وزارة التعليم العالي والبحث العلمي
الجامعة المستنصرية
كلية التربية

مجلة كلية التربية

مجلة علمية محكمة

العدد السادس

2012

هيأة التحرير

مجلة كلية التربية
مجلة – متخصصة – محكمة
تصدرها كلية التربية / الجامعة المستنصرية

قسيمة اشتراك

سعر النسخة الواحدة
داخل البلد : (12.500) اثنا عشر ألفا وخمسمئة دينار عراقي
خارج البلد : (60 $) ستون دولاراً

الاشتراك السنوي
داخل البلد : (85000) خمسة وثمانون ألف دينار عراقي
خارج البلد : (550$) خمسمئة وخمسون دولاراً

الاسم : -
العنوان :-

يكتب الصك باسم مجلة كلية التربية/ الجامعة المستنصرية

العنوان البريدي :- الجامعة المستنصرية / كلية التربية
مجلة كلية التربية
مكتب بريد الجامعة المستنصرية
ص.ب 46219

مجلة كلية التربية

مجلة علمية محكمة تصدرها كلية التربية بالجامعة المستنصرية

1) تنظر المجلة البحوث العلمية الأصيلة التي تتوافر فيها شرائط البحث في الإحاطة والاستقصاء ومنهج البحث العلميّ وخطواته .
2) يشترط ألاّ يكون قد قدم للنشر في أيّ مكان آخر .
3) لا يجوز لصاحب البحث أو المقالة أو أيّة جهة أخرى إعادة نشر ما سبق من دراسات أو نشر ملخص عنه في أيّ كتاب أو صحيفة أو دورية إلا بعد مرور سنة أشهر على تاريخ نشره في مجلة كلية التربية.وبموافقة خطية من رئيس التحرير.
4) المجلة تحتفظ بحقها في أن تحذف الصياغة أو تتركها أو تعيدها بما يتناسب و الملاحظات العلمية التي يشير إليها المحكمون أو القواعد اللغوية السليمة .
5) تتلقى المجلة البحوث للنشر من داخل الجامعة المستنصرية وخارجها مكتوبة باللغة العربية ، أو بلغة أجنبية، على أن يرافق مقدم البحث العلمي ملخصاً باللغة العربية في حدود (100-150) كلمة في كل من اللغتين العربية والانكليزية لبحثه وأن يكتب الاختصاص الدقيق على البحث .
6) تعرض البحوث المقدمة للنشر في المجلة في حالة قبولها مبدئياً على المحكمين من ذوي الاختصاص يُختارون بسرية تامة وذلك لبيان مدى أصالتها وجديتها وقيمة نتائجها وسلامة طريقة عرضها، ثمّ مدى صلاحيتها للنشر .
7) إذا قدم باحث دراسة ثم عاد وسحبها أو إذا كان البحث لا يصلح للنشر فهو ملزم بدفع التكاليف التي يقدرها رئيس تحرير المجلة التي أنفقت على تقويم البحث أو المقالة .
8) ترسل نسختان من البحث الى عنوان المجلة وذلك بالمواصفات الآتية : -
أ. أن تحمل اسم الكاتب باللغتين العربية والانكليزية .
ب. أن تكون مطبوعة على الآلة الكاتبة بمسافات مزدوجة بين الأسطر .
ج. لا تزيد عدد صفحات البحث بما فيها الأشكال والرسوم وغيرها عن عشرين صفحة .

د. تقدم البحوث منضدة على قرص ليزري ومرفقة بنسخة من البحث مطبوعة على الورق .

9) إنّ هيأة تحرير المجلة تثبت قائمة المصادر والمراجع في نهاية البحث لذا يستحسن أن يتقيد مقدمو البحوث بشكليات أساليب العرض والتسميات والمصطلحات والمراجع والرموز بالطريقة الموضحة في أدناه-

أ. إثبات الهامش بالنسبة للمصادر وذلك عند ذكر المصدر لأول مرة على النحو الآتي :-

ذكر اسم المؤلف كاملاً مع تاريخ وفاته – الهجري موضوعاً بين قوسين . ذكر اسم المصدر كاملاً مكتوباً بالحرف الغامق إذا كان عربياً وبحروف مائلة إذا كان باحدى اللغات الاوربية . ذكر عدد الاجزاء ، ذكر اسم المحقق ومكان الطبع ودار النشر وسنة النشر .

