面向高速保密通信的激光混沌物理随机数发生器研究进展

李 璞[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光电工程研究所, 山西 太原 030024

摘要 物理随机数在密码学、通信及国家安全等领域具有重要应用价值。传统的物理随机数发生器受限于熵源(如热噪声等)带宽的限制,码率仅处于Mb/s量级。近年来,随着宽带光子熵源(如混沌激光、放大自发辐射噪声)的出现,研究学者提出了众多高速随机数产生方案。其中,混沌激光由于其高带宽、大幅度、易集成等特性,获得了人们的极大关注,被广泛应用于Gb/s量级物理随机数的产生。结合国内外研究现状,对基于混沌激光的物理随机数产生方案进行了综述,分析了各方案的优势及不足,归纳总结了当前混沌物理随机数发生器的研究热点,并指出了其未来可能的发展方向。

关键词 混沌激光; 半导体激光器; 随机数发生器; 保密通信

中图分类号 O436 **文献标识码** A doi: 10.3788/LOP51.060002

Research Progress in Physical Random Number Generator Based on Laser Chaos for High-Speed Secure Communication

Li Pu[1,2] Wang Yuncai[1,2]

[1]*Key Laboratory of Advanced Transducers and Intelligent Control System, Ministry of Education, Taiyuan University of Technology, Taiyuan, Shanxi* 030024, *China*

[2]*Institute of Optoelectronic Engineering, College of Physics and Optoelectronics, Taiyuan University of Technology, Taiyuan, Shanxi* 030024, *China*

Abstract Physical random numbers have great application value in the fields of cryptography, communication and national security. Conventional physical random number generators are limited by the low bandwidth of applied entropy sources such as thermal noise and thus have low bit rates at Mb/s order. With the appearance of wideband photonic entropy sources (e.g. chaotic laser and amplified spontaneous noise) in recent years, lots of schemes for high-speed random number generation are proposed. Among them, chaotic laser attracted many attentions due to its merits such as high bandwidth, large amplitude fluctuation and ease of integration. According to the international research situation, physical random number generation schemes based on chaotic laser are overviewed. Through analyzing their own advantages and disadvantages, current hot spots in the studies are summarized and some possible development orientations in the future are pointed out.

Key words chaotic laser; semiconductor laser; random number generator; secure communication

OCIS codes 190.3100; 140.5960; 060.4510

1 引 言

随机数在蒙特卡罗(Monte Carlo)模拟、统计抽样、人工神经网络等科学计算方面有着广泛应用。尤其

收稿日期: 2014-01-06; **收到修改稿日期**: 2014-02-25; **网络出版日期**: 2014-05-16

基金项目: 国家自然科学基金(60927007,61227016,61001114,61205142)

作者简介: 李 璞(1986—),男,博士研究生,主要从事混沌激光应用方面的研究。E-mail: lipu8603@126.com

导师简介: 王云才(1965—),男,博士,教授,主要从事混沌激光产生与应用及光通信等方面的研究。

E-mail: wangyc@tyut.edu.cn(通信联系人)

在保密通信领域,产生安全可靠的随机数(又称为密钥)关系到国防安全、金融稳定、商业机密和个人隐私等众多方面。香农(Shannon)的理论研究证明,只要保证所使用的随机数或密钥是完全随机的,且与所要加密的信息长度一致并一次使用,那么它就是完全不可破解、绝对安全的[1]。在现代数字通信中,光纤通信波分复用(WDM)系统单信道速率已达10 Gb/s,并正向40 Gb/s发展,要实现这种绝对安全的"一次一密"保密方案,就要求所产生的随机数不可预测,且码率不低于现有光通信的信息传输速率。

随机数发生器可分为两类:伪随机数发生器和物理随机数发生器。伪随机数发生器是通过对一些算法赋予不同的种子,可以用计算机便捷地生成具有一定周期、快速(码率达Gb/s量级)的随机数。但伪随机数存在两大缺点:一旦算法与种子被破解,则密钥不仅可以复制、甚至可以预测;产生的随机序列长度有限,存在周期性。随着计算能力的不断提高,以伪随机数为密钥被破解的事件层出不穷[2]。即使是在对安全性要求不高的大规模蒙特卡罗模拟中,伪随机数的应用也可能导致系统化的错误[3]。

而物理随机数发生器可以保证科学计算的准确性及保密通信的安全性。它利用自然界物理熵源的微观量子机制或宏观随机现象产生出无法预测、非周期的随机数。传统的物理随机数发生器多利用电阻热噪声[4]、振荡器相位噪声[5]、单光子随机性[6-7]及混沌电路[8]等来提取随机数,但受限于这些熵源的带宽,其码率有限(典型码率处于Mb/s量级),距离现代信息的传输速率有很大差距。

近年,伴随着新型宽带光子熵源(如放大的辐射噪声[9]、激光相位噪声[10]、混沌激光[11]等)的出现,研究学者提出了众多高速物理随机数的实现方案。其中,混沌激光由于其高带宽、大幅度、易集成等特性,引起了人们的极大关注。自2008年日本埼玉大学Uchida等[11]证实采用混沌半导体激光器可产生速率达Gb/s量级的物理随机数之后,又涌现出了大量基于混沌激光的高速物理随机数产生方案,或采用不同结构的混沌光源以改善熵源特性、或改进后续处理方法以获得更高的随机码产生速率,或两者兼而有之[12-31]。

本文针对已报道的基于混沌激光产生高速物理随机数的方案进行了综述,从随机码速率、实现难易程度、系统稳定性等角度比较了各方案的优劣,归纳总结了当前研究热点,并指出了未来的可能发展方向。

2 当前研究现状

根据各方案采用的技术手段不同,将混沌物理随机数发生器划分为了两大类:基于光电子技术和基于全光技术的方案。下面将沿着这一思路,逐步对混沌物理随机数发生器各方案进行展开。

2.1 基于光电子技术的方案

基于光电子技术的方案是指用快速光电转换器将混沌激光信号转换为电信号,进而在电域内完成随机数提取的实现方案。按照提取随机数时采用模数转换器(ADC)种类的不同,再将基于光电子技术的产生方案进一步细分为基于1位ADC提取技术和基于多位ADC提取技术的方案。具体如下:

2.1.1 基于1位ADC的随机数提取方案

2008年,Uchida课题组实验证实[11]:两个独立的光反馈型混沌激光器(laser 1、laser 2)发出的光信号经快速光电转换后,产生两路相应的混沌电信号;继而,它们被各自对应的1位ADC(1-bit ADC 1、1-bit ADC 2)比较量化后,产生两组独立的二进制码序列。这两组二进制码再经一异或门(XOR)处理,最终可得到实时速率达1.7 Gb/s的物理随机码序列,质量满足国际随机数测试标准NIST及Diehard。具体实验装置如图1所示。图中SL表示半导体激光器;FC表示光耦合器;F表示光纤;VR表示可变光纤反射镜;ISO表示光隔离器;VA表示可调光衰减器;PD表示光电探测器;AMP表示电放大器,Th1和Th2分别表示两个ADC各自的比较阈值电压。该方案采用两个独立混沌激光器,是为了利用异或处理消除掉光反馈混沌激光器固有的弱周期性。Uchida等提出的这个方案标志着物理随机数发生器的速率可由Mb/s量级跃居到Gb/s量级,掀起了人们研究高速物理随机数发生器的热潮。

紧接着,该小组对此方案作了进一步改进,利用光子集成的混沌激光源(如图2所示)替换了图1中由分立光学元件构建的两个混沌激光器(laser 1和laser 2),获得了码率达2.08 Gb/s的物理随机码[12]。图2(d)中DFB表示分布反馈激光器,SOA表示半导体光放大器。该方案采用集成光源,为整个系统的小型化及实用化奠定了基础。

