CHINACRYPT 2004

密码学进展——CHINACRYPT'2004

第八届中国密码学学术会议论文集

陈克非 李 祥 编

科学出版社
www.sciencep.com

密码学进展—CHINACRYPT'2004

第八届中国密码学学术会议论文集

陈克非　李　祥　编

国家自然科学基金重大研究计划项目(编号：90104005)
国家自然科学基金项目(编号：60173032,60273049,60303026)

科学出版社
北　京

内 容 简 介

本书是2004年在无锡召开的第八届中国密码学学术会议论文集。书中共收集密码学各个分支的研究论文73篇，主要内容包括序列密码、分组密码、公钥密码、非传统密码、数字签名、秘密共享、多方计算、密码协议、信息隐藏、代数、信息论与编码、网络安全与系统安全、密码应用等。

本书可供从事密码学、数学和计算机通信专业的科技人员以及高等院校相关专业的师生参考。

图书在版编目(CIP)数据

密码学进展:CHINACRYPT'2004 第八届中国密码学学术会议论文集/陈克非,李祥编. —北京:科学出版社,2004
ISBN 7-03-013217-3

Ⅰ.密… Ⅱ.①陈… ②李… Ⅲ.密码-理论-学术会议-中国-文集
Ⅳ.TN918.1-53

中国版本图书馆CIP数据核字(2004)第026623号

策划编辑:鞠丽娜 /责任编辑:韩 洁
责任印制:吕春珉 /封面设计:王 浩

科学出版社 出版
北京东黄城根北街16号
邮政编码:100717
http://www.sciencep.com
双青印刷厂 印刷
科学出版社发行 各地新华书店经销
*
2004年4月第 一 版 开本:787×1092 1/16
2004年4月第一次印刷 印张:30 1/4
印数:1—2000 字数:702 000

定价:60.00元
(如有印装质量问题,我社负责调换〈路通〉)

第八届中国密码学学术会议
程序委员会

主　　席：李　祥　（贵州大学）
副 主 席：陈克非　（上海交通大学）
　　　　　　曹珍富　（上海交通大学）
委　　员：（按姓氏笔画排序）
　　　　　　于秀源　（杭州师范学院）
　　　　　　王育民　（西安电子科技大学）
　　　　　　王萼芳　（北京大学）
　　　　　　冯克勤　（清华大学）
　　　　　　刘木兰　（中国科学院系统科学研究所）
　　　　　　朱　洪　（复旦大学）
　　　　　　何大可　（西南交通大学）
　　　　　　李大兴　（山东大学）
　　　　　　杨义先　（北京邮电大学）
　　　　　　沈世镒　（南开大学）
　　　　　　肖国镇　（西安电子科技大学）
　　　　　　张焕国　（武汉大学）
　　　　　　周锦君　（解放军信息工程大学）
　　　　　　陶仁骥　（中国科学院软件研究所）
　　　　　　黄民强　（中国科学院系统科学研究所）
　　　　　　黄祖良　（中国科学院软件研究所）
　　　　　　龚奇敏　（信息产业部第三十研究所）
　　　　　　裴定一　（中国科学院研究生院）

会议秘书：王立斌　（上海交通大学）

前　　言

第八届中国密码学学术会议于2004年在无锡召开，本书收集了在这次会议上报告的73篇论文，内容涉及序列密码、分组密码、公钥密码、非传统密码、数字签名、秘密共享、多方计算、密码协议、信息隐藏、代数、信息论与编码理论、网络安全、系统安全、密码应用等研究课题。这些论文反映了我国密码学学术界的当前研究动态，也展现出我国密码学研究与应用的学术水平。

本次会议共收到投稿论文180篇，每篇论文至少由两位专家评审，最后由程序委员会讨论决定，录用论文73篇，其中56篇全文录用，17篇为短文录用。

我们衷心感谢所有向本次会议投稿的作者对会议的关心与支持；感谢程序委员会的所有成员，他们为从众多的稿件中选出更具代表性的论文参加会议交流付出了很多劳动。我们还要感谢会议的主办单位上海交通大学计算机系、信息安全工程学院、密码与信息安全实验室的老师和研究生，他们在本次会议的筹备和组织安排上默默地工作；还要感谢航天信息股份有限公司，他们在会议的组织筹备过程中伸出了援助之手。正是由于各方的共同努力，使本次会议得以顺利举行。最后，还要感谢王立斌博士和科学出版社责任编辑鞠丽娜、韩洁女士，他们为本次论文集的出版做了大量细致和繁琐的工作。本论文集的出版得到了科学出版社的大力支持，在此向他们表示衷心的感谢。

