激光与光电子学进展

自发辐射放大的量子随机数快速后处理方法

童启夏，胡莹莹，何德勇*，韩正甫**
中国科学技术大学中国科学院量子信息重点实验室，安徽 合肥 230026

摘要 在实用化的高速量子随机数产生器的应用中，使用Toeplitz矩阵作为后处理方法提取量子随机数随机性已成为一种主要的技术路线。然而，Toeplitz矩阵更适合于硬件计算而不适合软件运算，通常需要搭建专门的现场可编程门阵列(FPGA)电路才能进行快速运算。基于自发辐射放大(ASE)的量子随机产生器，提出一种基于简单哈希函数的快速后处理方式。这种方式的时间复杂度仅为$O(N)$，小于Toeplitz矩阵的$O(N\log N)$，并且相对另一种常用的后处理方法，最低有效位(LSBs)后处理，具有更高的随机数提取效率。实验中由所提后处理方法计算得到的随机数已通过美国国家标准与技术研究所(NIST)随机性检测。

关键词 量子随机数；自发辐射放大；哈希函数；后处理方法；随机性检测
中图分类号 O436 **文献标志码** A **DOI**：10.3788/LOP230839

Fast Post-processing Method for Practical Quantum Random Number Generators Based on Spontaneous Emission Amplification

Tong Qixia, Hu Yingying, He Deyong*, Han Zhengfu**
CAS Key Laboratory of Quantum Information, University of Science and Technology of China, Hefei 230026, *Anhui, China*

Abstract In practical applications of high-speed quantum random number generators, using Toeplitz matrices as a post-processing method to extract the randomness of quantum random numbers has become a major technology roadmap. However, Toeplitz matrices are more suitable for hardware calculations than for software calculations and typically require that specialized field programmable gate array (FPGA) circuits be constructed for fast calculations. Based on the quantum random generator of spontaneous emission amplification (ASE), a fast post-processing method based on a simple hash function is proposed. The time complexity of this method is only $O(N)$, which is less than $O(N\log N)$ of a Toeplitz matrix, and compared with another commonly used post-processing method, least significant bit (LSB) post-processing has higher efficiency in random number extraction. The random number calculated by the proposed post-processing method in the experiment passes the randomness test of the national institute of standards and technology (NIST) in the United States.

Key words quantum random number; amplified spontaneous emission; hash function, post-processing-method; randomness test

1 引 言

随机数产生器可以用于密码学、彩票、线上游戏以及众多领域[1]。虽然伪随机数产生器(PRNGs)已经能够满足一般生产生活需求，但是在对于随机性和安全性有着更高要求的情况下，量子随机数产生器(QRNGs)便是一个更为可靠的选择。例如，现在实用化的量子密钥分发(QKD)系统已经能够达到GHz的通信重复频率，相应地需要超过Gb/s的实时随机数产生器[2]。因此，许多研究者们开始寻找高速的随机噪声源以及从其中提取随机性的方法。

大多数QRNGs是基于量子光学原理的，如基于真空涨落噪声的QRNGs[3]、基于激光相位随机噪声的QRNGs[4]、基于自发辐射放大噪声(ASE)的QRNGs[5-9]，以及基于拉曼散射的QRNGs[10]等。其中，ASE噪声源的优势在于其具有足够宽的带宽和很

收稿日期：2023-03-10；**修回日期**：2023-03-20；**录用日期**：2023-03-22；**网络首发日期**：2023-04-02
基金项目：国家自然科学基金(62271463)
通信作者：*hedeyong@mail.ustc.edu.cn；**zfhan@ustc.edu.cn

低的电子学背景噪声，因此使用非常简单的光学与电子学测试系统就能将其中的随机性高效地提取出来，并且实现Gb/s的随机数产生速率[7]。

然而，和大多数QRNGs方案一样，ASE-QRNGs难以直接产生均匀分布的随机数。因此，在完成随机物理量的提取之后，还需要对其进行后处理才能得到可用的均匀分布随机数[8]。在这里最先应用的是最低有效位(LSBs)等后处理算法[9]，随后有基于Toeplitz矩阵的后处理算法[11]。目前，基于Toeplitz矩阵的后处理算法已成为各种QRNGs的主要后处理算法之一[12]。然而，Toeplitz矩阵是一种更适应硬件计算而不是软件计算的算法，其矩阵运算引起的时间开销一般为$O(N\log N)$，因此Toeplitz矩阵运行的时间会随着输入的随机序列的长度N的增大而急剧增加[13]。