ب. ذكر المراجع :

ذكر اسم المؤلف كاملاً ثم اسم المرجع ورقم الطبعة ومكان الطبع واسم المطبعة وسنة النشر ويلي ذلك المجلد ورقم الصفحة .

ج. محاضر المؤتمرات

ذكر اسم المؤلف كاملاً ، ذكر اسم الدراسة او المقالة موضوعة بين علامتي اقتباس ، ذكر اسم الكاتب كاملاً، ذكر اسم المحررين ان كانوا غير واحد او الإشارة للأول وأردافه بكلمة (آخرون) ، ذكر اسم المطبعة والجهة الناشرة ومكان النشر وتاريخ النشر ثم الصفحة.

د. ذكر اسم صاحب المقالة كاملاً موضوعاً بين علامتي اقتباس " " ذكر اسم المجلة بالحرف الغامق للعربية ، وبالحروف المائلة للأوربية ورقم المجلد (السنة بين قوسين) ورقم الصفحة .

10) أ. عند ورود آية قرآنية كريمة يذكر رقمها واسم سورتها وذلك في الهامش.

ب. عند ورود حديث نبوي شريف يجب ذكر مظان ومصادر تخريجه مع ذكر الجزء أن وجد – ورقم الصفحة .

ج. عند الاستشهاد بمخطوط يذكر اسم المؤلف كاملاً وعنوان المخطوط كاملاً ، وذكر اسم المكان المحفوظ فيه هذا المخطوط ويشار الى تاريخ النسخة ، وعدد اوراقها ، ويذكر رقم الورقة مع بيان الوجه او الظهر المأخوذ منه الاقتباس . ويشار لوجه الورقة بالرمز (أ) كما يشار لظهرها بالرمز (ب) .

11) عند ورود اسماء اعلام في متن البحث فانها تكتب كاملة مع ذكر تاريخ الوفاة بالهجري والميلادي موضوعة بين قوسين إذا كانت من اعلام التراث العربي الاسلامي .

12) تكون أرقام التوثيق متسلسلة موضوعة بين قوسين ، فإذا كانت أرقام التوثيق في الصفحة الأولى مثلاً قد انتهت عند رقم (4) فمعنى ذلك أن رقم التوثيق الصفحة الثانية سيبدأ بالرقم (5) .

13) التقليل من الملاحظات الهامشية في صفحات البحث وإعطاؤها رموزاً كنجمة مثلا.

14) أ . الأشكال والرسومات والبيانات والمواد التوضيحية الأخرى توضع في اماكن مناسبة مع ما يشير اليها في محتوى البحث وتكون مصورة على القرص الليزري .

ب. يراعى ان تكون صفحات البحث متسلسلة الترقيم بحيث يشمل ذلك صفخات البخث بما فيها الصور الفوتوغرافية والأشكال والرسوم والبيانات والمواد التوضيخية الأخرى .

15) يكون حجم حرف متن البحث (16) وحرف الهامش (14) .

16) ترسل البحوث وجميع المراسلات المتعلقة بالمجلة على العنوان الآتي :

جمهورية العراق – بغداد
الجامعة المستنصرية – مكتب بريد الجامعة المستنصرية -
ص. ب. 46219 {عمادة كلية التربية} .

رقم الأيداع في دار الكتب والوثائق ببغداد 599 لعام 1997

Analysis of the Sequence Generated from Modified Geffe Generator

Muna Jaafar Raheem
Computer Science Dept./College of Science/Mustansiriya University
Email: munmnmun@yahoo.com

تقديم البحث:2011/10/2
قبول نشر البحث:2012/3/14

Abstract

Linear Feedback Shift Register (LFSR) systems used widely in stream cipher systems field. Golomb used the recurrence relation to find the next state values of single LFSR depending on initial values, s.t. he can be considered the first who can construct a linear equations system of a single LFSR. Attacking of key generator means attempt to find the initial values of the combined LFSR's.

This Paper introduces developing of Geffe generator by increasing the LFSR's from (3) to (5) with new combining function which has good statistical properties. The new generator called Modified Geffe generator.

In this paper, firstly, a Golomb's method introduced to construct a linear equations system of a single LFSR. Secondly, this method developed to construct a linear equations system of key generator (a LFSR system) where the effect of combining function of LFSR is obvious. Lastly, before solving the linear equations system, the existence and the uniqueness of the solution must be tested, then solving the linear equations system using one of the classical methods like Gauss Elimination. Find the solution of linear equations system means find the initial values of the generator. The new proposed generator treated as a practical example of this work.

