利用概率整形提升非对称 Y-00 协议密钥分发速率*

陆晖晖[1)2)3)] 马雨心[1)2)3)] 贾志伟[4)] 秦菲菲[1)2)3)] 李璞[1)2)3)†] 秦玉文[1)2)3)]

王云才[1)2)3)]

1)（广东工业大学，信息工程学院，先进光子技术研究院，广州 510006）

2)（广东工业大学，通感融合光子技术教育部重点实验室，广州 510006）

3)（广东工业大学，广东省信息光子技术重点实验室，广州 510006）

4)（太原理工大学，新型传感器与智能控制教育部重点实验室，太原 030024）

摘 要

提出了一种结合概率整形技术的非对称 Y-00 协议密钥分发方案，通过调整 QAM 信号各星座点出现的概率提高信号传输质量，从而有效提升密钥分发速率.同时，还分析了不同概率整形因子对密钥分发速率和安全性的影响，并引入保密增强技术对初始密钥进行压缩，显著提升了密钥的安全强度.实验结果表明：在 25 km 的标准单模光纤上，利用该方法可实现 13.76 Mbit/s 的密钥分发速率，相较于原非对称 Y-00 协议密钥分发方案速率提升了 3 个数量级.该方案为探索兼容于现行光通信系统的物理层高速安全密钥分发提供了一种解决思路.

关键词：物理随机数，Y-00 协议，密钥分发，概率整形，保密增强

基金：国家重点研发计划（批准号：2024YFB2808400）、国家自然科学基金（批准号：62531005,62322504,62305073）、广东省重点领域研发计划（批准号：2024B0101030001）、山西省基础研究计划项目（批准号：202203021221079）、光电融合集成与通信感知教育部重点实验室开放基金（批准号：PICCSC202505）资助的课题.

† 通信作者. E-mail: lipu8603@126.com

1 引 言

光纤通信凭借其高带宽特性，已成为海量数据传输的核心承载方式. 但光纤链路距离长、部署环境复杂，难以抵御窃听攻击. 因此，通常需要对传输信息进行加密以确保通信过程的安全，密钥的安全分发也随之成为保障信息安全的核心前提[1,2].

基于复杂数学难题的密码学算法被广泛用于密钥分发[3]，其安全性依赖于经典计算机求解特定数学难题的计算时间复杂度，但随着量子计算技术的快速发展，这一安全性正面临日益严峻的潜在威胁[4]. 相比之下，物理层密钥分发技术的安全性依赖于物理现象而非计算复杂度，受到了广泛关注.

物理层密钥分发技术主要包括量子密钥分发[5-9]、超长光纤激光器[10-13]、激光混沌同步[14-20]、光纤信道互易性[21-26]等. 量子密钥分发在理论上证明了其无条件安全，然而在实际应用中仍面临许多阻碍，例如严苛的量子探测设备要求、量子信道难以兼容光纤通信系统等[27, 28]. 在超长光纤激光器密钥分发方案中，通常会使用光纤布拉格光栅在通信链路中构建超长谐振腔，使用其独立的随机码来调制激光波长或光谱，从不同的激光状态中筛选出一致的密钥. 基于激光混沌同步的密钥分发需要向硬件参数匹配的两台激光器注入相同的驱动光源，以实现键控混沌同步，从高度相关的混沌信号中提取出一致的密钥. 基于光纤信道互易性的密钥分发方案则是使用干涉仪或偏振分析器从光纤通道中提取高度相关的物理参数（信道噪声、偏振状态、偏振模色散），进而将其量化为对称密钥. 然而，需要注意的是，上述方案都需要在通信链路中引入额外的器件才能实现密钥分发，在一定程度上增加了与现有光纤通信系统融合的复杂度.

基于 Y-00 协议[29-33]的密钥分发方案无需部署额外的器件，与现有的光纤通信系统完全兼容. 目前相关方案已有相关报道[34, 35]：通信双方利用 Y-00 协议映射的高阶 QAM 信号测量信道误码率，同时从高度相关的误码率曲线中提取密钥. 然而，现有方案是以安全预共享运行密钥为前提的. 针对这一局限性，最近学者们进一步提出了无需预共享运行密钥的方案[36]：利用非对称 Y-00 协议映射的高阶 QAM 信号误码率差异，通信双方可在公共信道中安全交换密钥，但其密钥分发速率仅处于 kbit/s 量级.

这里，我们提出了一种改进方案：利用概率整形技术调整高阶信号星座点出现的概率，从而提升信号的传输质量，最终提升密钥分发速率. 为了证明这一方案的可行性，我们在 25 km 的光纤链路上开展了原理性验证实验. 结果显示，利

用该方法可将密钥分发速率提升至 13.76 Mbit/s；而且，窃听方与合法方的密钥互信息趋近于 0——这意味着窃听者无法获取任何相关信息. 相较基于 Y-00 协议的同类技术，本方案在兼顾其安全性的同时，实现了密钥分发速率的有效提升——3 个数量级.

