第32卷 第23期 计 算 机 工 程 2006年12月
Vol.32 No.23 Computer Engineering December 2006
·工程应用技术与实现· 文章编号：1000—3428(2006)23—0244—03 文献标识码：A 中图分类号：TP393

SHA-2(512)热噪声随机数发生器

王玉华[1]，牛丽萍[2]，张焕国[1]，沈志东[1]
(1. 武汉大学计算机学院，武汉 430079；2. 武汉大学遥感信息工程学院，武汉 430079)

摘 要：密码学的快速发展，使得安全协议和密码算法的强度越来越依赖于随机数质量。该文提出了一种新的安全随机数发生器结构，该结构是基于SHA-2(512)哈希函数，该函数的强度确保所生成随机数的不可预测性。给出了该函数的FPGA实现结构。考虑到性能、功耗、灵活性、费用和面积等要求，所提出的结构在许多应用中都是一种灵活解决方案。

关键词：SHA-2(512)；热噪声；随机数

Thermal Noise Random Number Generator Based on SHA-2(512)

WANG Yuhua[1], NIU Liping[2], ZHANG Huanguo[1], SHEN Zhidong[1]
(1. School of Computer Science, Wuhan University, Wuhan 430079;
2. School of Remote Sensing Information Engineering, Wuhan University, Wuhan 430079)

【Abstract】 With the rapid development of cryptography, the strength of security protocols and encryption algorithms consumingly relies on the quality of random number. This paper presents a new and security random number generator. The philosophy architecture is based on SHA-2 (512), whose security strength ensures the unpredictability of the produced random numbers. Furthermore, an FPGA-based implementation of architecture is described. The proposed architecture is a flexible solution in many applications taking into account the performance, power consumption, flexibility, cost and area.

【Key words】 SHA-2(512); Thermal noise; Random number

1 概述

随着密码学的快速发展，高质量随机数的需求迅速增长。非对称算法中公钥/私钥密钥对由随机数位流生成[1]；在认证协议对称算法中，验证时生成密钥所需要的填充字节和填充值要用到随机数[2]。智能卡的应用中为了对抗旁路攻击而采取的对抗措施也要求有高质量的随机数[3]。密码系统的安全性主要依赖于随机序列的不可预测性[4]。因此，设计性能优越的随机数发生器比较困难。

密码学中使用的随机数发生器通常有两种：真随机数发生器和伪随机数发生器。真随机数发生器由物理噪声源提供随机序列，而伪随机数发生器是根据确定算法将短密钥随机扩展成长序列。从密码学的角度上来讲，真正安全的随机数发生器生成的序列不存在多项式时间算法。具有多项式时间算法的序列 s，对于它的前 l 位，可以以大于 1/2 的概率预测 $(l+1)st$ 位[5]。根据单农的通信数学理论，密码学角度上安全的随机数发生器，k位长输出流的熵应该尽可能地接近k。

在许多要求随机数的应用中，我们通常使用伪随机数发生器，伪随机数发生器通常使用确定算法，在一个初始值基础上生成随机数，而这个初始值很容易被观察者替换成另一个随机数。由于算法通常公开，初始值就成为随机性的唯一来源，而伪随机数发生器输出序列的熵从来都不会大于初始值的熵，因此伪随机数发生器的初始值应该由具有真随机性的发生源提供。在自然界中，有许多物理现象具有随机性，例如分时操作中单位时间内处理的用户数、外围设备占用CPU的时间、电子噪声和放射性衰减等[5]。但对于硬件实现，热噪声是理想选择。然而，由于带宽限制、工艺局限、老化、温度漂移和干扰等问题，即使进行了很好的设计，所生成的随机数也会有一定的相关性。为解决这个问题，我们会采取一些措施来处理所生成的随机数。

本文提出一种新的随机数发生器，该随机数发生器基于热噪声和 SHA-2 (512)，并且以硬件实现。在该结构中，物理随机数发生器生成原始随机位流，SHA-2 (512)对其进行处理消除由物理随机数发生器产生的不理想特性。SHA-2 (512)对原始位流进行高度压缩提供了更强的不可预测性，同时也提高了体系的安全强度。系统所生成的随机数字长为 512 位，这个长度在所有的随机数应用中都可以接受。

