高速小型化光量子随机数发生器

魏世海, 樊矾, 杨杰, 黄伟, 何远杭, 李大双, 徐兵杰*
西南通信研究所保密通信重点实验室, 四川 成都 610041

摘要 利用超辐射发光二极管的放大自发辐射噪声作为量子随机熵源,设计并实现了一种高速小型化光量子随机数发生器(QRNG)。为减小经典噪声及不完美器件对随机性带来的影响,基于对量子熵源的最小熵估计,在现场可编程门阵列中,对每次采集序列的相邻比特位进行异或操作,并截取低 12 位作为最终随机序列。该 QRNG 的随机数的实时产生速率达 1.4 Gb/s,可实时传输至上位机用户端,且能长时间稳定工作,具备实用化潜力。

关键词 量子光学; 量子随机数发生器; 小型化; 超辐射发光二极管; 放大自发辐射
中图分类号 TN29 **文献标识码** A **doi**: 10.3788/CJL201845.0512001

Ultrafast Compact Optical Quantum Random Number Generator

Wei Shihai, Fan Fan, Yang Jie, Huang Wei, He Yuanhang, Li Dashuang, Xu Bingjie
Science and Technology on Communication Security Laboratory, Institute of Southwestern Communication, Chengdu, Sichuan 610041, *China*

Abstract An ultra-fast compact optical quantum random number generator (QRNG) is designed and realized by using the amplified spontaneous emission (ASE) noise of superluminescent light-emitting diodes as the quantum random entropy source. In order to reduce the influences of the classical noise and imperfect devices on the randomness and based on the minimum entropy estimation for the quantum entropy source, the exclusive OR (XOR) operation of the adjacent bits for the each collected sequence is conducted and the 12-least-significant bit is intercepted as the final random sequence in the high speed field programmable gate array in real-time. The proposed QRNG with a real-time random number generation rate of 1.4 Gb/s can directly deliver to a host computer and work stably for a long time, which possesses the practical application potential.

Key words quantum optics; quantum random number generator; miniaturization; superluminescent light-emitting diode; amplified spontaneous emission
OCIS codes 270.5568; 060.5565; 270.5565

1 引 言

随机数在日常生活中扮演着十分重要的角色,并且被广泛应用于科学和工程领域中,如科学模拟和量子保密通信等。随着电子信息技术的迅猛发展和计算能力的大幅提高,人们对随机数的随机性要求越来越高。在科学模拟中,若采用的随机数的随机性不佳,科学模拟的结果可能是错误的。在量子保密通信系统中,随机序列的随机性和产生速率直接决定了系统的安全性及密钥分发速率。因此,如何得到高速、高质量的真随机数是目前研究的热点之一。

依据产生方式的不同,随机数发生器分为伪随机数发生器和物理随机数发生器。伪随机数发生器利用确定性的数学算法产生统计上近似随机的序列,其随机性完全取决于初始种子,不是真正不可预

收稿日期: 2017-10-31; **收到修改稿日期**: 2017-12-13
基金项目: 国家自然科学基金(61771439,61501414,61702469,61602045)、国家密码发展基金(MMJJ20170120)、四川省青年科技基金(2017JQ0045)、保密通信重点实验室基金(6142103040105)
作者简介: 魏世海(1991—),男,硕士研究生,主要从事量子保密通信方面的研究。E-mail: shellwei@163.com
导师简介: 李大双(1963—),男,博士,研究员,主要从事量子保密通信方面的研究。E-mail: lds629209@126.com
* **通信联系人**。E-mail: xbjpku@163.com

测的序列。物理随机数发生器基于不可预测的物理噪声，分为基于经典噪声的随机数发生器和基于量子噪声的随机数发生器。前者所采用的噪声源可以用经典物理进行完整描述，如电子元器件的热噪声[1]、振荡器的抖动[2]、时钟漂移[3]或混沌物理信号[4-8]，本质上是一种确定性的物理过程，产生的随机数不具有严格意义上的真随机性。量子随机数发生器(QRNG)基于量子力学内禀的随机性，是迄今唯一能产生理论上完全不可预知的随机序列的随机数发生器[6]。

