared randomness.

Experimental demonstrations have validated QEPS at speeds up to 560 Gbps (32-QAM over 80 km) with BER below the forward error correction threshold, confirming its feasibility for real-world high-speed quantum-secure optical communications. The experimental results consistently show that without decryption, the measured BER remains at approximately 48–49%, demonstrating the effectiveness of the encryption in preventing unauthorized reception.

4. Physical-Layer Security Principle: Phase Synchronization Barrier

This section synthesizes the security arguments common to Quantum Encryption in Phase Space (QEPS) implementations as advanced in the literature. Rather than proposing new formal proofs, we distill the operational principles and experimental evidence that collectively establish QEPS’s security foundation. The central thesis—that randomized unitary transformations disrupt the phase reference essential for coherent detection—has been consistently validated across phase-only (QEPS-p), displacement-based (QEPS-d), and dynamic displacement operator (QEPS-dd) implementations [21–23,42]. We contrast this physical-layer mechanism with classical computational security and other optical encryption paradigms, situating QEPS within the broader landscape of quantum-inspired security for optical communications.

4.1. The Phase Synchronization Imperative in Coherent Detection

Accurate demodulation in coherent optical communication necessitates establishing a stable phase reference at the receiver. Carrier phase recovery (CPR), essential for decoding quadrature amplitude modulation (QAM) signals, depends fundamentally on the presence of a structured constellation in phase space. In conventional coherent systems, DSP-based phase recovery typically follows one of two paradigms:

1. Active phase recovery (e.g., blind phase search, decision-directed phase-locked loops) estimates and compensates phase drift using known statistical or structural properties of the transmitted symbols.
2. Passive phase mitigation (e.g., differential encoding, phase-diverse reception) reduces sensitivity to phase noise through signal design without explicit feedback.

Both approaches assume that received symbols cluster around a finite, stable set of constellation points—an assumption that QEPS deliberately violates by encrypting information directly at the coherent-state level prior to standard modulation.

4.2. The Phase Synchronization Barrier: Core Mechanism

The security rationale for QEPS stems from its ability to cryptographically deny the phase reference required for coherent detection. By applying symbol-by-symbol unitary transformations—phase shifts, displacements, or their combination—QEPS encrypts the data-bearing coherent state $|\beta\rangle$ into:

$$|\psi_{\text{enc}}\rangle = \hat{D}(\alpha)\hat{\phi}(\phi)|\beta\rangle = |\alpha + e^{-i\phi}\beta\rangle,$$

where the encryption parameters (α, ϕ) are derived from a secret key and vary dynamically. This process deliberately destroys the structured clustering of constellation points in phase space that is essential for any DSP-based carrier recovery algorithm.

For an authorized receiver possessing the key, decryption (applying $\hat{U}_{\text{key}}^{-1}$ at the appropriate DSP stage) restores the original QAM constellation before CPR is attempted. The DSP then operates on a legitimate signal, achieving phase synchronization and yielding low bit-error rate (BER).

For an eavesdropper, however, the encrypted signal presents a fundamental obstruction. While initial DSP steps (synchronization, equalization) may process the encrypted waveform, the critical CPR stage fails. Without the correct inverse transformation, the received symbols do not converge to a discrete constellation but instead form a diffuse cloud in phase space. Consequently, the eavesdropper cannot establish a meaningful phase reference—a condition termed the phase synchronization barrier in QEPS literature.

Numerical simulations and experimental studies consistently report that without the secret key, eavesdroppers' BER saturates near 50% regardless of the DSP strategy employed [22,42]. This operational result forms the primary evidence for QEPS security: the signal is rendered physically undecodable to unauthorized parties.

4.3. Core Security Rationale: Basis Randomization and Restoration

The phase synchronization barrier described above can be fundamentally understood as a consequence of basis randomization at the coherent-state level. At its essence, QEPS leverages a shared secret of effectively unlimited length to dynamically randomize the communication basis for coherent states carrying K-PSK or K-QAM symbols. The secret key controls a sequence of unitary transformations—phase rotations, displacements, or their combination—that collectively define a time-varying encryption basis.

This basis randomization directly implements the phase synchronization barrier: by randomizing the communication basis, QEPS ensures that coherent detection without the secret key amounts to measurement in a misaligned basis, leading to the observed 50% BER.

For authorized communication, the legitimate receiver applies the inverse transformation sequence using the same shared secret, thereby restoring the original communication basis before coherent detection and demodulation. This restoration process reconstructs the structured constellation necessary for standard digital signal processing (DSP) algorithms to succeed.

For an eavesdropper lacking the secret, the intercepted signal remains encoded in a randomized basis. Coherent detection—requiring precise phase synchronization with the transmitted signal—effectively constitutes a measurement in a random basis. As established in quantum measurement theory, such misaligned measurements yield maximally ambiguous results. In practical terms, this manifests as a bit error rate (BER) approaching 50%, equivalent to random guessing, regardless of the eavesdropper's receiver sophistication or computational resources.