2 随机数发生器的系统结构

随机数发生器的系统结构如图 1 所示，该系统包含两个部分：热噪声物理随机数发生器和 SHA-2 (512) 哈希函数。

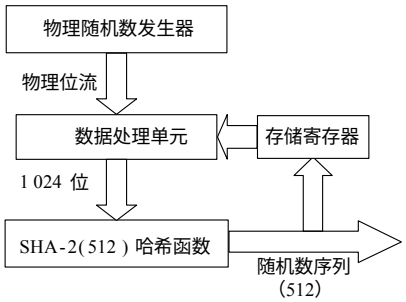

图 1 随机数发生器的系统结构

基金项目：国家自然科学基金资助重点项目(60373087，90104005)；国家教育部博士点基金资助重点项目(20020486046)
作者简介：王玉华(1973－)，女，博士，主研方向：流密码及其应用；牛丽萍，硕士；张焕国，教授、博导；沈志东，博士
收稿日期：2005-12-22 **E-mail：**yuhua.w@tom.com

在该系统中，由热噪声所产生随机数序列的质量受许多因素的影响，这些因素使得所产生的随机序列有一定的相关性。为了消除这些相关性，提高序列的统计特性，我们设计了一个消除相关性的算法去修正原始序列。系统利用SHA-2(512)的高度压缩特性来消除原始随机序列的不理想特性。对于恢复给定信息摘要的原始信息，SHA-2(512)哈希函数具有的高安全级别确保了计算上的不可行性，这在密码学的应用中很重要。因此我们选择了 SHA-2(512)作为系统的消除相关性算法。

系统的整个操作过程很简单。第 1 次进行数据处理时，物理随机数发生器生成初始数据块，SHA-2(512)处理这个初始数据块，生成第 1 个随机数。第 2 个随机数的生成不同于第 1 个随机数的生成，SHA-2(512)输入数据有些差异。在第 2 次数据生成过程中，SHA-2(512)第 1 次处理后的数据存储到存储寄存器中，和物理随机数发生器提供的噪声位流一起被数据处理单元处理后作为 SHA-2(512)第 2 次输入数据，这个数据被处理后生成第 2 个随机数。这个过程在以后的数据处理中一直重复。

3 物理随机数发生器电路

随机数发生器的物理随机数发生器部分由一个热噪声电路组成。这个热噪声电路由 3 部分组成：物理噪声源，放大电路和信号转换电路。物理随机数发生器的结构如图 2 所示。

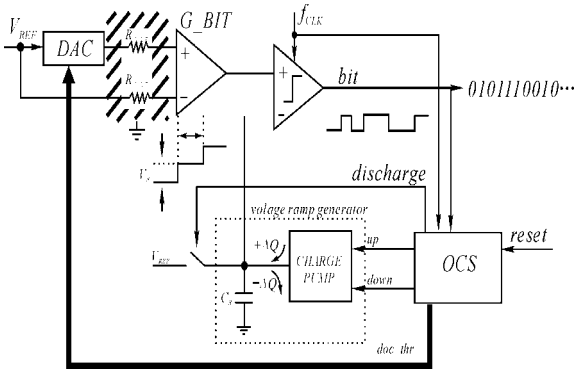

图 2 物理随机数发生器电路

在上面的电路结构中，集成的电阻为整个系统提供热噪声；放大器将热噪声放大，被放大后的热噪声和一个钟控比较仪的参考电压相比较，将比较后的结果作为一个随机位输出，便形成了随机位流。 然而，由于很多因素都可能将非随机特性引入随机位流，使得生成的随机位流随机特性很差。电路基片、电源和外部干扰都可能引起输出位流的周期性模式从而影响序列的随机特性，这在许多应用中都是要认真考虑的，尤其是在智能卡应用中。为了消除这些因素的影响，在上面的电路中，我们采取了一些措施。热噪声电路使用交叉设计并外接地线。放大电路中，使用复杂的 PSRR 拓扑结构，并且设计了一个零失调系统来调控电路中电压的失调。

这个零失调系统也由 3 部分组成 数模转换电路(DAC)，斜坡电压发生器和调零控制系统 (OCS)。DAC 扫描输入电压偏差，一旦发现放大器的电压有偏差（放大器在线性区域工作)，通过斜坡电压发生器，比较仪的参考电压将在V_{REF} 附近浮动以消除失调电压的影响。这个过程由OCS 通过下面程序进行控制：

```
OCS( input: bit; output: dac_thr, up, down, discharge)
{   reset:   discharge='1'; wait for T_RST;
             discharge='0'; dac_thr=0;
   stage1: while (bit='0' and dac_thr<N_TH)
             dac_thr++;
   stage2: while (1) {
             if (bit='0')   then
                 down='1';
             else
                 up='1';
                 wait for T_S;
                 down='0'; up='0';}
}
```

