Kuang and Chan *EPJ Quantum Technology* (2023) 10:26
https://doi.org/10.1140/epjqt/s40507-023-00183-0

EPJ Quantum Technology
a SpringerOpen Journal

RESEARCH Open Access

Quantum encryption in phase space with displacement operators

Randy Kuang[1*] and Adrian Chan[1]

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

Abstract

In photonic computing, the quantum systems consist of coherent states and squeezed coherent states. Common quantum gates found in these systems are: phase shift, displacement, and squeezing gates. These gates are all unitary and reversible. Outside of quantum systems, coherent states also plays a significant role in coherent optical communications with speeds of hundreds of gigabits per second. Secure optical communications is generally implemented at the data layer with classical symmetric encryption such as Advanced Standard Encryption or AES. This inevitably allows any wiretapping to capture the transmitted data either in the plaintext mode or in the encrypted ciphertext mode in the optical infrastructure. The recent and rapid developments in Quantum computing further lift up the need for quantum secure communications in the optical infrastructure. This paper proposes a novel quantum encryption in the coherent optical domain utilizing a displacement operator and implementing with IQ-MZM optical modules, called Quantum Encryption in Phase Space or QEPS. The communication peers share a secret used to seed cryptographic pseudo random number generators to produce a synchronized random number at both the transmitter and receiver. The synchronized random numbers are used to establish displacement operators to encrypt the coherent states at the transmission and decrypt the cipher coherent states at the receiver. Therefore, malicious parties tapping along the fibre line would not extract the message in transit from optical domain due to a high Bit Error Rate or BER. The optimal displacement operator is split into a standard 16-QAM and a random phase shift operator to enhance the transmission security. We analysis the transmission security with the wiretap channel model for semantic security. We have simulated the QEPS encryption and decryption for two data modulation schemes: QPSK and 16-QAM over 80 km for transmission speeds of 56 Gbps for QPSK and 112 Gbps for 16-QAM.

Keywords: Coherent State; Quantum Encryption; Quantum Decryption; Symmetric encryption; QKD; Symmetric cryptography; QPP; Quantum Communication; Quadrature Amplitude Modulation or QAM; QPSK; IQ-MZM; Displacement Operator; Phase Shift Operator; Coherent Detection; Digital Signal Processing or DSP

1 Introduction

Cryptography can be simply classified into two categories: symmetric and asymmetric. Symmetric cryptography requires a pre-shared key used to encrypt plaintexts and decrypt ciphertexts. The most well-known symmetric encryption algorithm currently used to se-

cure data is Advanced Encryption Standard or AES [1]. AES encryption supports three different key sizes: 128 bits, 192 bits, and 256 bits. For security against the threat of quantum computers, the National Institute of Standards and Technology or NIST currently recommends the use of a 256-bit truely random key for AES encryption against the quantum brute search algorithm proposed by Grover in 1996 [2]. Another well-known symmetric encryption is One-Time-Pad or OTP which has been proven to have perfect secrecy by Shannon in 1948 [3]. However, some restraint to OTP is that it requires the exact same key length as the plaintext length and that the key can only be used once. A new symmetric encryption algorithm has been proposed by Kuang and Bettenburg in 2020 [4], using Quantum Permutation Pad or QPP expressed in terms of permutation matrices. QPP can be considered as an extension of OTP for quantum computing. In 2022, Kuang and Barbeau proposed to build a universal cryptography using QPP [5]. A trial implementation of QPP inside IBM's quantum computer was recently reported by Kuang and Perepechaenko in 2022 [6–8].

Asymmetric cryptography, commonly known as public key cryptography, is used to establish a shared key or session key between communication peers to securely encrypt their communications. The most well-known public key algorithms is RSA [9, 10], which is based on the difficulty of the prime factorization problem, Diffie-Hellman or DH [11], which is based on the difficulty of the discrete logarithm problem, elliptic-curve cryptography [12], which is used for key establishment, and elliptic-curve digital signature algorithms or ECDSA [13]. These public key algorithms form the foundation of the Public Key Infrastructure or PKI for today's information security.

In 1994, Shor proposed a novel algorithm based on quantum mechanics [14], using quantum bits or qubits. Based on the Shor's algorithm, the NP-hard problems: the prime factorization and discrete logarithm, are no longer NP-hard but polynomial time complexity. In November of 2017, NIST began its standardization process for Post-Quantum Cryptography or PQC and has since completed its third round finalists with lattice-based algorithms called Kyber [15], Saber [16], and NTRU [17] and with code-based Classic McEliece [18] for Key Encapsulation Mechanism (KEM). NIST announced Kyber as its selection for KEM and its fourth round candidates in July 2022. Recently, some of the NIST candidate algorithms in Round 3 and Round 4 have been reported to be vulnerable. SIDH [19] and its instantiation SIKE [20] by Robert in 2022 [21] and later more efficient secret recovery by Castryck and Decru in 2022 [22], achieving secret recovery for NIST security level V in less than 2 hours with a laptop. The second major break was by Beullens in early 2022 where he found a new key recovery attacks against Rainbow's digital signature based on the multivariate public key cryptosystem. With just a laptop, Beullens was able to return the secret key over a weekend [23]. Finally, a new cryptoanalysis was recently proposed by Wenger et al. in 2022 [24], using Machine Learning or ML for secret recovery. They have shown that their ML model is able to completely recover the secrets for small to medium lattice dimensions up to $n = 128$. They are working on further improvements to increase its capability for full-scale industry specification. It may still take unknown efforts to achieve this goal, however, this advancement has already opened a new era of cryptoanalysis with ML, especially combining ML with quantum computing.

On the other hand, Kuang, Perepechaenko, and Barbeau in 2022 proposed a novel PQC algorithm called Multivariate Polynomial Public Key (MPPK) encapsulation [25, 26], based on the NP-complete problem of the modular Diophantine Equation Problem.

MPPK offers smaller key and ciphertext sizes with specific inclusion of noise variables to enable it to randomize encryption for the property of IND-CPA. More interestingly, the same authors proposed a new digital signature scheme called MPPK DS in 2022 [27]. MPPK KEM and DS intended to utilize the NP-complete problem for achieving quantum safe objectives.

With quantum system such as photons to implement public key cryptography, Bennett and Brassard in 1984 proposed a novel mechanism by leveraging the physical uncertainty principle of quantum systems, later called as BB84 QKD [28]. Their paper titled "Quantum cryptography: Public key distribution and coin tossing". Indeed, BB84 can be considered as a quantum implementation of Diffie-Hellman (DH) type key exchange protocol. The public key in the DH key exchange is the prime number p. One user called Alice chooses a random secret a to evaluate $A = p^a$ to be sent to Bob, the other user called Bob also chooses a random number b to evaluate $B = p^b$ to be sent to Alice. Then, a shared secret $s = A^b \bmod p = B^a \bmod p = p^{ab} \bmod p$ can be established. In BB84 QKD, photons behave like the public key, Alice, the transmitter, randomly chooses her secret encoding basis and secret bit to quantum mechanically encode into the photon and then sends this photon to Bob. Bob then needs to randomly choose a measurement basis to measure the photon and record the measurement. If Bob chooses the same basis as Alice's encoding basis, quantum mechanics states that Bob reveals the right secret encoded by Alice. However, instead of sending another photon back to Alice, Bob makes an announcement regarding the measuring basis, which can be considered as sending p^b in the DH protocol to Alice. In the ideal case, both Alice and Bob can then establish the shared secret through this method, however, the practical implementation still requires post-processing to correct errors to complete the process of key establishment. This may be the reason why Bennett and Brassard called their protocol as "Quantum cryptography: Public key distribution".

QKD has been proven to offer information theoretical secure key distribution by Renner, Gisin,and Kraus in 2005 [29], if implemented properly. Over the past three decades, vast amounts of research and implementations have been reported on QKD. Furthermore, many implementation variants of QKD have been reported such as: discrete variable QKD with single photons or DV-QKD [30, 31], continuous variable QKD with quadratures of coherent states or CV-QKD [32–34], and twin-field QKD overcoming the distance limitation or TF-QKD [35–41]. TF-QKD proposed by Lucamarini et al. [35] is a fantastic idea to achieve secret sharing quantum mechanically, even more closely mimicking the quantum implementation of DH protocol, with both Alice and Bob perform the same quantum encoding. Figure 1 illustrates the essential protocol directly from [35]. TF-QKD turns a two-party protocol of BB84 QKD into a three-party protocol with an untrusted Charlie party in-between the two communicators. Please refer to the original paper by Lucamarini et al. [35] for a detail description. Here, we will briefly summarize the key points of TF-QKD:

1. Alice and Bob have identical roles in the protocol, very unique compared to the DH scheme;
2. In addition to code phases as standard BB84 QKD with phase encoding, TF-QKD also introduces randomized global phases, equally sliced in the range $[0, 2\pi)$ into M slices, where $M = 16$ was found to be the optimal parameter;
3. Phase modulators at both Alice and Bob are used to modulate the total phase shifts which includes the random global phase, basis bit and secret key bit phases; then

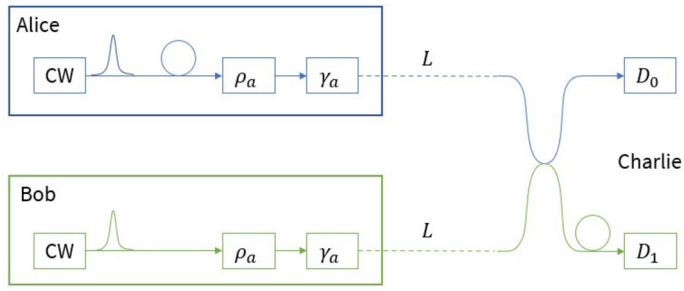

Figure 1 Illustration of TF-QKD scheme. CW is a continuous wave laser; ρ_a and ρ_b are the global randomized phase; γ_a and γ_b are the modulated phase encoding; L is the length of the fiber; D_0 and D_1 are the detectors

both the modulated coherent states of Alice and Bob are transmitted over an identical quantum channels independently to Charlie at the middle;

4. Charlie combines the two coherent states through his beam combiner causing interference and detects the optical signal at D_0 and D_1; Charlie then publicly announces the single detection click events at D_0 and D_1, while ignoring double clicks;
5. Alice and Bob record the single clicks and then announce their random global phase slices and basis chosen. At the end, they form the raw secret;
6. Finally, they apply post processing to establish the shared secret.