This basis randomization mechanism differs fundamentally from conventional encryption in both scope and implementation:

- Scope: Operates at the physical waveform level rather than the digital bit level.
- Secret Nature: Utilizes a continuously evolving parameter stream rather than a fixed-length cryptographic key.
- Security Consequence: Creates physical undecodability rather than computational hardness.

The experimental evidence reviewed in Section 5 consistently validates this mechanism, showing authorized receivers achieving BERs below forward error correction thresholds while unauthorized receivers experience BERs near 50% across all QEPS variants.

4.4. Security Evolution Across QEPS Variants

4.4.1. QEPS-p: Phase-Only Encryption

QEPS-p employs random phase-shift operators $\hat{\phi}(\phi)$ to rotate constellation points around the origin while preserving amplitudes. The resulting cipher forms concentric amplitude rings. While an eavesdropper may infer partial amplitude information, randomized phase relationships prevent stable carrier phase recovery, enforcing the phase synchronization barrier [42]. Studies present QEPS-p in two cryptographic contexts: as a symmetric encryption scheme with shared phase sequences, or as a public-key-like mechanism (QPKE) in round-trip architectures where security arises from inability to coherently reverse an unknown public phase transformation [25].

4.4.2. QEPS-d: Displacement-Based Encryption

QEPS-d employs random displacement operators $\hat{D}(\alpha)$ to translate constellation points across phase space. This obscures both amplitude and phase information, presenting a cipher constellation with no discernible structure. Experimental analyses confirm that without the displacement sequence, both active and passive DSP methods fail due to absence of differential or clustered features, maintaining the 50% BER barrier [22].

4.4.3. QEPS-dd: Dynamic Displacement Operator Encryption

QEPS-dd combines both operations: $\hat{D}(\alpha)\hat{\phi}(\phi)$, where the effective displacement $\alpha + (e^{-i\phi} - 1)\beta$ depends on the data symbol β . This introduces data-dependent randomness, making the cipher appear as continuous noise in phase space. Research indicates this dynamic randomization prevents adaptive tracking, ensuring robust security even against sophisticated DSP-based attacks.

4.5. Contrast with Classical Digital Encryption

In conventional digital encryption (e.g., AES), encrypted data are transmitted using standard modulation formats. An eavesdropper can recover digital ciphertext with high fidelity using standard coherent receivers; security then relies entirely on computational hardness of decrypting that ciphertext.

In contrast, QEPS encrypts at the analog coherent-state level before modulation. The resulting waveform does not conform to a standard QAM constellation and is physically undecodable without the secret key. Even with ideal coherent receivers and advanced DSP, eavesdroppers cannot recover usable digital symbols because the requisite phase synchronization is cryptographically denied at the physical layer. Thus, while AES provides digital-layer security (ciphertext recoverable, but hard to decrypt), QEPS provides physical-layer security (ciphertext unrecoverable as structured symbols).

4.6. The Nature of Secrecy and Attack Considerations

A key distinction from classical symmetric encryption lies in the nature of the secret. In conventional systems, the secret is a finite digital key (e.g., 256 bits), and adversaries can recover structured ciphertext for offline cryptanalysis. In QEPS, the effective secret is a continuously varying stream of physical parameters $(\alpha(t), \phi(t))$. Unauthorized receivers may acquire I/Q samples of the scrambled waveform but lack the dynamic parameter stream needed to restore a structured constellation before symbol decisions. Consequently, the effective secret space grows with transmission duration and symbol rate.

Research further notes that QEPS presents no structured algebraic surface at the physical layer akin to those targeted by analytical attacks in classical cryptography (e.g., linear or differential cryptanalysis). For eavesdroppers, meaningful data recovery requires establishing correct symbol decisions after QAM demapping—contingent on knowing time-

dependent encryption parameters. Absent this knowledge, DSP chains yield essentially random outputs at demapping stages. Attacks thus reduce to exhaustive searches over continuously varying physical parameters, bounded by physical noise and measurement uncertainty rather than mathematical cryptanalysis.

In public-key configurations (QPKE), no static secret exists; security is enforced solely by physical impossibility of coherently demodulating phase-randomized signals without access to complete round-trip exchanges.

4.7. Assessment of Security Analysis in QEPS Literature

The security arguments reviewed here—centered on the phase synchronization barrier—are characteristic of physical-layer security approaches where protection stems from practical implementation constraints rather than abstract mathematical assumptions. While formal cryptographic proofs in reductionist frameworks remain less developed for QEPS compared to classical algorithms, the consistent experimental evidence across multiple studies provides strong operational validation. The demonstrated 50% BER for eavesdroppers across various modulation formats and channel conditions constitutes a direct, measurable security metric. Future research may seek to formalize these physical arguments within information-theoretic or computational models, but current literature establishes QEPS security through demonstrated physical denial of decoding capability—a distinct paradigm from traditional computational security.