目　录

序列密码

分组密码

公钥密码、秘密共享、多方计算

非传统密码

数字签名

密码协议

信息隐藏

代数、信息论与编码

网络安全与系统安全

密码应用

序列密码

On the Statistical Properties and Linear Span of FCSR Sequences[1)]

Honggang Hu Dengguo Feng

(State Key Laboratory of Information Security, Graduate School of Chinese Academy of Sciences, Beijing, PRC, 100039)

(Institute of Electronics, Chinese Academy of Sciences, Beijing, PRC, 100080)

Abstract In this paper, the statistical properties of Feedback with Carry Shift Register (FCSR) sequences are analyzed in detail. It shows that the FCSR sequences have ideal statistical properties, such as: symbol number, block number, run property, correlation property and etc. And it is also proved that the linear span of the FCSR sequences is very large under 1 or 2 symbols substitution. This allows us to design FCSR stream ciphers similar to previously proposed Linear Feedback Shift Register (LFSR) stream ciphers.

Keywords FCSR LFSR Statistical property Linear span 2-adic Span

1. Introduction

Pseudorandom sequences, with a variety of statistical properties are important in many areas of communications and computing. The development of a good pseudorandom number generator is very important and has been a hot topic in cryptography and communication. A good pseudorandom sequence generator should have large period, large linear span, good randomness. It is well known that a linear shift register may be found efficiently for a given sequence using B-M algorithm.

1)This work was supported by National Key Foundation Research "973" Project(No. G1999035802), National Nature Science Foundation Project (No. 60273027) and National Excellent Youth Science Foundation Project (No. 60025205).

Therefore, the linear span is a critical index for assessing the strength of a sequence.

Klapper and Goresky[2,3] proposed a new type of pseudorandom number generator-Feedback with Carry Shift Register (FCSR). The register have many properties analogous to that of LFSR. And they also proposed a new index for assessing the strength of a binary sequence—2-adic span. And they also analyzed the statistical properties of the FCSR sequences[3~5,7~10], but their analysis isn't adequate. In paper[6], the lower bound of the linear span of the FCSR sequences under some special conditions is given. In this paper, we analyzed the symbol number, block number , run property and correlation property of the FCSR sequences in detail. The result shows that the FCSR sequences have ideal statistical property. Furthermore, we compute the linear span of the FCSR sequences under 1 or 2 symbol substitution. And the result shows that the FCSR sequences have large 1 or 2-error linear span. Therefore, the FCSR sequences are ideal key sequences at present.

In section 2, we briefly review FCSR; In section 3, we analyze the distributional properties of the FCSR sequences in detail; In section 4, we analyze the correlation properties of the FCSR sequences; In section 5, we prove that the linear span of the FCSR sequences is large under 1 or 2 symbol substitution. Finally, section 6 contains the conclusion.

2. FCSR

Let q be an odd positive integer with the binary expansion $q=q_0+q_1 2+q_2 2^2+\cdots+q_r 2^r$, where $q_0=-1$, and $q_i\in\{0,1\}, 1\leqslant i\leqslant r$. The coefficients $q_1, q_2, \cdots, q_r$ may be looked on as taps on a feedback register as in the following definition and figure. The same definition is also contained in paper [6].

Definition 1[5] The FCSR with connection integer q is a feedback register with r bits of storage plus small amount of auxiliary memory containing an integer for carry. If the contents of the register are $(a_{r-1}, a_{r-2}, \cdots, a_0)$ and the memory is m, then the operation of the shift register is defined as follows:

(1) Take an integer sum $\sigma=\sum_{k=1}^{r} q_k a_{r-k}+m$.

(2) Shift the contents one step to the right, while outputting the rightmost bit a_0.

(3) Put $a_r\equiv\sigma \bmod 2$ into the leftmost cell of the shift register.

(4) Replace m with $m=(\sigma-a_r)/2$.