尽管以上两个方案在一定条件下可以输出高质量随机数,但仍存在缺陷:由于混沌信号的均值通常不

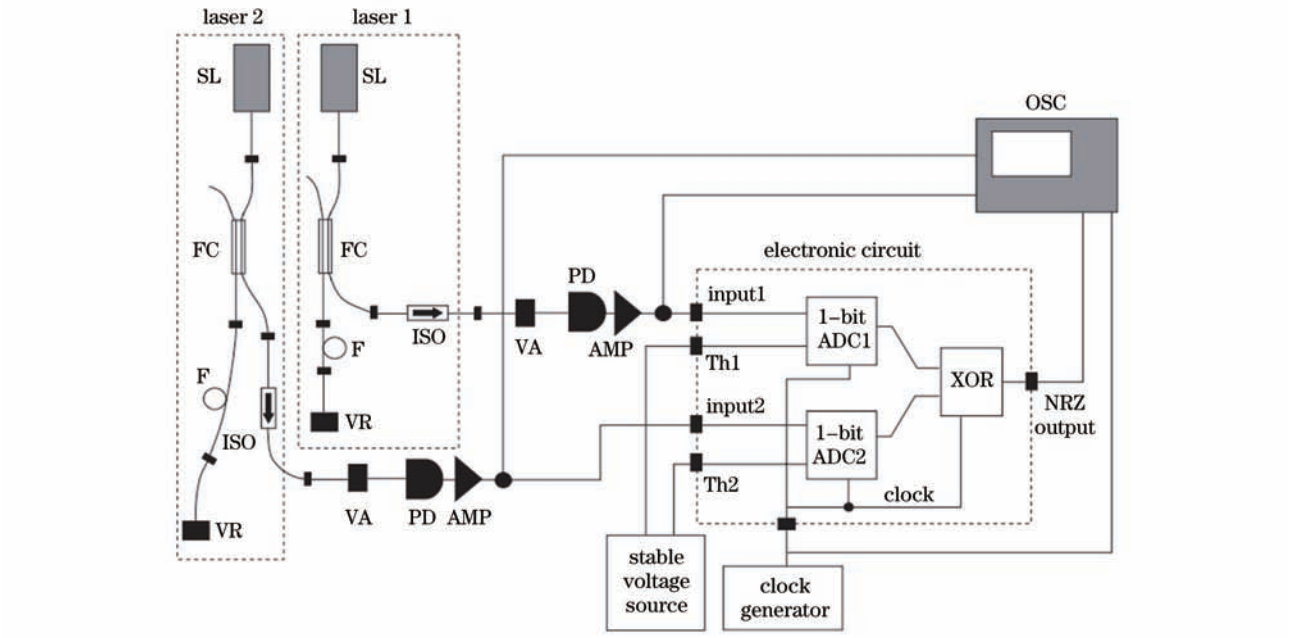

图1 Uchida课题组提出的物理随机数发生器方案

Fig. 1 Physical random number generator from Uchida′s group

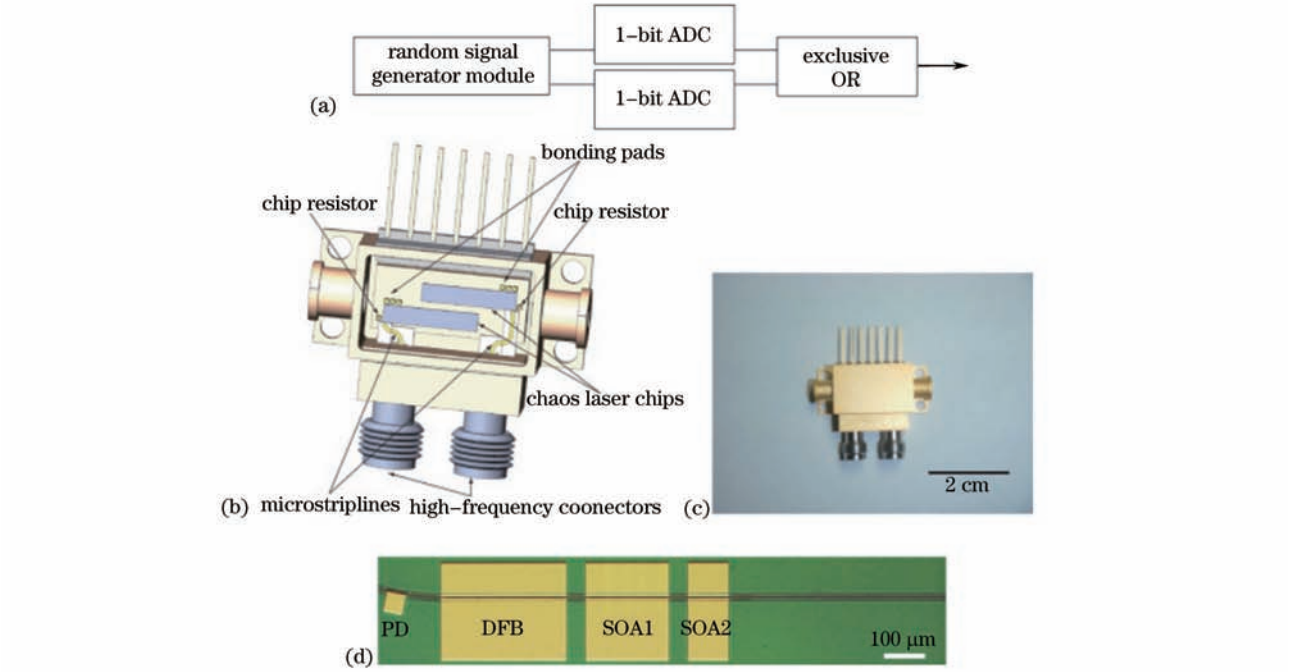

图2 Uchida课题组光子集成混沌激光源。(a) 随机数产生原理框图;(b) 光子集成混沌激光源内部构造和(c)外部图片;(d)内部光反馈混沌激光芯片构造

Fig.2 Photonic integrated chaotic laser (PIC) from A.Uchida et al. (a) Schematic of random number generator; (b) internal and (c) external structure of PIC; (d) chaotic chip structure

稳定,其方案在用1位ADC量化时,必须不断进行精密的阈值调节,这对于实际应用是很不利的。

针对这一问题,本课题组于2012年提出了延迟差分比较方案,如图3(a)所示[13]。图中PC表示偏振控制器,40/60表示40/60光耦合器,OI表示光隔离器,VOA表示光衰减器,T表示T型连接器,Delay表示电延迟线,OSC表示示波器,TODL表示可调光延迟线,XOR表示异或门。利用差分比较器对宽带混沌信号延迟作差,极大改善混沌信号的对称性,使其均值稳定在0;在时钟控制的触发器作用下,完成对该对称信号的量化;经后续异或处理后,可获得高质量随机数。该方法能有效避免精确的阈值电压调节,提高了系统抗干扰

能力。

与此同时,我们另一项研究证实,单个混沌激光器经50/50耦合器等分成两路,每路信号经各自1位ADC转换成二进制码后,通过一定条件下的延迟异或处理,可彻底消除光反馈混沌激光器弱周期性的影响,进而产生高质量的物理随机数[14]。具体实验装置如图3(b)所示。这就进一步精简了基于1位ADC随机数提取方案中所需混沌激光器的数目(即由至少两个减少到了一个),降低了系统复杂度,并能节约成本。

