第 33 卷 第 5 期 计 算 机 工 程 2007 年 3 月
Vol.33 No.5 Computer Engineering March 2007
·博士论文· 文章编号：1000—3428(2007)05—0032—04 文献标识码：A 中图分类号：TP918.1

基于 FCSR 和 LSFR 相结合的密钥流生成器

郑 宇[1]，何大可[1]，唐小虎[1,2]，邓子健[1]
(1. 西南交通大学信息科学与技术学院，成都 610031；2. 东南大学移动通信国家重点实验室，南京 210096)

摘 要：分析了由 Schneier 提出的 FCSR 和线性反馈移位寄存器（LFSR）相结合的密钥流生成器的结构特性，给出了其可生成密钥流的周期和线性复杂度的理论上界，讨论如何选择 LFSR 和 FCSR 的参数以使产生的密钥流具有较好的伪随机特性，并使其周期和线性复杂度尽可能接近理论上界。利用美国技术与标准局（NIST）提供的 STS 软件包进行生成器选定参数下输出的密钥流的 8 项随机性测试，结果表明，在该文论述的参数选择方法下，生成器产生的序列具有良好的伪随机特性。利用 FPGA 实现了该密钥流生成器，并通过与 5 种现有流密码方案实现结果的性能比较发现，该方案具有较高的密钥流吞吐量和性价比，可在移动终端实施。
关键词：带进位反馈移位寄存器；线性移位寄存器；2-adic 复杂度；线性复杂度；随机性检测

Key Stream Generator Based on Combination of FCSR and LFSR

ZHENG Yu[1], HE Dake[1], TANG Xiaohu[1,2], DENG Zijian[1]
(1. School of Information Science & Technology, Southwest Jiaotong University, Chengdu 610031;
2. National Mobile Communication Research Lab., Southeast University, Nanjing 210096)

【Abstract】 A novel stream cipher based on the combination of FCSR and LFSR is proposed by Schneier, which is paid close attention by researchers. In this paper, the properties of this stream cipher are analyzed and the theoretical upper bound of period and that of linear complexity are presented. Then, how to select the parameters of FCSR and LFSR is discussed so that the output sequences can access the theory up bound as much as possible. Meanwhile, the pseudorandom properties of generated sequence are checked by eight tests in NIST STS package. According to the testing results, the generated sequences have good pseudorandom properties if the parameters are selected as the proposed rule. The stream cipher is realized in FPGA and compared with the implementation result of other stream ciphers, which proves this stream cipher is very efficient and can be employed in mobile equipment.
【Key words】 FCSR; LFSR; 2-adic span; Linear span; Test of pseudo-randomness

1993 年，Klapper和Goresky提出了带进位的反馈移位寄存器[1,2]，并对这易于实现的序列生成器进行了初步分析[3~6]。由于FCSR与LFSR结构上的相似和Z_2与$GF_2[x]$的相似，因此导致了FCSR与LFSR平行的研究思路，但与LFSR一样，FCSR也无法单独作为密钥流生成器。

Schneier在文献[9]中提出了LFSR和FCSR相结合的序列生成器（详见 1.2 节）。该方案利用带进位加运算和异或运算分别打破LFSR和FCSR的代数特性，以获得更大的混淆。因此，更加难以被分析和破解。该序列生成器公布后被广泛的引用和转载[10,11]，但目前对该序列生成器进行分析的文章非常少，生成器的性能以及产生的伪随机序列的伪随机特性到底如何也没有相应的评价。

本文分析了该密钥流生成器的结构和输出序列的周期以及线性复杂度特性，给出了相应的理论上界，并讨论了如何选择LFSR和FCSR的参数，以保证生成器产生的序列具有尽可能好的伪随机性。同时，参照文献[11]的测试方法，利用美国国家技术与标准局（NIST）的STS软件包[12]测试了该生成器产生的密钥流的平衡性、均匀性、线性复杂度、游程特性、deBruijn特性[3]、线性独立性和可压缩性等随机性指标，有助于揭示和进一步研究该组合生成器的特性。最后在FPGA上实现了该算法，并与文献[14]中现有几种流密码方案的FPGA实现结果进行了比较，有利于深入了解该算法的性能和效率。

