物理学报 Acta Physica Sinica
Chinese Physical Society
Institute of Physics, CAS

# 基于单向注入垂直腔面发射激光器系统的密钥分发

张浩　郭星星　项水英

# Key distribution based on unidirectional injection of vertical cavity surface emitting laser system

Zhang Hao　Guo Xing-Xing　Xiang Shui-Ying

引用信息 Citation: Acta Physica Sinica, **67**, 204202 (2018)　DOI: 10.7498/aps.67.20181038
在线阅读 View online: http://dx.doi.org/10.7498/aps.67.20181038
当期内容 View table of contents: http://wulixb.iphy.ac.cn/CN/Y2018/V67/I20

---

# 基于单向注入垂直腔面发射激光器系统的密钥分发*

张浩 郭星星 项水英†

(西安电子科技大学通信工程学院, 综合业务网国家重点实验室, 西安 710071)

( 2018 年 5 月 28 日收到; 2018 年 6 月 23 日收到修改稿 )

随机源对于信息理论安全的密钥分发至关重要, 本文提出了一种基于单向注入垂直腔面发射激光器系统的密钥分发方案. 首先基于单向注入的方式产生无时延特征的激光混沌信号, 并通过单向注入驱动两个从激光器产生带宽增强的混沌同步信号. 然后经过采样、量化以及异或等后处理, 生成密钥流. 数值仿真结果表明, 在单阈值情况下, 合法用户之间的误比特率低至1% 左右, 合法用户与窃听者之间的误比特率都高于10%; 在双阈值情况下, 误比特率可以低至$10^{-6}$. 最后, 对生成的密钥流进行了 NIST 随机性测试. 该方案有效地增强了密钥分发的安全性.

**关键词**: 垂直腔面发射激光器, 密钥分发, 保密通信, 混沌同步

**PACS:** 42.55.Px, 82.40.Bj, 05.45.–a **DOI:** 10.7498/aps.67.20181038

## 1 引 言

如今, 信息安全的重要性不言而喻, 为了保障信息在传输过程中的安全, 通信双方在发送信息前必须用密钥对信息加密, 在接收信息后也要用密钥解密. 因此, 如何保障密钥分发的安全性是非常关键的. 安全密钥分发大致可以分为两类, 一类是基于算法的安全密钥分发, 著名的Diffie-Hellman密钥分发[1]就是基于窃听者有限计算能力假设下的数学难题方案; 另一类是基于物理信息理论的安全密钥分发, 以量子密钥分发[2]和基于随机源的密钥分发为主. 激光混沌因其良好的随机特性[3−5], 可以作为物理随机源, 基于激光混沌随机源的密钥分发方案中[6−9], 双方用户通过对公共信道上的同一随机信号进行观测记录, 协商出公共密钥. 2012年, Yoshimura等[6]使用一个激光器驱动两个激光器达到混沌同步, 经过双方随机相位调制导致混沌同步系数发生变化, 根据同步系数来确定密钥, 同时指出该方案还可以级联. 2013年, Koizumi等[7]实验研究了在共同注入情况下的密钥分发方案, 采用级联的同步响应激光器, 可以有效抵御窃听者的攻击, 该方案可以在距离120 km和相位调制频率2 MHz的情况下, 达到64 kb/s的密钥产生速率. 2015年, 太原理工大学Wang等[8]提出在互耦合激光器系统中采用信息协商的密钥分发方案, 协商方式是通过奇偶校验的方式定位错误比特在矩阵中的位置, 然后删除错误比特. 2017年, 电子科技大学Jiang等[9]提出基于随机偏振光注入的密钥分发方案, 其中驱动激光器通过时延反馈产生激光混沌, 并驱动另外两个激光器实现混沌同步, 然后通过可调偏振旋转器控制垂直腔面发射激光器(VCSELs)的偏振角, 根据两个VCSELs的同步系数确定密钥, 该方案产生的密钥安全性较高.

随机源对于信息安全的密钥分发至关重要, 一些学者采用半导体激光器系统产生的混沌信号作为随机源, 但是, 这些随机源大都存在时延特征, 并且带宽较小. 时延特征通常由激光器的反馈回路导致, 将降低激光混沌载波的复杂度, 使得攻击者可

* 国家自然科学基金 (批准号: 61674119) 和国家自然科学基金青年科学基金 (批准号: 61306061) 资助的课题.

† 通信作者. E-mail: jxxsy@126.com

 

能利用时延特征处的弱周期性窃取信息, 对信息安全的威胁较大[10,11]. 本文提出一种基于单向注入VCSELs混沌同步系统的密钥分发方案, 通过建立不带反馈的混沌同步模型, 利用单向注入的方式产生混沌信号, 驱动两个激光器产生带宽增强的混沌同步信号, 然后经过采样、量化以及异或等后处理, 生成密钥流.

本文内容安排如下: 首先介绍基于激光混沌的密钥分发系统模型和速率方程; 其次研究单向注入方式产生激光混沌信号, 并分析激光混沌信号的时延特征和带宽; 接着研究两个激光器 (合法用户) 之间的同步特性; 然后分别研究合法用户之间以及非法用户与合法用户之间的密钥误比特率; 最后研究激光器参数失配带来的影响和密钥随机性.

## 2 基于VCSELs的密钥分发系统模型

### 2.1 理论模型

基于单向注入VCSELs混沌同步系统的密钥分发方案如图1所示. I-VCSEL的输出光单向注入到D-VCSEL并使其实现无时延特征的混沌输出, D-VCSEL的混沌输出光再经过光耦合器 (OC) 一分为二, 分别注入到VCSELA和VCSELB中实现混沌同步[12,13], 对VCSELA和VCSELB产生的混沌载波进行后处理产生密钥keyA和keyB. 光纤信道上的光隔离器 (OI) 是为了保证光的单向传输, 可调光衰减器 (VA) 的作用是调节注入到激光器中的光强度, 偏振分束器 (PBS) 的作用是线性偏振分解VCSEL的输出光到$x$偏振模式 (XP) 和$y$偏振模式 (YP), 光电探测器 (PD和IPD) 的作用是将光信号变为电信号, 模数转换器 (ADC) 是将模拟信号转变成数字信号, XOR是将产生的比特进行移位异或处理, 虚线框中是假想的窃听者Eve对密钥安全性的攻击, Eve可以从光纤中分流一路来自随机源 (D-VCSEL) 的输出, 能够对D-VCSEL的混沌输出序列进行分析.