The global randomized phases modulated onto the coherent states plays a unique role in the security of the scheme as it can also be considered as a quantum encryption with quantum phase shifting operators $\hat{G}(\phi)$: $\hat{G}(\phi)|\alpha\rangle = |e^{j\phi}\alpha\rangle$ with $|\alpha\rangle = |re^{j\phi_0}\rangle$ denoting the coherent state with intensity r^2 and phase ϕ_0. We also know the phase shifting operator is unitary and reversible: $\hat{G}(\phi)\hat{G}^{-1}(\phi) = 1$.

In general, TF-QKD is not only applicable for long distance, capable of overcoming the distance limitation of traditional QKD, but it is also suitable for short distance. In addition to the public announcement of measuring bases in BB84 QKD, TF-QKD also publicly announces the randomized global phases in order to obtain the raw secret string. Therefore, to improve security by removing the public announcements for measuring bases and global phases, a shared secrets between Alice and Bob is required. A straightforward method to solve this shared secret step is to turn TF-QKD into a virtual three-party protocol:

1. Bob $\longrightarrow$ Bob Tx;
2. Alice $\longrightarrow$ Bob Rx;
3. Charlie $\longrightarrow$ Alice.

This virtual three party protocol creates a new variant of TF-QKD through a round trip configuration called Quantum Public Key Envelope or QPKE by Kuang and Bettenburg in 2020 [42]. Due to the nature of the round trip scheme, the self-shared random number generator RNG can apply a random global phases per coherent pulse without the need for public announcements. This QPKE scheme can also work at higher intensities because Bob randomly encrypts the transmitted coherent states, and when it reaches Alice, she can modulate her secret using any standard Phase Shifting Keying (PSK) format, such as QPSK. Once the optical signal returns to Bob Rx, the decryption can be applied using the same phase shifting operator, however, with the opposite self-shared phase. Then co-

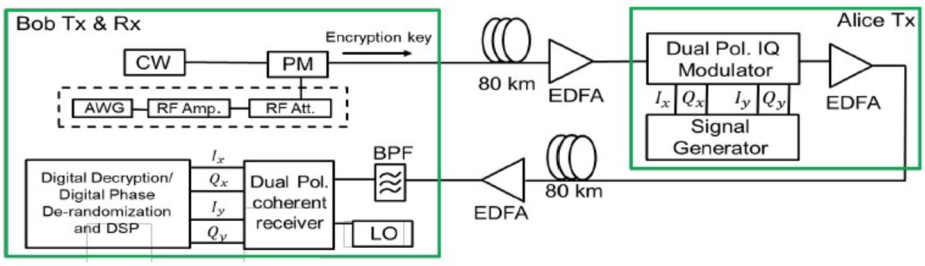

Figure 2 Illustration of TF-QKD scheme from [46]

herent detection can be performed to extract the secret that Alice modulated. A variety of simulations have been reported recently [43–45]. The first experimental implementation was reported by Shahriar et al. in 2022 as shown in Fig. 2 [46] with key rates of 200 Gbps over 80 km. This variant of TF-QKD can also be called Coherent-based Two-field QKD because it uses two coherent state sources: signal and local oscillator or LO, unlike the twin fields in conventional TF-QKD. Since then, the name has changed to Quantum Encryption in Phase Space or QEPS, considering its encryption and decryption in the quantum/optical domain i.e. phase space with phase shift gates implemented using phase modulator. However, QEPS with the phase shift gate encryption only works for data modulation schemes that use PSK schemes. It has been determined and verified theoretically that for quadrature amplitude modulation or QAM schemes, there is a small amplitude information leakage which would provide some information to a malicious party.

In this paper, we further generalize the encryption with the displacement operator, $\hat{D}(\beta)$, for coherent states. This generalization, called Quantum Encryption in Phase Space with displacement operator or QEPS-d, would be naturally applied to encrypt coherent states for coherent optical communications either with a symmetric or with a asymmetric scheme. Section *QEPS with Displacement Operator* introduces the definition of displacement operator used for coherent state encryption and decryption and simulates the encryption and decryption with a displacement operator. Section *Security Analysis* discusses the security analysis using the wiretap channel model.

2 QEPS with displacement operator

In this section, we will first describe coherent states and the displacement operator with their definitions and characteristics, then discuss how to implement the displacement operator with IQ-MZM Modulation. Finally, at the end of this section we will describe the mechanism of QEPS-d as well as its implementation over today's coherent optical networks.

2.1 Coherent states and displacement operator

Coherent state refers to the specific quantum state of the Quantum Harmonic Oscillator or QHS. In 1963, Glauber extended the concept of the traditional coherence in optics [47]. Here, we will briefly introduce the concise definition of the coherent state using Dirac notation as follows,

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

where $|0\rangle$ refers to the vacuum state and $\hat{D}(\alpha)$ is the displacement operator. That means, $\hat{D}(\alpha)$ displaces the vacuum state to a coherent state $|\alpha\rangle = |re^{j\phi}\rangle$, with the amplitude $r = |\alpha|$ and the phase shift ϕ. The coherent state can be also written in a complex modulation form $\alpha = x_I + jx_Q$ with x_I as its in-phase component and x_Q as its quadrature component. This complex modulation form is often used in coherent optical communications.

A coherent state has a specific expression with the annihilation operator $\hat{a}$, operating on a Fock state $|n\rangle$: $\hat{a}|n\rangle = n|n-1\rangle$ or on a coherent state $\hat{a}|\alpha\rangle = \alpha|\alpha\rangle$, and the creation operator $\hat{a}^\dagger$, operating on a Fock state $|n\rangle$: $\hat{a}^\dagger|n\rangle = n|n+1\rangle$. The concise definition of the coherent state using annihilation operators is as follows,

$$|\alpha\rangle = e^{\alpha\hat{a}^\dagger - \alpha^*\hat{a}}|0\rangle. \tag{2}$$

It is clearly seen from Eq. (1) and Eq. (2) that the displacement operator is defined as

$$\hat{D}(\alpha) = e^{\alpha\hat{a}^\dagger - \alpha^*\hat{a}}. \tag{3}$$

From the definition of the displacement operator $\hat{D}(\alpha)$, we can directly see

$$\hat{D}^\dagger(\alpha) = \left[e^{\alpha\hat{a}^\dagger - \alpha^*\hat{a}}\right]^\dagger = e^{\alpha^*\hat{a} - \alpha\hat{a}^\dagger} = \hat{D}^{-1}(\alpha) = \hat{D}(-\alpha) \tag{4}$$

this demonstrates that the displacement operator is an unitary reversible operator $\hat{D}(\alpha)\hat{D}^\dagger(\alpha) = 1$. If we apply the displacement operator $\hat{D}(\alpha)$ to a coherent state $|\beta\rangle$ together with Eq. (3), we have

$$\hat{D}(\alpha)|\beta\rangle = \hat{D}(\alpha)\hat{D}(\beta)|0\rangle = e^{\frac{1}{2}(\alpha\beta^* - \alpha^*\beta)}\hat{D}(\alpha+\beta)|0\rangle, \tag{5}$$

where we can obtain,

$$\hat{D}(\alpha)\hat{D}(\beta) = e^{\frac{1}{2}(\alpha\beta^* - \alpha^*\beta)}\hat{D}(\alpha+\beta) = e^{\delta_{\alpha\beta}}\hat{D}(\alpha+\beta), \tag{6}$$

where $\delta_{\alpha\beta} = \frac{1}{2}(\alpha\beta^* - \alpha^*\beta)$ is the global phase associated with the coherent states $|\alpha\rangle$ and $|\beta\rangle$. Using the same operations as Eq. (6), but with a displacement operator $\hat{D}(\beta)$ operating on a coherent state $|\alpha\rangle$, we can obtain similar results,

$$\hat{D}(\beta)\hat{D}(\alpha) = e^{\frac{1}{2}(\beta\alpha^* - \beta^*\alpha)}\hat{D}(\alpha+\beta) = e^{-\delta_{\alpha\beta}}\hat{D}(\alpha+\beta). \tag{7}$$

Therefore, it is clearly seen from Eq. (6) and Eq. (7) that two different displacement operators are not commutable. Although there is a global phase factor $e^{\delta_{\alpha\beta}}$ appearing in $\hat{D}(\alpha)\hat{D}(\beta)$ and $e^{-\delta_{\alpha\beta}}$ appearing in $\hat{D}(\beta)\hat{D}(\alpha)$, this extra global phase will not impact the actual amplitude and phase measurements of the resultant coherent state $|\alpha+\beta\rangle$. Based on the actual impact on measurement, we will introduce a variant of the commutable displacement operator $\hat{d}(\alpha)$ by excluding the extra global phase factor as follows,

$$\begin{aligned} &\hat{d}(\alpha)|\beta\rangle = \hat{d}(\beta)|\alpha\rangle = |\alpha+\beta\rangle; \\ &\hat{d}(\alpha)\hat{d}(\beta) = \hat{d}(\beta)\hat{d}(\alpha) = \hat{d}(\alpha+\beta). \end{aligned} \tag{8}$$

