DOI:10.16136/j.joel.2022.12.0243

小型化高速实时量子随机数发生器的设计与实现

许华醒[1],张 平[1*],王昌雷[1],戴 金[2],刘梦婕[2],汪 猛[2]

(1.中国电子科技集团公司电子科学研究院 社会安全风险感知与防控大数据应用国家工程研究中心,北京 100041;2.安徽安匠信息科技有限公司,安徽 芜湖 241000)

摘要:量子随机数基于量子力学的内禀特性,通过量子物理过程产生理论上完全不可预测的真随机数,在信息安全、计算机、量子通信等诸多领域有着重要的应用。为满足量子随机数发生器实用化应用需求,本文提出了一种基于多光子态散粒噪声测量的量子随机数发生器设计与实现方案,实现了小型化、高速率、实时量子随机数发生器,量子随机数实时输出速率可达103.2 Mbps,满足《GM/T 0005-2012 随机性检测规范》的随机性测试标准,具备连续稳定工作能力。

关键词:量子随机数;小型化;高速;实时

中图分类号:O431.2 **文献标识码**:A **文章编号**:1005-0086(2022)12-1255-08

Design and implementation of miniaturized high-rate real-time quantum random number generator

XU Huaxing[1], ZHANG Ping[1*], WANG Changlei[1], DAI Jin[2], LIU Mengjie[2], WANG Meng[2]

(1. National Engineering Research Center for Public Safety Risk Perception and Control by Big Data, China Academy of Electronics and Information Technology, Beijing 100041, China; 2. Anhui Anjiang Information Technology Company, Wuhu, Anhui 241000, China)

Abstract: Based on the inherent properties of quantum mechanics, quantum random numbers produce theoretically completely unpredictable true random numbers through quantum physical processes, and have important applications in many fields such as information security, computers, and quantum communications. In order to meet the practical application requirements of quantum random number generator, this paper proposes a quantum random number generator design and implementation scheme based on multiphoton state bulk noise measurement, which realizes a miniaturized, high-rate, real-time quantum random number generator, and the real-time output rate of quantum random number can reach 103.2 Mbps, which meets the randomness test standard of GM/T 0005-2012 Randomness Test Specification and has the ability to work continuously and stably.

Key words: quantum random number; miniaturized; high-rate; real-time

1 引 言

随机数在当今社会生活和科学研究中有着广泛的应用[1],如模拟计算、统计分析、信息安全、量子通信等。随机数的随机性优劣对信息安全等应用至关重要,如何获得随机性更好的随机数甚至获得理想的真随机数已成为一个热门的研究方向。目前随机数生成的主要方案大致分为3类:

1)伪随机数算法

通过数学上的确定性算法产生伪随机数,包括线性同余发生器[2]、反馈移位寄存器等[3],虽然该方法可以获得很高的随机数产生速率,但产生的随机序列完全由种子决定,存在一定的周期性和可预测性,不满足某些依赖真随机数的实际应用需求。

2)经典物理噪声

基于经典物理的噪声源来产生随机数,如混沌系统[4]、电路中的热噪声[5]、自由运转的振荡器

* E-mail:zp_i@163.com

收稿日期:2022-04-08 修订日期:2022-05-30

等[6]，所采用的噪声源可以用经典物理进行完整描述，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。

3）量子随机数

量子随机数[7]基于量子力学的内禀特性，由完全随机的物理过程产生，是目前唯一理论上完全不可预测的随机数序列产生方案。

随着近年来量子计算、量子通信等量子信息技术的快速发展，量子随机数发生器的研究也取得显著进步[8,9]。由于光子的量子效应显著，加之激光调控技术的成熟和光学器件的丰富，从光学系统中提取随机数成为量子随机数发生器的主流技术方案。

2 光量子随机数方案

基于光场量子态产生随机数的方法主要包括：单光子探测[10-16]、激光相位噪声[17-19]、自发辐射噪声[20,21]、量子真空起伏等[22-24]。下面重点介绍几种基于单光子探测的量子随机数生成方案，并基于此提出一种小型化高速实时量子随机数发生器设计与实现方案。