2基于概率整形的非对称Y-00协议密钥分发方案

2. 1 Y-00协议

Y-00 协议的核心思想是利用运行密钥将数据进行加密调制，将数据掩藏在通信链路中固有的量子噪声里，从而实现物理层加密. 通信链路中的量子噪声主要包括光电探测器的散粒噪声及掺铒光纤放大器的自发辐射噪声，这类噪声具有随机性，使得窃听者难以从噪声中提取有效信息.

图 1 是执行 Y-00 协议的示意图：16 QAM 信号 I/Q 两路的各 2 bit 数据分别被 2 bit 运行密钥加密，进而生成的加密数据映射成 256 QAM 信号. 例如，I 路原始数据[D_I=(D_1,D_2)]，状态基[B_I=(B_1, B_2)]，密文 E_I 可以表示为：

$$E_I = \left(D_1 \oplus B_2, D_2 \oplus B_2, B_I\right) \tag{1}$$

Q 路原始数据的处理过程则同 I 路相同. 如此，当链路噪声的幅度超过高阶调制信号的相邻信号电平时，窃听者就无法准确区分真实发射信号电平，从而无法准确获取数据信息. 鉴于同一运行密钥下加密的不同数据在星座空间中的排列是等距的，若将其判决门限设置在两个星座点的中点，当接收到的星座点信号于判决门限内，合法方利用预先共享的运行密钥却可将数据准确判决出来.

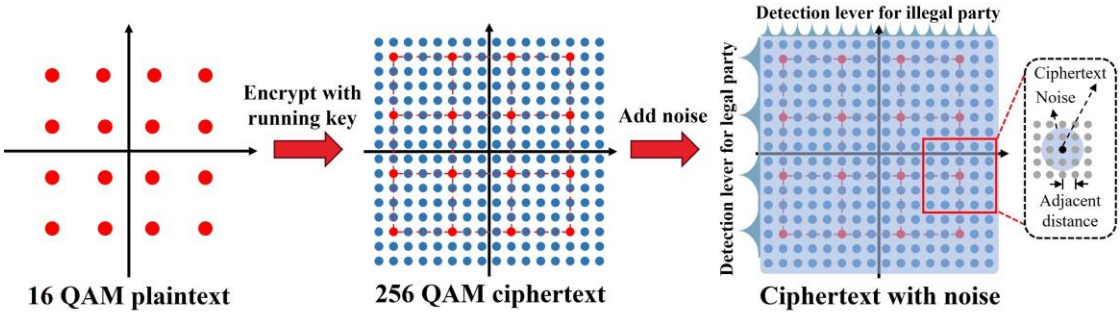

图 1 Y-00 协议示意图

Fig. 1 Schematic diagram of Y-00 protocol

噪声掩盖数（Number of Masked Signal，NMS）是衡量系统安全性的重要指标，表示每个星座点可以被噪声掩盖的数量，高阶 QAM 信号的 NMS 定义为[37]：

$$\Gamma = \left(\frac{2\bar{\sigma}_{16QAM}}{\Delta}\right)^2 \tag{2}$$

其中$2\bar{\sigma}_{16QAM}$表示高阶QAM信号解映射为16 QAM信号时，每个星座点的噪声均方根，其计算公式如下：

$$\bar{\sigma}_{16QAM}=\sqrt{\frac{1}{32}\sum_{n=1}^{16}(\sigma_{I,n}^2+\sigma_{Q,n}^2)} \tag{3}$$

其中$\sigma_{I,n}^2$和$\sigma_{Q,n}^2$表示解映射后第n个星座点I/Q分量的噪声方差. △表示高阶QAM信号幅度归一化后，相邻信号星座点的距离，表示为：

$$\Delta=\frac{2}{2^M-1} \tag{4}$$

M为高阶QAM信号I/Q路的调制阶数. 在星座图上，每个星座点对应独特的数据和运行密钥，若窃听者能够准确探测出发送信号的真实坐标，则可以反向推测出数据信息. 而在噪声掩盖范围内，仅包含一个正确的密文信号，因此窃听者探测失败概率（Detection Failure Probability，DFP）可以表示为：

$$DFP\approx 1-\frac{1}{\Gamma} \tag{5}$$

以图1为例，该密文信号的NMS=9，当窃听者探测该信号时，探测到的是噪声覆盖范围内9个信号星座点中的任意一个，而这9个星座点对应的数据和运行密钥都不相同，因此其DFP=8/9. 随着信号的调制阶数增加，相邻星座点的欧氏距离随之变小，噪声对信号的掩盖效果越佳，进而增大窃听者探测失败概率.

2. 2 概率整形

概率整形(Probability Shaping, PS)是通信中常用的一种技术，其核心原理是将均匀分布的二进制序列转换为服从特定概率分布的星座点序列，从而提高低幅度星座点的出现概率，降低高幅度星座点的出现概率. 这种方式可降低系统所需的平均发射功率，因此在相同发射功率下，概率整形信号星座图的欧氏距离较常规信号星座图有明显提升，从而增大判决门限并使得系统的误码率降低[38]. 实现概率整形的核心模块是分布匹配器，其中恒定成分分布匹配器（Constant Composition Distribution Matcher, CCDM）是一种典型且高效的结构，其作用是使得信号星座点出现的概率服从麦克斯韦-玻尔兹曼分布：

$$P_X(x)=\frac{\exp\left\{-V\left[Re(x)^2+Im(x)^2\right]\right\}}{\sum_{x\in X}\exp\left\{-V\left[Re(x)^2+Im(x)^2\right]\right\}} \tag{6}$$

上述公式中，V 为概率整形因子，$Re(x)$和 $Im(x)$分别代表星座点的实部和虚部的

幅值. 概率整形因子 V 的取值决定信号星座点的分布，随着 V 增大，意味着低幅度星座点出现的概率更高，QAM 信号星座点越向中心聚拢.