本文使用ASE-QRNGs作为实验系统产生一组量子随机数，并提出一种基于LSBs后处理方法和最大游程进行压缩的新型后处理方法。对于一段800 Mb的随机比特，Toeplitz后处理算法和所提算法的随机数后处理时间分别为360 min与10 min。另一方面，简单的LSBs算法最大能提取400 Mb的随机比特，而所提算法可以提取408 Mb的随机比特，具有更高的提取效率。且使用该算法处理得到的随机数已通过美国国家标准与技术研究所(NIST)随机性检测。

2　基本原理

2.1　实验过程

实验中，使用的ASE量子随机数生成器的示意图如图1所示。首先，用一个基于掺铒光纤放大器(EDFA)原理的ASE光源[ASE-c-100-B(T)]产生一个均匀增益的从1530 nm到1567 nm的宽谱光。然后，使用一个通道选定在CH13(中心频率为1550.12 nm、带宽为0.5 nm)的密集波分复用器(DWDM)对选定频率进行滤波。使用滤波器的主要原因是整个宽谱光的均匀性难以保证，会影响光电探测器的探测一致性，从而影响随机数的性质。经过滤波之后，使用一个频率为20 GHz的高速光电探测器(PD)来检测光信号，并将它转换成电信号。这样，就可以使用高速示波器以及其内含的高速采样数模转换器(Tektronix DSA71254B，50 Gs/s，8 bit-ADC)得到原始的随机比特序列。最后，将示波器采样得到的数据离线传入个人电脑上使用后处理算法处理原始序列得到新的序列。

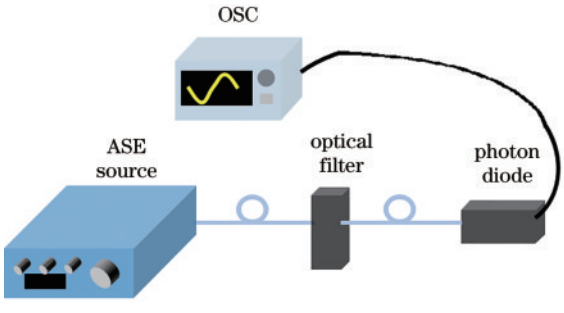

图1　基于ASE的量子随机数产生器的实验原理图

Fig. 1　Experimental schematic diagram for quantum random number generators based on ASE

假设光学滤波器和电子学滤波器的响应函数为高斯型，通常这是一个合理的近似，那么通过探测后光电流信号的功率谱密度$S(f)$[8]也是一个高斯分布，其表达式为

$$S(f)=R^2S_0^2B_{\mathrm{BP}}\sqrt{\frac{\pi}{8\ln 2}}\exp\left[-(\ln 2)\left(\frac{1}{B_{\mathrm{LP}}^2}+\frac{1}{B_{\mathrm{BP}}^2}\right)f^2\right],\tag{1}$$

式中：R为探测器响应度；S_0为光信号功率；f为信号频率；B_{BP}是光学滤波器的带宽，也即本实验中的DWDM的带通带宽；B_{LP}为电子学滤波器，也即本实验中的光电探测器的低通带宽。受到光电探测器截止带宽限制，实际测得的噪声功率谱密度通常不是一个完美的高斯分布，而更接近于一个伽马分布[8]。最后，实验得到的随机序列分布的伽马分布拟合曲线如图2所示，其中，横坐标为8 bit-ADC采样的ASE电压，纵坐标为总计数。

