光学学报

10 Gbit/s量子随机数生成中多路实时高效后处理

张江江[1,2]，郭龑强[1,2*]，郑治沧[1]，林发定[1]，郭晓敏[1,2]

[1]新型传感器与智能控制教育部重点实验室，太原理工大学物理与光电工程学院，山西 太原 030024；

[2]密码科学技术国家重点实验室，北京 100878

摘要 为了实现量子随机数实时安全高速后处理，在实验上利用平衡零拍探测将采集得到的量子真空噪声中的4个相互独立的高频边带模式作为熵源，在单通道240 MSa/s采样率、16位模数转化条件下进行四路并行提取，并在现场可编程门阵列(FPGA)中完成多路实时Toeplitz-Hash安全高速后处理。实现了大规模Toeplitz矩阵分解及多周期分布处理，从而保证了硬件的稳定运行；研究了不同矩阵规模和通道数下安全后处理的硬件资源占有率，最终在四路Toeplitz-Hash后处理条件下，实现了FPGA逻辑资源占有率为62%、实时速率为10.44 Gbit/s的量子随机数生成。每两路通道之间量子随机数的互相关和互信息分别在10^{-3}和10^{-6}以下，且合并输出的量子随机数通过了NIST、Diehard和TestU01测试，为其在高速保密通信的实际应用中提供重要支撑。

关键词 量子光学；量子随机数发生器；多路实时后处理；现场可编程门阵列；平衡零拍探测

中图分类号 O431.2 **文献标志码** A **DOI**：10.3788/AOS202242.2327003

Multiplex Real-Time and High-Efficiency Post-Processing in 10 Gbit/s Quantum Random Number Generation

Zhang Jiangjiang[1,2], Guo Yanqiang[1,2*], Zheng Zhicang[1], Lin Fading[1], Guo Xiaomin[1,2]

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

[2]*State Key Laboratory of Cryptology, Beijing* 100878, *China*

Abstract In order to realize the real-time, secure, and high-speed post-processing for quantum random number generation, this work experimentally takes four independent high-frequency sideband modes from quantum vacuum noise as entropy sources using balanced homodyne measurement. In addition, the paper performs four-channel parallel extraction under a sampling rate of 240 MSa/s and 16-bit analog-to-digital conversion in each channel and achieves multiplex real-time, and high-speed Toeplitz-Hash post-processing in a field programmable gate array (FPGA). The large-scale Toeplitz matrix is decomposed, and multi-cycle distributed processing is performed to ensure the stable operation of hardware. Furthermore, the paper investigates the hardware resource occupancy rate of secure post-processing with different matrix sizes and channel numbers, and finally realizes four-channel Toeplitz-Hash post-processing with an FPGA logical resource occupancy rate of 62% and quantum random number generation with a real-time rate of 10.44 Gbit/s. The cross correlation and mutual information of quantum random numbers between every two channels are below 10^{-3} and 10^{-6}, respectively, and the accumulatively generated quantum random numbers pass the NIST, Diehard, and TestU01 tests. Therefore, this work provides important support for the practical applications of quantum random numbers in high-speed and secure communication.

Key words quantum optics; quantum random number generator; multiplex real-time post-processing; field programmable gate array; balanced homodyne detection

收稿日期：2022-04-21；**修回日期**：2022-06-09；**录用日期**：2022-06-20

基金项目：国家自然科学基金(62075154, 61875147, 62175176, 61731014)、山西省重点研发计划-国际科技合作(201903D421049)、山西省回国留学人员科研资助项目(HGKY2019023)

通信作者：*guoyanqiang@tyut.edu.cn

1 引 言

随机数在信息科学、统计学、密码学中发挥着基础且重要的作用，决定着信息系统的安全[1-2]。量子随机数因其内禀量子随机性及信息论可证的安全性已受到广泛关注，并在信息安全应用中变得日益重要[3-5]。目前，已有多种量子随机数产生方案，如基于光子分布及到达时间[6-8]、相位噪声[9-11]、拉曼散射[12-13]、衰减光脉冲[14]、放大自发辐射[15-16]、隧穿效应[17]等。在上述方案中，有的因单光子探测带宽限制量子随机数生成速率难以突破 Gbit/s 量级，还有的因设备器件数量相对较多、系统相对复杂，不利于集成。基于真空态量子正交分量起伏[18-23]产生量子随机数的方案，在生成速率及实用化方面有着自身的优势：真空态量子噪声为不同频率间彼此独立、互不相关的宽带白噪声，且不受攻击者关联控制，可测量提取高速随机序列的连续变量熵源。

理想情况下基于真空量子分量起伏可以制备不被复制和预测的量子随机数，但是在实际过程中不可避免地会受到经典噪声影响[24-25]，导致量子随机数的安全性和生成质量降低，故需对原始随机数进行安全的后处理[26-29]。在众多物理随机数后处理方案中，Toeplitz-Hash后处理作为信息论可证的安全后处理方法，已被应用于基于现场可编程门阵列（FPGA）实时后处理实验研究中。目前利用 FPGA 实时后处理制备的真空态量子随机数速率已达 3.2 Gbit/s[30]、6 Gbit/s[31-32]、8.05 Gbit/s[33]，而实际应用中需要的量子随机数实时产率至少达到 10 Gbit/s[34]，同时需要匹配高速的数据采集和实时高效的安全后处理。但上述后处理过程中模数转换（ADC）采样频率高达 GSa/s 量级，这将对 FPGA 硬件处理资源及性能提出较高要求，后处理会受到 FPGA 硬件资源的限制，减缓了量子随机数实用化进程。因此，基于有限资源的 FPGA 如何实现对大量原始随机序列的高速实时安全后处理，并高效利用 FPGA 硬件资源已成为量子随机数实用化过程中尚待解决的问题。