目前，基于对设备的信赖程度，QRNG 被分为三类[6]。第一类为实用化 QRNG，第二类为自检测 QRNG，第三类为半自检测 QRNG[9-12]。实用化 QRNG 需要充分信任设备，通过建立适当的物理模型对设备进行描述，这类 QRNG 的随机数产生速率比较高。自检测 QRNG 能够在不信任设备的条件下获得随机数，但是产生速率较低。半自检测 QRNG 介于前两类发生器之间，通过信任部分设备获得较高的随机数产生速率。目前，基于激光光子技术的 QRNG 因其出色的性能和较为成熟的工艺而成为 QRNG 技术的主流。此类 QRNG 技术属于第一类 QRNG[13]，具体方式包括测量单光子(基于强衰减的激光脉冲)的随机透射和反射[14-15]，测量相干态(基于连续激光场)相邻两个光子的时间间隔[16-18]，测量相干态(基于强衰减的激光脉冲)的光子数[19-20]，测量激光的相位噪声[21-24]，测量真空涨落噪声[25-26]，测量放大自发辐射(ASE)的噪声[27-32]等。

然而，现有的实用化 QRNG 方案或产品在一定程度上都存在不足，包括产生速率不高、实时性不好以及实用性不佳等。首先，以瑞士 ID Quantique 公司生产的商用 QRNG 产品(Quantis)为例，其随机数的实时产生速率只能达到 4～16 Mb/s，难以满足量子密钥分发(QKD)系统的需求。其次，尽管部分文献报道的 QRNG 实验方案的随机数生成速率可达10 Gb/s量级，但绝大多数的实验结果都是离线的等价生成速率，无法进行实时应用。最近，中国科技大学的 Nie 等[21]基于激光相位噪声的测量，获得了高达 68 Gb/s 的随机数离线生成速率，并基于此方案实现了一个实时生成速率达 3.2 Gb/s 的 QRNG[22]，但是该 QRNG 结构较复杂、器件较多，且需要动态实时反馈控制，因而其小型化设计的难度相对较大。此外，为了获得更高速的 QRNG，ASE 噪声得到广泛研究并被用作 QRNG 的噪声源。瑞士日内瓦大学的 Martin 等[27]基于 ASE 噪声实现了实时产生速率为 1.25 Gb/s 的 QRNG；北京大学的 Xu 等[25]基于 ASE 噪声实现了离线生成速率达 40 Gb/s 的 QRNG。尽管二者都采用了 ASE 噪声作为量子熵源，但是前者采用的是后向抽运的掺饵光纤，后者采用的是超辐射发光二极管(SLED)；在噪声探测上，前者采用的是雪崩光电二极管(APD)，后者采用的是普通光电探测器(PD)；在电流信号放大上，前者采用的是跨阻放大，后者采用的是普通微波放大器(AMP)；在后处理算法上，前者采用现场可编程门阵列(FPGA)实时后处理数据，得到的是实时产生的随机数，而后者采用示波器采样，后处理算法是离线的。前者提出的 QRNG 更具有实用化价值，但是其结构相对复杂，不利于小型化；后者提出的 QRNG 主要用来评估 QRNG 的潜在性能，不能实时产生随机数。

因此，随机数产生速率、实时性以及小型化是 QRNG 设计和应用中的三个关键要素。为了获得具有实际应用价值的 QRNG，本文利用 SLED 的 ASE 噪声作为量子熵源，基于 FPGA 实现数据实时后处理，采用通用串行总线(USB)3.0 作为高速数据传输接口，设计实现了一种同时具有高速、实时、小型化、高稳定等实用化特征的 QRNG。该 QRNG 产生的随机数可直接传输至用户端，实时生成速率达 1.4 Gb/s，并且随机性能通过了 NIST、DIEHARD 以及 ENT 随机数检验包测试。

2　QRNG 的物理机理及实现方案

2.1　QRNG 的物理机理

QRNG 的基本物理架构如图 1 所示，包含了量子熵源、数据探测、数据采集以及数据后处理部分。SLED 是一种介于发光二极管和激光器之间的半导体器件。SLED 随机产生的自发辐射被耦合到波导进行放大，得到输出光场，其随机性体现为光场的强度噪声。SLED 的输出光强本质上来自于原子的自发辐射。当 SLED 中大量的原子以一定概率在不同的能级之间进行自发辐射时就会产生大量光子，光子通过波导耦合效应进入到介质中，经由介质的增益(材料增益、模式增益等)进行放大，最终在介质的端面上输出 ASE 光噪声信号。输出的 ASE 光信号由自发辐射和光增益共同决定。光增益是由介质决定的一个相对固定的过程，而自发辐射则是一个量子随机过程——不同原子发生自发辐射效应的概率是完全随机的[32]。从原理上讲，SLED 端面输出的 ASE 瞬时光功率也是随机的，因此SLED被认为是

