DOI: 10.3969/j.issn.1007-5461.2023.06.013

基于真空涨落的高速量子随机数产生

金振阳[1], 万相奎[1*], 廖 涛[1], 陈柳平[2]

(1 湖北工业大学太阳能高效利用及储能运行控制湖北省重点实验室, 湖北 武汉 430068;
2 国开启科量子技术(北京)有限公司, 北京 102629)

摘 要: 随着量子密钥分发 (QKD) 系统的深入研究与应用, 随机数的质量和产生速率面临着更大的挑战。为了满足随机数在QKD系统以及对于密钥安全性要求较高的场景下的使用, 提出一种基于真空涨落产生真随机数的实验方案。相比于传统方案使用的2 × 2偏振分束器 (BS), 该方案采用单模1 × 2的BS来实现光路的传输, 不仅节省了装置成本, 同时还得到了较高的随机数产生速率。在9.68 dBm光强的作用下, 得到量子噪声与经典噪声的信噪比为11.92 dB。对通过12 bit的模数转换器采集到的数据进行分析, 结果显示经典噪声和真空散粒噪声均符合高斯分布, 通过计算得到最小熵为9.92, 原始数据经过安全性可被信息论证明的托普利茨 (Toeplitz) 后处理, 最终实现7.6 Gbit/s的量子随机数产生, 并且通过了Nist随机数标准测试, 验证了方案的可行性。

关 键 词: 量子通信; 真空涨落; 量子随机数; 最小熵; 后处理

中 图 分 类 号 : TN202; O413 **文 献 标 识 码 :** A **文章编号:** 1007-5461(2023)06-00933-10

High speed quantum random number generation based on vacuum fluctuations

JIN Zhenyang[1], *WAN Xiangkui* [1*], *LIAO Tao*[1], *CHEN Liuping*[2]

(1 Hubei Key Laboratory for High-efficiency Utilization of Solar Energy and Operation Control of Energy Storage System, Hubei University of Technology, Wuhan 430068, China;
2 QUDOOR, Beijing 102629, China)

Abstract: With the deeper research and application of quantum key distribution (QKD), the quality and generation rate of random numbers are facing greater challenges. In order to meet the use of random numbers in QKD system and in the scenarios with high requirements for key security, an experimental scheme for generating true random numbers based on vacuum fluctuations is presented. Compared with the 2 × 2 polarization beam splitter (BS) used in traditional solution, a single mode 1 × 2 BS is used in the proposed scheme to realize the transmission of optical path, which not noly saves device costs but also obtains a high random number generation rate. Under the action of 9.68 dBm light intensity, the signal-to-noise ratio of quantum noise to classical noise of 11.92 dB is obtained. The data collected through a 12

基金项目: 国家自然科学基金 (61571182)

作者简介: 金振阳 (1998 -), 湖北武汉人, 研究生, 主要从事量子通信方面的研究。E-mail: 1105989018@qq.com

导师简介: 万相奎 (1976 -), 博士, 教授, 博士生导师, 主要从事人工智能应用技术、可穿戴监护或检测仪器开发及量子信息技术应用方面的研究。E-mail: xkwan@hbut.edu.cn

收稿日期: 2022-07-22; **修改日期:** 2022-08-16

*通信作者。

bits analog-to-digital converter is analyzed. The results show that both the classical noise and the vacuum shot noise are in accordance with Gaussian distribution, and the calculated minimum entropy is 9.92. The original data is subjected to Toeplitz post-processing, whose security can be proved according to information theory. Finally, the quantum random number generation with the rate of 7.6 Gbit /s is acheived, and it successfullly passes the NIST random number standard test, verifying the feasibility of the scheme.

Key words: quantum communication; vacuum fluctuation; quantum random number; minimum entropy; post processing

0 引 言

作为一种底层资源, 随机数广泛应用于各领域, 如量子通信、密码学以及数值模拟等[1−3]。尤其是随着量子计算机的出现, 在通信安全等方面对随机数质量的要求越来越高。量子随机数能够凭借它本身具有的真随机性在一定程度上抵抗量子计算机, 因此, 相较于传统的伪随机数[4], 量子随机数更具优势。

