基于本地真随机相位键控的信道互易性密钥分发*

袁豪[1)2)3)] 马雨心[1)2)3)] 贾志伟[4)] 刘文杰[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)

(2026 年 1 月 13 日收到; 2026 年 3 月 21 日收到修改稿)

密钥的安全分发是保障加密通信安全的核心前提. 与依赖计算复杂度的密码算法不同, 物理层密钥分发技术利用物理随机过程构建密钥, 为安全通信提供了新途径. 本文提出并实验证明了一种基于本地真随机相位键控的信道互易性密钥分发方案. 该方案利用宽带光载波与非对称马赫-曾德尔干涉仪构建相位隐藏传输结构, 由本地端的物理随机数发生器产生密钥并对宽带光载波进行相位键控; 采用时延补偿技术确保双向传输的信道互易性, 使通信双方获得高相关的干涉信号; 再通过无源相位解调算法从干涉信号中提取随机相位键控码, 实现密钥共享. 实验结果表明, 在 25 km 的标准单模光纤传输链路上, 利用该方法可实现 1 Gbit/s 速率的安全密钥分发, 误码率低至 2.4‰, 满足光通信中常用的硬判决前向纠错 (HD-FEC) 阈值要求. 该方案无须预先共享熵源信息及可信第三方, 在保障密钥分发安全性的同时, 具有兼容现有光纤通信设施的应用潜力.

关键词: 物理随机数, 本地相位键控, 信道互易性, 物理层安全
DOI: 10.7498/aps.75.20260059 **CSTR:** 32037.14.aps.75.20260059

1 引 言

随着互联网技术的迅猛发展, 社会生产与生活中的敏感数据传输规模呈指数级增长, 数据泄露、非法窃听等安全威胁也随之加剧, 亟须安全的密钥分发机制构建可靠的加密通信链路, 以保障数据传输的安全性.

物理层密钥分发技术凭借其物理原理与自然随机过程的不可预测性, 有望提供解决方案. 例如, 量子密钥分发方案基于量子不可克隆原理, 理论上可实现无条件安全[1,2]; 基于巨型光纤激光器的密钥分发方案, 通过控制超长谐振腔的激射波长或自由光谱范围, 可安全协商出一致的密钥[3–5]; 而基于激光混沌同步的密钥分发方案, 则利用两个参数匹配的激光器在“共驱”或“互耦合”结构下实现混沌同步, 可生成高相关性的密钥波形[6–10]. 然而, 量子信道难以兼容现有光纤通信系统[2]; 超长光纤谐振腔导致密钥分发速率与通信距离呈反比, 其速率仍局限于 100 bit/s 量级[3–5]; 尽管宽带光学混沌可使密钥分发速率达 Gbit/s 量级[8–10], 但参数匹配激光器的制备难度极大.

基于信道互易性的密钥分发方案, 因能与数据传输共享同一光纤信道, 在兼容现有光纤基础设施

* 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, 62275054)、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) 和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

方面具有显著优势. 该方案利用光相位[11,12]、偏振态[13–15]和偏振模色散[16]等信道特征的随机波动可实时提取密钥, 其安全性源于特定位置的窃听者无法获取整个信道的动态变化信息. 但光纤信道所处的外部环境扰动通常较为稳定的, 导致密钥生成速率低于 1 kbit/s[12–16]. 采用算法生成的伪随机信号对信道进行主动加扰, 可有效突破这一速率瓶颈. 例如, 主动偏振加扰[17–19]、扰动信号星座图的振幅和相位[20]以及加速干涉结构中的相位波动[21]等方法, 能够将速率提升至 Gbit/s 量级[17–20]. 然而, 上述信道加扰方案在实现互易性时存在以下局限: 或需依赖预共享的伪随机数在用户端执行相同的信道加扰操作, 或需将加扰模块部署在信道中间节点, 并依赖额外的可信第三方控制.

本文提出了一种基于本地真随机相位键控的信道互易性密钥分发方案. 通信双方在各自的非对称马赫-曾德尔干涉结构中引入本地真随机相位键控, 并通过键控时延补偿保障双向传输的干涉信号满足互易性, 最终解调出共享密钥. 为了证明本方案的可行性, 在 25 km 的光纤链路上开展了原理性验证实验. 结果显示: 利用该方法可实现 1 Gbit/s 的真随机密钥安全分发, 合法用户误码率低至 2.4‰; 而且, 窃听者与合法用户的最大互相关趋近于 0, 无法获取任何密钥信息. 作为一种本地真随机的非对称信道加扰方法, 该方案不仅无需预先共享熵源信息, 还避免了可信第三方的引入, 有效解决了信道加扰型互易性密钥分发方案潜在的安全隐患.

