基于 Rijndael 密码的伪随机比特产生器*)

Pseudo-Random Bit Generator Based on Rijndael

王宏霞[1] 虞厥邦[1] 范明钰[2]

(电子科技大学光电子技术系570实验室 成都610054)[1]

(清华大学电子工程系 北京100084)[2]

Abstract It is important to generate random number in cryptography. In this paper, we design Pseudo-random Bit Generator (PRBG), based on Rijndael with a block length of 256 and a cipher key length of 256 by applying the OFB mode. The random nature and the security have been analyzed. The PRBG is also easy to be realized in application.

Keywords Block cipher, Pseudo-random sequence, Security

1 引言

在计算机网络深入普及的信息时代,信息本身就是时间,就是财富。信息的传输通过脆弱的信道,信息存储于"不设防"的计算机系统中,如何保护信息的安全已成为当今普遍关注的重大问题,密码技术是有效且可行的办法。我们知道随机数对密码的研究有着十分重要的作用,序列密码的关键在于伪随机数的产生,在许多协议的执行期间也需要产生随机数。通过抛掷硬币或其它物理处理来产生随机数是费时费钱的,所以在实际中通常使用伪随机比特产生器(PRBG),一个 PRBG 是用一个短的随机比特串("种子")开始且把它扩展成更长"看起来随机"的比特串,这样一个 PRBG 降低了在实际使用中需要的随机比特的总数目,在一般的计算机程序语言中,随机函数通常基于线性同余或有限域理论来产生随机数,虽然其速度非常快,但是不安全,从线性移位寄存器(LFSR)得到的 PRBG 也是相当不安全的,这些 PRBG 虽在模拟中相当有用,但对密码应用来说保密性很差,文[4]提出的 RSA 生成器虽然其安全性是基于破译 RSA 体制的困难性,但实际实现时由于模乘法的运算使得速度很慢,为此,本文基于 Rijndael 密码,利用分组密码的输出反馈(OFB)工作模式设计了 PRBG,计算机仿真结果表明得到的0-1随机比特串随机性好,满足 Golomb 提出的随机性三个公设,且安全强度高,实际实现时速度较快,从而便于应用。

2 Rijndael 密码简介

为了更好地理解我们所设计的 PRBG,这里有必要对 Rijndael 密码作一简单介绍。Rijndael 密码是美国国家标准技术研究所(NIST)于1998年8月20日公布的15个 AES(Advanced Encryption Standard)候选算法之一,现已进入第二轮筛选出的5个候选算法,NIST 最终将在这5个候选算法中选出一个作为 AES,Rijndael 密码是一个迭代分组密码,其分组长度和密钥长度都可变,分组长度和密钥长度可以独立地指定为128/192/256比特,圈数(Nr)为分组长度和密钥长度的函数。圈变换由四个不同的变换组成,在伪 C 代码的记法中,我们有:

```
Round (State, RoundKey)
{
    ByteSub (State);
    ShiftRow (State);
    MixColumn (State);
    AddRoundKey (State, RoundKey)
}
```

密码的结尾圈稍微有点不同,只是把 MixColumn 这一变换去掉而已,圈密钥 (RoundKey)按规定的方式从扩展密钥中取出,扩展密钥由密码密钥经变换而得到,而不直接指定,且对密码密钥的选取没有任何限制。总的来说,Rijndael 密码由以下三个部分组成:

(1) 一个初始圈密钥加;

(2) Nr-1圈;

(3) 一个结尾圈。

*)本课题得到电子科技大学抗干扰国防重点实验室资助。王宏霞 博士生,研究方向为计算机安全、保密通信等。虞厥邦 教授,博士生导师,研究方向为非线性电路、计算智能等。范明钰 博士后,研究方向为计算机网络安全,ATM 网络技术,计算智能等。

从 Rijndael 密码的加密过程来看，它其实是一个复杂的非线性变换，具体内容请参考文[6]。

3 伪随机比特产生器机制

文[2]给出了设计 PRBG 的一系列准则，文[6]指出有许多方法使 Rijndael 密码可以用来形成满足这些准则的 PRBG，并给出了一个例子。本节中我们应用 Rijndael 密码的 OFB 模式来形成一个 PRBG，其中使用的分组长度和密钥长度都是256比特。图1是 PRBG 的原理框图，反馈寄存器作为 Rijndael 分组密码的输入，密钥 k 作为一个"种子"，在第 i 次密码迭代中，先计算 $\mathrm{Rijndael}_k(R_{i-1})$（初始向量 R_0 无需保密），然后将变换后的256比特选最左边的 n 比特作为伪随机比特串的输出，同时，这 n 比特密钥直接反馈至 Rijndael 密码的输入端。