Definition 2[5] The 2-adic span of a binary eventually period sequence $a=(a_0, a_1, \cdots)$ is the smallest value of r, which occurs among all FCSRs whose output is the sequence $a=(a_0, a_1, \cdots)$.

If $a=(a_0, a_1, \cdots)$ is strictly periodic of period T, set $\alpha=\sum_{i=0}^{\infty} a_i 2^i$, then $\alpha=-\frac{\sum_{i=0}^{T-1} a_i 2^i}{2^T-1}$.

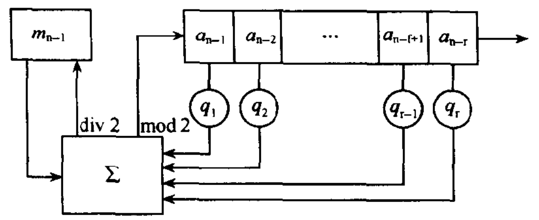

Figure Feedback with carry shift register

There is a one-to-one relationship between the sets $\{-p/q \mid p,q \in Z, p,q>0\}$ and $\{a \mid a=(a_0,a_1,\cdots)$ is an eventually periodic binary sequence$\}$. If $(p,q)=1$ and q is odd, then the eventual period T of the sequence associated with $\alpha=-p/q$ is $T=ord_q(2)$. If the readers want to know more about 2-adic numbers, please refer to paper [5] and its references.

Remark The integer 2 in the above can be replaced by any prime integer $d \geqslant 3$ and the corresponding connection integer q is $-1+\sum_{i=1}^{r} q_i d^i$, where $q_i \in \{0,1,\cdots,d-1\}$ (If the readers want to know why $q=-1+\sum_{i=1}^{r} q_i d^i$, please refer to section 4 of paper [5]). Consequently, T is replaced by $T=ord_q(d)$ and α is replaced by $\alpha=-\frac{\sum_{i=0}^{T-1} a_i d^i}{d^T-1}, a_i \in Z_d$.

Now we will give the definition of l-sequence which is the analog of m-sequence.

Definition 3[5] An l-sequence is a periodic sequence (of period $T=\phi(q)$) which is obtained from an FCSR with connection integer q for which d is a primitive root.

Definition 4[6] q is a positive integer, if d is a primitive root mod q, then q is called d-prime.

If q has a primitive root, then[14] q must be $2, 4, q=p^e$ or $2p^e$, where p is an odd prime number, $e \geqslant 1$. In this paper we only consider the case $q=p^e$.

3. Distributional Properties

In the following we will show that the sequences based on odd prime power connection integer for which d is a primitive root have excellent distributional properties. Such properties follows from the primitivity of d.

Analogous to the trace representation of linear recurring sequences, the FCSR sequences have the following exponential representation.

Proposition 1[5] Suppose a periodic sequence $a=(a_0,a_1,\cdots)$ is generated by an FCSR with connection integer q. Let $\gamma=d^{-1} \bmod q$, then there exists $A \in Z_q$ such that $a_i = A\gamma^i \pmod q \pmod d, i=0,1,2,\cdots$

Proof Let $-\frac{p_0}{q}=\sum_{i=0}^{\infty}a_i d^i$, $-\frac{p_1}{q}=\sum_{i=0}^{\infty}a_{i+1}d^i$, we have

$-d\frac{p_1}{q}+a_0=-\frac{p_0}{q}$, so $dp_1=a_0q+p_0$, $p_1\equiv d^{-1}p_0 \bmod q$,

$a_0\equiv-\frac{p_0}{q} \bmod d\Rightarrow -qa_0\equiv p_0 \bmod d\Rightarrow a_0\equiv p_0 \bmod d$.

Similarly, $a_i=p_i \bmod d$, $p_{i+1}=d^{-1}p_i \bmod q$, so there exists a $A\in Z_q$ such that $a_i=A\gamma^i$ (mod q)(mod d), $i=0,1,2,3,\cdots$

In the following we suppose $d^r<q<d^{r+1}$.

Lemma 1 Suppose that the rational expression of α is just $-\frac{A}{q}$. Then $a_0=b_0$, $a_1=b_1$, $\cdots$, $a_{s-1}=b_{s-1}$ with s given elements from Z_d and $s\leqslant r$ if and only if $A\equiv -qh \bmod d^s$, where $h=\sum_{i=0}^{s-1}b_i d^i$.

