第 43 卷 第 1 期/2023 年 1 月/光学学报 研究论文

光学学报

基于生成对抗网络的混沌激光同步优化

赵安可[1]，江宁[1*]，王超[2]，刘世勤[1]，邱昆[1]

[1]电子科技大学信息与通信工程学院，四川 成都 611731；

[2]中国空间技术研究院卫星应用总体部，北京 100081

摘要 提出并验证了一种基于深度学习的混沌激光同步优化方案，在共同外腔半导体激光器驱动注入同步系统中，引入生成对抗网络对初始的混沌同步信号进行优化。所提方案的主要优点在于：实现了混沌信号的时延标签抑制和复杂度提升；显著改善了混沌信号幅值分布的对称性；大幅降低了驱动端和本地端的相关性，提升了同步系统的私密性。此外，将优化后的混沌信号应用于物理熵源，在高质量混沌同步的基础上，验证了速率高达 4.1 Gbit/s、误码率低于 10^{-3} 的高速同步物理随机数产生。

关键词 激光光学；混沌激光；光反馈；混沌同步；生成对抗网络；物理随机数

中图分类号 TN248.4 **文献标志码** A **DOI**：10.3788/AOS220994

1 引 言

半导体激光器在外光反馈、外光注入和光电反馈等外部扰动作用下会展现出丰富的非线性，通过设置一定的扰动条件，能使其输出由恒定状态过渡到混沌态，从而产生拥有高带宽和类随机性等特点的混沌激光[1-4]。相比于真正的噪声，混沌信号的优势是能够实现同步控制，因此在许多领域都有着重要的应用。例如，混沌激光不仅可以作为光载波为光纤通信系统提供物理层安全[5-12]，还可以用作高速随机数和密钥生成的物理熵源[13-20]。

香农的理论研究证明，当加密明文采用的密钥同时满足不短于明文长度、密钥随机且只能一次性使用时，即可认为通信是绝对安全的[21]，而这种“一次一密”加密方式的关键是如何生成高速随机密钥。传统密钥分配技术主要是基于各类密码学的加密算法，其安全性取决于窃密者的计算能力和计算资源。但随着量子计算机的出现与发展，这种基于计算安全的密钥分配技术面临被破解的风险，因此学者们提出另一类基于物理现象的密钥分配方法，其中包括量子密钥分配[22]和基于混沌激光的密钥分配[13-16]。量子密钥分配被公认是无条件安全的，但是在密钥分发速率和分发距离方面还面临着挑战，目前密钥生成的最高速率为 Mbit/s 量级[23]。

混沌激光已被证明可用于密钥分配系统，为其提供可靠的物理熵源，通过构建混沌激光同步，从中提取出高速随机密钥。相比于量子密钥分发技术，混沌激光密钥分发虽然不能提供无条件的安全性，但是在密钥分发速率、硬件成本、与传统光纤通信系统的兼容性等方面具有显著优势。Argyris 等[24]提出了基于双向耦合结构的高质量混沌激光同步系统，通过单比特量化和前向纠错的后处理技术，在实验中获得了速率为 1.05 Gbit/s、密钥不一致率为 10^{-2} 的同步物理随机数，首次证明了混沌激光在 Gbit/s 量级密钥分配中的潜力。此后，学者们又陆续提出了几种基于混沌激光熵源的 Gbit/s 同步物理随机数产生方案[25-28]。

共同外部驱动光注入是混沌密钥分配系统的主要同步结构，采用外腔半导体激光器（ECSL）作为驱动源在实际中最易于实现，并且具有良好的鲁棒性。但是，这种同步系统在应用中面临以下问题：1）光反馈为混沌同步信号引入了时延特征，使得信号复杂度受限；2）混沌信号具有不对称的幅值分布，影响了密钥生成的随机性；3）外部驱动信号和本地端同步信号存在较高的相关性，降低了同步系统的安全性。针对上述问题，本文提出一种光反馈 ECSL 驱动注入同步的优化方案，引入生成对抗网络对初始混沌同步信号进行优化，同时实现混沌信号时延标签抑制、幅值分布对称性改善和同步系统私密性提升。

2 基本原理

生成对抗网络（GAN）是一种强大的生成模型，该

收稿日期：2022-04-19；**修回日期**：2022-05-28；**录用日期**：2022-06-29；**网络首发日期**：2022-07-10

基金项目：国家自然科学基金（62171087，61671119）、中央高校基本科研业务费（ZYGX2019J003）、四川省科技计划项目（2021JDJQ0023）