这里T_{RST}是指比较仪的重启时间，N_{TH}是指DAC的门限数，T_S是指斜坡电压发生器调整电压的时间。我们在电路中用一个小的电容C_S（建议用 3pF）使得电压调节器（Charge Pump）获得一个小幅电压（约 1mV)。在不影响白噪声带宽的条件下，比较仪输入端的反馈电路可对放大器输出段的噪声波普进行高通过滤，截取频率为 $f_c = \frac{V_S}{2\pi T_S}$， $T_S = n \cdot T_{CLK}$，以此消除电路中失调电压。

4 SHA-2(512)哈希函数

现代密码学中哈希函数通常被称作单项函数。哈希函数是一个计算上有效的函数，它将任意长度的二进制串映射成固定长度串。哈希函数单方向操作的方式和通常的分组密码不同。这表明哈希函数能生成任何初始值的输出串，但对于任意给定的哈希输出却不可能计算出它原始值。即由于对于给定摘要在计算上不可能恢复原始信息，这种算法的安全性是可以确保的。

SHA-哈希函数由NIST 设计，用于数字签名标准。SHA-1 算法的主要操作是将长度不小于 512 位的输入信息转换成 160 位的输出信息（信息摘要)。SHA-1 是世界上最有名的哈希函数，但这个设计的安全级别只是相当于 80 位的分组密码。因此，2002 年 8 月 26 日，NIST 宣布批准FIPS 180-2，FIPS 180-2 介绍了 3 种新哈希函数规范SHA-2(256,384,512)。SHA-2 (512)在提供给输入数据块的安全位数上有很大不同。哈希函数安全级别和信息摘要长度直接相关，这在随机数发生器应用中是非常重要。本文的系统充分利用了SHA-2（512）高压缩比率来消除上面提到的不理想因素影响，提高所生成随机数的统计特性。

SHA-2(512)哈希函数的结构如图 3 所示。

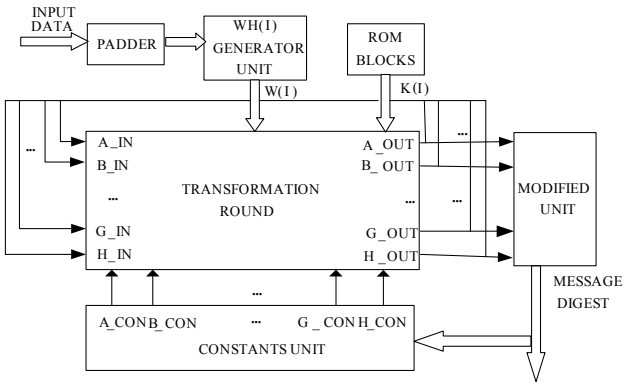

图 3 SHA-2（512）哈希函数结构

PADDER 填充输入数据将它们转换成为 1 024 位的块，这些 1 024 位的块会被顺序处理。被填充的数据由下面的过程来生成：一个逻辑“1”，后面接 m 个“0”和一个 64 位的整数，这些被附在输入数据的末尾，生成长度为 1 024 倍数长度的

填充数据，64 位的整数表明输入数据长度，被填充后的数据是 1 024 位的倍数。填充后的数据被分割成 N 个等长度的数据块 $M^1 \cdots M^N$ 并且按照下面的公式顺序处理。

$$\begin{cases} W_i = M^i & 0 \le i \le 15 \\ W_i = \sigma_1 W_{i-2} + W_{i-7} + \sigma_0 W_{i-15} + W_{i-16} & 15 < i < 80 \end{cases}$$

标准规定一种算法的基本转换要对数据进行 80 次的操作。80×64-位ROM 块被用来预定义K_i常量。在最后阶段，修正函数处理数据并将处理后的结果输出。

5 实验结果

系统的结构用 VHDL 来描述并且用 XINLINX FPGA Vertex Device (v300pq240)集成实现。本文的随机数发生器集成实现的结果如表 1 所示。

表 1 FPGA 实现结果

Allocated Area	Used/allocation	Utilization
Fun. Generators	5 268/6 144	86%
CLB Slices	2 710/3 072	88%
Dffs or Latches	4 182/6 144	68%
Frequency	80MHz	

统计质量是衡量随机数序列的主要指标。因此，我们采用了FIPS140-1 和SP800-22 两种测试标准对所生成的随机序列进行检测。所有的测试都是在长度为 10^6位的基础上进行。由物理随机数发生器生成的原始位序列和被SHA-2(512)处理后的序列都能通过FIPS140-1 测试，但是对SP800-22 测试，两种随机位序列的测试结果是不相同的。表 2 和表 3 展示了用SP800-22 测试对两种随机位序列的测试结果。从两个表中可以看出，由SHA-2(512)哈希函数处理过的随机位序列有着更好的统计特性。

