学校编码：10384　　分类号_____密级_____

学号：20051301685　　UDC_____

厦门大学

硕 士 学 位 论 文

基于核衰变的真随机数发生器设计

The design of the true random number generator based on the nuclear decay

周毅鸿

指导老师姓名：黄文达 教授

申请学位级别：硕 士

专 业 名 称 ：微电子学与固体电子学

论文提交日期：2008 年 5 月

论文答辩日期：2008 年 6 月

学位授予单位：厦 门 大 学

学位授予日期：2008 年 月

答辩委员会主席：_____

评　　阅　　人：_____

2008 年 6 月

厦门大学学位论文原创性声明

兹呈交的学位论文，是本人在导师指导下独立完成的研究成果。本人在论文写作中参考的其他个人或集体的研究成果，均在文中以明确方式标明。本人依法享有和承担由此论文而产生的权利和责任。

声明人（签名）：

年 月 日

厦门大学学位论文著作权使用声明

本人完全了解厦门大学有关保留、使用学位论文的规定。厦门大学有权保留并向国家主管部门或其指定机构送交论文的纸质版和电子版，有权将学位论文用于非赢利目的的少量复制并允许论文进入学校图书馆被查阅，有权将学位论文的内容编入有关数据库进行检索，有权将学位论文的标题和摘要汇编出版。保密的学位论文在解密后适用本规定。

本学位论文属于

1.保密（），在　　年解密后适用本授权书。

2.不保密（　）

（请在以上相应括号内打“√”）

作者签名：　　日期：　　年　　月　　日

导师签名：　　日期：　　年　　月

摘 要

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。

核衰变信号是自然界的真随机源，由核衰变得到的序列虽然是真随机序列但却不能满足均匀性和独立性要求。因此必须利用软件的方式加以优化。本文采用与伪随机序列异或方式对其进行优化。为了最大限度利用所得真随机数，笔者用VB开发了远程访问真随机源且能嵌入Web使用的控件。

本设计的关键技术在于核衰变信号的引入和获取及对输出的随机序列进行均匀性和独立性的处理,以及可以远程访问真随机源且能嵌入Web使用的控件设计。本文解决该课题主要做以下几个方面介绍：

第一章：介绍了利用LabVIEW 软件开发虚拟仪器的基本方法以及相关开发技术。

第二章:介绍数据采集的相关概念与技术及如何利用LabVIEW软件进行数据采集。

第三章：介绍随机数在信息安全中的应用，重点介绍密码学的相关技术。

第四章：开发两种基于核衰变的真随机数发生器的数据采集系统。详细介绍了系统的工作原理，并对所得结果进行均匀性和独立性的验证。

第五章：利用Datasocket和ActiveX技术，开发基于ActiveX技术的VI网络化验证码生成器。

关键词： 真随机数；LabVIEW；ActiveX

Abstract

With the development of the computer technolegy, data safety is more and more important to us. Almost all code system require unpredictable key to encrypt data ,Therefore how to acquire true random number become a urgent problem to people.

Nuclear disintegration signal is the natural source of the true random number, the true random sequence acquired form nuclear disintegration is the true random sequence, but it can't satisfy the requirement of the equality and independence to the random number. So we need to optimize it by software. The article adopts the method to optimize that let the true random sequence with the pseudo random sequence. In order to use the random number acquired furthest, the author designs a control by the VB software which can access the data in a long-distance situation and can be imbedded in a Web.

The key technology of the design is introduction and acquisition of nuclear disintegration signal, the optimization to the random sequence and the design of the control which can access the data in a long-distance situation and can be imbedded in a Web. It will be discussed in this paper from several sides.

The thesis has four chapters:

Chapter 1 introduces the methods designing virtual instrument by LabVIEW and the technology related to the design.

Chapter 2 introduces the concept and technology related to the data acquisition and how to use the LabVIEW software to acquiring.

Chapter 3 introduces the application of random number in information safety, specially introduces the technology related to the cryptology.

Chapter 4 designs two system of true random number generator based on the nuclear decay, introduces the theory of system and confirm the equality and independence to the random number.

Chapter 5 designs the internet identification code generator using the technology of Datasocket and ActiveX .