根据VCSEL激光器的自旋反转模型, I-VCSEL, D-VCSEL, VCSELA和VCSELB的速率方程描述如下[14−16]:

$$\frac{\mathrm{d}E^{\mathrm{I}}_{x,y}}{\mathrm{d}t}=\kappa(1+\mathrm{i}\alpha)(N^{\mathrm{I}}E^{\mathrm{I}}_{x,y}-E^{\mathrm{I}}_{x,y}\pm\mathrm{i}n^{\mathrm{I}}E^{\mathrm{I}}_{y,x})\mp(\gamma_{\mathrm{a}}+\mathrm{i}\gamma_{\mathrm{p}})E^{\mathrm{I}}_{x,y}+F^{\mathrm{I}}_{x,y}, \tag{1}$$

$$\begin{aligned}\frac{\mathrm{d}E^{\mathrm{D}}_{x,y}}{\mathrm{d}t}=&\kappa(1+\mathrm{i}\alpha)(N^{\mathrm{D}}E^{\mathrm{D}}_{x,y}-E^{\mathrm{D}}_{x,y}\pm\mathrm{i}n^{\mathrm{D}}E^{\mathrm{D}}_{y,x})\mp(\gamma_{\mathrm{a}}+\mathrm{i}\gamma_{\mathrm{p}})E^{\mathrm{D}}_{x,y}\\&+k_1E^{\mathrm{I}}_{x,y}(t-\tau_1)\exp(-\mathrm{i}2\pi(f_1\tau_1-\Delta f_1t))+F^{\mathrm{D}}_{x,y},\end{aligned} \tag{2}$$

$$\begin{aligned}\frac{\mathrm{d}E^{\mathrm{A,B}}_{x,y}}{\mathrm{d}t}=&\kappa(1+\mathrm{i}\alpha)(N^{\mathrm{A,B}}E^{\mathrm{A,B}}_{x,y}-E^{\mathrm{A,B}}_{x,y}\pm\mathrm{i}n^{\mathrm{A,B}}E^{\mathrm{A,B}}_{y,x})\mp(\gamma_{\mathrm{a}}+\mathrm{i}\gamma_{\mathrm{p}})E^{\mathrm{A,B}}_{x,y}\\&+k_2E^{\mathrm{D}}_{x,y}(t-\tau_2)\exp(-\mathrm{i}2\pi(f_{\mathrm{D}}\tau_2-\Delta f_2t))+F^{\mathrm{A,B}}_{x,y},\end{aligned} \tag{3}$$

$$\frac{\mathrm{d}N^{\mathrm{I,D,A,B}}}{\mathrm{d}t}=\gamma_N[\mu-N(1+|E^{\mathrm{I,D,A,B}}_x|^2+|E^{\mathrm{I,D,A,B}}_y|^2)+\mathrm{i}n(E^{\mathrm{I,D,A,B}}_xE^{\mathrm{I,D,A,B}^*}_y-E^{\mathrm{I,D,A,B}}_yE^{\mathrm{I,D,A,B}^*}_x)], \tag{4}$$

$$\frac{\mathrm{d}n^{\mathrm{I,D,A,B}}}{\mathrm{d}t}=-\gamma_{\mathrm{s}}n-\gamma_n[n(|E^{\mathrm{I,D,A,B}}_x|^2+|E^{\mathrm{I,D,A,B}}_y|^2)+\mathrm{i}N(E^{\mathrm{I,D,A,B}}_yE^{\mathrm{I,D,A,B}^*}_x-E^{\mathrm{I,D,A,B}}_xE^{\mathrm{I,D,A,B}^*}_y)], \tag{5}$$

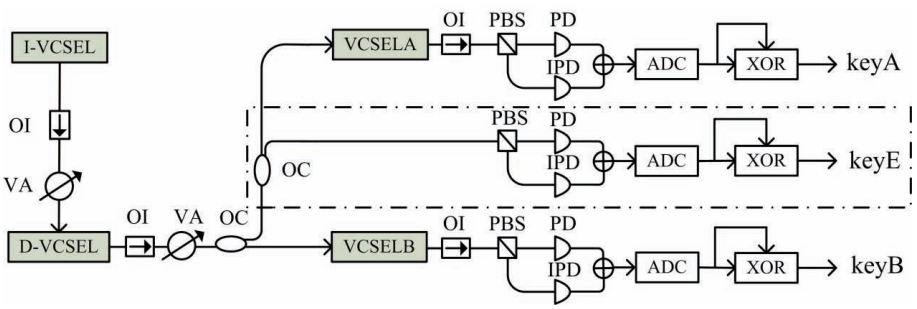


图1 密钥分发系统结构示意图

Fig. 1. System structure diagram of key distribution.