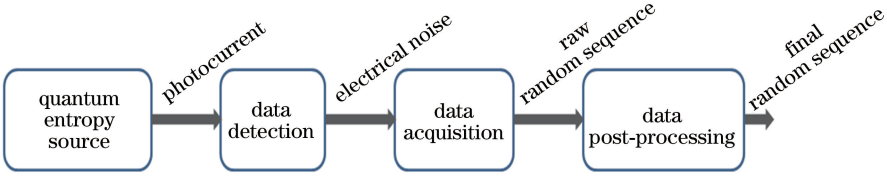

图 1　QRNG 的基本物理架构

Fig. 1　Basic physical infrastructure of QRNG

一种良好的物理噪声源[6,13]。

通过电学和光学方程建立 SLED 放大自发辐射源的数学物理模型，以描述自发辐射、波导耦合、增益放大、载流子的动态变化、法布里-珀罗腔等综合物理过程[32]。对于一个长度为 L、两个端面反射率分别为 r_1 和 r_2 的法布里-珀罗腔，有

$$P_L(\omega)\Delta\omega=\frac{\hbar\omega}{2\pi}n_{sp}\Delta\omega\exp(g_nL-1)\times\frac{(1-r_1^2)[r_2^2\exp(g_nL)+1]}{[1-r_1r_2\exp(g_nL)]^2},\quad(1)$$

式中 $P_L(\omega)$ 为自发辐射在 $\Delta\omega$ 频率区间上的功率；ω 为圆频率；$\hbar$ 为普朗克常量；n_{sp} 为自发辐射因子；g_n 为横向模式 n 对应的模式增益，利用材料增益 $g_m(x,y,z)$ 计算得到。由(1)式可知，此类器件的输出光场线宽极大(达到 10 THz 量级)，远大于 PD 的带宽，因而器件的输出光场线宽理论上近似于白噪声。

SLED 作为量子熵源，与其他实用化的 QRNG 方案比较，具有如下特性。在实用性上，SLED 的 ASE 噪声功率谱具有平坦特性，并且 SLED 的线宽非常宽(达到 10 THz 量级)，近似理想的白噪声，具有超高随机数产生速率；SLED 的出射光功率较高，出射光可以直接通过一般的 PD 进行转换，并且输出稳定。此外，在电路设计上，光路简单，无需复杂的干涉环路和反馈控制电路，易于实现小型化。在原理上，SLED 的 ASE 噪声可作为量子熵源[6,13]。

SLED 的 ASE 噪声带宽极大，而 PD 的响应带宽有限，因此可将 ASE 噪声视为高斯白噪声[28]，PD 探测的过程可等效为 ASE 噪声经过一个光带通滤波器。

ASE 噪声经过光带通滤波器被转换成电信号，再通过低通滤波输出电流信号 $i(t)$。$i(t)$ 的功率谱密度依赖于带通滤波器和低通滤波器的传递函数。

$$|H_{BP}(f)|^2=\exp\left[-(4\ln 2)\frac{(f-f_0)^2}{B_{BP}^2}\right],\quad(2)$$

$$|H_{LP}(f)|^2=\exp\left[-(\ln 2)\frac{f^2}{B_{LP}^2}\right],\quad(3)$$

式中 $H_{BP}(f)$、$H_{LP}(f)$ 分别为带通滤波器和低通滤波器的传递函数，f 为频率，f_0 为中心频率，B_{BP} 和 B_{LP} 分别为带通滤波器和低通滤波器的 3 dB 带宽。输出电流 $i(t)$ 的功率谱密度为

$$S_i(f)=R^2S_0^2\,|H_{LP}(f)|^2\times\int|H_{BP}(f')H_{BP}(f+f')|^2\,\mathrm{d}f'=R^2S_0^2B_{BP}\sqrt{\frac{\pi}{8\ln 2}}\exp\left[-(\ln 2)\left(\frac{1}{B_{LP}^2}+\frac{1}{B_{BP}^2}\right)f^2\right],\quad(4)$$