将概率整形技术与量子噪声流加密结合，相当于对高阶 QAM 信号进行概率整形. 随着信号调制阶数的提高，概率整形带来的增益也越来越明显. 例如，图 2 是 PS-16 QAM 经 Y-00 协议加密前后星座分布图.

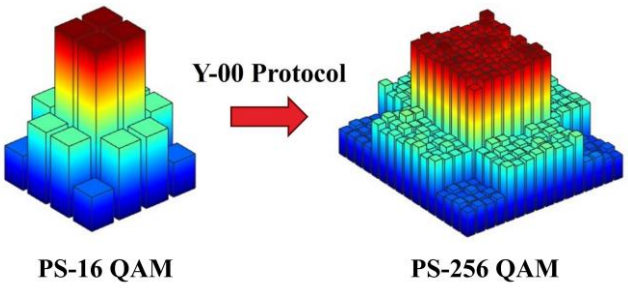

图 2 PS-16QAM 经 Y-00 协议加密前后星座图

Fig. 2 Constellation diagrams of PS-16 QAM signal: pre-encryption vs. post-encryption via the Y-00 protocol

2. 3 方案提出

图 3 是一种结合概率整形技术的非对称 Y-00 协议密钥分发方案. 其中，黑色箭头表示比特数据传输链路，蓝色箭头表示光信号传输链路，而红色箭头表示数据处理流程链路. 在发送端（Alice），原始数据 Data 经概率整形后生成服从特定概率分布的发送数据 D_{A1}. D_{A1} 被运行密钥 KeyA 经 Y-00 协议加密映射为高阶 QAM 信号并发送至接收方（Bob）. 在传输过程中，高阶调制信号极易受到链路中量子噪声的影响，当噪声幅值大于相邻星座点之间的距离时，每个星座点都将有效隐藏在噪声之下，从而防止窃听者准确地探测到星座点的真实坐标，进一步推测出传输的数据.

Bob 使用自己的运行密钥对 Alice 发送来的信号进行解映射，得到数据 D_{B1}，随后异或上拓展密钥 KeyE 得到 D_{B2}. 其中，KeyE 是真随机密钥 Key 经过拓展 K 次得来的，例如，Key={101…}，K=3，则 KeyE={111000111…}. 最后，D_{B2} 被 KeyB 重新加密并映射为高阶 QAM 信号，发回 Alice. 这里需要注意的是，Bob 用于加密的 KeyB 会根据 D_{B1} 的值发生变化，具体为：

$$KeyB^{*}=\begin{cases}\overline{KeyB}, if\ D_{B1}\ is\ even\\ KeyB, if\ D_{B1}\ is\ odd\end{cases} \tag{7}$$

Alice 使用与加密相同的运行密钥 KeyA 解映射 Bob 发送的信号得到接收数

据 D_{A2}. 随后将 D_{A1} 和 D_{A2} 配对分组，每组包含 K 对 D_{A1}/D_{A2} 组合，并计算每组的平均误码率得到误码率曲线，记为 $BER(t)$. 最终 Alice 按照公式(8)判决密钥，其中 T 为 $BER(t)$的均值：

$$Key=\begin{cases}1, BER(t)\geq T\\ 0, BER(t)<T\end{cases} \tag{8}$$

值得注意的是，本方案中的 Data、KeyA、KeyB、Key 均是由物理随机数发生器产生的比特数据.