2 实验装置

所提方案的实验装置如图 1(a) 所示, 合法通信方 (Alice 和 Bob) 均配置一个非对称的马赫-曾德尔干涉仪 (asymmetric Mach-Zehnder interferometer, AMZI), 并通过 25 km 标准单模光纤 (single-mode fiber, SMF) 链路连接. 双方采用独立的宽带光源作为密钥传输载波, 经光纤环形器 (circulator, CIR) 注入各自的 AMZI 中. 每个 AMZI 通过两个均匀分光比的光纤耦合器 (optical coupler, OC) 分为上下两个臂: 上臂采用基于布尔混沌电路[22]的物理真随机数发生器 (true random number generator, TRNG) 作为密钥熵源, 输出两路相同的射频信号驱动双向相位调制器 (bidirectional phase modulator, Bi-PM), 分别对两个传输方向上的光信号进行相位键控, 实现对上臂的主动加扰; 下臂用可调光延迟线 (variable optical delay line, VDL), 调节两臂之间的光程差远大于宽带光源的相干长度, 形成非对称的臂长配置; 偏振控制器 (polarization controller, PC) 则用于调节两臂之间的偏振态, 以提高干涉信号的可见度. 最终, 双方利用 3 个

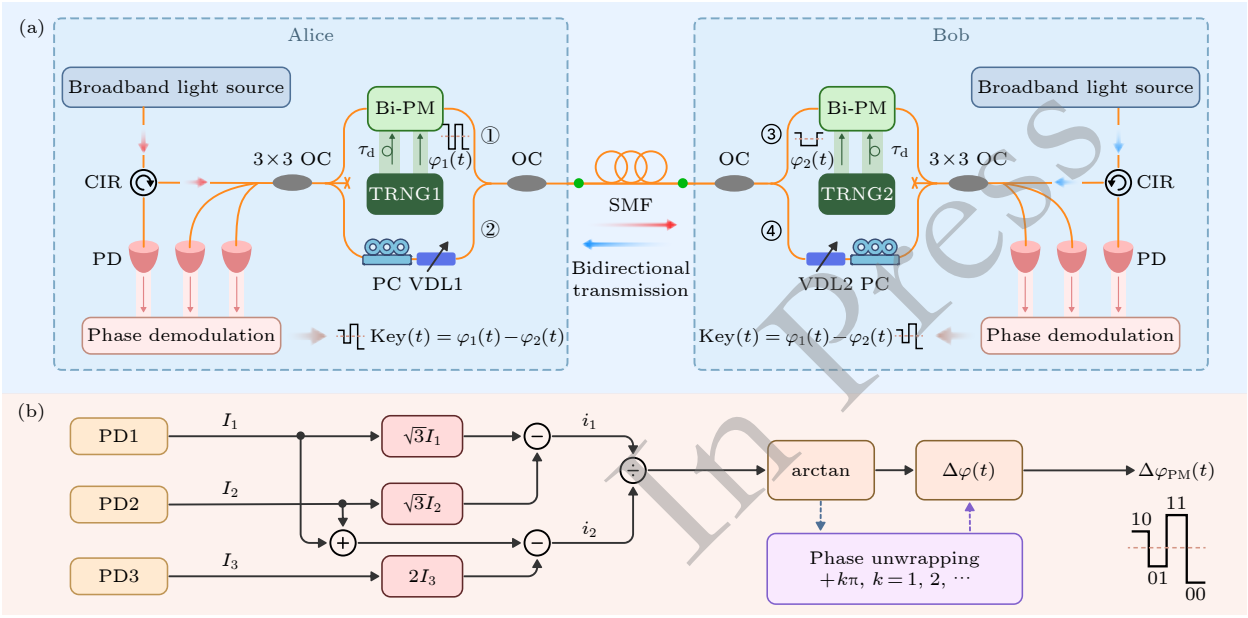

图 1 (a) 基于本地真随机相位键控的信道互易性密钥分发实验装置示意图; (b) 相位解调算法的处理流程图

Fig. 1. (a) Experimental diagram of the channel reciprocity key distribution based on local true random phase-keying; (b) data processing of the phase demodulation algorithm.

光电探测器 (photodetector, PD) 检测 3×3 耦合器输出的干涉信号, 经相位解调处理后提取相位键控码实现密钥共享.

本系统中, 宽带光源的带宽超过 3.5 THz, 相干长度约为 80 μm. 相位键控的调制格式为双极性不归零码, 调制频率为 500 MHz. 通过精确调整两个 VDL 以匹配双方的 AMZI 臂长 (确保路径“①+④”和“②+③”之间的光程差小于宽带光源的相干长度以使其满足干涉条件), Alice 与 Bob 各自的 3 个 PD 将检测到与相位键控频率相同的干涉信号. 由于两条干涉光路均经过相同的公共链路, 因此该链路上的机械振动与温度波动不会引入额外的相位差, 进而不会影响合法接收端的干涉可见度, 使系统对公共信道的环境干扰具有高鲁棒性. 这里指出, 本系统采用两个 VDL 是为了灵活控制 Alice 和 Bob 端延迟线长度, 以在两端构建非对称的臂长, 实现双向的相位隐藏传输. 原理上也可使用单个 VDL 实现: 即 Alice 首先利用器件尾纤长度构建一个臂长固定的 AMZI 结构; 随后, Bob 通过器件尾纤长度与单个延迟线调节双方 AMZI 的臂长匹配, 可进一步简化系统硬件结构, 降低部署成本.