本文基于平衡零拍测量的真空态量子分量起伏产生量子随机数的方案，利用从宽带量子散粒噪声内提取的 4 个高频边带作为熵源，对其进行四路并行实时 Toeplitz-Hash 安全高速后处理。实验测量噪声功率谱及四路频带提取后的原始随机序列强度分布，并利用 NIST 最小熵测量原始随机比特的熵含量；分析了 FPGA 中大规模 Toeplitz-Hash 矩阵拆分成不同规模小矩阵及其在不同通道数下进行后处理的硬件资源占用率，通过优化矩阵规模、采样范围及时序，确定量子条件最小熵和提取比例，最终在低采样率、高有效量化位数的条件下，实现了四路实时并行的高速量子随机数产生及安全高效后处理，并且生成的量子随机数通过相关性及多项随机性测试，保证了其生成及实时高效后处理质量。

2 实验装置与熵源制备

2.1 四路实时并行量子随机数产生及后处理实验装置

基于真空态量子噪声的四路实时量子随机数产生及后处理实验装置如图 1 所示。该系统主要由光场平衡零拍探测和熵源信号量化后处理两部分构成。一台中心波长为 1550 nm 的单模激光器作为本底振荡（LO），由高精度电流源及温控源控制，最大输出功率为 15 mW。利用由多组半波片（HWP）和偏振分束器（PBS）组成的偏振控制及分束装置，确保真空态和 LO 干涉，最终形成功率比为 50∶50 的两束平衡光进入带宽为 1.6 GHz 的平衡探测器。两路光信号在光电转换后，经减法器（Sub）差分放大后输出，获得平衡零拍探测带宽内的真空散粒噪声信号。随后信号被分成 4 路，分别进行四路混频滤波，以提取不同中心频率的量子边带模式；通过 4 个采样率为 240 MSa/s、量化位数为 16 的 ADC 实时采样量化获取原始随机比特。获得的原始随机比特进入 FPGA 实行多路并行的实时 Toeplitz-Hash 后处理。经实时安全处理后生成的高速量子随机数通过高速串行计算机扩展总线（PCIE）上传到存储设备，用于后期的离线随机性测试及应用。

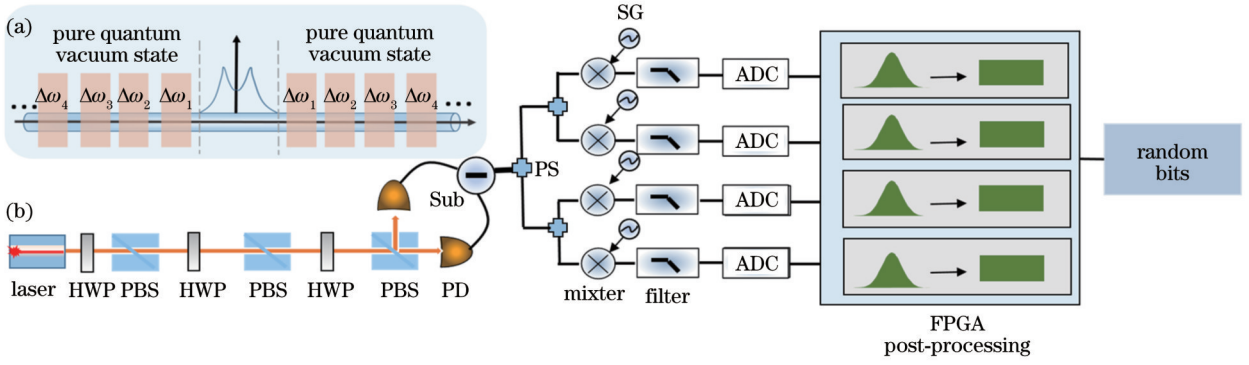

图 1 基于真空态正交分量起伏的多路实时量子随机数产生及后处理实验的装置图

Fig. 1 Experimental setup of multiplex real-time quantum random number generation and post-processing based on quadrature fluctuations of vacuum state

2.2　真空边频模熵源多路并行提取

基于以上真空态量子随机数产生实验装置，对熵源进行平衡零拍测量并提取其中多路量子边带模式。图2所示为测量得到的1.6 GHz带宽内的散粒噪声功率谱，量子散粒噪声强度高于电子学噪声强度10 dB以上，以保证在宽带量子噪声条件下获得较高的信噪比。对四路边频模式进行提取，中心频率分别为200、500、800、1100 MHz，每路低通滤波截止带宽均为120 MHz，以实现4个不同中心频率的边频模式熵源制备。四路子熵源分别由不同的ADC采样量化，每一路均通过优化采样量化范围实现ADC的最优采样，随后对四路真空边带模式熵源进行原始信号的分析评测。

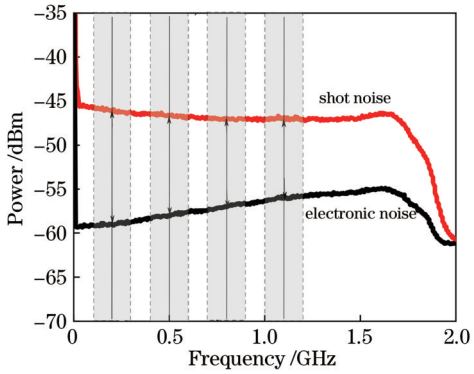

图2　真空态量子散粒噪声功率谱的测量结果

Fig. 2　Measured power spectra of quantum shot noise of vacuum state

利用美国国家标准NIST 800-90B熵评估测试[35]进行评测，完成对4个通道原始信号的随机分布特性及熵值测试。实验中对熵源采样的ADC量化精度为16位，即每个样本空间的大小为2^{16}，根据测试要求采用低8位信号进行熵值测试，4个通道熵值测试结果如图3所示。所得的最小熵来自10个测试项的最小值，每8-bit位依次为5.576、5.274、5.510、5.493，相应的最大熵值分别为7.965、7.947、7.978、7.976，测试结果表明提取的四路子熵源具有良好的随机质量。

