引用本文：张宸瑜，禹钧译，张振荣. 基于相空间动态位移算子的量子加密通信的研究[J]. 光通信技术，2026，50(5)：93-97

基于相空间动态位移算子的量子加密通信的研究

张宸瑜，禹钧译，张振荣*
（广西大学 计算机与电子信息学院，南宁 530004）

摘要：针对量子密钥分发需要专用设备和成码率低的缺点，提出一种基于相空间动态位移算子(DDO)的量子加密(QEPS-dd)方案，该加密方式在既有的相干光通信架构中引入发送端数字加密与接收端逆变换处理，并使用Optisystem光学仿真软件对该加密方案进行了仿真模拟。结果表明，QEPS-dd方案通过引入DDO构建状态依赖随机化机制在本次背靠背理想信道下实现零误码率，采用静态(PSO)和位移算子(DO)双重复合加密，在兼容现有相干光通信硬件架构的前提下，实现了单光纤信道内密钥分发与加密数据的传输、接近理论极限的安全阈值，为应对量子计算威胁提供了可扩展的实用安全防护路径。

关键词：光通信；动态位移算子；相空间；量子安全框架
中图分类号：TN256　　**文献标志码：**A　　**文章编号：**1002-5561(2026)05-0093-05
DOI：10.13921/j.cnki.issn1002-5561.2026.05.015

Research on quantum encrypted communication based on dynamic displacement operators in phase space

ZHANG Chenyu，YU Junyi，ZHANG Zhenrong*
（School of Computerand Electronics，Information，Guangxi University，Nanning 530004，China）

Abstract：To address the drawbacks of quantum key distribution，which requires dedicated equipment and suffers from low key generation rates，a quantum encryption scheme based on phase space dynamic shift operator is proposed. This encryption method introduces digital encryption at the transmitter and inverse transformation processing at the receiver into the existing coherent optical communication architecture. The results demonstrate that the QEPS-dd scheme achieves zero bit error rate under ideal back-to-back channel conditions by introducing a state-dependent randomization mechanism via Direct detection orthogonality(DDO). By employing static phase shift operator(PSO) and displacement operator(DO)dual composite encryption，the proposed scheme enables simultaneous key distribution and encrypted data transmission within a single fiber channel，while maintaining compatibility with existing coherent optical communication hardware architectures. Furthermore，it approaches the theoretical security threshold，providing a scalable and practical security pathway to counter quantum computing threats.

Key words：optical communications，dynamic displacement operator，phase-space，quantum-secure framework

0 引言

量子计算的快速发展对传统的密码学构成了重大威胁，使得传统的加密方案在量子计算面前不再安全[1-4]，亟需寻找新的加密方式以对抗量子计算的威胁。量子密钥分发(QKD)利用量子特性使密钥在传输的过程中具备理论上的无条件安全性，因此成为当前研究热点之一。但是，QKD的传输依赖专用设备，需要对现有的光网络进行较大改造，且在现有的条件下QKD成码率较低；此外，QKD仅用于密钥传输，而非直接的信息传输。为此，Kuang R等人[5-7]提出了一种在经典相干光通信框架下结合量子操作的相空间量子加密(QEPS)方案，该方案通过在现有经典相干光接收机上执行量子操作来实现信号加密。这种新颖的方式既实现了与经典相干光系统的兼容性，又保障了量子加密的安全性。早期相位加密(QEPS-p)[8-9]方案和位

收稿日期：2025-04-25。
基金项目：广西重点研发计划项目(桂科AB23075155、桂科AB23075112)资助。

作者简介：张宸瑜(2000—)，男，硕士研究生，现就读于广西大学计算机与电子信息学院计算机技术专业。主要研究方向为相空间量子加密、相干光通信物理层安全及光通信仿真建模研究，涉及动态位移算子加密机制及其在经典相干光通信系统中的应用验证。
***通信作者：**张振荣(1976—)，男，博士，教授，主要研究方向为通信网络及光纤传感技术。



移加密（QEPS-d）方案虽通过编码实现安全传输，但二者所依赖的静态加密机制难以有效应对量子计算发展带来的量子计算安全威胁。QEPS-p虽能抵御即时性攻击，但其加密星座图中环形特征的存在会导致幅值信息的无意识泄露，而QEPS-d的静态位移机制由于无法实现充分的随机化，依然面临被预测的安全风险。