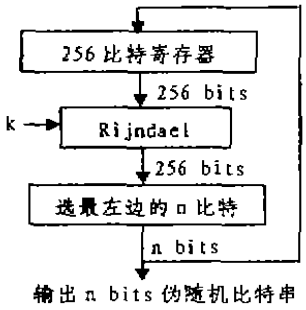

图1 伪随机比特产生器

4 统计随机性

要分析 PRBG 产生的伪随机序列是否具有良好的随机特性，可通过分析其主要的统计特性是否与真正的随机序列的统计特性相一致。为了度量0-1序列的随机性，*Golomb* 提出了下列三个公设：

(1)一个周期中"0"与"1"的数目基本平衡；

(2)一个周期中，1游程的个数占游程总数的1/2，2游程的个数占游程总数的$1/2^2$，…，c 游程的个数占游程总数的$1/2^c$，且相同长度的0-游程与1-游程的数目基本平衡；

(3)自相关函数为二值函数。

针对上述三个公设，我们分别用计算机仿真来进行检验。基于 MATLAB 平台，把随机发生器的"种子"置零，以0.5为门限值产生长为256的0-1行向量作为 Rijndael 密码的种子密钥，用我们所设计的 PRBG 产生了长为4000的0-1随机序列，图2是该序列的 χ^2（自由度为1，显著水平取5%）检验结果，从图2中可看出随着序列长度 N 的增加，χ^2 值趋于减小，且对于任意长度的序列，χ^2 值均小于 $\chi^2_{0.05}(1)$ 的临界值3.84，并且随着 N 的增加，χ^2 值贴近于0，这说明此随机序列"0"与"1"的数目基本平衡。通过改变 Rijndael 密码的种子密钥，得到2000个长度为80的不同序列，设序列中"0"与"1"的数目之差为 L，经过大量运算，结果有243个平衡序列，$|L|=2$ 的序列有412个，并且随着序列长度的增加，序列的平衡特性逐渐改善，因此本文所设计的 PRBG 满足随机性第一公设。

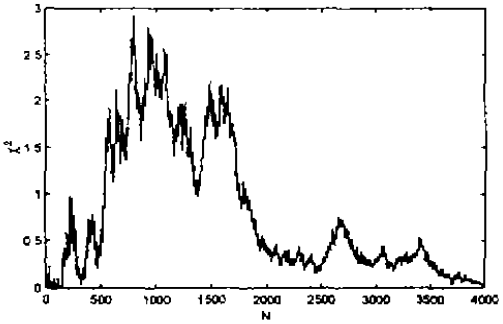

图2 伪随机序列的 χ^2 检验（N=4000）

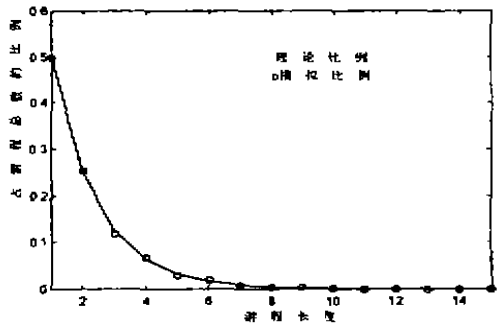

图3 伪随机序列的游程分布（N=4000）

图3是"种子"为零的条件下，PRBG 所产生的长度为4000的0-1序列的游程分布测试结果。从图中可看出不同长度的游程个数占游程总数的比例都接近于第二公设的比例，并且0-游程与1-游程的数目相等，均为991个。改变 PRBG 的种子密钥，经过多次测试，发现所得的伪随机序列的游程分布均接近于理论分布结果，这说明本文所设计的 PRBG 满足随机性第二公设。

0-1序列 $\{x_i\}$ 的归一化自相关函数定义为

$$ac(\tau)=\frac{1}{N}\sum_{i=0}^{N-1}(-1)^{x_i}(-1)^{x_{i+\tau}},\ 1-N\leqslant\tau\leqslant N-1$$

按照上述自相关函数定义，我们对本文所设计的 PRBG 产生的伪随机序列进行了计算，图4是"种子"为零的条件下，长度为4000的0-1序列的归一化自相关，其中相关间隔 τ 从−1000到1000。从图4可看出伪随机序列的自相关函数具有 δ 函数特性，因此 PRBG 满足

随机性第三公设。

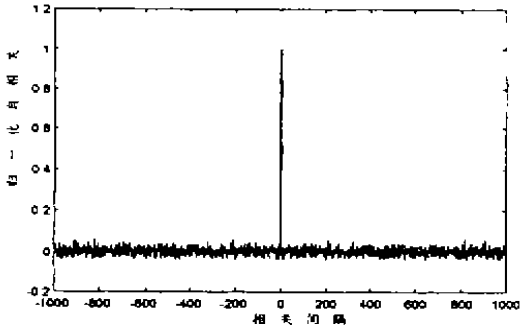

图4 伪随机序列的归一化自相关(N=4000)