其中I, D, A和B分别代表四个激光器(I-VCSEL, D-VCSEL, VCSELA和VCSELB), $E_x$和$E_y$是XP和YP的慢变复电场, $N$是总载流子数目, $n$是左旋和右旋载流子数目的差值, $\alpha$表示线宽增强因子, $\kappa$表示场衰减速率, $\gamma_N$表示$N$的衰减速率, $\gamma_s$表示自旋反转速率, $\gamma_a$表示线性二色性, $\gamma_p$表示线性双折射性, $\mu$表示归一化电流($\mu=1$表示阈值电流), $\lambda$表示波长; $k_1$表示I-VCSEL注入到D-VCSEL的耦合强度, $k_2$表示D-VCSEL注入到VCSELA或VCSELB的耦合强度; $\Delta f_1 = f_I - f_D$表示I-VCSEL与D-VCSEL之间的频率失谐, $\Delta f_2 = f_D - f_{A,B}$表示D-VCSEL与VCSELA, VCSELB之间的频率失谐; $\tau_1$和$\tau_2$分别是I-VCSEL到D-VCSEL的注入时延和D-VCSEL到VCSELA, VCSELB的注入时延, 由于注入时延对系统输出动态没有什么影响, 因此可以忽略, 即$\tau_1=\tau_2=0$; $F_{x,y}$表示郎之万噪声[9], 定义为$F_x = \sqrt{\beta_{sp}/2}(\sqrt{N+n}\xi_1 + \sqrt{N-n}\xi_2)$, $F_y = -i\sqrt{\beta_{sp}/2}(\sqrt{N+n}\xi_1 - \sqrt{N-n}\xi_2)$, 其中$\xi_1$和$\xi_2$是均值为0, 方差为1的独立高斯白噪声; $\beta_{sp}$是自发辐射噪声的速率. 耦合强度$k_1$和$k_2$的范围是$0 < k_1, k_2 \leqslant 50\ \text{ns}^{-1}$, 频率失谐$\Delta f_1$和$\Delta f_2$的范围是$-20\ \text{GHz} \leqslant \Delta f_1, \Delta f_2 \leqslant 20\ \text{GHz}$. 上述速率方程是在matlab平台上采用四阶龙格库塔算法求解, 步长为1 ps, 其他的参数取值[9,14,15]为$\alpha=3$, $\kappa=300\ \text{ns}^{-1}$, $\gamma_N=1\ \text{ns}^{-1}$, $\gamma_s=50\ \text{ns}^{-1}$, $\gamma_a=0.1\ \text{ns}^{-1}$, $\gamma_p=10\ \text{ns}^{-1}$, $\mu=2.7$, $\lambda=850\ \text{nm}$, $\beta_{sp}=10^{-6}$.

## 3 结果与讨论

### 3.1 单向注入产生混沌信号

首先, 用分岔图的方式观察系统输出从周期态到混沌状态的演化过程. 设定工作电流为$\mu=2.7$, 此时XP和YP共存且强度接近. 图2是D-VCSEL的输出强度随耦合强度$k_1$和频率失谐$\Delta f_1$变化的分岔图. 当图2(a)的参数$\Delta f_1=0$, 可以看出D-VCSEL的输出是从周期状态到混沌状态, 最后回

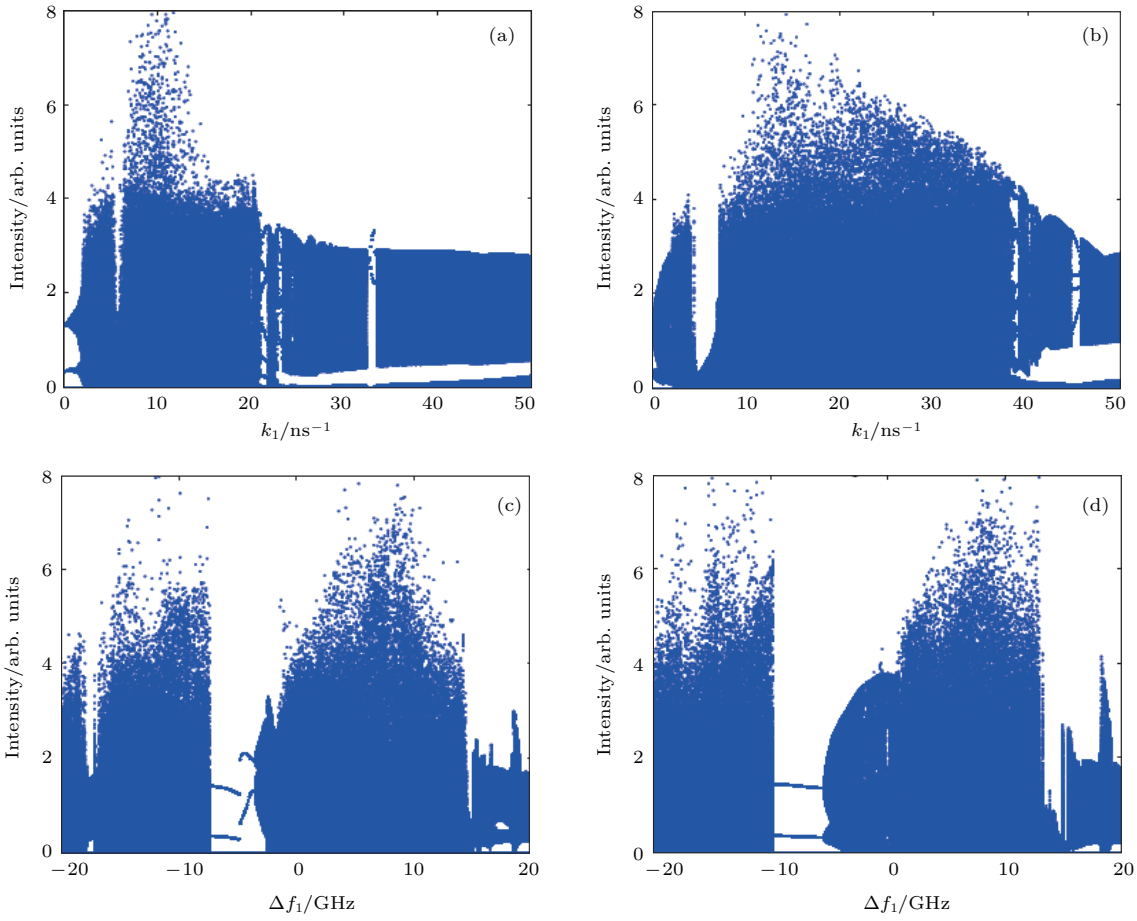


图2 D-VCSEL的输出强度随耦合强度$k_1$和频率失谐$\Delta f_1$变化的分岔图

Fig. 2. Bifurcation diagram of the output intensity of D-VCSEL as fuction of $k_1$ and $\Delta f_1$.