目前量子随机数的产生方案已有多种, 其中的主流方案大多依赖光源来产生量子随机数。最早出现的是单光子方案: 单光子路径测量、光子到达时间测量、光子数分布等[5−7]。由于单光子方案产生速率受限, 研究人员提出连续光源方案, 以此来获得更大的熵源带宽, 从而提高随机数的生成速率, 典型方案有放大自发辐射噪声、激光相位噪声和真空散粒噪声[8−10]。在相位噪声方案上, 研究人员提出了脉冲激光方案, 实现了高速量子随机数的产生[11]。

基于真空散粒噪声的量子随机数方案相较于其他方案有着明显优势: 真空态易制备、系统简单, 易于集成化、散粒噪声理论上是白噪声, 具有无穷大的带宽, 因此可一次采样得到大量的原始随机数。基于此方案, 中国科学技术大学设计了一种高速、实时、集成化的芯片式量子随机数发生器 (QRNG)[12], 此外, 研究人员提出了各种集成化的QRNG方案[13−16]。

为了探究真空散粒噪声方案的不同实验条件对随机数产生的影响, 不同于传统方案 (采用保偏分束器BS)[17], 本文提出了采用单模1 × 2的50:50分束器来完成光路部分的搭建, 并分析了探测器输入不平衡时造成采样失败的原因。光信号通过400 MHz带宽的平衡零差探测器以及25 dB的跨阻放大器 (TIA), 并在电脑上采用12 bit的模数转换器 (ADC) 量化散粒噪声信号得到原始随机数, 最后通过可证明安全性的托普利茨 (Toeplitz) 后处理手段提取出真随机数。

1 实验分析

1.1 常见方案对比

对基于光源实现量子随机数产生的方案原理及其优劣进行总结, 如表1所示。

1.2 实验原理

在量子世界相空间中, 量子态的准概率分布可用Wigner函数表示为[18]

$$W(\boldsymbol{x},\boldsymbol{p})=\frac{1}{\pi}\exp(-\boldsymbol{x}^2-\boldsymbol{p}^2), \tag{1}$$

表1 基于光源实现量子随机数产生的常见方案比较

Table 1 Comparison of common schemes for generating quantum random numbers based on light sources

随机源类型	物理原理	主要优势	速率(量级)	主要挑战
空间分辨性	光子路径叠加测量	1) 方案原理简单, 便于建模; 2) 具有明显的量子非确定性; 3) 理论上, 该方案能产生完美的理想二进制序列	Mbps	1) 两路探测器不平衡; 2) 探测器死时间
光子数分辨性	一定时间内光子数统计	1) 无需双路探测器, 平衡性提高; 2) 输出序列偏置大幅降低	Mbps	1) 光子分辨能力; 2) 探测器死时间
时间分辨性	光子到达时间差统计	1) 装置只存在一个探测器, 避免多路探测不平衡; 2) 可在一次测量中将时间差量化成多个bit	Mbps	1) 时间精度; 2) 探测器死时间
真空涨落	散粒噪声测量	1) 真空态易制备; 2) 对探测效率不敏感; 3) 探测所得可一次量化为多个比特	Mbps～Gbps	1) 经典噪声占比大; 2) 零差探测器带宽
相位噪声	激光相位噪声波动	1) 机理明确; 2) 相位噪声方差、最优功率等指标都有系统的分析方法, 便于选值	Mbps～Gbps	1) 相位漂移; 2) 设备体积大

式中: $\boldsymbol{x}$和$\boldsymbol{p}$是真空态中的正则分量, 分别表示位置和动量。根据海森堡不确定性原理, 运动粒子的位置和动量无法同时测量, 因此可以提取位置或者动量信息作为随机数源。当对$\boldsymbol{x}$分量进行测量时引入波函数, 其概率分布可表示为

$$\left|\psi(\boldsymbol{x})\right|^2=\int_{-\infty}^{+\infty}W(\boldsymbol{x},\boldsymbol{p})\,\mathrm{d}\,\boldsymbol{p}=\frac{1}{\sqrt{\pi}}\exp(-\boldsymbol{x}^2)\,. \tag{2}$$

由 (1) 式可见$\boldsymbol{x}$分量和$\boldsymbol{p}$分量是对称的, 对其中任一分量进行测量, 其测量结果的概率均符合 (2) 式所示的高斯分布。

