第 49 卷 第 4 期/2022 年 2 月/中国激光 研究论文

中国激光

基于对称相移键控混沌同步的高速密钥安全分发

武超人[1,2]，高华[1,2]，王龙生[1,2*]，郭园园[1,2]，王安帮[1,2]，王云才[1,2]

[1]太原理工大学新型传感器与智能控制教育部重点实验室，山西 太原 030024；

[2]太原理工大学物理与光电工程学院，山西 太原 030024

摘要 提出一种基于对称相移键控混沌同步的高速密钥安全分发方案：混沌驱动信号对称地经过两个非平衡马赫-曾德尔干涉仪驱动无外腔反馈的响应激光器，并通过随机键控马赫-曾德尔干涉仪中的相位调制器实现相移键控混沌同步。通信双方对相移键控混沌同步时序进行双阈值量化产生随机密钥，然后交换、对比键控参数并筛选出参数相同（即键控相位相同）时的随机密钥作为一致密钥，实现密钥分发。本方案中，混沌驱动信号经过非平衡马赫-曾德尔干涉仪产生了基于延时自干涉的非线性变换，降低了驱动信号与响应信号之间的相关性（～0.25），提高了密钥分发的安全性。此外，利用共驱无外腔反馈响应激光器构成开环同步结构，缩短混沌同步恢复时间至～1.8 ns，提高了密钥分发速率。数值仿真结果表明，在误码率为 3.8×10^{-3} 的条件下，可实现 1.28 Gbit/s 的高速密钥安全分发。

关键词 光通信；半导体激光器；混沌激光；混沌同步；密钥分发；保密通信

中图分类号 TN248.4 **文献标志码** A **doi**：10.3788/CJL202249.0406001

1 引 言

信息安全的核心是保密通信。“一次一密”是绝对安全的保密通信[1]，其实现的关键在于高速密钥安全分发。随着计算机算力的不断提升，基于数学算法的密钥分发在原理上始终存在着被破解的安全隐患。物理层的密钥分发具有更高的安全性，如量子密钥分发[2-3]、基于光纤激光器的密钥分发[4]、基于信道噪声的密钥分发[5]等。然而，受密钥分发机制或物理熵源带宽的限制，上述物理层密钥分发速率仅为 bit/s 至 kbit/s 量级，难以满足高速通信的速率需求。

研究发现，半导体激光器在外部扰动下可产生宽带混沌激光，其输出光强具有大幅度随机起伏特征，可产生速率在 Gbit/s～Tbit/s 量级的高速物理随机数[6-7]。此外，参数匹配的激光器可实现混沌同步[8-10]，通过对混沌同步波形量化可产生相关的高速物理密钥[11]。因此，利用混沌激光作为物理熵源，并结合混沌同步，有望实现高速物理密钥分发。Uchida 教授团队提出并实验验证了基于光反馈激光器相移键控混沌同步的密钥分发方案，实现了速率约 180 kbit/s 的密钥分发[12-13]。需要指出的是，光反馈激光器构成闭环结构，其反馈光路的随机相移键控导致激光器需要长时间振荡才可以再次实现混沌同步——同步恢复时间达数十纳秒，限制了密钥分发速率。国内学者在基于混沌同步的密钥分发速率提升方面开展了一些探索性的研究，例如：江宁教授课题组提出了基于动态不可预测后处理[14]、交替步进算法后处理[15]、垂直腔面发射激光器动态随机偏振同步的密钥分发方案[16]；项水英教授课题组提出一种基于带宽增强混沌同步的密钥分发方案[17]。值得注意的是，上述方案均利用混沌激光器

收稿日期：2021-05-31；**修回日期**：2021-06-17；**录用日期**：2021-06-30

基金项目：国家自然科学基金（61805170，61822509，62035009，61713014，61961136002，61805171）、山西省“1331”工程重点创新团队项目、山西省高等学校中青年拔尖创新人才计划基金、山西省重点研发计划国际科技合作项目（201903D421012）、广东省信息光子技术重点实验室（广东工业大学）开放课题（GKPT20-01）、广东省引进创新创业团队项目

通信作者：*wanglongsheng@tyut.edu.cn

驱动响应激光器构建混沌同步——驱动信号与响应信号之间存在残余相关性。基于该相关性，窃听者可直接通过驱动信号获取部分相关密钥，导致密钥分发安全性有所降低。此外，程孟凡教授课题组和张耀辉研究员课题组分别探索了基于模/数混合混沌同步与半导体超晶格混沌同步的密钥分发方案[18-19]。

本文提出一种基于对称相移键控混沌同步的高速密钥安全分发方案。在该方案中，混沌驱动信号经过非平衡马赫-曾德尔(M-Z)干涉仪产生基于延时自干涉的非线性变换，降低了驱动信号与响应信号之间的相关性，从而提高密钥分发的安全性。此外，响应激光器无外腔反馈，构成开环结构，可缩短混沌同步恢复时间，从而提高密钥分发速率。基于上述优点，通过数值模拟实现了速率为 1.28 Gbit/s 的高速密钥安全分发。

2　方案与理论模型

图 1 为所提密钥分发方案示意图。镜面(M)和光反馈驱动激光器(DFB-D)输出的混沌信号经耦合器(FC)分成两路，对称地经过两个非平衡 M-Z 干涉仪[延迟线(ODL)的长度相同]，并注入到通信双方(Alice 和 Bob)的响应激光器(DFB-A 和 DFB-B)。利用随机比特发生器(RBG)产生的随机码键控相位调制器(PM)：当双方相位相同时，DFB-A 和 DFB-B 输出的混沌信号可实现混沌同步；反之，则不同步。上述混沌信号经光电探测器(PD)探测与双阈值量化(quantization)产生随机密钥，并与相位键控参数一同存储到记录器(recorder)中。通过交换、对比，筛选出相位键控参数相同时的随机密钥作为一致密钥，实现密钥分发。