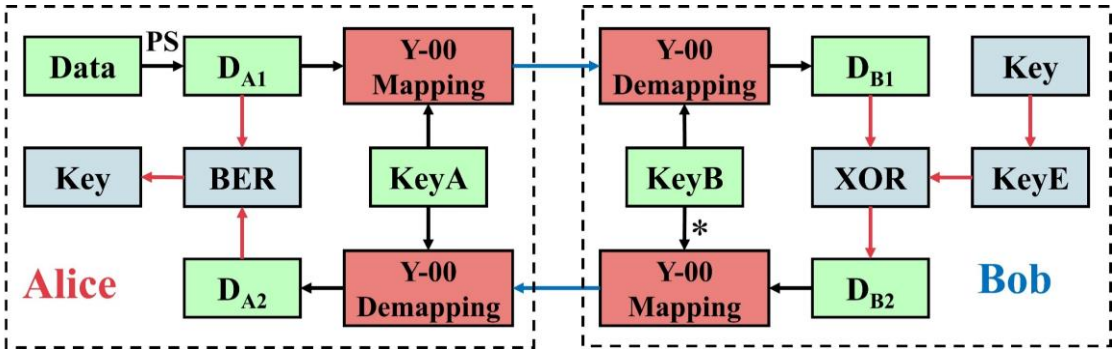

图 3 密钥分发方案示意图

Fig. 3 Schematic diagram of key distribution scheme

3 实验方案

3. 1 系统搭建

所提方案的实验装置图如图 4 所示，Alice 端由窄线宽激光器（Laser）、I/Q 调制器（I/Q modulator）、任意波形发生器（AWG）组成，接收端由掺铒光纤放大器（EDFA）、相干接收机（Receiver）、示波器（Oscilloscope）构成. Alice 端首先由窄线宽激光器生成波长为 1550 nm、功率为 10 dBm、线宽低于 100 kHz 的光载波. 在 DSP 中，系统首先将随机比特数据 Data 映射的 16 QAM 信号进行概率整形，整形后得到的 PS-16 QAM 信号实部和虚部数据对应 D_{A1}. 随后，系统采用随机数发生器产生的运行密钥 KeyA，依据 Y-00 协议将 D_{A1} 加密并映射为 PS-$2^8\times2^8$ QAM 信号，并将其符号速率设为 10 Gbaud. 该信号经滚降因子为 0.1 的根升余弦滤波器完成脉冲成型后，依次执行重采样、削峰等操作优化信号特性，并输入到采样率为 90 GSa/s 的 AWG 中，完成数字信号转模拟电信号的转换. 最终，光载波与模拟电信号一同送入 I/Q 调制器完成光学调制，并通过 25 km 标准单模光纤发送至接收端.

在 Bob 端，接收信号首先经 EDFA 将光功率放大至-10 dBm 以补偿链路损耗，放大后的信号经过偏振控制器调整其偏振态. 同时，窄线宽激光器的另一通道生

成波长、线宽、功率等参数均与光载波保持一致本振光（Local Oscillator, LO），用于相干解调. 相干接收机是信号解调的关键器件，它集成了一个 90° 光混频器和四路平衡探测器，用于信号光与本振光的相干混频与解调. 最终，信号光被转为 I/Q 两路电信号，并由高带宽示波器以 80 GSa/s 的采样率捕获. Bob 将接收到的数字信号在 DSP 中进行离线处理，包括 IQ 正交化、色散补偿、偏振均衡、载波相位恢复等，恢复出的 PS-2^8×2^8 QAM 信号星座图如图 4 所示. Bob 使用独立于 Alice 的随机数发生器产生运行 KeyB 和密钥 Key. 其中密钥 Key 经拓展 K 次变成 KeyE，KeyB 用来解密恢复出的星座图得到 D_{B1}，随后将 D_{B1} 异或上 KeyE 并重新加密发回 Alice.

Alice 执行与 Bob 相同的接收步骤获得加密的信号星座图，随后使用 KeyA 对星座图解密获得 D_{A2}. 最终执行误码率曲线计算、密钥判决操作获取密钥.

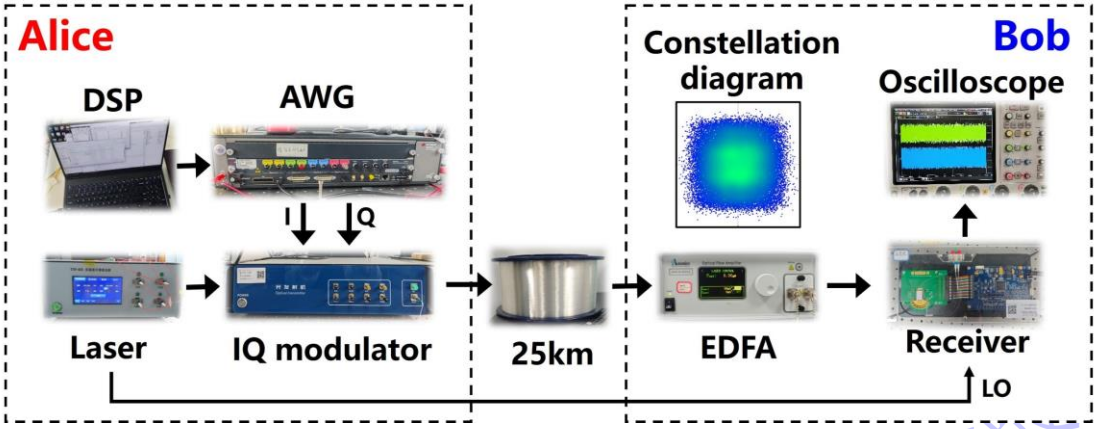

图 4 实验装置

Fig. 4 Experimental setup

3. 2 实验结果

本方案中系统的信号传输速率设为 10 Gbaud；调制格式为 2^8×2^8 QAM；密钥拓展次数 K 设为 200 至 1600，步进为 200；概率整形因子 V 设为 0、0.1、0.3、0.5（V=0 代表 QAM 信号未进行概率整形）. 密钥分发速率（Key Distribution Rate, KDR）定义为信号发送的波特率与密钥拓展次数的比值，即 KDR=Baud/K，在固定波特率的条件下，KDR 与 K 成反比.

为模拟实际窃听场景，我们使用 10：90 的光纤耦合器接入通信链路进行分光，将 10%的光信号反馈至 Eve 的接收端，模拟其窃听 Alice 发送和接收的高阶 QAM 信号. Eve 使用其运行密钥解映射得截获的信号，并执行与 Alice 相同的计算误码率曲线、判决密钥步骤.