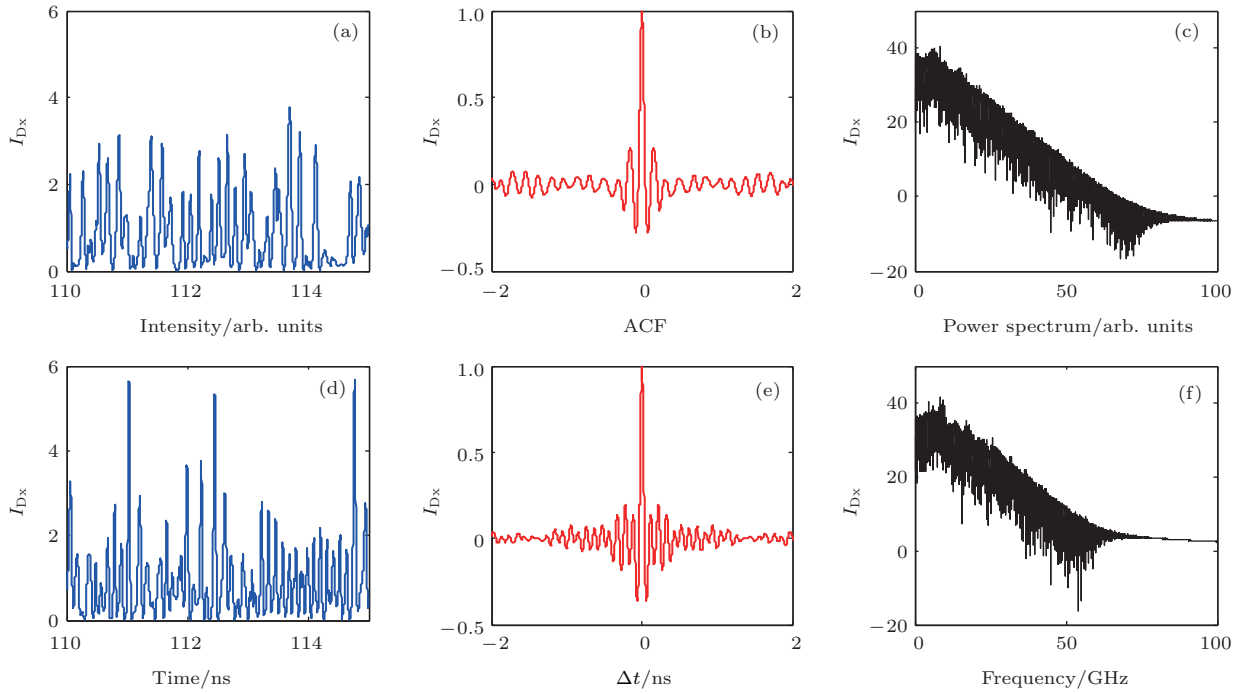


图 3 D-VCSEL 的 XP (a), (d) 输出时序; (b), (e) 自相关曲线; (c), (f) 功率谱

Fig. 3. (a), (d) Time series, (b), (e) autocorrelation function, (c), (f) power spectra, for the XP of the D-VCSEL.

到多周期状态. 当图 2 (b) 的参数 $\Delta f_1 = 5$ GHz, 可以看出当耦合强度 $0 < k_1 < 5$ ns$^{-1}$ 时, D-VCSEL 输出动态由周期态变化到准周期状态, 当耦合强度 5 ns$^{-1}$ $< k_1 <$ 38 ns$^{-1}$ 时, D-VCSEL 的输出动态从周期态变化到混沌状态, 处于混沌状态的耦合强度范围非常宽. 为了进一步说明混沌参数条件, 图 2 (c) 和图 2 (d) 的参数取值分别为 $k_1 = 15$ ns$^{-1}$, $k_1 = 20$ ns$^{-1}$, 可以看出 $\Delta f_1$ 处于正频率失谐时 ($0 \leqslant \Delta f_1 \leqslant 10$ GHz), D-VCSEL 的输出容易处于混沌区域.

通过对图 2 的分岔图分析, 本节选择频率失谐 $\Delta f_1 = 5$ GHz. 图 3 是在频率失 $\Delta f_1 = 5$ GHz 时, 在 $k_1 = 15$ ns$^{-1}$ (第一行) 和 $k_1 = 25$ ns$^{-1}$ (第二行) 两个不同耦合强度下 D-VCSEL 的时间序列、自相关和功率谱曲线. 在这两种情况下, 从时间序列上看都处于混沌状态, 自相关曲线中的次峰值很小, 功率谱曲线相当平滑.

通过图 1—图 3 的分析, 本文选择 $\mu = 2.7$, $\Delta f_1 = 5$ GHz 和 $k_1 = 15$ ns$^{-1}$ 作为产生混沌的工作参数, 接下来的内容中都使用这组参数.

## 3.2 同步特性研究

在 D-VCSEL 混沌光的驱动下, VCSELA 和 VCSELB 之间能够达到混沌同步, 本节研究这三个 VCSELs 之间的同步特性. 一方面, 因为 VCSEL 激光器两个线性偏振模式之间存在反相位相关现象 [17], 所以, 如果使用 XP 产生密钥, 那么 YP 在一定程度上会暴露 XP; 另一方面, 虽然本方案没有引入回路时延, 但是激光器自身的弛豫振荡周期仍然会对密钥随机性造成一定的影响, 因此本方案对两个偏振模式做差. 借鉴文献 [9] 的做法, 取 $I_i = I_{iy} - I_{ix}$, 其中 $i = \mathrm{D}, \mathrm{A}, \mathrm{B}$. 使用互相关函数来分析两路混沌信号之间的同步特性, 公式如下 [17]:

$$C_{p,q}(\Delta t) = \frac{\langle [I_p(t-\Delta t) - \langle I_p(t-\Delta t)\rangle][I_q(t) - \langle I_q(t)\rangle]\rangle}{\sqrt{\langle [I_p(t-\Delta t) - \langle I_p(t-\Delta t)\rangle]^2\rangle \langle [I_q(t) - \langle I_q(t)\rangle]^2\rangle}}, \tag{6}$$

式中 $p, q = \mathrm{D}, \mathrm{A}, \mathrm{B}$ $(p \neq q)$, $\langle\ \rangle$ 表示时间平均, $C = 1$ 表示两路混沌信号完全同步.

