文章编号 1004-924X(2019)07-1492-08

量子随机数高斯噪声信号发生器

余恒炜^{1,2},孙晓娟^{2,3},王星辰^{1,2},蒋 科^{2,3},吴 忧^{2,3},

程东碧^{1,2},石芝铭^{2,3},贾玉萍^{2,3},黎大兵^{2,3}*

(1. 中国科学技术大学 微电子学院,安徽 合肥 230026;

2. 中国科学院大学 材料与光电研究中心, 吉林 长春 130033;

3. 中国科学院 长春光学精密机械与物理研究所 发光学及应用国家重点实验室, 吉林 长春 130033)

摘要:现有的高斯噪声信号发生器都是采用数学计算的方式生成随机数的,这种方式不能实现真正的随机信号,与实际 噪声信号不符。本文提出基于量子随机数的高斯噪声信号发生器,通过单光子探测器对选择路径的光子信号的探测作 为随机数的来源,实现基于真随机的高斯噪声信号发生器。将得到的随机数经过 WGN 高斯算法处理得到高斯噪声信 号,在 FPGA 中使用 verilog 语言实现。对产生的噪声信号进行幅度谱和功率谱分析,结果表明产生的噪声信号幅度值 在 0~255 之间变化,幅度谱服从高斯分布,噪声信号的功率谱在 20 dB 上下均匀波动,服从均匀分布,满足高斯白噪声 的特性。与现有的噪声信号发生器相比,基于量子随机数的实现方式,其随机数来源清晰,能够做到真正的随机性,为实 现真随机数的高斯噪声信号发生器提供了一种简易的方案。

关 键 词:高斯噪声;单光子;随机数源;幅度谱;功率谱

中图分类号:O413;TN911.22 文献标识码:A doi:10.3788/OPE.20192707.1492

Quantum random number Gaussian noise signal generator

YU Heng-wei^{1,2}, SUN Xiao-juan^{2,3}, WANG Xing-chen^{1,2}, JIANG Ke^{2,3}, WU-You^{2,3}, CHENG Dong-bi^{1,2}, SHI Zhi-ming^{2,3}, JIA Yu-ping^{2,3}, LI Da-bing^{2,3}*

(1. University of Science and Technology of China, Microelectronics Institute, Hefei 230026, China;
2. Center of Materials Science and Optoelectronics Engineering, University of Chinese Academy of Sciences, Changchun 130033, China;
3. State Key Laboratory of Optics and Applications, Changchun Institute of Optics, Fine Mechanics and Physics, Chinese Academy of Sciences, Changchun 130033, China) * Corresponding author, E-mail: lidb@ciomp.ac.cn

Abstract: The existing method used to generate Gaussian noise signals is to generate random numbers through mathematical calculation. However, this method cannot achieve a true random signal nor can it match the actual noise signal. In this study, a Gaussian noise signal generator based on a quantum random number is proposed. A single-photon detector detects the photon signal of the selected path as the source of the random number and realizes the Gaussian noise signal generator based on a true ran-

收稿日期:2018-12-11;修订日期:2019-01-29.

基金项目:国家重点研发计划资助项目(No. 2016YFB0400900);政府间国际合作创新项目(No. 2016YFE0118400); 吉林省重点研发资助计划(No. 20180201026GX);中科院青促会资助项目(No. 2015171)

dom number. The random number is processed by a weighted Girvan-Newman Gaussian algorithm to obtain the Gaussian noise signal, which is implemented using the Verilog language in a field programmable gate array. The results show that the amplitude of the generated noise signal varies from 0 to 255. A statistical analysis of the amplitude spectrum obeys the Gaussian distribution. The power spectrum of the noise signal fluctuates uniformly at approximately 20 dB and follows a uniform distribution, thus satisfying the characteristics of the Gaussian white noise. Compared with existing methods based on quantum random numbers, the source of the random number is distinct in the present case, and the proposed generator can achieve real randomness. A simple scheme for realizing a true random number for a Gaussian noise signal generator is therefore presented.