2.1 单光子路径选择方案

单光子路径选择方案[10,11]是早期出现的量子随机数生成方案，一个随机比特决定于单光子与分束器相互作用时对于传播路径做出的选择，这种选择是真随机的，因为单光子通过分束器后的测量塌缩是量子行为。如图1所示，单光子源（single-photon source，SPS）输出的单光子经过一个50∶50的分束器（Splitter）时会有一半的概率透射，也有一半的概率被反射。透射或反射的单光子分别由两个单光子探测器（single-photo detector，SPD）中的一个探测，定义其中一个SPD接收到光子时为“1”，另一个为“0”，由于单光子的探测是随机过程，所以一次探测事件就会产生一个随机比特。

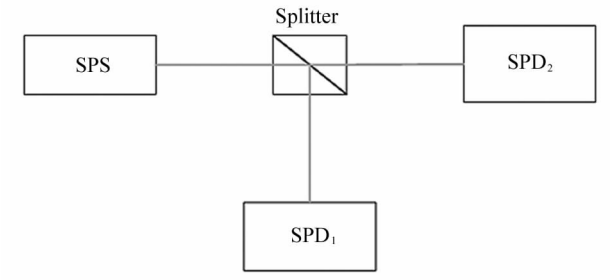

图1 单光子路径选择方案

Fig. 1 Single-photon path selection scheme

这种方案原理上能够产生理想的量子随机数，但现实中却较为困难。首先难以获得精确的50∶50的分束器；其次两个SPD也无法做到完全相同的探测效率，这都会使得最终产生的随机数存在偏置；更重要的是从产生速率上看，受限于SPD的死时间等因素，这种方案产生量子随机数的速率较低。

2.2 单光子时间间隔方案

单光子时间间隔方案[12-14]通过测量相邻两个单光子的到达时间间隔来产生随机数。如图2所示，单光子激光器发出的两个单光子分别到达一个SPD的时间间隔具有量子随机性，对时间间隔进行测量并量化后就可以获得多个随机比特。

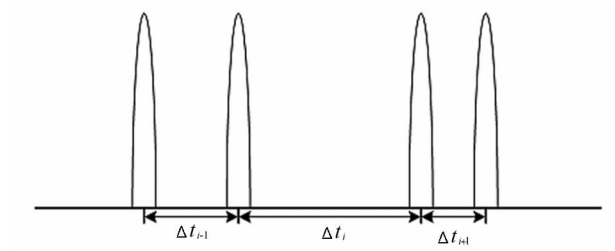

图2 单光子时间间隔方案

Fig. 2 Single-photon time interval scheme

这类方案也是基于单光子探测的，SPD的死时间等问题没有解决，依然是限制量子随机数生成速率进一步提高的主要因素。

2.3 等间隔光子计数方案

等间隔光子计数方案[15,16]主要通过测量相同时间间隔内到达探测器的光子数量来产生随机数。如图3所示，时间 T 内到达探测器的光子数量是随机的，对于理想的SPS，其光子数服从泊松分布，即：

$$P(n)=\frac{\mu^n}{n!}\mathrm{e}^{-\mu}, \tag{1}$$

式中，n是到达的光子数，μ为平均到达的光子数，$P(n)$为光子数为 n 的概率。

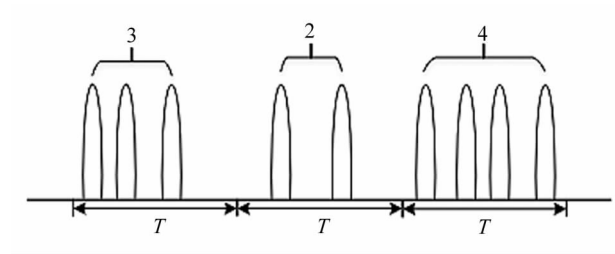

图3 等间隔光子计数方案

Fig. 3 Equal interval photon counting scheme

直接通过探测单位时间内到达的光子数进行编码产生的随机数存在偏差，需要进行后处理才能获得满足真随机数标准的随机数。对于高速量子随机数发生器来说，相对复杂的后处理算法难以满足实

时处理的要求,以大多基于离线处理的方式来实现。

量子随机数要从技术研究走向应用,需要便于集成在应用系统中,故量子随机数发生器首先要实现小型化。目前量子随机数技术突破很快,但主要在量子随机数生成速率等指标上,而量子随机数发生器体积较大,如基于激光相位噪声的量子随机数发生器,在应用中通常为 1U 机箱大小。导致体积大的原因主要包括两个方面,一是光路体积较大,尚未实现光集成应用,二是高速量子随机数的后处理相对复杂(如 Toeplitz 矩阵、Hash 矩阵算法),使得后处理电路较大且功耗也较大,同时相对复杂的后处理算法难以满足实时处理的要求,大多基于离线处理的方式来实现。小型化量子随机数发生器应用最为广泛的是瑞士 ID Quantique 公司的 Quantis QRNG 产品系列,其量子随机数发生器生成速率最大为 16 Mbps,虽然具备了小型化,但由于速率较低也难以满足应用需求