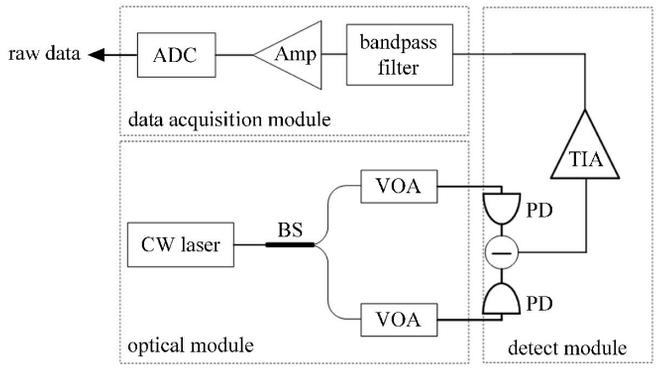
最终探测到的散粒噪声除了量子噪声以外, 不可避免地会包含部分电子学的经典噪声 (主要由热噪声、不完美平衡探测引入的本底噪声和电子学噪声等因素产生)。本实验中量子噪声来源于真空散粒噪声, 即使空间中没有任何物质, 仍然会存在量子涨落现象, 理论上, 真空散粒噪声是由于真空涨落引发的观测数据的统计涨落[19]。经典噪声也是高斯白噪声, 与量子噪声独立同分布, 混合叠加后最终观测到的散粒噪声同样为高斯噪声, 将其方差记为

$$N=N_{\mathrm{c}}+N_{\mathrm{q}}\,, \tag{3}$$

式中: N_{c}为经典噪声方差, N_{q}为量子噪声方差。在真空散粒噪声方案系统中, 量子噪声与经典噪声的比定义为

$$R_{\mathrm{QCN}}=10\lg\left(\frac{N_{\mathrm{q}}}{N_{\mathrm{c}}}\right). \tag{4}$$

实验中, 经典噪声的功率通常不会有太大变化 (其由系统因素产生, 因此无法消除), 可以通过增大本底光 (LO) 光强来增大量子噪声在测量结果中的占比, 以得到更大的R_{QCN}。更大的R_{QCN}意味着熵源的量子噪声占比更高, 经典噪声的影响会更小。



ADC: analog-to-digital converter; Amp: amplifier; CW: continuous wave; VOA: variable optical attenuator; BS: beam splitter; TIA: trans-impedance amplifier; PD: photon detector

图 1 实验方案示意图

Fig. 1 Schematic diagram of the experiment

首先, 选用中心波长为 1550 nm 的单模半导体连续激光器作为 LO 光源, 光信号经过 50:50 的 BS 后被分成 2 束能量相同的光, 一束透射一束反射; 对于真空输入端, 在 VOA (型号: JW3303) 处使用的是紧密接触 (PC) 接口, 回波损耗约 15 dB。当使用 2 × 2 的 BS 时, 真空输入端通过物理手段用光纤头保护帽进行遮光处理, 以确保只有真空态输入, 真空输入端作为一个反射面, 接收到 VOA 处反射回来的光, 再次反射到 BS 处, 通过 LO 光后又一次被放大, 这将会导致测量结果不稳定, 测量到的能量时高时低。使用的 1 × 2 的 BS 本质上和 2 × 2 型一样, 只不过 1 × 2 的 BS 是将输入端的短纤在回损测试工序中截断了, 然后点上了紫外光线 (UV) 固化胶来增加产品的回损。真空端仍然从截断的一段输入, UV 固化胶的存在可以在极大程度上抑制光的反射, 从而采到稳定的散粒噪声信号。实验中, 需要保证平衡零差探测器 (型号: THORLABS PDB770C DC 400MHz) 2 个输入端信号的强度差值尽可能小, 因此在两路分别接上 VOA 对输入到探测器的光强进行调整, 达到近似平衡的状态以获得较高信噪比的探测结果。经过探测器后, 共模信号被抑制, 真空态的随机信息转换为电信号, 此时通过 TIA (型号: PE15A1008) 将噪声信号放大后再通过一个通频带在 100～750 MHz 的带通滤波器, 以滤掉直流信号及部分经典噪声, 从而提高量子噪声的占比[20]。为分析信号的方差, 需要用到频谱仪 (Keysight N9020B 10Hz-26.5 GHz), 通过频谱仪可以直接读出 R_{QCN}, 并通过示波器 (型号: DSOV134A) 读出散粒噪声的时域信息。

2 实验结果

2.1 时域测量结果

激光器工作时, 从激光器端输出的 LO 光光强实测为 9.86 dBm, 是该激光器在实验环境下能达到的最大光强。在两个 VOA 处测得输出功率分别为 4.83 dBm 和 4.72 dBm, 此时观察到的信号和理论分析结果一致, 经典噪声和量子噪声叠加, 经过带通滤波器滤除部分低频信号及直流分量, 结果同样是高斯分布。当激光器关闭时, 真空态对输出的影响可以忽略不计, 此时测量到的结果即为经典噪声。散粒噪声与经典噪声的统计分布和时序分布分别如图 2、图 3。