Key words: Gauss noise; single photon; random number source; amplitude spectrum; power spectrum

1 引 言

GaN 基材料是一种直接宽带隙半导体材料, 由于它具有直接宽带隙,原子键强,热导率、电子 饱和漂移速度、击穿电压高、耐高温、发光效率高 等优点,被认为是研制光电子器件的理想半导体 材料,被广泛地应用于光电子领域^[1]。目前,基于 GaN 材料的光电探测器在火焰检测、导弹告警、 电弧检测等领域具有重要的应用价值。在 GaN 基探测器光电信号检测中噪声一直是最为重要的 影响因素,设计一套合适的系统来模拟噪声对信 号的影响具有重要的意义^[2-4]。

目前,大多数噪声信号都是建立在高斯噪声 基础之上,通过高斯噪声信号发生器对通信系统 中的噪声信道进行模拟,容易掌握通信系统中的 噪声规律,对提高信噪比具有重大意义。市场上 的高斯噪声信号发生器都是采用数学计算的方式 生成随机数来产生高斯噪声信号。北京航空航天 大学通过 M 序列产生伪随机数的方法实现高斯 噪声信号;南京大学通过 wallace 算法的方式生 成伪随机数实现高斯噪声;北京科奇公司通过 DDS 直接频率合成的方法生成高斯噪声信号,其 信号发生器的频率为 8~50 kHz,噪声发生器的 频率较低。国际上也对高斯噪声信号发生器展开 了深入的研究,日内瓦大学通过 BOX-MULLER 算法产生高斯噪声信号, Agilent 公司和 Tektronix 公司研制的高斯噪声信号发生器得到了广泛 的应用[5-6],该发生器是通过伪随机数的方式来生 成高斯噪声信号的。这种伪随机数的方式是通过 数学计算生成随机数,信号来源简单,不能真正地

做到不可预测性,难以满足探测器实际应用过程 中噪声随机的特性。因此需要研究一种新的噪声 信号生成方式,以实现与现实噪声吻合度高的随 机噪声信号。

本文在结合前人研究的基础上提出一种新的 高斯噪声生成方法,即基于量子随机数的高斯噪 声信号发生器。本方法是一种基于真随机数生成 高斯噪声信号的方式。相比于原始的伪随机方 式,能够实现真正的随机性。量子随机数高斯噪 声发生器是基于 GaN 雪崩探测器探测光子信号 对路径随机选择形成随机数码流,生成高斯噪声 的一种方案^[7],更符合噪声系统的要求,能够更有 效地模拟通信系统中信道噪声的情况,为提高信 噪比提供了一种可靠的方案。

2 基于量子随机数高斯噪声信号发 生器的设计

2.1 结构设计

图 1 为基于量子随机数高斯噪声信号发生器 的结构框图。它主要由紫外 LED 光源(UV-LED)、衰减器、分束器、单光子探测器、甄别器、单 稳态触发器以及 FPGA 处理模块构成^[8]。紫外 LED 光源由 UVLED 光源和恒流源驱动电路两 部分组成,UVLED 采用 280 nm 的紫外 LED。 衰减器由减光片和光功率计组成。分束器采用的 是 50:50 的光纤分束器,把一路光信号分成两 路。探测器由 GaN 雪崩二极管构成,甄别器由滞 回比较器构成,单稳部分采用的是 D 触发器,可 编程逻辑门阵列(Field Programmable Gate Array, FPGA)处理部分将随机数码流生成高斯噪声。

图 1 高斯噪声信号发生器的结构框图 Fig. 1 Block diagram of Gaussian noise signal generator

2.2 工作原理

基于量子随机数高斯噪声信号发生器的工作 原理是将真随机数码流转换为高斯噪声。首先, 将 UVLED 产生的紫外光信号经过衰减器衰减 后得到单光子信号,UVLED 输出的光功率用功 率计检测记为 P_1 ,单光子的光能量为 hv,记为 P_2 。其中,h 为普朗克常数,v 为对应波长的光频 率。调节衰减器的衰减值得到单光子信号,衰减 值 ATT 为:

$$ATT = 10 \log(P_2/P_1).$$
 (1)

单光子信号通过 5050 分束器输出,在其中一 个输出端放置单光子探测器。当光子经过分束器 时,选择每条路径的概率是 1/2,其中一端的探测 器可以探测到光子信号,产生随机数^[9-10],这种随 机数源的随机性强并且来源清晰。