1 基于 FCSR 和 LFSR 的密钥流生成器

1.1 FCSR

FCSR 如图 1 所示。

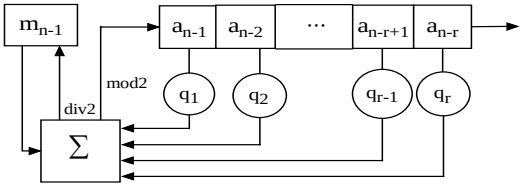

图 1 FCSR 的结构

设移位寄存器的级数为 r，抽头系数 $q_i \in GF(2)$，$i = 1, 2, ..., r$。在某时刻进位寄存器值为 $m_{n-1} \in N$，移位寄存器每个单元的值为 $a_{n-1}, a_{n-2}, ..., a_{n-r+1}, a_{n-r} \in GF(2)$。FCSR 按以下规则运算：

基金项目：全国百篇优秀博士论文作者专项基金资助项目（200341）；四川省青年科技基金资助项目(04ZQ026-048)；东南大学移动通信国家重点实验室开放基金资助项目
作者简介：郑 宇(1979－)，男，博士生，主研方向：通信保密，信息系统安全工程，密码学；何大可、唐小虎，教授、博导；邓子健，硕士生
收稿日期：2006-05-16 **E-mail：**zhyu_swjtu@163.com

(1)计算整数和 $\sigma=\sum_{i=1}^{r}q_i a_{n-i}+m_{n-1}$ ；

(2)寄存器右移 1 位，输出最右边的比特a_{n-r}；

(3)计算 $a_n=\sigma \bmod 2$ ；

(4)替换 $m_n=(\sigma-a_n)/2$。

定理 1[1] 有理数 $\alpha=p/q$ 和二元终归周期序列a＝（$a_0,a_1,a_2,\ldots$）之间存在一一对应关系，对应规则是序列a为有理数的 2-adic展开，即 $\alpha=\sum_{i=0}^{\infty}a_i 2^i$。其中 $q=\sum_{i=1}^{r}q_i 2^i-1$ 为奇有理数，是能生成该序列的FCSR的连接数；$p=\sum_{k=0}^{r-1}\sum_{i=0}^{k}q_i a_{k-i}2^k-m_{r-1}2^r$。序列是严格周期的充分必要条件是 $\alpha\le 0$ 且 $|\alpha|<1$。

定理 2[4] 如果p和q互素，$-q<p\le 0$，q为奇数，则 $\alpha=p/q$ 的 2-adic展开序列的周期为$T=ord_q(2)$。

定理 3[4] 任何终归二元周期序列均可由FCSR产生。

定义 1[4] 序列a的 2-adic复杂度为实数 $\varphi_2(a)=\log_2\Phi(p,q)$，其中 $\Phi(p,q)=\max(|p|,|q|)$。

定义 2[2] de Bruijn特性是指任意相同长度的子序列在样本序列中出现的次数相差不大于 1。

定义 3[7] q为素数，且 2 为模q的本原根，则q是 2-素数。若 $q=2p+1$，p，q都是 2-素数，则q称为强 2-素数。

1.2 FCSR 和 LFSR 相结合的密钥流生成器

图 2 为 Schneier 提出的 LFSR 和 FCSR 相结合的序列生成器构造方案。该生成器的左半部由 4 个 LFSR 进行带进位加后输出序列，并以钟控方式驱动右半部分 4 个 FCSR。当左半部分输出为 1 时，各个 FCSR 进行移位操作，否则，右半部分保持上一次输出。最后将左右两个部分的输出结果进行异或运算便得到最终的输出序列。由于利用带进位加打破了 LFSR 的代数特性，而用异或运算搅乱了 FCSR 的代数特性，因此该密钥流生成器被期望具有良好的混淆特性和伪随机性。