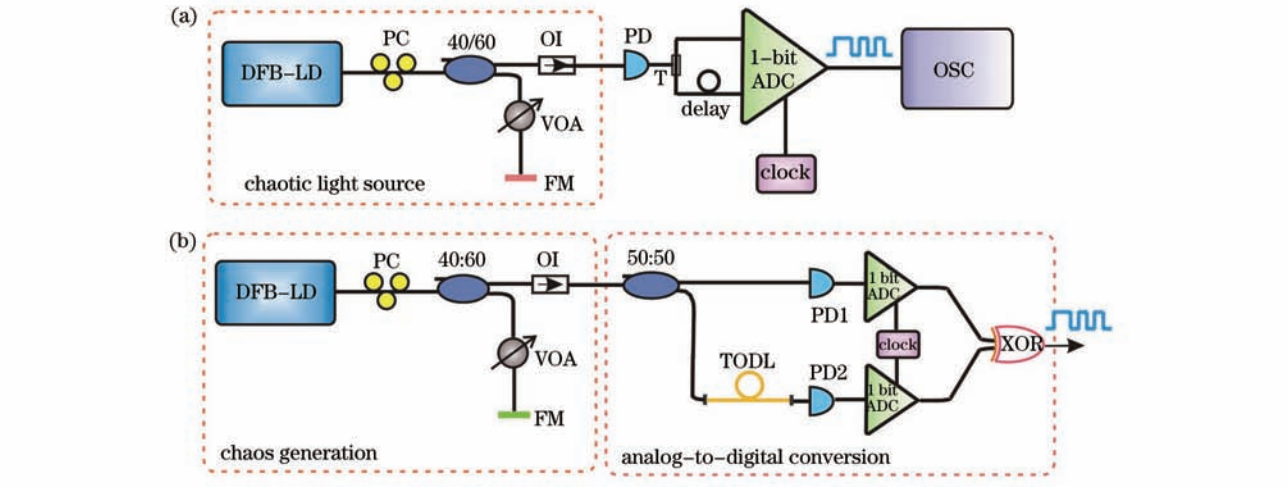

图3 本课题组提出的两个随机数产生方案。(a)延迟差分比较方案;(b)延迟异或方案

Fig.3 Two methods for random number generation from our group. (a) Scheme based on delay differential comparison; (b) scheme based on delay XOR technique

2013年,基于以上两项研究发现,本课题组成功研发了一台基于混沌激光的实时、高速物理随机数发生器样机(如图4所示)[15],其码率在0~4.5 Gb/s之间连续可调,可连续稳定工作至少24 h[15]。图4(a)是装置原理图,其中LD表示半导体激光器,OC表示光环形器,COM表示比较器,DFF表示触发器,CLK表示时钟。

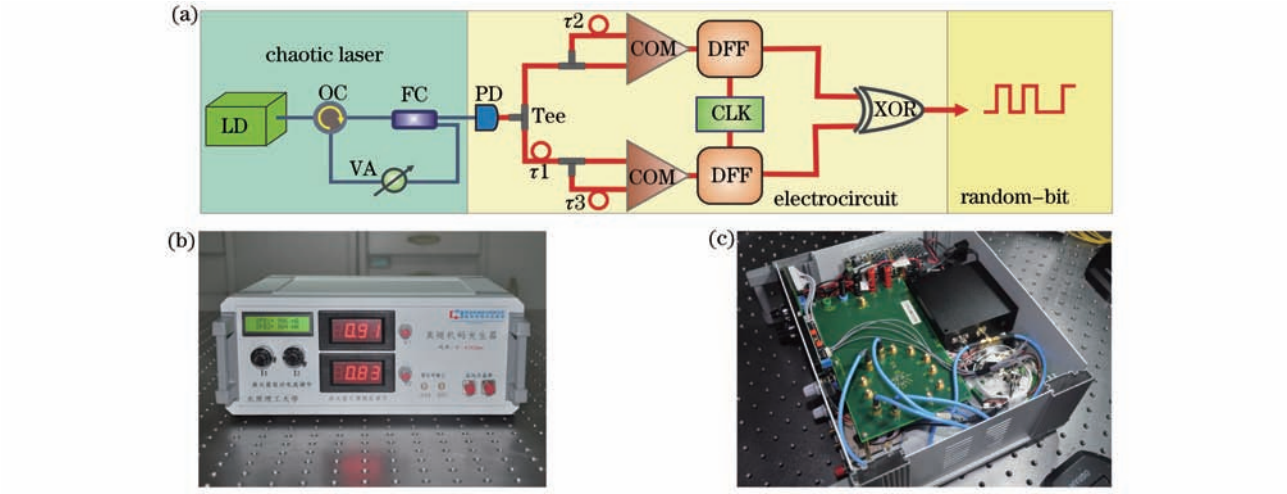

图4 本课题组研制的4.5 Gb/s物理随机数样机。(a)内部原理图;(b)样机外观照片;(c)样机内部构造照片

Fig.4 Prototype of 4.5 Gb/s physical random bit generator from our group. (a) Schematic block diagram; (b) external and (c) internal photograph of the prototype

2.1.2 基于多位ADC的随机数提取方案

为了更大幅地提高随机数发生速率,研究学者们又陆续提出了各种各样的基于多位ADC的随机数提取方案。不同于1位ADC(一个采样点仅对应一位0码或1码),多位ADC可将每个采样点量化为多位二进制码,这就大大提高了采样点信息的利用率。

2009年,以色列巴伊兰大学Reidler等[16]提出利用8位ADC对混沌信号进行量化编码提取随机数的设想,并进行了离线证实。具体地,单个半导体激光器在空间光反馈作用下产生强度随机起伏的混沌光信号,

如图5(a)所示。图中的BS、ND和M分别表示光分束器、中性密度滤波器及镜子。后续的随机数提取过程如图5(b)所示,混沌信号经光电转换器变成电信号;该信号输入一个2.5 GHz时钟触发下的8位ADC(8-bit A/D)中,每个采样点被编码成8位二进制码;再经过一个移位缓存器(Buffer),通过对相邻的两个采样点对应的8位二进制码进行差分处理,保留最低有效位(LSBs)5位,最终获得了等效速率为12.5 Gb/s(2.5 GS/s × 5 LSBs)的随机数序列。需要特别指出的是,该方案将物理随机码产生速率提高到了10 Gb/s量级;不仅如此,它还能克服混沌激光信号分布不对称的缺陷,避免了精确阈值调节,极大增强了系统稳健性。随后,该小组于2010年进一步对此方案进行了改善,通过增加后续差分处理的级数,使得码率可有效突破混沌激光信号带宽的限制[17]。其研究结果表明,当增加差分处理级数至16时,采样率设为20 GS/s,保留最低有效位15位,可获得等效速率达300 Gb/s(20 GS/s×15 LSBs)的超高速物理随机数。

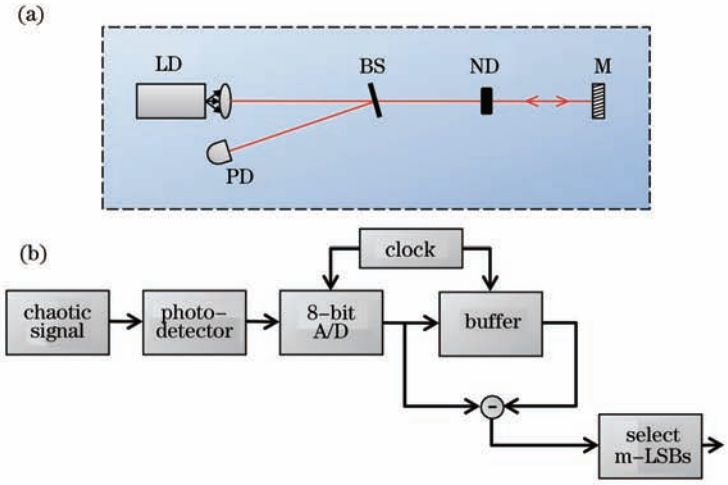

图5 I. Reidler等提出的基于8位ADC的随机数提取方案。(a)混沌激光器原理图;(b)随机数提取方法

Fig.5 Random number extraction scheme based on a 8-bit ADC proposed by I. Reidler *et al.*. (a) Chaotic laser structure; (b) method for random number extraction

尽管上述基于8位ADC提取随机数的方案有着如此众多的优势,但它们采用的混沌激光器是基于外部空间光反馈方式构建的,因而系统对外部环境的变化仍会敏感。鉴于此,2010年希腊雅典大学Argyris等[18]