为了获取真随机相位键控码 (密钥), 采用图 1(b) 所描述的相位解调算法对干涉信号进行解调处理. 由于 3×3 耦合器任意两个输出端口之间存在 2π/3 的相位差 [23], 因此 AMZI 输出的三路干涉信号可以表示如下:

$$Ik(t) = A + B\cos\left[\Delta\varphi_{\mathrm{PM}}(t) + \Delta\varphi_{\mathrm{e}}(t) + k\cdot\frac{2\pi}{3}\right], \tag{1}$$

其中, A 和 B 分别为直流和交流分量的幅度, $\Delta\varphi_{\mathrm{PM}}(t)$ 为待解调的密钥信息, $\Delta\varphi_{\mathrm{e}}(t)$ 表示用户终端环境变化引起的相位噪声, k 为耦合器输出端口的编号 ($k = 1, 2, 3$). 相位解调的数据处理流程如下:

1) 利用三角函数的数学关系, 计算出两路正交的信号:

$$i_1(t) = -3B\sin[\Delta\varphi_{\mathrm{PM}}(t) + \Delta\varphi_{\mathrm{e}}(t)],$$

和

$$i_2(t) = -3B\cos[\Delta\varphi_{\mathrm{PM}}(t) + \Delta\varphi_{\mathrm{e}}(t)].$$

2) 将 $i_1(t)$ 和 $i_2(t)$ 两路正交的信号相除, 并利用 $\arctan(x)$ 函数进行反正切运算可得干涉信号的相位信息:

$$\Delta\varphi(t) = \arctan[i_1(t)/i_2(t)] = \Delta\varphi_{\mathrm{PM}}(t) + \Delta\varphi_{\mathrm{e}}(t).$$

由于 $\arctan(x)$ 函数的值域为 $(-\pi/2, \pi/2)$, 当相位变化幅度超过该区间时, 需进一步执行相位解包裹处理. 而本系统将总的相位键控幅度被控制在 PM 的半波电压范围内, 因此无需额外相位解包裹, 有效降低了相位解调的计算复杂度. 此外, 由于环境波动引起的低频相位噪声 $\Delta\varphi_{\mathrm{e}}(t)$ 为百赫兹量级 [11], 远低于本系统中百兆赫兹变化频率的相位键控信号 $\Delta\varphi_{\mathrm{PM}}(t)$, 故 $\Delta\varphi_{\mathrm{e}}(t)$ 的影响可忽略不计.

在两条干涉光路“①+④”和“②+③”中, 由于 TRNG1 和 TRNG2 相互独立, 经两次本地相位键控后, 双方干涉信号的相位解调结果 $\Delta\varphi_{\mathrm{Alice}}(t)$ 和 $\Delta\varphi_{\mathrm{Bob}}(t)$ 可以表示为

$$\Delta\varphi\mathrm{Alice}(t) = \varphi_{\mathrm{TRNG1}}(t+\tau) - \frac{1}{2}\varphi_{\mathrm{TRNG2}}(t+\tau_{\mathrm{d}}), \tag{2}$$

$$\Delta\varphi\mathrm{Bob}(t) = \frac{1}{2}\varphi_{\mathrm{TRNG2}}(t+\tau) - \varphi_{\mathrm{TRNG1}}(t+\tau_{\mathrm{d}}), \tag{3}$$

其中, $\varphi_{\mathrm{TRNG}}(t)$ 表示 TRNG 产生的相位调制信号, τ 为公共信道的传输时延, τ_{d} 是对调制信号施加的主动时延. 1/2 系数为 TRNG2 调制时的幅度衰减因子, 用于产生四电平密钥. 由 (2) 式和 (3) 式可知, 为确保干涉光路在两个传输方向上经历相同的相位差, 通信双方需对各自 TRNG 的其中一路输出信号施加时延以补偿信道传输时间 (主动时延 τ_{d} 等于信道时延 τ), 使得总相位差满足 $\Delta\varphi_{\mathrm{Alice}}(t) = -\Delta\varphi_{\mathrm{Bob}}(t)$, 即可实现本地相位键控调制的双向传输互易性.

表 1 详细描述了相位调制期间的具体相位编码规则, 明确了 $\varphi_{\mathrm{TRNG1}}(t)$ 和 $\varphi_{\mathrm{TRNG2}}(t)$ 两次相位调制与总相位差 $\Delta\varphi(t)$ 的编码对应关系. 其中, 编码比特与相位值一一对应, 这些相位值是通过调

表 1 相位调制期间的相位编码表

Table 1. Phase coding table during phase modulation.

调制信号	调制格式	编码比特	相位值
$\varphi_{\mathrm{TRNG1}}(t)$	双极性NRZ码	1	π/3
		0	−π/3
$\varphi_{\mathrm{TRNG2}}(t)$	双极性NRZ码	1	π/6
		0	−π/6
$\Delta\varphi_{\mathrm{Alice}}(t)$或 $\Delta\varphi_{\mathrm{Bob}}(t)$	四电平相位差	10	π/2
		11	π/6
		00	−π/6
		01	−π/2

节 TRNG 输出射频电压与 PM 半波电压的比值进行控制, 旨在产生电平分布均匀的干涉信号, 降低相位解调的误码率.

3 实验结果

图 2 是通信双方进行本地相位键控调制及 PD 接收干涉信号的实验结果. 为准确测量信道时延 τ, 先在系统中仅保留 Alice 端施加相位调制 (TRNG1 产生两路无时延的相同射频信号, 驱动 Bi-PM 对两个传输方向的光信号进行相同的相位键控调制), 随后在 Alice 与 Bob 端采集 200 万个样本点的干涉信号并计算二者的互相关 (cross-correlation, CC) 曲线, 结果如图 2(a) 所示. 在延迟 123.531 μs 处出现一个清晰的峰值, 该峰值即为光沿着公共信道的传输时延 τ; 而 CC 曲线 0.2 ns 的半峰全宽, 则与相位键控周期一致.