式中 R 为探测效率，S_0 为输入的 ASE 噪声，f' 为频率积分变量。由(4)式可知，$S_i(f)$ 为高斯型，其 3 dB 带宽为

$$B_{noise}=\left(\frac{1}{B_{LP}^2}+\frac{2}{B_{BP}^2}\right)^{-1/2}。\quad(5)$$

经推导，输出光电流 $i(t)$ 的强度噪声也服从高斯分布[28]，其均值和方差分别为

$$\langle i\rangle=RS_0B_{BP}\sqrt{\frac{\pi}{4\ln 2}},\quad(6)$$

$$\sigma_i^2=R^2S_0^2B_{BP}^2\left(\frac{\pi}{4\ln 2}\right)\left(1+\frac{B_{BP}^2}{2B_{LP}^2}\right)^{-1/2}。\quad(7)$$

然而，由于经典噪声的存在以及器件的不完美性质，经过模数转换得到的原始序列不满足均匀分布，存在一定的偏置和冗余，需要进行一定的数据后处理操作，以使最终的随机数序列满足统计均匀性。后处理的方案繁多，包括截位异或(XOR＋m－LSB，m 为可提取的随机比特数目)法[24]、Toeplitz 矩阵算法[22,27]以及 Trevisan′s 提取器[33-34]等。为了平衡随机性和实用性，采用截位异或算法。ASE 噪声经过光电探测后得到正比于光强的电噪声，经过离散化采样后，输出结果符合高斯分布，如图 2(a)所示；经截位异或法后处理后，得到最终满足实际应用需求的均匀分布的随机序列，其统计直方图如图 2(b)所示。

2.2　QRNG 的物理实现方案

小型化光 QRNG 系统示意图如图 3 所示。该系统包含量子熵源、噪声信号探测及放大、数据采集

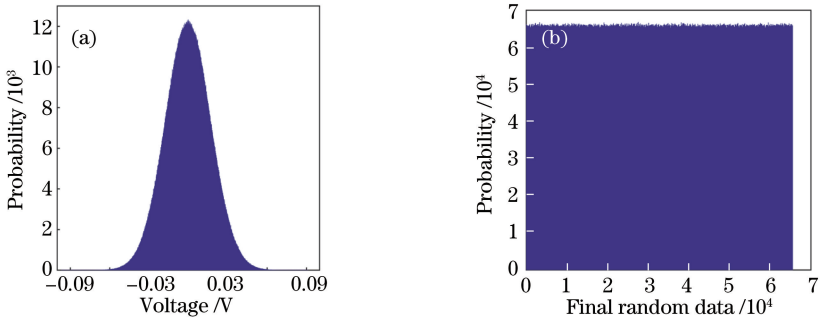

图 2　随机序列的统计直方图。(a)原始的;(b)最终的

Fig. 2　Statistical histogram of random sequence. (a) Raw; (b) final

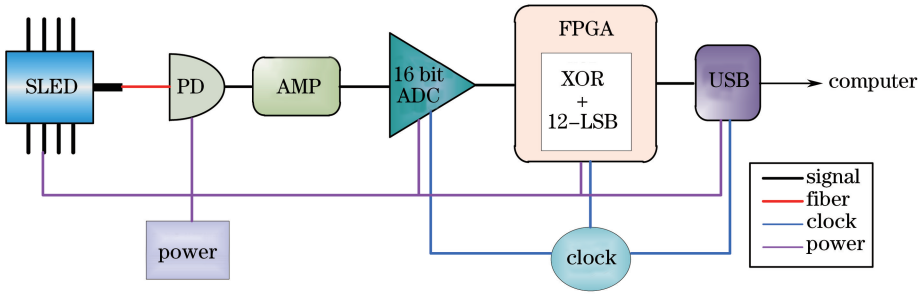

图 3　具有简单光路的小型化 QRNG 系统示意图

Fig. 3　Schematic of compact QRNG system with simple optical paths

与处理、数据传输等模块。上述模块均集成在尺寸为 140 mm×60 mm×1.8 mm 的印制电路板(PCB)上,构成了一个完整的 QRNG 系统,如图 4 所示。

该系统采用由 100 mA 恒定电流驱动的八管脚蝶形封装 SLED(GR1346Q-A,中国电子科技集团公司第四十四研究所),通过恒定温度控制电路来保证 SLED 工作在稳定状态。SLED 的出射光通过光纤传输到带宽为 1.5 GHz 的 PD 上,探测得到正比于 ASE 噪声的电流信号。该电流信号经多级低噪声 AMP 放大,再通过采样速率为 125 Mb/s 的 16 位高精度模数转换器(ADC)采集得到初始随机序列。初始随机序列经过高速 FPGA 进行实时数据后处理,得到最终的随机序列。最终的随机序列通过 USB 3.0 接口实时传输至上位机进行严格的随机性检验及应用。