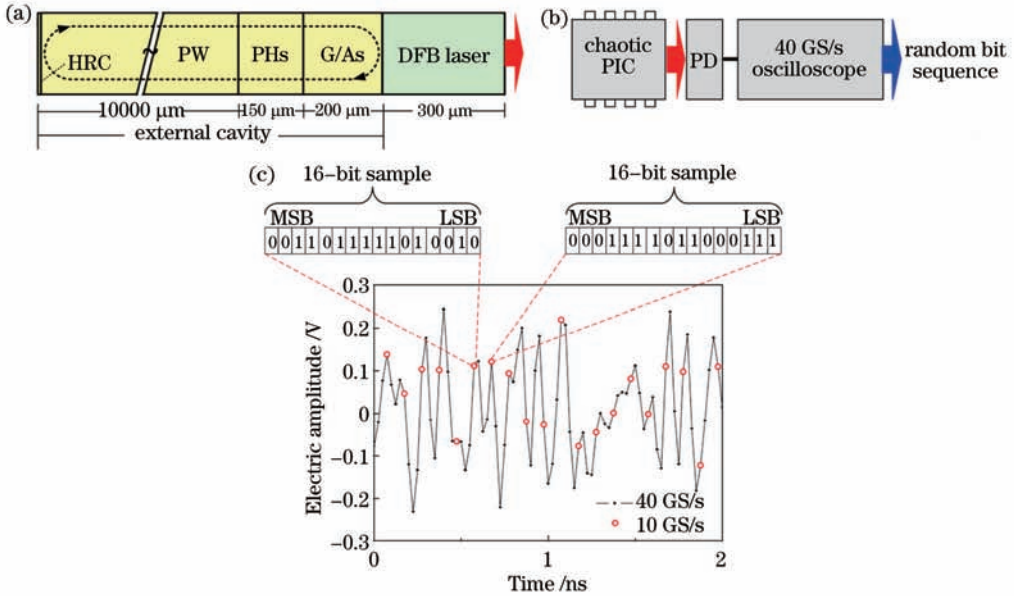

图6 A. Argyris等提出的基于16位ADC提取随机数的方案。(a)光子集成混沌激光器;(b)实验装置示意图;(c)随机数提取方法。

Fig.6 Random number extraction scheme based on a 16-bit ADC from A. Argyris *et al.*. (a) Photonic integrated chaotic laser; (b) experimental setup; (c) method for random bit extraction

利用光子集成混沌激光器作为熵源来提取随机数，以期增强混沌系统稳定性。而且在其方案中，他们还提出了一种基于多位ADC提取随机数的新技术，简化了后续处理的复杂度，具体方案如图6所示。光子集成的微型混沌激光器输出的混沌信号，经光电转换器转换为电信号，采用16位ADC进行量化，并在10 GS/s采样时钟触发下，直接保留最低有效位14位，无需其他后续处理，可产生等效速率为140 Gb/s(10 GS/s×14 LSBs)的高质量随机码。

除此以外，人们还采用其他类型的混沌激光器(如偏振反馈式混沌激光器、光注入型混沌激光器、带宽增强型混沌激光器、光反馈半导体环形激光器等)在不同程度上改善熵源随机特性、提高系统性能。而且，在这些方案中不乏新的后续处理技术(如并行处理技术、“过采样”技术等)以产生超高速物理随机数序列。

例如，西班牙巴利阿里大学Oliver等[19]采用偏振旋转反馈方式构建的混沌半导体激光器作为物理熵源(如图7所示)，在选择合适的偏转角度和反馈强度时，采用类似于Argyris等的随机数提取办法，利用采样率为1 GS/s的8位ADC量化编码，直接保留最低有效位4位，无需其他进一步的后续处理过程，获得了等效速率为4 Gb/s(1 GS/s×4 LSBs)的随机码。于2013年又进一步证实了：如果换做更高位ADC，在适当条件下该方案的速率可进一步提升至480 Gb/s，几乎逼近信息理论极限[20]。图中ATT和FM分别对应光衰减器和法拉第转镜。

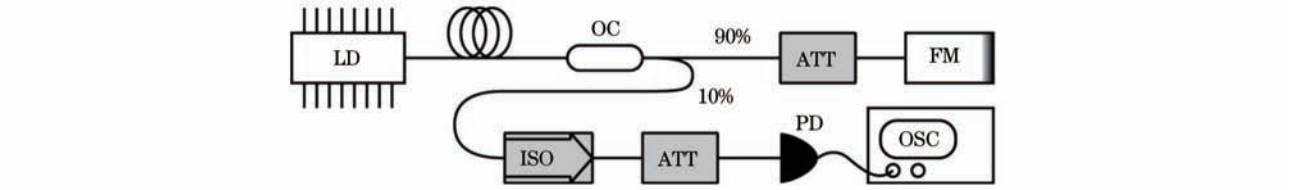

图7 N.Oliver等采用偏振旋转反馈半导体激光器提取随机数的实验装置图

Fig.7 Experimental setup for random number generation based on a semiconductor laser with polarization-rotated feedback from N.Oliver *et al.*

2011年，我国西南大学夏光琼小组采用光纤连接的互注入半导体激光器产生混沌激光信号亦可大大改善系统的稳定性，并能获得高速随机数[21-22]。采用的互注入半导体激光器如图8(a)所示，两个半导体激光器(SL1和SL2)在各自的温度控制器(TC)和电流驱动器(CC)作用下，经过各自对应的10/90耦合器相互注入对方激光腔中，利用可调光衰减器(VA)和偏振控制器(PC)合理调节互注入强度和偏振态，最终可产生10 GHz高带宽混沌激光信号，经光隔离器(OI)输出。进一步，该信号经光电探测器(PD)转换为电信号，由示波器记录。通过合适的后续处理过程可以获得高速随机数，如图8(b)所示。该小组研究工作证实：1)当

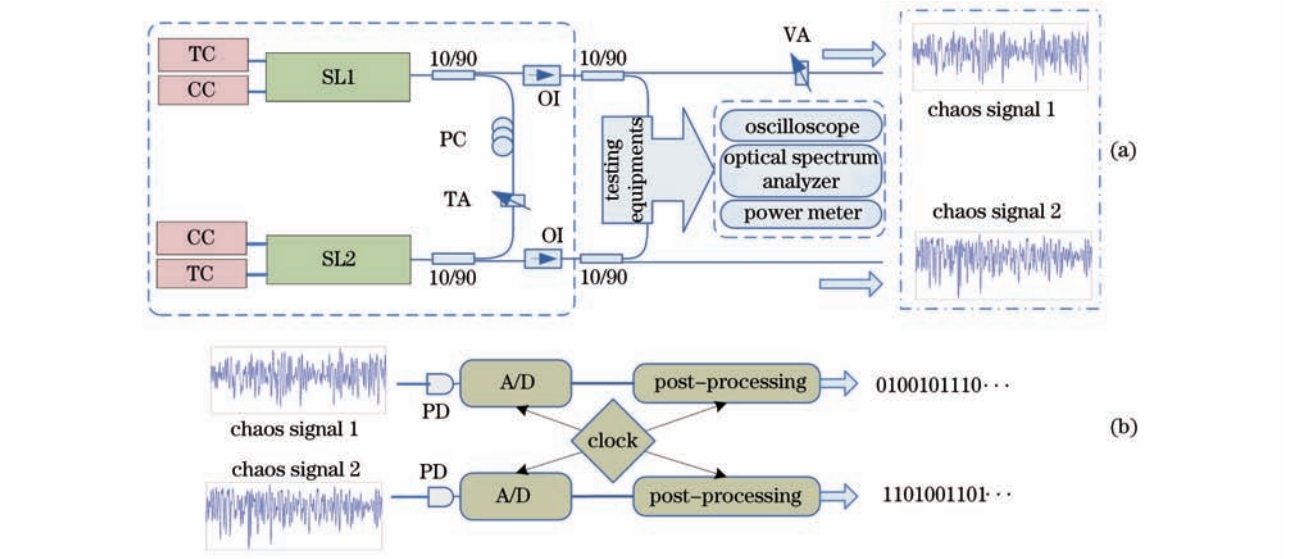

图8 夏光琼小组提出的基于互注入混沌激光器的8位ADC随机数提取方案

Fig.8 Scheme for random number generation based on an 8-bit ADC and mutually injected chaotic lasers from the group of Guangqiong Xia