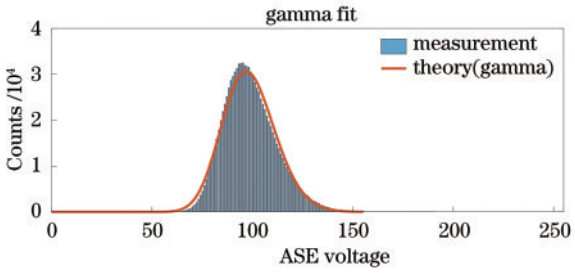

图2　测得实验数据的最佳伽马拟合

Fig. 2　Best gamma fitting of measured experimental data

2.2　后处理方法

所提算法可对原始随机数进行有效提取，最终提取效率σ为

$$\sigma=\frac{m}{n}+\alpha\beta,\tag{2}$$

式中：m为通过LSBs方法计算最小熵保留下来的最高有效位；n为一个n比特位(n-bit)序列长度[14]；在实际中，总能使用如冯·诺伊曼操作等简单哈希方法将原始序列转换成(0,1)比例均衡序列，并将这个过程的提取效率记为α[15]；β为根据最大游程计算得到的提取效率。

2.2.1　平衡非均匀随机序列的游程计算

因为测试的随机数是一个非常接近高斯分布的概率分布，所以可以建立一个数学模型[16-18]来描述这样一段长度为N的(0,1)非均匀随机序列：将该序列划分为n段，每一段长度为M的比特序列，每一段序列L_k

随机地满足L_+或者L_-分布。其中，任一个比特x_i在上述分布中出现0或1的概率如下：

$$\begin{cases} P\left[x_i=1|x\in L_+(x)\right]=a \\ P\left[x_i=0|x\in L_+(x)\right]=1-a \end{cases}, \tag{3}$$

$$\begin{cases} P\left[x_i=1|x\in L_-(x)\right]=1-a \\ P\left[x_i=0|x\in L_-(x)\right]=a \end{cases}, \tag{4}$$

$$\begin{cases} 0\leqslant a\leqslant 1 \\ i=1,2,\cdots,N \end{cases}。 \tag{5}$$

记L_+或者L_-分布出现的概率为

$$\begin{cases} P(L_k=L_+)=b \\ P(L_k=L_-)=1-b \end{cases}, \tag{6}$$

$$\begin{cases} 0\leqslant b\leqslant 1 \\ k=1,2,\cdots,n \end{cases}。 \tag{7}$$

对于这样一段非均匀随机序列，可以通过如下方法计算它的游程长度t以及它的概率分布$P_{ab}(t)$，$t=1,2,\cdots,N$，记$P_{ab}(t)$为从第1个比特开始的连续1的长度的概率，先考虑以下3种特殊的情况。

$$P_{ab}(t)=\left(ba^M\right)^t。 \tag{8}$$

图3第2行和第3行为连续L_+分布中出现1次L_-分布的情况，2种情况的概率相同，且此时的概率为

$$P_{ab}(t)=(1-b)(1-a)^M\left(ba^M\right)^{t-1}。 \tag{9}$$

进一步地，将所有可能的情况叠加得到一般情况：

$$P_{ab}(t)=C_t^0\left(ba^M\right)^t+C_t^1(1-b)(1-a)^M(ba^M)^{t-1}+\cdots+C_t^t\left[(1-b)(1-a)^M\right]^t。 \tag{10}$$

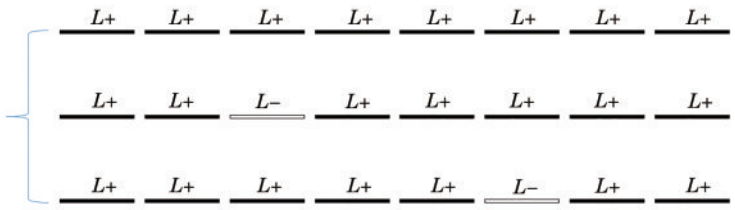

图3　非均匀序列的游程计算

Fig. 3　Calculating run lengths of nonuniform sequences.

式(10)中，若$b=1/2$，则意味着L_+或者L_-分布完全随机出现，则可以通过二项式展开定理将式(10)写为

$$P_{ab}(t)=C_t^0\left(\frac{a^M}{2}\right)^t+C_t^1\left[\frac{(1-a)^M}{2}\right]\left(\frac{a^M}{2}\right)^{t-1}+\cdots+C_t^t\left[\frac{(1-a)^M}{2}\right]^t, \tag{11}$$

$$P_{ab}(t)=\left(\frac{1}{2}\right)^{1-M}\left[\left(\frac{a}{2}\right)^M+\left(\frac{1-a}{2}\right)^M\right]^t。 \tag{12}$$