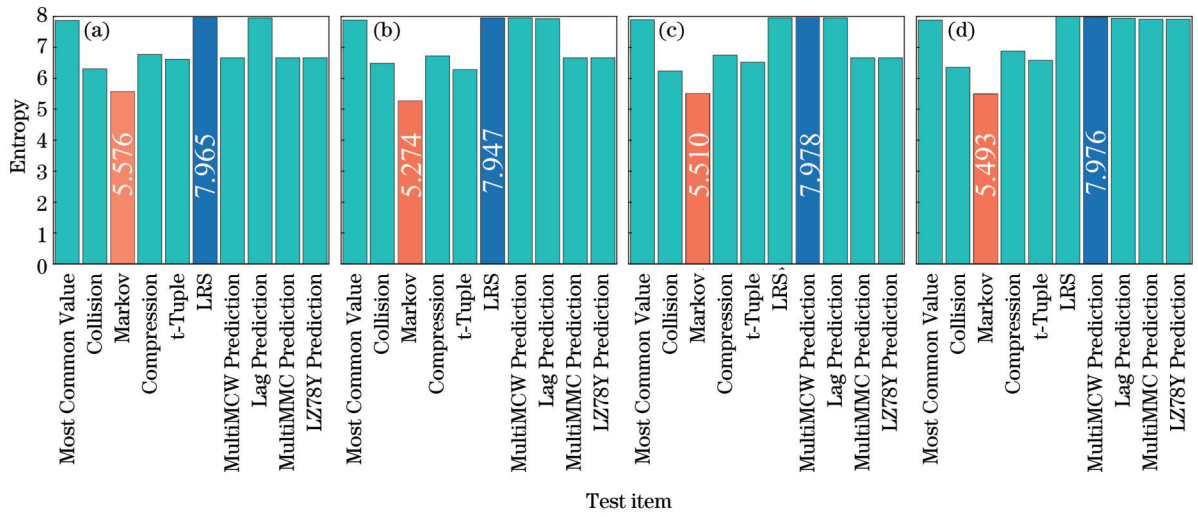

图3　四路子熵源信号的NIST熵值评估测试结果

Fig. 3　Test results of NIST entropy for four sub-source signals

3　多路实时高效后处理

3.1　四路Toeplitz-Hash后处理流程设计及算法优化

Toeplitz-Hash后处理是一种信息论可证且硬件可实现的安全后处理，可有效剔除原始序列中可被窃听者获取的经典噪声信息。基于对四路真空量子噪声子熵源的提取，在单片FPGA中实现Toeplitz-Hash后处理，但大规模Toeplitz矩阵会给有限资源的FPGA带来严重消耗，故对大规模Toeplitz矩阵进行拆分，同时利用多路并行后处理来降低对硬件资源的占用率。如图4所示，在FPGA中建立4路通道来对多个量子熵源的频带模式进行后处理。

充分利用FPGA的逻辑资源来最优化量子随机数产率，四通道Toeplitz后处理结构框架如图4所示，采集原始信号经ADC量化后进入FPGA，将大规模Toeplitz矩阵拆分为子矩阵(SUB)以在多个时钟周期内稳定执行，同时利用与处理(AND)代替乘法器，避免由较高资源占用率引起的时序收敛难问题，且利用异或门(XOR)代替加法器，将所有拆分后的矩阵处理结果按位异或后得到整个Toeplitz矩阵的提取结果。

Toeplitz-Hash安全后处理过程中不涉及浮点或连续函数运算，可充分利用FPGA硬件平台的优势。如式(1)所示，以$x \times y$规模的Toeplitz矩阵为例，每一行矩阵元分别与ADC量化的原始比特相乘，并对相乘的结果进行相加，得到最终的安全随机序列，即处理长度为y的原始序列乘法和加法运算各需执行$x \times y$次。

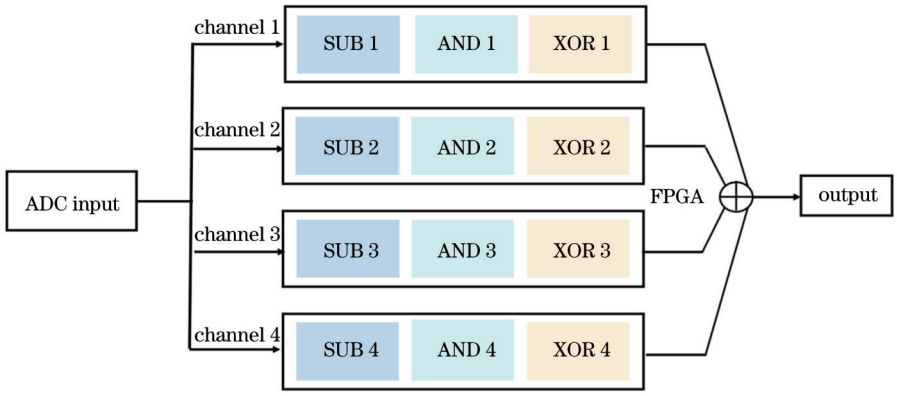

图 4　Toeplitz后处理四通道流程设计框架

Fig. 4　Procedure framework of four-channel Toeplitz post-processing

$$\begin{bmatrix} t_x & t_{x+1} & \cdots & t_{x+y-1} \\ t_{x-1} & t_x & \cdots & t_{x+y-2} \\ \vdots & \vdots & & \vdots \\ t_2 & t_3 & \cdots & t_{y+1} \\ t_1 & t_2 & \cdots & t_y \end{bmatrix} \times \begin{bmatrix} d_1 \\ d_2 \\ \vdots \\ d_{y-1} \\ d_y \end{bmatrix} = \begin{bmatrix} a_1 \\ a_2 \\ \vdots \\ a_{x-1} \\ a_x \end{bmatrix}, \quad (1)$$