经过放大后测量到的散粒噪声电压值约为 900 mV, 经典噪声电压值约为 300 mV。探测器输出电流方差可表示为[21]

$$\sigma^2 \approx 4E_{\mathrm{L}}^2\left[\delta X_{\mathrm{S}}^2(t)\cos^2\phi+\delta P_{\mathrm{S}}^2(t)\sin^2\phi\right], \tag{5}$$

式中: E_{L}为本底光电场, δX_S和δP_S分别表示振幅分量和相位分量, ϕ表示探测器两输入端的相对相位差。当$\phi=0$时, 所得方差为X分量的量子涨落; 当$\phi=\pi/2$时, 方差为P分量的量子涨落。真空态在相空间中各向同性, 因此不需要使用保偏器件来固定相位差。实验中测得, 当调节VOA使得两端输出功率差值约为0.5 dB时, 探测器输出电流会被滤波器滤掉, OSC上无信号显示。实质上是由于探测器两输入端差值过大时直流分量无法完全消除, 导致低频信号占比变大, 使输出信号主要频率集中在通频带之外, 从而OSC上无信号显示。

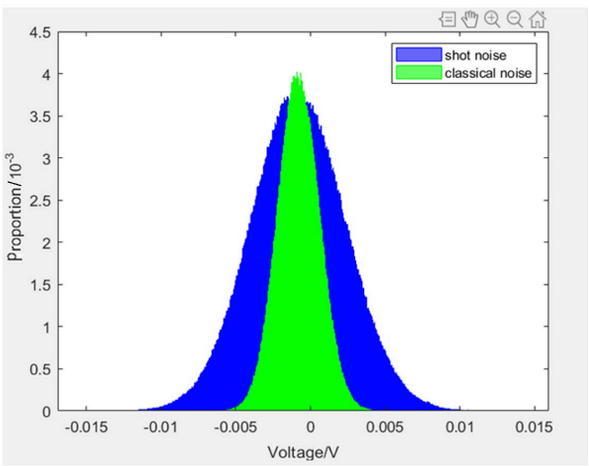


图2　散粒噪声与经典噪声统计分布

Fig. 2 Statistical distribution of shot noise and classical noise

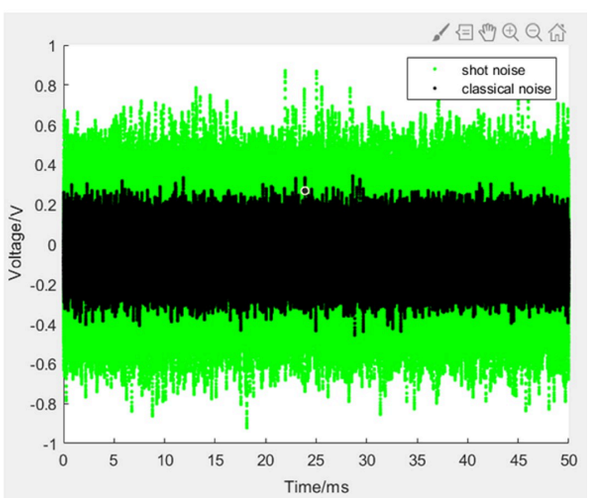
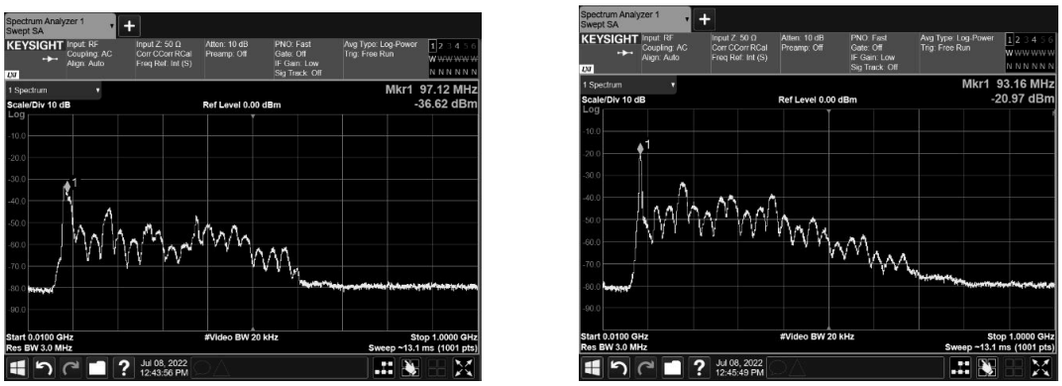