考虑$M=1$时的特殊情况，有

$$P_{ab}(t)=\left[\frac{a}{2}+\left(\frac{1-a}{2}\right)\right]^t=\left(\frac{1}{2}\right)^t。 \tag{13}$$

此时，得到了均匀分布序列的游程分布的情况。进一步地，如果先使用简单哈希函数将原始序列转换成(0,1)比例平衡的均匀序列，那么$b=\frac{1}{2}$这个条件便总是满足的，记此时的随机序列为平衡非均匀序列，其游程分布可以由式(12)改写为

$$P_a(t)=\left(\frac{1}{2}\right)^{1-M}\left[\left(\frac{a}{2}\right)^M+\left(\frac{1-a}{2}\right)^M\right]^t。 \tag{14}$$

2.2.2　平衡非均匀随机序列压缩

考虑对上述平衡非均匀随机序列进行压缩，即每间隔距离η保留1比特而舍弃其余数据。对进行$\eta(\eta\geqslant M)$压缩之后的新的比特序列进行游程计算分析，根据上述推论可得

$$P_a(t)=C_t^0\left(\frac{a}{2}\right)^t+C_t^1\left[\frac{(1-a)}{2}\right]\left(\frac{a}{2}\right)^{t-1}+\cdots+C_t^t\left[\frac{(1-a)}{2}\right]^t, \tag{15}$$

$$P_a(t)=\left[\frac{a}{2}+\left(\frac{1-a}{2}\right)\right]^t=\left(\frac{1}{2}\right)^t。 \tag{16}$$

这也正是均匀分布时的游程分布情况，此时的提取效率为

$$\beta=\frac{1}{\eta}。 \tag{17}$$

同样对于$\eta(\eta<M)$压缩之后的新的比特序列进行游程计算分析，w为每一段L_k经过η压缩操作之后保留的比特，可得

$$P_a(t)=C_t^0\left(\frac{a^w}{2}\right)^t+C_t^1\left[\frac{(1-a)^w}{2}\right]\left(\frac{a^w}{2}\right)^{t-1}+\cdots+C_t^t\left[\frac{(1-a)^w}{2}\right]^t, \tag{18}$$

$$P_a(t)=\left(\frac{1}{2}\right)^{1-w}\left[\left(\frac{a}{2}\right)^w+\left(\frac{1-a}{2}\right)^w\right]^t。 \tag{19}$$

由于$w>1$，此时的游程分布不满足均匀分布时

的游程情况，所以认为此时进行 η 压缩操作并不能改善序列的随机性质。综上可得，只有满足 $\eta \geqslant M$ 的压缩方式才能平衡非均匀序列，得到均匀序列。这里，也提出了一种寻找压缩因子 η 的方法，该方法描述如下。

若存在两列平衡非均匀分布的随机比特序列，其游程分布分别记为

$$\begin{cases} P_{a_1}(t)=\left(\frac{1}{2}\right)^{1-M_1}\left[\left(\frac{a}{2}\right)^{M_1}+\left(\frac{1-a}{2}\right)^{M_1}\right]^{t_1} \\ P_{a_2}(t)=\left(\frac{1}{2}\right)^{1-M_2}\left[\left(\frac{a}{2}\right)^{M_2}+\left(\frac{1-a}{2}\right)^{M_2}\right]^{t_2}。 \end{cases} \tag{20}$$

如果 $\left|P_{a_1}(t)-P_{a_2}(t)\right|<e$，且 e 足够小，则可以认为这两个随机序列的游程分布是近似的。若其中第 2 个序列可以视为均匀分布情况，即 $M_2=1$，此时有

$$\left|P_{a_1}(t)-P_{a_2}(t)\right|=\left|\left(\frac{1}{2}\right)^{1-M_1}\left[\left(\frac{a}{2}\right)^{M_1}+\left(\frac{1-a}{2}\right)^{M_1}\right]^{T_1}-\left(\frac{1}{2}\right)^{T_2}\right|<e, \tag{21}$$