数据后处理算法采用 XOR＋m－LSB 算法。

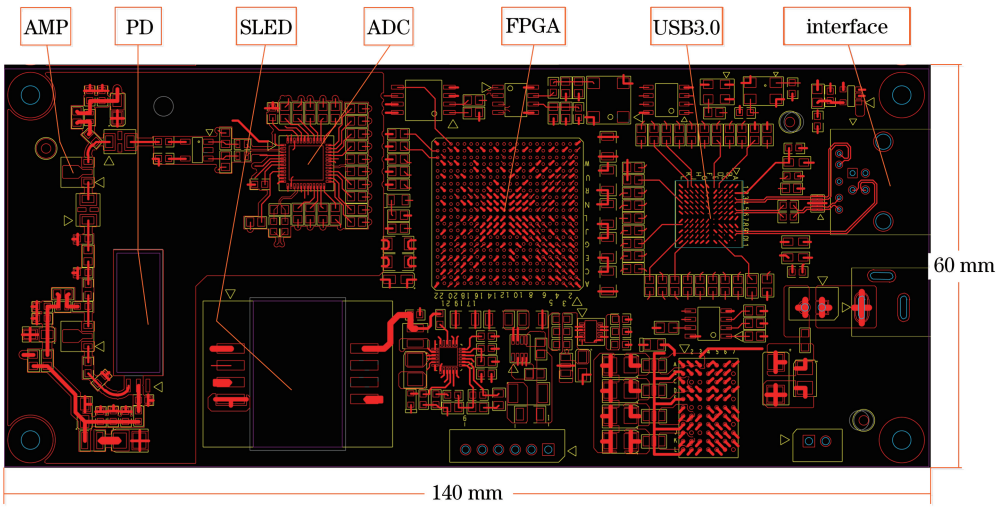

图 4　QRNG 的 PCB 图

Fig. 4　PCB plot of QRNG

异或法对相邻的两个数进行异或操作，得到一组新数据，能有效减小序列的偏置和自相关系数；截位法截取每次采样数据的靠后几位数据作为有效位，在多比特 ADC 的采样结果中，数据比特位数越靠后，其取值区间越小，随机性及均匀性越好。异或及截位运算十分简单，可以在 FPGA 上高速快捷地实现，并且该算法不引入任何冗余扩充或额外的经典噪声，可较好地提取量子的随机性。截取位数的选择是由初始随机序列的最小熵决定的。初始数据最小熵的计算方法如下：首先，采集一段原始随机数序列，将其每 16 位进行一次分段；其次，统计每一个分段中数据的取值，以及每一个取值所对应的频数；然后，根据频数统计结果计算出每一种取值所对应的频率；最后，选择统计频率中频率的最大值，通过最小熵公式计算出最小熵。通过上述计算方法，对采集的256 Mbit初始数据进行计算，得到最小熵为12.386 bit(经多次反复验证，该数值保持稳定，大于或等于12 bit)，意味着 ADC 每次采集的初始数据中可提取的随机比特数目等于12，故采用 XOR＋12－LSB 的后处理方法。利用上位机的数据采集软件实时采集随机数，并利用 CPU 内部的时钟计时，计算得到最终实时随机数的生成速率为 1.4 Gb/s。

3　QRNG 的系统性能分析

图 5 所示为自相关系数，其中红线是通过采集强度噪声信号得到的原始数据的自相关特性曲线。采用 XOR＋12－LSB 后处理算法对原始采样数据进行操作，可以得到实时产生速率为1.4 Gb/s 的随机数，该随机数的自相关特性曲线如图 5 中蓝线所示。通过对比可知，利用实时 XOR＋12－LSB 后处理算法得到的随机数序列的自相关系数显著减小。