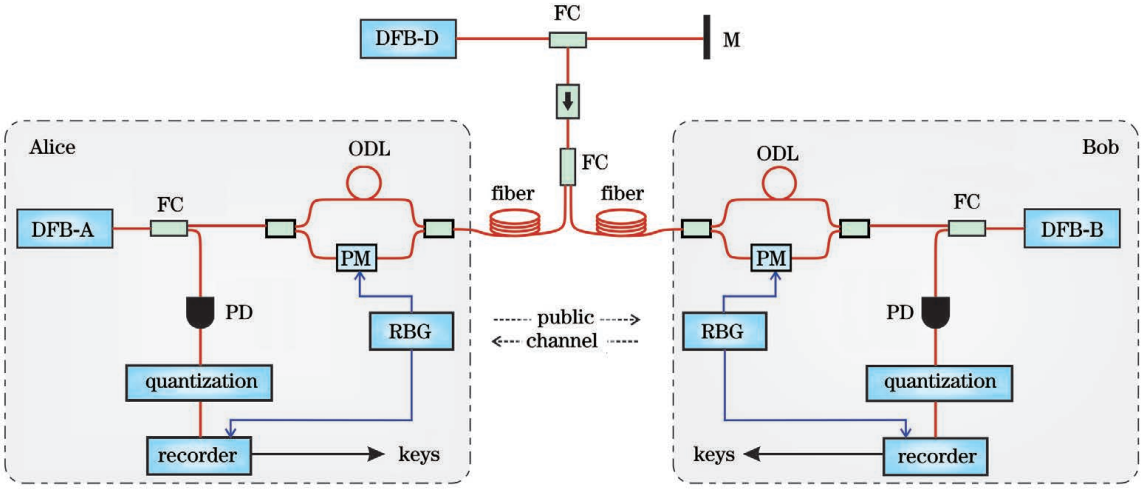

图 1　所提密钥分发方案示意图

Fig. 1　Schematic of proposed key distribution scheme

利用 Lang-Kobayashi 速率方程[20]建立密钥分发系统模型，并由四阶 Runge-Kutta 算法进行求解，即

$$\frac{\mathrm{d}E_{\mathrm{D}}}{\mathrm{d}t}=\frac{1}{2}(1+\mathrm{i}\alpha)\left[\frac{g(N_{\mathrm{D}}-N_{0})}{1+\varepsilon|E_{\mathrm{D}}|^{2}}-\tau_{p}^{-1}\right]E_{\mathrm{D}}+\frac{K_{\mathrm{f}}}{\tau_{\mathrm{in}}}E_{\mathrm{D}}(t-\tau_{\mathrm{f}})+F_{\mathrm{D}},\tag{1}$$

$$\frac{\mathrm{d}E_{\mathrm{A,B}}}{\mathrm{d}t}=\frac{1}{2}(1+\mathrm{i}\alpha)\left[\frac{g(N_{\mathrm{A,B}}-N_{0})}{1+\varepsilon|E_{\mathrm{A,B}}|^{2}}-\tau_{p}^{-1}\right]E_{\mathrm{A,B}}+\frac{K_{\mathrm{j}}}{\tau_{\mathrm{in}}}\frac{\mathrm{i}}{2}E_{\mathrm{D}}(t-\tau_{\mathrm{j},1})\exp(-\mathrm{i}\omega_{\mathrm{D}}\tau_{\mathrm{j},1}+\mathrm{i}\Delta\omega t)+$$
$$\frac{K_{\mathrm{j}}}{\tau_{\mathrm{in}}}\frac{\mathrm{i}}{2}E_{\mathrm{D}}(t-\tau_{\mathrm{j},2})\exp(-\mathrm{i}\omega_{\mathrm{D}}\tau_{\mathrm{j},2}-\mathrm{i}P_{\mathrm{A,B}}\phi_{\mathrm{A,B}}+\mathrm{i}\Delta\omega t)+F_{\mathrm{A,B}},\tag{2}$$

$$\frac{\mathrm{d}N_{\mathrm{D,A,B}}}{\mathrm{d}t}=\frac{I_{\mathrm{D,A,B}}}{qV}-\frac{N_{\mathrm{D,A,B}}}{\tau_{\mathrm{n}}}-\frac{g(N_{\mathrm{D,A,B}}-N_{0})}{1+\varepsilon|E_{\mathrm{D,A,B}}|^{2}}E_{\mathrm{D,A,B}}^{2},\tag{3}$$

式中：E 为电场复振幅；N 为载流子密度；D 代表驱动激光器 DFB-D，A 和 B 分别代表响应激光器 DFB-A 和 DFB-B；K_{f} 表示光反馈强度，其定义为激光器反馈光与输出光的功率比；τ_{f} 表示反馈延迟时间；$\tau_{\mathrm{j},1}$ 和 $\tau_{\mathrm{j},2}$ 分别表示 M-Z 干涉仪两臂的传输延时；$P_{\mathrm{A,B}}\in\{0,1\}$ 表示通信双方的随机键控参数；$\phi_{\mathrm{A,B}}$ 表示相位调制器的键控相位，相位差 $\Delta\phi=|\phi_{\mathrm{A}}-\phi_{\mathrm{B}}|$；$K_{\mathrm{j}}$ 表示光注入强度，其定义为驱动激光器注入光与响应激光器输出光的功率比；$\Delta\omega=\omega_{\mathrm{A,B}}-\omega_{\mathrm{D}}$ 表示驱动激光器与响应激光器的角频率

失谐，其中 $\omega_{A,B,D}$ 表示静态激光器的角频率；$F_{D,A,B}=\sqrt{2\beta N_{D,A,B}}\chi_{D,A,B}$ 表示激光器自发辐射产生的 Langevin 噪声，其中 β 为自发辐射因子，$\chi_{D,A,B}$ 为服从标准正态分布的独立随机变量。(1)式等号右侧第二项表示镜面光反馈电场，第二项表示经过非平衡 M-Z 干涉仪的混沌驱动信号。