探测器探测到光子信号后会产生雪崩电流经 过甄别器进行甄别,单稳后输出高电平信号,没有 光子信号的时候产生低电平信号,这样会产生原 始的随机数码流。每 8 bit 的随机数码流作为随 机数信号输出,要产生一个服从某种分布的随机 数,可以先求出其分布函数的反函数解析式,再将 一个在[0,1]区间内均匀分布的随机数值代入其 中,就可以计算出服从某种分布随机数。高斯分 布密度函数为:

$$f(x) = \frac{1}{\sqrt{2\pi}} \exp\left(-\frac{x^2}{2}\right). \tag{2}$$

采用 Box-Muller 变换法产生高斯分布随机数,若 R_1 , R_2 表示[0,1]均匀分布随机数,将 R_1 , R_2 代入高斯密度分布公式(2)的因变量中,再取 其反函数即可得到高斯分布随机数如下:

$$\xi = \sqrt{-2\ln R_1 \cos 2\pi R_2},$$

$$\eta = \sqrt{-2\ln R_1 \sin 2\pi R_2}.$$
(3)

把得到的随机信号进行 WGN 算法处理后, 送入到 FPGA 中进行处理,生成噪声信号,对得 到的噪声信号进行验证,是否满足高斯噪声信号 的特征。所谓高斯噪声是指它的概率统计特性服 从高斯分布而它的功率谱密度又是均匀的。确切 的说,只要噪声的功率谱密度的宽度远大于它所 作用的系统的带宽,并且在系统带宽内,它的功率 谱密度基本上是常数,就可以作为白噪声进行处 理。白噪声的功率谱密度为:

$$S_n(f) = \frac{N_0}{2},\tag{4}$$

其中 N₀ 为单边功率谱密度,满足均匀分布。

3 实验结果与讨论

图 2 为基于量子随机数高斯噪声方案中 UVLED 的驱动方案原理图,其中 UVLED 的驱 动方案采用数控恒流源驱动模式。由于 LED 的 电流随电压的波动较大,LED 两端电压微小的变 化会使得其两端电流指数倍增长,采用恒流驱动 模式能够防止电压的波动损坏 LED 芯片^[11]。本 实验中 UVLED 驱动模块采用 LF353 运放芯片, 通过模数转换器 TLC5615 控制运放的输入端电 压。该数模转换器采用 SPI 通信协议,通过 3 根 串行总线控制运放芯片输入端的电压;通过改变 输入端的电压调节 UVLED 两端的电流,调整 UVLED 的发光功率。



图 2 UVLED 驱动电路 Fig. 2 Driver circuit of UVLED

利用光谱响应测试系统获得 UVLED 的 EL 光谱曲线,如图 3 所示。用于制备 UVLED 的 AlGaN 材料通过金属有机物化学气相沉积法在 蓝宝石衬底上获得,其发光波长为 280 nm。本研 究把 UVLED 产生的光信号经过衰减后通过分 束器输出,被输出端的探测器探测到,产生原始的 随机数码流。

图 4 为量子随机数产生的方案,通过探测器 对光子信号的探测来产生随机码流,光子信号经

第 27 卷





过路径选择后被探测器探测到,探测器 1 探测到 的光子信号的概率 P=1/2,产生雪崩电流。然后 把雪崩电流经过放大器放大,通过甄别、单稳输出 得到稳定的 LVTTL 电平信号,设置甄别器两端 的甄别电平,测试时调节滑动变阻器 Rt1 的阻值 设置甄别电平为 50 mV^[12-13],能够有效地提取出 雪崩信号,甄别输出后的信号送入 D 触发器中进 行单稳。最后输出稳定的 LVTTL 电平信号,记 为原始的随机数信号,存入到寄存器 Reg 中。每 8 bit 的原始随机数作为随机数信号输出,假设输 出的随机数信号为:

 $Reg[7:0] = \{0,1,1,0,0,0,1,0\}.$ (5)