Keywords: Linear Feedback Shift Register (LFSR), Linear Equations System, Gauss Elimination Method, Geffe generator.

تحليل المتتابعة المولدة من مولد جيف المطور

م.م. منى جعفر رحيم
قسم علوم الحاسوب/كلية العلوم/الجامعة المستنصرية

خلاصة

لقد استخدمت انظمة المسجل الزاحف الخطي ذو التغذية التراجعية بشكل واسع في مجال انظمة التشفير الانسيابي. استخدم كولومب العلاقة التكرارية لايجاد قيم الحالة التالية لمسجل زاحف منفرد بالاعتماد على القيم الابتدائية له لذلك اعتبر اول من استطاع انشاء نظام معادلات خطية لمسجل زاحف منفرد. ان مهاجمة مولد مفاتيح يعني محاولة ايجاد القيم الابتدائية لمسجلاته الزاحفة.

تم في هذا البحث تطوير مولد جيف من خلال زيادة عدد المسجلات الزاحفة من (٣) الى (٥) مع دالة مركبة لها خواص احصائية جيدة. المولد الجديد يدعى مولد جيف المطور.

في هذا البحث، اولا تم عرض طريقة كولومب لانشاء نظام معادلات خطية لمسجل زاحف منفرد. ثانيا، تم تطوير هذه الطريقة لانشاء نظام معادلات خطية لمولد مفاتيح (منظومة مسجلات زاحفة) والتي يظهر فيها جليا تأثير الدالة المركبة. واخيرا، وقبل الشروع بحل ذلك النظام الخطي، علينا اختبار وجود ووحدانية الحل لهذا النظام ومن ثم حل هذا النظام باستخدام احدى الطرق التقليدية المعروفة مثل طريقة كاوس للحذف. ان حل نظام المعادلات الخطية يعني ايجاد القيم الابتدائية للمسجلات الزاحفة المشتركة في المولد. المولد المقترح الجديد، كان المثال العملي لهذه البحث.

1. Introduction

A LFSR System (LFSRS) consists of two main basic units. First, is a feedback function and initial state values [1]. The second one is, the Combining Function (CF), which is a Boolean function [2]. Most of all Stream Cipher System's are depending on these two basic units. Figure (1) shows a simple diagram of LFSRS consists of n LFSR's.

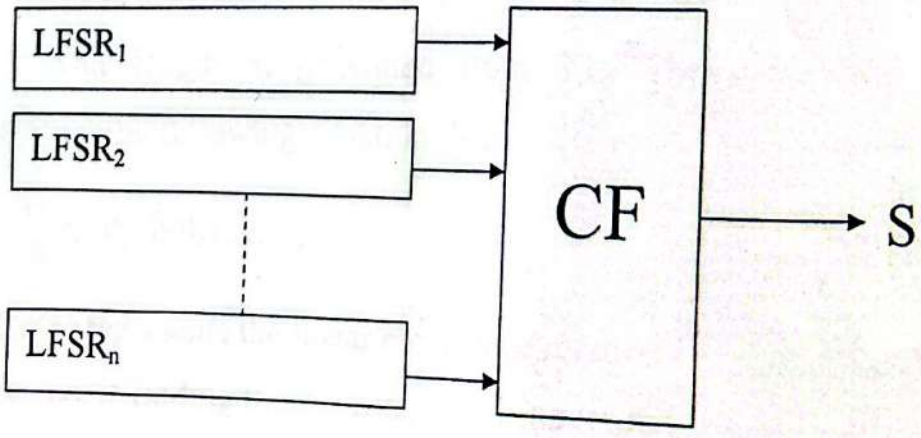

Figure (1) A system of n_LFSR's.

This paper aims to find the initial values for every LFSR in the system depending on the following information:

1. The length of every LFSR and its feedback function are known.
2. The CF is known.
3. The output sequence S (keystream) generated from the LFSRS is known, or part of it, practically, that means, a probable word attack be applied [1].

This work consists of three stages, constructing linear equations system, test the uniqueness of the solution of this system, and lastly, solving the linear equations system.

2. Constructing a Linear Equations System for Single LFSR

Before involving in solving the Linear Equations System (LES), it should show how could be the LES of a single LFSR constructed, since its considered a basic unit of LFSRS. Let's assume that all LFSR that are used are maximum LFSR, that means, Period (P)=2^r-1, where r is LFSR length.