激光器的参数设置如下：透明载流子密度 $N_0=1\times10^{-6}\ \mu m^{-3}$，载流子寿命 $\tau_n=2.3$ ns，光子寿命 $\tau_p=1.6$ ps，微分增益系数 $g=6\times10^{-3}\ \mu m^3\cdot ns^{-1}$，线宽增强因子 $\alpha=6$，增益饱和因子 $\varepsilon=1\times10^{-5}\ \mu m^3$，自发辐射因子 $\beta=1.0\times10^{-3}$，激光器腔内往返时间 $\tau_{in}=7.3$ ps，有源区体积 $V=100\ \mu m^3$。角频率 $\omega_D=1.22\times10^{15}$ rad/s，角频率失谐 $\Delta\omega=0$ GHz，阈值电流 $I_{th}=9.8$ mA，偏置电流 $I_D=2.5I_{th}$，$I_{A,B}=1.2I_{th}$，反馈强度 $K_f=0.03$，注入强度 $K_j=0.2$，反馈时延 $\tau_f=3$ ns。M-Z 干涉仪两臂的传输延时分别为：$\tau_{j,1}=1$ ns，$\tau_{j,2}=2$ ns。

3　结果与讨论

3.1　M-Z 干涉仪非线性变换、驱动与响应相关性

首先，分析非平衡 M-Z 干涉仪对混沌驱动信号的非线性变换的影响。图 2 所示为混沌驱动信号经过 M-Z 干涉仪前、后的时序、频谱与互相关曲线，此时 M-Z 干涉仪两臂延时分别为 $\tau_{j,1}=1$ ns，$\tau_{j,2}=2$ ns。通过对比图 2(a)、(c)的时序可以发现，混沌信号经过 M-Z 干涉仪前、后的时域波形存在明显差异，且后者时域振荡明显加快。这主要是因为混沌激光相位动态频谱的低频分量分布比较均匀，延时自干涉会将混沌激光的相位动态转化为强度动态，从而使输出的强度频谱表现出与相位频谱相似的特征，使强度频谱低频抬起，并引入新的高频分量，从而展宽频谱，如图 2(b)、(d)的频谱所示。基于上述延迟自干涉非线性变换，经过 M-Z 干涉仪前、后混沌信号的相关性 C 仅为 0.15，如图 2(e)所示。

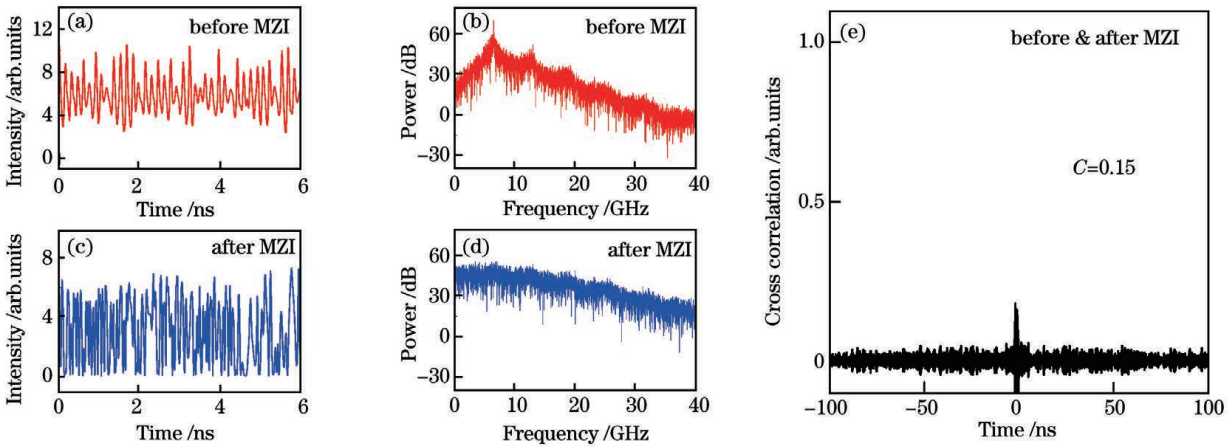

图 2　混沌驱动信号经过 M-Z 干涉仪(MZI)前、后的时序、频谱、互相关曲线。(a)(c)时序；(b)(d)频谱；(e)互相关曲线

Fig. 2　Time series, RF spectra, and cross correlation curve of chaotic driving signal before and after passing through the M-Z interferometer. (a)(c) Time series; (b)(d) RF spectra; (e) cross correlation curve

接下来，分析 M-Z 干涉仪的非线性变换对驱动与响应相关性的影响。图 3(a)中，注入强度 $K_j=0.2$，为了便于比较，将驱动激光器 DFB-D 输出混沌信号的时序和无 M-Z 干涉仪时响应激光器 DFB-A 输出混沌信号的时序进行了垂直平移。从图 3(a)可以定性看出：在无 M-Z 干涉仪的条件下，驱动与响应混沌时序具有较高的相似性；而在有 M-Z 干涉仪的条件下，驱动与响应混沌时序存在明显差异。进一步的定量分析结果如图 3(b)所示：无 M-Z 干涉仪时，驱动与响应混沌时序的互相关系数高达 0.82；有 M-Z 干涉仪时，互相关系数仅为 0.25。上述结果表明，基于 M-Z 干涉仪的非线性变换，DFB-D 与 DFB-A 输出混沌信号之间的相关性得到了有效抑制，避免了窃听者直接通过驱动信号获取同步混沌信号产生相关密钥，提高了密钥分发系统的安全性。

3.2　相移键控混沌同步

通信双方通过键控相位调制器实现相移键控混沌同步：双方相位差 $\Delta\phi=0$ 时，时序如图 4(a)所示，此时 DFB-A 与 DFB-B 的混沌信号高度相似，对应的关联点如图 4(b)所示，互相关系数可达 0.99；当双方相位差 $\Delta\phi=\pi$ 时，时序如图 4(c)所示，此时 DFB-A 与 DFB-B 的混沌信号有明显区别，对应的关联点如图 4(d)所示，互相关系数为 0.12。上述结