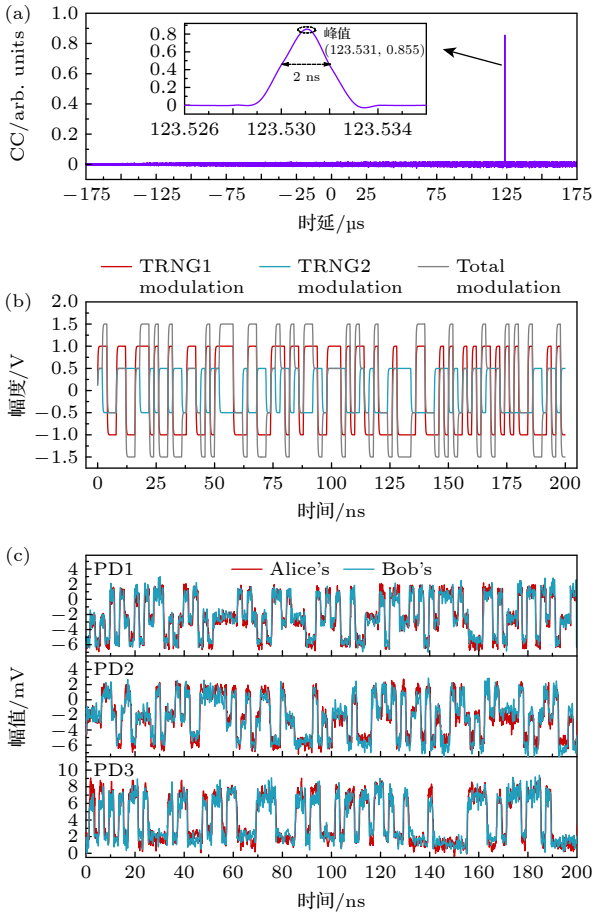

图 2 相位键控调制及干涉信号的实验结果 (a) 信道时延测量; (b) TRNG1 和 TRNG2 产生的相位键控信号; (c) Alice 和 Bob 检测到的干涉信号

Fig. 2. Experimental results of phase-shift modulation and interference signals: (a) Channel time-delay measurement; (b) phase-keying modulation signals generated by TRNG1 and TRNG2; (c) interference signals detected by Alice's PD and Bob's PD.

基于上述测得的信道时延, 通信双方用 TRNG 分别驱动各自的 Bi-PM 完成双向互易的本地相位键控调制. 如图 2(b) 所示, 通过将 Bob 端 TRNG2 的调制幅度减半, 总相位差能够形成四电平分布. 这种四电平的相位调制格式, 可在相同键控频率下使比特生成速率提升 1 倍. 图 2(c) 为 Alice 与 Bob 端接收到的三路干涉信号. 根据 (1) 式, PD 检测到的干涉信号是总相位差 $\Delta\varphi(t)$ 叠加上 3×3 耦合器附加相移的余弦函数. 因此, 在总相位差 $\Delta\varphi(t)$ 相同的情况下, 三路干涉信号呈现出差异化的电平分布特征. 实验中通过调整 TRNG 射频电压与 PM 半波电压的比值, 可控制相位键控的调制深度, 最终获得电平分布均匀且电平间隔最大的三路干涉信号, 有效提升了系统的抗噪能力. 需要说明的是, Alice 与 Bob 端的 PD1, PD2 采用了交流耦合的光电探测器, 其内部电容滤除了信号的直流分量, 导致输出干涉信号存在负的电压值.

图 3 是 Alice 与 Bob 对干涉信号进行相位解调提取共享密钥的实验结果. 图 3(a) 为相位解调后的密钥波形, 而图 3(b) 为 24 ns 时间窗口内的局部放大图及密钥波形的量化过程. 量化规则如下: 根据解调信号的幅度分布划为 4 个判决区间; 对于 2 ns 的采样时间间隔, 存在 20 个采样点, 选择分布计数最高的区间作为判决区间; 然后将 4 个区间的幅度分别量化为“10”, “11”, “00”和“01”, 对应于两个 TRNG 的输出比特. 每 2 ns 可生成 2 bit 密钥, 因此该系统实现了 1 Gbit/s 的密钥生成速率. 图 3(c) 为双方密钥波形的互相关曲线, 最大互相关系数 0.914, 表明信道互易性确保了双方解调的密钥具有高相关性.

采集 1000 组每组 1 Mbit 长度的密钥序列, 测得误码率为 2.4‰, 低于光纤通信中的硬判决前向纠错 (hard-decision forward error correction, HD-FEC) 阈值 3.8‰. 这表明可以使用 FEC 技术有效地纠正残留的错误比特. 进一步, 为了评估密钥的随机性, 根据美国国家标准与技术局制定的 NIST SP 800-22 随机数测试标准对所获得的密钥进行随机性测试. 测试结果如图 3(d) 所示: 15 项测试的 P 值 (P-value) 均大于 0.0001, 通过率高于 0.9806, 表明该方案生成的密钥具有统计无偏性与相互独