为实现量子随机数实用化应用,本文基于多光子态散粒噪声测量原理提出了一种小型化高速实时的量子随机数发生器实现方案。使用激光二极管与阵列探测器集成封装作为量子熵源,能够实现量子随机数发生器的小型化。通过探测器阵列进行光子数探测,有效地解决了 SPD 随机数生成速率的瓶颈,可以实现高速的量子随机数。同时采用简单的异或后处理算法,大大减轻了电路处理需求、缩小了电路体积且能够实时生成量子随机数。研制了 106 mm×60 mm×20 mm 的小型化量子随机数发生器,通过实时数据采集,量子随机数的实时生成速率可以达到 103.2 Mbps,随机数序列的随机性满足国家密码局《GM/T 0005-2012 随机性检测规范》[25](检测序列 1 Gbit 随机数据)。进一步通过更长序列 10 Gbit 随机数据的随机性检测,以及连续采集 1 000 Gbit 随机数据,分割成 1000 个 1 Gbit 随机数据的随机性检测,验证了该方案具备连续稳定的工作能力。

3　系统设计

本节主要介绍基于多光子态散粒噪声测量的小型化高速实时量子随机数发生器的设计方案。

3.1　系统组成

量子随机数发生器系统方案如图 4 所示,主要包括量子熵源和数据后处理两部分。其中量子熵源部分包含量子态制备模块,即量子光源和量子态测量模块,即硅探测器。数据后处理部分包含运算放大、模数转换、主控单元。当从量子熵源得到原始数据后,通过数据后处理得到近似理想的随机比特序列。

系统各组成部分的功能如下:

量子光源:一组可调直流驱动的近红外发光二极管(LED)发出的脉冲光,作为量子随机数的信号光源;

硅探测器:一组具有光子数分辨能力的探测器阵列,将光信号转换成电信号;

运算放大器:将探测器输出的电信号进行放大;

模数转换:高速模数转换器(ADC)采集放大后的电信号并数字化为高速原始随机数;

主控单元:对原始数据进行异或后处理,实时产生符合理想真随机数特征的量子随机数,同时监控系统的工作状态并生成反馈控制信号,并根据反馈控制信号调节量子光源的工作状态,实现温度反馈补偿控制,使整个设备稳定工作。

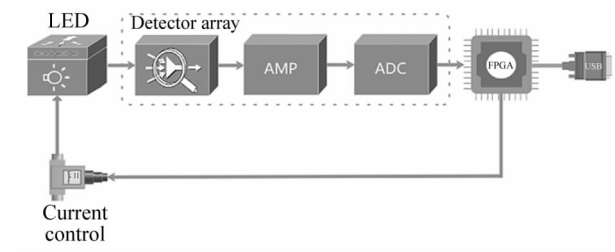

图 4　量子随机数发生器系统方案

Fig. 4　Quantum random number generator scheme

3.2　基于阵列的测量方案

由于受到探测器转换速率的影响,单个探测器对光子的探测采集速率无法满足产生高速量子随机数的需求。本文提出的基于阵列的多光子态散粒噪声测量方案,如图 5 所示,通过密集的阵列排布,每个光子探测器都会形成一个比特的数据,从而提高随机数产生的速率。