Let SR_r be a single LFSR with length r, let $A_0=(a_{-1},a_{-2},\ldots,a_{-r})$ be the initial value vector of SR_r, s.t. a_{-j}, $1\leq j\leq r$, be the component j of the vector A_0, in another word, a_{-j} is the initial bit of stage j of SR_r, let $C_0^T=(c_1,\ldots,c_r)$ be the feedback vector, $c_j\in\{0,1\}$, if $c_j=1$ that means the stage j is connected. Let $S=\{s_i\}_{i=0}^{m-1}$ be the sequence (or $S=(s_0,s_1,\ldots,s_{m-1})$ read "S vector") with length m generated from SR_r. The generation of S depending on the following equation [3]:

$$s_i=a_i=\sum_{j=1}^{r}a_{i-j}c_j \quad i=0,1,\ldots \qquad \ldots(1)$$

Equation (1) represents the linear recurrence relation.

The objective is finding the A_0, when r, C_0 and S are known.

Let M be a r×r matrix, which is describes the initial phase of SR_r

$M=(C_0|I_{r\times r-1})$, where $M^0=I$.

Let A_1 represents the new initial of SR_r after one shift, s.t.

$$A_1=A_0\times M=(a_{-1},a_{-2},\ldots,a_{-r})\begin{pmatrix} c_1 & 1 & \cdots & 0 \\ c_2 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ c_r & 0 & \cdots & 0 \end{pmatrix}=(\sum_{j=1}^{r} a_{-j}c_j\ ,a_{-1},\ldots,a_{1-r}).$$

In general,

$A_i=A_{i-1}\times M$, i=0,1,2,… …(2)

Equation (2) can be considered as a recurrence relation, so we have:

$A_i=A_{i-1}\times M=A_{i-2}\times M^2=\ldots=A_0\times M^i$ …(3)

The matrix M^i represents the i phase of SR_r, equations (2,3) can be considered as a Markov Process s.t., A_0, is the initial probability distribution, A_i represents probability distribution and M be the transition matrix [4].

notice that:

$M^2=[C_1C_0|I_{r\times r-2}]$ and so on until get $M^i=[C_{i-1}\ldots C_0|I_{r\times r-i}]$, where $1\le i<r$.

When $C_P=C_0$ then $M^{P+1}=M$.

Now let's calculate C_i [5] s.t.

$C_i=M\times C_{i-1}$, i=1,2,… …(4)

Equation (1) can be rewritten as:

$A_0\times C_i=s_i$, i=0,1,..,r-1 …(5)

When i=0 then $A_0\times C_0=s_0$ is the 1st equation of the LES,

i=1 then $A_0\times C_1=s_1$ is the 2nd equation of the LES, and

i=r-1 then $A_0\times C_{r-1}=s_{r-1}$ is the r^{th} equation of the LES.

In general:

$A_0\times \mathbf{C}=S$

C represents the matrix of all C_i vectors s.t. …(6)

$\mathbf{C}=(C_0C_1\ldots C_{r-1})$

…(7)

The LES can be formulated as: ...(8)

$Y=[\,C^T|S^T]$

Y represents the extended matrix of the LES.

Example (1)

Let the SR_4 has $C_0{}^T=(0,0,1,1)$ and $S=(1,0,0,1)$, by using equation (4), we get:

$$C_1=M\times C_0=\begin{pmatrix}0&1&0&0\\0&0&1&0\\1&0&0&1\\1&0&0&0\end{pmatrix}\begin{pmatrix}0\\0\\1\\1\end{pmatrix}=\begin{pmatrix}0\\1\\1\\0\end{pmatrix}$$, in the same way, $C_2=\begin{pmatrix}1\\1\\0\\0\end{pmatrix}$, $C_3=\begin{pmatrix}1\\0\\1\\1\end{pmatrix}$

From equation (6) we have:

$$A_0\begin{pmatrix}0&0&1&1\\0&1&1&0\\1&1&0&1\\1&0&0&1\end{pmatrix}=(1,0,0,1)$$, this system can be written as equations:

$a_{-3}+a_{-4}=1$

$a_{-2}+a_{-3}=0$

$a_{-1}+a_{-2}=0$

$a_{-1}+a_{-3}+a_{-4}=1$

(for simplicity we can omitted the sign (-)).