图 4 (a) 和图 4 (b) 分别给出了 D-VCSEL 与 VCSELA, VCSELA 与 VCSELB 在参数空间 $\Delta f_2$ 和 $k_2$ 上的同步系数演化图. 从图中可以看出, 当频率失谐 $\Delta f_2 < 0$ 时, VCSELs 之间的同步系数更高一些, 在相同的频率失谐条件下, 耦合强度 $k_2$ 越大, 同步系数越高, 最终会达到注入锁定的状态. 为了尽可能降低 VCSELA 和 VCSELB 之间的密钥误比特率, 本方案中的 VCSELA 与 VCSELB 之间的同步系数要足够高, 同时, 为了防止 Eve 对光纤链路

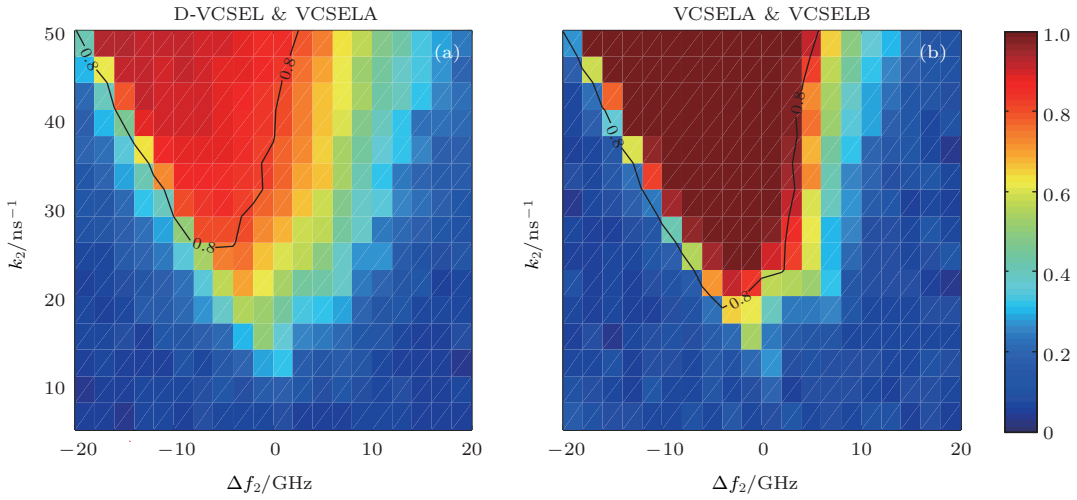


图 4 同步系数二维演化图

Fig. 4. 2D evolution of synchronization coefficient.

的窃听, D-VCSEL 与 VCSELA(VCSELB) 之间的同步系数要尽可能低. 在这两个条件的权衡下, 可以选择 $\Delta f_2 = 0$ GHz, $k_2 = 35$ ns$^{-1}$, VCSELA 与 VCSELB 之间的同步系数高达 0.99, 而 D-VCSEL 与 VCSELA 之间的同步系数只有 0.74. 在这个参数条件下, D-VCSEL 输出 $I_{\rm D}$ 的带宽 $B_{\rm D} = 13.97$ GHz [18], 略高于 XP 输出的带宽 ($B_{\rm Dx} = 12.94$ GHz), VCSELA 的输出 $I_{\rm A}$ 带宽 $B_{\rm A} = 17.02$ GHz. 从这个结果可以看出光注入方式拓展了带宽, 有利于从混沌信号中提取随机比特.

### 3.3 可调参数对密钥误比特率的影响

通过上一节的研究, 我们发现由于激光器工作参数条件和自发辐射噪声的影响, VCSELA 和 VCSELB 之间的同步不是完美的. VCSELA 和 VCSELB 作为两个合法用户的激光器, 在经过采样、量化处理之后生成的密钥流难免存在一定的误比特率, 本文中采用的密钥序列长度为 $2 \times 10^6$. 因此, 有必要研究 VCSELA 和 VCSELB 之间的误比特率. 误比特率是传输错误的比特个数占总比特个数的比例. 在本方案中, 需要为两个合法用户生成相同的密钥, 在此使用一位 ADC 的量化方案 [19].

目前, 主要有单阈值和双阈值量化方法 [20,21], 为了研究可调参数对密钥误比特率的影响, 首先对单阈值方法进行采样、量化处理的过程进行分析. 在这里假定采样频率为 4 GHz, 通过对采样值进行计算分析, 确定一个阈值强度 $T$, 如果采样点的输出强度大于 $T$, 密钥取值为“1”, 否则取值为“0”, 单阈值方式下密钥的产生速率为 4 Gbit/s.

为了方便比较合法用户与非法用户之间的误比特率, 图 5 (a) 和图 5 (b) 分别给出了 D-VCSEL 与 VCSELA, VCSELA 与 VCSELB 的误比特率曲线图. 从图 5 (a) 中可以看出 D-VCSEL 与 VCSELA 之间的误比特率都高于 10.0%, 从图 5 (b) 中可以观察到 VCSELA 与 VCSELB 在适当的负频率失谐 ($-10$ GHz $< \Delta f_2 < 0$ GHz) 条件下, 随着耦合强度 $k_2$ 逐渐增大, 误比特率逐渐降低, 误比特率可低至 0.33%. 在频率偏移 $\Delta f_2 = 0$ GHz, 耦合强度 $k_2 = 35$ ns$^{-1}$ 的参数条件下, 非法用户 Eve (D-VCSEL) 与合法用户 Alice (VCSELA) 之间的误比特率 BER = 16.64%, 合法用户 (VCSELA 和 VCSELB) 之间的误比特率 BER = 1.67%.

由此可见, 虽然单阈值量化方法实际应用简单, 但是产生的密钥误比特率相对比较高. 为了降低误比特率, 本文进一步采用双阈值量化方法 [20,21], 用 $r$ 表示保留率, 密钥分发速率为 $r \times 4$ Gbit/s.

为了更清晰地分辨误比特率的大小, 对误比特率结果取对数. 图 6 给出了三种不同保留率 ($r = 0.5, 0.7, 0.9$) 情况下误比特率的变化曲线, 图 6 (a) 中耦合强度 $k_2 = 30$ ns$^{-1}$, 图 6 (b) 中 $k_2 = 35$ ns$^{-1}$. 双阈值量化方法与图 5 (b) 中单阈值量化方法的曲线走势基本一致, 同时可以看出双阈值量化中保留率 $r$ 越低, 误比特率越低. 其他条件保持一致, 频率失谐在 $-8$ GHz $\leqslant \Delta f_2 \leqslant 0$ GHz 范围内, 与图 5 (b) 比较, 图 6 (a) 中双阈值量化在保留率 $r = 0.7$ 时的误比特率最高, 只达到单阈值结果的 1/10. 从图 6 (a) 与图 6 (b) 的结果对比得到, 在

频率失谐 $\Delta f_2$ 和保留率 $r$ 相同的情况下, 耦合强度 $k_2 = 35\ \mathrm{ns}^{-1}$ 时的误比特率降低为 $k_2 = 30\ \mathrm{ns}^{-1}$ 时的 1/10. 本文只讨论了保留率 $r = 0.5, 0.7, 0.9$ 这三种情况下的误比特率, 可以明显发现双阈值量化方法大大降低了 VCSELA 与 VCSELB 之间的误比特率, 从图 6 的趋势可以看出, 当采用更高的耦合强度 $k_2$ 和更低的保留率 $r$ 时, 误比特率会达到 $\log_{10}(\mathrm{BER}) < -6$.