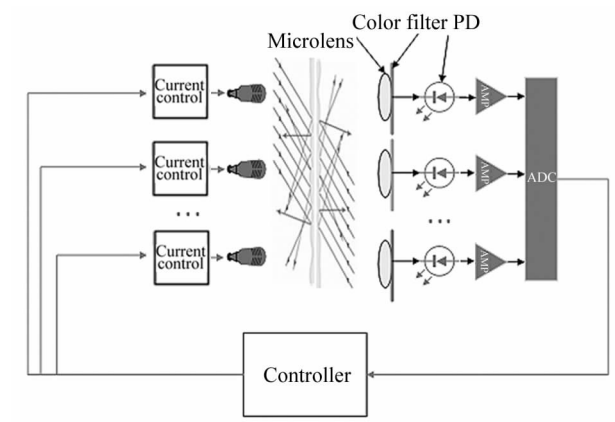

图 5　探测器阵列

Fig. 5　Detector array

多光子态散粒噪声测量方案是基于相干光场的光子数服从 Poisson 分布原理。在对相干光场进行测量时，根据量子测量理论，相干态会以一定的概率随机塌缩到光子数态，并且根据相干态的二阶相干性可知，相干态光子出现的时间是彼此独立的。所以在相同时间间隔的探测过程中，调节相干光场的强度，使具有光子数分辨能力的探测器工作在线性区，探测到的光子数量为相互独立事件，以此产生真随机数。方案使用探测器阵列，可有效解决单个探测器方案数据生成速率的瓶颈，可支持高速随机数生成。

本方案通过近红外 LED 发出的脉冲光量子，经过光束整形后到达探测器，使用具有光子数分辨能力的光子探测器测量接收到达的光子数，基于该种探测采集架构，极大地扩展了可获取的随机比特信息。针对探测到的原始数据，采用简单的异或后处理算法提取熵源信息，从而构建出从光源到探测再到数据后处理的完整多光子态散粒噪声测量系统，得到最终的量子随机数序列。

3.3　实时后处理

光子数的计数是由光电转换器来完成的，由于光电器件的不完美特性，实际光电转换器得到的数值还包含暗电流、热噪声等经典噪声，这些噪声会对随机数的随机性产生影响。要得到完美的随机数序列，量子熵的提取工作是必要的，故而数据的后处理环节是必不可少的。

通过测量得到随机变量 X，X 是由经典物理噪声 X_c 和量子噪声 X_q 构成，且 X_q 和 X_c 是相互独立的。所以：

$$X = X_q + X_c。 \tag{2}$$

系统的量子噪声 X_q 服从式(1)的泊松分布，根据二元信息最小熵的公式可以得出系统的最小熵为：

$$H_{\min}(X) = -\log_2[\max(\frac{\mu^n}{n!}e^{-\mu})] = -\log_2[\frac{\mu^{[\mu]}}{|\mu|!}\times e^{-\mu}], \tag{3}$$

式(3)计算了不同平均光子数下系统的最小熵，如图 6 所示，当光子数为 1 000 时，熵值约为 6.31 bit；当光子数为 10 000 时，熵值约为 7.97 bit。

系统的经典物理噪声 X_c 主要包括：

1）放大器噪声，其标准模型是加性高斯噪声(additive Gaussian noise)，该噪声独立于每个光电探测器并且与信号强度无关，主要是由热噪声引起的，热噪声与探测器的温度正相关。放大器噪声是系统“读出噪声”的主要部分。

2）暗电流噪声，由阵列探测器暗电流引起的散粒噪声，这种噪声有时也被称为暗电流散粒噪声。

在设计中，硬件上采用降噪和补偿技术，降低经典物理噪声的占比，使得量子噪声与经典物理噪声的信噪比达到 30 dB 以上。

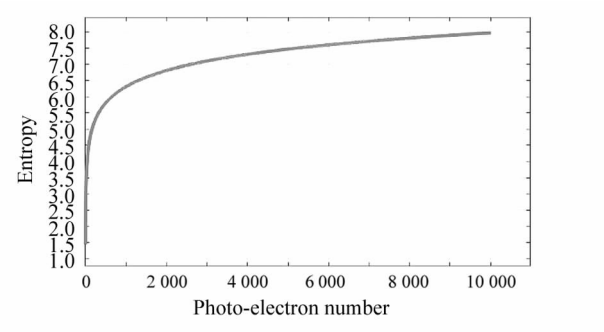

图 6　平均光子数与量子熵关系图

Fig. 6　Diagram of average number of photons and quantum entropy

随机性提取算法一般分为两种，一种是确定性的随机性提取算法，一种是种子随机性提取算法。确定的随机性提取，最大的优势在于只需要输入数串 S_i，并且使用很少的计算资源，就可以得到结果数串 S_o。本文采用确定性的异或的随机提取算法，该随机提取算法实现了如下功能：

$$\mathrm{Ext}:\{0,1\}^{12}\rightarrow\{0,1\}^{1}。 \tag{4}$$

实际是将一个 12 bit 的随机数串通过异或算法转化为一个短的 1 bit 的随机数串。

3.4　性能分析

系统设计使用有效位数为 12 bit 的光电转换器，其中包含了经典噪声和量子随机信息。采用的提取方式为将 12 bit 的数据进行异或处理输出 1 bit 的最终量子随机数，本方案设计中光源产生的平均光子数实测约为 7 000，根据式(3)计算的最小量子熵约为 7.7 bit，输出的随机数比特远小于理论量子熵。本方案中使用 2 000 000 个探测阵列单元，每秒探测 60 次，每个阵列单元每次探测产生 1 bit 的量子随机数，理论上可实时生成的量子随机数速率约为 120 Mbps。