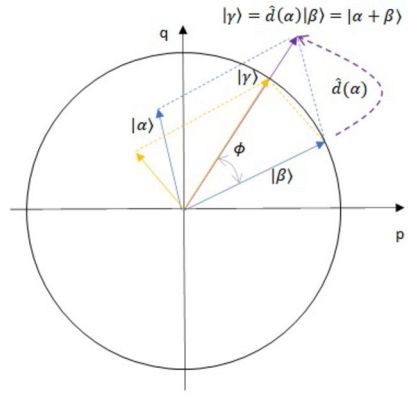

Figure 3 Illustration of displacement operator $\hat{d}(\alpha)$ as well as the phase shift operator $\hat{d}(\alpha = |\beta|e^{j\phi})$, operating on a coherent state $|\beta\rangle$

We illustrate the displacement operator in Fig. 3. It is easily seen that a displacement operation of $\hat{d}(\alpha)$ on a coherent state $|\beta\rangle$ is equivalent to performing an addition of two complex vectors α and β in the phase space, when ignoring the global phase factor $\delta_{\alpha\beta}$. Shown in yellow is also the phase shift operator operating on the coherent state $|\beta\rangle$. This case demonstrates that the phase shift operator is just a special case of the displacement operator $\hat{d}(\alpha = |\beta|e^{j\phi})$ without changing the amplitude of $|\beta\rangle$.

Equation (8) also demonstrates that a displacement operator $\hat{d}(\alpha)$ can be split into two or more sub-displacement operators: $\hat{d}(\alpha) = \hat{d}(\alpha_1)\hat{d}(\alpha_2)$ if $\alpha = \alpha_1 + \alpha_2$. This feature benefits our implementation of randomly chosen displacement operators by splitting it into a standard QAM for $\hat{d}(\alpha_1)$ as seen in the next section and a random phase operator $\hat{d}(\alpha_2)$ [42].

However, it should be noticed that once the a displacement operator $\hat{d}(\alpha_2)$ is specifically used as phase shift operator $\hat{\varphi}(\phi)$, the operation order does indeed matter because displacement operator $\hat{d}(\alpha)$ is generally not commutable with a phase shift operator $\hat{\varphi}(\phi)$ or so-called uncertainty principle $\hat{d}(\alpha)\hat{\varphi}(\phi)|\beta\rangle \neq \hat{\varphi}(\phi)\hat{d}(\alpha)|\beta\rangle$. This uncertainty relationship becomes the base of the proposed QEPS encryption mechanism. It requires the attacker to accurately know the encryption operators used at the transmission end. If not, any attempt decryption actually becomes a new encryption to the coherent state $|\beta\rangle$.

Finally, in the QEPS-d subsection displacement operators will be shown to be capable of being performed in different orders, even possible in different domains such as coherent optical domain for both encryption and decryption or coherent optical domain for encryption and then in the electrical domain for decryption after coherent detection.

2.2 Displacement operator, IQ-MZM modulator and coherent detection

For coherent optical communications, the transmission side mainly consists of a laser diode or LD, emitting coherent pulses, a Data to Analogue Converter or DAC (also called Arbitrary Waveform Generator or AWG), and a In-phase/Quadrature Mach-Zehnder Modulators or IQ-MZM used to modulate data in both amplitude and phase of a coherent state or called Quadrature Amplitude Modulation (QAM). Figure 4 illustrates how digital data is modulated onto the coherent optical signal or coherent state with an IQ-MZM. For QAM modulation, the most common modulation schemes are 16-QAM for 4-bits of data, 32-QAM for 5-bits of data, 64-QAM for 6-bits of data, and so on. Each coherent state or signal pulse represents 4, 5, and 6 bits in 16-QAM, 32-QAM, and 64-QAM, respectively.

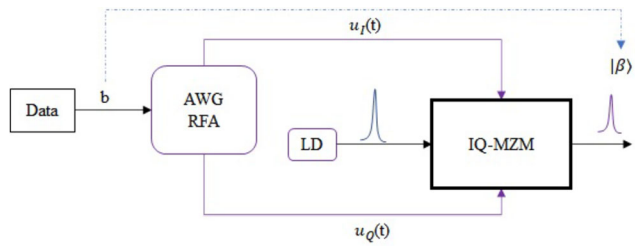

Figure 4 Illustration of the process to modulate data b with IQ-MZM into a coherent state $|\beta\rangle$

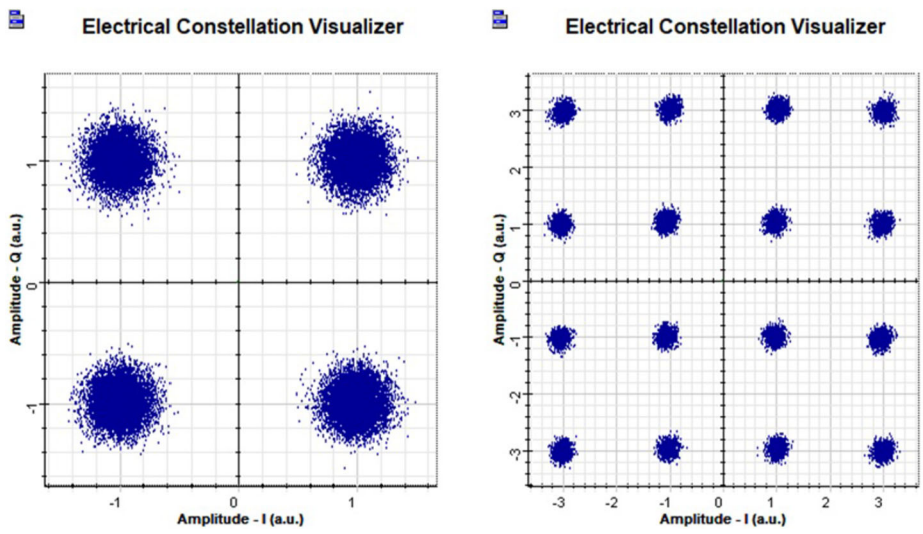

Figure 5 Illustration of data b mapping to QAM modulations with QPSK and 16-QAM. On the one hand, each constellation point is expressed with I-component and Q-component of the modulated coherent state in the phase space. On the other hand, each constellation point represents a coherent state associated with a bit string. For QPSK, the constellation points represents 00, 01, 10, 11. For 16-QAM, the constellation points represents a 4-bit string

Based on the selected M-QAM, the data stream would be segmented into $\log_2 M$ bit segments. Each data segment b is first converted into voltages through a AWG where two outputs are given based on the complex modulation form of data b. One output, $u_I(t)$, is supplied to the IQ-MZM's I input arm and the other output, $u_Q(t)$, is supplied to IQ-MZM's Q input arm. Once the laser source LD emits a coherent pulse and passes through the IQ-MZM, the output pulse, $|\beta\rangle$, represents data, b, as shown in Fig. 4. By considering the initial coherent pulse emitted from LD as $|0\rangle$, the IQ-MZM modulation can be expressed in terms of quantum mechanics: $|\beta\rangle = \hat{d}(\beta)|0\rangle$.

Figure 5 demonstrates the relationship between the binary data element b and the I/Q quadrature representation for coherent states. This figure displays two different constellations: QPSK with 4 constellation points and 16-QAM with 16 constellation points.

Coherent detection has been well-established during the past decades and can be generalized into two methods: homodyne detection and heterodyne detection. The main difference is that homodyne detection uses the exact same frequency for both the signal laser and local oscillator, while heterodyne detection uses a different frequency for the local oscillator compared to the signal laser. Figure 6 illustrates a typical coherent detec-

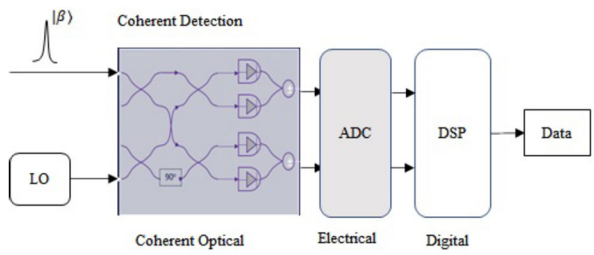

Figure 6 Illustration of a typical coherent detection scheme to extract transmitted data from coherent signal states back to binary data stream

tion scheme to extract transmitted data from coherent signal states back to a binary data stream. LO refers to the local oscillator, coherent state $|\beta\rangle$ refers to the input modulated signal, ADC refers to analogue to digital converter, and DSP refers to the digital signal processing used to compensate and correct all environment causes from the transmission point to the receiving point. For standard modulation schemes, DSP can correctly compensate the environment factors with a good acceptable Bit-Error-Rate or BER.