4.8. Summary: The Phase Synchronization Barrier in Perspective

The phase synchronization barrier represents a distinct security primitive operating at the intersection of quantum optics and communication theory. It leverages quantum noise of coherent states and practical necessity of phase-synchronized local oscillators to create cryptographic obstruction. Research consistently shows this barrier is:

- Physical rather than computational: Security stems from signal properties, not mathematical hardness.
- Operationally validated: Eavesdroppers' BER approaches 50% in experimental demonstrations.
- Compatible with existing infrastructure: Implemented using standard coherent transceivers and DSP.
- Inherently quantum-resistant: Immune to attacks from both classical and quantum computers, as it does not rely on computational assumptions vulnerable to quantum algorithms.

This distinguishes QEPS not only from classical digital encryption but also from other physical-layer approaches like chaotic encryption, which typically rely on synchronization mechanisms and computational hardness of reconstructing dynamics. By cryptographically controlling phase synchronization itself, QEPS establishes a robust security foundation for next-generation optical networks, as evidenced by the body of work reviewed herein.

5. Experimental Review

This section reviews the principal experimental demonstrations validating Quantum Encryption in Phase Space (QEPS) for coherent optical communications. Three main configurations are discussed: the quantum public key encryption (QPKE) implementation using QEPS-p in a round-trip architecture reported in CLEO and IPC proceedings [21,49], the phase-only symmetric encryption (QEPS-p) implementation reported in Scientific Reports [42], and the displacement-operator encryption (QEPS-d) implementation reported in EPJ Quantum Technology [23].

5.1. QPKE: Quantum Public Key Encryption via Round-Trip Architecture

The QPKE implementation—a practical instantiation of the QEPS-p principle within a round-trip architecture—demonstrates public-key-like functionality at the physical layer using a round-trip architecture with QPSK modulation [21,49]. As illustrated in Figure 2, this infrastructure eliminates the need for pre-shared symmetric keys while maintaining physical-layer security through a unique round-trip protocol.

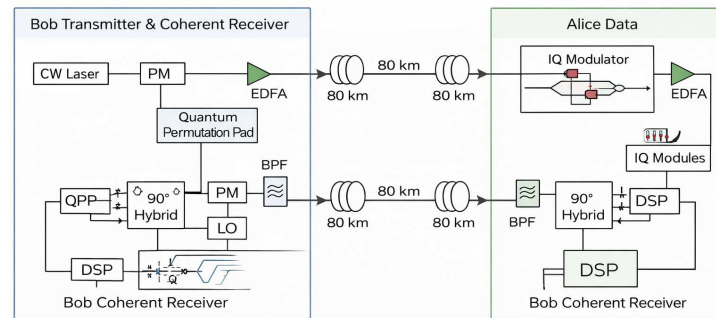


Figure 2. Round-trip QPKE implementation diagram, adapted from [21]. The protocol operates as follows: (1) Bob generates a phase-randomized carrier using a phase modulator (PM) driven by a Quantum Permutation Pad (QPP); (2) This encrypted “envelope” is sent to Alice over 80 km fiber; (3) Alice modulates her data onto the scrambled carrier using an IQ modulator; (4) The doubly-modulated signal returns to Bob, who applies the inverse phase transformation (using the synchronized QPP) before coherent detection and DSP. EDFAs maintain signal power throughout the links.

The QPKE protocol operates as follows:

1. Bob (initiator) generates a random phase sequence using a Quantum Permutation Pad (QPP) and applies it to a continuous-wave (CW) laser via a phase modulator (PM), creating an encrypted “envelope” signal.
2. This phase-randomized carrier is transmitted to Alice over an 80 km standard single-mode fiber link with Erbium-Doped Fiber Amplifier (EDFA) compensation.
3. Alice receives the scrambled carrier and modulates her secret data (at 56 Gbps) onto it using an IQ modulator, effectively “hiding” her information within Bob’s phase randomization without learning or storing the phase sequence.
4. The doubly-modulated signal returns to Bob over another 80 km link. Bob possesses the original phase sequence and applies the inverse phase transformation via synchronized QPP before coherent detection using a 90° hybrid and local oscillator, followed by digital signal processing (DSP).

The critical security insight is that Alice never learns Bob’s phase randomization, and an eavesdropper intercepting either the forward or return path sees only phase-randomized signals. Experimental validation at 200 Gb/s (QPSK over 80 km SMF) demonstrated that authorized communication between Bob and Alice achieves error-free performance, while eavesdroppers on either path experience BER near 50%.

Further security analysis in [49] explored various eavesdropping scenarios, confirming that without access to the complete round-trip exchange and knowledge of the phase randomization, the system maintains robust physical-layer security. This QPKE implementation represents a significant departure from conventional encryption by enabling public-key functionality without computational hardness assumptions, instead relying on the physical impossibility of coherently demodulating phase-randomized signals.

5.2. QEPS-p: Experimental Demonstration of Phase Mask Encryption

The QEPS-p experimental study presents the first systematic experimental validation of phase-based quantum encryption applied to classical coherent optical links using commercially available transceiver components [42]. Building upon the QPKE concept, this work demonstrates the symmetric key version of phase encryption where both transmitter and receiver share the same phase sequence.