4　实验结果与分析

4.1　量子随机数发生器研制

基于系统设计，本节给出了具体的实验设置、研制模块和检测结果。系统光电转换的物理过程如图 7 所示，其中光子数为 n_p，量子效率为 η，光子转换的

电子数为 n_e,暗噪声为 n_d,模拟信号增益为 G,读出噪声记为 δ_q,模数信号转换的结果为 y。光子通过光电转换器件,将光子转换为光电子存储在电容阱中,通过模拟放大器将电压信号放大,最终通过模数转换器,输出最终的数字信号。在设计中使用的光源为 860 nm 的近红外光源,光源使用恒流源驱动发射脉冲光,脉冲光的平均光子数测量为 6 758,选用的探测器的量子效率为 $\eta=25\%$,模拟信号增益为 $G=1$,ADC 为 12 位模数转换器。

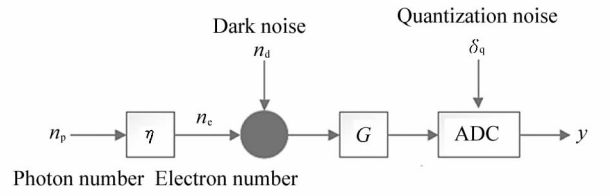

图 7　量子随机数光电转换过程

Fig. 7　Photoelectric conversion process of quantum random number

研制的量子随机数发生器如图 8 所示,其尺寸为 106 mm×60 mm×20 mm,功耗约为 2 W,采用 USB2.0 为输出接口和供电接口,实测的量子随机数输出速率为 103.2 Mbps。

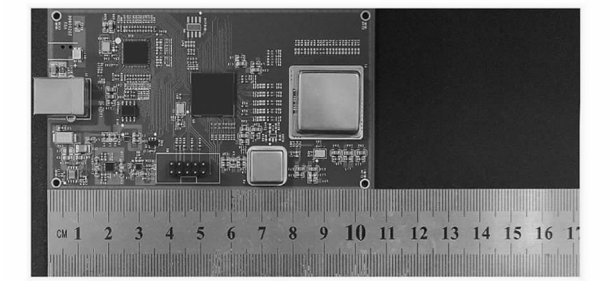

图 8　量子随机数发生器模块实物图

Fig. 8　Physical map of quantum random number generator module

4.2　随机性检测

在量子随机数发生器量子光源不点亮处于无光的情况下,采集了 10^6 bit 未经后处理的经典噪声数据,统计结果如图 9 所示,经典噪声的统计分布符合高斯分布,经典噪声对原始随机数的影响不超过 ±4。在量子随机数发生器量子光源点亮处于正常工作的条件下,采集 10^6 bit 未经后处理的原始随机数数据,光电子数与读出值为线性关系,通过统计计算,光电子数量的统计特性如图10所示,均值为 6 758,方差为 7 154,最小值为 6 368,最大值为 7 112,均值与方差的比值为 0.945,接近于理想泊松分布;经典噪声数值占原始随机数数值约为 0.6‰,对量子随机数的影响可以忽略。图 10 中的曲线为理想泊松分布模型,柱状图为光电子数的实际统计结果,实测结果与理论分析一致。