Proof

$$-\frac{A}{q}=a_0+a_1d+\cdots+a_{s-1}d^{s-1}+a_sd^s+\cdots\Leftrightarrow$$

$$-\frac{A}{q}\equiv a_0+a_1d+\cdots+a_{s-1}d^{s-1} \bmod d^s\Leftrightarrow$$

$$A\equiv -qh \bmod d^s$$

Theorem 1 Suppose that the connection integer is p^e, $e\geqslant 1$, p is an odd prime, then the number of block $(b_0,b_1,\cdots,b_{s-1})$ is $\left[\frac{q-1}{d^s}\right]$ or $\left[\frac{q-1}{d^s}\right]+1$ when $e=1$, $\left[\frac{q-1}{d^s}\right]-\left[\frac{\left[\frac{q-1}{d^s}\right]}{p}\right]-1$, $\left[\frac{q-1}{d^s}\right]-\left[\frac{\left[\frac{q-1}{d^s}\right]}{p}\right]$ or $\left[\frac{q-1}{d^s}\right]-\left[\frac{\left[\frac{q-1}{d^s}\right]}{p}\right]+1$ when $e\geqslant 2$, where $s\leqslant r$.

Proof Let $A_0\equiv -qh \bmod d^s$, where $h=\sum_{i=0}^{s-1}b_i d^i$, $0<A_0<d^s$, according to lemma 1, the solutions of $A\equiv -qh \bmod d^s$ can be represented by A_0+d^sk, $k=0,1,2,3,\cdots$. Since $A_0+d^sk\in Z_q^*$, $k\leqslant\left[\frac{q-1}{d^s}\right]$. So when $e=1$, the number of block $(b_0,b_1,\cdots,b_{s-1})$ is $\left[\frac{q-1}{d^s}\right]$ or $\left[\frac{q-1}{d^s}\right]+1$, when $e\geqslant 2$, if $A_0\equiv 0 \bmod p$, $k\not\equiv 0 \bmod p$, the number of such k is $\left[\frac{q-1}{d^s}\right]-\left[\frac{\left(\frac{q-1}{d^s}\right)}{p}\right]-1$, so the number of block $(b_0,b_1,\cdots,b_{s-1})$ is $\left[\frac{q-1}{d^s}\right]-\left[\frac{\left(\frac{q-1}{d^s}\right)}{p}\right]-1$ or $\left[\frac{q-1}{d^s}\right]-\left[\frac{\left(\frac{q-1}{d^s}\right)}{p}\right]$, if $A_0\not\equiv 0 \bmod p$, $k\not\equiv -A_0d^{-s} \bmod p$, the number of such k is $\left[\frac{q-1}{d^s}\right]-\left[\frac{\left(\frac{q-1}{d^s}\right)}{p}\right]$, so the number of block $(b_0,b_1,\cdots,b_{s-1})$ is $\left[\frac{q-1}{d^s}\right]-\left[\frac{\left(\frac{q-1}{d^s}\right)}{p}\right]$ or

$$\left[\frac{q-1}{d^s}\right]-\left[\frac{\left(\frac{q-1}{d^s}\right)}{p}\right]+1.$$

Remark This theorem is almost the same as proposition 10.1 of paper [8].

Corollary 1 The number of element a is $\left[\frac{q-1}{d}\right]$ or $\left[\frac{q-1}{d}\right]+1$ when $e=1$,

$\left[\frac{q-1}{d}\right]-\left[\frac{\left[\frac{q-1}{d}\right]}{p}\right]-1$, $\left[\frac{q-1}{d}\right]-\left[\frac{\left[\frac{q-1}{d}\right]}{p}\right]$ or $\left[\frac{q-1}{d}\right]-\left[\frac{\left[\frac{q-1}{d}\right]}{p}\right]+1$ when $e\geqslant 2$,

where $a\in Z_d$.

Theorem 2 The number of block$(b_0,b_1,\cdots,b_{s-1})$ is less than 2, where $s>r$.