Figure 3 (adapted from Figure 2 of [42]) illustrates the experimental implementation. At the transmitter (Alice), a continuous-wave (CW) laser is first modulated by a phase modulator (PM) driven by a deterministic pseudo-random sequence generated from a shared random number generator (RNG). The phase-encrypted optical carrier is then passed through an IQ modulator, which encodes the information-bearing in-phase (I) and quadrature (Q) symbols. The encrypted signal is transmitted over an 80 km standard single-mode fiber link.

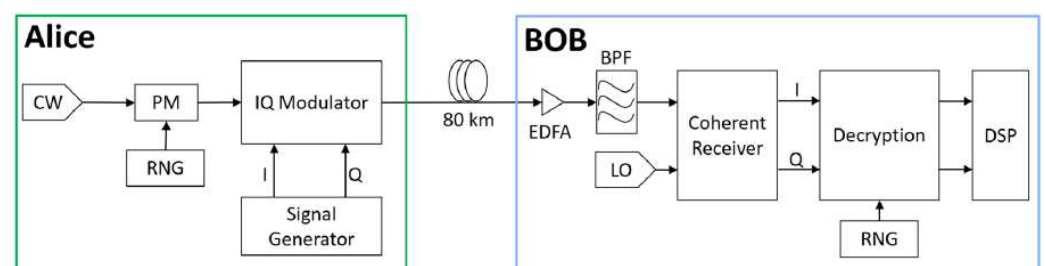


Figure 3. Implementation diagram of phase-only Quantum Encryption in Phase Space (QEPS-p), adapted from Figure 2 of [42]. At the transmitter (Alice), a continuous-wave (CW) laser is modulated by a random phase modulator (PM) driven by a synchronized random number generator (RNG), followed by an IQ modulator encoding the information-bearing I/Q symbols. After transmission over an 80 km fiber link, the receiver (Bob) performs coherent detection using a local oscillator (LO). Decryption using the synchronized RNG is applied prior to digital signal processing (DSP), restoring a standard QAM constellation and enabling carrier phase recovery. Without access to the phase sequence, an unauthorized receiver cannot establish phase synchronization, rendering DSP ineffective.

At the receiver (Bob), coherent detection is performed using a local oscillator, after which the inverse phase operation—driven by the synchronized RNG—is applied before digital signal processing. This ordering is critical: only after decryption does the received signal recover a structured constellation suitable for carrier phase recovery and standard DSP, explicitly enforcing the DSP trust boundary described in Section 4.

The experimental results, summarized in Figure 5 of [42], demonstrate the security impact of phase masking on coherent reception. Using a 16-QAM modulation format, the study compares system performance with and without correct phase decryption. When the phase mask is unknown, the received constellation collapses into a rotationally symmetric ring structure, and carrier phase recovery algorithms fail to converge. As a result, the measured bit error rate (BER) at an unauthorized receiver approaches the random-guessing limit. In contrast, when the correct phase sequence is applied, the original QAM constellation is restored, and the authorized receiver achieves BER performance comparable to an unencrypted coherent link.

Additional experiments reported in [42] extend these observations across multiple modulation formats, including 4-PSK, 16-PSK, and high-order QAM, under practical optical signal-to-noise ratios. In all cases, phase masking effectively denies stable phase synchronization to unauthorized receivers while preserving reliable communication for authorized users. These results experimentally confirm the core QEPS-p security principle:

randomized phase encryption destroys the phase reference required for coherent DSP, thereby enforcing physical-layer security through a phase synchronization barrier.

5.3. QEPS-d: Experimental Validation Using Displacement Operator Encryption

Subsequent work experimentally validated the QEPS framework using random displacement operators rather than phase-only transformations. In “Experimental demonstration of quantum encryption in phase space with displacement operator in coherent optical communications,” displacement operator encryption was applied to coherent states prior to modulation and transmission over a standard coherent optical link [23]. The displacement operator technique (DOCS) randomizes both amplitude and phase by translating constellation points in the two-dimensional phase plane.

This implementation demonstrated that authorized users, with knowledge of the displacement operator parameters, can correctly undo the random displacements and recover the transmitted data with low BER. Unauthorized receivers, in contrast, experienced BER values close to 50% when any mismatch occurred in the displacement coefficients, amplitudes, or phases. The work also explored dual-polarization encryption, applying independent displacement operators to orthogonal polarizations to further increase randomness and resist eavesdropping [23]. These experimental results support the premise that displacement-based encryption further diminishes residual structure in the encrypted signal’s phase space, reinforcing the physical-layer security afforded by the QEPS approach.

Together, these experimental investigations confirm that QEPS implementations can be integrated with existing coherent optical communication infrastructure and that both phase-only and displacement-based encryption effectively deny coherent phase recovery to unauthorized receivers. Security is evidenced by randomized measurement statistics and BER saturation near the random-guessing limit in the absence of the secret encryption parameters, consistent with the phase synchronization barrier described in Section 4.