通信作者：*uestc_nj@uestc.edu.cn

模型包括两个互相博弈的神经网络，它们在训练过程中通过不断迭代优化，最终能够达到纳什均衡[29-30]。简单来说，GAN的主要学习任务是实现概率分布转换，即通过输入数据来产生逼近目标概率分布的数据。由光反馈ECSL产生的混沌信号，具有不对称的幅值概率分布，在密钥分配中，这种非对称性限制了密钥生成的速率和随机性。因此，在混沌激光同步系统中引入GAN，可以优化混沌信号幅值分布的对称性，进而实现更高速率随机密钥的生成。

图1展示了GAN的基本结构，其主要由一个生成器(G)和一个判别器(D)组成。生成器G将生成逼近真实数据分布的伪数据作为目标，而判别器D将准确判别输入数据是将真实数据还是将伪造数据作为目标。在对抗训练中，G和D通过不断的迭代进行优化，当D不能正确判别其输入为真实数据还是生成数据时，便达到了最优状态。

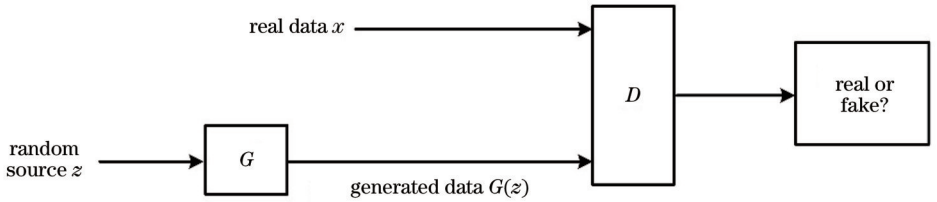

图1　GAN模型的基本结构

Fig. 1　Basic structure of GAN model

GAN的训练通常使用交替的方式对G和D进行优化。优化过程通过随机梯度下降法进行网络参数的更新，从而使损失函数趋于最小值。训练过程中，生成器与判别器在每步中各训练一次。在训练D时，需要固定G的参数。当输入为真实数据和生成数据时，D对应的输出分别为1和0。D的损失函数可以使用交叉熵函数来描述，即

$$J(D)=\frac{1}{2}E_{x\sim p_{\text{data}}(x)}\left[\log D(x)\right]-\frac{1}{2}E_{z\sim p_z(z)}\left\{\log\left\{1-D\left[G(z)\right]\right\}\right\},\tag{1}$$

式中：$p_{\text{data}}(x)$为真实数据的分布；$p_z(z)$为生成数据的分布；$D(x)$为输入真实数据x时D正确判别的概率；$D[G(z)]$为输入生成数据$G(z)$时D正确判别的概率。同样地，在训练G时，需要固定D的参数，G的损失函数可以描述为

$$J(G)=\frac{1}{2}E_{z\sim p_z(z)}\left\{\log\left\{1-D\left[G(z)\right]\right\}\right\}。\tag{2}$$

GAN总的目标函数可以表示为

$$\min_G\max_D V(D,G)=E_{x\sim p_{\text{data}}(x)}\left[\log D(x)\right]+E_{z\sim p_z(z)}\left\{\log\left\{1-D\left[G(z)\right]\right\}\right\}。\tag{3}$$

在优化过程中，首先进行生成器训练，使目标函数$V(D,G)$最小化；随后进行判别器训练，使目标函数$V(D,G)$最大化；上述训练过程交替进行，最终G将生成足够逼真的数据，使D无法正确区分，即D的输出概率稳定在0.5。

图2为基于共同光反馈ECSL驱动注入的混沌激光同步系统实验结构图。同步系统采用常规的光反馈ECSL作为外部驱动，驱动端分布反馈(DFB)激光器的部分输出经反馈腔反射回激光器中，通过光衰减器将反馈强度设置为−20 dB，从而使激光器产生混沌激光。将DFB激光器的工作电流设置为13.2 mA，约为其阈值电流的1.5倍。驱动端输出的混沌激光经光耦合器分为两路，分别输入两个本地端的从激光器(SL)中。本实验采用开环同步系统，即本地端的SL1和SL2不带有光反馈，相较于闭环同步，开环同步具有更强的系统鲁棒性。在相同且足够强的光注入情形下，SL1和SL2通过注入锁定的作用产生混沌同步激光。实验中将注入光功率设置为−20 dBm。初始同步信号经光电转换后，在采样率为100 GSa/s数字实时示波器中存储，并输入至GAN进行后续处理。

图3所示为本实验搭建的GAN具体结构。与传统的GAN不同，本实验中GAN的目的是将初始混沌信号转换为逼近高斯分布的复杂混沌信号，因此，训练中目标数据为符合标准正态分布的高斯噪声信号，且在训练中该信号保持不变，生成器G的输入为示波器采集到的初始混沌信号。本文选取的序列长度为2×10^6，该长度足以实现既定的训练目标，对应的平均计算时间约为0.026 s，采用的显卡型号为NVIDIA GeForce GTX 1650。对于初始混沌信号，实验中将1000个连续的采样点作为一组样本，分别输入到生成器和判别器中。由于输入数据为一维时间序列，为了保持混沌信号的采样率，需要将输入和输出设置为相同的维度，因此直接采用全连接层并结合激活函数来搭建网络。图3给出了具体的网络结构和使用的激活函数，其中生成网络和判别网络均只包含一个隐藏层。