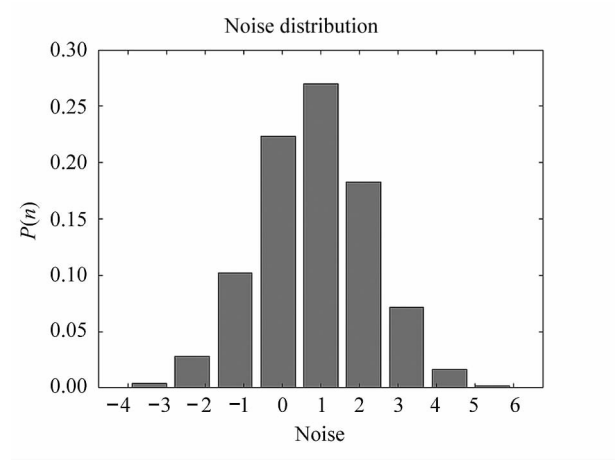

图 9　经典噪声统计分布

Fig. 9　Statistical distribution of classical noise

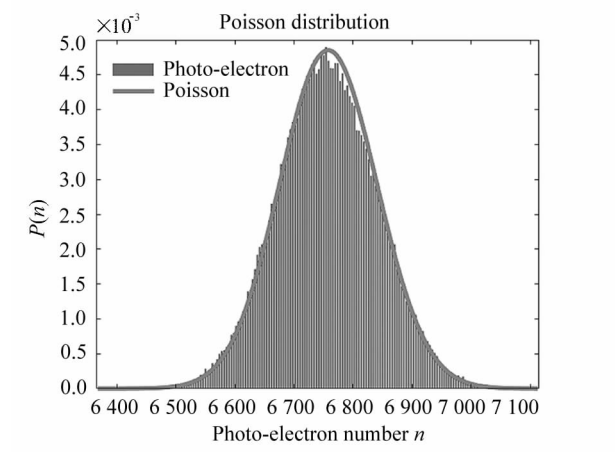

图 10　原始随机数统计分布

Fig. 10　Statistical distribution of raw random numbers

进一步对量子随机数发生器输出的随机数进行随机性检测,随机性检测依据《GM/T 0005-2012 随机性检测规范》,统计 P-value 值不小于显著性水平 α($\alpha=0.01$)的样本数,记样本数量为 s,则通过检测的样本数 K 应满足式(5):

$$K \geq s \times (1-\alpha-3\sqrt{\frac{\alpha(1-\alpha)}{s}})。\tag{5}$$

在进行随机性检测时,采集 1 Gb 的随机数序列,分成 1 000 组,即 $s=1\,000$,每组数据长度为 10^6 bit。若通过的样本数量 $K\geqslant 981$,则认为随机序列通过检测。

检测的结果如表1所示。可以看到随机性检测的所有的测试项目均通过。

表1 1 Gbit 数据的随机性检测结果(s=1 000)

Tab. 1 Randomness testing results of 1 Gbit data(s=1 000)

SN	Test items	Parameters	Statistics	Results
1	Frequency (Monobit)	/	997/1 000	Pass
2	Frequency (Block)	m=100	988/1 000	Pass
3	Poker	m=4	991/1 000	Pass
		m=8	989/1 000	Pass
4	Overlapping template matching	m=2, 2^{m-1}	994/1 000	Pass
		m=2, 2^{m-2}	991/1 000	Pass
		m=5, 2^{m-1}	987/1 000	Pass
		m=5, 2^{m-2}	985/1 000	Pass
5	Runs (total)	/	991/1 000	Pass
6	Runs (distribution)	/	986/1 000	Pass
7	Longest run	m=10 000	992/1 000	Pass
8	Binary derivation	k=3	989/1 000	Pass
		k=7	989/1 000	Pass
9	Autocorrelation	d=1	991/1 000	Pass
		d=2	987/1 000	Pass
		d=8	986/1 000	Pass
		d=16	986/1 000	Pass
10	Binary matrix rank	M=Q=32	990/1 000	Pass
11	Cumulative sums	Forward	995/1 000	Pass
		Backward	997/1 000	Pass
12	Approximate entropy	m=5	985/1 000	Pass
13	Linear complexity	m=500	986/1 000	Pass
14	Universal statistical	L=7, Q=1 280	986/1 000	Pass
15	Discrete Fourier transform	/	992/1 000	Pass

表2 10 Gbit 数据的随机性检测结果(s=10 000)

Tab. 2 Randomness testing results of 10 Gbit data(s=10 000)