式中：$t_1, t_2, \cdots, t_{x+y-1}$为Toeplitz矩阵的元素；$d_1, d_2, \cdots, d_y$为ADC量化后的原始比特；$a_1, a_2, \cdots, a_x$为Toeplitz矩阵处理后的结果。由于本实验选用的Kentex-7芯片的查找表为6输入2输出，如表1所示，对于576×768的Toeplitz矩阵，四路后处理所需的乘法和加法的总运算次数约为353万次，后处理乘法和加法处理需要约71万个查找表，而Kentex-7一共只能提供约20万个查找表资源，因此无法直接实现576×768及更大矩阵规模的多路后处理。

表 1　四通道后处理矩阵拆分前后的运行次数以及处理周期

Table 1　Total operation number and processing cycle of four-channel post-processing before and after splitting matrix

Matrix	96×144	192×256	384×512	408×544	456×608	576×768
Pre-split	110592	393216	1572864	1775616	2217984	3538944
After-split	12288	24576	49152	52224	58368	73728
Processing cycle	9	16	32	34	38	48

为了保证硬件的稳定运行，将大规模Toeplitz矩阵后处理过程进行拆分，通过增加后处理所需的时钟处理周期来分步实现大规模Toeplitz矩阵的乘法。如表1所示，在576×768 Toeplitz矩阵拆分后，四路后处理所需的乘法和加法的总运行次数约为7.3万次，需要约1.5万个查找表，运行时需要48个时钟周期，矩阵拆分后运行次数约为拆分前的2%，运行次数明显降低，从而有效提升了Toeplitz矩阵的后处理效率，为FPGA的多路并行后处理奠定了基础。同时，为了使ADC量化后的原始比特能及时被Toeplitz-Hash后处理实时提取，拆分后矩阵列数为ADC量化位数16。拆分后的子矩阵按顺序处理原始比特，每个子矩阵的处理过程都在一个时钟周期内完成，处理y个原始随机序列需要$y/16$个时钟周期，FPGA在每个时钟周期都能读取ADC量化的16位原始随机比特进行处理，因此矩阵拆分后并不影响后处理的实时性与性能。

3.2　多路实时Toeplitz-Hash后处理的硬件实现

对矩阵规模及算法优化后，在FPGA中可构建最优的硬件后处理模型，然而由于FPGA资源的限制，需要监测FPGA执行不同规模矩阵时的资源占用情况，以达到更高的实时量子随机数提取速率。本实验在Kentex-7的FPGA上进行了不同矩阵规模的后处理并对资源消耗进行监测，以找到合适的后处理硬件配置方案。Toeplitz矩阵可以由$x+y-1$个元素构造规模为$x \times y$的矩阵，通过构造不同的矩阵规模及利用不同的后处理通道数分析FPGA的资源占用情况。在240 MHz单通道后处理时钟频率、ADC 16-bit量化条件下，根据实验中Toeplitz-Hash并行四路后处理的最优条件，可实现支持3.84、7.68、11.52、15.36 Gbit/s实时速率的原始比特随机提取器。实验上使用Kentex-7型FPGA可提供约203800个查找表(LUT)，分析了不同通道、不同矩阵规模后处理条件下FPGA查找表的资源消耗，结果如图5所示。可以发现，对于576×768的Toeplitz矩阵，单通道Toeplitz-Hash后处理的FPGA查找表资源仅使用了98966个查找表，占用查找表总量的比例约为48%，不仅没有充分利用FPGA的硬件资源，处理实时输入的原始比特速率也低于多通道后处理。但对于576×768的Toeplitz矩阵，在进行三通道后处理时，使用了176926个FPGA查找表，占用约86%的硬件资源，此时处理实时原始比特的速率为11.52 Gbit/s，不能完成对更高原始比特速率15.36 Gbit/s的处理，更大的矩阵规模及更多的通道数受到FPGA硬件资源量的限制。为了处理更高实时速率的原始比特，以下考虑四通道、更优矩阵规模、更低资源占有率的实时后处理。

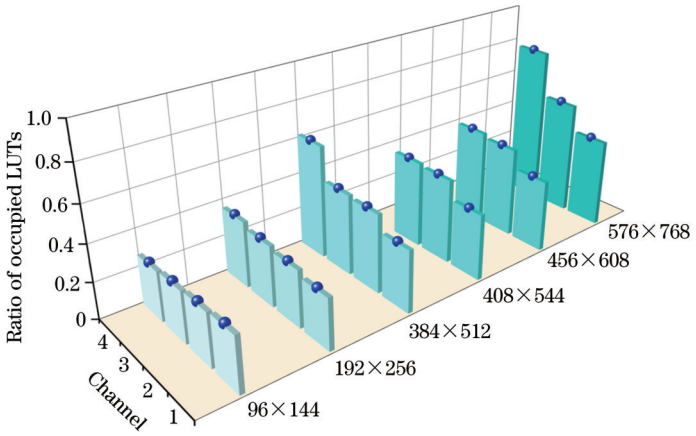

图 5　不同通道数、不同矩阵规模 Toeplitz-Hash 后处理时 FPGA 的硬件资源占用

Fig. 5　FPGA hardware resource occupancy of different channels and matrix size in Toeplitz-Hash post-processing

根据信息论的 Leftover-Hash 引理确定每路通道原始数据中量子随机数的提取比例，Toeplitz-Hash 安全后处理的最终随机数提取比例与 Toeplitz 矩阵的行向量和列向量直接相关，利用 $x \times y$ 的 Toeplitz 矩阵处理序列长度为 y 的原始随机比特，可提取序列长度为 x 的安全随机数，矩阵规模和量子条件最小熵的关系为

$$x \leqslant y \times H_{\min} - \log_2 \frac{1}{\varepsilon_{\text{hash}}^2}, \tag{2}$$