式中：T_1 为第 1 个序列的最大游程长度；T_2 为第 2 个序列的最大游程长度。对于一串足够长的比特序列，此时的情况自然满足 e 足够小的前提，对于第 1 个平衡非均匀序列，选取一个合适的 η 值进行压缩，便可以将该序列转换为均匀分布的序列，也即是所提基于最大游程进行压缩的方法。η 的表达式为

$$\eta=T_1-T_2+1。 \tag{22}$$

3　分析与讨论

在实验过程中，注意到 ASE 光源的强度会影响光电探测器输出的电压强度，也即示波器 ADC 采样得到的随机数分布，如表 1 所示。当降低光源强度时，ADC 输出的随机数高位比特几乎难以输出有效的随机信息，这一点可通过最小熵反映。对于感兴趣的最小熵 $H_{\min}$ 的小数位，也就是在 LSBs 方法中被直接舍弃的高位比特，使用压缩因子 η 将 $H_{\min}$ 对应的高位比特部分保留。T_1 为最小熵的高比特位的最大游程，T_2 为最小熵的低比特位的最大游程，两者的差值表示了对应均匀分布的偏离程度。

以光功率为 40 mW 时测试得到的数据为例进行说明。使用探测 ASE 噪声得到的 100 Mb 的 8-bit 随机数据，共 800 Mb，计算此时的最小熵，为 4.95，$T_1=27$，$T_2=24$，压缩因子 $\eta=4(27-24+1)$。经过 LSBs 等简单哈希函数与最大游程计算的后处理方法，得到长度为 408 Mb 的比特序列，分为 400 组送入 NIST 检测程序进行检测，检测结果如表 2 所示。在置信程度 $\alpha=0.01$ 时，P 值应该大于 0.0001，比例应该大于 390/400 或者 238/246。可以看到，输出序列通过了全部的随机性测试项，这说明数据的随机性满足均匀随机数的标准。

表 1　不同光功率下比特序列的最大游程、压缩因子和最小熵

Table 1　Longest run length of bit sequences, compression factor and min-entropy of bit sequences under different ASE power

Power of ASE / mW	Longest run length of bit sequences T					Compression factor η	Min-entropy $H_{\min}$
	bit-3	bit-4	bit-5	bit-6	bit-7		
10	26	26	26	481		456	4.11
20	22	23	25	42		18	4.66
30	22	22	24	36		13	4.80
40	23	25	24	27		4	4.95
50		24	24	32	254	223	5.09
60		24	26	32	163	132	5.17

表 2　NIST 随机性检测结果[19]

Table 2　Results of the NIST-STS test suite for bit sequences[19]

Statistical test	P-value	Proportion
Frequency	0.3267	395/400
Block frequency	0.9357	394/400
Cumulative sums	0.0213	395/400
Runs	0.6371	400/400
Longest run	0.1041	391/400
Rank	0.0028	396/400
FFT	0.3753	399/400
Non overlapping template	0.1154	397/400
Overlapping template	0.7744	397/400
Universal	0.2190	396/400
Approximate entropy	0.1742	395/400
Random excursions	0.1824	243/246
Random excursions variant	0.4607	245/246
Serial	0.0609	398/400
Linear complexity	0.4846	398/400

所提后处理方法可以实现非常快的计算速度，原因在于其时间复杂度仅为 $O(N)$，与 Toeplitz 矩阵的时间复杂度 $O(N\log N)$ 相比，可以运行得更快。在实验中，当采集的数据达到 800 Mb 时，所提后处理方法和 Toeplitz 矩阵在 Matlab 上的运行时间为分别 10 min 和 360 min。同时，也比较了不同数据规模时，使用两种后处理方法分别花费的时间，所提方法总是能够比 Toeplitz 矩阵运行得更快，如图 4 所示。对一个 100 Mb 的 8-bit 的随机序列，若最小熵 $H_{\min}=4.95$，使用一般的 LSBs 后处理方法能提取最大比特数为 400 Mb，而所提方法能够提取出 408 Mb 的随机比特，具有更高的提取效率。

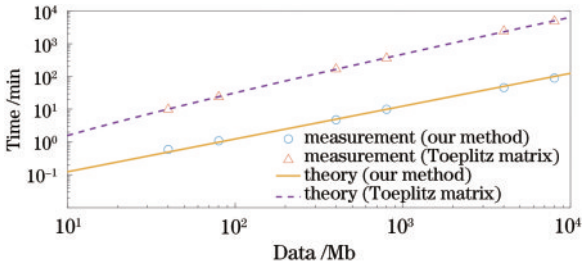

图 4 所提方法与 Toeplitz 矩阵对不同规模的随机比特进行后处理时花费的时间对比

Fig. 4 Comparison of the time spent on post-processing random bits of different scales between the proposed method and the Toeplitz matrix