把输出的随机数信号进行函数变换,得到高 斯分布的随机数,使用 WGN 函数随机抽取 Reg [7:0],记为 *u*,得到的高斯随机数为:

$$WGN = WGN(u).$$

将高斯随机数送入 FPGA 中进行后处理得 到高斯噪声信号。





Fig. 4 Random number generation circuit

高斯噪声的产生方法采用 DDS 直接频率合成的方式,DDS 直接频率合成能产生连续相位信号的转换时间短、成本低,在频率不是特别高的场合比较适用。由于随机信号来源于探测器对光子信号的计数,受限于探测器的响应时间,选择DDS 直接频率合成的方式比较合适。把得到的高斯随机数送入到 FPGA 中进行后处理,每次读

取 8 bit 的随机数^[14-15]。本文中 FPGA 芯片采用 ALTER 公司的 Cyclone IV FPGA 芯片, FPGA 的最小系统电路如图 5 所示。通过 FPGA 内部 的 ROM IP 核,载入高斯随机数查找表文件就可 以产生对应的噪声信号。

把原始随机数据通过 MATLAB 进行高斯算法(WGN)处理得高斯噪声数据存入到查找表文

(6)

件中,在 FPGA 中载入查找表到 ROM IP 核中, 对 ROM IP 核进行寻址得到高斯噪声。这里运 用 MATLAB 进行算法处理可以避免 FPGA 进 行复杂的数据运算,提高 FPGA 的处理速度,易 于实现。DDS 直接频率合成的方式是当每一个 CLK 时钟上升沿到达时,由 FPGA 输出一个随机 地址作为 ROM 查找表的地址,ROM 查找表通过 地址查询到每个地址对应的内存中存有的高斯噪 声信号^[16],查找表文件如表 1 所示。这种方法实 现简单,具有高分辨率和快速转换时间等优点。

11	间到味户旦认识出来
Tab. 1	Result of Gauss signal
CLK 地址	高斯噪声
0	152
1	255
2	0
3	2
4	153

古斯哈吉木比主姓田



图 5 FPGA 最小系统 Fig. 5 Minimum system of FPGA

把经过 FPGA 处理后得到的噪声信号通过 Modelsim 进行仿真验证,对生成的噪声信号进行 1 min 的采样,由图 6 可以清楚地看到噪声信号 的幅度信息,文章采用的是每 8 bit 的随机数码流 做为随机数信号,每 8 bit 的随机数生成噪声信 号,噪声信号的幅度在 $0\sim255$ 之间随机变化。在 图 6 中,可以看到噪声信号的幅度信息在随机变 化。为了进一步验证产生的噪声信号是否满足高 斯噪声信号的要求,是否在幅度上服从高斯分布, 在频率上服从均匀分布^[17],这里给出了进一步的 验证,读取 1 min 和 10 min 的噪声信号,计算出 它的幅度曲线和功率谱曲线,测试它的幅度谱是 否满足高斯分布,功率谱是否满足均匀分布。测 试结果如图 7 和图 8 所示。

图 7 为所测噪声信号的幅度谱。由图 7 可 知,噪声信号幅度在 0~255 之间变化,符合由 8 bit 的随机数产生噪声信号的实现原理,纵坐标表 示采样的 1 min 内出现噪声信号的次数。由图 7 (a)可知,在 1 min 的采样时间内,噪声信号的幅 度分布满足高斯曲线分布的趋势。为了进一步验 证生成噪声信号的可靠性,本文增加了采样时间, 把采样时间增加到 10 min,图 7(b)为 10 min











Fig. 7 Amplitude spectra of Gauss noise

图 6 高斯噪声信号 Fig. 6 Noise of Gauss signal

采样的噪声信号幅度谱分布曲线,由图可知,增加 采样时间噪声信号幅度谱分布和高斯分布越来越 接近,因此本次生成的噪声信号在幅度上满足高 斯分布的要求。

功率谱是验证噪声是否满足高斯分布的另一 有效手段^[18-20],因此对它进行了测试与分析。图 8为所测信号的功率谱,由图可知,功率谱振幅分 布平坦,在 20 dB上下均匀波动,满足高斯噪声信 号功率谱分布的要求。由此再次证明,本文提出 的基于量子随机数噪声发生器满足高斯噪声要 求。因此,本文提出的基于量子随机数的方法是 产生噪声的有效手段,为研究探测器的行为提供 了有效的噪声来源。



