LFCSR:基于 FCSR 的新密码学部件

董丽华[1],曾 勇[2],王春红[3],胡予濮[1]
(1. 西安电子科技大学 ISN 国家重点实验室,陕西西安 710071;2. 西安电子科技大学网络与信息安全学院,陕西西安 710071;
3. 中船重工集团第七二二研究所,湖北武汉 430205)

摘 要: 为了有效抵抗 M Hell 与 T Johansson 对基于带进位反馈移位寄存器(Feedback with carry shift Register,FCSR)的流密码的实时攻击,本文给出了一个使用密码学部件(FCSR)的新方法. 在该方法中,只需要将 FCSR 的有效进位单元的内容与线性反馈移位寄存器(Linear Fedback Shift Regsiters,LFSR)的对应比特进行异或,随后即可执行原 FCSR 的运算. 以新方法得到的组合部件的状态转移函数依然是二次的,因而对代数攻击和相关攻击有天然的免疫性,尤其重要的是理论分析与实验结果表明新的组合部件的所有进位单元的输出序列是独立的,无偏的,具有良好的统计特性,因而可以有效的阻止 M Hell 与 T Johansson 对基于 FCSR 的流密码的实时攻击以及其它类似攻击.

关键词: 密码学; 流密码; 带进位反馈移位寄存器; 滤波生成器
中图分类号: TN918 **文献标识码:** A **文章编号:** 0372-2112 (2018)08-1924-07
电子学报 URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2018.08.017

LFCSR:A Novel FCSR-Based Cryptographic Primitive

DONG Li-hua[1],ZENG Yong[2],WANG Chun-hong[3],HU Yu-pu[1]
(1. *National ISN Key Laboratory,Xidian University,Xi'an,Shaanxi* 710071,*China*;
2. *School of Cyber Engineering,Xidian University,Xi'an,Shaanxi* 710071,*China*;
3. *No.* 722 *Research Institute of CSIC,Wuhan,Hubei* 430205,*China*)

Abstract: We propose a novel FCSR-based cryptographic primitive for efficiently resisting M. Hell and T. Johansson's real-time crypt-analysis on FCSR-based stream ciphers. With this proposed primitive in the application, we simply need to xor the bit in the carry unit with the corresponding state bit in a LFSR. Then just perform the original operation of the FCSR. Analysis and experimental results show that: the transition function of the proposed primitive is still quadratic, thus it provides an intrinsic resistance to algebraic attacks and correlation attacks; and it is very important that all the sequences generated by the carry cells are independent, unbiased and have good statistical properties, thus can prevent the attack of Hell and Johansson and other similar attacks on FCSR-based stream ciphers.

Key words: cryptography; stream cipher; Feedback with Carry Shift Register(FCSR); filtered generator

1 引言

基于线性反馈移位寄存器(Linear Feedback Shift Registers,LFSR)的流密码由于其具有运行速度快,硬件实现规模小等特点可以被有效地应用于信息传输系统的加密保护,因而一直备受生产企业和研究者的关注. 但是随着对 LFSR 的性质研究的不断深入以及密码分析方法的逐渐成熟,对这一类型的流密码先后出现了包括相关攻击,代数攻击,区分攻击,猜测确定性攻击在内的若干分析方法[1~7]. 这些攻击方法在理论上成为可能的主要原因在于利用了 LFSR 内部状态线性更新的弱点.

为了征集到安全有效的流密码方案,欧盟在信息社会技术规划中支持了一项大密码计划 NESSIE (New European Schemes for Signatures, Integrity and Encryption)[8],在该研究计划中共征集到六个流密码设计方案,然而这六个流密码设计方案均未能通过 NESSIE 公开的安全性测试.

为了弥补这一缺憾,ECRYPT 开展了一项新的流密码研究计划 eSTREAM[9],该计划经过 4 年的努力,征集了 34 个流密码设计方案,3 轮的筛选最终选定了 7 个流密码设计方案. 在上述流密码的标准化过程中,为了弥补 LFSR 的内部状态线性更新的弱点,涌现了大量的非线性设计部件,这些新兴非线性设计部件具有很大的应用潜力及发展前景,科学工作者在理论和

收稿日期:2016-11-07;修回日期:2018-06-07;责任编辑:马兰英
基金项目:国家重点研发计划(No. 2016YFB0800601;111 基地项目(No. B16037)

实验上都已做了大量的工作[10~15]. 其中带进位反馈移位寄存器(Feedback with Carry Shift Register,FCSR)是美国学者 A Klapper 和 M Goreskey 提出的一种新型的流密码设计部件[16],有着与 LFSR 几乎完全相似的良好伪随机特性,同时因其结构简洁且状态转移函数是非线性性的而倍受关注. F Arnault 与 T Berger 在 FCSR 的基础上添加线性滤波函数得到了新型流密码生成器 F-FCSR[17],由于其相继通过了 NIST 的统计测试,以及 eSTREAM 的有效性测试,而倍受关注. 然而遗憾的是,由于其单次输出暴露了过多的信息,Martin Hell 与 Thomas Johansson 在亚密会上宣告可以实时攻破 F-FCSR[18]. 作为对 M Hell 与 T Johansson 攻击的理论支撑,Haixin Song 等人更是从理论上证明了 F-FCSR 的进位单元输出的概率分布是不均匀的[19]. 为了避免 M Hell 与 T Johansson 的实时攻击以及其它类似攻击,国内外密码学者先后提出了几种新的 FCSR 的使用方法. 例如环 FCSRs[20],向量 FCSRs[21,22] 以及 X-FCSR[23],但这些方法或者比较复杂,实现不易,或者安全性受到威胁[24,25]. 但由于 FCSR 所具有的优秀的伪随机性及天然的非线性,依然得到了广泛的关注[26~28],这些研究主要对 FCSR 的矩阵表示等理论有积极的参考价值.

为了丰富 FCSR 在流密码学中的应用方法,同时有效的抵抗 M Hell 与 T Johansson 的实时攻击以及其它类似攻击,本文,给出了 FCSR 的一种新的使用方法. 在该方法中,只需要添加一个 LFSR 到 FCSR 中. 理论分析表明,新结构的进位单元的输出概率分布是均匀的,因而可以有效的抵抗 M Hell 与 T Johansson 的实时攻击以及其它类似攻击.