3　分析与讨论

3.1　同步优化实验结果

图4对比了优化前后混沌信号的自相关函数(ACF)和幅值概率分布。为了分析混沌信号的时延标签(TDS)和复杂度，分别采用两种常用的分析方式——ACF和[31-34]排列熵(PE)[35-37]。排列熵的计算值反

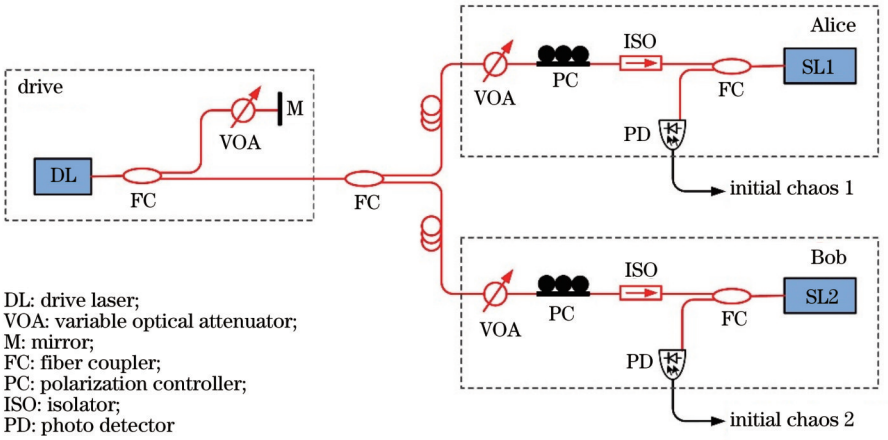

图 2　基于共同光反馈ECSL驱动注入的混沌激光同步系统实验结构图

Fig. 2　Experimental setup of chaos laser synchronization system based on common injection of an ECSL with optical feedback

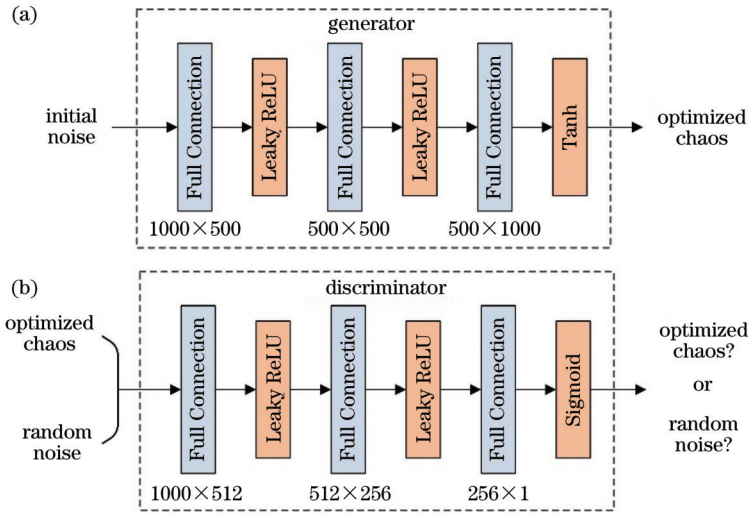

图 3　GAN结构图。(a)生成网络结构;(b)判别网络结构

Fig. 3　Structure diagram of GAN. (a) Generating network structure; (b) discriminating network structure

映了所求时间序列的复杂度,运算中需要进行归一化,将计算值限定在0到1之间,越接近1,则序列的复杂度越高。如图4(a)、(b)所示,光反馈ECSL驱动注入使得从激光器产生的初始混沌信号存在TDS,在62.3 ns反馈延时处能检测到明显的相关峰,并且该信号的幅值也呈现出不对称的概率分布,经计算初始混沌信号的复杂度和偏度分别为0.973和1.19。经过GAN优化后的结果如图4(c)、(d)所示。可以看到,优化信号的ACF曲线近似于狄拉克函数(δ),反馈延时处对应的TDS被完全抑制,复杂度提升至0.99。另外,优化后的幅值分布接近高斯分布,对称性得到显著改善,偏度减小至7.78×10^{-4},相较于优化前,优化后的偏度提升了3个数量级。