SN	Test items	Parameters	Statistics	Results
1	Frequency (Monobit)	/	9 906/10 000	Pass
2	Frequency (Block)	m=100	9 912/10 000	Pass
3	Poker	m=4	9 880/10 000	Pass
		m=8	9 909/10 000	Pass
4	Overlapping template matching	m=2, 2^{m-1}	9 893/10 000	Pass
		m=2, 2^{m-2}	9 899/10 000	Pass
		m=5, 2^{m-1}	9 905/10 000	Pass
		m=5, 2^{m-2}	9 906/10 000	Pass
5	Runs (total)	/	9 899/10 000	Pass
6	Runs (distribution)	/	9 875/10 000	Pass
7	Longest run	m=10 000	9 908/10 000	Pass
8	Binary derivation	k=3	9 907/10 000	Pass
		k=7	9 885/10 000	Pass
9	Autocorrelation	d=1	9 899/10 000	Pass
		d=2	9 901/10 000	Pass
		d=8	9 911/10 000	Pass
		d=16	9 903/10 000	Pass
10	Binary matrix rank	M=Q=32	9 895/10 000	Pass
11	Cumulative sums	Forward	9 901/10 000	Pass
		Backward	9 892/10 000	Pass
12	Approximate entropy	m=500	9 907/10 000	Pass
13	Linear complexity	m=500	9 901/10 000	Pass
14	Universal statistical	L=7, Q=1 280	9 883/10 000	Pass
15	Discrete Fourier transform	/	9 883/10 000	Pass

为了更好地评估量子随机数发生器的性能，进行了更严格和更长序列的测试。连续采集 10 Gbit 随机序列，分成 10 000 组，即 s=10 000，每组数据长度为 10^6 bit。通过式(4)计算得到 $K \geq 9\,871$，则认为随机序列通过检测。检测结果如表 2 所示，随机性检验的所有的测试项目均通过。

进一步，连续采集 1 000 Gbit 的数据，对数据进行 1000 次的随机性检测，在所有项目均通过的情况下，1 000 次随机性检测的通过次数为 876 次，每个检测项的失败次数以及失败时通过检测的样本数 K 如表 3 所示。所有检测项的失败次数总和为 146 次，共检测了 24 000 次，失败率为 0.61%。通过上述检测可知，量子随机数发生器具备连续稳定的工作能力。

表3 1 000 Gbit 数据的随机性检测结果(s=1 000)

Tab. 3 Randomness testing results of 1 000 Gbit data(s=1 000)

SN	Test items	Parameters	Tests	Failures (K<981)	K=974	K=975	K=976	K=977	K=978	K=979	K=980
1	Frequency (Monobit)	/	1 000	5	0	0	0	0	0	1	4
2	Frequency (Block)	m=100	1 000	0	0	0	0	0	0	0	0
3	Poker	m=4	1 000	2	0	0	0	0	0	1	1
		m=8	1 000	2	0	0	0	0	0	1	1
4	Overlapping template matching	m=2, 2^{m-1}	1 000	4	0	0	0	0	0	2	2
		m=2, 2^{m-2}	1 000	3	0	0	0	0	0	0	3
		m=5, 2^{m-1}	1 000	3	0	0	0	0	0	0	3
		m=5, 2^{m-2}	1 000	2	0	0	0	0	0	2	0
5	Runs (total)	/	1 000	3	0	0	0	0	0	0	3
6	Runs (distribution)	/	1 000	49	2	2	4	2	10	10	19
7	Longest run	m=10 000	1 000	4	0	0	0	0	0	1	3
8	Binary derivation	k=3	1 000	5	0	0	0	0	1	1	3
		k=7	1 000	4	0	0	0	0	0	2	2
9	Autocorrelation	d=1	1 000	3	0	0	0	0	0	0	3
		d=2	1 000	3	0	0	0	0	0	0	3
		d=8	1 000	2	0	0	0	0	1	1	0
		d=16	1 000	3	0	0	0	0	0	0	3
10	Binary matrix rank	M=Q=32	1 000	2	0	0	0	0	1	0	1
11	Cumulative sums	Forward	1 000	3	0	0	0	0	1	0	2
		Backward	1 000	1	0	0	0	0	0	0	1
12	Approximate entropy	m=5	1 000	3	0	0	0	0	0	1	2
13	Linear complexity	m=500	1 000	5	0	0	0	0	1	1	3
14	Universal statistical	L=7, Q=1280	1 000	17	0	0	0	2	5	2	8
15	Discrete Fourier transform	/	1 000	18	0	0	1	3	1	8	5

5 结　论

本文提出了一种基于多光子态散粒噪声测量的高速实时量子随机数发生器设计与实现方案,并研制了尺寸为 106 mm×60 mm×20 mm 的量子随机数发生器,实时输出随机数速率可达 103.2 Mbps,随机数的随机性满足《GM/T 0005-2012 随机性检测规范》,通过更长序列 10 Gbit 随机数据的随机性检测,以及连续采集 1000 Gbit 随机数据并分割成 1000 个 1 Gbit 随机数据的随机性检测,验证了该方案具备连续稳定的工作能力。

参考文献:

[1] HAYES B. Computing science:Randomness as a resource [J]. American Scientist,2001,89(4):300-304.