2.3 QEPS encryption and decryption with displacement operator

QEPS encryption in the quantum/optical domain can be achieved by using a displacement operator $\hat{d}(\alpha)$ on a coherent state $|\beta\rangle$

$$\hat{d}(\alpha)|\beta\rangle = |\gamma\rangle = |\alpha + \beta\rangle,$$

where $|\beta\rangle$ is called the plain coherent state and $|\gamma\rangle$ is called the cipher coherent state. Furthermore, due to advances in DSP, we can consider the transmission over the fibre line as ideal; DSP is able to compensate for environment factors such as dispersion, attenuation, etc. In the last subsection, we stated that the data modulation scheme can be a standard modulation scheme such as Quadrature Phase Shift Keying or QPSK with data represented by four phases or QAM with data represented by both an amplitude and a phase. These schemes will be used to validate the feasibility of the QEPS-d encryption with Displacement Operator. Simulations were performed in Optisystem of the QEPS-d encryption with $\hat{d}(\alpha)$ and decryption with $\hat{d}(-\alpha)$. First, we selected a standard QAM modulation for the purpose of illustrating the concept. We will use QPSK and 16-QAM for the modulation formats for data or $|\beta\rangle$ modulation and 16-QAM for the QEPS-d encryption and decryption format.

Figure 8 illustrates the simulation with a back-2-back or B2B and a 80 km long fiber configurations with eight detection constellation diagrams. The simulation parameters are listed in Table 1 and simulation layout is illustrated in Fig. 7.

QEPS-d was simulated with two data modulations denoted as coherent state, $|\beta\rangle$, implemented with modulation formats QPSK and 16-QAM, while the encryption, $\hat{d}(\alpha)$, was implemented with 16-QAM. The classical encryption key is used to seed a random number generator. The generated pseudo random numbers are then used to drive the voltages $u_I(t)$ and $u_Q(t)$ of IQ-MZM. Therefore, the shared secret at both the transmitter and receiver would produce the same pseudo random numbers for the displacement operator $\hat{d}(\alpha)$ at the transmitter and $\hat{d}(-\alpha)$ at the receiver.

Table 1 QEPS-d simulation parameters

Layout Parameter	Sequence length	65,536 bits
	Baudrate	28 Gbaud
	PM period	1024
CW Laser and LO Laser	Center wavelength	1550 nm
	Power	5 dBm
	Linewidth	0.1 MHz
	Azimuth	0.45 degree
IQ Modulator	Extinction ratio	20 dB
	Switching bias	3 V
	Insertion loss	5 dB
EDFA	Forward pump power	13-14 mW
	Forward pump wavelength	980 nm
	Loss at 1550 nm	0.1 dB/m
	Loss at 980 nm	0.15 dB/m
Optical Fiber	Length (1 spool)	80 km
	Attenuation	0.2 dB/km
	Dispersion	16.75 ps/nm/km
	Dispersion slope	0.075 ps/nm2/km
	Differential group delay	0.2 ps/km
	Effective area	80 μm^2

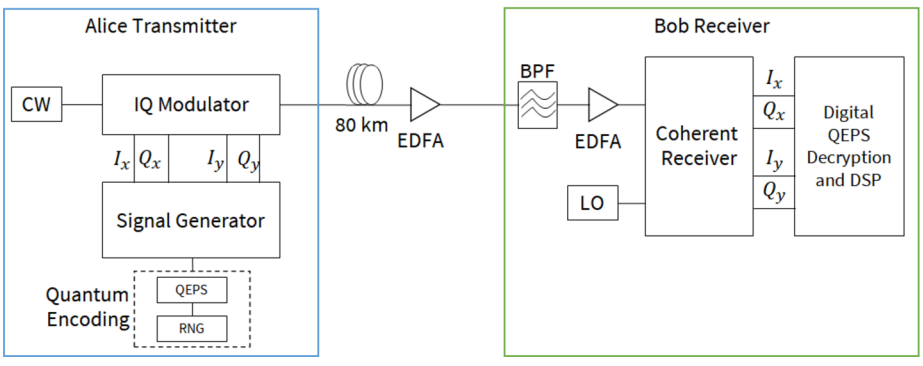

Figure 7 QEPS-d simulation layout. This layout contains the QEPS module for the $\hat{d}(\boldsymbol{\alpha}) = \hat{d}(\boldsymbol{\alpha}_1)\hat{d}(\boldsymbol{\alpha}_2)$ with $\hat{d}(\boldsymbol{\alpha}_2)$ to be a phase shift operator to be discussed later

Figure 8 illustrates the simulations of QEPS-d encryption and decryption for two configurations: back-2-back without fiber or B2B on the left four graphs and 80 km fiber link between transmitter and receiver on the right four graphs. Figure 8(a) displays the direct encryption of QPSK modulated coherent states representing a 2-bit data to be encrypted with $\hat{d}(\alpha)$, implemented with IQ-MZM and α representing the 4-bit encryption key converted through a DAC to apply 16-QAM. It is clearly seen that each QPSK data coherent state is mapped into 16 points by $\hat{d}(\alpha)$ with the 16-QAM encryption modulation. That is why the original QPSK constellation diagram becomes a distorted 64 point QAM constellation. Figure 8(b) is the constellation diagram from the coherent detection after using QEPS-d decryption $\hat{d}(-\alpha)$ without DSP processing. It can be seen that the QPSK constellation diagram is restored with a small bit error rate or BER. Figure 8(c) illustrates the detection with DSP processing directly from Fig. 8(a). It is clear that the original QPSK modulated data can not be restored. The BER is at 49%, very close to 50%, resulting in the malicious party being unable to decide whether the bit equal to 0 or 1. Once the DSP

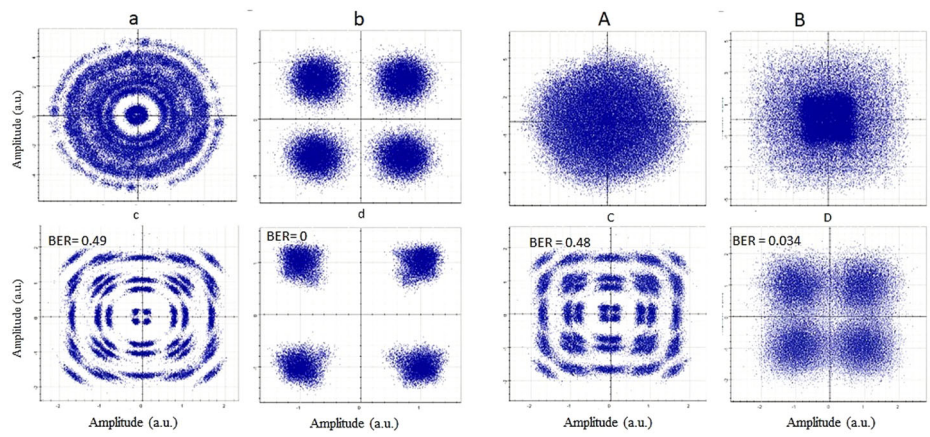

Figure 8 Illustration of a typical QPSK data modulation with 16-QAM QEPS encryption using displacement operator $\hat{d}(\boldsymbol{\alpha})$ for a back-to-back scheme without fibres. Fig. (a) is a constellation with $\hat{d}(\boldsymbol{\alpha})$ encryption and then direction coherent detection without decryption using $\hat{d}(-\boldsymbol{\alpha})$, and Fig. (b) denotes the constellation after $\hat{d}(-\boldsymbol{\alpha})$ decryption from Fig. (a). Fig. (c) is a constellation diagram applying DSP directly to Fig. (a). Fig. (d) is a constellation diagram applying DSP directly to Fig. (b). Figs. (A), (B), (C), (D) are the corresponding constellation diagrams at 80 km, respectively

is applied for the decrypted detection data as shown in Fig. 8(b), the nice clean QPSK constellation in Fig. 8(d) is restored with 0% BER.

Figure 8 right hand four graphs illustrate the same constellations as in the case of B2B, but over a 80 km fiber link. Figure 8(A) is the same constellation diagram from Fig. 8(a), but completely distorted by the physical 80 km fiber. Despite the fiber travel, the pattern is still visible with a lot of random background noise. The decrypted constellation Fig. 8(B) is completely different from Fig. 8(b) without any noticeable similarities to the QPSK constellation. Then the DSP compensated constellation Fig. 8(D) restores the QPSK pattern with a BER 3.5%. The interesting case is the constellation Fig. 8(C) with DSP compensations directly applied to Fig. 8(A), with a BER 48%. That means, it is impossible to extract useful transmitted data without performing decryption at the receiving side.

Figure 9 illustrates the constellation diagram for QEPS-d encryption and decryption using a 16-QAM for data modulation. The encrypted constellations for B2B configuration displays a 49-QAM pattern not $16 \times 16 \longrightarrow 256$-QAM. That is because the encryption $\hat{d}(\alpha)|\beta\rangle = |\alpha + \beta\rangle$ with α and $\beta \in [-3, -1, 1, 3]$. Thus, $|\gamma = \alpha + \beta\rangle$ with $\gamma \in [-6, -4, -2, 0, 2, 4, 6]$ which creates a constellation of 49 points or 49-QAM. After the decryption using $\hat{d}(-\alpha)$, Fig. 9(b) and Fig. 9(d) after DSP restores the data to the original standard 16-QAM constellations. However, with just DSP algorithms, it is impossible to restore 16-QAM constellation from the encrypted constellation in Fig. 9(a) as shown in Fig. 9(c), with a BER 45%.