2　FCSR 以及相关工作背景

2.1　FCSR

FCSR 的伽罗华结构的示例图[22]如图 1 所示,在该结构中,有两个寄存器,一个主寄存器 M 和一个进位寄存器 C.

假设 FCSR 的联接整数 $q=1-2d=-1+q_1 2+q_2 2^2+\cdots+q_r 2^r$,其中 d 的二进制展开式为 $d=\sum_{i=0}^{r-1} d_i 2^i$,则[22]:

(1)主寄存器 M 具有 r 个二进制存储单元,在时刻 t,主寄存器的状态可以表示为$(m_0(t),\cdots,m_{r-1}(t))$,其中 r 是 d 的比特长度. (2)进位寄存器 C 也具有 r 个二进制存储单元,在时刻 t,进位寄存器的状态可以表示为$(c_0(t),\cdots,c_{r-1}(t))$,其中 $c_i(t)=0$ 的充要条件为 $d_i=0$,这里 $0\le i\le r-1$. 记 $I_d=\{i\mid 0\le i\le r-2$ 且 $d_i=1\}$,称位于集合 I_d 中的存储单元为进位寄存器的有效进位单元. 进位单元的数目加 1 即为 d 的汉明重量.

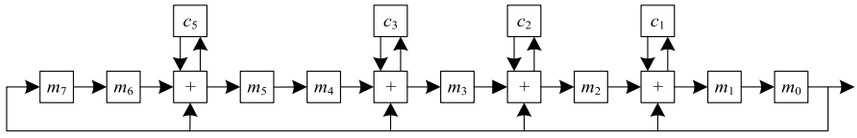

图1　FCSR的伽罗华结构其中q为349，故d=175，r=8

记 FCSR 在时刻 t 的状态为$(m(t),c(t))$,其中 $m(t)=\sum_{i=0}^{r-1} m_i(t)2^i$ 且 $c(t)=\sum_{i=0}^{r-1} c_i(t)2^i$,则 FCSR 在时刻 $t+1$ 的状态$(m(t+1),c(t+1))$更新过程如下[22]:

(1)若 $0\le i\le r-2$

且 $i\notin I_d$,则 $m_i(t+1)=m_{i+1}(t)$

且 $i\in I_d$,则:

$$m_i(t+1)=m_{i+1}(t)\oplus c_i(t)\oplus m_0(t)$$

$$c_i(t+1)=m_{i+1}(t)c_i(t)\oplus c_i(t)m_0(t)\oplus m_0(t)m_{i+1}(t)$$

$$m_{i-1}(t+1)+2c_i(t+1)=m_i(t)\oplus c_i(t)\oplus q_i m_0(t)$$

其中 $1\le i\le r-1$

(2)若 $i=r-1$,则 $m_{r-1}(t+1)=m_0(t)$

注意:状态转移函数是二次的.

2.2　M Hell 与 T Johansson 的实时密码学攻击

M Hell 与 T Johansson 的实时密码学攻击[18]的主要思想如下:

在如图 1 所示的 FCSR 的伽罗华结构中,每一次一旦反馈比特为 0,进位寄存器单元中为 0 的比特依然为 0,而为 1 的单元有 50% 的机会变为 0. 因而 t 时刻值为 0 的反馈比特会使得 $t+1$ 时刻的进位向量的汉明重量仅为 t 时刻汉明重量的一半. 那么如果主寄存器对最后一个进位加法的输入是全 1 序列,同时进位比特的初始值为 1,那么就会出现全 0 的反馈序列. 详细分析过程请参考文献[18]. 记 $c(t)=c(t+1)=\cdots=c(t+19)=(0,0,\cdots,0,1,0)$为事件 Ezero. 当事件 Ezero 发生时,反馈中会出现 20 个连续的 0,在 20 个连续时刻内,进位会保持常数. 然后为了使进位寄存器的重量变为 1,反馈中需要大概$\log_2 82$ 个 0,为了使进位寄存器保持 20 个时刻不变,反馈中需要有 19 个 0. 假设反馈比特是均匀分布的,则事件 Ezero 发生的概率近似为 2^{-26}.

假设事件 Ezero 出现,剩余的工作则是由密钥流 z

$(t)=z(t+1)=\cdots=z(t+19)$恢复主寄存器的内容. 时刻$t$,主寄存器和进位寄存器的内容为:

$$(M,C)(t)=(xx\cdots xx011\cdots1100,000\cdots0010)$$

这里"x"代表不确定元素,串"11…11"的长度为16. 随后状态更新如下$(M,C)(t+1)=(xx\cdots xx011\cdots1100,000\cdots0010)$这里串"11…11"的长度为15. $(M,C)(t+2)=(xx\cdots xx011\cdots1100,000\cdots0010)$这里串"11…11"的长度为14.

…….

$$(M,C)(t+15)=(xxxxxxxx\cdots xx0100,000\cdots0010)$$
$$(M,C)(t+16)=(xxxxxxxx\cdots xxx000,000\cdots0010)$$
$$(M,C)(t+17)=(xxxxxxxx\cdots xxxx10,000\cdots0010)$$
$$(M,C)(t,18)=(xxxxxxxx\cdots xxxxx1,000\cdots0010)$$
$$(M,C)(t+19)=(xxxxxxxx\cdots xxxxxx,??????????)$$

如此得到一个含160个未知数160个方程的方程组,其中"?"代表不需要知道的比特. 以高斯消元法经过160^3次运算可以求解该方程组. 详细分析过程请参考文献[18].

2.3 F-FCSR-H 的进位单元输出的概率分布

M Hell 与 T Johansson 于2008年的亚密会上仅通过实验给出了成功攻击 F-FCSR-H 的概率. 2012年,Haixin Song 等人从理论上证明了 F-FCSR-H 的进位单元的输出概率分布是不均匀的,从而为 M Hell 与 T Johansson 的实时密码学攻击提供了理论支撑. 接下来,我们将该分析过程的主要结果描述如下.