式中：$\varepsilon_{\text{hash}}$ 为 Hash 安全参数，表征经过后处理得到的随机数和理想完全随机的随机数之间的距离。利用采集得到的四路子熵源原始序列，经高斯拟合统计分布之后计算得到各个通道每 16 bit 的量子条件最小熵含量分别为 14.22、14.16、13.88、13.83，即量子条件最小熵含量比例依次为 88.86%、88.48%、86.77%、86.40%。对于中心频率为 200 MHz 的测量提取通道，其量子条件最小熵为 14.22，当安全参数为 2^{-50} 时，由式(2)可得 Toeplitz 矩阵规模为 354 × 512，即可得出最终量子随机数的提取比例为 69.14%。根据单路通道 3.84 Gbit/s 实时原始比特产生速率以及提取比例，可得到该通道量子随机数实时生成速率为 2.65 Gbit/s。对于提取中心频率为 500、800、1100 MHz 的其余 3 路通道，根据确定的安全参数和式(2)得到的 Toeplitz 矩阵规模为 353 × 512、344 × 512、342 × 512，故其余 3 路通道的提取比例依次为 68.94%、67.18%、66.79%，量子随机数实时生成速率依次为 2.64、2.58、2.57 Gbit/s。综合以上各路通道的随机数生成速率，可得最终四路并行量子随机数实时产生速率达到 10 Gbit/s 量级，并将 4 路通道经过安全后处理实时产生的量子随机数，通过 PCIE 接口输出到应用设备。在此四路并行 Toeplitz-Hash 后处理过程中，FPGA 使用了 126928 个查找表，占用约 62% 的硬件资源，可处理实时输入速率为 15.36 Gbit/s 的原始比特，硬件资源消耗相对于三通道最大可占用资源降低了 24%，最终量子随机数实时生成速率可达 10.44 Gbit/s，系统稳定性更高，且硬件资源的利用率明显提升。

3.3　四路实时 Toeplitz-Hash 后处理前后信号的统计分布

为了评测实时硬件后处理的信号统计分布，以下通过测量分析原始信号强度及后处理之后随机比特的统计分布，结果如图 6 所示。图 6(a1)～(d1)所示为测

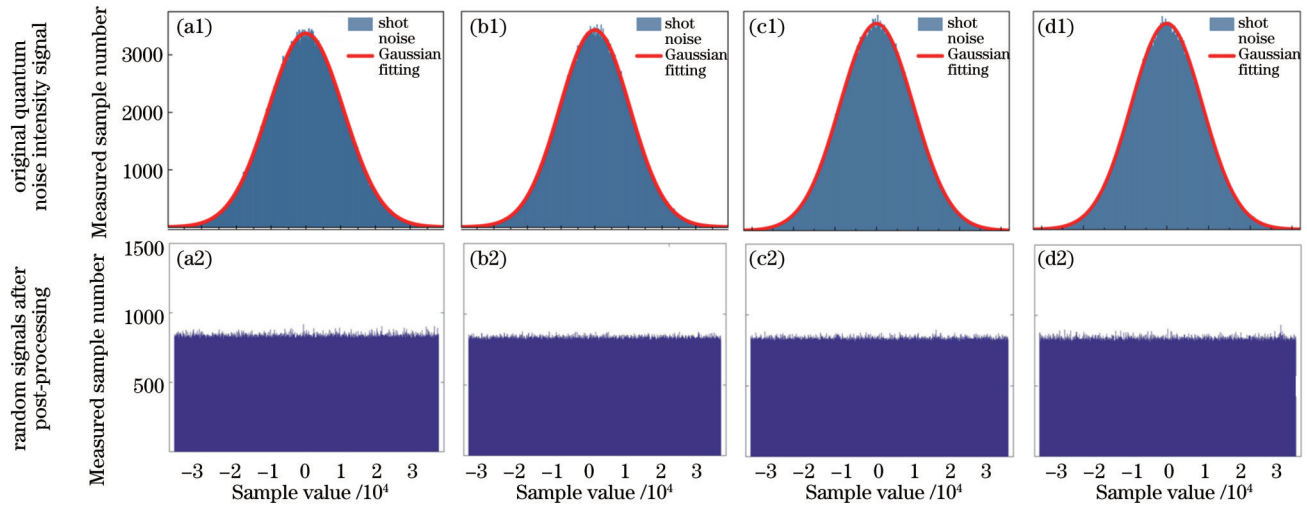

图 6　实时 Toeplitz-Hash 后处理前后信号的统计分布结果

Fig. 6　Statistical distribution of random signals before and after real-time Toeplitz-Hash post-processing

得的四路原始量子噪声强度信号的统计分布，其呈高斯随机分布。随后利用16-bit ADC对采集的原始信号进行多位高精度量化，进而通过实时Toeplitz-Hash后处理完成最终量子随机比特的安全输出，图6(a2)～(d2)所示为后处理之后四路量子随机比特所呈现的均匀分布，可以发现经Toeplitz-Hash后处理之后每路通道的16位比特都可均匀输出，展现出良好的实时硬件后处理效果。

4 基于实时后处理生成量子随机数的测试结果

为了评测生成的量子随机数及实时Toeplitz-Hash后处理质量，以下对四路并行高速实时后处理之后每两路通道量子随机数的相关性、互信息及最终四路总的随机性进行了测试。图7所示为四路通道中每两路生成量子随机数的互相关和互信息，通过对10^6以上的量子随机数进行统计分析，发现每两路通道随机比特之间的互相关和互信息分别低于10^{-3}和10^{-6}，表明不同通道之间产生的随机比特具有很低的相关性，可满足高质量并行量子随机数的产生要求。