针对上述局限，本文提出一种基于相空间动态位移算子（DDO）的量子加密（QEPS-dd）方案。

1 QEPS-dd方案的理论分析

1.1 QEPS-dd的安全框架

QEPS安全框架历经3个阶段的技术迭代：从初始的QEPS-p、演进至QEPS-d，最终发展为QEPS-dd。QEPS-dd安全框架如图1所示。QEPS-dd方案由连续波（CW）激光器、相位调制器（PM）、随机数发生器（RNG）、信号发生器、QEPS-dd加密器、IQ调制器、光纤传输链路、掺铒光纤放大器（EDFA）、本振激光器（LO）、相干光接收器以及QEPS-dd解密器与数字信号处理（DSP）模块组成，图中I_x、Q_x、I_y、Q_y分别为x、y 2个正交偏振支路的同相分量和正交分量。

QEPS-dd方案采用全链路加密流程，通过DDO融合相位旋转与位移操作，对相干态进行实时随机调制，使加密效果与算子本身相关。该机制不仅克服了QEPS-p中因环形星座分布导致的幅度信息泄漏问题，还解决了QEPS-d中静态位移参数易受逆向分析的缺陷，最终形成兼具高安全性与系统兼容性的量子加密框架。

本文以正交相移键控（QPSK）信号为例阐述QEPS-p加密原理。QPSK调制中符号分布于4个正交相位状态（0°、90°、180°、270°）。QEPS-p通过伪随机数生成器（PRNG）控制相移算子$\hat{P}(\phi)$，对原始相位状态施加随机相位偏移$\phi_j \in \{0°、90°、180°、270°\}$。加密过程可表示为

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

式中：$|\beta\rangle$为待加密的输入相干态，$|\beta e^{-i\phi_j}\rangle$为加密后相干态的复振幅，i为虚数单位，$j$为对应索引下选取的相移角度。

QEPS-d通过位移算子（DO）$\hat{d}(\alpha)$对相空间中的符号进行位移操作，其数学表达式为

$$\hat{d}(\alpha)|\beta\rangle = |\alpha + \beta\rangle \tag{2}$$

式中：α为位移参数，表示$\hat{d}(\alpha)$在相空间中引入的复平移量。

1.2 QEPS-dd原理

为克服静态相移算子（PSO）和DO的固有缺陷，QEPS-dd方案将PSO与DO深度融合，构建全新的DDO，其加密过程的数学表达式为

$$\hat{d}(\alpha,\ \phi)|\beta\rangle = \hat{d}(\alpha)\hat{P}(\phi)|\beta\rangle = |\alpha + e^{-i\phi}\beta\rangle \tag{3}$$

式中：$\hat{d}(\alpha,\ \phi)$为DDO，其由$\hat{d}(\alpha)$与$\hat{P}(\phi)$复合构成；β为相移算子的复振幅，对应原始调制符号在相空间中的坐标位置，$\beta = x_I + ix_Q$，x_I、x_Q分别表示输入调制符号的同相分量和正交分量，对应复振幅在相空间中的实部和虚部；ϕ为相移参数，用于控制$\hat{P}(\phi)$对输入态进行相位旋转，使其复振幅由β变换为$e^{-i\phi}\beta$。由此可见，QEPS-dd方案的加密过程并不是单独的相位旋转或固定平移，而是先通过PSO改变输入态的相位位置，再通过DO对旋转后的相干态进行平移，最终得到输出加密态$|\alpha + e^{-i\phi}\beta\rangle$，这等效定义了状态相关位移，其表达式为

$$\hat{d}(\alpha,\ \phi)|\beta\rangle = \hat{d}(\alpha + (e^{-i\phi} - 1)\beta)|\beta\rangle \tag{4}$$