The progression from QPKE (public-key-like) to symmetric QEPS-p and finally to QEPS-d demonstrates the versatility and scalability of the QEPS framework, offering multiple deployment options ranging from key-agreement-free QPKE to high-security symmetric encryption with displacement operators.

5.4. Summary of Experimental Performance and Achievements

Table 3 summarizes the key performance metrics and security outcomes from the experimental demonstrations of QEPS variants reviewed in this section.

Table 3. Experimental QEPS performance summary.

Variant	Architecture	Auth. BER	Unauth. BER
QPKE	Round-trip, PK-like	$<3.8 \times 10^{-3}$	~50%
QEPS-p	Symmetric phase key	$<3.8 \times 10^{-3}$	~50%
QEPS-d	Symmetric displacement key	$<3.8 \times 10^{-3}$	48–49%

Note: Auth. = Authorized, Unauth. = Unauthorized, BER = Bit Error Rate, FEC threshold $\approx 3.8 \times 10^{-3}$. Modulation formats: QPKE (QPSK), QEPS-p (16-QAM), QEPS-d (DP-QPSK/QAM). Data rates up to 200 Gb/s demonstrated.

The experimental results collectively demonstrate that:

- All QEPS variants successfully enforce a phase synchronization barrier at the physical layer, causing unauthorized receivers to experience a bit error rate (BER) near the theoretical maximum of 50%, equivalent to random guessing.
- Authorized receivers with the correct secret (or, in the case of QPKE, with the ability to apply the inverse transformation) achieve BER performance comparable to unen-

encrypted coherent links, typically below the forward error correction (FEC) threshold ($\sim 3.8 \times 10^{-3}$ for hard-decision FEC).

- The implementations support high-speed transmission (up to 200 Gb/s in experiments) over standard single-mode fiber spans of 80 km, confirming compatibility with existing optical infrastructure.
- Security does not depend on computational complexity but on the physical-layer denial of a stable phase reference, making it inherently resistant to advances in computing power, including quantum computing.
- The framework is versatile, supporting multiple cryptographic models: from public-key emulation (QPKE) that requires no pre-shared secret, to symmetric encryption (QEPS-p, QEPS-d) with enhanced randomness through displacement operators.

These experimental validations confirm that QEPS provides a practical, high-performance approach to physical-layer security for coherent optical communications, with security rooted in fundamental principles of quantum optics and coherent detection rather than in algorithmic complexity.

6. Conclusions

Quantum Encryption in Phase Space (QEPS) represents a transformative approach to securing optical communications by integrating cryptographic operations directly into the physical layer of coherent transmission systems. By exploiting the quantum-mechanical formalism of coherent states and unitary transformations, QEPS fundamentally redefines the security paradigm—shifting from reliance on computational complexity in the digital domain to enforcement of physical barriers in the analog domain. This review has systematically examined the theoretical foundations, security mechanisms, and experimental validations that establish QEPS as a viable and potent framework for next-generation optical security.

At its core, QEPS operates by applying randomized phase shifts, displacements, or combined dynamic operators to data-bearing coherent states before modulation, rendering the transmitted waveform indistinguishable from noise to any receiver lacking the precise inverse transformation. This mechanism disrupts the phase synchronization essential for coherent detection, creating what we term the phase synchronization barrier—a physical-layer obstruction that cannot be circumvented through computational means alone. The result is a cryptographic separation where authorized users achieve near-error-free communication, while eavesdroppers are relegated to bit-error rates approaching 50%, equivalent to random guessing.

The experimental progression from QPKE—a public-key-like round-trip protocol requiring no pre-shared secret—to symmetric QEPS-p and QEPS-d implementations demonstrates the framework's adaptability and practicality. These demonstrations, conducted at data rates up to 200 Gb/s over 80 km of standard fiber, confirm that QEPS can be seamlessly integrated into existing coherent transceiver architectures without sacrificing performance or compatibility. Crucially, security does not degrade with advances in computing power, positioning QEPS as a future-proof solution in an era of evolving computational threats, including those posed by quantum computers.

Nevertheless, the transition from experimental validation to widespread deployment presents several salient challenges. Key among these is the establishment of a scalable and secure key distribution mechanism for high-speed symmetric QEPS implementations. This challenge is uniquely addressed within the QEPS framework itself through a layered security architecture. The round-trip QPKE protocol can first be employed as a physical-layer key establishment mechanism, enabling two parties to agree upon a shared secret without pre-shared keys or reliance on computational hardness. This agreed secret can

then seed the generation of high-speed, symbol-by-symbol encryption sequences for a subsequent symmetric QEPS (p, d, or dd) data session. Alternatively, for environments where a public-key infrastructure is preferred, Post-Quantum Cryptography (PQC) algorithms can perform the initial key agreement, combining computational and physical-layer security. Additional challenges include comprehensive characterization of system performance under real-world channel impairments—such as nonlinearities and polarization effects—and the integration of QEPS within standardized optical transport ecosystems to ensure interoperability with conventional network protocols and management planes.