The simulation with 80 km fiber link is graphed in the right hand four graphs of Fig. 9. The encrypted constellation detected at 80 km is distorted from Fig. 9(a) to Fig. 9(A). The overall pattern is still clearly visible with some random background points due to fiber transmission. It is also shown from Fig. 9(A) that the density of points changes from higher inside to lower outside. This reflects the weights of each constellation points based on the encryption actual situations. The points at the edges of the constellation have a weight = 1. Figure 9(B) clearly demonstrates the distorted 16-QAM constellation after the correct decryption, $\hat{d}(-\alpha)$, has been applied. The original 16-QAM constellation is

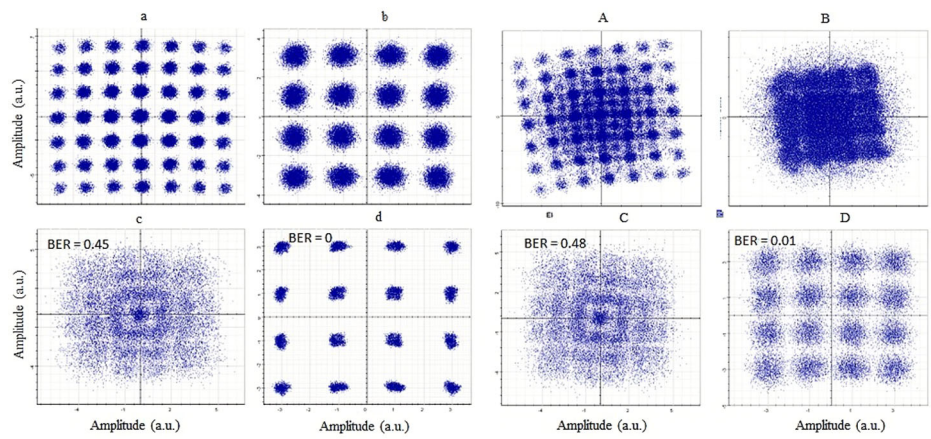

Figure 9 Illustration of a typical 16-QAM data modulation with 16-QAM QEPS encryption using displacement operator $\hat{d}(\boldsymbol{\alpha})$ for 80 km fibre link. Fig. (a) is a constellation with $\hat{d}(\boldsymbol{\alpha})$ encryption and then direction coherent detection without decryption using $\hat{d}(-\boldsymbol{\alpha})$, and Fig. (b) denotes the constellation after $\hat{d}(-\boldsymbol{\alpha})$ decryption from Fig. (a). Fig. (c) is a constellation diagram applying DSP directly for Fig. (a). Fig. (d) is a constellation diagram applying DSP for Fig. (b). Figs. (A), (B), (C), (D) are the corresponding constellation diagrams at 80 km, respectively

restored through DSP compensations as shown in Fig. 9(D) with an acceptable BER of 1%. Without applying the decryption with $\hat{d}(-\alpha)$ but directly applying DSP processing, Fig. 9(C) displays the somewhat random constellation with a large BER 48%.

Although the above simulations, Fig. 8 and Fig. 9, demonstrated that coherent detection without the correct decryption using $\hat{d}(-\alpha)$ results in a large BER (more than 45%), it does mean that it is impossible to extract the transmitted data. Although seemingly secure, the detected constellation diagram itself visually leaks some information at the edges of the constellation diagrams, especially the information of the displacement operator $\hat{d}(\alpha)$. In order to overcome this, we would have to use random continuous displacement operator $\hat{d}(\alpha)$ which would produce a truly random constellation diagram which leaks no information. It should also be noted that the edge of the constellation diagram does not necessarily associate with the edge of the displacement operator. As we described in the last section, by taking advantage of the displacements operator, $\hat{d}(\alpha)$, decoupling into $\hat{d}(\alpha_1)$ for a standard QAM modulation implementation and $\hat{d}(\alpha_2)$ for a random phase shift operator which has previously been implemented in [46].

Figure 10 illustrates the corresponding simulation as shown in Fig. 8 for QPSK data modulations but followed with a random phase shifting operator $\hat{d}(\alpha_2) \rightarrow \hat{\phi}(\varphi)$. It can clearly be seen from Fig. 10(a) that the random phase shift operator $\hat{d}(\alpha_2)$ completely erases the constellation pattern as seen in Fig. 8(a), or rings corresponding to each amplitude. There are total 5-6 rings from the center to the outer edge. As expected, the direct decryption for the B2B configuration in Fig. 10(b) can completely restore the QPSK constellation without error as shown in Fig. 10(d) together with DSP processing. However, without any sort of decryption performed the constellation with DSP from Fig. 10(a) gives a big BER 49%.

It is more interesting to see from Fig. 10(A) to Fig. 10(D) that the encryption with a displacement operator $\hat{d}(\alpha_1)$ and a random phase shift operator $\hat{d}(\alpha_2)$ turns the distorted 64 point QAM constellation Fig. 8(A) into a totally random constellation Fig. 10(A). This is exactly what we expect with an analog encryption. Without knowing the correct shared secret to control the phase shift operator, any form of attack from the detected random

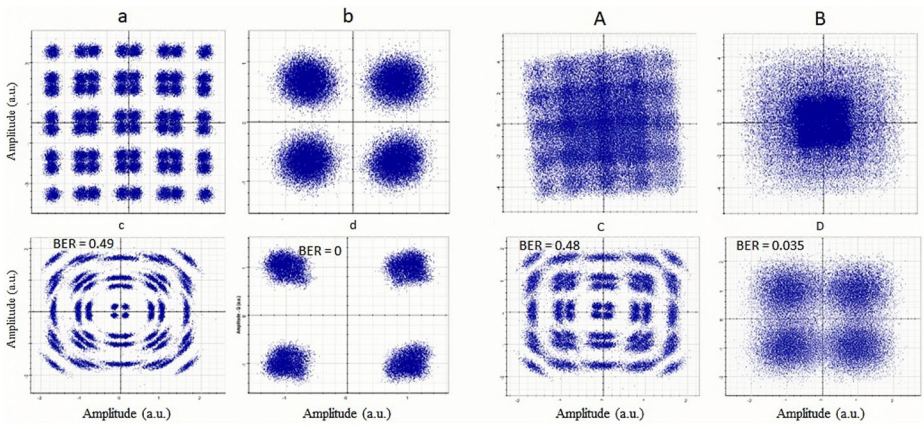

Figure 10 Illustration of a typical QPSK data modulation encrypted with $\hat{d}(\boldsymbol{\alpha}) = \hat{d}(\boldsymbol{\alpha}_1)\hat{d}(\boldsymbol{\alpha}_2)$ with $\hat{d}(\boldsymbol{\alpha}_1)$ applying a 16-QAM encryption and $\hat{d}(\boldsymbol{\alpha}_2)$ applying a random phase shift operator for back-to-back without fibre for the four graphs on the left hand side and for 80 km fiber for the four graphs on the right hand side. (a) is the constellation diagram with $\hat{d}(\boldsymbol{\alpha})$ encryption and then direction coherent detection without decryption using $\hat{d}(-\boldsymbol{\alpha})$, and (b) denotes the constellation diagram after $\hat{d}(-\boldsymbol{\alpha})$ decryption from (a). (c) is a constellation diagram applying DSP directly to (a). (d) is the constellation diagram applying DSP to (b). (A), (B), (C), (D) are the corresponding constellation diagrams at 80 km, respectively

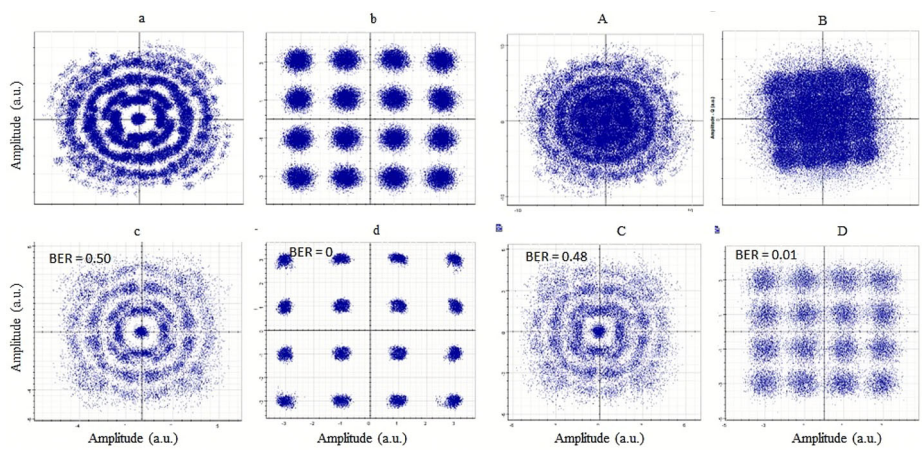

Figure 11 Illustration of a typical 16-QAM data modulation encrypted with $\hat{d}(\boldsymbol{\alpha}) = \hat{d}(\boldsymbol{\alpha}_1)\hat{d}(\boldsymbol{\alpha}_2)$ with $\hat{d}(\boldsymbol{\alpha}_1)$ applying a 16-QAM encryption and $\hat{d}(\boldsymbol{\alpha}_2)$ applying a random phase shift operator for back-to-back without fibre for the four graphs on the left hand side and for 80 km fiber for the four graphs on the right hand side. (a) is the constellation diagram with $\hat{d}(\boldsymbol{\alpha})$ encryption and then direction coherent detection without decryption using $\hat{d}(-\boldsymbol{\alpha})$, and (b) denotes the constellation diagram after $\hat{d}(-\boldsymbol{\alpha})$ decryption from (a). (c) is a constellation diagram applying DSP directly to (a). (d) is the constellation diagram applying DSP to (b). (A), (B), (C), (D) are the corresponding constellation diagrams at 80 km, respectively

constellation Fig. 10(A) will not extract any useful data as shown in Fig. 10(C) with a BER of 48%. For a trusted receiver with the pre-shared secret, the correct decryption with $\hat{d}(\alpha_1\hat{d}(\alpha_2)$ produces a constellation Fig. 10(B) and with DSP processing the correct QPSK constellation, Fig. 10(D), can be recovered with an acceptable BER 3.5%.