结论1 假设 F-FCSR-H 的各主寄存器单元的输出是独立均匀分布的二元随机变量,且主寄存器单元的输出与进位单元的输出相互独立,则n个进位单元的输出在相同时刻只有一个单元为1的概率为$\frac{1}{n(n+1)}$,其中$1\leq n\leq 82$.

结论2 假设 F-FCSR 的各主寄存器单元的输出是独立均匀分布的二元随机变量,且主寄存器单元的输出与进位单元的输出独立,同时记$Prob_1(n,l)$为l个连续时刻内n个进位单元的输出$(c_{j_{i_1}},c_{j_{i_2}},\cdots,c_{j_{i_n}})$取值$(0,\cdots,0,1)$的概率,其中$1\leq n\leq 82$,$1\leq j_{i_1}<j_{i_2}<\cdots<j_{i_n}\leq 160$,$1\leq i_1<i_2<\cdots<i_{n-1}<i_n\leq 82$,则:

$$\mathrm{Prob}_1(n,l)=\frac{1}{n(n+1)}\left(\left(\frac{1}{2}\right)^{2l-2}+\left(\frac{2^{n-1}+1}{2^n}\right)^{l-1}-\left(\frac{1}{2}\right)^{l-1}\right)$$

这两个结论表明 F-FCSR 的进位单元的输出序列不服从均匀分布,从而为 M Hell 与 T Johansson 的实时密码学攻击提供了有力的理论支撑.

3 LFCSR

3.1 LFCSR 结构框架

LFCSR 的伽罗华结构的示例图如图2所示,一个LFCSR仅由一个FCSR和一个LFSR组成,其中FCSR的有效进位单元与LFSR的对应寄存器单元逐比特异或,LFSR的链接多项式为$l(x)=1+a_1x+a_2x^2+\cdots+a_rx^r$. LFCSR在时刻$t+1$的状态$(m(t+1),c(t+1),l(t+1))$更新过程如下:

(1)$0\leq i\leq r-2$

$$l_i(t+1)=l_{i+1}(t)$$

若$i\notin I_d$,则$m_i(t+1)=m_{i+1}(t)$

若$i\in I_d$,则:

$$m_i(t+1)=m_{i+1}(t)\oplus c_i(t)\oplus m_0(t)$$
$$c_i(t+1)=m_{i+1}(t)c_i(t)\oplus c_i(t)m_0(t)\oplus m_0(t)m_{i+1}(t)\oplus l_i(t)$$

(2)$i=r-1$,

$$l_{r-1}(t+1)=a_1l_{r-1}(t)\oplus a_2l_{r-2}(t)\oplus\cdots\oplus a_rl_0(t)$$
$$m_{r-1}(t+1)=m_0(t)$$

注意:新结构的状态转移函数依然是二次的,因而可以有效抵抗代数攻击和相关攻击.

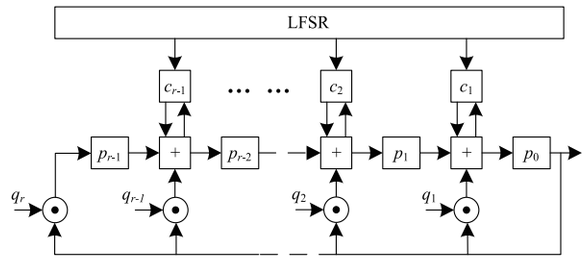

图2 基于FCSR的新型结构

3.2 LFCSR 的进位单元输出的概率分布

本节讨论LFCSR的进位单元输出的概率分布,包括l个连续时刻内,LFCSR的单个进位单元输出的概率分布;在同一时刻n个进位单元输出的概率分布以及l个连续时刻n个进位单元输出的概率分布. 以下使用与文献[19]中类似的假设,LFCSR的各主寄存器单元的输出都是定义在相同概率空间上的独立均匀分布的随机变量,且LFCSR的各主寄存器单元的输出与各进位单元输出独立. 研究结果表明LFCSR的各进位单元的输出概率分布是均匀的,因而可以有效的阻止 Hell 与 Johansson 的攻击以及其它对基于FCSR的流密码的类似攻击.

3.2.1 LFCSR 的单个进位单元输出的概率分布

定理1 LFCSR的有效进位单元输出序列$c_{j_k}(0)$,$c_{j_k}(1)$,…构成马尔科夫链,且$Prob(c_{j_k}(t+1)=a\,|\,c_{j_k}(t)=b)=\frac{1}{2}$,其中$a,b\in\{0,1\}$.

证明 由LFCSR的状态更新函数,得到:

$$c_{j_k}(t+1)=m_0(t)c_{j_k}(t)\oplus m_{j_k}(t)c_{j_k}(t)\oplus m_0(t)m_{j_k}(t)\oplus l_{j_k}(t)$$

即c_{j_k}在时刻$t+1$的状态只与m_0,m_{j_k},c_{j_k}以及l_{j_k}在时刻t的状态有关,而m_0,m_{j_k},l_{j_k}都与c_{j_k}独立,因而序列

$c_{j_k}(0), c_{j_k}(1), \cdots$构成马尔科夫链. 同时,

若 $c_{j_k}(t)=b=0$,则 $c_{j_k}(t+1)=m_0(t)m_{j_k}(t)\oplus l_{j_k}(t)$,因而

$$\text{Prob}(c_{j_k}(t+1)=a \mid c_{j_k}(t)=b)=\frac{1}{2}$$

若 $c_{j_k}(t)=b=1$,则 $c_{j_k}(t+1)=m_0(t)\oplus m_{j_k}(t)\oplus m_0(t)m_{j_k}(t)\oplus l_{j_k}(t)$,因而

$$\text{Prob}(c_{j_k}(t+1)=a \mid c_{j_k}(t)=b)=\frac{1}{2}.$$

因此 $\text{Prob}(c_{j_k}(t+1)=a \mid c_{j_k}(t)=b)=\frac{1}{2}$,其中 $a,b\in\{0,1\}$.

定理 2　对于 l 个连续时刻,有 $\text{Prob}(c_{j_k}(t)=a_0, c_{j_k}(t+1)=a_1,\cdots,c_{j_k}(t+l-1)=a_{l-1})=\frac{1}{2^l}$,其中 $a_i\in\{0,1\}, 0\le i\le l-1$.