同一个DDO对不同量子态的加密效果图如图2

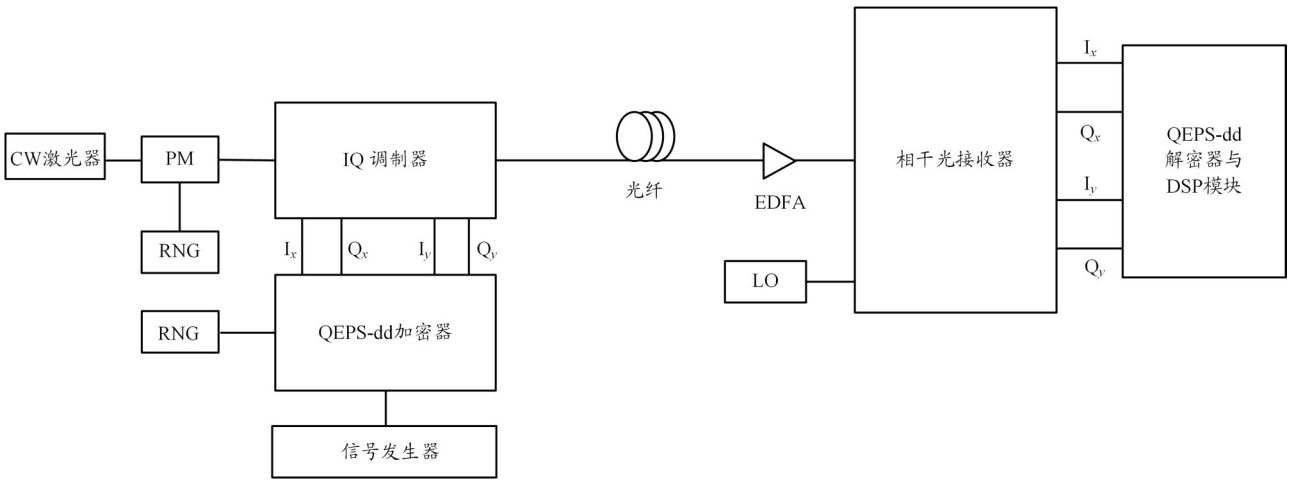


图1 QEPS-dd安全框架

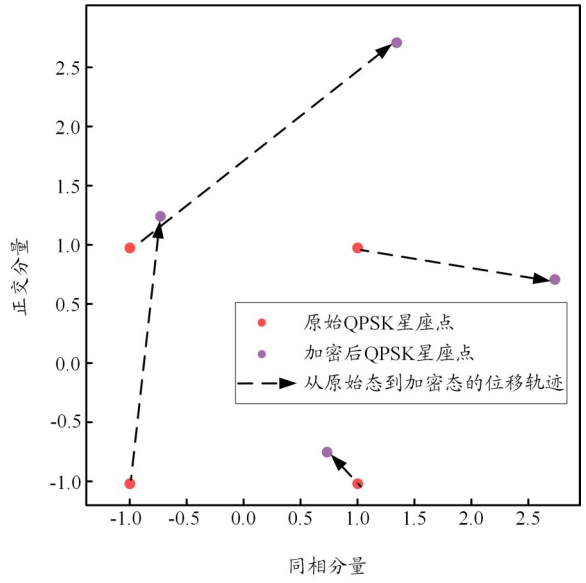


图2 同一个DDO对不同量子态的加密效果

所示。可以看出，加密后的星座点在相位空间中呈现差异化分布，这是由于同一个DDO会根据不同$|\beta\rangle$的幅值相位信息产生不同的位移效果，规避了传统静态位移中因固定参数导致的模式分析漏洞。

QEPS-dd方案中，不同DDO的连续作用一般具有非交换性，即改变其作用顺序通常会改变最终输出态。其数学表述为

$$\hat{d}(\alpha',\ \phi')\hat{d}(\alpha,\ \phi)|\beta\rangle \neq \hat{d}(\alpha,\ \phi)\hat{d}(\alpha',\ \phi')|\beta\rangle \tag{5}$$

由式(5)可知，DDO操作顺序的改变会生成完全不同的密文相干态。该特性从量子力学层面确保了加密过程的不可逆性：攻击者即使截获部分加密参数，也无法通过逆向操作推导出完整DDO序列。此外，非交换性导致解密复杂度呈指数级增长，这对于保证通信安全非常重要。