图 5 为不同条件下系统的速率与安全性能：随着密钥拓展次数的增加，Alice 判决密钥时的错误率显著下降. 同时，随着概率整形因子 V 的增大，Alice 实现无误码判决密钥所需的最小密钥拓展次数也相应减少. 而 Eve 在相同传输条件下所获密钥的错误率始终显著高于 Alice.

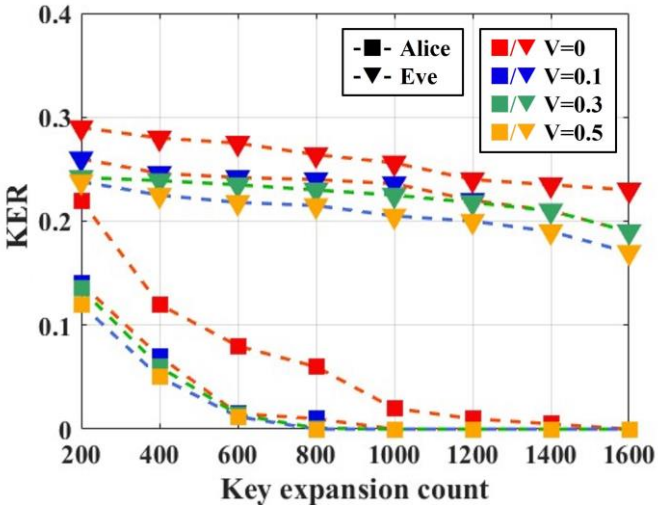

图 5 密钥拓展次数与概率整形因子对密钥错误率的影响

Fig. 5 Effects of key expansion count and probability shaping factor on KER

需注意的是，密钥拓展次数 K 与概率整形因子 V 并非越大越好，二者均需在安全性与效率之间进行权衡：一方面，密钥拓展次数增加虽然有利于合法方降低误码，但也意味着 Eve 在同一密钥提取周期内可能获取更多与密钥相关的信息；另一方面，概率整形的效果是将信号集中在幅值更低的中心区域，由于信号的发射功率是与其幅值的平方呈正相关的，因此相较于常规 QAM 信号，PS-QAM 信号所需的发射功率更低. 在发射机功率恒定的条件下，PS-QAM 信号相邻星座点之间的欧氏距离会大于常规 QAM 信号，相应的 NMS 也会变小. 随着概率整形因子的增大，PS-QAM 信号相邻星座点之间的距离进一步扩大，NMS 持续降低，此时 Eve 更容易通过对比 Alice 收发信号的星座图差异来推测密钥信息，导致系统的安全性降低.

综合考虑，本方案选取 V=0.1 作为系统参数. 在此参数配置下，仅需要进行 1000 次密钥拓展 Alice 便可无误码提取密钥. 由于正交调制使得 QAM 信号的 I/Q 两路能独立地承载信息，因此 KDR=10 Gbaud/1000×2=20 Mbit/s. 此时，Alice 和 Eve 的密钥错误率 KER 为 0.236. 理想情况下，Eve 无法获取任何有效信息时的 KER 应为 0.5，表明其对密钥比特的预测正确率等同于随机猜测. 而实验中 Eve 的 KER=0.236，表明 Alice 与 Eve 的密钥之间存在相关性. 为了降低这种相关性并提

升系统安全性，需要使用保密增强技术对密钥进行后处理操作，将部分泄露的原始密钥均匀映射为高度随机的最终密钥，使得窃听者即使掌握部分原始信息也无法推测出最终密钥的任何有效信息.

本系统所采用的保密增强技术是基于 SHA-512 散列函数完成的，该函数可将任意长度的输入比特串压缩为固定长度的 512 比特输出，通过多轮非线性运算和扩散机制确保输出密钥的高度随机性与不可逆性. 其中输出密钥长度与输入密钥长度的比值称为压缩比，为了保证最终密钥的安全性，压缩比应小于$(n\text{-}t\text{-}s)/n$[39]. 其中 n 为初始密钥长度，t 为 Eve 获取的信息量，s 为安全参数$(0<s<n\text{-}t)$.

当初始密钥长度为 10000bit 时，Eve 获取的信息量为：

$$t = n \times I\left(E:A\right) = n \times \left(H\left(A\right) - H\left(A|E\right)\right) \tag{5}$$

计算得到 $t\approx2112$. 我们选取安全参数 $s=1000$，此时压缩比为 0.688，Eve 与合法方之间的最终互信息为：

$$I\left(K;GV\right) = H\left(K\right) - H\left(K|GV\right) \le \frac{2^{-n+t+r}}{\ln 2} = \frac{2^{-s}}{\ln 2} \tag{6}$$

式中 r 为经保密增强后最终密钥的长度（$r=n\text{-}s\text{-}t$），经计算合法方与非法方之间密钥的互信息 $I(K;GV)\approx0$，意味着窃听者无法获取任何密钥信息. 最终计算得到密钥分发速率为 20 Mbit/s×0.688≈13.76 Mbit/s.