图5(a)展示了不同参数条件下,优化前后混沌信号TDS的抑制结果。实验中通过改变SL注入光功率来获得不同的混沌信号。所采用的TDS量化步骤为:首先,在ACF曲线中找到反馈延时对应的时刻;然后,以该时刻为中心,将附近1 ns作为选取的时间范围;最后,对该范围取绝对值,并将其中的最大值用作TDS量化值。图5(a)所示的结果表明,相比于初始混沌信号,优化信号的TDS得到了显著抑制,在不同注入功率下都降低至0.01以下的水平。为了验证分布的改善情况,采用KL(Kullback-Leibler)散度来量化优化信号分布和标准正态分布之间的差异,KL散度值越趋近于0,表示两个分布越相似。如图5(b)所示,原始混沌信号的KL散度值大于3,而经过优化后信号的KL散度大幅减小,在不同注入功率下均保持在小于0.01的低水平,表明优化后的分布近似于标准正态分布。上述结果证明,对于参数失配引入噪声的情况,该模型在较大的失配范围内具有良好的鲁棒性。对于响应激光器不同状态的输出,GAN都能实现TDS和幅值分布的优化,因此不需要重复训练。

为了量化分析同步质量,采用互相关函数衡量混沌信号之间的同步质量[15,26,38],通常选取其绝对值的最大值,即互相关系数(CC)来表示混沌信号的相关程度:CC值越接近1,表明同步质量越好;越接近0,则表

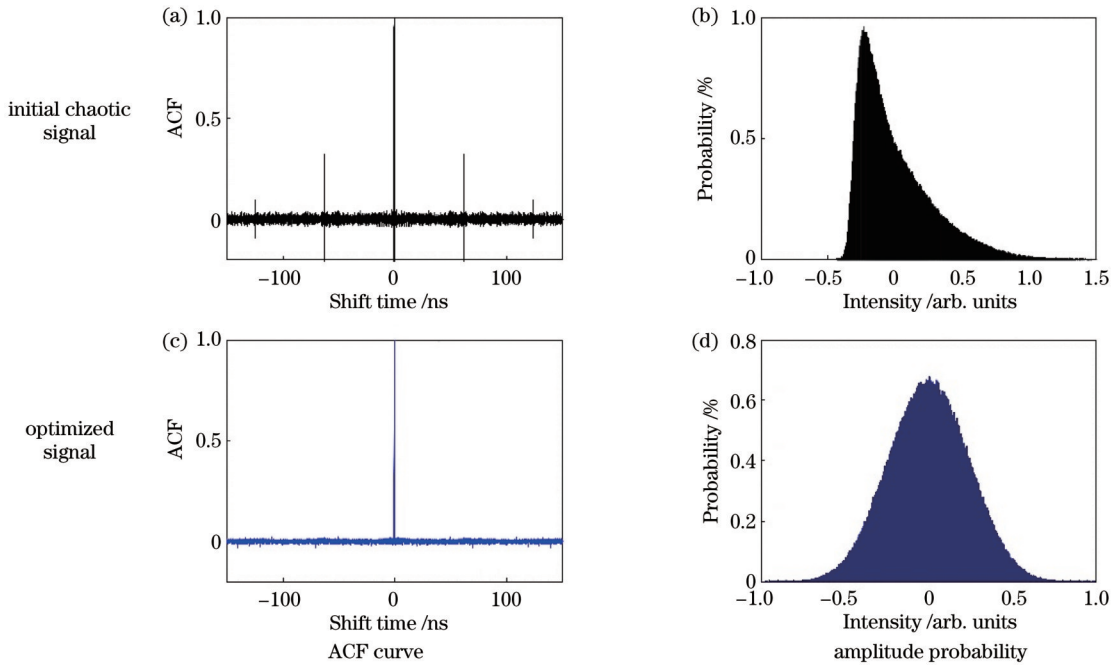

图 4　初始混沌信号和优化后信号的 ACF 曲线和幅值概率分布

Fig. 4　ACF curves and amplitude probability distributions of initial chaotic signal and optimized signal

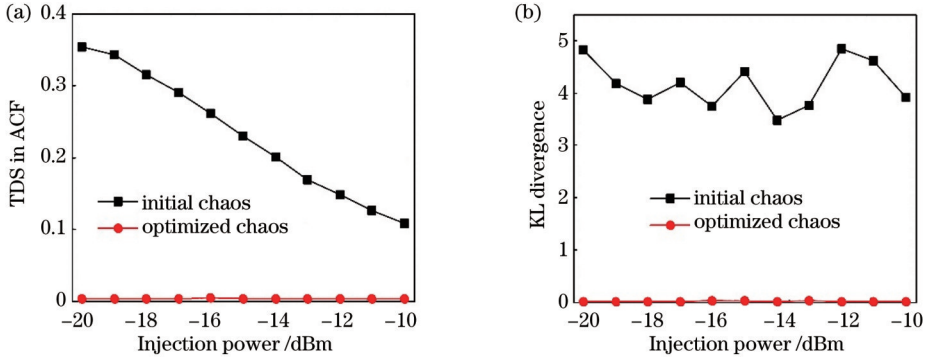

图 5　TDS 和 KL 散度值随注入光功率的变化。(a) TDS;(b) KL 散度值

Fig. 5　TDS and KL divergence values changed with injection power. (a) TDS; (b) KL divergence