采样率不高于混沌信号带宽时，即在采样率为2.5 GS/s的8位ADC和移位寄存器作用下，对相邻采样点对应的二进制码进行异或处理，保留最低有效位7位，离线获得了等效速率17.5 Gb/s（2.5 GS/s×7 LSBs）的随机码[21]；2）同时采用互注入半导体激光器的两路信号作为熵源，在采样率为2.5 GS/s的8位ADC和移位寄存器作用下，对相邻采样点对应的二进制码进行异或处理，保留最低有效位4位，离线获得了等效速率10 Gb/s（2.5 GS/s×4 LSBs）的“并行”随机数[22]。

2012年，比利时布鲁塞尔自由大学Nguimdo等[23]指出光反馈混沌半导体环形激光器输出的混沌信号作为熵源，可缩小熵源尺寸，具有很高的抗干扰能力，且能达到很高速率。如图9所示，光反馈混沌半导体环形激光器（SRL）可以同时产生两个模式的混沌信号，分别为顺时针模式（CW）和逆时针模式（CCW）。两路混沌信号分别经各自对应的光电探测器（PD）和8位ADC（采样率为10 GHz）量化为两束二进制序列，经异或门（XOR）处理后，保留最低有效位数4位，最终获得一路高速真随机码序列，等效速率可达40 Gb/s（10 GHz×4 LSBs）。

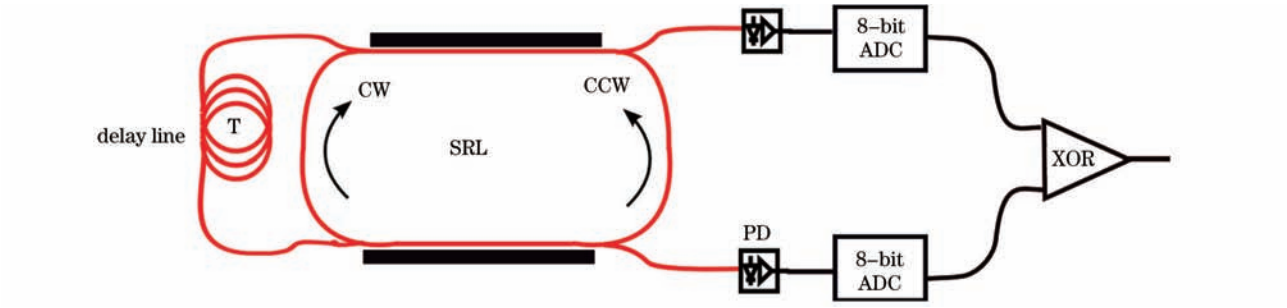

图9 R. M. Nguimdo等提出的基于光反馈半导体环形激光器的8位ADC随机数提取方案

Fig.9 Scheme for random number generation based on an 8-bit ADC and semiconductor ring laser with optical feedback from R. M. Nguimdo *et al.*

2012年，香港城市大学陈仕俊博士等[24]指出利用光注入半导体激光器产生的混沌激光将不再具有光反馈混沌激光器固有的那种弱周期性，更有利于高质量随机码的产生；并证实，当混沌信号带宽有限时，采用“过采样”技术也是可以获得高速随机码的。具体方案如图10所示：主激光器（ML）发出的激光经光衰减器（VA）和光环形器（CIR）注入从激光器（SL）可以获得无周期混沌信号输出，经光隔离器（OI）、光电转换器（PD）、放大器（A）及带宽为1.5 GHz的前置放大器（front end）作用后，被利用的混沌信号的实际带宽不高于1.5 GHz。在过采样率为10 GS/s的8位ADC（10 GHz ADC）作用后，选取相邻采样点的最低有效位3位，进行异或逻辑处理（XOR），可得到等效速率为30 Gb/s（10 GS/s×3 LSBs）的随机码。2013年，该小组又结合并行处理和外差检测技术，仍以光注入混沌激光器作为熵源，证实了100 Gb/s和200 Gb/s高速随机码的可行性[25]。

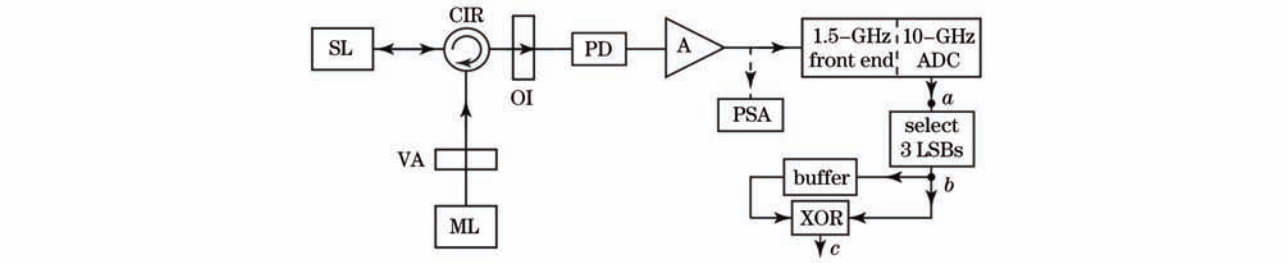

图10 香港城市大学陈仕俊博士等提出的基于8位ADC的随机数产生方案

Fig.10 Random number generation method based on an 8-bit ADC proposed by S. Chan *et al.*

事实上，除了采用过采样和并行处理等后续处理方式以外，直接对熵源带宽进行加强是一种更直接的提高速率方式。如2010年日本拓殖大学Hirano等[26]证实，将光反馈半导体激光器输出的混沌信号注入到另一个半导体激光器，在一定的注入强度和频率失谐条件下，混沌激光器的带宽可由9 GHz增强到16 GHz，这样就能允许多位ADC工作在非过采样的条件下获得超高速率随机数。具体工作过程：将该混沌激光信号分作两路（两路之间有一定延迟），各自经过一8位ADC（采样率为12.5 GS/s）量化编码后，可获得两路二进制码序列；通过对两路二进制码序列进行异或处理，并保留最低有效位6位，获得了码率达75 Gb/s（12.5 GS/s×6 LSBs）的物理

随机数。图11(a)和(b)分别是具体实验装置及后续处理过程示意图。

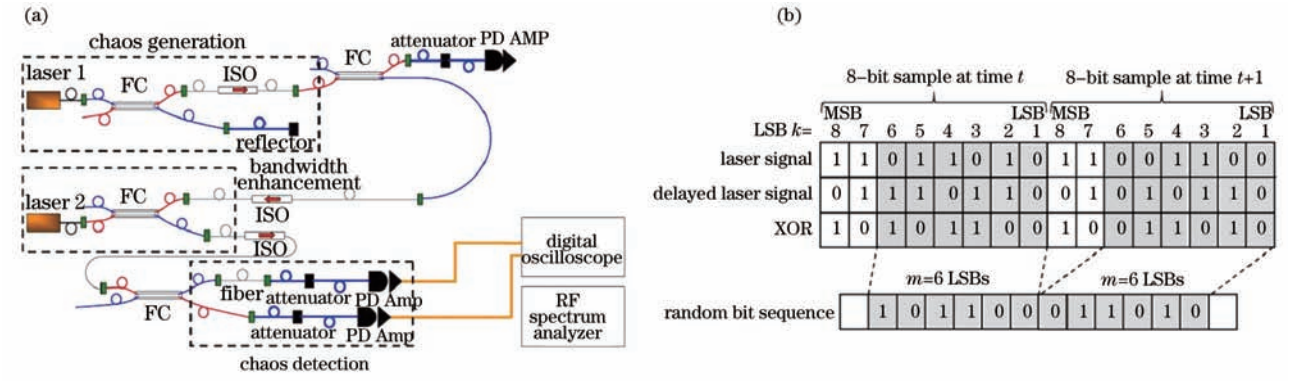

图11 Hirano等基于带宽增强型混沌信号产生高速随机数的方案。(a)实验装置图; (b)后续处理流程图

Fig.11 Fast random number generation scheme based on bandwidth-enhanced chaotic signal from K. Hirano *et al*.. (a) Experimental setup; (b) post-processing method

