文章编号:1008-0570(2007)12-1-0127-02

基于γ能谱测量的真随机数发生器设计

The Design Of The True Random Number Generator Based On The γ Spectrometry Measuring

(厦门大学)周毅鸿 黄文达
ZHOU YIHONG HUANG WENDA

摘要:本文介绍了一种基于γ能谱测量的真随机数发生器的设计,详细阐述了设计思路。以核脉冲信号作为真随机源,引进伪随机序列进行优化并对结果进行了检测分析。

关键词:γ能谱,真随机数发生器,labview软件,HM-407示波器,伪随机序列
中图分类号:TP393.08 **文献标识码:**A

Abstract: This paper introduces a design of true random number generator based on the γ spectrometry measuring, particularly describe the design methods.The acquisition of the true random number is based on the nuclear signal pulse.We introduces the pseudo random number sequence to raise the quality of the random numbers and give the analysis of the result.
Key word: γ spectrometry, True random number generator, Labview software, HM-407 oscillograph, Pseudo random number sequence.

技术创新

1 引言

随着计算机技术的发展和普及,数据安全越来越受到人们的重视,几乎所有的密码系统都需要不可预测的密钥进行加密,因此,如何快速得到真正的随机数成为当前人们迫切解决的问题。

衡量随机数好坏主要有两个标准,即要求它们是分布均匀,彼此独立的.当前,人们得到的随机数可分为两大类:伪随机数和真随机数.它们各有优缺点.伪随机数是由一个初始状态(或称为"种子")开始,通过一个确定的算法得到的,一旦给定算法和种子值暴露,序列输出便可预知,安全性不高.真随机数来源于不可预测的物理现象,比如,原子核衰变、大气噪声、电阻、二极管热噪声,等等.为了得到分布均匀,彼此独立的真随机数,我们对单一的随机数发生器模式进行改进,把软硬两种方式结合起来,让源于真实物理现象的真随机序列和基于算法而得到的伪随机序列进行异或操作,最终得到我们需要的真随机序列.

2 基于γ能谱测量的真随机数发生器的实现方法

2.1 基本原理

γ射线与物质的相互作用

放射性核素放射出来的带电粒子(α、β粒子以及内转换电子)与物质相互作用主要为电离、散射和吸收三个方面。γ射线是不带电的电磁辐射,它与物质的相互作用主要有光电效应,康普顿效应和电子对效应三个过程。

2.1.1 光电效应

入射的γ光子把能量全部转移给原子中的束缚电子,使之发射出来,而光子本身消失,这种过程称为光电效应。

2.1.2 康普顿效应

入射的γ光子与物质原子的核外电子发生非弹性碰撞,一部分能量转移给电子,使它脱离原子成为反冲电子,而散射光子的能量和运动方向发生变化,这一过程称为康普顿效应。

2.1.3 电子对效应

当γ光子从原子核旁边经过时,在原子核的库仑场作用下,γ光子转化为一个正电子和一个负电子,这种过程称为电子对效应。

2.2 核脉冲信号的获取及其随机性讨论

当γ射线入射至闪烁体时,产生的次级电子使闪烁体分子电离和激发,退激时发出大量光子。闪烁体发出的光子被闪烁体外的光反射层反射,会聚到光电倍增管的光阴极上。由于光电效应,光子在光阴极上打出光电子。光阴极上打出的光电子在光电倍增管中倍增,电子数目增加几个数量级,最后被阳极接收形成电压脉冲,此电压脉冲的幅度与γ射线在闪烁体内消耗的能量及产生的光强成正比。

在任一时刻,γ射线在闪烁体发生的光电效应,康普顿效应和电子对效应是随机的,因此产生的电压脉冲信号也是随机的。这三种效应产生的电子在闪烁晶体中产生闪烁发光。由于单能γ射线所产生的这三种电子能量各不相同,甚至对康普顿效应是连续的,因此相应一种单能γ射线,闪烁探头输出的脉冲幅度值是满足一定分布的真随机序列,由于前后两个脉冲来自于不同原子核的衰变,因此可以满足独立性的要求,由该真随机序列可以进一步构造出满足各种分布要求的真随机序列。