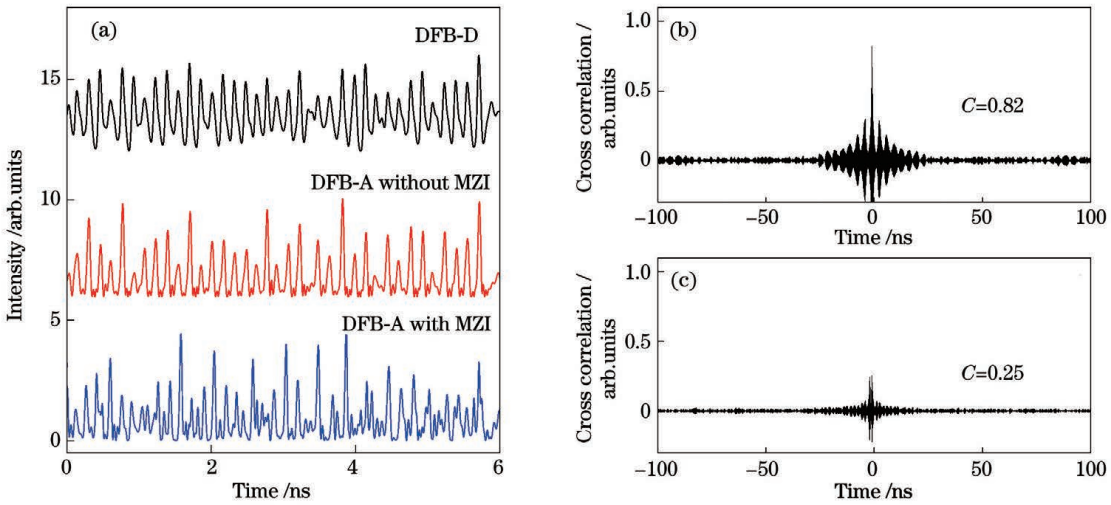

图 3 $K_j=0.2$ 时，有、无 M-Z 干涉仪时的混沌时序及互相关曲线。(a)DFB-D 的混沌时序和有/无 M-Z 干涉仪时 DFB-A 的混沌时序；(b)无 M-Z 干涉仪时 DFB-D 与 DFB-A 混沌时序的互相关曲线；(c)有 M-Z 干涉仪时 DFB-D 与 DFB-A 混沌时序的互相关曲线

Fig. 3 Time series and cross correlation curves with and without M-Z interferometer under $K_j=0.2$. (a) Time series of DFB-D and DFB-A with or without M-Z interferometer; (b) cross correlation curve of chaotic signals from DFB-D and DFB-A without M-Z interferometer; (c) cross correlation curve of chaotic signals from DFB-D and DFB-A with M-Z interferometer

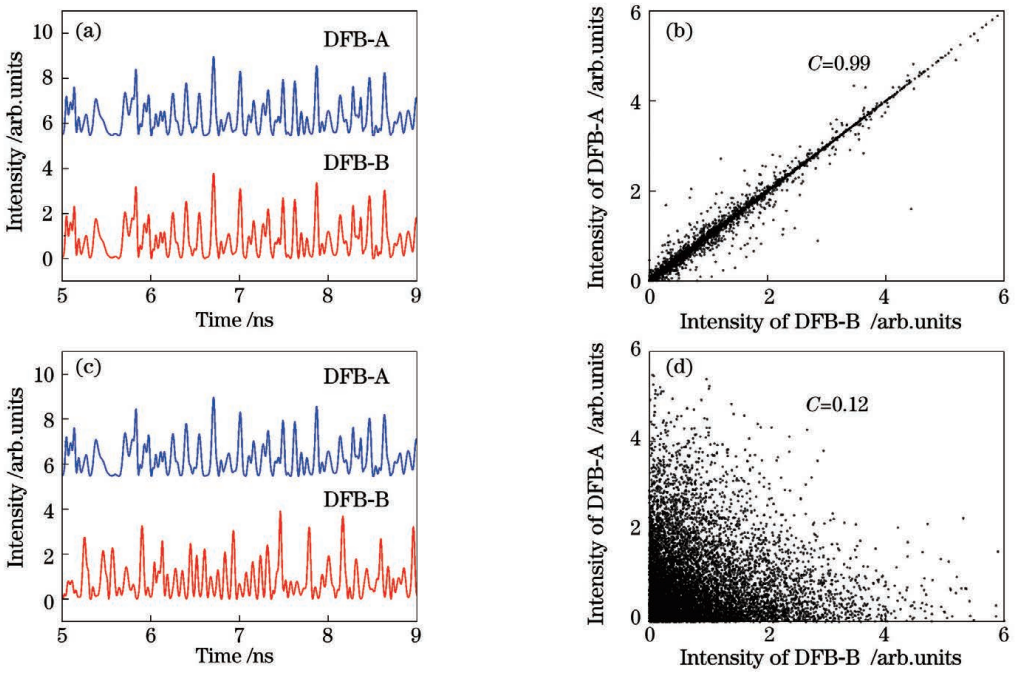

图 4 DFB-A 和 DFB-B 的时序与关联点图。(a)(b)相位差 $\Delta\phi=0$；(c)(d)相位差 $\Delta\phi=\pi$

Fig. 4 Time series and scatter plots of DFB-A and DFB-B. (a)(b) Phase difference $\Delta\phi=0$; (c)(d) phase difference $\Delta\phi=\pi$

果表明：当通信双方的键控相位相同时，DFB-A 与 DFB-B 的混沌信号可以实现高质量混沌同步；当键控相位不同时，DFB-A 与 DFB-B 的混沌信号无法实现同步。

图 5 所示为相移键控码和响应激光器 DFB-A/DFB-B 输出信号之间的短时互相关曲线。键控码的速率为 100 Mbit/s，短时互相关窗口为 2 ns，滑动步进为 0.1 ns。从图 5 可以看出：当通信双方键控相位相同时，可以实现互相关系数达 0.99 的高质量混沌同步；当键控相位不同时，互相关系数减小至

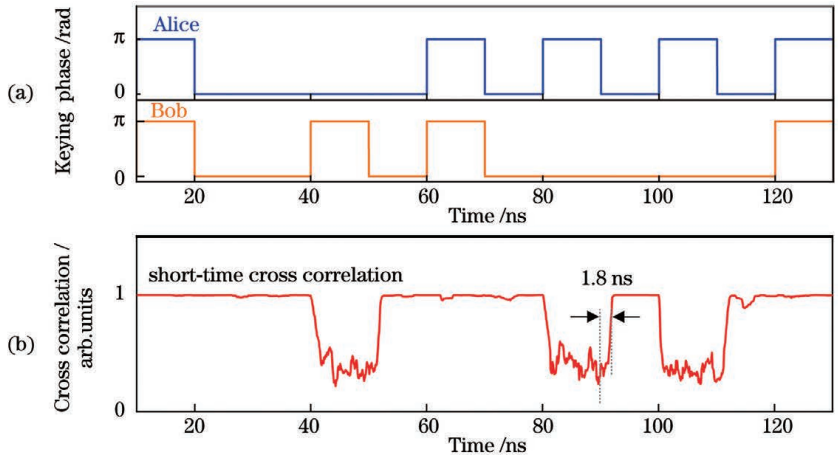

图 5　相移键控码和 DFB-A/DFB-B 输出信号之间的短时互相关曲线。(a)相移键控码;(b)短时互相关曲线

Fig. 5　Phase-shift-keying code and short-time cross correlation curve between DFB-A and DFB-B. (a) Phase-shift-keying code; (b) short-time cross correlation curve