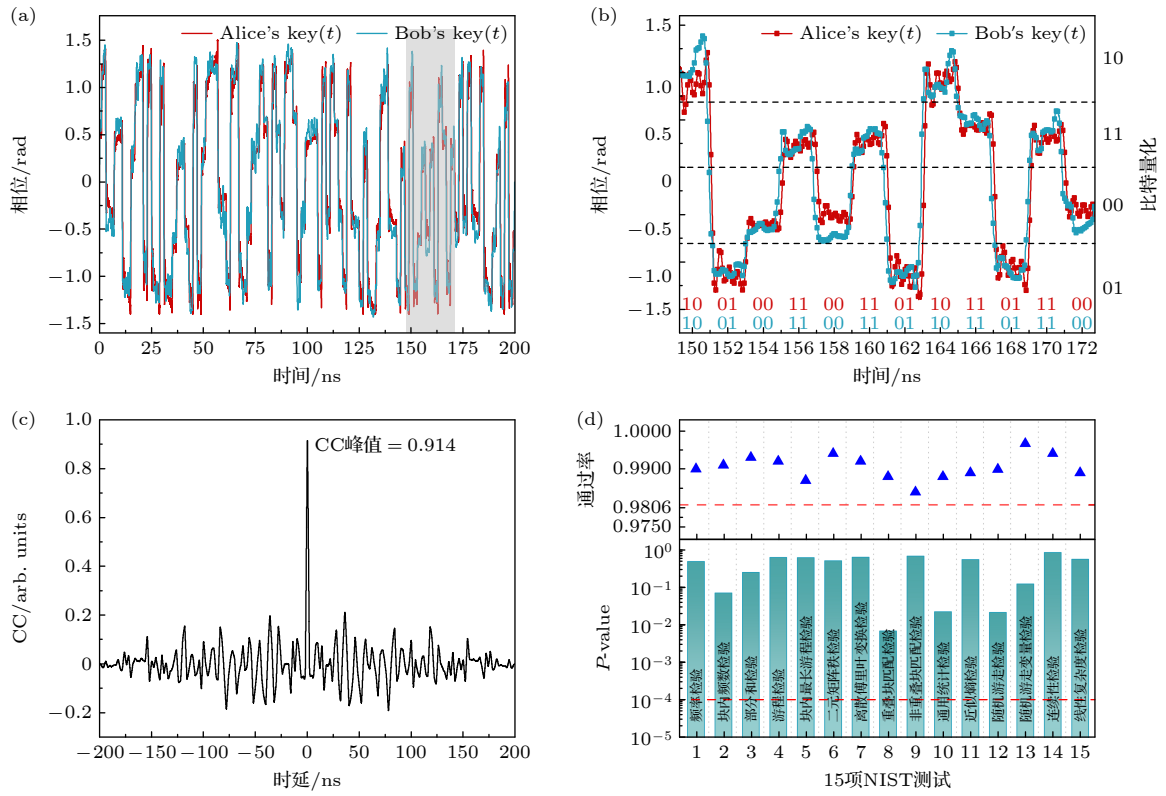

图 3 密钥分发实验结果 (a) 相位解调结果; (b) 密钥波形的量化; (c) Alice 和 Bob 之间的互相关曲线; (d) NIST 测试结果

Fig. 3. Key distribution experiment results: (a) Phase demodulation results; (b) quantization of key waveforms; (c) cross-correlation curve between Alice and Bob; (d) NIST test results.

立性——这源于合法用户端物理随机数发生器. 注: 本实验在恒温恒湿超净间实验室的减振光学平台上开展, 连续 6 h 测试期间, 误码率虽存在一定起伏, 但其最大值始终控制在 2.75‰以内, 远低于 HD-FEC 纠错阈值 3.8‰. 若要进一步保障系统长期稳定运行, 可考虑引入主动反馈等稳相优化方案.

4 安全性分析

本文通过实验和理论分析, 从物理机制上证明窃听者 (eavesdropper, Eve) 无法获取任何密钥信息. 图 4(a) 为 Eve 在公共链路中使用 10∶90 的光纤耦合器进行分光窃听的攻击模型, 需同时截获两个传输方向上的光信号才有可能重构密钥. 但如图 4(b) 所示, Eve 仅能检测到宽带光源的固有强度噪声, 其核心原因在于: 非对称的干涉结构与宽带光源的短相干长度特性, 使传输链路无法满足干涉条件. 相位键控信号被隐藏于宽带光源的相位噪声中, 远超现有电子设备的所能测量的范围. 图 4(c) 的窃听者与合法通信方之间的互相关曲线进一步验证了这一结论. 在任意传输方向上, Eve 和合法用户之间的最大互相关系数均接近于 0, 这意味着 Eve 无法获取任何密钥信息.

针对该分光窃听的实验结果, 可通过对光场传输特性进行理论分析予以证明. 对于均匀分光比的 3×3 耦合器和 2×2 耦合器, 由模式耦合理论可知其光场传输矩阵为 [23]

$$T_{3\times3\mathrm{OC}}=\frac{1}{\sqrt{3}}\begin{pmatrix}1 & \mathrm{e}^{\mathrm{j}\frac{2\pi}{3}} & \mathrm{e}^{\mathrm{j}\frac{2\pi}{3}}\\ \mathrm{e}^{\mathrm{j}\frac{2\pi}{3}} & 1 & \mathrm{e}^{\mathrm{j}\frac{2\pi}{3}}\\ \mathrm{e}^{\mathrm{j}\frac{2\pi}{3}} & \mathrm{e}^{\mathrm{j}\frac{2\pi}{3}} & 1\end{pmatrix}, \tag{4}$$

$$T_{2\times2\mathrm{OC}}=\frac{1}{\sqrt{2}}\begin{pmatrix}1 & j\\ j & 1\end{pmatrix}. \tag{5}$$

本系统中, 发送端 (Alice 或 Bob) 的 AMZI 的传输矩阵可表示为

$$T_{\mathrm{MZI}}=\begin{pmatrix}\mathrm{e}^{\mathrm{j}\varphi_{\mathrm{PM}}(t)} & 0\\ 0 & \mathrm{e}^{\mathrm{j}\varphi_{\mathrm{DL}}}\end{pmatrix}, \tag{6}$$

其中 $\varphi_{\mathrm{PM}}(t)$ 是施加到 MZI 上臂的相位键控信号 (即密钥信息), φ_{DL} 表示下臂 VDL 施加的相位延迟.