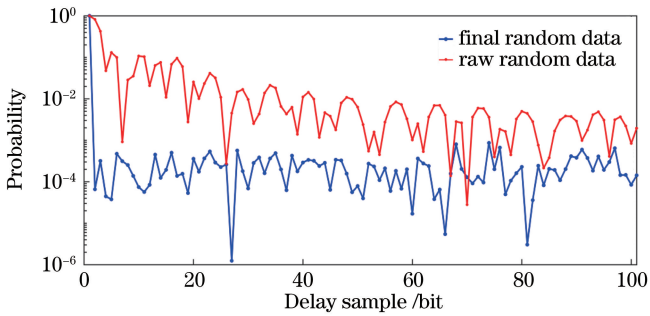

图 5　自相关系数

Fig. 5　Auto-correlation coefficients

为了评估该系统产生随机序列的随机性，应用了三种国际通用的随机性测试方法：NIST，DIEHARD 和 ENT。NIST 及 DIEHARD 的测试结果分别如图 6、7 所示，其中 DNA 为基因，OQSO 为四比特词稀少测试，OPSO 为二比特词稀少测试。可以看出，假定几率 p-value 的值都在 0.01～0.99 这个区间内，表明随机序列具有良好的随机性。在 ENT 的测试结果中，该序列每比特的熵值为 1.000000，数学平均值为 0.5000，序列的相关系数为 －0.000044，证明随机序列的随机性良好。

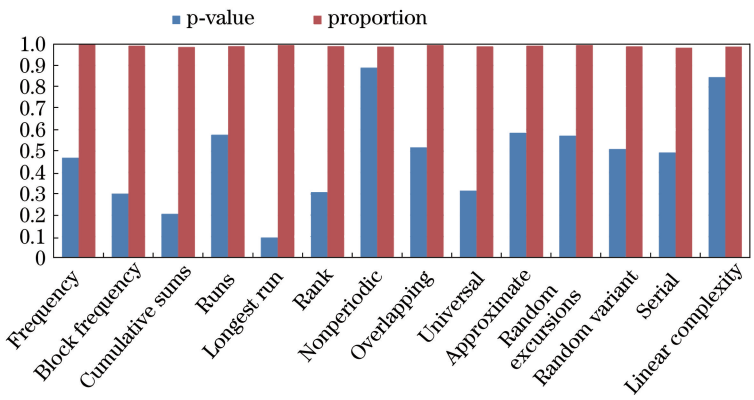

图 6　NIST 测试结果

Fig. 6　Results of NIST test

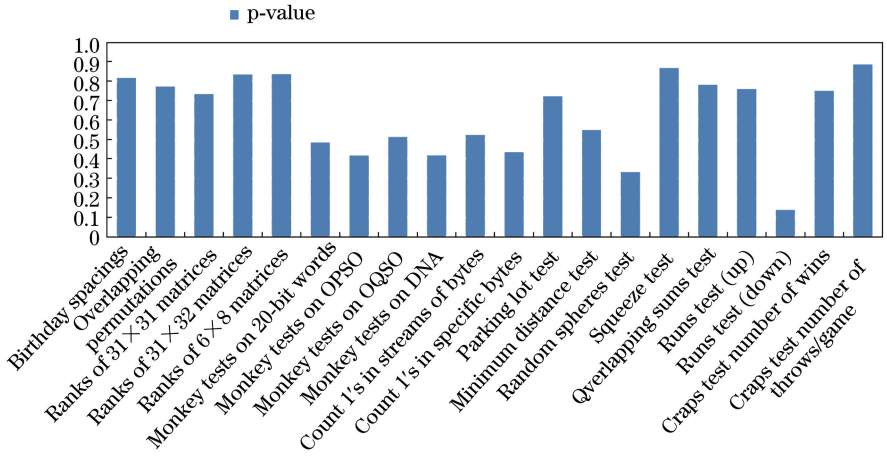

图 7　DIEHARD 测试结果

Fig. 7　Results of DIEHARD test

为了让 QRNG 产生的随机数具有稳定的随机性，即让量子熵源稳定工作在最佳点上，需要调节 SLED 的工作温度。通过查阅 SLED 的数据手册，可知其最佳工作温度为 25 ℃，因此通过自研的恒温控制电路使 SLED 恒定工作在25 ℃。此外，设计 QRNG 时，选择的电子元器件均为工业级，其工作温度范围可达－45～85 ℃。故一定的外界环境温度的变化不会对电子元器件的工作稳定性造成影响。基于以上设计，QRNG 板的工作状态不会受到温度变化的影响。

为了评估 QRNG 的长时间稳定性，首先让 QRNG 长时间工作，当工作时间长度为 0，24，48，72 h时，分别采集 QRNG 的原始随机序列以及最终随机序列，并测量原始随机序列的统计分布以及最小熵取值，结果分别如图 8、9 所示。可以看出，在不同工作时长下，原始随机序列的统计分布都近似于高斯分布且最小熵的变化很小。同时，对不同工作时间长度下采集的最终随机序列进行 NIST 及 DIEHARD 测试，结果表明，其均通过了随机性测试。基于以上实验结果，判断该 QRNG 能够较长时间地稳定工作。