图3　散粒噪声与经典噪声时序分布

Fig. 3 Time series distribution of shot noise and classical noise

2.2　频域测量结果

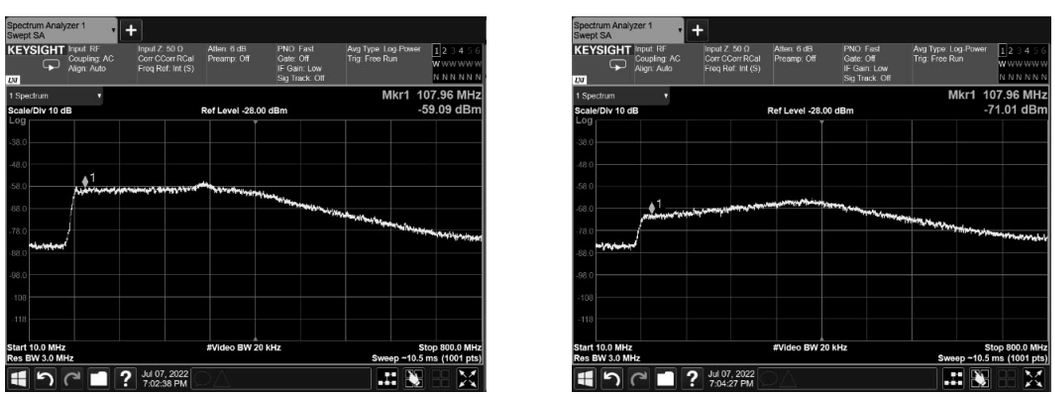
对比了使用1 × 2 BS与2 × 2 BS时的频域测量结果, 当使用2 × 2 BS时, 测量结果显示信号幅度不稳定, 图4为使用2 × 2 BS时散粒噪声的测量结果。可见, 由于PC接口的反射效应, 频谱幅度十分不稳定, 反射光的强度时高时低, 从而导致频谱测量一直抖动。当使用1 × 2的BS时, 如图5所示, 可以看到很明显的效果, 反射效应被消除, 频谱稳定。



(a) (b)

图4 2 × 2 BS下散粒噪声的频谱测量结果。(a) 反射光较弱; (b)反射光较强

Fig. 4 Spectrum measurement results of shot noise under 2 × 2 BS. (a) The reflected light is weak; (b) The reflected light is strong



(a) (b)

图5 1 × 2 BS下的频谱特性测量。(a) 散粒噪声; (b) 经典噪声

Fig. 5 Spectrum characteristic measurement under 1 × 2 BS. (a) Shot noise; (b) Classic noise

散粒噪声信号经过100～750 MHz的带通滤波后, 测得经典噪声和量子噪声分别为−71.01 dB、−59.09 dB, 根据 (4) 式计算出R_{QCN}为11.92 dB。文献 [17] 的实验过程中, 散粒噪声经过带通滤波以后, 测得R_{QCN}为9.71 dB, 且最终产生的随机数能够完成后续行业内认可的测试项目。表明真空态作为熵源具有良好的量子随机特性。理论上, R_{QCN}的值与本底光强正相关, 激光器功率需要尽可能达到最高, 但由于实验器件环境受限, 无法继续增大激光器光强。

2.3 最小熵分析结果

熵是热力学名词, 用来表示事物的混乱程度。在信息论中香农熵定义为

$$H_2(X)=-\sum_{i=1}^{n}p_i\log_2 p_i\,, \tag{6}$$

式中$p_i=P(X=x_i)$表示X值为x_i时的概率, 其值越小则熵越大, 表示携带的信息量越大, 不确定性越高。而对随机性的评估可以由最小熵来量化, 最小熵定义为

$$H_{\min}(x)=-\log_2\max P_i(X=x)\,, \tag{7}$$

表示在有第三方窃听者时猜中变量X的概率最大的情况下可提取的随机比特数, 通过计算出来的最小熵可以确定后处理所使用的矩阵行列比例。其中X的取值取决于ADC的量化范围, 实验选取12 bit ADC对电压值进行量化, 得到有效数据范围为0～4095的泊松分布, 经过后处理后将得到的10进制数转换成2进制数即可得到原始 "0" "1" 随机序列。