0.3 左右,无法实现同步。图 5 中黑色箭头所示区间为混沌同步恢复时间——键控相位由不同变为相同时,混沌同步系数增至 0.80 时所用的时间[21]。该同步恢复时间为 1.8 ns,明显低于闭环同步系统的同步恢复时间~68 ns[13]。本方案中同步恢复时间降低的原因在于响应激光器采用了开环结构,避免了闭环结构中混沌再同步时反馈外腔的多次振荡[22],使响应激光器在更短的时间内实现混沌再同步。

此外,为了评估缩短混沌同步恢复时间的稳定性,统计了 5000 个同步恢复时间,并绘制出图 6 所示的概率分布图。可以看到,同步恢复时间为 1.8 ns 的数据占比最高,且同步恢复时间在 2.0 ns 以内的数据占比超过 90%,这表明开环结构在缩短混沌同步恢复时间方面具有较高的稳定性。

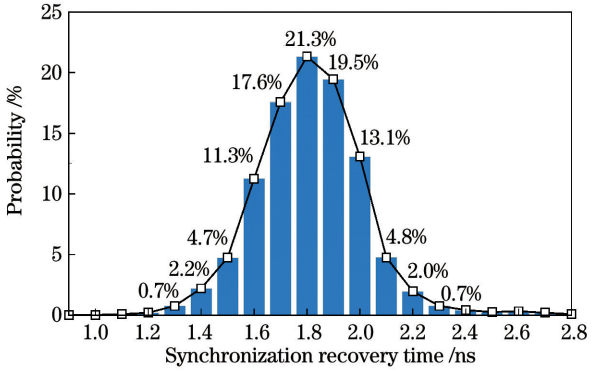

图 6　同步恢复时间的概率统计分布

Fig. 6　Probability distribution of chaos synchronization recovery time

3.3　密钥分发

合法通信方使用双阈值量化[13]方法对混沌信号进行量化,从而产生随机密钥,然后交换键控参数并对比筛选出参数相同(即键控相位相同)时对应的随机密钥作为一致密钥,实现密钥分发。在双阈值量化方案中,设置上、下阈值(V_+ 与 V_-),当采样点的幅值高于 V_+ 和低于 V_- 时,分别量化为 1 和 0;当采样点的幅值处于上、下阈值之间或恰好落于阈值 V_+ 与 V_- 上时,则舍弃该采样点。与传统的单阈值量化相比,双阈值量化可以降低分发密钥的误码率(BER),这是因为量化过程中舍弃了受噪声影响的部分混沌信号。

研究了相位参数失配和响应激光器内部参数失配对混沌同步以及不同保留率下密钥分发误码率的影响,在相同条件下,每个误码率测量 5 次。需要指出的是,保留率 $R=1.0$ 和 $R<1.0$ 分别表示单阈值量化与双阈值量化。图 7(a)表示 DFB-A 与 DFB-B 的混沌同步质量随相位参数失配的变化——固定 Alice 相位并改变 Bob 相位,实现键控失配。从图 7(a)可以看到,随着相位失配的增大,混沌同步质量逐渐降低。随着同步质量的下降,对应的误码率增大,如图 7(b)所示。此外,在固定的相位失配条件下,误码率随着保留率的减小而降低:当 $R=1.0$ 时,误码率高于 3.8×10^{-3},即高于前向纠错(FEC)阈值;减小保留率至 $R=0.5$,误码率可降低至 FEC 阈值以下,对应相位的失配范围为 -0.05π~0.05π;继续减小保留率至 $R=0.2$,误码率低于 FEC 阈值的相位失配范围增大至 -0.10π~0.10π。

图 7(c)~(f)所示为响应激光器内部参数(N_0、τ_p、τ_n、g、α)失配对混沌同步状态及不同保留率生成密钥误码率的影响。固定 DFB-A 的内部参数不变,改变DFB-B的内部参数,实现内部参数失配。