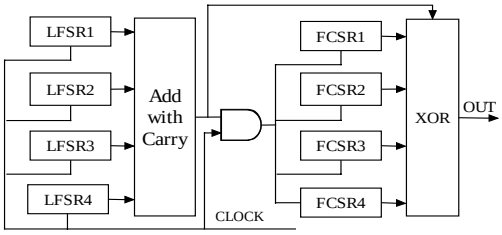

图 2 FCSR 和 LFSR 相结合的密钥流产生器

2 混合生成器的周期和线性复杂度分析

2.1 混合式生成器的分解

从图 2 可以看出，直接分析组合生成器的随机性指标非常困难。因此本文首先将该密钥流生成器分为以下左右两个部分来讨论。如图 3 所示，首先研究生成器的左半部分（定义为 LFSR_C）输出序列 c 的周期和线性复杂度。然后，将生成器右半部分视为如图 4 所示的 4 个基本钟控序列的组合，进一步讨论其输出序列进行异或后得到的 d 的伪随机性。最后将 c 和 d 进行异或运算便得到最终的输出序列。

为使生成器能输出伪随机性更好的密钥流，应按以下规则取值：LFSR1～LFSR4 的特征多项式分别取n_1，n_2，n_3和n_4次本原多项式，并保证生成的 4 个m序列的周期 $2^{n_1}-1,2^{n_2}-1,2^{n_3}-1,2^{n_4}-1$ 均为梅森素数。右半部分FCSR1～FCSR4 的q_1，q_2，q_3和q_4均取强 2-素数。

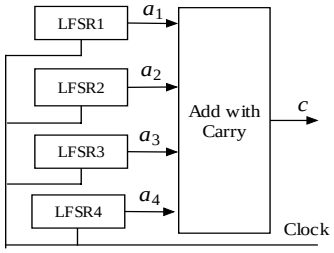

图 3 密钥流生成器的左半部—LFSR_C

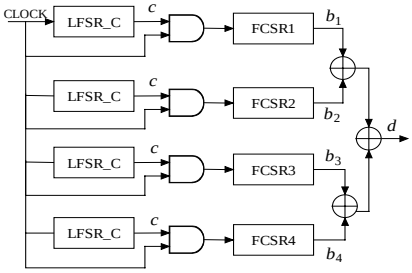

图 4 密钥流生成器右半部分的等价表示

2.2 对 LFSR_C 的分析

由于m序列也是终归二元序列，根据定理 3 可知，一个已知的m序列也可由FCSR来产生。因此，可求出m序列对应的 2-adic复杂度。以下T_i、q_i和 $\varphi_2(a_i)$ 分别为第i个LFSR产生序列的周期、等效的连接数和 2-adic复杂度。

推论 1 设$a_1,a_2,\ldots,a_n$是n个二元周期序列，c是它们的进位加输出序列，则c的 2-adic复杂度 $\varphi_2(c)$ 满足以下关系：

$$\varphi_2(c)\le\sum_{i=1}^{n}\varphi_2(a_i)+\log_2 n$$

证明：假设二元周期序列序列a_i对应的有理数$\alpha_i=p_i/q_i$，q_i为该序列的连接数。

则n个a_i序列带进位加之后的序列c对应的有理数为

$$\sum_{i=1}^{n}\alpha_i=\sum_{i=1}^{n}\frac{p_i}{q_i}=\frac{\sum_{i=1}^{n}(p_i\prod_{j=1,j\ne i}^{n}q_i)}{q_1q_2\ldots q_n}$$

因此根据定义 1，

$$\varphi_2(c)=\log_2[\Phi(\sum_{i=1}^{n}p_i\prod_{j=1,j\ne i}^{n}q_i,q_1q_2,\ldots,q_n)]\le\log_2[n\prod_{i=1}^{n}\Phi(p_i,q_i)]$$

$$=\sum_{i=1}^{n}\varphi_2(a_i)+\log_2 n$$

推论 2 设 a 为周期为 $T_a=2^N-1$ 的序列，则当 $2^{T_a}-1$ 为梅森素数时，序列对应的 FCSR 连接数 $q=2^{T_a}-1$。