Key word: True random number; Labview; ActiveX

目　录

Contents

引 言

随着计算机、Internet 网络技术的飞速发展，人类社会正在由工业化社会向信息化社会迈进。在信息社会里，信息安全越来越受到人们的关注,几乎所有的密码系统都需要不可预测的密钥进行加密,相当多的网站需要有随机的验证码来防御攻击，这些都需要有良好的随机数为它们的安全提供保障[1]。

随机数容易产生,但要在计算机上产生真正的随机数却并不容易。但真正的随机数是不可能通过具体的算法生成的,否则,生成的随机数序列就不是随机的。任何试图以算法生成随机数的人都将处在一种二难的境地。因此,真正的随机数序列应该是从各种物理的随机事件中提炼出来的,而不能通过某个具体的算法计算得到。从上述的论述中可以看出,真正的随机数序列只能来源于随机事件，要产生真随机数，只能借助于自然的力量，本文以核衰变信号做为随机源，是真正可靠的随机源。

在这方面的研究中，有人利用物理噪声源[2]。遗憾的是，真正的物理噪声源难以获得也难以在信息系统中直接使用,经过电路模拟之后的噪声源产生的随机数虽然与自然界的随机数相当接近，却终归不是真随机数。这方面国外还有一些例子：NSA（National Security Agency, 中文简称美国国安局或者国安局）在其硬件电路中使用电子干扰二极管，生成随机数；有些系统在磁盘驱动器中使用空气紊流或者是表面上的、连续网络信息包的随机到达时。在我国，现有的 WNG 系列随机数发生器芯片依照转币模型生成，是做得比较成功的物理噪声源芯片。

在数据采集处理方面，本文采用 NI 公司的 PCI-6014 数据采集卡采集数据，PCI-6014 是 NI 公司推出的一款基于 PCI 接口，功能强大的，即插既用的数据采集卡。以 LabVIEW 软件作为开发平台。LabVIEW 是 NI 推出的虚拟仪器开发平台软件，以其直观简便的编程方式、众多的源码级的设备驱动程序、多种多样的分析和表达功能支持,为用户快捷地构筑自己在实际生产中所需要的仪器系统创造了基础条件。LabVIEW 采用图形化编程语言 G 语言，产生的程序是框图的形式，易学易用，特别适合硬件工程师、实验室技术人员、生产线工艺技术人员的学习和使用，可在很短的时间内掌握并应用到实践中去。特别是对于熟悉仪器结构和硬件电路的硬件工程师、现场工程技术人员及测试技术人员来说，编程就像设计

电路图一样；因此，硬件工程师、现场工程技术人员及测试技术人员们学习LabVIEW 驾轻就熟，在很短的时间内就能够学会并应用 LabVIEW。也不必去记忆那眼花缭乱的文本式程序代码。

在这个网络时代，随机数的应用十分广泛，我们日常的网站都要有随机验证码来防御攻击，然而几乎所有的验证码生成器都是采用数学算法生成伪随机数，经过一定处理而得到验证码。也就是说所得的验证码不是真正的随机数，容易被破解，安全系数不高。为此，本文设计了一种基于真随机源的验证码生成器，其随机数来源于核衰变信号。

验证码生成器必须能够嵌入一般的 Web 网页中使用，而 LabVIEW 软件没办法实现此功能，于是我们考虑引入 ActiveX 技术，因为 ActiveX 的控件在完成虚拟仪器的网络化等方面有巨大的优越性，ActiveX 控件能与 web 浏览器结合在一起，执行速度快，可以用多种语言实现，能复用原有软件的源代码，从而提高了软件开发效率。它能快速开发出高效、简便的代码为 COM 组件的开发提供最大限度的代码自动生成以及可视化支持。

第一章 LabVIEW 开发平台概述

1.1、 基本概念

LabVIEW（Laboratory Virtual Instrument Engineering）是一种图形化的编程语言，它广泛地被工业界、学术界和研究实验室所接受，视为一个标准的数据采集和仪器控制软件[3]。LabVIEW 集成了与满足 GPIB、VXI、RS-232 和 RS-485 协议的硬件及数据采集卡通讯的全部功能。它还内置了便于应用 TCP/IP、ActiveX 等软件标准的库函数。这是一个功能强大且灵活的软件。利用它可以方便地建立自己的虚拟仪器，其图形化的界面使得编程及使用过程都生动有趣。

图形化的程序语言，又称为“G”语言。使用这种语言编程时，基本上不写程序代码，取而代之的是流程图或流程图。它尽可能利用了技术人员、科学家、工程师所熟悉的术语、图标和概念，因此，LabVIEW 是一个面向最终用户的工具。它可以增强你构建自己的科学和工程系统的能力，提供了实现仪器编程和数据采集系统的便捷途径。使用它进行原理研究、设计、测试并实现仪器系统时，可以大大提高工作效率。