为验证方案的加密有效性，Alice 和 Bob 利用协商得到的最终密钥进行保密通信测试：Alice 先将图片信息转为二进制比特流，再与密钥进行逐位异或完成加密并发送给 Bob，Bob 使用相同的密钥解密恢复图片. 其加解密结果及分析如图 7 所示：（a1）-（a3）分别对应加密图像、Bob 解密图像和 Eve 解密图像信息；（b1）-（b3）和（c1）-（c3）分别代表对应图像的直方图和相邻像素相关图. 加密后的图片 RGB 三个通道的直方图分布均匀，水平、垂直、对角三个方向的相邻像素相关性趋近于 0，加密效果良好. Bob 可正确解密出图像信息，而 Eve 使用窃听密钥解密得到的图像，其直方图分布平均，三个方向的相邻像素点之间无相关性（如表 1 所示），无法获取任何有效视觉信息，进一步验证了所提方案的安全性.

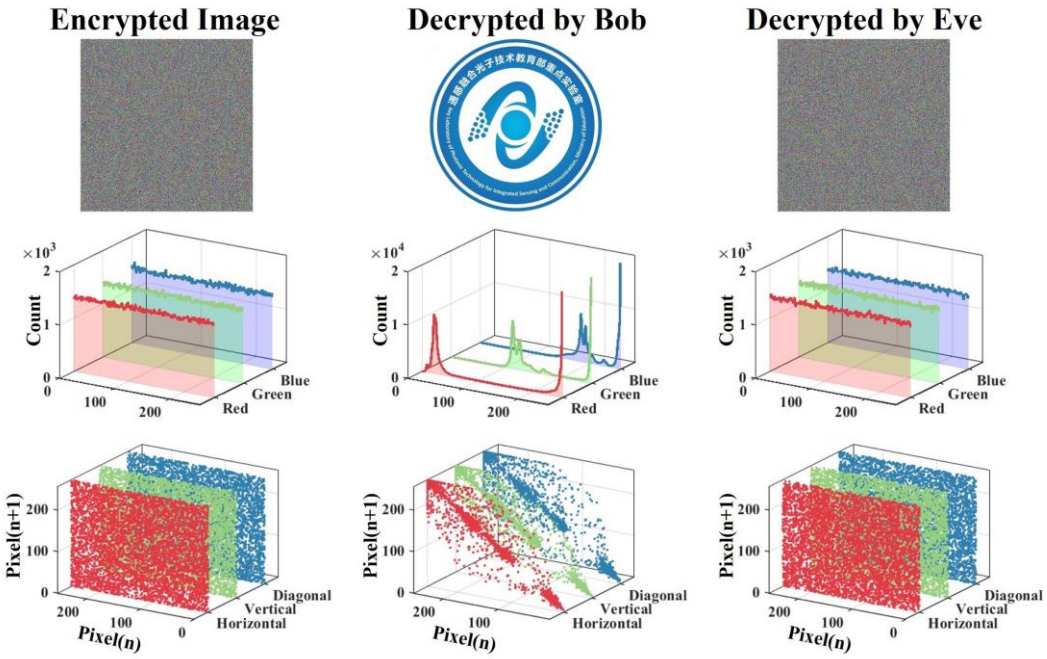

图 6 图像加解密结果

Fig. 6 Results of image encryption and decryption

表 1 相邻像素点相关性

Tab. 1 The correlation between adjacent pixel points

	Encrypted Image	Decrypted by Bob	Decrypted by Eve
Horizontal	0.003	0.978	0.013
Vertical	0.015	0.979	0.025
Diagonal	0.016	0.959	0.003

3. 3 结果讨论

本方案依托相干光通信技术的优势，对于更长传输距离和更高调制格式展现出良好的适配潜力. 一方面，相干光通信技术采用相干接收架构可大幅提升接收灵敏度，结合 DSP 技术可补偿链路传输带来的各类信号损伤，具备长距离传输的能力.随着传输距离的增大，信号受到的损耗、色散效应、非线性效应更为严重，导致接收信号的星座图更为发散，因此需要更多的密钥拓展次数才能实现无误码的密钥分发. 本文在 25 km 的光纤上进行验证性实验，对于不同长度的光纤链路，需要动态调整密钥拓展次数确保密钥的准确性；另一方面，系统中信号的最高调制阶数由器件的分辨率决定，本系统中 AWG 和示波器的分辨率均为 8 bit，因此能将信号最高调制为 PS-$2^8\times2^8$ QAM. 若搭配分辨率更高的设备，可实现更高阶的信号调制格式，进一步提升 NMS 和窃听者的 DFP，从而提升系统的安全性. 更

高阶的信号调制格式意味着解调算法更加复杂，同样需要动态调整密钥拓展次数确保双方获取的密钥是无误的.

此外，与其他物理层加密机制相比，混沌光通信对合法方的器件参数一致性要求极高，链路中的任意扰动都有可能破坏同步条件，使得通信的误码率飙升；码分多址光通信需要大量的地址码以及可灵活调节的编解码器才能实现安全通信，系统的复杂度高；隐蔽光通信将信息嵌入广泛存在的放大自发辐射（ASE）噪声中隐蔽传输，容易受到环境扰动，系统稳定性差. 上述方案因各种缺陷限制了其通信距离或兼容性，相较之下本方案具有无需部署额外器件、运行稳定性强、与光通信系统高度兼容等优势，具备大规模部署的应用潜力.