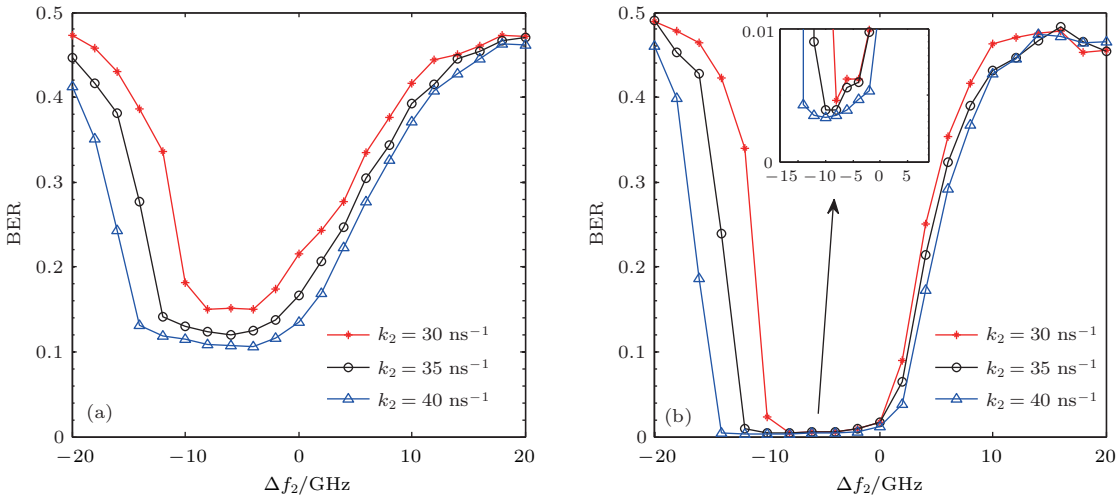


图 5 单阈值条件下 (a) D-VCSEL 和 VCSELA 之间的误比特率; (b) VCSELA 和 VCSELB 之间的误比特率

Fig. 5. Under the condition of single threshold value: (a) The bit error rate betweenr D-VCSEL and VCSELA; (b) the bit error rate between VCSELA and VCSELB.

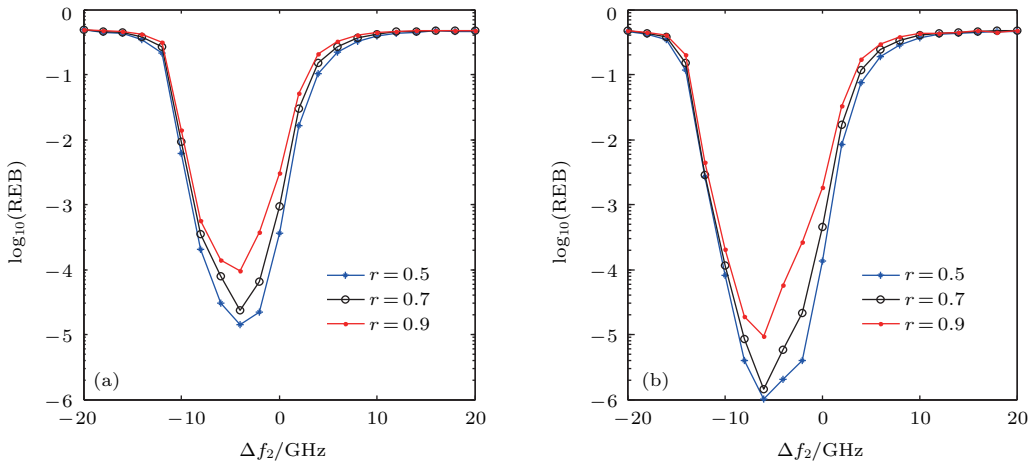


图 6 不同保留率下 VCSELA 与 VCSELB 之间误比特率图 (a) $k_2 = 30\ \mathrm{ns}^{-1}$; (b) $k_2 = 35\ \mathrm{ns}^{-1}$

Fig. 6. The bit error rate between VCSELA and VCSELB under different retention rate: (a) $k_2 = 30\ \mathrm{ns}^{-1}$; (b) $k_2 = 35\ \mathrm{ns}^{-1}$.

## 3.4 参数失配对密钥误比特率的影响

因为激光器参数可能存在一定的误差, 为了保证本方案的普适性, 需要讨论激光器参数失配造成同步系数下降, 从而导致误比特率上升的问题. I-VCSEL 和 D-VCSEL 组合起来产生混沌驱动信号, 这两个激光器参数的改变一般不影响 VCSELA 和 VCSELB 之间的同步性. VCSELA 与 VCSELB 由同一信号源驱动, 这两个激光器之间参数失配会造成混沌同步系数的下降, 假定 VCSELA 的参数不变, VCSELB 相对于 VCSELA 的参数变化比例描述为 [22]

$$\begin{cases} \Delta k = (k^{\mathrm{B}} - k^{\mathrm{A}})/k^{\mathrm{A}}, \\ \Delta\alpha = (\alpha^{\mathrm{B}} - \alpha^{\mathrm{A}})/\alpha^{\mathrm{A}}, \\ \Delta\gamma_N = (\gamma_N^{\mathrm{B}} - \gamma_N^{\mathrm{A}})/\gamma_N^{\mathrm{A}}, \\ \Delta\gamma_{\mathrm{s}} = (\gamma_{\mathrm{s}}^{\mathrm{B}} - \gamma_{\mathrm{s}}^{\mathrm{A}})/\gamma_{\mathrm{s}}^{\mathrm{A}}, \\ \Delta\gamma_{\mathrm{p}} = (\gamma_{\mathrm{p}}^{\mathrm{B}} - \gamma_{\mathrm{p}}^{\mathrm{A}})/\gamma_{\mathrm{p}}^{\mathrm{A}}, \\ \Delta\gamma_{\mathrm{a}} = (\gamma_{\mathrm{a}}^{\mathrm{B}} - \gamma_{\mathrm{a}}^{\mathrm{A}})/\gamma_{\mathrm{a}}^{\mathrm{A}}. \end{cases} \tag{7}$$