同时将经过四路安全后处理之后采集的量子随机数进行位图测试，图8为利用128×128的量子随机比特得出的4路通道和每两路通道间的比特位图，其中a～d表示4路通道，n表示对应通道的比特流，⊕表示异或运算。分别从4路通道选取128×128个随机比特位，依次将随机比特放入128×128的位图矩阵中，可直接得到4路各自随机数的相关性，从其位图可知图像无相关或固定规律，呈明显的随机分布；同时进行每两路之间随机比特的异或及位图相关分析，发现每两路之间无相关性且与单路随机比特也不相关，呈明显

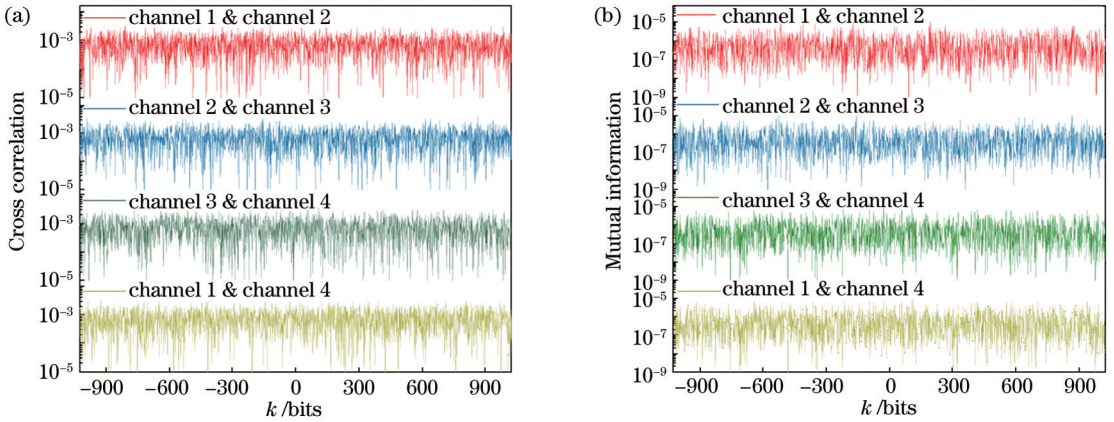

图7 每两路通道间量子随机比特的互相关和互信息。(a)互相关；(b)互信息

Fig. 7 Cross correlation and mutual information between quantum random bit streams of every two channels. (a) Cross correlation; (b) mutual information

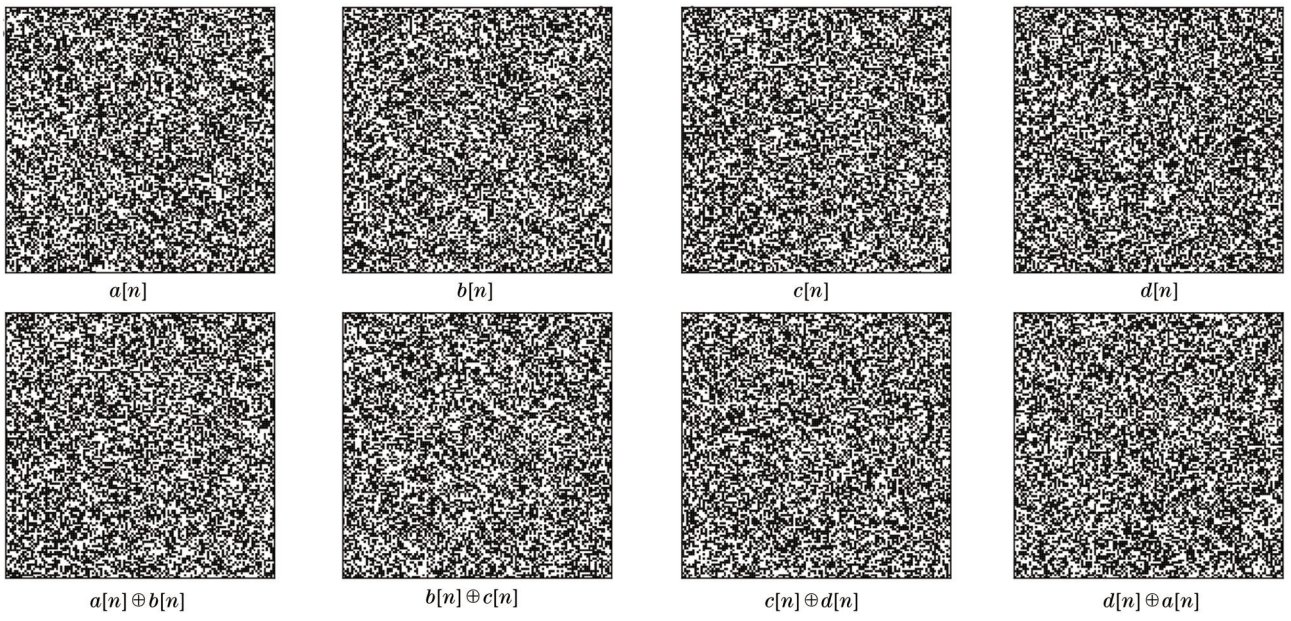

图8 并行四路各自量子随机比特流及每两路之间异或量子随机比特流的128×128位图

Fig. 8 128×128 bitmaps of each channel quantum random bit streams and every two interchannel XOR results

的随机分布，表明四路并行的量子随机数具有良好的随机性。

对最终实时生成的 10.44 Gbit/s 量子随机数进行随机性测试。首先，采用美国国家标准的 NIST 随机性测试方法对经过 Toeplitz-Hash 后处理的随机数进行检测。NIST 随机性测试包含 15 种随机测试项目，用来表征随机比特的随机性质量，每项测试都可通过 P 来反映实际的随机性指标。将并行四路经 Toeplitz-Hash 实时后处理产生的量子随机数进行每 1 Gbit 的 NIST 测试，每 1 Gbit 的样本数为 10^3，每个样本的随机数长度为 1 Mbit，当显著性水平 $\alpha=0.01$ 时，15 项测试的 P 值均大于 0.01，表明所提方法产生的量子随机数通过了 NIST 相应的全部测试项，测试结果如图 9 所示。