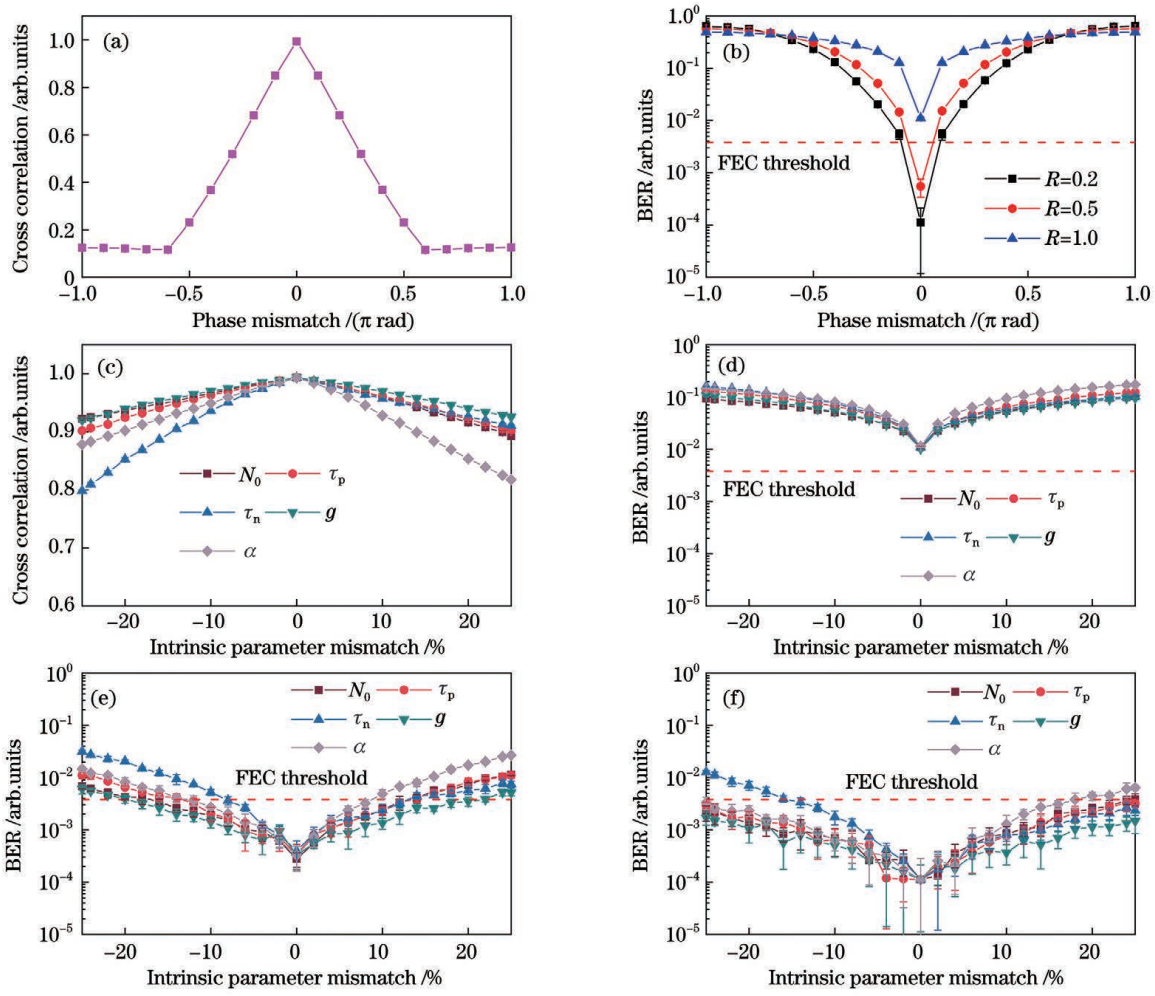

图 7　参数失配对混沌同步与误码率的影响。相位参数失配对(a)混沌同步性和(b)误码率的影响;(c)内部参数失配对混沌同步性的影响;保留率分别为(d)$R=1.0$、(e)$R=0.5$、(f)$R=0.2$ 时,内部参数失配对误码率影响

Fig. 7　Influence of parameter mismatch on chaos synchronization and bit error rate (BER). Influence of phase parameter mismatch on (a) chaotic synchronization and (b) BER; (c) influence of intrinsic parameter mismatch on chaotic synchronization; influence of intrinsic parameter mismatch on BER under (d) $R=1.0$, (e) $R=0.5$, and (f) $R=0.2$

从图 7(c)可以观察到,随着内部参数失配的增大,混沌信号的同步质量逐渐下降。图 7(d)所示为保留率 $R=1.0$ 时,误码率随内部参数失配的变化情况——误码率随着参数失配的增大而增大,即使在零失配的情况下误码率仍为 10^{-2} 量级。这与本课题组之前的实验结果[11]一致,即对混沌同步时序进行单阈值量化得到误码率为 7×10^{-2} 的密钥。图 7(e)所示为保留率 $R=0.5$ 时,内部参数失配在−8%～10%范围内,对应的误码率低于 FEC 阈值。如图 7(f)所示,继续降低保留率至 $R=0.2$,在 FEC 阈值以下的内部参数失配范围继续增大到−14%～18%。上述结果表明,通过合理选择双阈值量化的保留率并控制参数失配范围,可以得到误码率低于 FEC 阈值的密钥分发。需要注意的是,为了保证分发密钥的随机性,每次量化过程中需要调节上下阈值使密钥中 0 和 1 的占比分别为 50%左右。

进一步分析密钥分发的速率,计算公式为

$$v=0.5\times R\times r\times F,\tag{4}$$

式中:R 表示双阈值量化保留率;F 表示在混沌时序中提取密钥的降采样速率;r 表示有效同步时间比例,$r=(\tau_c-\tau_r)/\tau_c$,其中 τ_c 为键控码长,τ_r 为同步恢复时间。有效同步时间比例 $r=(10\ \text{ns}-1.8\ \text{ns})/10\ \text{ns}=0.82$,降采样速率 $F=6.25$ GSa/s——由响应激光器输出混沌信号的相关时间(约 0.16 ns)决定,保留率 $R=0.5$(对应的误码率为 3.8×10^{-3})。通过计算得到,在误码率为 3.8×10^{-3} 的条件下,密钥分发速率 v 为 1.28 Gbit/s。需要注意的是,为了消除混沌信号模拟带宽限制所导致的连续采样点间的相关性,降采样过程是必要的,这进一步保证了分发密钥的随机性。

最后，分析了在有/无 M-Z 干涉仪时，窃听者直接截取混沌驱动信号并在不同保留率下量化产生密钥的误码率，结果如图 8 所示。可以看到：对于无 M-Z 干涉仪的情况，窃听者通过降低双阈值量化保留率可以获得较低误码率的密钥：当保留率降低至约 0.27 时，误码率可降低至 FEC 阈值之下。原因在于驱动与响应之间具有较高的相关性[~0.82；如图 3(b)所示]。此时，窃听者通过混沌驱动信号可以获取与合法用户高度相关的密钥。相比之下，对于有 M-Z 干涉仪的情况，无论保留率如何改变，误码率总是高于无 M-Z 干涉仪的情况，并且误码率均大于 10^{-1}。这是因为 M-Z 干涉仪在混沌驱动信号的非线性变换中降低了驱动与响应之间的相关性[~0.25；如图 3(c)所示]，窃听者即使量化混沌驱动信号，也无法获取高度相关密钥，从而保证了密钥分发的安全性。