假设宽带光源的输入光场为

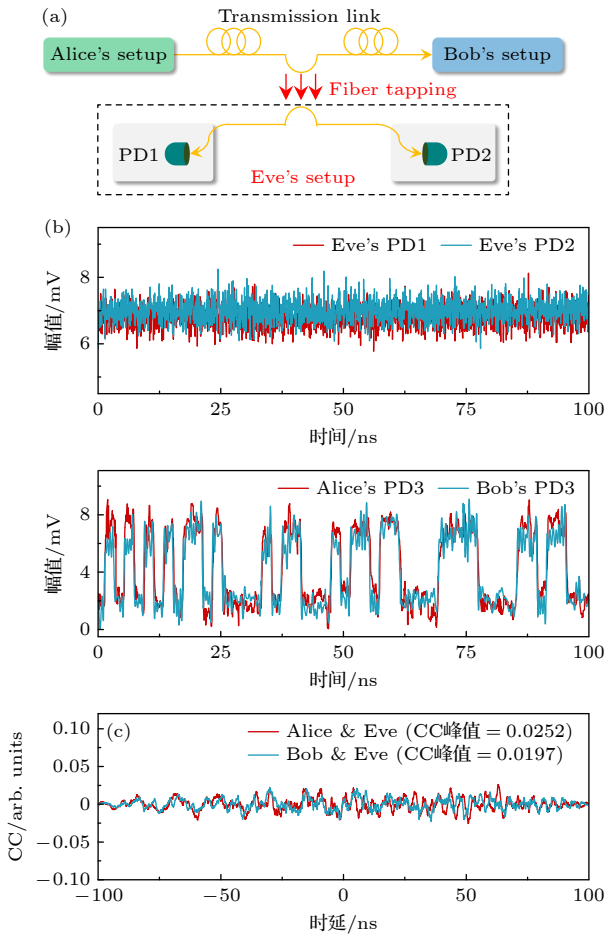

图 5 安全性分析实验结果 (a) 光纤链路分接窃听模型; (b) 窃听者与合法用户接收的强度信号; (c) 窃听者与合法用户的互相关曲线

Fig. 5. Security analysis experimental results: (a) The attack model of tapping the fiber link; (b) intensity signals received by eavesdroppers and legitimate users; (c) cross-correlation curve between eavesdroppers and legitimate users.

$$E_{\rm in}(t)=\begin{pmatrix} E_0 {\rm e}^{{\rm j}\varphi_{\rm s}(t)} \\ 0 \\ 0 \end{pmatrix}, \tag{7}$$

其中, E_0 是光场的振幅, $\varphi_{\rm s}(t)$ 是宽带光源的固有相位噪声, $\varphi_{\rm s}(t)$ 与其光谱带宽成正比.

利用 (4) 式—(7) 式, 可以计算 MZI 输出至公共信道的光场表达式为

$$\begin{aligned} E_{\rm out}(t) &= T_{2\times 2{\rm OC}}\cdot T_{\rm MZI}\cdot T_{3\times 3{\rm OC}}\cdot E_{\rm in}(t) \\ &= \frac{1}{\sqrt{6}}E_0\left\{{\rm e}^{{\rm j}[\varphi_{\rm s}(t+t_1)+\varphi_{\rm PM}]}+{\rm j}\cdot{\rm e}^{{\rm j}\left[\varphi_{\rm s}(t+t_2)+\varphi_{\rm DL}+\frac{2\pi}{3}\right]}\right\}, \end{aligned} \tag{8}$$

其中, t_1 和 t_2 分别表示光通过 MZI 的上臂和下臂所需时间.

因此, 发射到公共信道中的光信号强度为

$$\begin{aligned} I_{\rm out}(t) &= E_{\rm out}(t)\cdot E_{\rm out}^{*}(t) \\ &= \frac{1}{3}E_0^2\left\{1-\cos\left[\varphi_{\rm s}(t+t_2)-\varphi_{\rm s}(t+t_1)\right.\right. \\ &\quad \left.\left.+\varphi_{\rm DL}-\varphi_{\rm PM}(t)+\frac{\pi}{6}\right]\right\}. \end{aligned} \tag{9}$$

其交流分量的归一化波形由 (10) 式给出:

$$\begin{aligned} i_{\rm AC}(t) &= \cos\left[\varphi_{\rm s}(t+t_2)-\varphi_{\rm s}(t+t_1)\right. \\ &\quad \left.+\varphi_{\rm DL}-\varphi_{\rm PM}(t)+\frac{\pi}{6}\right]. \end{aligned} \tag{10}$$

由于 Alice 和 Bob 端 MZI 的臂长均为不对称设计, 因此光场传输时间 $t_1<t_2$. 在 (10) 式中, 宽带光源相位噪声项 $\varphi_{\rm s}(t+t_2)-\varphi_{\rm s}(t+t_1)\neq 0$, 相位键控信号 $\varphi_{\rm PM}(t)$ 被隐藏在宽带光源 3.5 THz 的相位噪声中. 当采用带宽几十 GHz 量级的 PD 检测时, 相当于对信号 $i_{\rm AC}(t)$ 施加一个低通滤波器, 经 PD 检测后, 交流项 $i_{\rm AC}(t)$ 将变为时间平均值 $\langle i_{\rm AC}(t)\rangle\approx 0$, 故仅能检测到 $E_0^2(t)$, 即宽带光源各个频率分量在 PD 上相互拍频产生的振幅 (强度) 噪声.