证明：设连接数为 q 的 FCSR 产生序列 a。根据定理 2 可知，a 的周期 $T_a=ord_q(2)$，即：$2^{T_a}=1 \bmod q$，q 是 $2^{T_a}-1$ 的因子。由于 $2^{T_a}-1$ 也是素数，因此只有 $q=2^{T_a}-1$。

推论 3 FCSR 产生序列的周期 $T=Euler(q)/k$，q为 FCSR 的连接数，$Euler(q)$ 为 q 的欧拉函数，$k\ge 2$ 为正整数。仅当 2 为模 q 的本原根时，周期达到最大值 $T=Euler(q)$。

证明：根据欧拉定理可知，当 q 与 2 互素时，$2^{Euler(q)}=1 \bmod q$；而由定理 2 可知 T 为 2 模 q 的阶，即 $2^T=1 \bmod q$。因此 $Euler(q)=kT$。仅当 2 为模 q 的本原

根时，周期达到最大值 $T = Euler(q)$。

定理 4 q不为 2 和 4，也不具有p^e或 $2p^e$的形式，（p为素数，e是正整数），则不存在模q的本原根。

性质 1 在目前发现的 41 个梅森素数中，仅当n_i=2,3,5 或 7 时，$T_i = 2^{n_i} - 1$和 $2^{T_i} - 1$均为素数。

由定理 1 和推论 1 可得，图 3 输出的序列 c 的 2-adic 复杂度为

$$\varphi_2(c) = \log_2 q_c \le \sum_{i=1}^{4} \varphi_2(a_i) + \log_2 4 = \log_2 4\prod_{i=1}^{4} q_i$$

因此，序列 c 的连接数 $q_c \le 4\prod_{i=1}^{4} q_i$。

根据定理 4 可知，以上推出的q_c在达到最大值 $4\prod_{i=1}^{4} q_i$ 时不具有模q_c的本原根。

因此对应序列的周期无法达到 $Euler(q_c)$。

根据推论 2 和 3，当 $2^{T_i} - 1$为素数时，LFSR_C 的周期可表示为

$$T(c) = Euler(q_c)/k \le Euler(\prod_{i=1}^{4} q_i)/k \le \prod_{i=1}^{4} (2^{T_i} - 2)/k$$

根据性质 1 可知，当且仅当n_i=2,3,5 或 7 时，$2^{T_i} - 1$均为素数，上式等号成立。由于目前发现的最大的梅森素数相当于T=24036583（n=25 便超过该范围），是否存在更大的n_i，使得 2^{T_i}-1 仍为素数，又转化为找素数的难题了。但从另一个方面考虑，合理选择n_i使得T_i为素数，增大 $2^{T_i} - 1$为素数或包含大的素因子的概率，从而可增大周期T（后面将利用STS软件测试具体的实例，以检验该取值方法的有效性）。

2.3 右半部分钟控序列生成器分析

右半部分可看作是 4 个基本钟控序列生成器的合成，其驱动部分就是 LFSR_C 的输出序列 c，周期为 $T(c)$。

定理 5[7] 如果FCSR的连接数q是 2-素数，则产生序列的线性复杂度小于等于 $(q+1)/2$；如果q=$2p$+1 是强 2-素数，则产生序列的线性复杂度等于p。