可以预见,如果将带宽增强型混沌熵源与"过采样"技术相结合,将能够实现更高速率的物理随机码产生。2012年,Uchida小组[27]利用不高于16 GHz的带宽增强型混沌信号作为物理熵源,在采样率为50 GS/s的8位ADC量化编码后,进行延迟'颠倒'异或处理,保留全8位,最终获得了等效速率达400 Gb/s(50 GS/s×8 LSBs)的物理随机码。具体方案流程如图12所示。

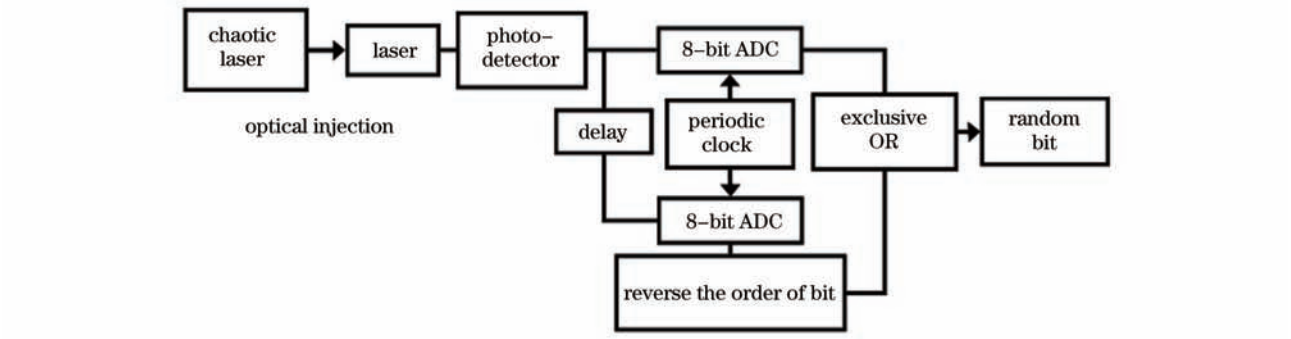

图12 Uchida课题组结合带宽增强型混沌与过采样技术产生超高速物理随机码的原理框图

Fig.12 Schematic diagram for ultra-fast random number generation combing enhanced-bandwidth chaos and over-sampling technique from A. Uchida's group

必须指出的是,尽管基于多位(8位或16位)ADC提取随机数的方案可以获得超高速率的随机数序列,但目前这些方案的证明过程往往是先利用高速示波器对混沌信号进行采集存储,再进行离线的理论分析、论证,其最终码率事实上是采样时钟频率与保留最低有效位数的简单数学乘积。换言之,这些超高码率还只是一些理论预期,而非实际输出的真实随机码码率。

实际上,基于以上多位ADC的方法构建一个真正的实时随机码发生器存在一定难度。一方面,基于多位ADC获取几十甚至几百Gb/s的高速随机数,需选用超高带宽的电ADC、超高带宽的异或门以及缓存器,这势必面临"电子瓶颈"的限制。如目前响应带宽最高的电ADC当属日本富士通公司的CHAIS ADC(http://www.fujitsu.com/downloads/MICRO/fma/pdf/56G_ADC_FactSheet.pdf),其带宽处于15 GHz附近,已几乎接近硬件带宽理论极限。另一方面,在如此高的工作速率下(几十Gb/s或几百Gb/s),要保持关键部件(如电时钟、电多位ADC、移位寄存器或缓存器)的精确同步也是一项不易完成的任务。

2.2 基于全光技术的方案

不同于基于光电子技术的方案,全光技术方案无需光电转换,直接在光域中对混沌信号进行量化编码,产生物理随机数序列。根据所采用混沌熵源类型的不同,全光混沌物理随机数发生器又可进一步细分为基于连续混沌信号和基于离散混沌信号的全光混沌物理随机数发生器。

2.2.1 基于连续混沌信号的全光物理随机数发生器

与前面介绍的光电子技术类似,该种随机数发生器也是利用光反馈或光注入半导体激光器产生的连续

混沌信号作为物理熵源。

2010年,本课题组提出并理论论证了基于混沌激光的全光物理随机数发生器[28]。具体方案如图13所示。其中HNLF、BPF和CW分别高非线性光纤、带通光滤波器和连续光信号。利用光注入和光反馈相结合的方式构建出带宽增强型混沌激光器,其输出的混沌信号带宽可达10 GHz以上。该混沌信号输入由Sagnac干涉仪构成的光纤型全光采样器产生出幅度随机起伏,但重复频率恒定的光脉冲序列;进一步,该脉冲序列经过一个四分之一波长相移型DFB激光器(λ/4 DFB)构成的全光比较器,被量化为一串二进制序列。最后,经过光纤型全光异或门处理,可获得10 Gb/s速率的全光随机数,如图13所示。该速率主要受限于混沌信号的带宽。

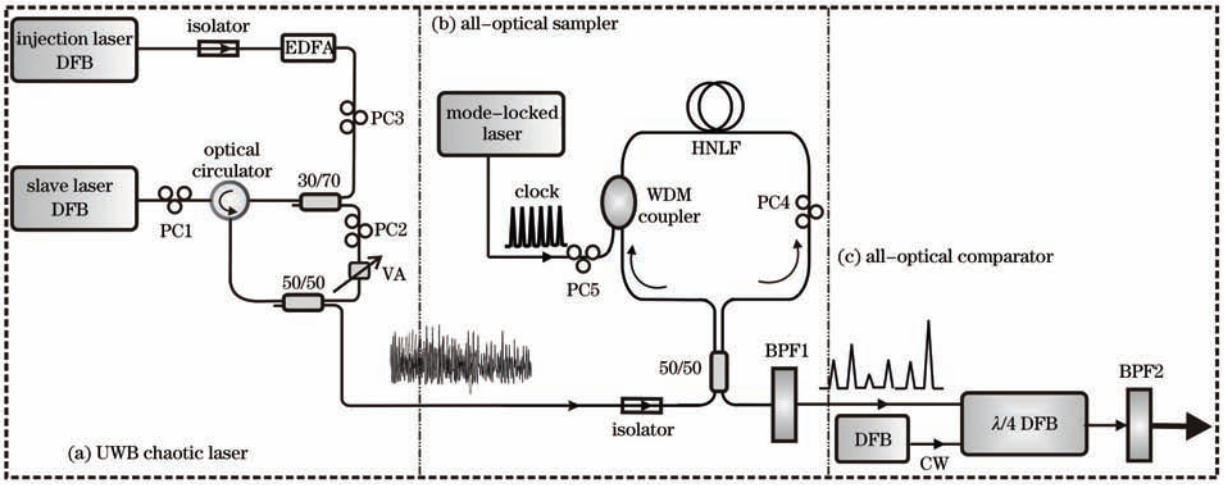

图13 本课题组提出的基于连续型混沌信号的全光随机数发生器示意图

Fig.13 Schematic diagram of all-optical random number generator based on enhanced-bandwidth continuous chaotic laser from our group

同年,鉴于混沌激光信号相干性差等不利因素的存在,对上述方案作了一定程度上的改善,如图14所示[29]。在改进型方案中,利用电光调制器(MZ)替换了原方案中的Sagnac干涉仪,直接将混沌信号的幅度信息调制到一串光时钟脉冲(MLL)上,等效于采样的目的。另一个改善之处在于,本方案中相移DFB激光器被用作全光触发器,兼具比较和保持两项功能,因此可以实现随机码占空比的连续可调,方便实际应用。其中3 dB表示3dB光耦合器,EDFA表示掺铒光纤放大器,FDL表示光纤延迟线,WDM表示WDM耦合器。

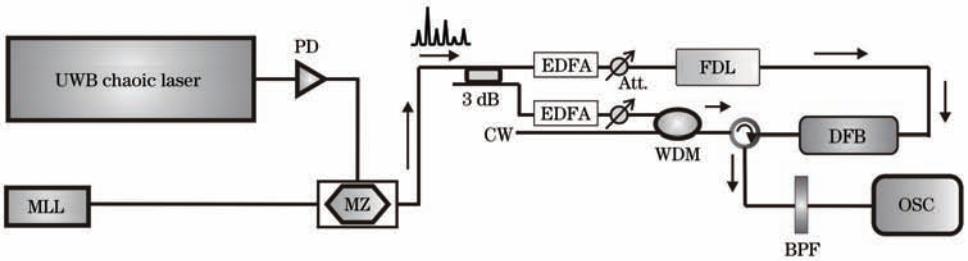

图14 基于连续型混沌信号的改进型全光随机数发生器装置示意图

Fig.14 Improved all-optical random number generator based on enhanced-bandwidth chaotic signal