Looking forward, QEPS opens several promising directions for both theoretical and applied investigation. These include hybrid architectures that combine physical-layer encryption with higher-layer cryptographic protocols, extensions to other coherent transmission domains such as wireless and satellite communications, and the exploration of advanced modulation formats and error-correction schemes tailored to encrypted waveforms. The framework also invites deeper inquiry into the information-theoretic limits of physical-layer security and its interplay with channel capacity and noise resilience.

In conclusion, QEPS establishes a new frontier in optical security—one where protection is embedded not merely in bits, but in the very photons that carry them. By leveraging the principles of quantum optics to enforce security through physical denial rather than mathematical obfuscation, it offers a robust, efficient, and inherently quantum-resistant approach to safeguarding the optical infrastructure that underpins the global digital economy. As research advances toward higher speeds, longer distances, and network-scale demonstrations, QEPS is poised to become a cornerstone of secure optical communications in the decades to come.

Funding: This research received no external funding.

Data Availability Statement: All data generated or analyzed during this study are included in this published article.

Acknowledgments: The author acknowledges the use of language AI tools, including DeepSeek V3.2 and Gemini 3 Flash, for language refinement and editorial assistance. Scientific analyses and conclusions remain the sole responsibility of the author.

Conflicts of Interest: R.K. is a co-founder and Chief Scientist of Quantropi Inc., a company developing post-quantum cryptographic technologies. He is an inventor on patents related to phase-only Quantum Encryption in Phase Space (QEPS) and associated cryptographic frameworks that may be related to this work. No direct external funding was received for this study.

References

1. Shor, P.W. Algorithms for quantum computation: discrete logarithms and factoring. In Proceedings of the 35th Annual Symposium on Foundations of Computer Science, Santa Fe, NM, USA, 20–22 November 1994; pp. 124–134. [CrossRef]
2. Bernstein, D.J. Introduction to Post-Quantum Cryptography. In *Post-Quantum Cryptography*; Bernstein, D.J., Buchmann, J., Dahmen, E., Eds.; Springer: Berlin/Heidelberg, Germany, 2009; pp. 1–14. [CrossRef]
3. Bennett, C.H.; Brassard, G. Quantum cryptography: Public key distribution and coin tossing. In Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India, 10–12 December 1984; pp. 175–179.
4. Wootters, W.K.; Zurek, W.H. A single quantum cannot be cloned. *Nature* **1982**, *299*, 802–803. [CrossRef]
5. Reddy, M.; Mohan, B. Comprehensive Analysis of BB84, A Quantum Key Distribution Protocol. *arXiv* **2023**, arXiv:2312.05609. [CrossRef]
6. Shor, P.W.; Preskill, J. Simple proof of security of the BB84 quantum key distribution protocol. *Phys. Rev. Lett.* **2000**, *85*, 441–444. [CrossRef]
7. Lo, H.K.; Chau, H.F. Unconditional security of quantum key distribution over arbitrarily long distances. *Science* **1999**, *283*, 2050–2056. [CrossRef] [PubMed]
8. Grosshans, F.; Grangier, P. Continuous variable quantum cryptography using coherent states. *Phys. Rev. Lett.* **2002**, *88*, 057902. [CrossRef] [PubMed]