根据定理 5 可知，当图 4 中 4 个FCSR的q_i=$2p_i$+1 均为强 2-素数时，各个FCSR单独工作（即不与左边输出的驱动序列c联动）时输出序列fc_i均为l序列，各个fc_i对应的周期$T(fc_i)$=q_i−1 和线性复杂度$L(fc_i)$=p_i+1（i=1,2,3,4）分别达到最大值。同时，根据文献[13]中的结论可知，单个基本钟控序列b_i的周期$T(b_i)$和线性复杂度$L(b_i)$分别为

$$T(b_i) = \frac{T(c)\cdot T(fc_i)}{\gcd(\omega, T(fc_i))} = \frac{T(c)\cdot 2p_i}{\gcd(\omega, 2p_i)}, \quad \omega = \sum_{i=0}^{T(c)-1} a_i$$

$$L(b_i) = T(c)\cdot L(fc_i) = T(c)\cdot(p_i + 1)$$

由于p_i为 2-素数，则 $\gcd(\omega, 2p_i)$ 只能取 1，2 或p_i，因此，$2p_iT(c) \ge T(b_i) \ge 2T(c)$。所以，在硬件开销允许的条件下，适当增大FCSR的连接数，并确保q为强 2-素数，有利于增大单个钟控序列b_i的周期和线性复杂度的上界。

性质 2 设a_1, a_2, a_3, a_4是$GF(2)$上的 4 个序列，则线性复杂度 $L(a_1 \oplus a_2 \oplus a_3 \oplus a_4) \le L(a_1) + L(a_2) + L(a_3) + L(a_4)$，周期 $T(a_1 \oplus a_2 \oplus a_3 \oplus a_4) = T(a_1)\cdot T(a_2)\cdot T(a_3)\cdot T(a_4)$。

根据性质 2 可知，当 q 均为强 2-素数时，图 4 中输出序列 d 的线性复杂度 $L(d)$和周期 $T(d)$的上界分别满足：

$$L(d) \le \sum_{i=1}^{4} L(b_i) = T(c)\cdot(\sum_{i=1}^{4} p_i + 4)$$

$$T(d) \le \prod_{i=1}^{4} T(b_i) \le 16\cdot T(c)^4 \cdot \prod_{i=1}^{4} p_i$$

因此，

$$L(c \oplus d) \le T(c)\cdot(\sum_{i=1}^{4} p_i + 5)$$

$$T(c \oplus d) \le 16\cdot T(c)^5 \cdot \prod_{i=1}^{4} p_i$$

3 密钥流的伪随机性测试

美国国家技术与标准局NIST推出的STS软件包是当前伪随机性测试中最具权威的工具，已用来检验AES候选算法的伪随机特性。本文选用STS提供的 16 种随机性测试方法有代表性的 8 种方法（见表 1）对生成器产生的密钥流进行测试。根据STS的规定，测试的单次评测结果 $P-value \in [0,1]$，若 $P-value \ge 0.01$ 则被检验序列通过该项测试，且P-$value$值越大，表明被测样本的该项伪随机特性越好。否则，样本不能通过测试[12]。

表 1 选用的随机性测试方法

	测试方法	说明
1	The Frequency Test	检验 0，1 出现的次数是否平衡
2	The Runs Test	游程测试
3	The Cumulative Sums (Cusums) Test	测试序列局部的累加和以检验均匀性
4	The Linear Complexity Test	测试序列的线性复杂度(包括复杂度轮廓)特性
5	The Binary Matrix Rank Test	序列中相邻子序列的线性相关性测试
6	Maurer's "Universal Statistical" Test	检验序列是否可作无损压缩并以此测试其随机性
7	The Serial Test	测试序列的 deBruijn 特性
8	The Discrete Fourier Transform Test	测试序列离散傅立叶变换后的峰值以检验其周期性

为证实 2.2 节的推断，为LFSR_C的 4 个LFSR选择以下 2 组参数，并产生 2×10^7bit长的序列$\{a_k\}$进行DFT和线性复杂度测试。其中LFSR的联结多项式均为本原多项式。

$$f_1(x) = x^{13} + x^4 + x^3 + x + 1,\ f_2(x) = x^{17} + x^3 + 1,$$
$$f_3(x) = x^{19} + x^6 + x^5 + x + 1,\ f_4(x) = x^{23} + x^5 + 1 \quad (1)$$

$$f_1(x) = x^{14} + x^7 + 1,\ f_2(x) = x^{18} + x^{12} + x^{11} + x + 1,$$
$$f_3(x) = x^{20} + x^3 + 1,\ f_4(x) = x^{24} + x^4 + x^3 + x + 1 \quad (2)$$