加密后的信号通过光纤传输。尽管光纤衰减会降低信号功率，但DSP模块与EDFA可有效补偿传输损耗[10]。在接收端，DSP通过逆DDO完成解密操作，表达式为

$$\hat{d}^{-1}(\alpha,\ \phi) = \hat{P}^{-1}(\phi)\hat{d}^{-1}(\alpha) \tag{6}$$

解密后，加密信息可恢复为原始状态，表达式为

$$\hat{d}^{-1}(\alpha,\ \phi)|\alpha + e^{-i\phi}\beta\rangle = |\beta\rangle \tag{7}$$

由式(7)可知，在理想条件下，采用正确的逆DDO可恢复原始输入相干态$|\beta\rangle$，验证了其可逆性与可靠性。在本文设置的背靠背(B2B)仿真条件下，接收端采用与发送端匹配的相移和位移参数，并按加密操作的逆序完成解密后，统计得到的误码率(BER)为0，表明在本次仿真的有限测试序列内未检测到误码，该方案在上述条件下能正确恢复信号。

与静态的QEPS-p或QEPS-d方案不同，DDO的状态相关位移会干扰信号模式的解析。通过对DDO进行序贯应用，可构造出一个组合密钥空间，从而大幅提升系统对暴力破解攻击的抗性。

2 仿真结果与分析

2.1 仿真设计

基于图1的QEPS-dd仿真框架图，本文在Optisystem中开发了QEPS-dd方案的通信仿真系统。该系统以相干光通信系统的基本架构为基础，通过集成DDO加密模块，实现了相位空间量子加密的全流程仿真。实验中，大部分参数保持与相干光通信系统相同，仅在系统中加入了一些加密仿真的参数和信息。表1列出了仿真系统的关键参数配置。通过OptiSystem与Matlab对QEPS-dd进行联合仿真，其中OptiSystem负责主要的光通信模块，Matlab通过代码实现经典相干光通信加密，并将加密算子应用于信号。

本系统采用DDO实现量子加密，由PSO与DO协同构成。PSO采用5组特定相移角度(24°、48°、72°、96°、120°)，通过伪随机序列动态选择，确保相位随机性；DO基于16进制正交幅度调制(16-QAM)生成位移参数，其复平面分布覆盖I/Q四象限，增强位移不可预

表1 仿真参数

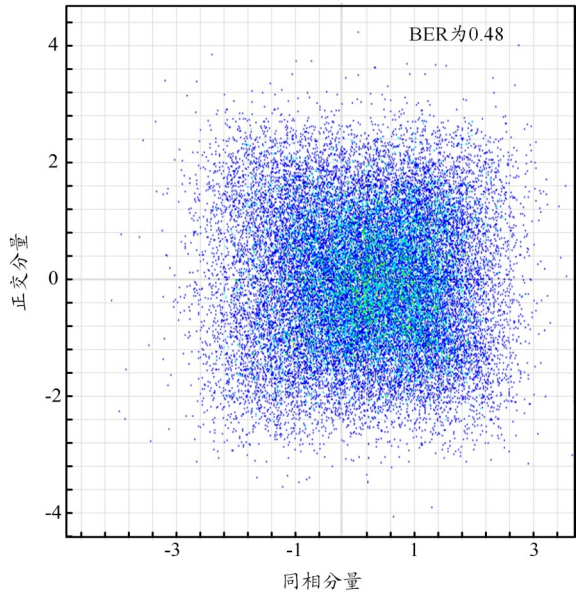
配置类别	参数	数值
布局参数	序列长度/bits	6 553 6
	波特率/Gbaud	28
	偏振模色散周期	1 024
CW激光器和LO激光器	中心波长/nm	1 550
	功率/dBm	5
	线宽/MHz	0.1
	方位角/(°)	45
IQ调制器	消光比/dB	20
	开关偏置电压/V	3
	插入损耗/dB	5
EDFA	前向泵浦功率/mW	13~14
	前向泵浦波长/nm	980
	1550 nm处的损耗/(dB/m)	0.1
	980 nm处的损耗/(dB/m)	0.15
光纤	长度/km	80
	衰减/(dB/km)	0.2
	色散/(ps·nm^{-1}·km^{-1})	16.75
	色散斜率/(ps·nm^{-2}·km^{-1})	0.075
	差分群时延/(ps·km^{-1})	0.2
	有效面积/μm^2	80