2.2.2 基于离散混沌信号的全光物理随机数发生器

通过上面的分析,可以看出上述所有方案中采用的混沌信号均是连续型混沌信号。要想成功提取随机数,必须经过采样和量化两个单元技术。这就造成系统复杂度较高,而且采样过程中时钟抖动的存在,可能会引起信噪比的劣化。当速率高达Gb/s时,这个影响将变得极为显著。

针对这一问题,于2012年提出并论证了基于偏振旋转锁模光纤环形激光器(MLFRL)输出的离散混沌激光的全光物理随机数发生器[30]。所谓离散型混沌信号是指一串幅度随机起伏、重复频率却固定不变的光脉冲序列。具体方案如图15(a)所示。一个偏振旋转光纤环形激光器,在合适的抽运功率下,可以产生脉冲幅度混沌,如图15(b)所示。该信号直接输送到相移DFB激光器构成的全光触发器,量化成高质量物理随机

数。该方案无需采样和异或处理过程,大大简化了系统。但由于光纤激光器的环长较大,限制了脉冲的重复速率,所以利用该方案仅获得了Mb/s量级的随机数序列输出。其中PDI表示偏振相关隔离器。

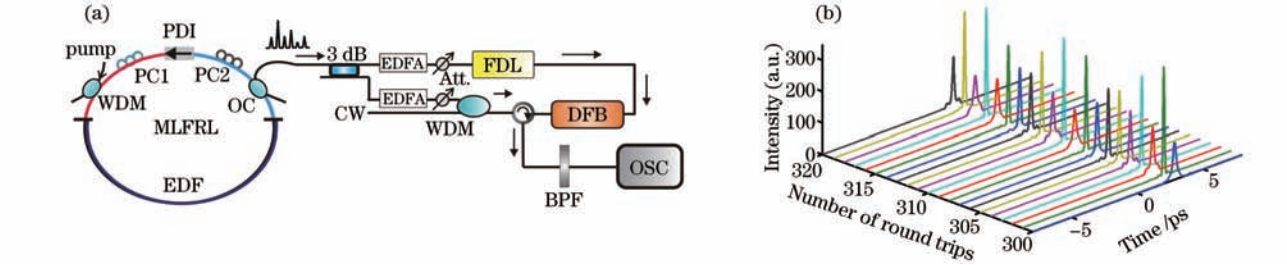

图15 基于偏振旋转光纤环形激光器的全光随机数发生器。(a) 装置示意图; (b)脉冲幅度混沌时序图

Fig.15 All-optical random number generator based on a polarization-rotated fiber ring laser. (a) Schematic diagram of setup; (b) time trace of pulse amplitude chaos.

2013年,本课题组对方案作了改善以提高码率,具体如图16所示[31]。利用光注入双区半导体激光器(two-section semiconductor laser)输出的混沌自脉动信号作为熵源,替代了光纤环形激光器。该种混沌自脉动也属于离散混沌信号,即幅度随机起伏、重复频率恒定的光脉冲序列。与被动锁模激光器不同的是,该混沌信号的重复速率可达GHz量级。在该方案中,通过合理调节体结构的双区激光器各外部参数,其速率可达10 GHz,经过全光触发器的作用后,最终产生了10 Gb/s的高速真随机码,如图17所示。这里指出,图16中的标注含义与图14及15标注含义相同。

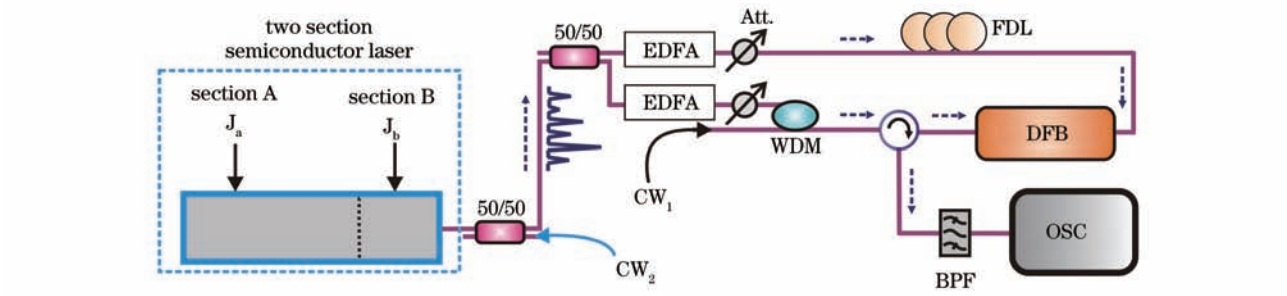

图16 基于光注入双区半导体激光器的全光随机数发生器装置示意图

Fig.16 Schematic diagram of all-optical random number generator based on a two-section semiconductor laser with optical injection

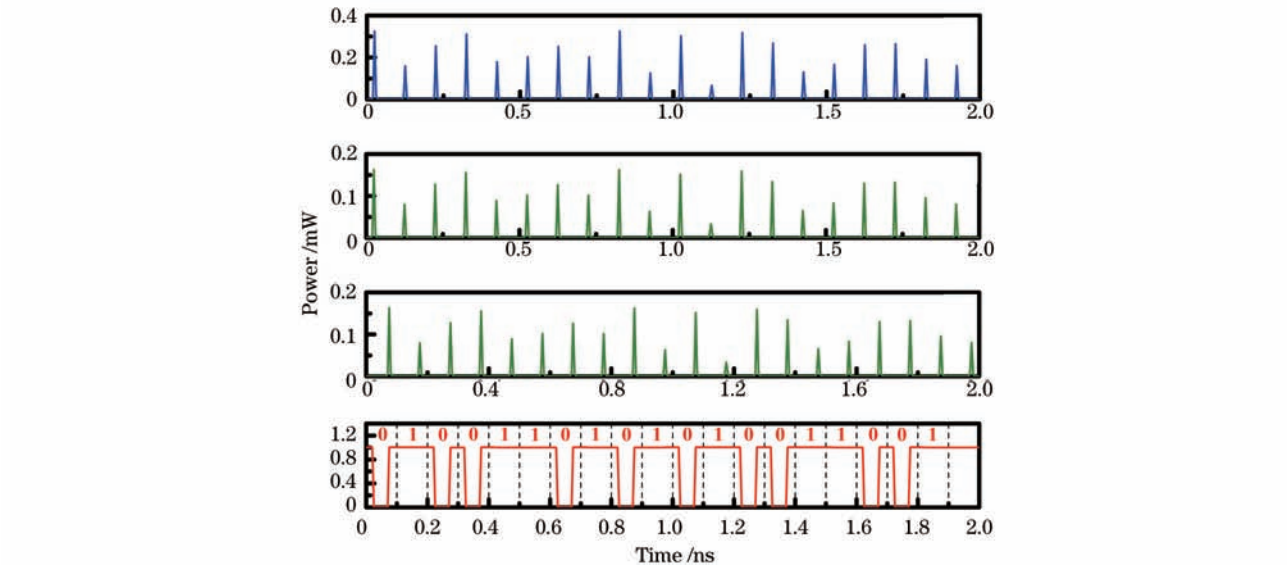

图17 基于光注入双区半导体激光器的全光量化结果。(a)混沌自脉动时序; (b) set信号;(c)reset信号;(d)随机码输出

Fig.17 All-optical quantization results based on a two-section semiconductor laser with optical injection. (a) Chaotic self-pulsation time-series; (b) set signal; (c) reset signal; (d) random bit time-series