Proof Let $h=\sum_{i=0}^{s-1}b_i d^i$, suppose that there exist A and B such that $-A/q\equiv h \bmod d^s$ and $-B/q\equiv h \bmod d^s$, then $A/q\equiv B/q \bmod d^s \Leftrightarrow A\equiv B \bmod d^s$, so $A=B$ since $A,B\in F_q^*$, it is a contradiction.

Theorem 3 Suppose that the connection integer is $p^e, e\geqslant 1$, p is an odd prime, then the difference between the number of block$(b_0,b_1,\cdots,b_{s-1})$ is not larger than 1 when $e=1$, not larger than 2 when $e\geqslant 2$, where $s\leqslant r$.

Proof It follows from theorem 1 directly.

Theorem 4 The number of runs of length s is $(d-1)^2 d\left[\frac{q-1}{d^s}\right]$ or $(d-1)^2 d\left(\left[\frac{q-1}{d^s}\right]+1\right)$ when $e=1$,

$$(d-1)^2 d\left(\left[\frac{q-1}{d^s}\right]-\left[\frac{\left(\frac{q-1}{d^s}\right)}{p}\right]-1\right), (d-1)^2 d\left(\left[\frac{q-1}{d^s}\right]-\left[\frac{\left(\frac{q-1}{d^s}\right)}{p}\right]\right) \text{or}$$

$$(d-1)^2 d\left(\left[\frac{q-1}{d^s}\right]-\left[\frac{\left(\frac{q-1}{d^s}\right)}{p}\right]+1\right) \text{when } e\geqslant 2, \text{where } s\leqslant r-2.$$

Proof Since the number of block $(a,b,b,\cdots,b,b,c), a\neq b, c\neq b$ is $d(d-1)^2$, the result is obvious by theorem 1.

Theorem 5 $a=(a_0,a_1,\cdots)$ is a l-sequence generated by an FCSR with connection integer q, the period of a is $T=\varphi(q)=p^{e-1}(p-1)$, then $a_i+a_{i+T/2}=d-1$.

Proof According to proposition 1,

$$a_{i+T/2}=A\gamma^{i+T/2}(\bmod q)(\bmod d)=(-A\gamma^i)(\bmod q)(\bmod d)=(q-(A\gamma^i \bmod q)) \bmod d$$
$$=d-1-A\gamma^i(\bmod q)(\bmod d)$$
$$=d-1-a_i, \text{so } a_i+a_{i+T/2}=d-1$$

Corollary 2 The 0 run and $d-1$ run of length more than r don't exist.

Proof If such sequences exist, then according to lemma 1, $A\equiv -qh \bmod d^{r+1}\equiv 0 \bmod d^{r+1}$, so $A=0$ since $A\in Z_q^*$, it is a contradiction. According to theorem 5, the d-1 run of length more than r also doesn't exist.

Corollary 3 The number of b equals to the number the number of d-1-b, where $b\in$

Z_d. Furthermore, the l-sequence is balanced if $d=2$.

4. Correlation Properties

The correlation property is an important index of a pseudorandom sequence. In this section, we will investigate the correlation properties of l-sequence. The correlation properties of l-sequence include arithmetic correlation property and common correlation property.

Suppose that a periodic sequence $\alpha=(a_0,a_1,\cdots)$ is generated by an FCSR with connection integer q, its period is $T=\varphi(q)$, and $\beta=(a_t,a_{t+1},\cdots)$ is obtained from α by shifting to left by t steps, $\gamma=(b_0,b_1,\cdots)$is the sum of α and β with carry, $\gamma'=(b'_0,b'_1,\cdots)$ is the sum of $\gamma=(b_0,b_1,\cdots)$ and 1 with carry. We have the following theorem.

The following theorem indicates the property of arithmetic autocorrelation of l-sequence.

Theorem 6 $\alpha,\beta,\gamma,\gamma'$ is as above, if there exist $i_0, 0\leqslant i_0<T$, such that $b_{i_0}\neq d-1$, then there exist a $T_0]T$ such that γ or γ' is a l-sequence with period T_0.