为了消除宽带光源的相位噪声以获取干涉信号, 窃听者必须构建与合法用户完全一致的 AMZI 结构. 但是, 在缺乏系统先验知识的情况下, Eve 只能随机猜测系统参数, 并在 80 μm 相干长度内匹配 AMZI 的臂长. 实验中, 即使双方 AMZI 的下臂长度由 4 m 器件尾纤构成, Eve 的臂长成功匹配的概率也仅有 10^{-5}, 且增加光源带宽或扩展臂长至公里尺度, 可进一步提升 Eve 的猜测难度.

这里我们证明即使 Eve 猜到 AMZI 的结构参数, 仍然无法获取正确的密钥序列. 与图 4(a) 类似, 假设 Eve 在公共链路上成功搭建两套与合法双方完全一致的 AMZI 结构 (不施加相位调制), 分别窃听两个方向的光信号. Eve 可采用相同的解调方法, 从干涉信号中提取相位键控信息, 并将两个方向的窃听结果叠加, 以获取四电平密钥波形. 然而, 合法通信双方可在各自本地端 (信号进入公共链路之前) 分别引入一段长度不等的光纤, 使得 Eve 在公共链路上窃听的两路信号存在不同的路径延迟, 导致两个解调结果之间存在严重的时延失配. 具体而言, Eve 窃听所得的密钥波形可表示为

$$\Delta\varphi_{\rm Eve}(t)=\varphi_{\rm TRNG1}(t+t_1)-(1/2)\varphi_{\rm TRNG2}(t+t_2),$$

其中, t_1 和 t_2 分别为 Eve 在两个传输方向上窃听

相位键控信号时对应的路径延迟. 而合法通信双方的密钥波形如 (2) 式和 (3) 式所示, 可统一记为

$$\Delta\varphi_{\mathrm{Alice/Bob}}(t) = \varphi_{\mathrm{TRNG1}}(t) - (1/2)\varphi_{\mathrm{TRNG2}}(t).$$

当 Alice 与 Bob 在各自 AMZI 前端接入长度不同的光纤时, 将引入不对称的路径延迟, 即 $t_1 \neq t_2$. 由于 TRNG1 和 TRNG2 为相互独立且不可预测的物理熵源, $\varphi_{\mathrm{TRNG1}}(t+t_1)$ 与 $\varphi_{\mathrm{TRNG2}}(t+t_2)$ 的叠加结果 $\Delta\varphi_{\mathrm{Eve}}(t)$ 会因时延失配而呈现完全不同的电平分布. 因此, 即便 Eve 成功复制了合法双方的 AMZI 结构, 信道时延的不对称性以及 TRNG 的不可预测性, 仍能有效阻止 Eve 从窃听结果重构出正确的四电平密钥序列.

对于 Eve 可能实施的光注入攻击 (不切断光纤, 耦合注入) 与拦截发送攻击 (切断光纤, 重新注入), 本系统仍具有抗攻击能力. 这两类攻击的本质均为 Eve 向合法双方注入自身编码调制的光信号, 以伪造或篡改最终生成的密钥. 本文考虑最坏的攻击场景, 即 Eve 可以切断公共链路, 并向 Alice 和 Bob 两端注入相同强度调制的光信号, 冒充合法通信双方检测到的干涉信号, 进而控制密钥的生成. 针此类攻击, 合法通信双方可利用耦合器从本地 AMZI 的任意一臂分出少量光信号进行实时监测: 在系统正常工作时, 由于非对称臂长不满足干涉条件, AMZI 任意一臂仅能检测到宽带光源的强度噪声; 然而, 一旦遭受光注入或拦截发送攻击, 两个臂均会检测到携带 Eve 强度调制特征的非法光信号. 因此, 在合法双方 AMZI 的任意一臂进行实时信号监测, 可以有效识别并抵御 Eve 发起的此类注入攻击. 注意, 这里重点阐明系统安全性的物理机理与理论依据, 对窃听信息量的定量估算不在本文讨论范围内, 相关建模与深入分析将在后续工作中系统开展.

5 结 论

针对信道加扰型互易性密钥分发方案存在的安全隐患, 本文提出并实验证明了一种改进方案: 通过在本地端引入真随机相位键控, 结合非对称的马赫-曾德尔干涉结构与短相干长度光源, 在保障密钥隐写传输的同时, 实现了本地真随机加扰的信道互易性. 结果表明: 在 500 MHz 的相位键控频率下, 所提方案能够在 25 km 单模光纤传输链路上实现 1 Gbit/s 的安全密钥分发, 且合法用户的误码率为 2.4‰, 满足光通信中常用的硬判决前向纠错 (HD-FEC) 阈值要求. 窃听者仅能检测到宽带光源的强度噪声, 与合法用户的互相关趋近于 0, 无法获取任何密钥信息. 这种本地真随机的非对称加扰机制, 无需预先共享伪随机数或引入可信第三方, 为实现兼容现有光纤通信设施的安全密钥分发提供了可行路径.