9. Weedbrook, C.; Pirandola, S.; García-Patrón, R.; Cerf, N.J.; Ralph, T.C.; Shapiro, J.H.; Lloyd, S. Gaussian quantum information. *Rev. Mod. Phys.* **2012**, *84*, 621–669. [[CrossRef](#)]
10. Scarani, V.; Bechmann-Pasquinucci, H.; Cerf, N.J.; Dušek, M.; Lütkenhaus, N.; Peev, M. The security of practical quantum key distribution. *Rev. Mod. Phys.* **2009**, *81*, 1301–1350. [[CrossRef](#)]
11. Pirandola, S.; Andersen, U.L.; Banchi, L.; Berta, M.; Bunandar, D.; Colbeck, R.; Englund, D.; Gehring, T.; Lupo, C.; Ottaviani, C.; et al. Advances in quantum cryptography. *Adv. Opt. Photonics* **2020**, *12*, 1012–1236. [[CrossRef](#)]
12. Yin, J.; Cao, Y.; Li, Y.H.; Ren, J.G.; Liao, S.K.; Zhang, L.; Cai, W.Q.; Liu, W.Y.; Li, B.; Dai, H.; et al. Measurement-device-independent quantum key distribution over 404 km optical fiber. *Phys. Rev. Lett.* **2016**, *117*, 190501. [[CrossRef](#)]
13. Deng, F.G.; Long, G.L. Secure direct communication with a quantum one-time pad. *Phys. Rev. A* **2004**, *69*, 052319. [[CrossRef](#)]
14. Hu, J.Y.; Yu, B.; Jing, M.Y.; Xiao, L.T.; Jia, S.T.; Qin, G.Q.; Long, G.L. Experimental quantum secure direct communication with single photons. *Light Sci. Appl.* **2016**, *5*, e16144. [[CrossRef](#)] [[PubMed](#)]
15. Pan, D.; Liu, Y.C.; Niu, P.; Zhang, H.; Zhang, F.; Wang, M.; Song, X.T.; Chen, X.; Zheng, C.; Long, G.L. Simultaneous transmission of information and key exchange using the same photonic quantum states. *Sci. Adv.* **2025**, *11*, eadt4627. [[CrossRef](#)] [[PubMed](#)]
16. Wang, C.; Deng, F.G.; Li, Y.S.; Liu, X.S.; Long, G.L. Quantum secure direct communication with high-dimension quantum superdense coding. *Phys. Rev. A* **2005**, *71*, 044305. [[CrossRef](#)]
17. Zhou, Z.; Sheng, Y.; Niu, P.; Yin, L.; Long, G.; Hanzo, L. Measurement-device-independent quantum secure direct communication. *Sci. China Phys. Mech. Astron.* **2020**, *63*, 230362. [[CrossRef](#)]
18. Sheng, Y.B.; Zhou, L.; Long, G.L. One-step quantum secure direct communication. *Sci. Bull.* **2022**, *67*, 367–374. [[CrossRef](#)]
19. Li, X.J.; Wang, M.; Pan, X.B.; Zhang, Y.R.; Long, G.L. One-Photon-Interference Quantum Secure Direct Communication. *Entropy* **2024**, *26*, 811. [[CrossRef](#)]
20. Zhang, S.; Zheng, C. Quantum Secure Direct Communication Technology-Enhanced Time-Sensitive Networks. *Entropy* **2025**, *27*, 221. [[CrossRef](#)]
21. Shahriar, K.A.; Khalil, M.; Chan, A.; Chen, L.R.; Kuang, R.; Plant, D.V. Physical-Layer Secure Optical Communication Based on Randomized Phase Space in Pseudo-3-Party Infrastructure. In Proceedings of the Conference on Lasers and Electro-Optics, San Jose, CA, USA, 15–20 May 2022; p. SF4L.3. [[CrossRef](#)]
22. Kuang, R.; Chan, A. Quantum encryption in phase space with displacement operators. *EPJ Quantum Technol.* **2023**, *10*, 26. [[CrossRef](#)]
23. Khalil, M.; Chan, A.; Chen, L.R.; Plant, D.V.; Kuang, R. Quantum-Inspired Encryption Using Displacement Operators in Coherent Optical Communications. In Proceedings of the Advanced Photonics Congress 2024, Québec City, QC, Canada, 29 July–1 August 2024; p. SpW2H.6. [[CrossRef](#)]
24. Zhang, C.; Kuang, R.; Wen, K.; Dong, C.; Wu, T.; Zhang, Z. Toward Practical Quantum Encryption in Phase Space: Simulated QPSK and 16-QAM with Dynamic Displacement Operators. *Research Square* **2025**. [[CrossRef](#)]
25. Kuang, R.; Bettenburg, N. Quantum Public Key Distribution using Randomized Glauber States. In Proceedings of the 2020 IEEE International Conference on Quantum Computing and Engineering (QCE), Denver, CO, USA, 12–16 October 2020; pp. 191–196. [[CrossRef](#)]
26. Wu, B.; Zhang, W.; Zhou, H.; Dong, J.; Wang, Y.; Zhang, X. Partially coherent optical chip enables physical-layer public-key encryption. *Opto-Electron. Adv.* **2025**, *8*, 250098. [[CrossRef](#)]
27. Tang, X.; Xu, Z.; Gao, C.; Xiao, Y.; Liu, L.; Zhang, X.; Xi, L.; Xu, H.; Bai, C. Physical layer encryption for coherent PDM system based on polarization perturbations using a digital optical polarization scrambler. *Opt. Express* **2023**, *31*, 26791–26806. [[CrossRef](#)]
28. Li, R.; Gong, X.; Zhang, Q.; Qin, W.; Hou, W.; Guo, L. High-speed coherent optical encryption/decryption system based on cross-phase encoding. *Opt. Express* **2025**, *33*, 33021–33032. [[CrossRef](#)] [[PubMed](#)]
29. Gao, X.; Gu, W.; Deng, Z.; Li, X.; Ye, J.; An, Y.; Bi, S.; Wang, A.; Wang, Y.; Qin, Y.; et al. 40 Gb/s Secure Coherent Optical Communication Based on Electro-Optic Phase Feedback Encryption. *IEEE Photonics Technol. Lett.* **2024**, *36*, 481–484. [[CrossRef](#)]
30. Tan, S.H.; Ouyang, Y.; Rohde, P.P. Practical somewhat-secure quantum somewhat-homomorphic encryption with coherent states. *Phys. Rev. A* **2018**, *97*. [[CrossRef](#)]
31. Liu, Y.; Dong, Z.; Zhu, Y.; Peng, D.; Wang, Y.; Zhang, Y.; Wang, F.; Zhu, W.; Li, D.; Liu, X. Three-channel robust optical encryption via engineering coherence Stokes vector of partially coherent light. *Photonix* **2024**, *5*, 8. [[CrossRef](#)]
32. Larger, L.; Goedgebuer, J.P. Encryption using chaotic dynamics for optical telecommunications. *Comptes Rendus Phys.* **2004**, *5*, 609–611. [[CrossRef](#)]
33. Chen, W.; Mao, X.; Wang, J.; Zhang, R.; Wang, L.; Jia, Z.; Li, P.; Wang, A.; Wang, Y. Optical Chaos Generation and Applications. *Adv. Photonics Res.* **2025**, *6*, 2500055. [[CrossRef](#)]
34. Yu, M.; Wang, H.; Ji, Y.; Zhang, Y. Ultra-wideband chaotic optical communication based on electro-optic differential feedback loop. *Opt. Commun.* **2023**, *545*, 129729. [[CrossRef](#)]
35. Xie, Y.; Yang, Z.; Shi, M.; Zhuge, Q.; Hu, W.; Yi, L. 100 Gb/s coherent chaotic optical communication over 800 km fiber transmission via advanced digital signal processing. *Adv. Photonics Nexus* **2024**, *3*, 016003. [[CrossRef](#)]