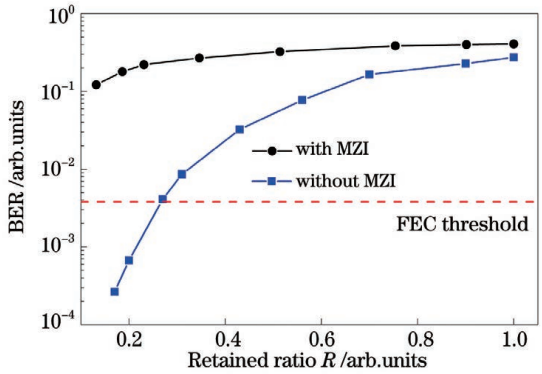

图 8 有、无 M-Z 干涉仪时，窃听者直接量化混沌驱动信号产生密钥的误码率

Fig. 8 BER as a function of retained ratio when eavesdropper intercepts and quantizes the chaotic drive signal from key distribution system with and without M-Z interferometer

4 结 论

提出一种基于对称相移键控混沌同步的高速密钥安全分发方案。利用非平衡 M-Z 干涉仪的延时自干涉对混沌驱动信号进行非线性变换，将驱动信号与响应信号之间的相关性降低至 0.25，避免窃听者直接从混沌驱动信号中获取部分相关密钥，从而提高密钥分发的安全性；利用无外腔反馈的共驱半导体激光器构成开环混沌同步结构，避免了闭环结构中混沌信号在反馈外腔的多次振荡，缩短混沌同步恢复时间至 1.8 ns，从而提高密钥分发速率。数值模拟研究了相移键控混沌同步，混沌同步恢复时间稳定性、相位参数失配和激光器内部参数失配对混沌同步质量与密钥分发误码率的影响，评估了密钥分发的误码率与安全性。最终，在误码率为 3.8×10^{-3} 时，实现了速率为 1.28 Gbit/s 的高速密钥安全分发。

参 考 文 献

[1] Shannon C E. Communication theory of secrecy systems[J]. The Bell System Technical Journal, 1949, 28(4): 656-715.

[2] Pang X L, Yang A L, Zhang C N, et al. Hacking quantum key distribution via injection locking[J]. Physical Review Applied, 2020, 13(3): 034008.

[3] Zhao G H, Zhao S H, Yao Z S, et al. Quantum key distribution analysis for filtering scheme based on double fiber Bragg grating[J]. Chinese Journal of Lasers, 2013, 40(9): 0918001.
赵顾颢, 赵尚弘, 幺周石, 等. 基于双光纤布拉格光栅滤波的量子密钥分发误码率分析[J]. 中国激光, 2013, 40(9): 0918001.

[4] El-Taher A, Kotlicki O, Harper P, et al. Secure key distribution over a 500 km long link using a Raman ultra-long fiber laser[J]. Laser & Photonics Reviews, 2014, 8(3): 436-442.

[5] Zhang L M, Hajomer A A E, Yang X L, et al. Error-free secure key generation and distribution using dynamic Stokes parameters[J]. Optics Express, 2019, 27(20): 29207-29216.

[6] Uchida A, Amano K, Inoue M, et al. Fast physical random bit generation with chaotic semiconductor lasers[J]. Nature Photonics, 2008, 2(12): 728-732.

[7] Yan Q R, Cao Q S, Zhao B S, et al. High speed random number generator based on digitizing bandwidth-enhanced chaotic laser signal[J]. Chinese Journal of Lasers, 2015, 42(11): 1102004.
鄢秋荣, 曹青山, 赵宝升, 等. 基于数字化带宽增强混沌激光信号的高速随机源[J]. 中国激光, 2015, 42(11): 1102004.

[8] Jiang N, Zhao A, Xue C, et al. Physical secure optical communication based on private chaotic spectral phase encryption/decryption[J]. Optics Letters, 2019, 44(7): 1536-1539.

[9] Li Q L, Lu S S, Bao Q, et al. Bidirectional signal transmission based on two coupled chaotic semiconductor lasers[J]. Chinese Journal of Lasers, 2018, 45(5): 0506001.
李齐良, 卢珊珊, 包琪, 等. 基于耦合混沌半导体激光器之间双向信号传输的研究[J]. 中国激光, 2018, 45(5): 0506001.

[10] Li Q, Deng T, Wu Z M, et al. Security-enhanced bidirectional long-distance chaos secure

communication[J]. Chinese Journal of Lasers, 2018, 45(1): 0106001.
李琼, 邓涛, 吴正茂, 等. 安全性增强的双向长距离混沌保密通信[J]. 中国激光, 2018, 45(1): 0106001.
[11] Wang L S, Wang D M, Gao H, et al. Real-time 2.5-Gb/s correlated random bit generation using synchronized chaos induced by a common laser with dispersive feedback[J]. IEEE Journal of Quantum Electronics, 2020, 56(1): 1-8.
[12] Yoshimura K, Muramatsu J, Davis P, et al. Secure key distribution using correlated randomness in lasers driven by common random light[J]. Physical Review Letters, 2012, 108(7): 070602.
[13] Sasaki T, Kakesu I, Mitsui Y, et al. Common-signal-induced synchronization in photonic integrated circuits and its application to secure key distribution [J]. Optics Express, 2017, 25(21): 26029-26044.
[14] Xue C P, Jiang N, Qiu K, et al. Key distribution based on synchronization in bandwidth-enhanced random bit generators with dynamic post-processing [J]. Optics Express, 2015, 23(11): 14510-14519.
[15] Jiang N, Zhao X Y, Zhao A K, et al. High-rate secure key distribution based on private chaos synchronization and alternating step algorithms[J]. International Journal of Bifurcation and Chaos, 2020, 30(2): 2050027.
[16] Jiang N, Xue C P, Liu D, et al. Secure key distribution based on chaos synchronization of VCSELs subject to symmetric random-polarization optical injection[J]. Optics Letters, 2017, 42(6): 1055-1058.
[17] Zhang H, Guo X X, Xiang S Y. Key distribution based on unidirectional injection of vertical cavity surface emitting laser system[J]. Acta Physica Sinica, 2018, 67(20): 204202.
张浩, 郭星星, 项水英. 基于单向注入垂直腔面发射激光器系统的密钥分发[J]. 物理学报, 2018, 67(20): 204202.
[18] Zhao Z X, Cheng M F, Luo C, et al. Semiconductor-laser-based hybrid chaos source and its application in secure key distribution[J]. Optics Letters, 2019, 44(10): 2605-2608.
[19] Liu W, Yin Z Z, Chen X M, et al. A secret key distribution technique based on semiconductor superlattice chaos devices[J]. Science Bulletin, 2018, 63(16): 1034-1036.
[20] Lang R, Kobayashi K. External optical feedback effects on semiconductor injection laser properties [J]. IEEE Journal of Quantum Electronics, 1980, 16(3): 347-355.
[21] Wang L S, Chao M, Wang A B, et al. High-speed physical key distribution based on dispersion-shift-keying chaos synchronization in commonly driven semiconductor lasers without external feedback[J]. Optics Express, 2020, 28(25): 37919-37935.
[22] Vicente R, Perez T, Mirasso C R. Open-versus closed-loop performance of synchronized chaotic external-cavity semiconductor lasers[J]. IEEE Journal of Quantum Electronics, 2002, 38(9): 1197-1204.