图7给出了在单阈值量化情况下, 密钥误比特率随着参数失配程度的变化曲线, 参数失配程度的范围是[−10%, 10%], 星形、圆圈、圆点、方框、上三角、叉号依次代表参数$\kappa, \alpha, \gamma_N, \gamma_\mathrm{s}, \gamma_\mathrm{p}, \gamma_\mathrm{a}$, 五角星表示所有参数. 从图中可以看出参数$\kappa$, $\alpha$和$\gamma_N$对误比特率的影响较大, 而参数$\gamma_\mathrm{s}$, $\gamma_\mathrm{p}$和$\gamma_\mathrm{a}$的变化对误比特率的影响很小. 另外, 当所有参数同时出现失配时, 误比特率上升得最快. 因此, 为了产生低误比特率的高速同步密钥, VCSELA应该与VCSELB尽可能地匹配. 如果误码率增大, 还可以使用双阈值量化和纠错码技术[13]进行改善.

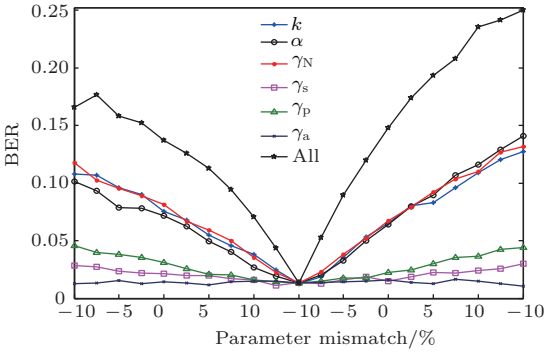


图7 误比特率随参数失配程度的曲线图

Fig. 7. The bit error rate as a fuction of the parameters mismatch.

### 3.5 密钥随机性测试

仅对VCSELA和VCSELB的输出进行采样量化很难产生随机性很高的密钥流, 还需要对量化产生的比特进行后处理来提高密钥的随机性. 在这一小节, 通过简单的移位异或后处理方式增强密钥的随机性.

密钥随机性使用美国国家技术标准局的NIST SP820-22套件测试, 该套件一共包含15项测试[23,24], 每1 Mbit大小序列会给出一个$P$-value. 在显著水平$\alpha = 0.01$时, 如果$P$-value $> 0.0001$, 就说明通过了检验随机性. 由于VCSELA和VCSELB产生的比特非常相似, 因此只需要测试VCSELA产生的随机比特. 在$k_2 = 40$ ns$^{-1}$, $\Delta f_2 = 0$ GHz的条件下采样, 通过单阈值量化, 再移位60位比特进行异或操作产生40 Mbit数据, 可以通过NIST随机性测试. 表1给出了随机性测试结果.

表1 随机性测试结果

Table 1. Results of NIST statistical test.

| Statistical test | $P$-value | Proportion | Result |
|---|---|---|---|
| Runs | 0.000296 | 37/40 | 通过 |
| Longest run | 0.078086 | 40/40 | 通过 |
| Frequency | 0.275709 | 37/40 | 通过 |
| Block frequency | 0.141256 | 40/40 | 通过 |
| Cumulative sums | 0.484646 | 38/40 | 通过 |
| Rank | 0.637119 | 40/40 | 通过 |
| Non overlapping template | 0.003577 | 40/40 | 通过 |
| Overlapping template | 0.275709 | 38/40 | 通过 |
| Universal | 0.021262 | 40/40 | 通过 |
| FFT | 0.637119 | 40/40 | 通过 |
| Approximate entropy | 0.437274 | 40/40 | 通过 |
| Serial | 0.437274 | 40/40 | 通过 |
| Linear complexity | 0.875539 | 40/40 | 通过 |
| Random excursions | 0.242986 | 24/25 | 通过 |
| Random excursions variant | 0.015065 | 25/25 | 通过 |

## 4 结 论

本文提出了一种基于单向注入VCSELs系统的密钥分发方案, 使用D-VCSEL产生几乎无时延特征的混沌信号, 驱动VCSELA和VCSELB实现混沌同步. 并对VCSELA和VCSELB之间的混沌同步特性进行了分析, 确定了高质量的混沌同步参数范围, 之后通过采样、量化、异或操作产生密钥流.

接着分析了通信双方的密钥误比特率, 为了保证安全性, 同时分析了窃听者Eve和合法用户VCSELA之间的误比特率. 结果表明, 在单阈值情况下, 密钥产生速率为4 Gbit/s, 合法用户之间的误比特率低至1%左右, 合法用户与窃听者之间的误比特率都高于10%.

为了进一步降低合法用户之间的误比特率, 采用双阈值量化方法, 对三种保留率下的误比特率进行了分析. 结果显示, 在损失一半比特的情况下(密钥产生速率为2 Gbit/s), 误比特率可以低至$10^{-6}$. 接着研究了VCSELA和VCSELB之间参数失配时, 同步质量下降导致误比特率提高的情况, 指出误比特率对参数$\kappa$, $\alpha$和$\gamma_N$比较敏感. 最后, 对本系统产生的密钥随机性做了NIST测试. 值得注意的是, 基于VCSEL混沌激光器的随机数产生及密钥分发的相关实验验证对光通信信息安全领域也有至关重要的意义, 将作为下一步的研究重点.