产生的随机序列被期望携带更多的信息, 也就是熵尽可能大。理论表明, 当$p_i = 1/n$时香农熵最大, 即数据满足均匀分布。数据越接近均匀分布则熵值越大, 因此, 为了接近均匀分布而对数据进行了后处理, 后处理可以消除数据的偏置, 减少经典噪声带来的边信息, 同时增大数据的可靠性[22]。基于真空涨落方案的随机数产生实验受限于探测器的400 MHz带宽, 使用800 MHz的ADC采样率, 测得原始数据的最小熵为9.92, 意味着每12 bit的量化数据能够提取到9.9 bit的真随机数, 提取比例需要 ⩽ 82.5%, 保守处理, 可以确定后续处理原始数据的提取比例大小为 80%。

采用大型Toeplitz矩阵进行后处理, 这是一种信息论可证的后处理方法, 其结构可以表示为

$$\boldsymbol{T}=\begin{bmatrix} c_m & c_{m+1} & \cdots & c_{m+n-2} & c_{m+n-1} \\ c_{m-1} & c_m & \cdots & c_{m+n-3} & c_{m+n-2} \\ \vdots & c_{m-1} & \ddots & \vdots & \vdots \\ c_2 & \vdots & \ddots & c_n & c_{n+1} \\ c_1 & c_2 & \cdots & c_{n-1} & c_n \end{bmatrix}, \tag{8}$$

矩阵的元素$c_1 \sim c_{m+n-1}$表示{0, 1}随机序列, 可以发现, 每一行元素右移一位并给第一位补上新的随机数而得到下一行元素, 因此共需随机数种子数为$m + n - 1$。基于上述最小熵的测量分析, 确定参数$m = 3276$、$n = 4096$, 经过Toeplitz矩阵后处理后, 最终量子随机数的产生速率为7.6 Gbit/s。

3　随机性测试

将采集到的噪声信号量化后得到原始的随机数, 原始数据经过Toeplitz矩阵进行后处理, 得到最终的随机数。为了验证最终生成的随机数是否满足真随机, 对比了随机序列自相关系数在后处理前后的差异, 结果如图6所示。

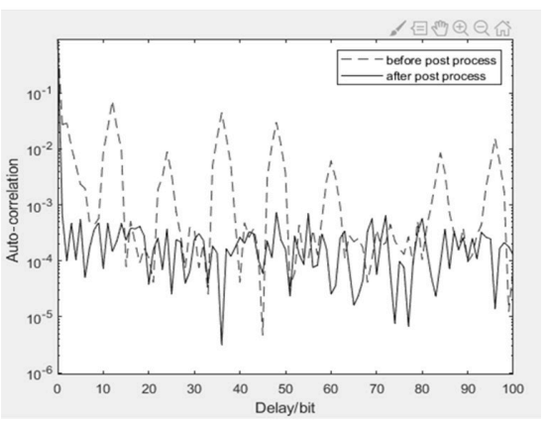


图6　处理前后的自相关系数

Fig. 6　Auto-correlation coefficient before and after treatment

由图可见, 原始数据中较大的自相关系数明显降低, 说明原始数据经过后处理之后自相关性减弱, 随机性得到提高。同时, 数据处理之前呈现图2所示的高斯分布, 而经过后处理的数据呈现出近似均匀分布, 如图7所示。