所有的 LabVIEW 应用程序，即虚拟仪器（VI），它包括前面板、程序框图以及图标/连结器三部分。

1．前面板

前面板是图形用户界面，也就是 VI 的虚拟仪器面板，这一界面上有用户输入和显示输出两类对象，具体表现有开关、旋钮、图形以及其他控制（control）和显示对象（indicator）。图 1.1 所示是一个随机信号发生和显示的简单 VI 是它的前面板，上面有一个显示对象，以曲线的方式显示了所产生的一系列随机数。还有一个控制对象——开关，可以启动和停止工作。显然，并非简单地画两个控件就可以运行，在前面板后还有一个与之配套的程序框图[4]。

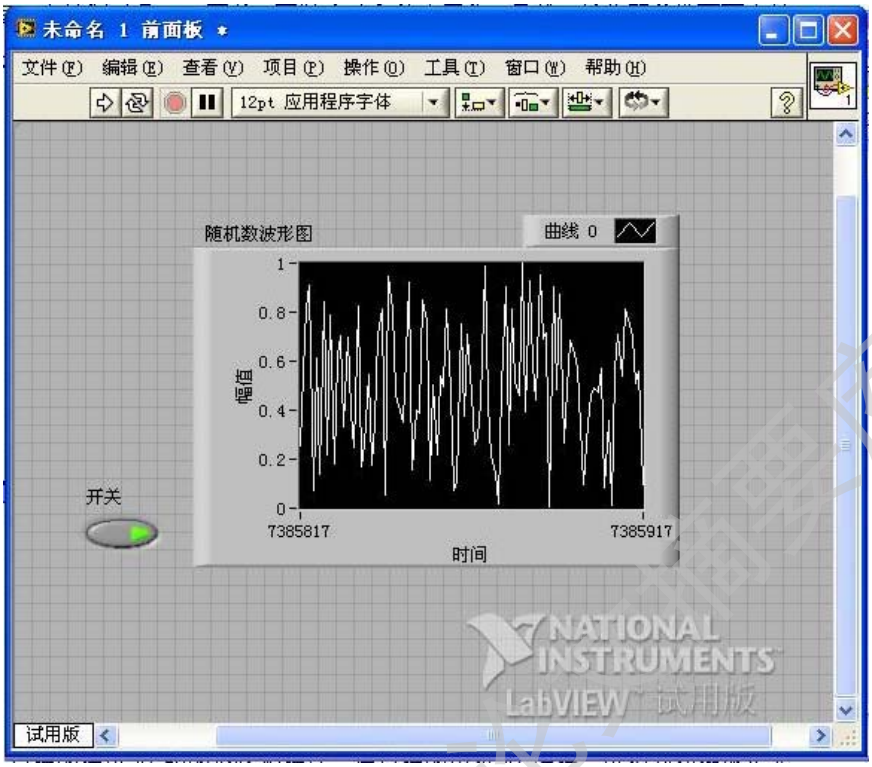

图 1.1 前面板

2. 程序框图

程序框图提供 VI 的图形化源程序。在程序框图中对 VI 编程，以控制和操纵定义在前面板上的输入和输出功能。流程图中包括前面板上的控件的连线端子，还有一些前面板上没有，但编程必须有的东西，例如函数、结构和连线等。图 1.2 是与图 1.1 对应的流程图[5]。我们可以看到流程图中包括了前面板上的开关和随机数显示器的连线端子，还有一个随机数发生器的函数及程序的循环结构。随机数发生器通过连线将产生的随机信号送到显示控件，为了使它持续工作下去，设置了一个 While Loop 循环，由开关控制这一循环。

图 1.2 程序框图

如果将 VI 与标准仪器相比较，那么前面板上的东西就是仪器面板上的东西，而流程图上的东西相当于仪器箱内的东西。在许多情况下，使用 VI 可以仿真标准仪器，不仅在屏幕上出现一个惟妙惟肖的标准仪器面板，而且其功能也与标准仪器相差无几。

3. 图标/连接器

图标和连接器指定了数据流进流出VI的路径。VI具有层次化和模块化的特性，既可以作为顶层程序，又可以作为其他程序的子VI。图标可把VI表示成子VI以供其他程序调用，而连接器则定义了VI 与调用它的程序数据交换的输入输出端口。