明同步质量越差。图 6 对比了优化前后的同步实验结果,其中虚线曲线对应驱动端激光器 DL 和本地端激光器 SL1 的互相关函数,实线曲线对应两个本地端激光器 SL1 和 SL2 的互相关函数。如图 6(a)所示,DL 和 SL1 输出信号之间的互相关系数约为 0.81。由于驱动信号经过公共链路传输至本地端,DL 和 SL1 较高的相关性会使本地端同步信号存在泄漏的风险,从而降低了系统的安全性。如图 6(b)所示,优化后 DL 和 SL1 输出信号之间的互相关系数降低至 0.01 以下,表明这两个信号之间几乎不存在相关性,通过该优化方案使同步系统的私密性得到了显著增强。SL1 和 SL2 输出的混沌同步信号在优化前后的互相关系数均为 0.983,证明所提方案中 GAN 不会破坏信号的同步性,能够获得高品质的混沌同步信号。

3.2　高速同步物理随机数产生

接下来验证上述混沌同步优化方案在同步物理随机数生成方向的应用。所使用的后处理主要包括双阈值量化和延时比特异或[19,26],其中双阈值量化拥有上下两个阈值:较高的阈值 $T_h=T_m+\alpha\cdot\sigma$,较低的阈值 $T_L=T_m-\alpha\cdot\sigma$,其中 α 为阈值系数,用于描述上下阈值之间的距离,σ 为同步信号的标准差,T_m 为幅度均值。通过比较上下阈值和采样点的幅度来确定量化的比特:将幅度大于 T_h 的采样点判定为 1,小于 T_L 的采样点判断为 0。对幅度大于 T_L 且小于 T_h 的采样点进行标记并记录该处的索引值,Alice 和 Bob 交换这些索引后,将所有索引对应的采样点丢弃。定义最终保留的随机比特个数和初始采样点的数量之比为 γ,最终根据 γ 的值可以确定同步随机比特序列的实际生成速率。

图 7 所示为阈值系数 α 取不同值时对同步随机序列误码率(BER)的影响。可以看到,优化后信号的 BER 明显低于原始混沌同步信号的 BER,这是因为通过优化,幅值分布的对称性明显改善。$\alpha=0$ 即不丢弃

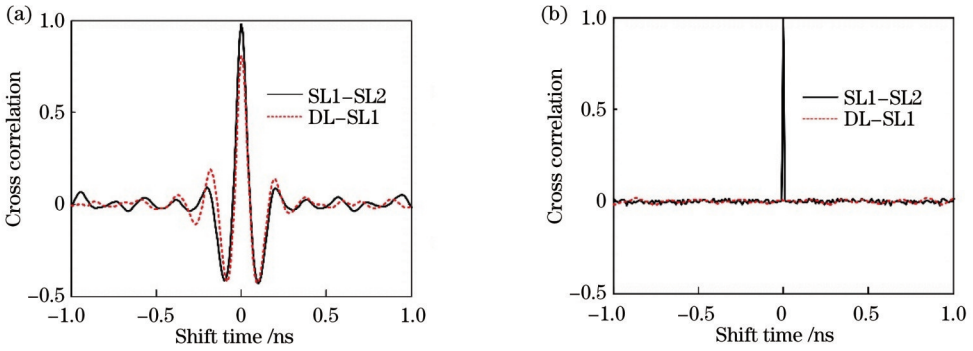

图 6 优化前后驱动信号和本地端信号之间的相关性。(a)优化前;(b)优化后

Fig. 6 Cross correlation between driving signal and local signal before and after optimization. (a) Before optimization; (b) after optimization

任何采样点时,BER约为0.1,对应于采用一位量化时取得的结果。随着α的增加,BER呈现出近似线性下降的趋势,当α大于0.125时,BER降至前向纠错门限(3.8×10^{-3})以下。将α设置为0.15,从而使同步随机比特序列的BER低于10^{-3},此时对应的保留比γ为0.82。同步随机数的最终生成速率与γ对应,即等于采样率和γ的乘积,因此同步物理随机数的实际生成速率为4.1 Gbit/s。实际应用中,缩短GAN的优化时间,有利于提升密钥分发的实时性。为了检测随机数的质量,采用国际上广泛使用的随机性测试集NIST SP800-22作为评价标准[13,16-19],结果表明所提方案产生的4.1 Gbit/s同步物理随机数通过了随机性标准测试。