We display the QEPS encryption for 16-QAM data modulation in Fig. 11 for the B2B and 80 km fiber line respectively. In the B2B configuration, the encrypted constellation Fig. 11(a) clearly demonstrates a transformation from a 49 point QAM pattern in Fig. 8(a)

to 7 rings representing the amplitudes of the cipher coherent states. The direct DSP processing still produces the similar rings with a big BER 49%. The correct decryption restores the data back to its original form, a 16-QAM data constellation with 0 BER as shown in Fig. 11(d). In the case of a 80 km fiber line, the detection cipher constellation creats a random ring constellation Fig. 11(A). It produces a distorted 16-QAM with a scattered random background points seen in Fig. 11(B). Once the DSP processing is applied, the transmitted 16-QAM data constellation is obtained with a slightly larger BER of 1%. For any attacks without knowing the shared secret, Fig. 11(C) indicates that it is impossible to extract any useful data.

2.4 Speed

The above simulations utilized a Baudrate of 28GBaud, so the achieveable communication speed for QPSK data modulation was 56 Gbps and for 16-QAM data modulation was 112 Gbps. If polarization multiplexing was used, which is possible with our encryption method, then the bit rate would be doubled.

2.5 Alternatives to QKD

QKD was designed to take the physical uncertainty principle of photons in order to maintain its information theoretic security. However, in the practical implementations, single photon source are generally replaced with weak coherent sources. Furthermore, QKD currently requires a pre-shared key to perform post-processing for authentication. If that pre-shared key is used to seed a cryptographic pseudo random number generator such as pseudo Quantum Random Number Generator or pQRNG [48], QEPS can become a practical alternative to QKD over current coherent optical network with commercial available coherent optical modules.

QEPS can be implemented in a round trip configuration so that Bob at the transmission side is capable of creating a random envelope $|\alpha\rangle$ produced from $\hat{d}(\alpha) = \hat{d}(\alpha_1)\hat{d}(\alpha_2)$. This random envelope operates on an coherent state emitted from a laser diode and the resultant signal then sends $|\alpha\rangle$ to the remote Alice. Once received, Alice will randomly generates her secret $k \longrightarrow |\beta\rangle$ and modulate it into $\hat{d}(\beta)|\alpha\rangle \longrightarrow |\alpha+\beta\rangle$ and return it back to Bob. When $|\alpha+\beta\rangle$ arrives at Bob, he can decrypt the received signal with $\hat{d}(-\alpha)|\alpha+\beta\rangle \longrightarrow |\beta\rangle$ then perform coherent detection to recover the Alice's secret k. The benefit to implementing the configuration in a round trip is to improve security through a self-shared random secret for authentication. This is in contrast to the commonly used pre-shared secret method. This round trip QEPS is similar to the RSA public key scenario [42] and the traditional QKD is similar to Diffie-Hellman public key algorithm.

QKD takes the advantage of the uncertainty principle from two conjugate bases for single photons, while QEPS benefits from randomly chosen displacement operator, $\hat{d}(\alpha)$, to create its uncertainty in the measured constellation, pushing the detected bits towards the maximum BER of 50% for the Eve.

3 Security analysis

In addition to Shannon's perfect secrecy [3] with a pre-shared key cryptosystem, Wyner also made his notion of secrecy system called the wiretap channel [49] without any pre-shared key between communication peers Alice and Bob. The main assumption for Wyner's wiretap channel is a less noisy channel between Alice and Bob than the wiretap

channel between Alice and Eve and the randomness of the message at the transmitter Alice. There are some challenges on these two conditions: messages to be transmitted may be files, images, plain language documents with language alphabets which results in patterns and the wiretap channel for the Eve may not actually be more noisy than the main channel between Alice and Bob. Thangaraj et al. in 2004 [50] discussed the limits and coding methods of the Wyner wiretap channel for application of coding with Low-Density Parity Check or LDPC. Maurer and Wolf in 2000 considered the information theoretical security of Wyner's wiretap channel based on correlated randomness and public discussion [51]. Nafea and Yener in 2017 [52] proposed a new wiretap channel model called wiretap channel II for strong secrecy capacity. Bellare et al. in 2012 proposed their cryptographic treatment of the wiretap channel for semantic security [53, 54].

Wyner's wiretap channel may not be limited only to physical layer secure communications. Classical cryptosystems such as symmetric encryption using AES or OTP and asymmetric encryption such as RSA or Diffie-Hellman can also be interpreted with Wyner's wiretap channel model where the main channel between Alice and Bob is noiseless for ciphertexts transmission. Alice encrypts messages M with the encryption key, transmits the ciphertexts $\mathcal{E}(M)$ to Bob and Bob can decrypt the ciphertexts $\mathcal{E}(M)$ with the decryption key for M. Then, Eve intercepts the ciphertexts over the wiretap channel $\mathcal{E}(M)$. The mutual information between the Eve and Alice is defined as $I(M, Z = \mathcal{E}(M)) < \epsilon$ with $\epsilon > 0$. In this case, Eve is able to receives an identical ciphertext $Z = \mathcal{E}(M)$ as Bob. However, without the decryption key, Eve can only perform a brute force search of the message M. The value of ϵ in the mutual information $I(M, Z = \mathcal{E}(M))$ depends on the required security level and cryptographic algorithms. The mutual information $I(M, Z = \mathcal{E}(M))$ between Alice and the Eve can be written as

$$I\big(M, Z = \mathcal{E}_K(M)\big) = \sum_{x \in \mathcal{M}} \sum_{z \in \mathcal{Z}} P(x,z) \log \frac{P(x,z)}{P(x)P(z)}, \tag{9}$$

where $P(x), P(z), P(x,z)$ are the probability distributions of the plaintext message, the probability distributions of the ciphertext, and joint probability distribution of the plaintext and ciphertext, respectively. $\mathcal{E}_K(.)$ denotes the encryption algorithm with a key K. In order to achieve good security against Eve, the encryption is required to produce a good uniform distribution of the ciphertext. Then the mutual information $I(M, Z = \mathcal{E}(M))$ can be re-expressed

$$I\big(M, Z = \mathcal{E}_K(M)\big) \longrightarrow I\big(K, Z = \mathcal{E}_K(M)\big) = H(K) - H\big(K|Z = \mathcal{E}_K(M)\big), \tag{10}$$

where the random variable K has a uniform distribution. While knowing the key $k \in K$ and the message associated with the ciphertext $Z = \mathcal{E}(M)$, the message $m \in M$ can be decrypted. In Eq. (10), $H(K)$ is the entropy of the random variable K and $H(K|Z = \mathcal{E}_K(M))$ is the entropy of the random variable key under the given condition of knowing the ciphertext Z. In the ideal case of truly random distributions of K and encrypted ciphertext with a proven encryption algorithm such as OTP, the mutual information $I(K, Z = \mathcal{E}_K(M))$ is equal to zero. However, the practical case would be $I(K, Z = \mathcal{E}_K(M)) < \epsilon$ with $\epsilon \geq 0$.

Bellare et al. in 2010 proposed a new model of semantic security or *ss* for the wiretap channel [53, 54] using the *ss* ADVantage

$$\mathrm{ADV}^{\mathbf{ss}}\big(\mathcal{E}, Z = \mathcal{E}(M)\big) = \max_M \big(\mathrm{GP}\big(M|\mathcal{E}(M)\big) - \mathrm{GP}(M)\big), \tag{11}$$

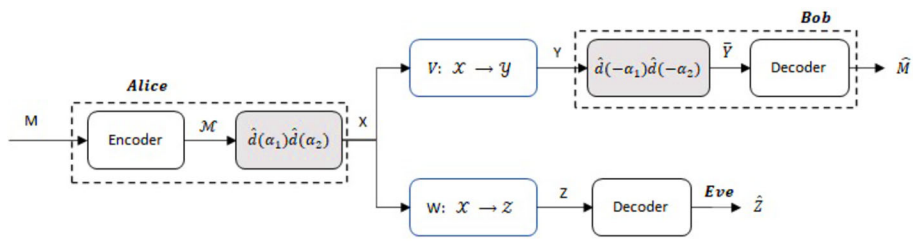

Figure 12 Illustration of Wyner's wiretap channel for QEPS-d encryption. The dashed box at the transmitter side represents a standard data modulation such as QPSK together with the QEPS-d encryption. The dashed box at the receiver side represents standard coherent detection together with the QEPS-d decryption. In this model, we assume the Eve also has the same standard coherent detection as Bob and knows what the data modulation is at the transmitter

where the maximum is over all random variables M, GP(M) is the Guessing Probability of M without any condition and GP($M|\mathcal{E}(M)$) is the Guessing Probability with the known ciphertext $\mathcal{E}(M)$.

We plan to adapt this advantage definition as shown in Eq. (11) with the wiretap channel for our QEPS security analysis. One reason for this is our QEPS encryption is a physical analog encryption with coherent states which creates the wiretap channel as shown in Fig. 12. We assume that Alice, Bob and Eve all have their standard encoder and decoder for coherent state modulation and demodulation. We also assume that Eve has a DSP module to correct and compensate the transmission impairments. In order to make the physical channel between Alice and Bob to be less noisy, we enable Alice's transmitter with the QEPS encryption or $\hat{d}(\alpha)$ and Bob's receiver with the QEPS decryptor $\hat{d}(-\alpha)$. Basically, the QEPS encryption or $\hat{d}(\alpha)$ makes the transmission channel and the wiretap channel extremely noisy, but the trusted receiver Bob can remove the injected noises through the pre-shared secret and QEPS decryptor. Then using DSP processing, Bob will be able to correctly extract Alice's transmitted data. However, since Eve does not have the same capability as Bob, her wiretap channel will remain extremely noisy.