虽然第 1 组参数 LFSR 的级数（13,17,19,23）均小于第 2 组（14,18,20,24），但图 5 和图 6 表明，前者产生序列的周期和线性复杂度特性均优于后者产生的序列。因此，可证明 2.2 节推断的有效性。在该 2 组参数下 LFSR_C 产生的两个序列的其它伪随机特性基本相近，在此不再给出。

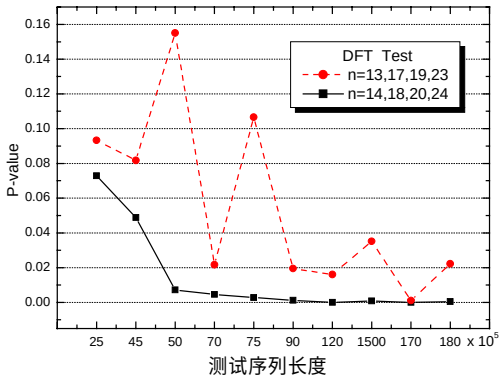

图 5 LFSR_C 在 2 组参数下输出序列的 DFT 测试结果比较

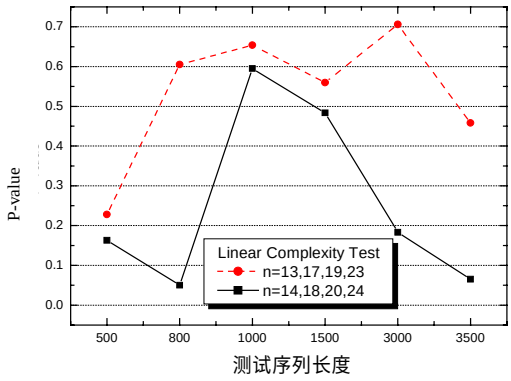

图 6 LFSR_C 在两组参数下输出序列的线性复杂度测试结果比较

4 密钥流生成器的性能分析

选取文献[14]中相同的 FPGA 器件 Xilinx Virtex-Ⅱ-2V250FG256 作为平台，在第 3 节选取的参数条件下，该密钥流生成器在 ModeSim 中的仿真综合结果见表 2。图 7 为该密钥流生成器与 5 种现有的流密码(A5/1,RC4,W7,E0,Helix)在相同平台下的 FPGA 实现结果的吞吐量/slice 比较（具体的各个算法描叙见文献[14]）。可发现该算法在耗费很小资源的前提下，可达到 160.2Mbps 的密钥流吞吐量，具有较高的性能，因此，可在移动终端实施，实现对 4G 移动通信系统中 100Mbps 高速数据的加密。

表 2 LFSR+FCSR 密钥流生成器的 FPGA 硬件实现结果的性能参数

时延	频率	吞吐量	Slice	等效逻辑门数	吞吐量/slice	存储器最大消耗
6.24 ns	160.2 Mbps	160.2 Mbps	87	2 088	1.84	70MB