Proof Suppose that the rational representation of α is $-\frac{A}{q}$, the rational representation of β is $-\frac{B}{q}$, then the rational representation of γ is $-\frac{A+B}{q}$, if $A+B=q$, $\gamma=(d-1,d-1,d-1,\cdots)$, since $-1=\sum_{i=0}^{\infty}(d-1)d^i$; if $A+B<q$ and $e=1$, γ is a l-sequence with period p-1; if $A+B>q$ and $e=1$, the rational representation of γ' is $-\frac{A+B-q}{q}$, thus γ' is a l-sequence with period $p-1$; if $e\geqslant 2$, suppose that $p^{e_0}\mid(A+B)$, $0\leqslant e_0<e$, if $A+B<q$, the rational representation of γ is $-\frac{\frac{A+B}{p^{e_0}}}{p^{e-e_0}}$, thus γ is a l-sequence with period $p^{e-e_0-1}(p-1)$; if $A+B>q$, the rational representation of γ' is $-\frac{\frac{A+B-q}{p^{e_0}}}{p^{e-e_0}}$, thus γ' is a l-sequence with period $p^{e-e_0-1}(p-1)$.

Definition 5 Suppose that $S=(s_0,s_1,\cdots)$ and $T=(t_0,t_1,\cdots)$ are 2 sequences over F_q with period N, then the Hamming distance $d(S,T)$ between S and T is the cardinality of the set$\{i\mid s_i\neq t_i, 0\leqslant i<N\}$.

The following theorems indicate the property of Hamming autocorrelation of l-sequence.

Theorem 7 $\alpha=(a_0,a_1,\cdots)$is generated by an FCSR with connection integer q, its period is $T=\varphi(q)$, and $\beta=(a_t,a_{t+1},\cdots)$ is obtained from α by shifting to left by t steps, if $t<r$, then $(d^{t+1}-d^t)\left[\frac{q-1}{d^{t+1}}\right]\leqslant d(\alpha,\beta)\leqslant(d^{t+1}-d^t)\left[\left(\frac{q-1}{d^{t+1}}\right)+1\right]$ when $e=1$, or $(d^{t+1}$

$-d^t)\left(\left[\frac{q-1}{d^{t+1}}\right]-\left[\frac{\left(\frac{q-1}{d^{t+1}}\right)}{p}\right]-1\right) \leqslant d(\alpha,\beta) \leqslant (d^{t+1}-d^t)\left(\left[\frac{q-1}{d^{t+1}}\right]-\left[\frac{\left(\frac{q-1}{d^{t+1}}\right)}{p}\right]+1\right)$ when $e\geqslant 2$.

Proof Since the number of block $(b_1, b_2, \cdots, b_t, b_{t+1})$, $b_1 \neq b_{t+1}$ is $d^{t+1}-d^t$, by theorem 1, the result is obvious.

Lemma 2 $\alpha=(a_0, a_1, \cdots)$ and $\beta=(b_0, b_1, \cdots)$ are 2 l-sequences generated by an FCSR with connection integer q, let $\alpha'=(a_1, a_2, \cdots)$, $\beta'=(b_1, b_2, \cdots)$, then $d(\alpha,\beta)=d(\alpha',\beta')$.

Theorem 8 $\alpha=(a_0, a_1, \cdots)$ and $\beta=(b_0, b_1, \cdots)$ are 2 l-sequences generated by an FCSR with connection integer q, then $d(\alpha,\beta)\geqslant\left[\frac{p-1}{r+1}\right]+1$ when $e=1$ and $d(\alpha,\beta)\geqslant\left[\frac{p^{e-1}(p-1)}{r+1}\right]+1$ when $e\geqslant 2$.

Proof According to lemma 2, we can suppose $a_0\neq b_0$, and the other $T-1=\varphi(q)-1$ elements can be divided into $\left[\frac{T}{r+1}\right]$ blocks with length more than r, so $d(\alpha,\beta)\geqslant\left[\frac{T}{r+1}\right]+1$ by theorem 2. The result is obvious since $T=p-1$ when $e=1$, and $T=p^{e-1}(p-1)$ when $e\geqslant 2$.

Remark The lower bound above is trivial, and more tight bound is desirable.

5. Linear Span

The linear span is a critical index for assessing the strength of a sequence. In this section, we will investigate the linear span and k-error linear span of the l-sequence generated by an FCSR. In general, to decide the linear span or k-error linear span of a l-sequence is difficult, so we will investigate only under some special condition. But such condition is very useful in practice. In paper [6], the authors derived a lower bound on the linear span of a binary sequence generated by a Feedback with Carry Shift Register under the following condition: q is a power of a prime such that $q=r^e(e\geqslant 2)$ and $r=2p+1$, where r and p are 2-prime. And their result showed that the linear span of an FCSR with a strong 2-prime is half of the period.