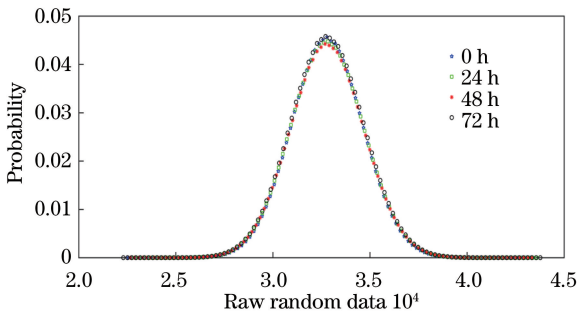

图 8　不同工作时长下原始随机序列的统计分布

Fig. 8　Statistical distributions of raw random sequences with different working time lengths

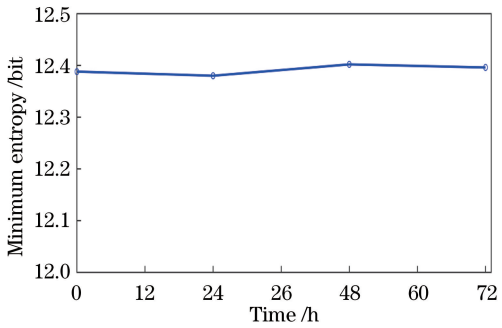

图 9　不同工作时长下原始随机序列的最小熵

Fig. 9　Minimum entropy among raw random sequences with different working time lengths

4　结　　论

设计并实现了一种实时随机数产生速率达 1.4 Gb/s 的小型化光 QRNG。该 QRNG 利用 SLED 的 ASE 噪声作为量子熵源，与现有的 QRNG 系统相比，该 QRNG 同时具有随机数产生速率高、实时性好和稳定性强的特点，且体积较小，便于实际应用。所用的八脚蝶形封装的激光器，探测器电路以及 ADC 外围电路等光学电学模块仍然占据了较大的空间，因此未来计划针对这部分器件及电路进行集成化封装，力争使该 QRNG 的尺寸达到芯片量级。

参　考　文　献

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

615-621.

[2] 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.

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

[4] Li P, Wang Y C. Research progress in physical random number generator based on laser chaos for high-speed secure[J]. Laser & Optoelectronics Progress, 2014, 51(6): 060002.
李璞, 王云才. 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[J]. 激光与光电子学进展, 2014, 51(6): 060002.

[5] Zhou Q, Hu Y, Liao X F. Ture random number generators based on mouse movement and chaos systems[J]. Acta Physica Sinica, 2008, 57(9): 5413-5418.
周庆, 胡月, 廖晓锋. 基于鼠标轨迹和混沌系统的真随机数产生器研究[J]. 物理学报, 2008, 57(9): 5413-5418.

[6] Ma X F, Yuan X, Cao Z, *et al*. Quantum random number generation[EB/OL]. (2016-05-10)[2017-06-03]. https://arxiv.org/abs/1510.08957v2.

[7] Yan Q R, Zhao B S, Zhang H, *et al*. Optical quantum random number generator based on parity of the number of photons detected in equal time intervals [J]. Acta Photonica Sinca, 2015, 44(6): 172-176.
鄢秋荣, 赵宝升, 张华, 等. 等时间间隔内光子数奇偶随机性的光量子随机源[J]. 光子学报, 2015, 44(6): 172-176.

[8] Lü Y X, Niu L B, Zhang J Z, *et al*. 500 Mb/s fast true random bit generator based on chaotic laser[J]. Chinese Journal of Lasers, 2011, 38(5): 0502010.
吕玉祥, 牛利兵, 张建忠, 等. 基于混沌激光的500 Mb/s高速真随机数发生器[J]. 中国激光, 2011, 38(5): 0502010.

[9] Pivoluska M, Plesch M. Device independent random number generation[J]. Acta Physica Slovaca, 2015, 64(6): 600-663.

[10] Vivoli V C, Sekatski P, Bancal J D, *et al*. Comparing different approaches for generating random numbers device-independently using a photon pair source[J]. New Journal of Physics, 2015, 17(2): 023023.