证明　若 $l=1$,则 $\text{Prob}(c_{j_k}(t)=a_0)=\frac{1}{2}$,结论成立.

假设对于 $l-1$ 个连续时刻,定理成立,则:

$$\begin{aligned}
&\text{Prob}(c_{j_k}(t)=a_0, c_{j_k}(t+1)=a_1,\cdots,c_{j_k}(t+l-1)=a_{l-1})\\
&=\text{Prob}(c_{j_k}(t+l-1)=a_{l-1} \mid c_{j_k}(t)\\
&=a_0, c_{j_k}(t+1)=a_1,\cdots,c_{j_k}(t+l-2)=a_{l-2})\\
&\quad\cdot\text{Prob}(c_{j_k}(t)=a_0, c_{j_k}(t+1)=a_1,\cdots,\\
&\quad c_{j_k}(t+l-2)=a_{l-2})=\text{Prob}(c_{j_k}(t+l-1)\\
&=a_{l-1} \mid c_{j_k}(t+l-2)=a_{l-2})\cdot\text{Prob}(c_{j_k}(t)\\
&=a_0, c_{j_k}(t+1)=a_1,\cdots,c_{j_k}(t+l-2)=a_{l-2})
\end{aligned}$$

由定理 1 以及归纳假设知:

$$\begin{aligned}
&\text{Prob}(c_{j_k}(t)=a_0, c_{j_k}(t+1)=a_1,\cdots,c_{j_k}(t+l-1)=a_{l-1})\\
&=\frac{1}{2}\cdot\frac{1}{2^{l-1}}=\frac{1}{2^l}
\end{aligned}$$　　结论成立.

对于 l 个连续时刻,只有满足独立均匀分布的二元随机变量序列取任意值的概率方为$\frac{1}{2^l}$,因而定理 2 的结论表明 LFCSR 的单个进位单元输出序列是满足独立均匀分布的二元随机序列.

3.2.2　在同一时刻 n 个进位单元输出的联合概率分布

定理 3　$\text{Prob}(c_{j_1}(t)=a_0, c_{j_2}(t)=a_1,\cdots,c_{j_n}(t)=a_{n-1})=\frac{1}{2^n}$,其中 $a_i\in\{0,1\}, 0\le i\le n-1$.

证明　若 $n=1$,则 $\text{Prob}(c_{j_1}(t)=a_0)=\frac{1}{2}$,结论成立.

若 $n>1$,假设对于 $s<n$ 的所有 s 有定理成立,其中 s 是进位单元的数目,则:

$$\begin{aligned}
&\text{Prob}(c_{j_1}(t+1)=a_0, c_{j_2}(t+1)=a_1,\cdots,c_{j_n}(t+1)=a_{n-1})\\
&=\text{Prob}\left(\begin{matrix}m_0(t)c_{j_1}(t)\oplus m_{j_1}(t)c_{j_1}(t)\oplus m_0(t)m_{j_1}(t)\oplus l_{j_1}(t)=a_0,\cdots,\\ m_0(t)c_{j_n}(t)\oplus m_{j_n}(t)c_{j_n}(t)\oplus m_0(t)m_{j_n}(t)\oplus l_{j_n}(t)=a_{n-1}\end{matrix}\right)\\
&=\text{Prob}(m_{j_1}(t)c_{j_1}(t)\oplus l_{j_1}(t)=a_0,\cdots,m_{j_n}(t)c_{j_n}(t)\oplus l_{j_n}(t)\\
&=a_{n-1}, m_0(t)=0)\\
&+\text{Prob}\left(\begin{matrix}c_{j_1}(t)\oplus m_{j_1}(t)c_{j_1}(t)\oplus m_{j_1}(t)\oplus l_{j_1}(t)=a_0,\cdots,\\ c_{j_n}(t)\oplus m_{j_n}(t)c_{j_n}(t)\oplus m_{j_n}(t)\oplus l_{j_n}(t)=a_{n-1}, m_0(t)=1\end{matrix}\right)
\end{aligned}$$

这里

$$\begin{aligned}
&\text{Prob}(m_{j_1}(t)c_{j_1}(t)\oplus l_{j_1}(t)=a_0,\cdots,m_{j_n}(t)c_{j_n}(t)\oplus l_{j_n}(t)=a_{n-1}, m_0(t)=0)\\
&=\text{Prob}\left(\begin{matrix}m_{j_1}(t)c_{j_1}(t)\oplus l_{j_1}(t)=a_0,\cdots,m_{j_n}(t)c_{j_n}(t)\oplus l_{j_n}(t)=a_{n-1},\\ m_0(t)=0, m_{j_1}(t)=0,\cdots,m_{j_n}(t)=0\end{matrix}\right)\\
&+\cdots+\text{Prob}\left(\begin{matrix}m_{j_1}(t)c_{j_1}(t)\oplus l_{j_1}(t)=a_0,\cdots,m_{j_n}(t)c_{j_n}(t)\oplus l_{j_n}(t)=a_{n-1},\\ m_0(t)=0, m_{j_1}(t)=1,\cdots,m_{j_n}(t)=1\end{matrix}\right)\\
&=\text{Prob}(l_{j_1}(t)=a_0,\cdots,l_{j_n}(t)=a_{n-1}, m_0(t)=0,\\
&m_{j_1}(t)=0,\cdots,m_{j_n}(t)=0)+\cdots+\text{Prob}(c_{j_1}(t)\oplus l_{j_1}(t)=a_0,\cdots,\\
&c_{j_n}(t)\oplus l_{j_n}(t)=a_{n-1}, m_0(t)=0, m_{j_1}(t)=1,\cdots,m_{j_n}(t)=1)\\
&=\frac{1}{2^{n+1}}(2^{-n}C_n^0+2^{-1}C_n^1 2^{-n+1}+2^{-2}C_n^2 2^{-n+2}+\cdots+2^{-n}C_n^n)=\frac{1}{2^{n+1}}
\end{aligned}$$