2.3 真随机数发生器系统设计

真随机数发生器系统如图1所示,当放射源发出的γ射线进入闪烁体时,γ光子即与闪烁体中的原子、分子及晶体系统发生相互作用(如光电效应,康普顿散射和电子对效应等)。相互作用的结果产生次级电子,γ光子的能量转化为次级电子的动能。探头的闪烁体是荧光物质,它被次级电子激发而发出荧光,这些

周毅鸿:硕士研究生

光子射向光电倍增管的光阴极。由于光电效应,在光阴极上打出光电子,每个光电子在光电倍增管中的打拿极(倍增极)上打出多个电子,这些电子又在其他级的打拿级上,打出更多的电子,经过多次倍增,最后有大量电子射向管子的阳极,转变成电信号输出。通常,光电倍增管输出的脉冲幅度较小,所以必须经过线性脉冲放大器放大后,再输入到电脑中进行幅度分析。因闪烁探头输出的脉冲幅度值是满足一定分布的真随机序列,并不是我们希望得到的分布均匀的序列,于是,我们再进行数据处理加工,最后得到分布均匀的真随机序列。

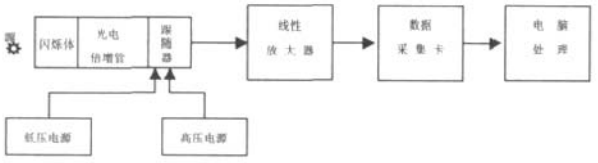

图1　真随机数发生器系统

2.3.1 数据采集以及 Labview驱程设计

采用 HAMEG 公司生产的 HM-407 示波器进行数据采集,该采集卡拥有 100MS/s 的采样率,这足以满足我们的要求.

由于 HM-407 只有 VB 的驱程,不能用于 Labview软件中,为此我们特别编写了 Labview的驱程,具体如图 2 所示,该示波器采用串口与电脑通信,首先初始化串口函数,波特率为 9600Baud,数据长度 8 位,奇偶校验位无,停止位 2 位。接着,向串口写入十六进制命令,最后读回 8192 字节的数据,至此,我们初步实现了电脑与示波器 HM-407 的数据通信。

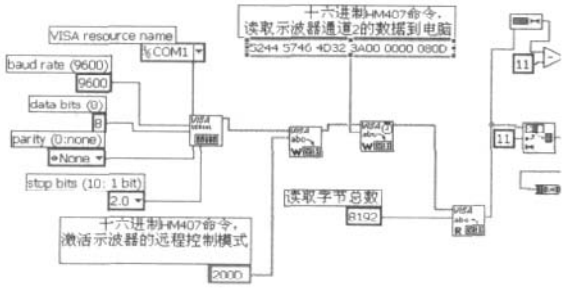

图 2　HM-407 示波器 Labview 驱程

2.3.2 数据处理和加工

由于采集到的真随机序列不是均匀分布的,于是我们用如下方法改进,对所生成的伪随机序列和采集到的真随机序列(转换成二进制序列)进行异或操作,如图 3 所示。

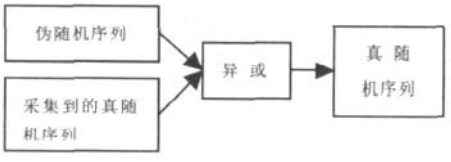

图 3　数据处理

在采集到的信号中,设产生 1 的概率为 a,那么,产生 0 的概率为 1-a。一般来说,a 不等于 1-a(也就是它不能很好的满足均匀性要求)。在所得到的伪随机数中,设产生 1 的概率为 b,产生 0 的概率为 1-b。由于该序列严格满足均匀性和独立性的要求,所以 b 和 1-b 都趋于 1/2。异或后,产生 1 的概率 P(1)=a*(1-b)+(1-a)*b,产生 0 的概率为 P(0)=a*b+(1-a)*(1-b)。由于 b 和 1-b 都趋于 1/2,P(1) 和 P(0) 都趋于 1/2*[a+(1-a)]=1/2(即满足均匀性要求)。

3 结果检验

高质量的随机数序列必须通过一系列的统计检验来检测随机序列的分布均匀性、相关性等。我们选用的检验方法如下:

1.比特分布检测。这是随机数发生器最基本的检测标准,用以判断随机序列是否满足分布的均匀性。主要测试长为 n 比特的序列中 0 和 1 的个数,理想情况 0 和 1 等概率分布。

2.频度检测。利用假设检验检测序列独立性的一种方法。

3.跟随特性检测(又称转移检测)。序列的跟随特性指序列中相邻元素的出现情况。主要用来测试长为 n 比特的序列中 00,01,10,11 的概率是否相等。采样低频采样的措施有利于保证输出数的跟随特性。

4.游程检测。游程是由连续 0 或者 1 组成的序列,并且其前后元素与游程的元素不同。游程数目为序列长度的一半时,产生的随机序列较好。设 Jc 为输出序列中相邻两位取不同值的次数,C_k 为连续 k 个值相同的次数,他们的期望值满足公式:$E(Jc)=(n+1)/2$ $E(c_k)=2^{-(k+1)}(n-k+3)$。

在本设计所生成的随机数中选取连续的 255 个数,转化为二进制序列进行检验。

结果见下表:

表 1 独立性和均匀性检验

项目	比特分布	频度检测	跟随特性检测	游程检测
理论值	$n_0=n_1$	$X\alpha^2=(n_0-n_1)^2/n$	序列 00,01,10,11 出现的概率相等	$E(Jc)=(n+1)/2=128$; $C_1=64.25, C_2=32.13, C_3=16.07, C_4=8.04, C_5=4.02, C_6=2.01, C_7=1$
实际值	$n_0=127, n_1=128$ $n_0^2+n_1^2$	$X\alpha^2=1^2/255<3.841$	00:61 次;01:65 次;10:65 次;11:63 次;	$E(Jc)=124$; $C_1=67, C_2=28, C_3=16, C_4=7, C_5=3, C_6=2, C_7=1$
意义	均匀分布	符合独立性	符合独立性	符合独立性

4 结论

经验证,由本设计所产生的真随机序列通过了四项随机性测试。证明了我们所生成的真随机序列是能够很好的满足均匀性和独立性要求的,且它是源于不可预测的物理现象,所以我们最终得到的序列是真正不可预测的、独立的和均匀的随机序列。

本文作者创新点:

以 γ能谱测量数据作为真随机源,彻底解决随机数易被破解问题。巧妙利用简单的异或操作解决真随机源的分布不均问题。编写示波器 HM407 的 LABVIEW 驱动程序,使其高性能的数据采集功能得到充分应用。

参考文献:

[1] 戴道宣,戴乐山.近代物理实验[M]. 北京:高等教育出版社 2006

[2] 北京第三研究所. 野外 γ能谱测量[M]. 北京:原子能出版社 1977

[3] 万艳,林晓伟,李炜,郑学仁,冯禀刚,真随机数发生器芯片的设计[A].大众科技,2006(2)

[4] 伍华健.公开密钥密码体系在网络安全中的应用研究[J].微计算机信息.2006,12-1:14-16.

作者简介:周毅鸿(1981-),福建龙海人,男,汉族,硕士研究生,研究方向:虚拟仪器,计算机网络方面;通讯作者:黄文达(1964-),福建闽清人,男,汉族,教授,从事虚拟仪器和基于网络的自动化测量与控制研究。(下转第 154 页)

技术创新

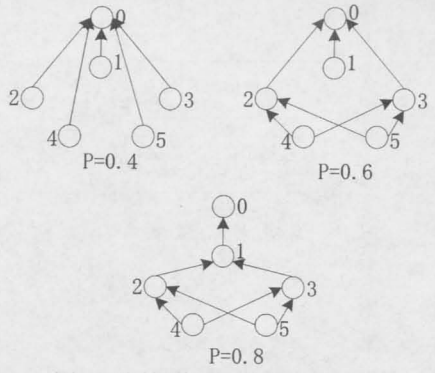

图 2 不同阀值下网络拓扑变化图

图 3 时延与跳数的关系图

通过实验，我们得出如图 3 所示的一个关系图。在 Twait2 不变的情况下，时延与 Twait1 的关系，当 Twait1 减小时，网络的时延可以明显减少。但是通过实验得知，在 Twait1 很小的情况下，节点可能没有收到具有最小跳节点发出的建立可靠最小跳数场的消息，因而网络内拓扑变化很大，而当 Twait1 增大到一个定值后，网络的拓扑变化将非常小。