36. Jacobo, A.; Soriano, M.C.; Mirasso, C.R.; Colet, P. Chaos-Based Optical Communications: Encryption Versus Nonlinear Filtering. *IEEE J. Quantum Electron.* **2010**, *46*, 499–505. [[CrossRef](#)]
37. Kanakidis, D.; Argyris, A.; Bogris, A.; Syvridis, D. Influence of the decoding process on the performance of chaos encrypted optical communication systems. *J. Light. Technol.* **2006**, *24*, 335–341. [[CrossRef](#)]
38. Ye, J.; Gao, X.; Li, X.; Yang, H.; An, Y.; Xu, P.; Wang, A.; Dong, X.; Wang, Y.; Qin, Y.; et al. Physical layer security-enhanced optical communication based on chaos masking and chaotic hardware encryption. *Opt. Express* **2024**, *32*, 27734–27747. [[CrossRef](#)] [[PubMed](#)]
39. Zhang, C.; Wang, H.; Yang, H.; Ji, Y. Chaotic optical communication decryption framework based on the conv-transformer model. *Opt. Express* **2025**, *33*, 44071–44086. [[CrossRef](#)] [[PubMed](#)]
40. Glauber, R.J. Coherent and incoherent states of the radiation field. *Phys. Rev.* **1963**, *131*, 2766–2788. [[CrossRef](#)]
41. Kuang, R. Quantum encryption in phase space with dynamic displacement operators and quantum permutation pad. *Acad. Quantum* **2025**, *2*, 1–10. [[CrossRef](#)]
42. Chan, A.; Khalil, M.; Shahriar, K.A.; Plant, D.V.; Chen, L.R.; Kuang, R. Encryption in Phase Space for Classical Coherent Optical Communications. *Sci. Rep.* **2023**, *13*, 12965. [[CrossRef](#)]
43. Kuang, R. Quantum Permutation Pad for Quantum Secure Symmetric and Asymmetric Cryptography. *Acad. Quantum* **2025**, *2*, 1–21. [[CrossRef](#)]
44. Taylor, M.G. Coherent Detection for Fiber Optic Communications Using Digital Signal Processing. In Proceedings of the Optical Amplifiers and Their Applications/Coherent Optical Technologies and Applications, Whistler, BC, Canada, 25–30 June 2006; p. CThB1. [[CrossRef](#)]
45. Zhou, X.; Yu, J. Digital signal processing for coherent optical communication. In Proceedings of the 2009 18th Annual Wireless and Optical Communications Conference, Newark, NJ, USA, 1–2 May 2009; pp. 1–5. [[CrossRef](#)]
46. Zhao, J.; Liu, Y.; Xu, T. Advanced DSP for Coherent Optical Fiber Communication. *Appl. Sci.* **2019**, *9*, 4192. [[CrossRef](#)]
47. Khalil, M.; Plant, D.V.; Chan, A.; Chen, L.R.; Kuang, R. Experimental demonstration of quantum encryption in phase space with displacement operator in coherent optical communications. *EPJ Quantum Technol.* **2024**, *11*, 49. [[CrossRef](#)]
48. Kuang, R.; Barbeau, M. Quantum Permutation Pad for Universal Quantum-Safe Cryptography. *Quantum Inf. Process.* **2022**, *21*, 211. [[CrossRef](#)]
49. Shahriar, K.A.; Khalil, M.; Chan, A.; Chen, L.R.; Kuang, R.; Plant, D.V. Security Performance of Physical-Layer Encryption Based on Randomized Phase Space in Optical Fiber Communication. In Proceedings of the 2022 IEEE Photonics Conference (IPC), Vancouver, BC, Canada, 13–17 November 2022; pp. 1–2. [[CrossRef](#)]

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.