4 结 论

本文针对探测器应用过程中传统噪声信号 的产生方式是基于伪随机数序列生成的,产生 的随机数不能做到真正随机的问题,提出一种 基于量子随机数高斯噪声信号发生器的方法。 该方法采取光子对路径的选择生成真随机数, 进而通过 FPGA 处理的方式生成高斯噪声信

参考文献:

- [1] GROWDEN T A, ZHANG W D, BROWN E R, et al.. Near-UV electroluminescence in unipolar-doped, bipolar-tunneling GaN/AlN heterostructures
 [J]. Light: Science & Applications, 2018, 7(2): 17150.
- BIANCO V, MEMMOLO P, LEO M, et al..
 Strategies for reducing speckle noise in digital holography [J]. Light: Science & Applications, 2018, 7: 48.
- [3] YUAN G H, VEZZOLI S, ALTUZARRA C, et al.. Quantum super-oscillation of a single photon
 [J]. Light: Science & Applications, 2016, 5(8): e16127.
- [4] CASPANI L, XIONG C L, EGGLETON B J, et al.. Integrated sources of photon quantum states based on nonlinear optics [J]. Light: Science & Applications, 2017, 6(11): e17100.
- [5] 聂友奇. 量子随机数实验研究[D]. 合肥: 中国科 学技术大学, 2017.
 NIE Y Q. Experimental Study of Quantum Random Number Generation [D]. Hefei: University of Science and Technology of China, 2017. (in Chinese)
- [6] 秦雪陈. 混合同余法产生随机噪声的 FPGA 实现
 [J]. 电子设计工程, 2015, 23(9): 123-126.
 QIN X CH. Mixed congruential method to generate random noise on FPGA[J]. *Electronic Design Engineering*, 2015, 23(9): 123-126. (in Chinese)
- [7] 申艳,王新民,陈后金. 基于 FPGA 的高斯白噪声 发生器设计[J].现代电子技术,2009,32(23): 197-200.
 SHEN Y, WANG X M, CHEN H J. Design of white Gaussian noise generator based on FPGA[J]. *Modern Electronics Technique*, 2009, 32(23): 197-200. (in Chinese)

号,最后利用 Matlab 进行复杂的运算,减小对 FPGA 资源的占用。结果表明,噪声信号在 0~255随机分布,功率谱在 20 dB 上下均匀波 动。随着采样时间从 1 min 增加到 10 min,幅度 谱和功率谱均满足高斯噪声的要求。这种基于 光子对路径随机选择能够做到真正的随机,不 具有固定的规律性,能够广泛地应用到通信系 统和遥测系统里,有效地提高通信系统的抗干 扰能力。

- [8] 王鹏宇,翟丽丽,石巨峰. 基于 FPGA 的参数可调 高斯白噪声发生器的设计[J]. 舰船电子对抗, 2013,36(4):113-115,120.
 WANG P Y, ZHAI L L, SHI J F. Design of Gaussian white noise generator with adjustable parameters based on FPGA[J]. Shipboard Electronic Countermeasure, 2013,36(4):113-115,120. (in Chinese)
- [9] 骆乐,吴长强,林杰,等. 基于光子计数激光雷达的时域去嗓[J]. 光学 精密工程, 2018, 26(5): 1175-1180.
 LUO L, WU CH Q, LIN J, et al.. Time-domain denoising based on photon-counting LiDAR[J]. Opt. Precision Eng., 2018, 26(5): 1175-1180. (in Chinese)
- [10] 刘启能, 刘沁. 大型 LED 矩形阵列光斑照度的均 匀性研究[J]. 发光学报, 2018, 39(5): 699-705.
 LIU Q N, LIU Q. Illumination uniformity of large LED rectangular array[J]. Chinese Journal of Luminescence, 2018, 39(5): 699-705. (in Chinese)
- [11] 刘明哲,李鹏翀,邓高强,等. 6H-SiC 衬底上 Al-GaN 基垂直结构紫外 LED 的制备[J]. 发光学报, 2017, 38(6): 753-759.
 LIU M ZH, LI P CH, DENG G Q, et al.. Fabrication of vertical structure ultraviolet LED on 6H-SiC substrate[J]. Chinese Journal of Luminescence, 2017, 38(6): 753-759. (in Chinese)
- [12] 包兴臻,梁静秋,梁中翥,等.像素分割对 LED 电流密度及光照度分布的影响[J].发光学报, 2016,37(11):1399-1407.
 BAO X ZH, LIANG J Q, LIANG ZH ZH, et al.. Current density and irradiance distribution of lightemitting-diode-array device with divided pixels[J]. Chinese Journal of Luminescence, 2016,37(11): 1399-1407. (in Chinese)
- [13] 符佳佳,曹海城,赵丽霞,等.不同封装材料的中 功率 GaN 基 LED 器件老化分析[J].发光学报,