且

$$\begin{aligned}
&\text{Prob}\left(\begin{matrix}c_{j_1}(t)\oplus m_{j_1}(t)c_{j_1}(t)\oplus m_{j_1}(t)\oplus l_{j_1}(t)=a_0,\cdots,\\ c_{j_n}(t)\oplus m_{j_n}(t)c_{j_n}(t)\oplus m_{j_n}(t)\oplus l_{j_n}(t)=a_{n-1}, m_0(t)=1\end{matrix}\right)\\
&=\text{Prob}\left(\begin{matrix}c_{j_1}(t)\oplus m_{j_1}(t)c_{j_1}(t)\oplus m_{j_1}(t)\oplus l_{j_1}(t)=a_0,\cdots,\\ c_{j_n}(t)\oplus m_{j_n}(t)c_{j_n}(t)\oplus m_{j_n}(t)\oplus l_{j_n}(t)=a_{n-1},\\ m_0(t)=1, m_{j_1}(t)=0,\cdots,m_{j_n}(t)=0\end{matrix}\right)+\cdots\\
&+\text{Prob}\left(\begin{matrix}c_{j_1}(t)\oplus m_{j_1}(t)c_{j_1}(t)\oplus m_{j_1}(t)\oplus l_{j_1}(t)=a_0,\cdots,\\ c_{j_n}(t)\oplus m_{j_n}(t)c_{j_n}(t)\oplus m_{j_n}(t)\oplus l_{j_n}(t)=a_{n-1},\\ m_0(t)=1, m_{j_1}(t)=1,\cdots,m_{j_n}(t)=1\end{matrix}\right)\\
&=\text{Prob}\left(\begin{matrix}c_{j_1}(t)\oplus l_{j_1}(t)=a_0,\cdots,c_{j_n}(t)\oplus l_{j_n}(t)=a_{n-1},\\ m_0(t)=1, m_{j_1}(t)=0,\cdots,m_{j_n}(t)=0\end{matrix}\right)+\cdots\\
&+\text{Prob}(l_{j_1}(t)=a_0\oplus 1,\cdots,l_{j_n}(t)=a_{n-1}\oplus 1, m_0(t)=1,\\
&m_{j_1}(t)=1,\cdots,m_{j_n}(t)=1)=\frac{1}{2^{n+1}}(2^{-n}C_n^0+2^{-1}C_n^1 2^{-n+1}+2^{-2}\\
&\cdot C_n^2 2^{-n+2}+\cdots+2^{-n}C_n^n)=\frac{1}{2^{n+1}}
\end{aligned}$$

因而有 $\text{Prob}(c_{j_1}(t)=a_0, c_{j_2}(t)=a_1,\cdots,c_{j_n}(t)=a_{n-1})=\frac{1}{2^n}$.　　结论成立.

只有 n 个独立均匀分布的随机变量在同一时刻取任意值的概率方为$\frac{1}{2^n}$,因此,定理 3 表明在同一时刻 LFCSR 的 n 个进位单元输出的概率分布是均匀的.

3.2.3 l 个连续时刻 n 个进位单元输出的联合概率分布

定理 4

$\mathrm{Prob}(c_{j_1}(t+1)=a_{1,0},c_{j_2}(t+1)=a_{1,1},\cdots,c_{j_n}(t+1)=a_{1,n-1}|$
$c_{j_1}(t)=a_{0,0},c_{j_2}(t)=a_{0,1},\cdots,c_{j_n}(t)=a_{0,n-1}=\dfrac{1}{2^n}$，其中 $a_{i,j}\in\{0,1\}$，$i=0$ 或者 $1,0\leqslant j\leqslant n-1$.