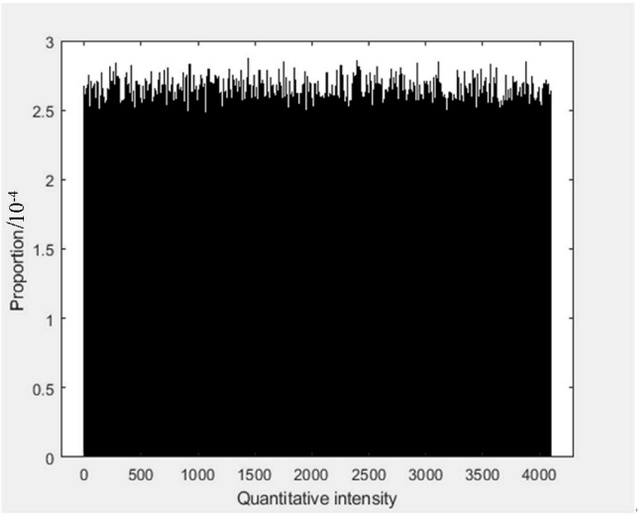


图7 处理后的数据分布

Fig. 7 Data distribution after processing

对最终的随机数进行了行业内认可的Nist检测。按照Nist标准的测量方法将采集到的1 Gbit真随机数数据分成1000份, 每份数据1 Mbit, 当各个测试项中有大于等于981份数据通过时, 表明该项目合格。为了避免偶然性, 选择了4组数据, 如图8所示, 结果显示所采集的数据均通过了Nist测试, 证明了实验产生的随机数具有真随机性。

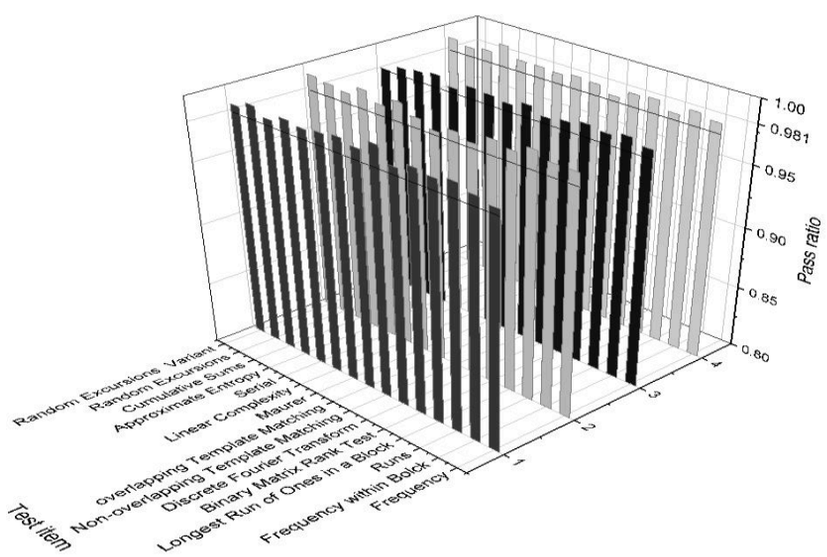


图8 Nist测试结果

Fig. 8 Test result of Nist

4 结 论

基于测量真空散粒噪声的原理, 提出了一种真随机数的提取实验方案。采用单模1 × 2分束器, 节省了成本, 同时观察到在采用2 × 2单模分束器情况下进行实验出现的反射效应, 对比分析了两种方案在频谱仪上测量结果的差异。通过最大化本底光强尽可能提高实验环境下的R_{QCN}, 最终使其达到11.92 dB, 采集到了具有良好量子随机性的真随机数。采用12 bit高分辨率ADC来提取原始随机数, 有效提高了真随机数的产

生速率, 并通过信息论可验证安全性的Toeplitz后处理手段, 按80%比例提取随机数, 同时对比了后处理前后自相关系数的变化, 最终实现了7.6 Gbit/s的随机数产生。所采集到的随机数全部通过行业内所认可的Nist检测标准, 证明了该方案最终输出的随机数质量合格, 能够满足量子密钥分发系统等高安全性场景的需求。实验通过OSC采集到原始数据, 仅仅是采取离线手段提取真随机数, 利用真空散粒噪声产生随机数的方案潜力巨大, 目前该方案的速率受限于探测器的探测带宽, 未来工艺水平提升并研发出更高带宽的探测器时, 其速率会更高。此外, 基于真空散粒噪声的方案所用光学器件简易, 容易搭建, 在后续实现集成化设备实时采样的工作中, 更容易做到小型化。

参考文献:

[1] Li G. Research status of quantum communication technology [J]. *Electronic Component and Information Technology*, 2022, 6 (3): 111-113.
李 赓. 量子通信技术研究现状 [J]. 电子元器件与信息技术, 2022, 6(3): 111-113.

[2] Li H. Application of network information security based on cryptography [J]. *Modern Informationn Technology*, 2022, 6(6): 104-106, 109.
黎 浩. 基于密码学的网络信息安全应用 [J]. 现代信息科技, 2022, 6(6) : 104-106, 109.

[3] Lundow P H, Markström K. Efficient computation of permanents, with applications to Boson sampling and random matrices [J]. *Journal of Computational Physics*, 2022, 455: 110990.