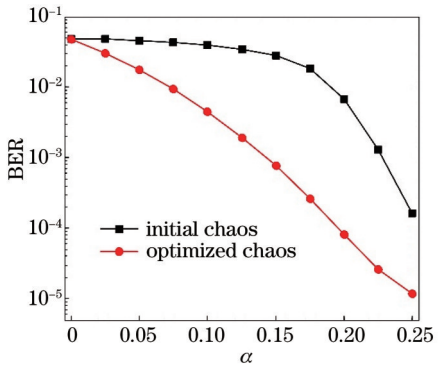

图 7 同步随机序列误码率随阈值系数α的变化

Fig. 7 Influence of threshold coefficient α on the bit error rate (BER) of synchronized random bit sequence

4 结 论

提出一种共同光反馈ECSL驱动注入同步的优化方案。通过搭建GAN对初始混沌同步信号进行优化,同时实现了混沌信号的TDS抑制和幅值分布对称性改善,并且大幅降低了驱动信号和本地端同步信号之间的相关性,提升了同步系统的私密性。此外,还验证了高速和高一致性的物理随机数同步。在复杂混沌信号同步的基础上,通过双阈值量化提取出速率达4.1 Gbit/s量级、BER低于10^{-3}的同步随机比特序列。上述研究工作在高速密钥分配领域拥有良好的应用前景,可为“一次一密”保密通信提供高速可靠的随机密钥。

参 考 文 献

[1] Ohtsubo J. Semiconductor lasers: stability, instability and Chaos [M]. Cham: Springer, 2017.

[2] Sciamanna M, Shore K A. Physics and applications of laser diode chaos[J]. Nature Photonics, 2015, 9(3): 151-162.

[3] 张艺腾, 贾志伟, 李青天, 等. 基于光反馈双模DFB激光器的宽带混沌信号产生[J]. 光学学报, 2021, 41(21): 2114001.
Zhang Y T, Jia Z W, Li Q T, et al. Broadband chaos signal generation based on dual-mode DFB laser with optical feedback [J]. Acta Optica Sinica, 2021, 41(21): 2114001.

[4] Li P, Cai Q, Zhang J G, et al. Observation of flat chaos generation using an optical feedback multi-mode laser with a band-pass filter[J]. Optics Express, 2019, 27(13): 17859-17867.

[5] Argyris A, Syvridis D, Larger L, et al. Chaos-based communications at high bit rates using commercial fibre-optic links[J]. Nature, 2005, 438(7066): 343-346.

[6] Lavrov R, Jacquot M, Larger L. Nonlocal nonlinear electro-optic phase dynamics demonstrating 10 Gb/s chaos communications[J]. IEEE Journal of Quantum Electronics, 2010, 46(10): 1430-1435.

[7] Ke J X, Yi L L, Xia G Q, et al. Chaotic optical communications over 100-km fiber transmission at 30-Gb/s bit rate[J]. Optics Letters, 2018, 43(6): 1323-1326.

[8] Yang Z, Yi L L, Ke J X, et al. Chaotic optical communication over 1000 km transmission by coherent detection[J]. Journal of Lightwave Technology, 2020, 38(17): 4648-4655.

[9] Gao X J, Cheng M F, Deng L, et al. Robust chaotic-shift-keying scheme based on electro-optical hybrid feedback system [J]. Optics Express, 2020, 28(8): 10847-10858.

[10] Wang L S, Mao X X, Wang A B, et al. Scheme of coherent optical chaos communication[J]. Optics Letters, 2020, 45(17): 4762-4765.

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

[12] Zhao A K, Jiang N, Liu S Q, et al. Physical layer encryption for WDM optical communication systems using private chaotic phase scrambling[J]. Journal of Lightwave Technology, 2021, 39(8): 2288-2295.

[13] Kanter I, Butkovski M, Peleg Y, et al. Synchronization of random bit generators based on coupled chaotic lasers and application to cryptography[J]. Optics Express, 2010, 18(17):