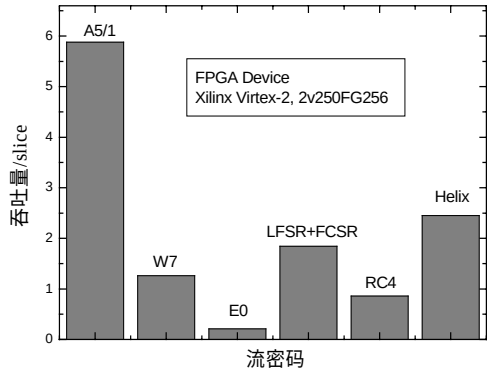

图 7 实现结果的比较

5 结论

本文将Schneier提出的FCSR和LFSR相结合的密钥流生成器分解为左右两个部分来研究，分析了输出序列的周期和线性复杂度特性，给出了理论上界。当LFSR1～LFSR4 的特征多项式分别取n_1，n_2，n_3和n_4次本原多项式，并保证生成的 4 个m序列的周期 $2^{n_1}-1,2^{n_2}-1,2^{n_3}-1,2^{n_4}-1$均为梅森素数，且右半部分FCSR1～FCSR4 的q_1,q_2,q_3和q_4均取强 2-素数时，该生成器输出的密钥流具有较好的伪随机特性。在该参数选择方法下，生成器输出的密钥流通过了NIST STS软件包的 8 项测试。通过与其它 5 种流密码方案的FPGA中实现的比较可发现，该生成器具有较高的性能和效率，能在资源相对紧张的移动终端实施，满足 4G 系统对密钥流产生速度在 100Mbps 以上的要求。本文给出的理论上界是在一定条件（LFSR 的连接多项式均取本原多项式，FCSR 的连接数均为强 2-素数）下给出的，且上界比较宽松，更严密和广泛的理论上界有待进一步的深入探讨。该成器产生的序列是否足够安全以作为密钥流使用，还需要利用各种攻击方法对之进行进一步分析。

参考文献

1 Kalapper A. 2-adic Shift Register[C]//Proc. of Fast Software Encryption Second International Workshop. Springer-verlag. 1994: 174-178.

2 Goresky M, Kalapper A. Feedback Register Based on Ramified Extensions of the 2-adic Number[C]//Proc. of Advances in Cryptology- Eurocrypt'94. 1994, 215-222.

3 Goresky M. Kalapper Large Periods Nearly de Bruijn FCSR Sequence[C]//Proc. of Advances in Cryptology-Eurocrypt'95. 1995, 263-273.

4 Kalapper A, Goresky M. Feedback Shift Registers, 2-adic Span and Combiners with Memory[J]. Journal of Cryptology, 1997, 10(1): 111-147.

5 Goresky M, Kalapper A. Arithmetic Cross-correlation of Feedback with Carry Shift Register Sequences[J]. IEEE Trans. on Info. Theory, 1997, 43(4): 1342-1345.

6 Goresky M, Kalapper A, Washington L. Fourier Transforms and the 2-adic Span of Periodic Binary Sequences[J]. IEEE Trans. on Info. Theory, 2000, 46(2): 687-691.

7 Seo C, Lee S, Sung Y. A Lower Bound on the Linear Span of FCSR[J]. IEEE Trans. on Info. Theory, 1997, 43(4): 691-693.

8 Qi Wenfeng, Xu Hong. Partial Period Distribution of FCSR Sequences[J]. IEEE Trans. on Info. Theory, 2003, 49(3): 761-765.

9 Schneier B. Applied Cryptography[M]. Prentice Hall, 1998.

10 Richter G. Design, Analysis, Implementation and Comparison of Stream Cipher Algorithms[D]. Department of Computer, Electrical and Electronic Engineering, University of Pretoria, 2002.

11 Shyrochin V P, VasyItsov I V, Karpinskij B Z. Investigations of the Basic Component of FCSR–generator[C]//Proc. of IEEE International Workshop on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Application. 2003-09.

12 Rukhin A, Soto J, Nechvatal J, et al. A Statistical Test Suite for Random and Pseudorandom Number Generator for Cryptographic Applications[Z]. 2004-05-01. NIST Special Publication 800-22, http://csrc.nist. gov/rng/SP800-22b.pdf.

13 杨　波. 现代密码学[M]. 北京：清华大学出版社, 2003: 27-28.

14 Galanis M D, Kitsos P, Kostopoulos G. Comparison of the Hardware Architectures and FPGA Implementations of Stream Ciphers[C]//Proc. of IEEE International Conference on Galanis, Electronics, Circuits and Systems. 2004-12.