面向多点通信 (网络化密钥分发) 的扩展需求, 可基于本系统依赖两节点间双向通信实现信道互易性的物理本质, 在组网应用中采用星型或环型拓扑结构. 然而, 该互易机制在组网扩展方面还存在现实挑战. 例如, 随着节点数量增加, 多链路间的时延校准难度提升, 各节点的时延补偿机制需满足更严格的互易性物理条件, 尚需进一步的理论设计与实验验证.

参考文献

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

[2] Diamanti E, Lo H K, Qi B, Yuan Z 2016 *npj Quantum Inf.* **2** 16025

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

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

[5] Tonello A, Barthélémy A, Krupa K, Kermène V, Desfarges-Berthelemot A, Shalaby B M, Boscolo S, Turitsyn S K, Ania-Castañón J D 2015 *Light Sci. Appl.* **4** e276

[6] Yoshimura K, Muramatsu J, Davis P, Harayama T, Okumura H, Morikatsu S, Aida H, Uchida A 2012 *Phys. Rev. Lett.* **108** 070602

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

[8] Böhm F, Sahakian S, Dooms A, Verschaffelt G, Van der Sande G 2020 *Phys. Rev. Appl.* **13** 064014

[9] 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

[10] Gao Z S, Ma Z Y, Wu S L, Gao H, Wang A B, Fu S N, Li Z H, Qin Y W, Wang Y C 2022 *Opt. Express* **30** 23953

[11] Kravtsov K, Wang Z, Trappe W, Prucnal P R 2013 *Opt. Express* **21** 23756

[12] Huang C R, Ma P Y, Blow E C, Mittal P, Prucnal P R 2019 *Opt. Express* **27** 32096

[13] Hajomer A A E, Yang X L, Sultan A, Hu W S 2018 *IEEE Photon. Technol. Lett.* **30** 704

[14] Zhang L M, Hajomer A A E, Yang X L, Hu W S 2019 *Opt. Express* **27** 29207

[15] Wu B, Zhou H L, Dong J J, Chen Y F, Zhu N H, Zhang X L 2024 *Nanophotonics* **13** 3717

[16] Zaman I U, Lopez A B, Al Faruque M A, Boyraz O 2018 *J. Lightwave Technol.* **36** 5903

[17] Zhang L M, Hajomer A A E, Hu W S, Yang X F 2021 *IEEE Photon. Technol. Lett.* **33** 289

[18] Shao W D, Qiu T H, Deng L, Yang Q, Dai X X, Liu D M, Cheng M F 2022 *Opt. Lett.* **47** 6125

[19] Huang X R, Xie Y H, Zhang L M, Wu Q, Chai Z, Li M Y, Yi L L, Hu W S, Yang X L 2025 *Opt. Lett.* **50** 3138

[20] Qiu T H, Shao W D, Deng L, Yang Q, Liu D M, Yu Y Q, Gao X J, Cheng M F 2023 *Opt. Lett.* **48** 3547

[21] Song Q H, Lai X, Chen Y C, Peng H K, Guo J C, Wu H Y, Jia B 2021 *Opt. Lett.* **46** 2264
[22] Zhang R, de S. Cavalcante H L D, Gao Z, Gauthier D J, Socolar J E S, Adams M M, Lathrop D P 2009 *Phys. Rev. E* **80** 045202
[23] Priest R G 1982 *IEEE Trans. Microw. Theory Tech.* **30** 1589

Channel reciprocity key distribution based on local true random phase-keying*

YUAN Hao [1)2)3)] MA Yuxin [1)2)3)] JIA Zhiwei [4)] LIU Wenjie [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, Ministry of Education of China, Guangdong University of Technology, Guangzhou* 51006, *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, Taiyuan* 030024, *China*)

(Received 13 January 2026; revised manuscript received 21 March 2026)

Abstract

In the era of exponentially growing sensitive data, secure key distribution mechanisms are urgently needed to establish reliable encrypted communication links. Channel reciprocity-based key distribution technologies possess significant advantages in compatibility with existing fiber-optic infrastructures, as they can share the same fiber channel with data transmission. However, constrained by the bandwidth of environmental fluctuations, such technologies generally suffer from low key generation rates, typically on the order of kbit/s. Although active channel scrambling schemes can increase the key distribution rate to the Gbit/s level, they require pre-shared pseudo-random algorithms or the introduction of trusted third parties, thus posing potential security vulnerabilities.

In this paper, a novel channel reciprocity scheme based on local true random phase-keying is proposed for high-speed secure key distribution. The scheme establishes a phase-concealed transmission structure using a broadband optical carrier and an asymmetric Mach–Zehnder interferometer. It employs a physical random number generator at the local end to generate random keys and performs phase-keying modulation on the broadband optical carrier. Time-delay compensation technology is adopted to ensure channel reciprocity during bidirectional transmission, enabling both communication parties to obtain highly correlated interference signals. Subsequently, a passive phase demodulation algorithm is used to extract the random phase-keying codes from the interference signals to achieve key sharing. Experimental results over a 25 km standard single-mode fiber link demonstrate that the proposed scheme achieves a secure key distribution rate of 1 Gbit/s at a phase-keying modulation frequency of 500 MHz. The bit error rate is as low as 2.4‰, which is well below the threshold of hard-decision forward error correction (3.8‰) widely adopted in commercial optical communication systems.

Keywords: physical random numbers, local phase-keying, channel reciprocity, physical-layer security.

DOI: 10.7498/aps.75.20260059 **CSTR:** 32037.14.aps.75.20260059

* 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, 62275054), the S&T Programme of Guangdong Province, China (Grant No. 2024B0101030001), the Fundamental Research Program of Shanxi Province, China (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