18292-18302.
[14] 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.
[15] 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.
[16] Gao H, Wang A B, Wang L S, et al. 0.75 Gbit/s high-speed classical key distribution with mode-shift keying chaos synchronization of Fabry-Perot lasers[J]. Light: Science & Applications, 2021, 10: 172.
[17] Li N Q, Kim B, Chizhevsky V N, et al. Two approaches for ultrafast random bit generation based on the chaotic dynamics of a semiconductor laser[J]. Optics Express, 2014, 22(6): 6634-6646.
[18] Xiang S Y, Wang B, Wang Y, et al. 2.24-Tb/s physical random bit generation with minimal post-processing based on chaotic semiconductor lasers network[J]. Journal of Lightwave Technology, 2019, 37(16): 3987-3993.
[19] Xue C P, Jiang N, Lü Y X, et al. Secure key distribution based on dynamic chaos synchronization of cascaded semiconductor laser systems[J]. IEEE Transactions on Communications, 2017, 65(1): 312-319.
[20] Li P, Guo Y, Guo Y Q, et al. Ultrafast fully photonic random bit generator[J]. Journal of Lightwave Technology, 2018, 36(12): 2531-2540.
[21] Shannon C E. Communication theory of secrecy systems[J]. Bell System Technical Journal, 1949, 28(4): 656-715.
[22] Gisin N, Ribordy G, Tittel W, et al. Quantum cryptography[J]. Reviews of Modern Physics, 2002, 74(1): 145-195.
[23] Xu F H, Ma X F, Zhang Q, et al. Secure quantum key distribution with realistic devices[J]. Reviews of Modern Physics, 2020, 92(2): 025002.
[24] Argyris A, Pikasis E, Syvridis D. Gb/s one-time-pad data encryption with synchronized chaos-based true random bit generators[J]. Journal of Lightwave Technology, 2016, 34(22): 5325-5331.
[25] Li X Z, Li S S, Chan S C. Correlated random bit generation using chaotic semiconductor lasers under unidirectional optical injection[J]. IEEE Photonics Journal, 2017, 9(5): 1505411.
[26] Zhao Z X, Cheng M F, Luo C K, et al. Synchronized random bit sequences generation based on analog-digital hybrid electro-optic chaotic sources[J]. Journal of Lightwave Technology, 2018, 36(20): 4995-5002.
[27] Zhao A K, Jiang N, Wang Y J, et al. Correlated random bit generation based on common-signal-induced synchronization of wideband complex physical entropy sources[J]. Optics Letters, 2019, 44(24): 5957-5960.
[28] 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): 2000208.
[29] Goodfellow I J, Pouget-Abadie J, Mirza M, et al. Generative adversarial networks[EB/OL]. (2014-06-10)[2021-02-05]. https://arxiv.org/abs/1406.2661.
[30] Maskin E. Nash equilibrium and welfare optimality[J]. The Review of Economic Studies, 1999, 66(1): 23-38.
[31] Rontani D, Locquet A, Sciamanna M, et al. Time-delay identification in a chaotic semiconductor laser with optical feedback: a dynamical point of view[J]. IEEE Journal of Quantum Electronics, 2009, 45(7): 1879-1891.
[32] Li S S, Li X Z, Chan S C. Chaotic time-delay signature suppression with bandwidth broadening by fiber propagation[J]. Optics Letters, 2018, 43(19): 4751-4754.
[33] Zhao A K, Jiang N, Zhang Y Q, et al. Semiconductor laser-based multi-channel wideband chaos generation using optoelectronic hybrid feedback and parallel filtering[J]. Journal of Lightwave Technology, 2022, 40(3): 751-761.
[34] 张依宁, 徐艾诗, 冯玉玲, 等. 光电反馈半导体激光器输出光的混沌特性[J]. 光学学报, 2020, 40(12): 1214001.
Zhang Y N, Xu A S, Feng Y L, et al. Chaos characteristics of the output from a semiconductor laser subject to optoelectronic feedback[J]. Acta Optica Sinica, 2020, 40(12): 1214001.
[35] Zunino L, Soriano M C, Fischer I, et al. Permutation-information-theory approach to unveil delay dynamics from time-series analysis[J]. Physical Review E, 2010, 82(4): 046212.
[36] Zhou P, Fang Q, Li N Q. Phased-array assisted time-delay signature suppression in the optical chaos generated by an external-cavity semiconductor laser[J]. Optics Letters, 2020, 45(2): 399-402.
[37] Zhao A K, Jiang N, Liu S Q, et al. Wideband complexity-enhanced chaos generation using a semiconductor laser subject to delay-interfered self-phase-modulated feedback[J]. Optics Express, 2019, 27(9): 12336-12348.
[38] 薛萍萍, 张建忠, 杨玲珍, 等. 半导体环形激光器的混沌同步及优化[J]. 光学学报, 2015, 35(4): 0414002.
Xue P P, Zhang J Z, Yang L Z, et al. Chaotic synchronization and optimization of semiconductor ring lasers[J]. Acta Optica Sinica, 2015, 35(4): 0414002.