5 速度和安全上的考虑

伪随机比特产生器的两个主要目标是快而安全，当然这两个需求有时是矛盾的。基于线性同余或 LFSR 的 PRBG 实际上是非常快的，但也是非常不安全的。文[6]指出 Rijndael 密码适合在多种处理器上和专用芯片上有效地实现，在通用处理器上用软件实现非常快，而对硬件的实现局限于两个特殊情形：速度相当高且没有规模限制的芯片；提高 Rijndael 密码执行速度的灵巧卡上的微型协处理器。因此，如果以软件或专用芯片的方式来实现我们所设计的 PRBG，其速度是非常快的。我们利用 TI 的 TMS320VC5402 DSP 芯片实现了本文所设计的 PRBG，速度可达到每秒产生 28kB 伪随机比特串。

现在我们来探讨一下本文 PRBG 的安全性，由于 Rijndael 密码算法的原形是 Square 算法，它的设计策略是宽轨迹策略，这种策略是针对差分分析和线性分析提出的，此外，文[6]指出对于6圈或更多圈的 Rijndael 密码，截段差分攻击和 Square 攻击均不比穷举密钥攻击快，并且 Rijndael 密码的 S-盒在 $GF(2^8)$ 域中的复杂表达式防止了对2圈或3圈以上的插入攻击，Rijndael 密码的密钥调度具有很高的扩散性和非线性性，使得相关密钥攻击不可能获得成功。总之，对 Rijndael 密码最有效的密钥恢复攻击是穷举密钥法，穷举密钥的期望尝试次数与密码密钥的长度有关，本文使用的 Rijndael 密码的密钥长度为256比特，因此密钥空间最大为 $2^{256}>10^{77}$ 个，假设一个密钥搜索软件每秒能搜索到 10^{30} 个密钥，即使让它昼夜不停地工作，至少也得花 3.6×10^{39} 年才能完成，可见在未知密码密钥的情况下，预测该 PRBG 的输出伪随机比特串很难实现。文[1]指出一个安全的 PRBG 除了其输出比特串难于预测外，其周期还必须足够长。文[6]阐明了 Rijndael 密码不会出现象 IDEA 中一样的弱密钥，且对密钥的选取没有限制条件，因此每一次密码迭代中就不会出现 Rijndael$_k(R_{i-1})=R_{i-1}$ 的情形，这样一来 PRBG 输出的伪随机比特串的周期就会保证足够大，可能的周期最大为 $(256!)^{2^{256}}\to\infty$。所以，PRBG 输出的伪随机比特串能够做到截获比周期短的一段时，不会泄露更多的信息，从而可以说本文的 PRBG 是安全的。

结束语 本文基于 Rijndael 密码，利用 OFB 工作模式设计了一个 PRBG，该 PRBG 通过使用不同的密码密钥来产生不同的伪随机比特串，如果把二进制比特串转换成十进制整数，就得到不同范围的整数形式的伪随机数。该 PRBG 的优点是随机性好，安全性强，易于实现，在计算机安全应用中提供了信息高度保密的手段。

参 考 文 献

1 Zeng K C, Yang C H, Wei D Y, Rao T R N. Pseudorandom Bit Generators in Stream-Cipher Cryptography. IEEE Computer, 1991, 24(2): 8～17

2 Kelsey J, Schneier B, Wagner D, Hall C. Cryptanalytic Attacks on Pseudorandom Number Generators. Fast Software Encryption, LNCS 1372, S. Vaudenay, Ed., Springer-Verlag, 1998. 168～188

3 Blum L, Blum M, Shub M. A Simple Unpredictable Pseudo-random Number Generator. SIAM J. Comput., 1986, 15: 364～383

4 Alexi W, Chor B, Goldreich O, Schnorr C P. RSA and Rabin Function: Certain Parts Are As Hard As The Whole. SIAM J. Comput., 1988, 17: 194～209

5 Golic J. Intrinsic Statistical Weakness of Key-stream Generators. Advances in Cryptology-Eurocrypt'94, Springer-Verlag, 1995. 91～103

6 Daemen J, Belgium V R. 美国21世纪加密标准候选算法. 北京：总参谋部机要局出版，1998. Also see Http://www.nist.gov/aes

7 Lenstra A K, Lenstra H W. Algorithms in number theory. Handbook of Theoretical Computer Science, Volume A: Algorithms and Complexity, 1990. 673～715