[4] Wang Y, Gong J, Wang M Y, *et al*. A pseudo-random number generator for integer chaotic map [J]. *Journal of Beijing University of Posts and Telecommunications*, 2022, 45(1): 58-62.
王 永, 龚 建, 王明月, 等. 一种整数混沌映射的伪随机数生成器 [J]. 北京邮电大学学报, 2022, 45(1): 58-62.

[5] Naveen J, Shatheesh S. Provably secure data sharing approach for personal health records in cloud storage using session password, data access key, and circular interpolation [J]. *International Journal on Semantic Web & Information Systems*, 2021, 17(4): 76-98.

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

[7] Tisa S, Villa F, Giudice A, *et al*. High-speed quantum random number generation using CMOS photon counting detectors [J]. *IEEE Journal of Selected Topics in Quantum Electronics*, 2015, 21(3): 23-29.

[8] Huang M, Chen Z Y, Zhang Y C, *et al*. A phase fluctuation based practical quantum random number generator scheme with delay-free structure [J]. *Applied Sciences*, 2020, 10(7): 2431.

[9] Guo X M, Liu R P, Li P, *et al*. Enhancing extractable quantum entropy in vacuum-based quantum random number generator [J]. *Entropy* (*Basel, Switzerland*), 2018, 20(11): 819.

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

[11] Abellán C, Amaya W, Jofre M, *et al*. Ultra-fast quantum randomness generation by accelerated phase diffusion in a pulsed laser diode [J]. *Optics Express*, 2014, 22(2): 1645-1654.

[12] Bai B, Huang J Y, Qiao G R, *et al*. 18.8 Gbps real-time quantum random number generator with a photonic integrated chip [J]. *Applied Physics Letters*, 2021, 118(26): 264001.

[13] Raffaelli F, Sibson P, Kennard J E, *et al*. Generation of random numbers by measuring phase fluctuations from a laser diode with a silicon-on-insulator chip [J]. *Optics Express*, 2018, 26(16): 19730.

[14] Raffaelli F, Ferranti G, Mahler D H, *et al*. A homodyne detector integrated onto a photonic chip for measuring quantum states and generating random numbers [J]. *Quantum Science and Technology*, 2018, 3(2): 025003.

[15] Roger T, Paraiso T, De Marco I, *et al*. Real-time interferometric quantum random number generation on chip [J]. *Journal of the Optical Society of America B*, 2019, 36(3): B137-B142.

[16] Huang L L, Zhou H Y. Integrated Gbps quantum random number generator with real-time extraction based on homodyne detection [J]. *Journal of the Optical Society of America B*, 2019, 36(3): B130.

[17] Liu R P, Cheng C, Wu M C, *et al*. High-speed quantum random number generation based on continuous variable vacuum noise [J]. *Study on Optical Communications*, 2019, 5: 22-27, 70.
刘日鹏, 成 琛, 吴明川, 等. 基于连续变量真空噪声量子随机数的高速产生 [J]. 光通信研究, 2019, 5: 22-27, 70.

[18] Leonhardt U, Paul H. Measuring the quantum state of light [J]. *Progress in Quantum Electronics*, 1995, 19(2): 89-130.

[19] Xu Y F. *Research on Key Technologies of Data Acquisition for the Quantum Random Number Generator Based on Vacuum Fluctuation* [D]. Beijing: Beijing University of Posts and Telecommunications, 2020.
徐逸凡. 真空态量子随机数发生器数据采集关键技术研究 [D]. 北京: 北京邮电大学, 2020.

[20] Liu R P. *High-entropy Quantum Random Number Generation Based on Vacuum State and Entropy Source Quantification* [D]. Taiyuan: Taiyuan University of Technology, 2019.
刘日鹏. 基于真空态高熵量子随机数产生及熵源量化研究 [D]. 太原: 太原理工大学, 2019.

[21] Huang W N. *Practical Security Analysis of Quantum Random Number Generator Based on Vacuum Fluctuation* [D]. Beijing: Beijing University of Posts and Telecommunications, 2020.
黄伟楠. 真空态量子随机数发生器的实际安全性研究 [D]. 北京: 北京邮电大学, 2020.

[22] Zhang X G. *High-speed Quantum Random Number Generator Based on Laser Phase Fluctuation* [D]. Hefei: University of Science and Technology of China, 2017.
张晓光. 基于激光相位波动的高速量子随机数发生器 [D]. 合肥: 中国科学技术大学, 2017.