4 结　论

针对非对称 Y-00 协议映射密钥分发方案存在的速率受限问题，提出并实验论证了一种改进方案：将概率整形技术与 Y-00 协议结合，并通过哈希函数压缩初始密钥，显著提升了最终密钥的安全强度. 实验分析了不同概率整形因子 V 对密钥分发速率和安全性的影响，结果表明：在 V=0.1、压缩比为 0.688 的条件下，所提改进方案的密钥分发速率提升至 13.76 Mbit/s，相较于非改进方案提升了 3 个数量级. 同时，非法方与合法方之间的密钥互信息趋近于 0，无法获取任何密钥信息，具有较高的安全性.

参考文献

[1] Wu Q, Ribezzo D, Sciullo G D, Cocchi S, Shaji D A, Zischler L A, Luis R, Serena P, Lasagni C, Bononi A, Hayashi T, Gagliano A, Martelli P, Gatto A, Parolari P, Boffi P, Bacco D, Zavatta A, Zhu Y X, Hu W S, Xu Z P, Shtaif M, Marotta A, Graziosi F, Mecozzi A, Antonelli C 2025 *Light-Sci Appl.* **14** 274

[2] Gao H, Wang A B, Wang L S, Jia Z W, Guo Y Y, Gao Z S, Yan L S, Qin Y W, Wang Y C 2021 *Light-Sci Appl.* **10** 172

[3] Yoon C S, Hong C H, Kang M S, Choi J W, Yang H J 2023 *Sci. Rep.* **13** 3810

[4] Li K, Yan P G, Cai Q Y 2021 *Fundam. Res.* **1** 85

[5] Bennett C H, Brassard G 2014 *Theor. Compu. Sci.* **560** 7

[6] Li W, Zhang L K, Tan H, Lu Y C, Liao S K, Huang J, Li H, Wang Z, Mao H K, Yan B, Li Q, Liu Y, Zhang Q, Peng C Z, You L X, Xu F H, Pan J W 2023 *Nat. Photonics* **17** 416

[7] Jouguet P, Kunz-Jacques S, Leverrier A, Anthony L, Philippe G, Eleni D 2013 *Nat. Photonics* **7** 378

[8] Lo H K, Curty M. Tamaki K 2014 *Nat. Photonics* **8** 595

[9] Liao, S K., Cai, W Q., Liu, W Y, Zhang L, Li Y, Ren J G, Yin J, Shen Q, Cao Y, Li Z P, Li F Z, Chen X W, Sun L H, Jia J J, Wu J C, Jiang X J, Wang J F, Huang Y M, Wang Q, Zhou Y L, Deng L, Xi T, Ma L, Hu T, Zhang Q, Chen Y A, Liu N L, Wang X B, Zhu Z C, Lu C Y, Shu R, Peng C Z, Wang J Y, Pan J W 2017 *Nature* **549** 43

[10] Scheuer J, Yariv A 2006 *Phys. Rev. Lett.* **97** 140502

[11] Tonello A, Barthelemy A, Krupa K, Kermene V, Desfarges-Berthelemot A, Shalaby B M, Boscolo S, Turitsyn S K, Ania-Castanon J D 2015 *Light-Sci Appl.* **4** e276

[12] Bar-Lev D, Scheuer J 2009 *Phys. Lett. A* **373** 4287

[13] El-Taher A, Kotlicki O, Harper P, Turitsyn S, Scheuer J 2014 *Laser Photonics Rev.* **8** 436

[14] Yoshimura K, Muramatsu J, Davis P, Uchida A, Harayama T 2012 *Phys. Rev. Lett.* **108** 070602

[15] Porte X, Soriano M C, Brunner D, Fischer I 2016 *Opt. Lett.* **41** 2871

[16] Jiang N, Xue C P, Liu D, Lv Y X, Qiu K 2017 *Opt. Lett.* **42** 1055

[17] Zhao Z X, Cheng M F, Luo C K, Deng L, Zhang M M, Fu S N, Tang M, Shum P, Liu D M 2019 *Opt. Lett.* **44** 2605

[18] Huang Y, Zhou P, Li N Q 2021 *Opt. Express* **29** 19675

[19] Liu S Q, Jiang N, Zhang Y Q, Wang C, Zhao A K, Qiu K, Zhang Q W 2022 *Opt. Express* **30** 32366

[20] Liang X S, Zhang C F, Luo Y F, Cui M W, Qiu K 2022 *Opt. Express* **30** 18310

[21] Maurer U M 1993 *IEEE Trans. Inf. Theory* **39** 733-742

[22] Shao W D, Cheng M F, Deng L, Yang Q, Dai X X, Liu D 2021 *Opt. Lett.* **46** 5910

[23] Song Q H, Lai X, Chen Y C, Peng H K, Guo J C, Wu H Y, Jia B 2021 *Opt. Lett.* **46** 2264

[24] Hajomer A A E, Zhang L M, Yang X L, Hu W S 2021 *J. Lightwave Technol.* **39** 1595