证明

$$\mathrm{Prob}\left(\begin{array}{l}c_{j_1}(t+1)=a_{1,0},c_{j_2}(t+1)=a_{1,1},\cdots,c_{j_n}(t+1)=a_{1,n-1}|\\ c_{j_1}(t)=a_{0,0},c_{j_2}(t)=a_{0,1},\cdots,c_{j_n}(t)=a_{0,n-1}\end{array}\right)$$
$$=\mathrm{Prob}\left(\begin{array}{l}m_0(t)=0,m_0(t)c_{j_1}(t)\oplus m_{j_1}(t)c_{j_1}(t)\oplus m_0(t)m_{j_1}(t)\oplus l_{j_1}(t)\\ =a_{1,0},\cdots,m_0(t)c_{j_n}(t)\oplus m_{j_n}(t)c_{j_n}(t)\oplus m_0(t)m_{j_n}(t)\oplus l_{j_n}(t)\\ =a_{1,n-1}|,c_{j_1}(t)=a_{0,0},c_{j_2}(t)=a_{0,1},\cdots,c_{j_n}(t)=a_{0,n-1}\end{array}\right)$$
$$+\mathrm{Prob}\left(\begin{array}{l}m_0(t)=1,m_0(t)c_{j_1}(t)\oplus m_{j_1}(t)c_{j_1}(t)\oplus m_0(t)m_{j_1}(t)\oplus l_{j_1}(t)\\ =a_{1,0},\cdots,m_0(t)c_{j_n}(t)\oplus m_{j_n}(t)c_{j_n}(t)\oplus m_0(t)m_{j_n}(t)\oplus l_{j_n}(t)\\ =a_{1,n-1}|,c_{j_1}(t)=a_{0,0},c_{j_2}(t)=a_{0,1},\cdots,c_{j_n}(t)=a_{0,n-1}\end{array}\right)$$
$$=\mathrm{Prob}(m_0(t)=0)\cdot\mathrm{Prob}\left(\begin{array}{l}m_{j_1}(t)c_{j_1}(t)\oplus l_{j_1}(t)=a_{1,0},\cdots,m_{j_n}(t)c_{j_n}(t)\oplus l_{j_n}(t)=a_{1,n-1}\\ |m_0(t)=0,c_{j_1}(t)=a_{0,0},c_{j_2}(t)=a_{0,1},\cdots,c_{j_n}(t)=a_{0,n-1}\end{array}\right)$$
$$+\mathrm{Prob}(m_0(t)=1)\cdot\mathrm{Prob}\left(\begin{array}{l}c_{j_1}(t)\oplus m_{j_1}(t)c_{j_1}(t)\oplus m_{j_1}(t)\oplus l_{j_1}(t)=a_{1,0},\\ \cdots,c_{j_n}(t)\oplus m_{j_n}(t)c_{j_n}(t)\oplus m_{j_n}(t)\oplus l_{j_n}(t)=a_{1,n-1},\\ |m_0(t)=1,c_{j_1}(t)=a_{0,0},c_{j_2}(t)=a_{0,1},\cdots,c_{j_n}(t)=a_{0,n-1}\end{array}\right)$$
$$=\mathrm{Prob}(m_0(t)=0)\cdot\mathrm{Prob}\left(\begin{array}{l}m_{j_1}(t)a_{0,0}\oplus l_{j_1}(t)=a_{1,0}|m_0(t)=0,\\ c_{j_1}(t)=a_{0,0},c_{j_2}(t)=a_{0,1},\cdots,c_{j_n}(t)=a_{0,n-1}\end{array}\right)$$
$$\cdot\mathrm{Prob}\left(\begin{array}{l}m_{j_2}(t)a_{0,1}\oplus l_{j_2}(t)=a_{1,1}|m_0(t)=0,\\ c_{j_1}(t)=a_{0,0},c_{j_2}(t)=a_{0,1},\cdots,c_{j_n}(t)=a_{0,n-1}\end{array}\right)$$
$$\cdot\cdots\cdot\mathrm{Prob}\left(\begin{array}{l}m_{j_n}(t)a_{0,n-1}\oplus l_{j_n}(t)=a_{1,n-1}|m_0(t)=0,\\ c_{j_1}(t)=a_{0,0},c_{j_2}(t)=a_{0,1},\cdots,c_{j_n}(t)=a_{0,n-1}\end{array}\right)$$
$$+\mathrm{Prob}(m_0(t)=1)\cdot\mathrm{Prob}\left(\begin{array}{l}a_{0,0}\oplus m_{j_1}(t)a_{0,0}\oplus m_{j_1}(t)\oplus l_{j_1}(t)=a_{1,0},\\ |m_0(t)=1,c_{j_1}(t)=a_{0,0},c_{j_2}(t)=a_{0,1},\cdots,c_{j_n}(t)=a_{0,n-1}\end{array}\right)$$
$$\cdot\mathrm{Prob}\left(\begin{array}{l}a_{0,1}\oplus m_{j_2}(t)a_{0,1}\oplus m_{j_2}(t)\oplus l_{j_2}(t)=a_{1,1}\\ |m_0(t)=1,c_{j_1}(t)=a_{0,0},c_{j_2}(t)=a_{0,1},\cdots,c_{j_n}(t)=a_{0,n-1}\end{array}\right)$$
$$\cdot\cdots\cdot\mathrm{Prob}\left(\begin{array}{l}a_{0,n-1}\oplus m_{j_n}(t)a_{0,n-1}\oplus m_{j_n}(t)\oplus l_{j_n}(t)=a_{1,n-1},\\ |m_0(t)=1,c_{j_1}(t)=a_{0,0},c_{j_2}(t)=a_{0,1},\cdots,c_{j_n}(t)=a_{0,n-1}\end{array}\right)$$
$$=\frac{1}{2}\cdot\frac{1}{2^n}+\frac{1}{2}\cdot\frac{1}{2^n}=\frac{1}{2^n}.$$ 结论成立.

定理 5 对于两个连续的时刻有：

$\mathrm{Prob}(c_{j_1}(t)=\alpha_{0,0},c_{j_2}(t)=\alpha_{0,1},\cdots,c_{j_n}(t)=\alpha_{0,n-1},$
$c_{j_1}(t+1)=\alpha_{1,0},c_{j_2}(t+1)=\alpha_{1,1},\cdots,c_{j_n}(t+1)=\alpha_{1,n-1}|)$
$=\dfrac{1}{2^{2n}}$，其中 $a_{i,j}\in\{0,1\}$，$i=0$ 或者 $1,0\leqslant j\leqslant n-1$.

证明 由定理 3 和 4，有：

$$\mathrm{Prob}\left(\begin{array}{l}c_{j_1}(t)=a_{0,0},c_{j_2}(t)=a_{0,1},\cdots,c_{j_n}(t)=a_{0,n-1},\\ c_{j_1}(t+1)=a_{1,0},c_{j_2}(t+1)=a_{1,1},\cdots,c_{j_n}(t+1)=a_{1,n-1}\end{array}\right)$$
$$=\mathrm{Prob}(c_{j_1}(t)=a_{0,0},c_{j_2}(t)=a_{0,1},\cdots,c_{j_n}(t)=a_{0,n-1})$$
$$\cdot\mathrm{Prob}\left(\begin{array}{l}c_{j_1}(t+1)=a_{1,0},c_{j_2}(t+1)=a_{1,1},\cdots,c_{j_n}(t+1)=a_{1,n-1}|\\ c_{j_1}(t)=a_{0,0},c_{j_2}(t)=a_{0,1},\cdots,c_{j_n}(t)=a_{0,n-1},\end{array}\right)$$
$$=\frac{1}{2^n}\cdot\frac{1}{2^n}=\frac{1}{2^{2n}}.$$ 结论成立.

一般地，有如下结论：

定理 6 对于 l 个连续的时刻有：

$$\mathrm{Prob}\left(\begin{array}{l}c_{j_1}(t)=a_{0,0},c_{j_2}(t)=a_{0,1},\cdots,c_{j_n}(t)=a_{0,n-1},\\ c_{j_1}(t+1)=a_{1,0},c_{j_2}(t+1)=a_{1,1},\\ \cdots,c_{j_n}(t+1)=a_{1,n-1},c_{j_1}(t+l-1)=a_{l-1,0},\\ c_{j_2}(t+l-1)=a_{l-1,1},\cdots,c_{j_n}(t+l-1)=a_{l-1,n-1}\end{array}\right)$$

其中 $a_{i,j}\in\{0,1\}$，$0\leqslant i\leqslant n-1,0\leqslant j\leqslant n-1$.

证明 若 $l=1$ 或 2，由定理 3 和 5 知道结论成立.