High-Speed Secure Key Distribution Based on Symmetric Phase-Shift-Keying Chaos Synchronization

Wu Chaoren[1,2], Gao Hua[1,2], Wang Longsheng[1,2*], Guo Yuanyuan[1,2], Wang Anbang[1,2], Wang Yuncai[1,2]

[1] *Key Laboratory of Advanced Transducers & Intelligent Control System, Ministry of Education, Taiyuan University of Technology, Taiyuan, Shanxi* 030024, *China*;
[2] *College of Physics and Optoelectronics, Taiyuan University of Technology, Taiyuan, Shanxi* 030024, *China*

Abstract

Objective The core of information security is secure communication. Shannon's secret communication scheme, "one-time-pad," requires that the key be discarded after use, the key length is larger than the information length, and the key generation cannot be predicted. The key distribution is mainly based on a mathematical algorithm. The security of the algorithm key depends on a computer's computing power. Using brute force still threatens the security of this scheme. Physical-layer key distribution has high security, such as quantum key distribution, key distribution based on fiber laser, and key distribution based on channel noise. However, limited by the key distribution mechanism or the bandwidth of the physical entropy source, the key distribution rate of the above

physical layer is only bit/s–kbit/s, which is difficult to meet the requirements of a high-speed communication rate.

A wideband chaotic laser can be produced by a semiconductor laser under an external disturbance. The time-domain waveform of a chaotic laser has the characteristics of large amplitude random fluctuations, which can generate high-speed physical random numbers from Gbit/s to Tbit/s. In addition, the parameter-matched laser can realize chaotic synchronization, and the high-speed correlated physical key can be generated by quantizing the chaotic synchronization waveform. Therefore, using a chaotic laser as a physical entropy source and combining it with chaotic synchronization is expected to achieve high-speed physical key distribution. Uchida et al. proposed a key distribution scheme based on optical feedback laser phase shift keying chaos synchronization and achieved a key distribution rate of approximately 180 kbit/s. Notably, the optical feedback laser constitutes a closed-loop structure. The random phase-shift-keying of the feedback optical path results in a long oscillation time for the laser to achieve chaos synchronization again, which results in a synchronization recovery time of tens of nanoseconds. Longer synchronization recovery time will limit the further improvement of the key distribution rate. To improve the key distribution rate, other methods have been proposed. For example, Jiang et al. proposed a key distribution scheme based on dynamic unpredictable post-processing, alternating step algorithm post-processing, and dynamic random polarization synchronization of vertical-cavity surface-emitting lasers. Xiang et al. proposed a key distribution scheme based on bandwidth enhanced chaotic synchronization. Notably, the above schemes use a chaotic laser to drive response laser to construct chaotic synchronization, but there is a residual correlation between the drive and response signals. Based on the correlation, an eavesdropper can directly obtain part of the relevant key through the drive signal, which causes the potential security threat of key distribution.

Methods In this study, a scheme of high-speed secure key distribution based on symmetric-phase-shift-keying chaos synchronization is proposed and numerically demonstrated. The chaotic drive signal was injected symmetrically into the response lasers without external feedback through two unbalanced Mach-Zehnder (M-Z) interferometers. Phase-shift-keying chaos synchronization was realized by randomly modulating phase modulators in the M-Z interferometers. The chaotic temporal waveforms with phase-shift-keying synchronization were quantized into random bits, which were stored in the recorders together with the corresponding keying parameters. After exchanging and comparing the keying parameters, legitimate users retained random bits generated from synchronized chaos as shared keys to realize the key distribution.

Results and Discussions In the proposed scheme, the unbalanced M-Z interferometer introduced a nonlinear transformation of delayed self-interference to the chaotic drive signal, which decreased the cross-correlation of drive and response signals to 0.25 (Fig. 3) and thus improved the security of key distribution. Moreover, the commonly driven response lasers without external feedback constituted an open-loop synchronization structure, which reduced the synchronization recovery time of dynamic phase-shift-keying chaos synchronization to 1.8 ns (Fig. 5) and thus improved the key distribution rate. We calculated the synchronization recovery time 5000 times and plotted the probability distribution, which showed that the open-loop synchronization structure had high stability in shortening the synchronization recovery time (Fig. 6). Then, we studied the mismatch effects of phase and intrinsic laser parameters on the chaos synchronization and bit error rate (BER) (Fig. 7) and evaluated the key distribution rate and security. In addition, we analyzed the BER of the key obtained by an eavesdropper intercepting the chaotic driving signal directly with or without an M-Z interferometer (Fig. 8).

Conclusions In this study, we propose a high-speed secure key distribution scheme based on symmetric-phase-shift-keying chaotic synchronization. Using the delayed self-interference of an unbalanced M-Z interferometer, the correlation between the drive and response signals is reduced to 0.25. The eavesdropper cannot directly obtain part of the relevant key from the chaotic drive signal to improve the key distribution security. An open-loop chaotic synchronization structure is constructed by a commonly driven semiconductor laser without external cavity feedback, which avoid multiple oscillations of chaotic signals in the feedback external cavity in the closed-loop structure, shorten the recovery time of chaotic synchronization to 1.8 ns, and improve the key distribution rate. Finally, when the BER is 3.8×10^{-3}, a high-speed secure key distribution at a rate of 1.28 Gbit/s is realized.

Key words optical communication; semiconductor lasers; chaotic laser; chaos synchronization; key distribution; secure communication