[25] Qiu T H, Deng L, Yang Q, Dai X X, Liu D M, Cheng M F 2024 *Opt. Lett.* **49**, 2001

[26] Wu B, Zhou H L, Dong J J, Chen Y F, Zhu N H, Zhang X L 2024. *Nanophotonics*

13 3717

[27] Niu Z K, Xie Y H, Xu G Z, Dai C H, Yang H, Zeng C Y, Shi M H, Li L, Pu G Q, Hu W S, Yi L L 2025 *Natl. Sci. Rev.* **12** nwaf112

[28] Luo H W, Zhang Z H, Dai L Q, Zhong L S, Yang Q, Deng L, Liu D M, Dai X X, Gao X J, Cheng M F 2024 *Commun. Eng.* **3** 27

[29] Yuen H P 2003 arXiv: quant-ph/0311061 [quant-ph]

[30] Nair R, Yuen H P, Corndorf E, Eguchi T 2006 *Phys. Rev. Appl.* **74** 052309

[31] Yuen H P 2009 *IEEE J. Sel. Top. Quantum Electron.* **15** 1630

[32] Barbosa G A, Corndorf E, Kumar P, Yuen H P 2003 *Phys. Rev. Lett.* **90** 227901

[33] Yuen H P, Nair R 2006 *Phys. Lett.* A **364** 112

[34] Wang X Q, Zhang J, Li Y J, Zhao Y L, Yang X Q 2019 *IEEE Photonics J.* **11** 1

[35] Yang X K, Li Y J, Gao G J, Zhao Y L, Zhang H B, Zhang J *Asia Communications and Photonics Conference* Hangzhou, China, 2018 pp. 1

[36] Lei C, Lin R, Li Y J, Wang B, Zhang M R, Zhao Y L 2023 *J. Lightwave Technol.* **41** 5599

[37] Nakazawa M, Yoshida M, Hirooka T, Kasai K *2014 Asia Communications and Photonics Conference (ACP)* Shanghai, China, 2014, pp. 1

[38] Sun J H, Jiang L, Yi A L, Feng J C, Deng X, Pan W, Luo B, Yan L S 2023 *Opt. Express* **31** 11344

[39] Bennett C H, Brassard G, Crepeau C, Maurer U M 1995 *IEEE Trans. Inf Theory* **41** 1915

Rate Optimization of Key Distribution Based on Asymmetric Y-00 Protocol Using Probability Shaping*

LU Huihui[1) 2) 3)] MA Yuxin[1) 2) 3)] JIA Zhiwei[4)] QIN Feifei[1) 2) 3)] LI Pu[1) 2) 3) †] QIN Yuwen[1) 2) 3)]

WANG Yuncai[1) 2) 3)]

1) (Institute of Advanced Photonics Technology, School of Information Engineering, Guangdong University of Technology, Guangzhou 510006, China)

2) (Key Laboratory of Photonic Technology for Integrated Sensing and Communication (Guangdong University of Technology), Ministry of Education of China, Guangzhou 510006, China)

3) (Guangdong Provincial Key Laboratory of Information Photonics Technology, Guangdong University of Technology, Guangzhou 510006, China)

4) (Key Laboratory of Advanced Transducers and Intelligent Control System, Ministry of Education, Taiyuan University of Technology, Taiyuan 030024, China)

Abstract

In the era of explosive growth in communication data, secure key distribution is urgently required to guarantee information security. Different from key distribution based on deterministic algorithms, physical-layer key distribution has attracted extensive attention owing to the inherent randomness of physical processes. Typical physical-layer key distribution methods mainly include quantum key distribution, ultra-long fiber laser, chaotic laser synchronization, fiber channel reciprocity, and the Y-00 protocol. In particular, key distribution schemes based on the Y-00 protocol exhibit great application potential, as they require no additional hardware and are fully compatible with existing optical fiber communication systems.

In this paper, we propose a novel key distribution scheme combining the probability shaping technology with the Y-00 protocol. This scheme significantly optimizes signal transmission performance by adjusting the occurrence probability of QAM constellation points, thereby effectively improving the key distribution rate (KDR). Meanwhile, we analyze the effects of different probability shaping factors on the KDR and the system security, and select the optimal value as the system parameter. Furthermore, privacy amplification is introduced to compress the initial key sequence to strengthen the security of the final key, and guarantee that eavesdroppers cannot obtain any effective key information. Experimental results demonstrate that the proposed method achieves a KDR of 13.76 Mbit/s over a 25 km standard single-mode fiber. This method provides a

feasible solution for exploring a high-speed and secure physical layer key distribution that is compatible with the current optical communication systems.

Keywords: Physical random numbers, Y-00 protocol, Key distribution, Probability shaping, Privacy amplification

---

* Project supported by the National Key Research and Development Program of China (Grant No. 2024YFB2808400), the National Natural Science Foundation of China (Grant Nos. 62531005, 62322504, 62305073), the Guangdong S&T Programme (Grant No. 2024B0101030001), the Fundamental Research Program of Shanxi Province (Grant No. 202203021221079), and the Opening Project of the Key Laboratory of Photonic-Electronic Integration and Communication-Sensing Convergence Ministry of Education (Grant No. PICCSC202505).

† Corresponding author. E-mail: lipu8603@126. com