2016, 37(10): 1230-1236.

FU J J, CAO H CH, ZHAO L X, et al.. Degradation analysis of mid-power GaN-based LEDs with different package materials[J]. Chinese Journal of Luminescence, 2016, 37(10): 1230-1236. (in Chinese)

[14] 李臻, 維超, 路腾腾, 等. 并行雪崩光电二极管阵列
 红外单光子探测系统[J]. 光学 精密工程, 2016, 24(10S):6-11.
 LI ZH, YAN CH, LU T T, *et al.*. Infrared sin-

gle photon detection system for parallel avalanche photodiode array[J]. *Opt. Precision Eng.*, 2016, 24(10S):6-11. (in Chinese)

- [15] 何妙妙,朱磊. 一种基于 FPGA 的高斯白噪声信号 发生器[J]. 信息通信, 2016(10):41-42.
 HE M M, ZHU L. A Gaussian white noise signal generator based on FPGA [J]. Information & Communications, 2016(10):41-42. (in Chinese)
- [16] 李飙,任艺,常本康.梯度掺杂结构 GaN 光电阴极的稳定性[J].中国光学,2018,11(4):677-683.
 LI B, REN Y, CHANG B K. Stability of gradi-

ent-doping GaN photocathode[J]. Chinese Optics, 2018, 11(4): 677-683. (in Chinese)

[17] 张博,张玉静.加性高斯白噪声信道中典型信号 的信噪比估计[J]. 滨州学院学报,2015,31(2): 69-72. ZHANG B, ZHANG Y J. Signal-noise ratio (SNR) estimation of typical signals over AWGN channel [J]. *Journal of Binzhou University*, 2015, 31(2): 69-72. (in Chinese)

- [18] 朱枫,张葆,李贤涛,等. 跟踪微分器在陀螺信号 去噪方面的应用[J]. Information & Communications, 2017, 10(3): 355-362.
 ZHU F, ZHANG B, LI X T, et al.. Application of tracking differentiator to gyro signal denoising [J]. Chinese Optics, 2017, 10(3): 355-362. (in Chinese)
- [19] 季志博,王辉,王磊,等. 一种大功率低噪声的智能可调 LED 驱动设计方法[J]. 液晶与显示, 2018,33(9):778-786.
 JI ZH B, WANG H, WANG L, *et al.*. Design

method for high power and low noise intelligent adjustable constant current source [J]. *Chinese Journal of Liquid Crystals and Displays*, 2018, 33(9): 778-786. (in Chinese)

[20] 夏润秋,刘洋. 基于 FPGA 的 PCI 总线红外图像 采集系统设计[J]. 液晶与显示,2018,33(9): 772-777.

> XIA R Q, LIU Y. Design and implementation of PCI bus infrared image acquisition system based on FPGA[J]. *Chinese Journal of Liquid Crystals and Displays*, 2018, 33(9): 772-777. (in Chinese)

通讯作者:



黎大兵(1975一),男,湖北通城人,研究 员,博士生导师,1998 年、2001 年于吉 林大学分别获得学士、硕士学位,2004 年于中国科学院半导体所获得博士学 位,主要从事 AlGaN 基宽禁带半导体 光电材料与器件的研究。E-mail: lidb @ciomp.ac.cn

(本栏目编辑:曹 金)

作者简介:



余恒炜(1992一),男,安徽池州人,硕士 研究生,主要从事光电探测器及其读出 电路方面的研究。E-mail: yhw520@ mail.ustc.edu.cn