若 $l>2$，假设对于所有满足 $s<l$ 的 s 个连续时刻有结论成立，则

$$\mathrm{Prob}\left(\begin{array}{l}c_{j_1}(t)=a_{0,0},c_{j_2}(t)=a_{0,1},\cdots,c_{j_n}(t)=a_{0,n-1},\\ c_{j_1}(t+1)=a_{1,0},c_{j_2}(t+1)=a_{1,1},\\ \cdots,c_{j_n}(t+1)=a_{1,n-1},c_{j_1}(t+l-1)=a_{l-1,0},\\ c_{j_2}(t+l-1)=a_{l-1,1},\cdots,c_{j_n}(t+l-1)=a_{l-1,n-1}\end{array}\right)$$
$$=\mathrm{Prob}\left(\begin{array}{l}c_{j_1}(t+1)=a_{1,0},c_{j_2}(t+1)=a_{1,1},\cdots,c_{j_n}(t+1)=a_{1,n-1},\\ c_{j_1}(t+l-1)=a_{l-1,0},c_{j_2}(t+l-1)=a_{l-1,1},\cdots,\\ c_{j_n}(t+l-1)=a_{l-1,n-1}|c_{j_1}(t)=a_{0,0},c_{j_2}(t)=a_{0,1},\cdots,\\ c_{j_n}(t)=a_{0,n-1}\end{array}\right)$$
$$\cdot\mathrm{Prob}(c_{j_1}(t)=a_{0,0},c_{j_2}(t)=a_{0,1},\cdots,c_{j_n}(t)=a_{0,n-1})$$

由定理 3 及归纳假设有：

$$=\frac{1}{2^{n(l-1)}}\cdot\frac{1}{2^n}=\frac{1}{2^{nl}}.$$ 结论成立.

4 实验结果

本节按照文献[19]提出的频数检测方法，以 FCSR 与 LFCSR 的进位单元的输出频率对其进位单元的输出概率进行了近似测试. 在测试中分别随机选取了 32 个不同的初始状态，并对每个初始状态连续运行了 2^{30} 个

时刻. 以 $E_{c_{j_1}}$ 为有效进位单元 c_{j_1} 取值 1,其它 81 个有效进位单元取值 0 这样一个事件,其中 $1 \le k \le 82, 1 \le j_1 < j_2 < \cdots < j_{82} \le 160$,则在 32 次随机实验的 2^{30} 个时刻内,事件 $E_{c_{j_1}}$ 的实验概率分布近似如表 1 和表 2 所示.

表 1　FCSR 中事件 $E_{c_{j_k}}$ 出现的实验概率分布

进位单元	次数	x (概率 $=2^{-x}$)	进位单元	次数	x (概率 $=2^{-x}$)
2	3303009	8.3447	148	121378	13.111
3	128	23.000	149	119739	13.1305
4	31114	15.0747	152	123268	13.0885
7	128421	13.0295	154	114659	13.193
9	123052	13.0911	155	86751	13.5954
…	…	…	156	28645	15.194

表 2　LFCSR 中事件 $E_{c_{j_k}}$ 出现的实验概率分布

进位单元	次数	x(概率 $=2^{-x}$)	进位单元	次数	x(概率 $=2^{-x}$)
2	0	0	148	0	0
3	0	0	149	0	0
4	0	0	152	0	0
7	0	0	154	0	0
9	0	0	155	0	0
…	…	…	156	0	0

实验结果表明:

(1)在独立性假设下,每个事件 $E_{c_{j_1}}$ 出现的概率应该是相同的,但是对于 FCSR,同[19]的分析,事件 $E_{c_{j_2}}$ 出现的概率为 $2^{-8.3447}$ 是最高的,事件 $E_{c_{j_3}}$ 出现的概率为 2^{-23} 较小,其它事件的出现概率比较接近. 因而,可以利用事件 $E_{c_{j_2}}$ 以文献[18]的方法对 FCSR 进行实时攻击.

(2)对于我们所设计的结构,在 32 次实验中事件 $E_{c_{j_1}}$ 对于 2^{30} 个连续时刻几乎均为 0,这与本文定理 7 中得到的独立性假设下的理论值非常接近.

实验结果与理论分析一致,因而,对于我们所设计的新结构找不到类似于 FCSR 的能以文献[18]的分析方法进行实时攻击的事件.

5　结论

本文给出了一个 FCSR 的新的使用方法,新结构 LFCSR 与 FCSR 的主要区别在于输出均衡的密码学部件的加入. 新结构 LFCSR 进位单元输出的均匀分布使得对 F-FCSR-H 的实时攻击对基于新结构 LFCSR 的生成器不再可行.

参考文献

[1] Dj Golic, J Menicocci, R. Edit probability correlation attacks on stop/go clocked keystream generators [J]. J Cryptology, 2003, 16(1): 41 – 68.

[2] Zhang B, Wu H, Feng D, Bao F. A fast correlation attack on the shrinking generator [A]. Topics in Cryptology-CT-RSA 2005. CT-RSA 2005 [C]. Springer, Berlin, Heidelberg. 2005. LNCS 3376: 72 – 86.

[3] Martin Hell, Thomas Johansson. Two new attacks on the self-shrinking generator [J]. IEEE Transactions on Information Theory, 2006, 52(8): 3837 – 3843.

[4] Faheem Masoodi, Shadab Alam and M U Bokhari. An analysis of linear feedback shift registers in stream ciphers [J]. International Journal of Computer Applications, 2012, 46(17): 46 – 49.

[5] Zhong X, Wang M, Zhang B, Wu S. A guess-then-algebraic attack on LFSR-based stream ciphers with nonlinear filter [A]. Information and Communications Security. ICICS 2014[C]. Springer, Cham. 2015. LNCS 8958: 132 – 142.

[6] Goli′c, J, Menicocci, R. A new statistical distinguisher for the shrinking generator [OL]. http://eprint. iacr. org/2003/041.

[7] Debraize B, Goubin L. Guess-and-determine algebraic attack on the self-shrinking generator [A]. Fast Software Encryption. FSE 2008 [C]. Springer, Berlin, Heidelberg, 2008. LNCS 5086: 235 – 252.