## 参考文献


[1] Diffie W, Hellman M 1976 *IEEE Trans. Inf. Theory* **22** 644

[2] Huang D, Huang P, Lin D, Wang C, Zeng G 2015 *Opt. Lett.* **40** 3695

[3] Li P, Wang Y C, Zhang J Z 2010 *Opt. Express* **18** 20360

[4] Guo X X, Xiang S Y, Zhang Y H, Wen A J, Hao Y 2018 *IEEE J. Quantum Electron.* **54** 2000308

[5] Zhang J B, Zhang J Z, Yang Y B, Liang J S, Wang Y C 2010 *Acta Phys. Sin.* **59** 7679 (in Chinese) [张继兵, 张建忠, 杨毅彪, 梁君生, 王云才 2010 物理学报 **59** 7679]

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

[7] Koizumi H, Morikatsu S, Aida H, Nozawa T, Kakesu I, Uchida A, Yoshimura K, Muramatsu J, Davis P 2013 *Opt. Express* **211** 7869

[8] Wang L, Guo Y, Sun Y, Zhao Q, Lan D, Wang Y, Wang A 2015 *IEEE J. Quantum Electron.* **51** 8000208

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

[10] Tang X, Wu J G, Xia G Q, Wu Z M 2011 *Acta Phys. Sin.* **60** 141 (in Chinese) [唐曦, 吴加贵, 夏光琼, 吴正茂 2011 物理学报 **60** 141]

[11] Yang F, Tang X, Zhong Z Q, Xia G Q, Wu Z M 2016 *Acta Phys. Sin.* **65** 118 (in Chinese) [杨峰, 唐曦, 钟祝强, 夏光琼, 吴正茂 2016 物理学报 **65** 118]

[12] Jiang N, Pan W, Yan L, Luo B, Xiang S, Yang L, Zheng D, Li N 2011 *IEEE J. Sel. Top. Quantum Electron.* **17** 1220

[13] Argyris A, Pikasis E, Syvridis D 2016 *J. Lightwave Technol.* **34** 5325

[14] Martin-Regalado J, Prati F, Miguel M San, Abraham N B 1997 *IEEE J. Quantum Electron.* **33** 765

[15] Zhang H, Xiang S Y, Zhang Y H, Guo X X 2017 *Appl. Opt.* **56** 6728

[16] Xiang S Y, Zhang H, Guo X X, Li J F, Wen A J, Pan W, Hao Y 2017 *IEEE J. Sel. Top. Quantum Electron.* **23** 1700207

[17] Hong Y, Paul J, Spencer P S, Shore K A 2006 *JOSA B* **23** 2285

[18] Lin F Y, Liu J M 2003 *Opt. Commun.* **221** 173

[19] Uchida A, Amano K, Inoue M, Hirano K, Naito S, Someya H, Oowada I, Kurashige T, Shiki M, Yoshimiri S, Davis P 2008 *Nat. Photonics* **2** 728

[20] Buskila O, Eyal A, Shtaif M 2008 *Opt. Express* **16** 3383

[21] Xue C, Jiang N, Qiu K, Lv Y 2015 *Opt. Express* **23** 14510

[22] Liu J, Wu Z M, Xia G Q 2009 *Opt. Express* **17** 12619

[23] Yang H B, Wu Z M, Tang X, Wu J G, Xia G Q 2015 *Acta Phys. Sin.* **64** 084204 (in Chinese) [杨海波, 吴正茂, 唐曦, 吴加贵, 夏光琼 2015 物理学报 **64** 084204]

[24] NIST Special Publication 800-22, 2001 http://csrc.nist.gov/groups/ST/toolkit/rng/documentation_software.html [2018-5-1]

# Key distribution based on unidirectional injection of vertical cavity surface emitting laser system*

Zhang Hao Guo Xing-Xing Xiang Shui-Ying†

(*State Key Laboratory of Integrated Service Networks, School of Telecommunication Engineering, Xidian University, Xi'an 710071, China*)

( Received 28 May 2018; revised manuscript received 23 June 2018 )

**Abstract**

Random source is important for the security of key distribution. In this paper, a novel secure key distribution scheme based on unidirectional injection of vertical cavity surface emitting laser (VCSEL) system is proposed. In the proposed scheme, a chaotic signal without time delay signature is generated by a VCSEL subject to unidirectional optical injection, which is regarded as a master laser. The chaotic signal generated by the master VCSEL is further injected into two slave VCSELs to obtain synchronized bandwidth-enhanced chaotic signals. After that, by sampling, quantizing and XOR operation on the two synchronized chaotic signals, two key streams can be obtained.

Based on the well-known spin-flip model, the time delay signature of chaotic signals generated by master VCSEL and the synchronization performance between the master VCSELs and two slave VCSELs are numerically investigated in detail. It is shown that by the unidirectional injection, the chaotic outputs can be achieved in the master VCSEL in a wide range of frequency detuning and coupling strength. More importantly, no time delay signature can be observed in the auto correlation function of the chaotic intensity time series generated by the master VCSEL. Besides, we find that high quality synchronization is achieved between the bandwidth-enhanced chaotic signals generated by two slave VCSELs under the common driving of master VCSEL. The synchronization coefficient between two slave VCSELs increases up to 0.99, and the synchronization coefficient between master VCSEL and salve VCSEL is only 0.74. Note that such a high quality synchronization between two slave VCSELs while relatively low quality synchronization between the master and slave VCSEL is conducible to ensuring the security of key distribution.

In addition, the effects of tunable parameters on key bit error rate are considered, and two quantization methods are employed for comparison. Numerical simulation results show that the key bit error rate between two legitimate users is as low as 1%, and the key bit error rate between legitimate user and eavesdropper is higher than 10% in the single-threshold case; the bit error rate can even be as low as $10^{-6}$ in the double-threshold case. The influence of parameter mismatch on key bit error rate is also discussed, and it is suggested that two salve VCSELs should be finely matched to ensure low bit error rate. Finally, NIST randomness test is performed for the generated key streams. Hence, the proposed scheme enhances the security of key distribution, which is valuable for further developing the chaos communication systems.

**Keywords:** vertical cavity surface emitting laser, key distribution, secure communication, chaotic synchronization

**PACS:** 42.55.Px, 82.40.Bj, 05.45.–a **DOI:** 10.7498/aps.67.20181038

* Project supported by the National Natural Science Foundation of China (Grant No. 61674119) and the Young Scientists Fund of the National Natural Science Foundation of China (Grant No. 61306061).

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