测性。最终，DDO通过实时结合PSO与DO参数，实现PSO和DO的耦合调制。

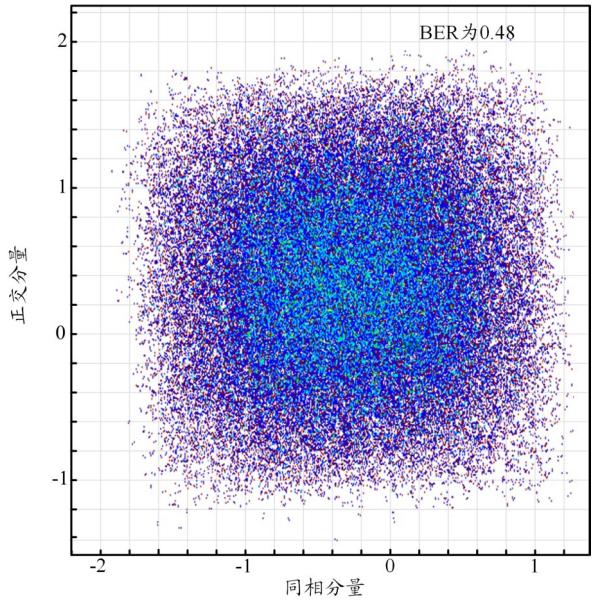
2.2 仿真结果分析

在B2B场景下，对发送端采用DDO加密、接收端分别采用未解密、仅采用PSO进行部分解密、仅采用DO进行部分解密、同时采用正确PSO和DO参数进行完整DDO解密4种策略的QPSK相干光通信系统进行仿真，结果如图3所示。从图3(a)可以看出，星座点呈现明显的随机扩散分布，无法形成标准QPSK星座点聚类，对应的BER为0.48，接近随机判决水平，说明在未掌握解密算子的情况下，接收端难以恢复原始信息。从图3(b)可以看出，由于DO未被正确抵消，接收星座图仍处于高度离散状态，BER仍为0.48，表明仅掌握相位参数不足以完成有效解密。从图3(c)可以看出，星座点仍无法回到标准QPSK判决区域，对应BER为0.49。从图3(d)可以看出，完整解密后，接收样本重新聚集到4个预期符号位置，为4个清晰的QPSK星座结构，BER降为0，说明原始信号能够被准确恢复。