Firstly, we will give the formal definition of the k-error linear span of a periodic sequence in the following.

Definition 6 Let $S=(s_0, s_1, s_2, \cdots, s_{N-1})^\infty$ be an N-periodic sequence over F_q and k be an integer with $1\leqslant k\leqslant N$, then the k-error linear span $L_{N,k}(S)$ of S is $\min_T L(T)$, where the minimum is extended over all N-periodic sequences $T=(t_0, t_1, t_2, \cdots, t_{N-1})^\infty$ over F_q for which the Hamming distance of the vectors $(s_0, s_1, s_2, \cdots, s_{N-1})$ and $(t_0, t_1, t_2, \cdots, t_{N-1})$ is at most k.

The following several propositions are the main result of paper [6].

Proposition 2[6] If $d=2$ and the connection integer q of an FCSR is 2-prime, then the linear span of the corresponding l-sequence is not larger than $\frac{q+1}{2}$.

Let $q=2p+1$, we have the following proposition.

Proposition 3[6] If $d=2$, q and p are 2-prime, then the linear span of the corresponding l-sequence is $p+1$.

Proposition 4[6] If $d=2$, q and p as above, then the linear span of the corresponding l-sequence is at least $m+2$, where m is the order of 2 modulo p.

The three propositions above shows that the linear span of l-sequence is large compared with m-sequences when $d=2$.

Theorem 9 If $d=2, q=2p+1$, q is 2-prime, p is an odd prime number and p is not 2-prime, then the linear span of the corresponding l-sequence is at least $2p-2$ under 1 symbol substitution.

Proof Suppose that the l-sequence is $a=(a_0, a_1, a_2, \cdots)$, we have $a_{i+\phi(q)/2}=1+a_i$ according to theorem 5, where $\phi(q)=q-1=2p$, thus $a_{i+p}=1+a_i$. Let

$$S(x)=\sum_{i=0}^{2p-1} a_i x^i=(1+x^p)S_p(x)+x^p(1+x+x^2+\cdots+x^{p-1}), \text{where}$$

$$S_p(x)=\sum_{i=0}^{p-1} a_i x^i, f(x)=S(x)+x^k, 0\leqslant k\leqslant 2p-1, \xi^p=1, \xi\neq 1.$$

We have $f(1)=p+1=0$, but $f(\xi)=\xi^k\neq 0$, therefore $\deg(f(x),(1+x^p)^2)\leqslant 2$, and the linear span a is at least $2p-2$ under 1 symbol substitution.

Theorem 10 If $d=2$, $q=2p+1$, p and q are 2-prime, then the linear span of the corresponding l-sequence is at least $2p$-2 under 1 symbol substitution, and at least $p+1$ under 2 symbols substitution.

Proof $a=(a_0, a_1, a_2, \cdots)$ and $S(x)$ are as above. By the similar way, the linear span of a is at least $2p-2$ under 1 symbol substitution. Let

$$f(x)=S(x)+x^{k_1}(1+x^{k_2}), 0\leqslant k_1<2p-1, 0<k_2<2p-k_1.$$

Let $\xi^p=1, \xi^t\neq 1, \forall\ 1\leqslant t<p$. We have $f(1)=p\neq 0$, and $f(\xi)=0$ if and only if $k_2=p$, so $f(x)=(1+x^p)S_p(x)+x^p(1+x+x^2+\cdots+x^{p-1})+x^{k_1}(1+x^p), 0\leqslant k_1<p$. Let $g(x)=\frac{f(x)}{1+x+x^2+\cdots+x^{p-1}}=(1+x)S_p(x)+x^p+x^{k_1}(1+x), \deg(g(x))\leqslant p$. If $g(\xi)=0$, then $(1+x+x^2+\cdots+x^{p-1})\mid g(x)$ since p is 2-prime, thus $g(x)=1+x+x^2+\cdots+x^{p-1}, x(1+x+x^2+\cdots+x^{p-1})$ or $1+x^p$. Since $g(1)\neq 0, g(x)$ must be $1+x+x^2+\cdots+x^{p-1}$ or $x(1+x+x^2+\cdots+x^{p-1})$.