[11] Zhu C, Zhou H Y, Yuan X, *et al*. Source-independent quantum random number generation[J]. Physical Review X, 2016, 6(1): 011020.

[12] Marangon D G, Vallone G, Villoresi P. Source-device-independent ultrafast quantum random number generation[J]. Physical Review Letters, 2015, 118(6): 060503.

[13] Yan Q R, Chao 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.

[14] Herrero-collantes M, Garciaes-Cartin J C. Quantum random number generators[J]. Review of Modern Physics, 2016, 89(1): 015004.

[15] Rarity J G, Owens P C M, Tapster P R. Quantum random-number generation and key sharing[J]. Journal of Modern Optics, 1994, 41(12): 2435-2444.

[16] Stefanov A, Gisin N, Guinnard O, *et al*. Optical quantum random number generator[J]. Journal of Modern Optics, 2000, 47(4): 595-598.

[17] Ma H Q, Xie Y, Wu L A. Random number generation based on the time of arrival of single, photons[J]. Applied Optics, 2005, 44(36): 7760-7763.

[18] Nie Y Q, Zhang H F, Zhang Z, *et al*. Practical and fast quantum random number generation based on photon arrival time relative to external reference[J]. Applied Physics Letters, 2014, 104(5): 051110.

[19] Ren M, Wu E, Liang Y, *et al*. Quantum random-number generator based on a photon-number-resolving detector[J]. Physical Review A, 2011, 83(2): 1293-1304.

[20] Applegate M J, Thomas O, Dynes J F, *et al*. Efficient and robust quantum random number generation by photon number detection[J]. Applied Physics Letters, 2015, 107(7): 175-179.

[21] Nie Y Q, Huang L, Liu Y, *et al*. The generation of 68 Gbps quantum random number by measuring laser phase fluctuations[J]. Review of Scientific Instruments, 2015, 86(6): 063105.

[22] Zhang X G, Nie Y Q, Zhou H, *et al*. Note: fully integrated 3.2 Gbps quantum random number generator with real-time extraction[J]. Review of Scientific Instruments, 2016, 87(7): 076102.

[23] Liu J, Yang J, Li Z, *et al*. 117 Gbit/s quantum random number generation with simple structure[J]. IEEE Photonics Technology Letters, 2017, 29(3): 283-286.

[24] Yang J, Liu J, Su Q, *et al*. 5.4 Gbps real time

quantum random number generator with simple implementation[J]. Optics Express, 2016, 24(24): 27475-27481.

[25] Xu F, Qi B, Ma X, *et al*. Ultrafast quantum random number generation based on quantum phase fluctuations[J]. Optics Express, 2012, 20(11): 12366-12377.

[26] Gabriel C, Wittmann C, Sych D, *et al*. A generator for unique quantum random numbers based on vacuum states[J]. Nature Photonics, 2010, 4(10): 711-715.

[27] Martin A, Sanguinetti B, Lim C C W, *et al*. Quantum random number generation for 1.25-GHz quantum key distribution systems[J]. Journal of Lightwave Technology, 2015, 33(13): 2855-2859.

[28] Williams C R, Salevan J C, Li X, *et al*. Fast physical random number generator using amplified spontaneous emission[J]. Optics Express, 2010, 18(23): 23584-23597.

[29] Wei W, Xie G, Dang A, *et al*. High-speed and bias-free optical random number generator[J]. IEEE Photonics Technology Letters, 2012, 24(6): 437-439.

[30] Liu Y, Zhu M Y, Luo B, *et al*. Implementation of 1.6 Tb/s truly random number generation based on a super-luminescent emitting diode[J]. Laser Physics Letters, 2013, 10(4): 045001.

[31] Huang M, Wang A, Li P, *et al*. Real-time 3 Gbit/s true random bit generator based on a super-luminescent diode[J]. Optics Communications, 2012, 325: 165-169.

[32] Li Z Q, Li Z M S. Comprehensive modeling of superluminescent light-emitting diodes[J]. IEEE Journal of Quantum Electronics, 2010, 46(4): 454-461.

[33] Jiang C, Yu Z W, Wang X B. Measurement-device-independent quantum key distribution with source state errors in photon number space[J]. Physical Review A, 2016, 94(6): 062323.

[34] Ma X, Xu F, Xu H, *et al*. Postprocessing for quantum random number generators: entropy evaluation and randomness extraction[J]. Physical Review A, 2013, 87(6): 944-948.