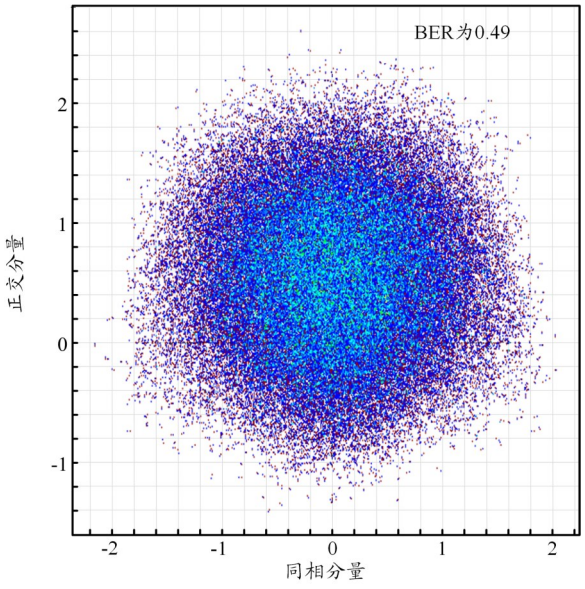
上述结果表明，QEPS-dd加密信号的完整恢复依



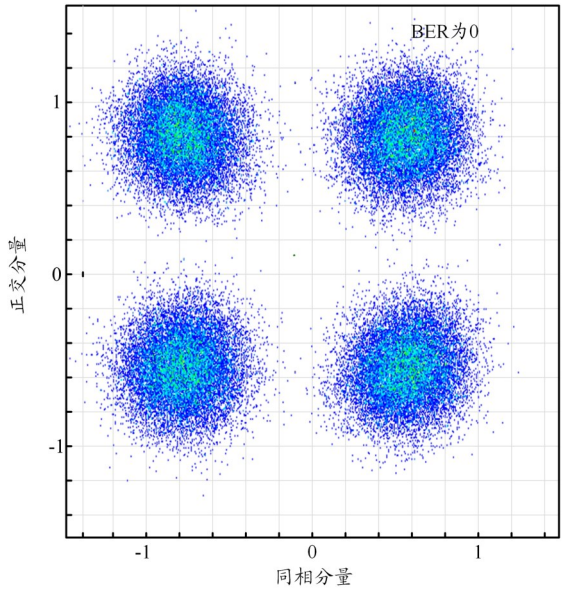
(a) 未解密时的接收星座



(b) 仅采用PSO进行部分解密的结果



(c) 仅采用DO进行部分解密的结果



(d) 同时采用正确PSO和DO参数进行完整DDO解密的结果

图3 B2B场景下发送端使用DDO加密，接收端使用不同解密方法的仿真结果

赖于PSO和DO的同步逆操作。单独使用PSO或DO均无法完成原始星座图重构，且对应BER仍接近0.5。相比QEPS-p中仅进行相位随机化可能保留幅度环形特征、QEPS-d中静态位移可能存在模式分析风险。QEPS-dd通过相位旋转与位移操作的动态耦合，使加密星座点在相空间中呈现更强的随机扩散特征。完整DDO解密能够恢复原始QPSK星座，而任一部分解密均无法恢复有效信息，验证了该加密方案在相干光通信系统中的可行性和抗部分解密能力。

3 结束语

本文提出了一种QEPS-dd方案。相较受限于基础设施兼容性问题与光子探测约束的传统QKD系统，QEPS-dd方案将量子增强加密技术与经典光通信系统相融合。该方案通过DDO的引入，有效消除了量子加密过程中可预测模式的存在，并构建了状态依赖的随机化机制，从而显著提升了系统抵御量子计算威胁的安全强度。结果表明：QEPS-dd方案可实现接近理论极限的安全阈值，非授权窃听者的BER趋近于0.5；其PSO和DO双重复合加密机制不仅同步解决了振幅与相位域的信息泄露风险，还能在不改变现有相干光通信系统硬件架构的前提下实现无缝兼容。在B2B场景下，PSO和DO的协同解密是实现原始信号完整恢复的必要条件，正确的解码情况下BER可以保持在0。本文提出的QEPS-dd方案通过量子加密与经典光传输的有机融合，在确保现有基础设施兼容性的前提下，构建了可扩展的量子安全防护体系，为应对新型计算威胁提供了有效技术路径。

参考文献：

[1] Bennett C H，Brassard G. Quantum cryptography：public key distribution and coin tossing[J]. Theoretical computer science，2014，560：7-11.

[2] Djordjevic I B. Physical-layer security and quantum key distribution [M]. Berlin：Springer，2019.

[3] Shor P W，Preskill J. Simple proof of security of the BB84 quantum key distribution protocol[J]. Physical Review Letters，2000，85(2)：441.

[4] Renner R，Gisin N，Kraus B. Information-theoretic security proof for quantum-key-distribution protocols[J]. Physical Review A-Atomic，Molecular，and Optical Physics，2005，72(1)：012332.

[5] Kuang R，Bettenburg N. Quantum public key distribution using randomized Glauber states[C]//IEEE. Proceedings of 2020 IEEE international conference on quantum computing and engineering(QCE). Denver，CO，USA：IEEE，2020：191-196.

[6] Khalil M，Chan A，Shahriar K A，et al. Security performance of public key distribution in coherent optical communications links[C]//IEEE. Proceedings of 2021 3rd international conference on computer communication and the Internet(ICCCI). Nagoya：IEEE，2021：123-129.

[7] Kuang R. Quantum encryption in phase space with dynamic displacement operators and quantum permutation pad[J]. Academia Quantum，2025，2：1-10.

[8] Chan A，Khalil M，Shahriar K A，et al. Encryption in phase space for classical coherent optical communications[J]. Scientific Reports，2023，13(1)：12965.

[9] Kuang R，Chan A. Quantum encryption in phase space with displacement operators[J]. EPJ Quantum Technology，2023，10(1)：26.

[10] Mable P F，Wang Zhexing，Deng Yanhua，et al. Optical layer security in fiber-optic networks[J]. IEEE Transactions on Information Forensics and Security，2011，6(3)：725-736.