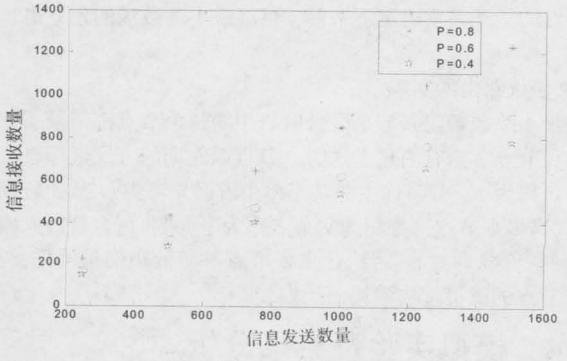

图 4 不同阀值下汇聚节点收包情况

图 4 说明的是在不同的阀值 P 的情况下，汇聚节点收到的数据包情况。网络中的节点向汇聚节点发送一定数量的数据包。在阀值 P 增大的情况下，汇聚节点收到了更多的数据包，这也说明了在阀值 P 增大的情况下，数据包的丢失越少，从而也验证了本算法的正确性。

5　结论

人们已经在无线传感器网络路由协议方面做了很多卓有成效的工作，并已有许多切实可行的成果。本文在最小跳路由协议的基础上，提出了一种基于可靠最小跳数场的路由协议，着重介绍了可靠最小跳场的建立过程，并对该过程中临时父子关系的确立以及链路评估方法进行详细的叙述。TinyOS 操作系统下的实验表明，基于可靠最小跳数场的路由协议在提高数据发送成功率上效果明显。

论文创新点:1. 提出了可靠最小跳数场的概念并对可靠最小跳数场的建立进行了研究。

参考文献

[1]李建中,李金飞,石胜飞.传感器网络及其数据管理的概念、问题与进展[J].软件学报，2003,14(10):1717~1727.
[2]刘昌鑫,夏春和.无线传感器网络路由协议比较研究[J].微计算机信息,2006,9-1:02-05.
[3]刘云璐,柴乔林,赵晋.无线传感器网络方向性分区路由算法[J].2006;1:26.
[4]孙利民,李建中,陈渝,朱红松.无线传感器网络[M].清华大学出版社,2005.

作者简介:李梁(1983-),男(汉族),江西吉安人,硕士研究生,主要从事无线传感器网络的研究;舒坚(1964-),男(汉族),江西南昌人,硕士生导师,教授,主要从事计算机网络和无线传感器网络的研究

Biography:Li Liang (1983-), Male (Han nationality), Jiangxi Province, Master, Major engaged in research of wireless sensor network.

(330063 江西 南昌 南昌航空工业学院计算机学院)李梁 刘琳岚 舒坚 陈英

(Nanchang Institute of Aeronautical Technology, School of Computer Science and Technology)LI Liang LIU Lin-Lan SHU Jian CHEN Ying

通讯地址:(330063 江西省南昌市丰和南大道 696 号南昌航空工业学院研究生处 93 信箱)李梁

(收稿日期:2007.9.03)(修稿日期:2007.11.05)

(上接第 128 页)

Biography:Zhou Yi-hong, borned in 1981,Longhai Fujian,Hang, male,master of college,Direction of research:visual instrument and internet. Email: carefree668@126.com;Huang Wen-da, borned in 1964, male,Minqing Fujian,Hang,professor of college,Direction of research:virtual instrument and automatic measurement and research of control based on internet. Email: wdhuang@xmu.edu.cn.

(361005 厦门 厦门大学 物理系)周毅鸿 黄文达

(Dept. of Physics, Xiamen Univ., Xiamen 361005, China) Zhou Yi-hong Huang Wen-da Sun Zhen-ning Xia Feng

通讯地址:(363100 福建省龙海市石码镇红树林小区景新阁 2 号楼 602)周毅鸿

(收稿日期:2007.9.03)(修稿日期:2007.11.05)