这里指出,当前全光随机数发生器的速率主要受限于连续混沌的带宽或离散混沌重复频率,通过改善熵源或采用新的后续处理办法可以获得进一步提高。比如,上述光注入双区激光器的重复速率之所以处于10 GHz附近,是因为采用的双区激光器结构属于体结构。如果换做量子点结构,它有望达到Tb/s[32]。再如,上述方案中的全光量化器实质上均属于一位全光ADC。如果换做多位全光ADC[33],其速率将获得成倍的增加。

3 结 论

综上所述,发展稳定、高带宽的混沌激光源和提高随机码产生速率是目前混沌物理随机数发生器的研究热点。利用光子集成技术可解决混沌源的稳定性和小型化问题,但如何在如此微观尺度下进一步提高混沌激光的带宽仍有待开展深入研究。随着光纤通信 WDM 系统单信道速率已达10 Gb/s并向 40 Gb/s发展,要实现大容量高速光通信的无条件安全,就要求实时大量地产生高速随机数。目前大幅提高随机数产生速率的方法主要有两种:第一种基于光电子技术,采用超高速的多位ADC,在电域中对混沌激信号进行量化处理;第二种利用全光信号处理技术,无需光电转换,直接在光域中对混沌激光信号进行随机数的提取。第一种方法理论上存在多种可能性,但如何构建出一个真实系统是下一步有待解决的问题。实际构建过程中可能涉及的困难会很多。比如,如何规避实现过程中必然遇到的“电子瓶颈”限制问题;如何在超高速率条件下,实现各单元器件(如多位ADC、缓存器、异或门、并串转换等)的精确同步等。而第二种方案,其速率能克服电子瓶颈限制,只要熵源带宽足够高,有望实现几十Gb/s甚至Tb/s的突破。而且,全光方案还具有抗电磁干扰,产生的全光随机数可与光网络直接兼容等优点,因此呈现出诱人的发展前景,值得进一步研究。

参 考 文 献

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

2 Gisin N, Ribordy G, Tittel W, *et al*.. Quantum cryptography [J]. Reviews of Modern Physics, 2002, 74(1): 145-195.

3 Ferrenberg A M, Landau D P, Wong Y J. Monte Carlo simulations: Hidden errors from ‘good’ random number generators [J]. Phys Rev Lett, 1992, 69(23): 3382-3384.

4 Petrie C S, Connelly J A. A noise-based IC random number generator for applications in cryptography [J]. IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications, 2000, 47(5): 615-621.

5 Bucci M, Germani L, Luzzi R, *et al*.. A high-speed oscillator-based truly random number source for cryptographic applications on a Smart Card IC [J]. IEEE Transactions on Computers, 2003, 52(4): 403-409.

6 Ren M, Wu E, Liang Y, *et al*.. Quantum random-number generator based on a photon-number-resolving detector [J]. Phys Rev A, 2011, 83(2): 023820.

7 Wei W, Guo H. Bias-free true random-number generator [J]. Opt Lett, 2009, 34(12): 1876-1878.

8 Stojanovski T, Pihl J, Kocarev L. Chaos-based random number generators-Part II: practical realization [J]. IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications, 2001, 48(3): 382-385.

9 Wei W, Xie G D, Dang A H, *et al*.. High-speed and bias-free optical random number generator [J]. IEEE Photon Technol Lett, 2012, 24(6): 437-439.

10 Qi B, Chi Y M, Lo H K, *et al*.. High-speed quantum random number generation by measuring phase noise of a single-mode laser [J]. Opt Lett, 2010, 35(3): 312-314.

11 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.

12 Harayama T, Sunada S, Yoshimura K, *et al*.. Fast nondeterministic random-bit generation using on-chip chaos lasers [J]. Phys Rev A, 2011, 83(3): 031803.

13 Zhang J Z, Wang Y C, Liu M, *et al*.. A robust random number generator based on differential comparison of chaotic laser signals [J]. Opt Express, 2012, 20(7): 7496-7506.

14 Zhang J Z, Wang Y C, Xue L G, *et al*.. Delay line length selection in generating fast random numbers with a chaotic laser [J]. Appl Opt, 2012, 51(11): 1709-1714.

15 Wang A B, Li P, Zhang J G, *et al*.. 4.5 Gbps high-speed real-time physical random bit generator [J]. Opt Express, 2013, 21(17): 20452-20462.

16 Reidler I, Aviad Y, Rosenbluh M, *et al*.. Ultrahigh-speed random number generation based on a chaotic semiconductor

laser [J]. Phys Rev Lett, 2009, 103(2): 024102.

17 Kanter I, Aviad Y, Reidler I, *et al*.. An optical ultrafast random bit generator [J]. Nature Photonics, 2010, 4(1): 58-61.

18 Argyris A, Deligiannidis S, Pikasis E, *et al*.. Implementation of 140 Gb/s true random bit generator based on a chaotic photonic integrated circuit [J]. Opt Express, 2010, 18(18): 18763-18768.

19 Oliver N, Soriano M C, Sukow D W, *et al*.. Dynamics of a semiconductor laser with polarization-rotated feedback and its utilization for random bit generation [J]. Opt Lett, 2011, 36(23): 4632-4634.

20 Oliver N, Soriano M C, Sukow D W, *et al*.. Fast random bit generation using a chaotic laser: approaching the information theoretic limit [J]. IEEE J Quantum Electron, 2013, 49(11): 910-918.

21 Tang Xi, Wu Jiagui, Xia Guangqiong, *et al*.. 17.5 Gbit/s random bit generation using chaotic output signal of mutually coupled semiconductor lasers [J]. Acta Physica Sinica, 2011, 60(11): 110509.
唐 曦, 吴家贵, 夏光琼, 等. 基于互注入半导体激光器的混沌输出产生 17.5 Gbit/s 随机码[J]. 物理学报, 2011, 60(11): 110509.

22 Wu J G, Tang X, Wu Z M, *et al*.. Parallel generation of 10 Gbits/s physical random number streams using chaotic semiconductor lasers [J]. Laser Phys, 2012, 22(10): 1476-1480.

23 Nguimdo R M, Verschaffelt G, Danckaert J, *et al*.. Fast random bits generation based on a single chaotic semiconductor ring laser [J]. Opt Express, 2012, 20(27): 28603-28613.

24 Li X, Chan S. Random bit generation using an optically injected semiconductor laser in chaos with oversampling [J]. Opt Lett, 2012, 37(11): 2163-2165.

25 Li X, Chan S. Heterodyne random bit generation using an optically injected semiconductor laser in chaos [J]. IEEE J Quantum Electron, 2013, 49(10): 829-838.

26 Hirano K, Yamazaki T, Morikatsu S, *et al*.. Fast random bit generation with bandwidth- enhanced chaos in semiconductor lasers [J]. Opt Express, 2010, 18(6): 5512-5524.

27 Akizawa Y, Yamazaki T, Uchida A, *et al*.. Fast random number generation with bandwidth- enhanced chaotic semiconductor lasers at 8×50 Gb/s [J]. IEEE Photon Technol Lett, 2012, 24(12): 1042-1044.

28 Li P, Wang Y C, Zhang J Z. All-optical fast random number generator [J]. Opt Express, 2010, 18(19): 20360-20369.

29 Wang Y C, Li P, Zhang J Z. Fast random bit generation in optical domain with ultrawide bandwidth chaotic laser [J]. IEEE Photon Technol Lett, 2010, 22(22): 1680-1682.

30 Li P, Wang Y C, Wang A B, et al.. Direct generation of all-optical random numbers from optical pulse amplitude chaos [J]. Opt Express, 2012, 20(4): 4297-4308.

31 Li P, Wang Y C, Wang A B, *et al*.. Fast and tunable all- optical physical random number generator based on direct quantization of chaotic self- pulsations in two- section semiconductor lasers [J]. IEEE J Sel Top Quantum Electron, 2013, 19(4): 0600208.

32 Rafailov E U, Cataluna M A, Sibbett W. Mode-locked quantum-dot lasers [J]. Nature Photonics, 2007, 1(7): 395-401.

33 Ikeda K, Abdul J M, Namiki S, *et al*.. Optical quantizing and coding for ultrafast A/D conversion using nonlinear fiber-optic switches based on Sagnac interferometer [J]. Opt Express, 2005, 13(11): 4296-4302.