Case 1: $g(x)=1+x+x^2+\cdots+x^{p-1}$. We have $S_p(x)=\sum_{i=0}^{(p-1)/2} a_i x^{2i}+x^{k_1}$, since $g(x)=(1+x)S_p(x)+x^p+x^{k_1}(1+x)$. But it is impossible by theorem 1.

Case 2: $g(x)=x(1+x+x^2+\cdots+x^{p-1})$. We have $S_p(x)=\sum_{i=0}^{(p-3)/2} a_i x^{1+2i}+x^{k_1}$, since

$g(x)=(1+x)S_p(x)+x^p+x^{k_1}(1+x)$. It is also impossible by theorem 1.

Therefore $\deg(f(x),(1+x^p)^2)\leqslant p-1$, and the linear span a is at least $2p-(p-1)=p+1$ under 2 symbols substitution.

6. Conclusion

Feedback with Carry Shift Register (FCSR) is the analog of Linear Feedback Shift Register (LFSR). And many properties about FCSR is still unclear. In this paper, we have analyzed the symbol number, block number , run property and correlation property of the FCSR sequences in detail. The result shows that the FCSR sequences have ideal statistical property. Furthermore, we compute the linear span of FCSR sequences under 1 or 2 symbol substitution. And the result shows that the FCSR sequences have large 1 or 2-error linear span. Therefore, the FCSR sequences are ideal key sequences at present. But better result about correlation property and linear span of l-sequence is desirable.

References

[1] Golomb S. Shift Register Sequences. Laguna Hills, CA: Aegean Park, 1982

[2] Klapper A. 2-adic Shift Register. Fast Software Encryption, Second International Workshop, LNCS, Berlin: Springer-Verlag, 1994, 809:174-178

[3] Goresky M, Klapper A. Feedback Registers Based on Ramified Extensions of the 2-adic Numbers. Advances in Cryptology-Eurocrypt'94, LNCS. Berlin: Springer-Verlag, 1995, 950:215-222

[4] Goresky M, Klapper A. Large Periods Nearly de Bruijn FCSR Sequences. Advances in Cryptology-Eurocrypt'95, LNCS. Berlin :Springer-Verlag, 1995, 921:263-273

[5] Klapper A, Goresky M. Feedback Shift Register, Combiners with Memory and 2-adic Span. J. Cryptology, 1997, 10:111-147

[6] Changho Seo, Sangjin Lee, Yeoulouk Sung, et al. A Lower Bound on the Linear Span of an FCSR. IEEE Trans. Info. Theory, March 2000, IT-46:691-693

[7] Goresky M, Klapper A. Arithmetic Crosscorrelations of Feedback with Carry Shift Register Sequences. IEEE Trans. Info. Theory, July 1997,IT-43:1342-1345

[8] Klapper A. Periodicity, Correlation, and Distribution Properties of d-FCSR Sequences. http://cs.engr.uky.edu/~klapper/ps/ramif.ps

[9] Klapper A. Efficient Multiply-With-Carry Random Number Generators with Optimal Distribution Properties. http://cs.engr.uky.edu/~klapper/ps/mwc.ps

[10] Klapper A. Distribution Properties of d-FCSR Sequences. http://cs.engr.uky.edu/~klapper/ps/d-dist.ps

[11] Goresky M, Klapper A, Washington L. Fourier Transforms and the 2-adic Span of Periodic Binary Sequences. IEEE Trans. Info. Theory, March 2000,IT-46: 687-691

[12] Rueppel R A. Analysis and Design of Stream Cipher. Berlin : Springer-Verlag, 1986

[13] Niederreiter H. Periodic Sequences with Large k-error Linear Complexity. IEEE Trans. Info. Theory , February 2003, IT-49: 501-505

[14] Ireland K, Rosen M. A Classical Introduction to Modern Number Theory. Second Edition. In: GTM. New York: Springer Verlag, 1990, 84

[15] Ding C, Xiao G, Shan W. The Stability Theory of Stream Ciphers(LNCS), Berlin: Springer-Verlag, 1991, 561