Under the bove considerations, we rewrite Eq. (11) for the QEPS wiretap channel

$$\mathrm{ADV}^{\mathbf{ss}}_{\mathrm{QEPS}}\big(\mathcal{E}_z, Z = \mathcal{T}_z\big(\mathcal{E}_{\mathrm{QEPS}}(M)\big)\big) = \max_M\big(\mathrm{GP}\big(M|\mathcal{T}_z\big(\mathcal{E}_{\mathrm{QEPS}}(M)\big)\big) - \mathrm{GP}(M)\big), \tag{12}$$

where $\mathcal{E}_z$ is the signal received by Eve from the wiretap channel, $\mathcal{E}_{\mathrm{QEPS}}(M)$ is the cipher coherent state of a message $m \in M$ encrypted with $\hat{d}(\alpha)$, $\mathcal{T}_z(.)$ is the transmission function of the wiretap channel from the transmission to the Eve detection, and $\mathrm{ADV}^{\mathbf{ss}}_{\mathrm{QEPS}}(.)$ is the advantage over the wiretap channel for QEPS encryption. As what we have seen in the last section, the constellation of $\mathcal{T}_z(.)$ demonstrates close to the maximum BER of 50% and it is impossible for the Eve to convert the receiving signal data to useful binary data. This is the unique feature of QEPS that differs it from classical encryption. It is capable of transmitting ciphertexts in the coherent domain. In order for $Z = \mathcal{T}_z(\mathcal{E}_{\mathrm{QEPS}}(M))$ to have a recognizable constellation with acceptable BER, the advantage in Eq. (12) is reduced to some classical cryptography as shown in Eq. (11), representing the encryption which is equivalent to be done in binary data mode. That means,

$$\mathrm{ADV}^{\mathbf{ss}}_{\mathrm{QEPS}}\big(\mathcal{E}_z, Z = \mathcal{T}_z\big(\mathcal{E}_{\mathrm{QEPS}}(M)\big)\big) \leq \mathrm{ADV}^{\mathbf{ss}}\big(\mathcal{E}, Z = \mathcal{E}(M)\big), \tag{13}$$

where $\mathrm{ADV}^{\mathbf{ss}}(\mathcal{E}, Z = \mathcal{E}(M))$ could be reduced to $\mathrm{GP}(K)$ for the given security requirement. For example, AES encryption for classical security requires $\mathrm{GP}(K) \leq 2^{-128}$ but for quantum security requires $\mathrm{GP}(K) \leq 2^{-256}$ with uniform probability distribution. For the proposed QEPS analog encryption, the encryption mechanism can not be simply reduced to any classical data encryption model. So, Eve can not take the advantage with any detection constellation to extract the plain message because its BER is close to the maximum value of 50%. Therefore, QEPS encryption with a random distributed key is semantic secure and gives less advantage to the eave than any classical cryptography, i.e.

$$\mathrm{ADV}^{\mathbf{ss}}_{\mathrm{QEPS}}\big(\mathcal{E}_z, Z = \mathcal{T}_z\big(\mathcal{E}_{\mathrm{QEPS}}(M)\big)\big) \leq 2^{-n} \tag{14}$$

with $n \geq 256$ for quantum security.

4 Conclusion

This paper proposes a novel quantum encryption in phase space or QEPS for coherent states with the unitary reversible displacement operator $\hat{d}(\alpha)$. The lower case displacement operator is the reduced formal displacement operator $\hat{D}(\alpha)$ by ignoring the global phase factor which does not impact the coherent detection measurement. The reduced displacement operator $\hat{d}(\alpha)$ behaves as an addition operator for coherent state $\hat{d}(\alpha)|\beta\rangle = |\alpha + \beta\rangle$ and also has commutativity: $\hat{d}(\alpha)\hat{d}(\beta) = \hat{d}(\beta)\hat{d}(\alpha)$ which largely help our implementation, especially for decryption with $\hat{d}(-\alpha)$. The decryption can be performed in the coherent optical mode before detection or in the electrical digital domain after the coherent detection. In order to enhance security in the amplitude of coherent states, the encryption operator $\hat{d}(\alpha)$ is proposed to split into a standard QAM implementation of $\hat{d}(\alpha_1)$ and a random phase shift operator $\hat{\phi}(\varphi)$. Using Optisystem, we simulated the QEPS encryption and decryption for two data modulation schemes, QPSK and 16-QAM, where we have achieved line speeds of 56 Gbps for QPSK and 112 Gbps for 16-QAM.

Finally, in this paper, we have also proved our encryption to be semantic secure if the shared secret has a truely random probability distribution through the wiretap channel model. QEPS can be implemented either in a symmetric configuration with a pre-shared secret for quantum secure communications for data and key distributions or in a asymmetric configuration with the self-shared true random secrets for authentication and decryption.

In the future, we plan to explore experimental implementations of our simulated system with commercially available coherent optical transceivers and optical modules.

Funding
The authors have no fundign to declare.

Abbreviations
QEPS, Quantum Encryption in Phase Space; QPP, Quantum Permutation Pad; QKD, Quantum KeyDistribution; DV-QKD, Discrete Variable QKD; CV-QKD, Continuous Variable QKD; TF-QKD, Twin-field QKD; OTP, One-Time-Pad; CNOT, Control-NOT gate; PRNG, Pseudo Random Number Generator; QRNG, Quantum Random Number Generator; pQRNG, Pseudo QRNG; QSDC, Quantum Secure Direct Communication; LD, Lase Diode; LO, Local Oscillator; PM, Phase Modulator; MZM, Mach-Zehnder modulators; IQ-MZM, In-phase and Quadrature MZM; ADC, Analogue to Digital Converter; DAC, Digital to Analogue Converter; DSP, Digital Signal Processing; QAM, Quadrature Amplitude Modulation; QPSK, Quadrature Phase Shift Keying.

Availability of data and materials
Partial data generated or analysed during this study are included in this published article and its supplementary information files. Any datasets used and/or analysed during the current study that have not been included in this

published article or its supplementary information files are available from the corresponding author on reasonable request.

Declarations

Ethics approval and consent to participate
Not applicable.

Consent for publication
Not applicable.

Competing interests
The authors declare no competing interests.

Author contributions
Both authors contributed to the work described in this paper. The authors jointly drafted and reviewed the manuscript and approved the submission. Dr. Kuang majorly contributed on QEPS algorithm and A. Chan contributed on the implementation of QEPS simulations with Optisystem.

Received: 14 December 2022 Accepted: 19 June 2023 Published online: 29 June 2023

References

1. National Institute of Standards and Technology: Advanced Encryption Standard (AES). https://csrc.nist.gov/publications/detail/fips/197/final. Access: 2022-06-29.
2. Grover LK. A fast quantum mechanical algorithm for database search. In: Proceedings of the twenty-eighth annual ACM symposium on theory of computing. 1996. p. 212–9.
3. Shannon CE. Communication theory of secrecy systems. Bell Syst Tech J. 1949;28(4):656–715.
4. Kuang R, Bettenburg N. Shannon perfect secrecy in a discrete Hilbert space. In: 2020 IEEE international conference on quantum computing and engineering (QCE). 2020. p. 249–55. https://doi.org/10.1109/QCE49297.2020.00039.
5. Kuang R, Barbeau M. Quantum permutation pad for universal quantum-safe cryptography. Quantum Inf Process. 2022;21:211. https://doi.org/10.1007/s11128-022-03557-y.
6. Kuang R, Perepechaenko M. Quantum encryption with quantum permutation pad in IBMQ systems. EPJ Quantum Technol. 2022;9:26. https://doi.org/10.1140/epjqt/s40507-022-00145-y.
7. Perepechaenko M, Kuang R. Quantum encrypted communication between two IBMQ systems using quantum permutation pad. In: 2022 11th international conference on communications, circuits and systems (ICCCAS). 2022. p. 146–52. https://doi.org/10.1109/ICCCAS55266.2022.9824836.
8. Perepechaenko M, Kuang R. Quantum encryption and decryption in IBMQ systems using quantum permutation pad. J Commun. 2022;17(12):972–8. https://doi.org/10.12720/jcm.17.12.972-978.
9. Rivest RL, Shamir A, Adleman L. A method for obtaining digital signatures and public-key cryptosystems. Commun ACM. 1978;21(2):120–6.
10. Furht B, editor. The RSA public-key encryption algorithm. Boston: Springer; 2006. p. 757–757.
11. Just M. In: van Tilborg HCA, Jajodia S, editors. Diffie–Hellman key agreement. Boston: Springer; 2011. p. 341–2.
12. Hankerson D, Menezes AJ, Vanstone S. Guide to elliptic curve cryptography. 1st ed. Berlin: Springer; 2010.
13. Johnson D, Menezes A, Vanstone SA. The elliptic curve digital signature algorithm (ECDSA). Int J Inf Secur. 2001;1(1):36–63.
14. Shor PW. Algorithms for quantum computation: discrete logarithms and factoring. In: Proceedings 35th annual symposium on foundations of computer science. Los Alamitos: IEEE; 1994. p. 124–34.
15. Bos J, Ducas L, Kiltz E, Lepoint T, Lyubashevsky V, Schanck JM, Schwabe P, Seiler G, Stehle D. Crystals – kyber: a CCA-secure module-lattice-based KEM. In: 2018 IEEE European symposium on security and privacy. 2018. p. 353–67. https://doi.org/10.1109/EuroSP.2018.00032.
16. D'Anvers J-P, Karmakar A, Sinha Roy S, Vercauteren F. Saber: module-LWR based key exchange, CPA-secure encryption and CCA-secure KEM. In: Joux A, Nitaj A, Rachidi T, editors. Progress in cryptology – AFRICACRYPT 2018. Cham: Springer; 2018. p. 282–305.
17. Schanck JM. A comparison of NTRU variants. 2018. Cryptology ePrint Archive, Paper 2018/1174. https://eprint.iacr.org/2018/1174.
18. Singh H. Code based cryptography: classic McEliece. 2019. https://doi.org/10.48550/ARXIV.1907.12754. https://arxiv.org/abs/1907.12754.
19. Jao D, De Feo L. Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies. In: Yang B-Y, editor. Post-quantum cryptography. Berlin: Springer; 2011. p. 19–34.
20. Jao D. Supersingular isogeny key encapsulation. 2020. https://sike.org/files/SIDH-spec.pdf.
21. Robert D. Breaking SIDH in polynomial time. 2022. Cryptology ePrint Archive, Paper 2022/1038. https://eprint.iacr.org/2022/1038.
22. Castryck W, Decru T. An efficient key recovery attack on SIDH (preliminary version). 2022. Cryptology ePrint Archive, Paper 2022/975. https://eprint.iacr.org/2022/975.
23. Beullens W. Breaking rainbow takes a weekend on a laptop. Cryptology. 2022. ePrint Archive, Paper 2022/214. https://eprint.iacr.org/2022/214.
24. Wenger E, Chen M, Charton F, Lauter K. SALSA: attacking lattice cryptography with transformers. 2022. Cryptology ePrint Archive, Paper 2022/935. https://eprint.iacr.org/2022/935.
25. Kuang R, Perepechaenko M, Barbeau M. A new post-quantum multivariate polynomial public key encapsulation algorithm. Quantum Inf Process. 2022;21:360. https://doi.org/10.1007/s11128-022-03712-5.