Synchronization Optimization of Chaotic Laser Based on Generative Adversarial Network

Zhao Anke[1], Jiang Ning[1*], Wang Chao[2], Liu Shiqin[1], Qiu Kun[1]

[1]*School of Information and Communication Engineering, University of Electronic Science and Technology of China, Chengdu* 611731, *Sichuan, China*;

[2]*Institute of Spacecraft Application System Engineering, China Academy of Space Technology, Beijing* 100081, *China*

Abstract

Objective Chaotic laser is proved able to be used in key distribution systems to provide a reliable physical entropy source. High-speed random keys can be extracted from a constructed chaotic laser synchronization system. The common

externally driven optical injection is the main synchronization structure of chaotic key distribution systems. External-cavity semiconductor lasers (ECSLs) are driving sources easiest to realize in practice and have good robustness. However, this synchronization system faces the following problems in application: 1) optical feedback introduces time delay characteristics into chaotic synchronization signals, which limits signal complexity; 2) chaotic signals have asymmetric amplitude distribution, which affects the randomness of key generation; 3) there is a high correlation between the external driving signal and the local synchronization signal, which reduces the security of the synchronization system.

Methods Generative adversarial networks (GANs) are a kind of powerful generative model, which includes two neural networks that are pitted against each other in a game-like scenario. They can finally reach a Nash equilibrium through continuous iterative optimization in the training process. The main learning task of a GAN is to realize the transformation of a probability distribution, namely to generate data approaching the target probability distribution through input data. The introduction of a GAN into a chaotic laser synchronization system can optimize the symmetry of chaotic signal amplitude distribution and then realize the generation of random keys at a higher rate.

Results and Discussions Fig. 4 compares the autocorrelation function (ACF) and amplitude probability distribution of chaotic signals before and after optimization. Two commonly used analysis methods, ACF and permutation entropy (PE), are used to analyze the time delay signature (TDS) and complexity of chaotic signals. The optical-feedback ECSL-driven injection makes the initial chaotic signal generated from the laser have TDS, and an obvious correlation peak can be detected at the feedback delay of 62.3 ns, whose amplitude also shows an asymmetric probability distribution [Figs. 4 (a) and (b)]. After calculation, the complexity and skewness of the initial chaotic signal are 0.973 and 1.19, respectively. The results after GAN optimization [Figs. 4 (c) and (d)] demonstrate that the ACF curve of the optimized signal is approximate to a Dirac function. The TDS corresponding to the feedback delay is completely suppressed, and the complexity is increased to 0.99. In addition, the optimized amplitude distribution is close to the Gaussian distribution, and the symmetry is significantly improved. The skewness is reduced to 7.78×10^{-4}, increased by 3 orders of magnitude. Fig. 5(a) shows the suppression results of chaotic signal TDS before and after optimization under different parameter conditions. The results indicate that compared with the initial chaotic signal, the optimized signal has significantly suppressed TDS, which is reduced to a level below 0.01 under different injection powers. The Kullback-Leibler (KL) divergence of the original chaotic signal is greater than 3, while that of the optimized signal is greatly reduced, which remains at a low level of less than 0.01 under different injection powers, indicating that the optimized distribution is close to a standard normal distribution. Fig. 7 shows the influence of the threshold coefficient α on the bit error rate (BER) of synchronous random sequences. The BER of the optimized signal is significantly lower than that of the original chaotic synchronization signal because the symmetry of the amplitude distribution is significantly improved through optimization. BER is about 0.1 at $\alpha=0$ (namely that no sampling point is discarded). With the increase in α, BER follows an approximately linear decline trend. When α is greater than 0.125, BER is below the forward error correction threshold (3.8×10^{-3}). Here α is set to 0.15 so that the BER of synchronous random bit sequences is lower than 10^{-3}, and the corresponding retention ratio γ is 0.82. The final generation rate of synchronized physical random numbers is 4.1 Gbit/s. To verify the quality of random numbers, this paper employs the randomness test set NIST SP800-22 as the evaluation standard, which is widely used internationally. The results show that the 4.1 Gbit/s synchronized physical random numbers generated by the proposed scheme can pass the standard test of randomness.

Conclusions Chaos synchronization is the basis for the application of optical chaos in the field of secure communication. However, the existing experimental systems of chaos synchronization have problems of asymmetric amplitude distribution, limited complexity, and insufficient privacy. This paper proposes and verifies a chaos synchronization optimization scheme based on deep learning. To optimize the initial synchronized chaotic signals, the paper introduces a GAN into the common signal-induced synchronization system which is driven by an ECSL with optical feedback. The main advantages of the proposed scheme are as follows: 1) the initial chaotic signals have suppressed TDS and improved complexity; 2) the symmetry of the amplitude distribution is significantly improved; 3) the correlation between the driving signal and the local signal is greatly reduced, which enhances the privacy of the synchronization system. In addition, the optimized chaotic signals are applied to the physical entropy source. On the basis of chaos synchronization, the paper verifies the generation of synchronized physical random numbers with a high rate of 4.1 Gbit/s and a BER lower than 10^{-3}.

Key words laser optics; chaotic laser; optical feedback; chaos synchronization; generative adversarial network; physical random numbers