[8] 冯登国. NESSIE 工程简介[J]. 信息安全与通信保密, 2001, (3): 36 – 39.

[9] Robshaw M. The eSTREAM project[A]. New Stream Cipher Designs [C]. Springer, Berlin, Heidelberg, 2008. LNCS 4986: 1 – 6.

[10] Elena Dubrova. An equivalence preserving transformation from the Fibonacci to the Galois NLFSRs [OL]. 2008, http://arxiv.org/PS_cache/arxiv/pdf/0801/0801.4079v2. pdf.

[11] Deb S., Biswas B., Kar N. (2015) Study of NLFSR and reasonable security improvement on trivium cipher [A]. Information Systems Design and Intelligent Applications. Advances in Intelligent Systems and Computing [C]. Springer, New Delhi, 2015. 339: 731 – 739.

[12] Shi T, Anashin V, Lin D. Linear weaknesses in t-functions [A]. Sequences and Their Applications-SETA 2012. SETA 2012 [C]. Springer, Berlin, Heidelberg, 2012. LNCS 7280: 279 – 290.

[13] Vladimir Anashin, Andrei Khrennikov, Ekaterina Yurova. T-functions revisited: new criteria for bijectivity/transitivity [J]. Des. Codes Cryptogr, 2014, 71(3): 383 – 407.

[14] François Arnault, Thierry P. Berger and Benjamin Pousse. A matrix approach for FCSR automata. Cryptography and Communications, 2011 [OL]. www. springerlink. com / index/J16174424270X56G. pdf.

[15] Paul Stankovski, Martin Hell, Thomas Johansson. An efficient state secovery attack on the X-FCSR family of stream ciphers[J]. J Cryptol, 2014, 27(1): 1 – 22.

[16] Klapper A, Goresky M. 2-Adic shift registers [A]. Fast

Software Encryption. FSE 1993 [C]. Springer, Berlin, Heidelberg. 1994. LNCS 809:174 – 178.
[17] Arnault F, Berger T P. (2005) F-FCSR: Design of a new class of stream ciphers [A]. Fast Software Encryption. FSE 2005 [C]. Springer, Berlin, Heidelberg. 2005. LNCS 3557:83 – 97.
[18] Hell M, Johansson T. (2008) Breaking the F-FCSR-H stream cipher in real time [A]. Advances in Cryptology-ASIACRYPT 2008. ASIACRYPT 2008 [C]. Springer, Berlin, Heidelberg. 2008. LNCS 5350:557 – 569.
[19] Song H, Fan X, Wu C, Feng D. On the probability distribution of the carry cells of stream ciphers F-FCSR-H v2 and F-FCSR-H v3 [A]. Information Security and Cryptology. Inscrypt 2011 [C]. Springer, Berlin, Heidelberg, 2012. LNCS 7537:160 – 178.
[20] Arnault F, Berger T, Lauradoux C, Minier M, Pousse B. A new approach for FCSRs [A]. Selected Areas in Cryptography. SAC 2009 [C]. Springer, Berlin, Heidelberg, 2009. LNCS 5867:433 – 448.
[21] Marjane A, Allailou B. Vectorial conception of FCSR [A]. Sequences and Their Applications-SETA 2010. SETA 2010 [C]. Springer, Berlin, Heidelberg, 2010. LNCS 6338:240 – 252.
[22] Allailou B, Marjane A, Mokrane A. Design of a novel pseudo-random generator based on vectorial FCSRs [A]. Information Security Applications. WISA 2010 [C]. Springer, Berlin, Heidelberg, 2011. LNCS 6513 :76 – 91.
[23] Berger T P, Minier M, Pousse B. Software oriented stream ciphers based upon FCSRs in diversified mode [A]. Progress in Cryptology-INDOCRYPT 2009. INDOCRYPT 2009 [C]. Springer, Berlin, Heidelberg, 2009. 5922:119 – 135.
[24] Stankovski P, Hell M, Johansson T. An efficient state recovery attack on the X-FCSR family of stream ciphers [J]. Journal of Cryptology, 2014, 27(1):1 – 22.
[25] Wang H, Stankovski P, Johansson T. A generalized birthday approach for efficiently finding linear relations inl-sequences [J]. Designs Codes & Cryptography, 2015, 74(1):41 – 57.
[26] Pei D, Lin Z, Zhang X. Construction of transition matrices for ternary ring feedback with carry shift registers [J]. IEEE Transactions on Information Theory, 2015, 61(5): 2942 – 2951.
[27] 刘鑫, 田甜, 戚文峰. 一类 LFSR 序列簇的 2-adic 复杂度 [J]. 系统科学与数学, 2015, 35(9):999 – 1007.
Liu xin, Tian tian, Qi wenfeng. The 2-adic complexity of a class of LFSR sequence families [J]. Journal of Systems Scieme and Mathematical Sciences, 2015, 35(9):999 – 1007. (in Chinese)
[28] Lin Z, Lin D, Pei D. Practical construction of ring LFSRs and ring FCSRs with low diffusion delay for hardware cryptographic applications [J]. Cryptography & Communications, 2017, 9(4):431 – 443.
[29] M. Goresky, A Klapper. Fibonacci and galois representations of feedback-with-carry shift registers [J]. IEEE Transaction on Information Theory, 2002, 48(11):2826 – 2836.

作者简介

董丽华 女, 1977 年生, 辽宁盘锦人, 西安电子科技大学副教授, 硕士生导师. 主要研究方向为密码学.
E-mail: lih_dong@ mail. xidian. edu. cn

曾 勇 男, 1978 年生, 湖南石门人, 西安电子科技大学副教授, 硕士生导师, 主要研究方向为信息安全、传感器网络安全等.
E-mail: yzeng@ mail. xidian. edu. cn

王春红 女, 1976 年生, 河南遂平人, 中船重工集团第七二二研究所高级工程师, 主要研究方向为通信安全.
E-mail: 4506532@ qq. com

胡予濮 男, 1955 年生, 河南濮阳人, 西安电子科技大学教授, 博士生导师, 主要研究方向为密码学、信息安全.
E-mail: yphu@ mail. xidian. edu. cn