26. Kuang R, Barbeau M. Performance analysis of the quantum safe multivariate polynomial public key algorithm. In: 2021 IEEE international conference on quantum computing and engineering (QCE). Los Alamitos: IEEE; 2021. p. 351–8.
27. Kuang R, Perepechaenko M, Barbeau M. A new quantum-safe multivariate polynomial public key digital signature algorithm. Sci Rep. 2022;12:13168.
28. Bennett CH, Brassard G. Quantum cryptography: public key distribution and coin tossing. Theor Comput Sci. 2014;560:7–11. https://doi.org/10.1016/j.tcs.2014.05.025.
29. Renner R, Gisin N, Kraus B. Information-theoretic security proof for quantum-key-distribution protocols. Phys Rev A. 2005;72:012332. https://doi.org/10.1103/PhysRevA.72.012332.
30. Djordjevic IB. Discrete variable (DV) QKD. In: Physical-layer security and quantum key distribution. Berlin: Springer; 2019.
31. Lai J-S, Lin X-Y, Qian Y, Liu L, Zhao W-Y, Zhang H-Y. Deployment-oriented integration of DV-QKD and 100 g optical transmission system. In: Asia communications and photonics conference (ACPC). vol. 2019. Optical Society of America. 2019. p. 2–1. http://opg.optica.org/abstract.cfm?URI=ACPC-2019-T2H.1.
32. Pirandola S, Mancini S, Lloyd S, Braunstein SL. Continuous-variable quantum cryptography using two-way quantum communication. Nat Phys. 2008;4(9):726–30. https://doi.org/10.1038/nphys1018.
33. Pirandola S, García-Patrón R, Braunstein SL, Lloyd S. Direct and reverse secret-key capacities of a quantum channel. Phys Rev Lett. 2009;102(5):050503. https://doi.org/10.1103/physrevlett.102.050503.
34. Weedbrook C, Pirandola S, García-Patrón R, Cerf NJ, Ralph TC, Shapiro JH, Lloyd S. Gaussian quantum information. Rev Mod Phys. 2012;84(2):621–69. https://doi.org/10.1103/revmodphys.84.621.
35. 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. https://doi.org/10.1038/s41586-018-0066-6.
36. Minder M, Pittaluga M, Roberts GL, Lucamarini M, Dynes JF, Yuan ZL, Shields AJ. Experimental quantum key distribution beyond the repeaterless secret key capacity. Nat Photonics. 2019;13(5):334–8. https://doi.org/10.1038/s41566-019-0377-7.
37. Wang R, Yin Z-Q, Lu F-Y, Wang S, Chen W, Zhang C-M, Huang W, Xu B-J, Guo G-C, Han Z-F. Optimized protocol for twin-field quantum key distribution. Commun Phys. 2020;3(1):149. https://doi.org/10.1038/s42005-020-00415-0.
38. Teng J, Lu F-Y, Yin Z-Q, Fan-Yuan G-J, Wang R, Wang S, Chen W, Huang W, Xu B-J, Guo G-C, Han Z-F. Twin-field quantum key distribution with passive-decoy state. New J Phys. 2020;22(10):103017. https://doi.org/10.1088/1367-2630/abbab7.
39. Chen J-P, Zhang C, Liu Y, Jiang C, Zhang W-J, Han Z-Y, Ma S-Z, Hu X-L, Li Y-H, Liu H, Zhou F, Jiang H-F, Chen T-Y, Li H, You L-X, Wang Z, Wang X-B, Zhang Q, Pan J-W. Twin-field quantum key distribution over a 511 km optical fibre linking two distant metropolitan areas. Nat Photonics. 2021;15(8):570–5. https://doi.org/10.1038/s41566-021-00828-5.
40. Wang S, Yin Z, He DEA. Twin-field quantum key distribution over 830-km fibre. Nat Photonics. 2022;16:154–61. https://doi.org/10.1038/s41566-021-00928-2.
41. Ark CH, Woo MK, Park BK, Kim Y-S, Baek H, Lee S-W, Lim H-T, Jeon S-W, Jung H, Kim S, Han S-W. $2 \times n$ twin-field quantum key distribution network configuration based on polarization, wavelength, and time division multiplexing. npj Quantum Inf. 2022;8:48. https://doi.org/10.1103/PhysRevA.103.012606.
42. Kuang R, Bettenburg N. Quantum public key distribution using randomized Glauber states. In: 2020 IEEE international conference on quantum computing and engineering (QCE). 2020. p. 191–6. https://doi.org/10.1109/QCE49297.2020.00032.
43. Khalil M, Chan A, Shahriar KA, Chen LR, Plant DV, Kuang R. Security performance of public key distribution in coherent optical communications links. In: 2021 3rd international conference on computer communication and the Internet (ICCCI). 2021. p. 123–9. https://doi.org/10.1109/ICCCI51764.2021.9486822.
44. Chan A, Khalil M, Shahriar KA, Chen LR, Plant DV, Kuang R. Security analysis of a next generation TF-QKD for secure public key distribution with coherent detection over classical optical fiber networks. In: 2021 7th international conference on computer and communications (ICCC). 2021. p. 416–20. https://doi.org/10.1109/ICCC54389.2021.9674320.
45. Chan A, Khalil M, Shahriar KA, Chen LR, Plant DV, Kuang R. On the security of an optical layer encryption using coherent-based TF-QKD in classical optical fiber links. In: 2022 4th international conference on computer communication and the Internet (ICCCI). 2022. p. 105–10. https://doi.org/10.1109/ICCCI55554.2022.9850244.
46. 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: 2022 conference on lasers and electro-optics (CLEO). 2022. p. 1–2.
47. Glauber RJ. The quantum theory of optical coherence. Phys Rev. 1963;130:2529–39. https://doi.org/10.1103/PhysRev.130.2529.
48. Kuang R, Lou D, He A, McKenzie C, Redding M. Pseudo quantum random number generator with quantum permutation pad. In: 2021 IEEE international conference on quantum computing and engineering (QCE). 2021. p. 359–64. https://doi.org/10.1109/QCE52317.2021.00053.
49. Wyner AD. The wire-tap channel. Bell Syst Tech J. 1975;54(8):1355–87. https://doi.org/10.1002/j.1538-7305.1975.tb02040.x.
50. Thangaraj A, Dihidar S, Calderbank AR, McLaughlin S, Merolla J-M. Applications of LDPC codes to the wiretap channel. 2004. https://arxiv.org/abs/cs/0411003.
51. Maurer U, Wolf S. Information-theoretic key agreement: from weak to strong secrecy for free. In: Preneel B, editor. Advances in cryptology — EUROCRYPT 2000. Berlin: Springer; 2000. p. 351–68.
52. Nafea M, Yener A. A new wiretap channel model and its strong secrecy capacity. IEEE Trans Inf Theory. 2018;64(3):2077–92. https://doi.org/10.1109/TIT.2017.2786541.
53. Bellare M, Tessaro S, Vardy A. A cryptographic treatment of the wiretap channel. 2012. https://doi.org/10.48550/ARXIV.1201.2205. https://arxiv.org/abs/1201.2205.
54. Bellare M, Tessaro S, Vardy A. Semantic security for the wiretap channel. In: Safavi-Naini R, Canetti R, editors. Advances in cryptology – CRYPTO 2012. Berlin: Springer; 2012. p. 294–311.

Publisher's Note