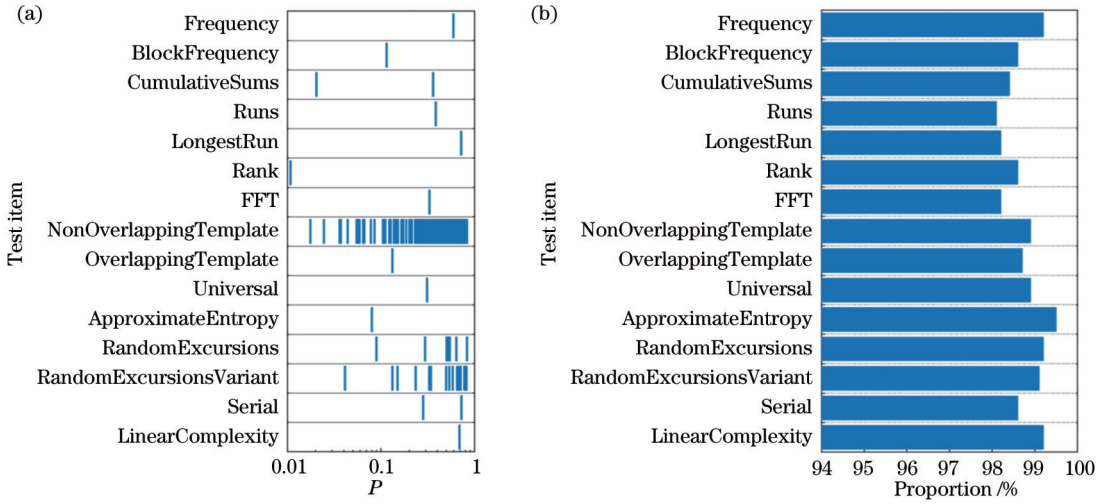

图 9　实时生成量子随机数的 NIST 测试结果。(a) P 值；(b) 资源占用比例

Fig. 9　NIST test results for real-time quantum random number. (a) P value; (b) resource usage ratio

针对并行四通道经 Toeplitz-Hash 实时后处理的量子随机数进行 Diehard 随机统计测试，结果如图 10 所示。测试结果表明，所有测试项最终的 P 值都在 0.01 到 0.99 的置信区间内，产生的量子随机数通过了 Diehard 统计测试套件的所有测试项。

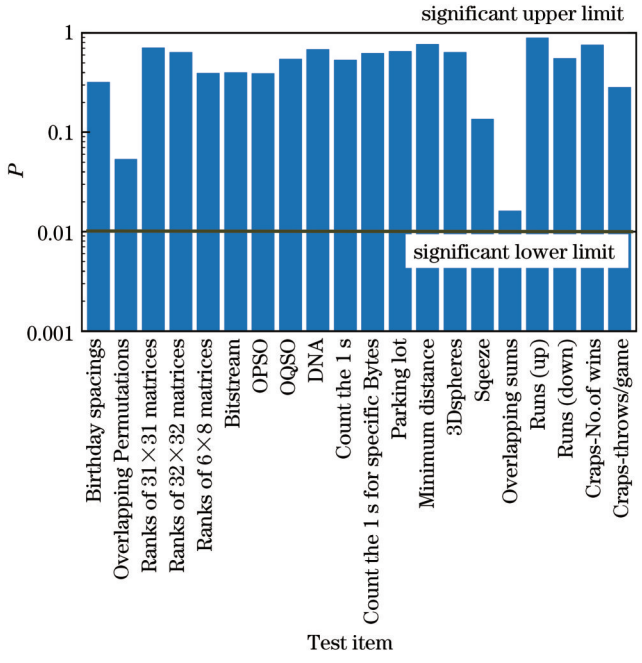

图 10　实时生成量子随机数的 Diehard 测试结果

Fig. 10　Diehard test results for real-time quantum random number

对高速实时生成的量子随机数进行 TestU01-SmallCrush 测试，结果如图 11 所示，所有 15 个测试项的 P 值都在 0.01 到 0.99 的置信区间内，表明产生的量子随机数通过了本次 TestU01 的随机性检测，再次验证了本实时量子随机数产生方案生成的随机数具有良好的随机性。