1.2 VI程序设计和调试

1. 程序设计

虚拟仪器的设计分为前面板设计和程序框图[6]：前面板设计窗口用于完成虚拟仪器前面板的设计；程序框图设计窗口完成虚拟仪器源代码的编写。

图1.3 前面板设计窗口

前面板设计窗口如图1.3 所示。在该窗口中，设计者可以利用工具模板中相应的工具选择控制模板中的相关的控件和指示器，拖放到窗口中的适当位置，并设置相应的标签。此时框图程序编辑窗口中会出现相应的前面板对象窗口图标。切换到程序框图设计窗口(如图1.4)，利用工具模板中相应的工具选择功能模板上相关的功能节点置于窗口中，使用连线工具将节点和端口连接，形成完整的框图程序，接着使用图标编辑器创建和编辑用户自定义的图标，完成虚拟仪器的设计工作。

图1.4 程序框图设计窗口

要将程序作为子VI,还必须定义VI 的连接器，使输入与输出端口能够与外部相连(给控件和指示器指定连接器端子)，同时创建图标以代表该子VI。

2．程序调试

LabVIEW 提供多种调试VI 程序的手段：通过加亮执行、单步、断点和探针帮助用户跟踪和观察经过VI的数据流。

在运行VI时，单击框图工具条中Highlight Execution 按钮可以动画演示框图执行情况，再次单击将恢复正常运行状态。单步执行是按照节点之间的逻辑关系，在数据连线上逐个节点的执行VI。设置断点则在工具面板上将鼠标切换至断点工具状态，单击框图程序中需要设置断点的地方，当程序运行到该断点时自动暂停。设置探针是在工具面板上将鼠标切换至探针工具状态，单击需要查看的数据连线，VI 运行时若有数据流经该连线将弹出对话框显示。

1.3 LabVIEW 软件特点

LabVIEW 软件具有丰富的功能，除了具有通俗易懂的图形化编程方式以及完整的调试工具外，还提供了丰富的数据采集、分析和存储的库函数[7]；32bit编译器编译生成32bit的编译程序，保证用户数据采集、测试或测量方案的高速运

行；LabVIEW 包括了PCI、GPIB、PXI、VXI、RS-232/485、USB 等各种仪器通信总线标准的所有功能函数；提供大量与外部代码或软件进行链接的机制，诸如DLL(动态连接库)、DDE(共享库)、ActiveX 等；具有强大的Internet 功能，支持常用的网络协议，方便网络、远程测控仪器的开发。以下具体介绍LabVIEW 各种外部接口和扩展以及它的网络通信方式。

1．LabVIEW 外部接口

LabVIEW 具有强大的外部接口能力，可以实现LabVIEW 与外部的应用软件、C 语言、Windows API、MATLAB 以及HiQ 等编程语言之间的通信。在LabVIEW中可以用的外部接口包括DEE、CIN、DLL、MATLAB Script 以及HiQ Script等。使用这些接口，可以充分利用其他软件的功能，甚至可以实现对系统驱动程序的调用，编写出功能强大的LabVIEW 应用软件[8]。

（1） 动态数据交换

动态数据交换(dynamic data exchange,DDE)是Windows 操作系统中一种基于消息的协议，用于在Windows 平台上的两个正在运行的应用程序之间动态交换数据，是进程间通信的一种方法。DDE 使用共享内存来实现进程之间的数据交换，并使用DDE 协议实现同步数据传递。DDE 协议是一组所有的DDE 应用程序都必须遵循的规则集。利用DDE，两个处于运行状态的程序之间可以相互发送或接收命令及数据，分别称为客户程序和服务器程序。DDE应用程序可以分为四种类型：客户、服务器、客户/服务器和监视器。客户程序向服务器程序请求数据或服务；服务器程序响应客户程序的数据或服务请求；客户/服务器程序既是客户程序又是服务器程序，它既可发出请求又可提供信息；监视器应用程序用于DDE 通信的调试。网络中应用程序之间的DDE 通信，必须利用网络动态数据交换服务器NetDDE Server 来实现。在LabVIEW 中可以利用LabVIEW DDE VIs 实现DDE 通信。

（2） 动态链接库

动态链接库(dynamic link library,DLL)是基于Windows 程序设计的一个非常重要的组成部分。动态链接库相对静态链接而言，所调用的函数代码没有被拷贝到应用程序的可执行文件中，仅仅在其中加入了所调用函数的描述信息。仅当应用程序被装入内存并开始运行时，在Windows 的管理下，在应用程序与相应的DLL 之间建立链接关系。当要执行DLL 中的函数时，根据链接信息，Windows 转