4 结 论

基于自发辐射放大(ASE)的量子随机产生器,提出一种基于简单哈希函数的快速后处理方式。这种方式的时间复杂度为 $O(N)$,小于 Toeplitz 矩阵的 $O(N\log N)$,且随着随机比特数据规模增加,会表现出更明显的计算速度优势。并且,所提方法相对一般的 LSBs 后处理方法具有更高的随机数提取效率,并且这个提取效率与最小熵的小数部分成正比。

参 考 文 献

[1] Herrero-Collantes M, Garcia-Escartin J C. Quantum random number generators[J]. Reviews of Modern Physics, 2017, 89(1): 015004.

[2] Boaron A, Korzh B, Houlmann R, et al. Simple 2.5 GHz time-Bin quantum key distribution[J]. Applied Physics Letters, 2018, 112(17): 171108.

[3] Symul T, Assad S M, Lam P K. Real time demonstration of high bitrate quantum random number generation with coherent laser light[J]. Applied Physics Letters, 2011, 98(23): 231103.

[4] Yang J, Liu J L, Su Q, et al. 5.4 Gbps real time quantum random number generator with simple implementation[J]. Optics Express, 2016, 24(24): 27475-27481.

[5] Kogelnik H, Yariv A K. Considerations of noise and schemes for its reduction in laser amplifiers[J]. Proceedings of the IEEE, 1964, 52(2): 165-172.

[6] Argyris A, Pikasis E, Deligiannidis S, et al. Sub-Tb/s physical random bit generators based on direct detection of amplified spontaneous emission signals[J]. Journal of Lightwave Technology, 2012, 30(9): 1329-1334.

[7] Zhang X G, Nie Y Q, Liang H, et al. FPGA implementation of Toeplitz hashing extractor for real time post-processing of raw random numbers[C]//2016 IEEE-NPSS Real Time Conference (RT), June 6-10, 2016, Padua, Italy. New York: IEEE Press, 2016.

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

[9] Wei S H, Yang J, Fan F, et al. Compact quantum random number generator based on superluminescent light-emitting diodes[J]. The Review of Scientific Instruments, 2017, 88(12): 123115.

[10] Bustard P J, England D G, Nunn J, et al. Quantum random bit generation using energy fluctuations in stimulated Raman scattering[J]. Optics Express, 2013, 21(24): 29350-29357.

[11] Ma X F, Xu F H, Xu H, et al. Postprocessing for quantum random-number generators: Entropy evaluation and randomness extraction[J]. Physical Review A, 2013, 87(6): 062327.

[12] Gehring T, Lupo C, Kordts A, et al. Homodyne-based quantum random number generator at 2.9 Gbps secure against quantum side-information[J]. Nature Communications, 2021, 12(1): 1-11.

[13] Mansour Y, Nisan N, Tiwari P. The computational complexity of universal hashing[J]. Theoretical Computer Science, 1993, 107(1): 121-133.

[14] Skorski M. Evaluating entropy for true random number generators: efficient, robust and provably secure[M]// Chen K F, Lin D D, Yung M. Information security and cryptology. Lecture notes in computer science. Cham: Springer, 2017, 10143: 526-541.

[15] Peres Y. Iterating von Neumann's procedure for extracting random bits[J]. The Annals of Statistics, 1992, 20(1): 590-597.

[16] Fan L M, Chen H, Chen M H, et al. Corrected runs distribution test for pseudorandom number generators[J]. Electronics Letters, 2016, 52(4): 281-283.

[17] Chaitin G J. On the length of programs for computing finite binary sequences[J]. Journal of the ACM, 1966, 13(4):547-569.

[18] Liu L F, Miao S X, Liu B C. On nonlinear complexity and Shannon's entropy of finite length random sequences [J]. Entropy, 2015, 17(4): 1936-1945.

[19] NIST. SP. 800-22r1a. A statistical test suite for random and pseudorandom number generators for cryptographic applications[EB/OL]. [2022-11-09]. https://csrc. nist. gov/publications/detail/sp/800-22/rev-1a/final.