[2] LEHMER D H. Mathematical methods in large-scale computing units[J]. Annals of the Computation Laboratory of Harvard University,1951,26:141-146.

[3] MATSUMOTO M,NISHIMURA T. Mersenne twister:a 623-dimensionally equidistributed uniform pseudo-random number generator[J]. ACM Transactions on Modeling and Computer Simulation,1998,8:3-30.

[4] 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.

[5] 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.

[6] 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.

[7] HERRERO COLLANTES M,GARCIA ESCARTIN J C. Quantum random number generators[J]. Review of Modern Physics,2017,89(1):015004.

[8] ZHOU H Y,ZENG P. Quantum random number generation [J]. Journal of Information Security Research,2017,3(1):23-35.
周泓伊,曾培. 量子随机数发生器[J]. 信息安全研究,2017,3(1):23-35.

[9] BRUNO S,ANTHONY M,HUGO Z,et al. Quantum random number generation on a mobile phone[J]. Physical Review X,2014,4(3):031056.

[10] STEFANOV A,GISIN N,GUINNARD O,et al. Optical quantum random number generator[J]. Journal of Modern Optics,2000,47:595.

[11] WU S,LIANG L M,LI C Z,et al. Optical quantum random number generator[J]. Acta Sinica Quantum Optica,2005,11(2):63-68.
吴双,梁林梅,李承祖,等. 光量子随机数发生器[J]. 量子光学学报,2005,11(2):63-68.

[12] WAYNE M A,JEFFREY E R,AKSELROD G M,et al. Photon arrival time quantum random number generation[J]. Journal of Modern Optics,2009,56(4):516-522.

[13] WAHL M,LEIFGEN M,BERLIN M,et al. An ultrafast quantum random number generator with provably bounded output bias based on photon arrival time measurements [J]. Applied Physics Letters,2011,98(17):171105.

[14] LI S,WANG L,WU L A,et al. True random number generator based on discretized encoding of the time interval between photons[J]. Journal of the Optical Society of America A,2013,30(1):124-127.

[15] 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):023820.

[16] 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 Sinica,2015,44(6):0627003.
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):0627003.

[17] GUO H,TANG W,LIU Y,et al. Truly random number generation based on measurement of phase noise of laser [J]. Physics Review E,2010,81,051137.

[18] XU F,QI B,MA X,et al. Ultrafast quantum random number generation based on quantum phase fluctuations[J]. Optical Express,2012,20:12366.

[19] 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,2015,86:063105.

[20] WILLIAMS C,SALEVAN J,LI X,et al,Fast physical random number generator using amplified spontaneous emis-

sion[J]. Optical Express, 2010, 18: 23584.

[21] ZHOU H, YUAN X, MA X. Randomness generation based on spontaneous emissions of lasers[J]. Physics Review A, 2015, 91: 062316.

[22] GABRIEL C, WITTMANN C, SYCH D, et al. A generator for unique quantum random numbers based on vacuum states[J]. Nature Photonics, 2010, 4: 711.

[23] SHI Y, CHNG B, KURTSIEFER C. Random numbers from vacuum fluctuations[J]. Applied Physics Letters, 2016, 109: 041101.

[24] ZHENG Z Y, ZHANG Y C, HUANG W N, et al. 6 Gbps real-time optical quantum random number generator based on vacuum fluctuation[J], Review of Scientific Instruments, 2019, 90(4): 43105.

[25] Randomness test specification: GM/T 0005-2012 [S/OL]. (2012-03-21) [2022-05-18]. http://www.gmbz.org.cn/main/viewfile/20180108023917940312.html.
随机性检测规范: GM/T 0005-2012[S/OL]. (2012-03-21) [2022-05-18]. http://www.gmbz.org.cn/main/viewfile/20180108023917940312.html.

作者简介:

张 平 (1981—),男,博士,高级工程师,主要从事量子通信及组网技术方面的研究.