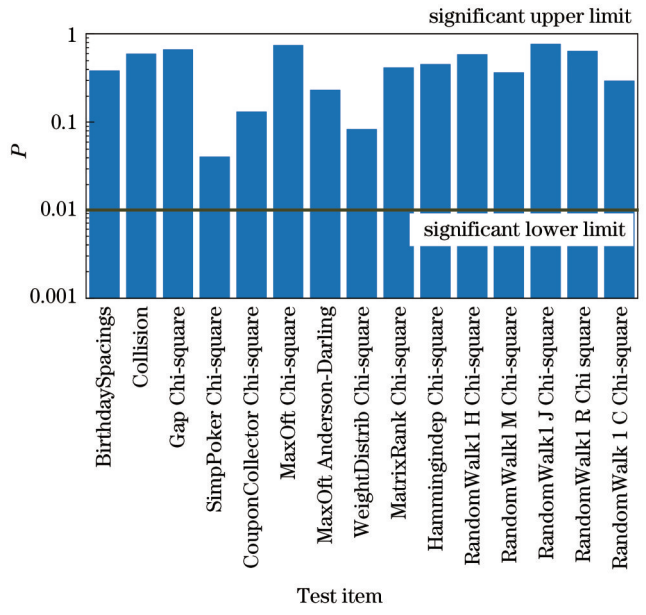

图 11　实时生成量子随机数的 TestU01-SmallCrush 测试结果

Fig. 11　TestU01-SmallCrush test results for real-time quantum random number

5 结 论

基于真空散粒起伏制备量子随机数方案，实验上利用宽带平衡零拍测量从熵源中并行提取了四路独立的高频边带量子噪声模式，在最优动态采样范围的条件下提高本底增益，进而增强了系统的量子熵含量，分析了各子熵源信号的NIST测试最小熵及量子条件最小熵。随后在FPGA内将大规模Toeplitz矩阵进行拆分，通过增加后处理所需的时钟运算周期数来分步实现大规模Toeplitz矩阵处理，同时对后处理过程算法进行优化，以降低运行复杂度，完成实时Toeplitz-Hash硬件后处理的构建。分析研究了不同矩阵规模和不同通道数量FPGA的资源消耗情况，最终在对矩阵规模和通道数优化后，实现了FPGA硬件资源消耗62%、单通道采样率为240 MSa/s、16-bit ADC量化的四路并行Toeplitz-Hash实时高效后处理，制备产生了速率为10.44 Gbit/s的量子随机数，在有效改善FPGA资源利用的同时提高了量子随机数的实时产生速率。不同通道间生成的量子随机数的互相关和互信息均在10^{-3}和10^{-6}以下，合并高速产生的量子随机数通过了NIST、Diehard、TestU01随机统计测试，为该量子随机数在保密通信中的应用提供了数据支撑。

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

[3] Ma X F, Yuan X, Cao Z, et al. Quantum random number generation[J]. npj Quantum Information, 2016, 2: 16021.

[4] Pirandola S, Andersen U L, Banchi L, et al. Advances in quantum cryptography[J]. Advances in Optics and Photonics, 2020, 12(4): 1012-1236.

[5] Lin X, Wang S, Yin Z Q, et al. Security analysis and improvement of source independent quantum random number generators with imperfect devices[J]. npj Quantum Information, 2020, 6: 100.

[6] 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.

[7] 鄢秋荣, 赵宝升, 刘永安, 等. 基于单光子脉冲时间随机性的光量子随机源[J]. 光学学报, 2012, 32(3): 0327001.
Yan Q R, Zhao B S, Liu Y A, et al. Optical quantum random number generator based on the time randomness of single-photon pulse[J]. Acta Optica Sinica, 2012, 32(3): 0327001.

[8] 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.

[9] 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]. Optics Letters, 2010, 35(3): 312-314.

[10] Guo H, Tang W Z, Liu Y, et al. Truly random number generation based on measurement of phase noise of a laser[J]. Physical Review E, 2010, 81(5): 051137.

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

[12] England D G, Bustard P J, Moffatt D J, et al. Efficient Raman generation in a waveguide: a route to ultrafast quantum random number generation[J]. Applied Physics Letters, 2014, 104(5): 051117.

[13] Hu Y Y, Lin X, Wang S, et al. Quantum random number generation based on spontaneous Raman scattering in standard single-mode fiber[J]. Optics Letters, 2020, 45(21): 6038-6041.

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

[15] Zhang Q, Zhou C H, Meng J W, et al. Parallel quantum random number generation based on spontaneous emission of alkaline earth[J]. Applied Physics Express, 2020, 13(1): 012015.

[16] Zhou H Y, Yuan X, Ma X F. Randomness generation based on spontaneous emissions of lasers[J]. Physical Review A, 2015, 91(6): 062316.

[17] Zhou H H, Li J L, Zhang W X, et al. Quantum random number generator based on tunneling effects in a Si diode[J]. Physical Review Applied, 2019, 11(3): 034060.

[18] 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.

[19] Shen Y, Tian L, Zou H X. Practical quantum random number generator based on measuring the shot noise of vacuum states[J]. Physical Review A, 2010, 81(6): 063814.

[20] 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.

[21] Zhu Y Y, He G Q, Zeng G H. Unbiased quantum random number generation based on squeezed vacuum state[J]. International Journal of Quantum Information, 2012, 10(1): 1250012.

[22] Guo X M, Cheng C, Wu M C, et al. Parallel real-time quantum random number generator[J]. Optics Letters, 2019, 44(22): 5566-5569.

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

[24] 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.

[25] 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.

[26] Raz R, Reingold O, Vadhan S. Extracting all the randomness and reducing the error in Trevisan's extractors[J]. Journal of Computer and System Sciences, 2002, 65(1): 97-128.

[27] 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.

[28] 魏世海, 樊矾, 杨杰, 等. 高速小型化光量子随机数发生器[J]. 中国激光, 2018, 45(5): 0512001.
Wei S H, Fan F, Yang J, et al. Ultrafast compact optical quantum random number generator[J]. Chinese Journal of Lasers, 2018, 45(5): 0512001.

[29] Shi Y C, Chng B, Kurtsiefer C. Random numbers from vacuum fluctuations[J]. Applied Physics Letters, 2016, 109(4): 041101.

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

[31] Xu B J, Chen Z Y, Li Z Y, et al. High speed continuous variable source-independent quantum random number generation[J]. Quantum Science and Technology, 2019, 4(2): 025013.

[32] 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): 043105.

[33] Drahi D, Walk N, Hoban M J, et al. Certified quantum random numbers from untrusted light[J]. Physical Review X, 2020, 10(4): 041048.

[34] Xu F H, Ma X F, Zhang Q, et al. Secure quantum key distribution with realistic devices[J]. Review of Modern Physics, 2019, 92(2): 025002.

[35] Turan M S, Barker E, Kelsey J, et al. Recommendation for the entropy sources used for random bit generation [EB/OL]. (2016-01-27) [2022-01-10]. https://csrc.nist.gov/csrc/media/publications/sp/800-90b/draft/documents/draft-sp800-90b.pdf.