表 2 物理随机数发生器的测试结果

	P Low	P High	Avg score	Pass Ratio
Frequency	0.762	0.873	0.805	0.967
Block-Frequency	0.706	0.849	0.810	1.000
Cusum-Forward	0.822	0.861	0.837	0.822
Cusum-Reverse	0.632	0.682	0.664	0.724
Runs	0.242	0.354	0.293	0.872
Long Runs of ones	0.102	0.172	0.135	0.662
Rank(32×32)	0.742	0.812	0.796	0.945
Spectral DFT	0.682	0.752	0.716	0.663
Non-overlapping	0.447	0.506	0.495	0.796
Overlapping	0.114	0.627	0.449	0.801
Universal (L=7,Q=1280)	0.427	0.521	0.483	0.812
ApproxEntropy(m=5)	0.462	0.521	0.793	0.897
Lempel-ziv Complexity	0.842	0.865	0.851	0.915
Linear Complexity	0.345	0.521	0.369	0.925
Serial(m=5), ($\nabla\Psi_m^2$)	0.632	0.682	0.664	0.724

表 3 SHA-2(512)处理后的序列测试结果

	P Low	P High	Avg score	Pass Ratio
Frequency	0.768	0.932	0.886	0.995
Block-Frequency	0.811	0.862	0.849	1 000
Cusum-Forward	0.917	0.943	0.925	0.987
Cusum-Reverse	0.612	0.689	0.668	0.992
Runs	0.323	0.361	0. 344	0.961
Long Runs of ones	0.187	0.446	0.213	0.885
Rank(32×32)	0.869	0.887	0.878	0.977
Spectral DFT	0.561	0.615	0.573	0.904
Non-overlapping	0.602	0.784	0.671	0.966
Overlapping	0.076	0.083	0.077	0.924
Universal (L=7,Q=1280)	0.437	0.677	0.593	0.992
Approx Entropy (m=5)	0.691	0.740	0.733	0.948
Lempel-ziv Complexity	0.365	0.419	0.396	0.998
Linear Complexity	0.294	0.315	0.310	0.972
Serial(m=5), ($\nabla\Psi_m^2$)	0.685	0.762	0.746	0.997

6 结论

本文提出了一种新的随机数发生器结构并用硬件加以实现。热噪声为我们提供了物理随机位流源，SHA-2(512)的安全强度和哈希函数的优势确保了所生成的随机数序列的不可预测性。所提出的随机数发生器结构在很多应用中都是一种灵活的解决方案，在该系统中，也可以用其他好的算法来处理物理随机数发生提供的原始随机序列以提高随机序列的统计特性。

参考文献

1 Callegari S, Rovatti R, Setti G. Embeddable ADC-based True Random Number Generator for Cryptographic Applications Exploiting Nonlinear Signal Processing and Chaos[J]. IEEE Transactions on Signal Processing, 2005, 53(2): 793-805.

2 Rankl W, Effing R. Smart Card Handbook(2nd Edition)[M]. New York: John Wiley & Sons, 2000.

3 Kocher P, Jaffe J, Jun B. Differential Power Analysis, Advance in Cryptology(Crypto´99)[M]. Heidelberg, Germany: Springe-Verlag, 1999: 388-397.

4 Tsoi K H, Leung K H, Leong P H W. Compact FPGA-based True and Pseudo Random Number Generators[C]. Proc. of the 11th Annual IEEE Symposium on Field-programmable Custom Computing Machines, 2003: 51-61.

5 Menezes A J, Van Oorschot P C, Vanstone A. Handbook of Applied Cryptography[M]. CRC Press, 2001.

（上接第 243 页）

种设计思路的样机。实验证明，该机器人可以实现直线运动与转向运动的合理、有效结合，转向角度、角速度可控，直线行进步距、速度可调，行动灵活可靠，实现了预期的设计目标。

下一步的工作包括：研制基于这种机械结构的适应特殊环境的机器足，如适应垂直光滑平面的吸盘式步足、适应导磁材料（如钢板表面、钢管内壁）上的电磁步足等。

参考文献

1 徐小云， 颜国正. 六足移动式微型仿生机器人的研究[J]. 机器人, 2002, (5): 427-429.

2 徐小云, 颜国正, 丁国清. 微型六足仿生机器人及其三角步态的研究[J]. 光学精密工程, 2002, 10(4): 392-396.

3 蒋新松. 机器人学导论[M]. 沈阳: 辽宁科学技术出版社, 1994.

4 ICP DAS 公司. DIO-24/144 使用说明书[Z]. 2005.

5 游志宇. VC中基于Windows的精确定时 VC知识库在线杂志[EB/OL]. http://www.vckbase.com/document/viewdoc/?id=1301.