Then the LES after using formula (8) is:

$$Y=\left[\begin{array}{cccc|c}0&0&1&1&1\\0&1&1&0&0\\1&1&0&0&0\\1&0&1&1&1\end{array}\right]$$ ...(9)

3. Modified Geffe Generator

3.1 Geffe Generator

The Geffe generator [5] is defined by three maximum-length LFSRs whose lengths r_1, r_2, r_3 are pair wise relatively prime, with nonlinear combining function:

$$F_3(x_1,x_2,x_3) = x_1*x_2 \oplus (1 \oplus x_2)*x_3 = x_1*x_2 \oplus x_2*x_3 \oplus x_3$$

(see figure (2)).

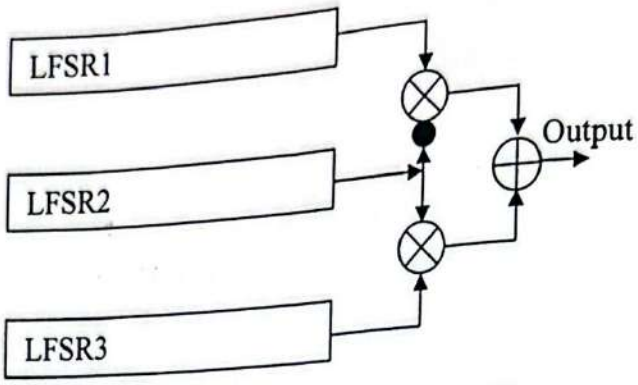

Figure (2) Geffe generator [5].

The keystream generated has period $(2^{r_1}-1)(2^{r_2}-1)(2^{r_3}-1)$ and linear complexity $LC=r_1r_2+r_2r_3+r_3$. The Geffe generator is cryptographically weak because information about the states of LFSR1 and LFSR3 leaks into the output sequence. Despite having high period and moderately high linear complexity, the Geffe generator succumbs to correlation attacks [1].

3.2 Modified Geffe Generator Description

Know we would improve this generator by choosing 5 LFSR's instead of 3 LFSR's, if the output of LFSR3 is 0 then we choose the xoring of LFSR1 and LFSR2, otherwise we choose the xoring of LFSR4 and LFSR5. The CF of this generator is:

$$F_5(x_1,x_2,x_3,x_4,x_5)=(x_1 \oplus x_2)*(x_3 \oplus 1) \oplus (x_4 \oplus x_5)*x_3 \quad \ldots(10\text{-a})$$

Or it can be written as follows:

$$F_5(x_1,x_2,x_3,x_4,x_5)=x_1 \oplus x_2 \oplus x_1x_3 \oplus x_2x_3 \oplus x_3x_4 \oplus x_3x_5 \quad \ldots(10\text{-b})$$

so we called this system Modified-Geffe generator.

3.3 Efficiency Criteria of Modified Geffe Generator

(a). Periodicity

The sequence S has period P(S) when $s_0=s_{P(S)}, s_1=s_{P(S)+1},\ldots$, the period of $LFSR_i$ denotes by $P(S_i)$, P(S) and $P(S_i)$ are least possible positive integers, so

$$P(S)=\text{lcm}(P(S_1),P(S_2),\ldots,P(S_n)) \quad \ldots(11)$$

The period of S which product from key generator depends on the LFSR unit only and there is no effect of CF unit.

P(S) will has lower bound when $r=r_i$ $\forall 1\le i\le n$, and upper bound when $P(S_i)$ are relatively prime with each other therefore $P(S_r)\le P(S)\le \prod_{i=1}^{n} P(S_i)$.

The objective is that key generator must have an upper bound to P(S) s.t.:

$$P(S)=\prod_{i=1}^{n} P(S_i) \quad \ldots(12)$$

It's known earlier that $P(S_i) \le 2^{r_i}-1$, and if the $LFSR_i$ has maximum period then $P(S_i)= 2^{r_i}-1$ [3].

Theorem (1) [6]

$P(S)=\prod_{i=1}^{n}(2^{r_i}-1)$ if and only if the following conditions are holds:

1. $GCD_n(P(S_i))=1$,.
2. the period of each LFSR has maximum period ($P(S_i)=2^{r_i}-1$).

For Modified Geffe generator $P(S)=\prod_{i=1}^{5}(2^{r_i}-1)$.

Example (2)

if r_i=2,3,…,6 for i =1,2,…,5, then:

P(S)=l.c.m(3,7,15,31,63)

$=$l.c.m($3^1.5^0.7^0.31^0$, $3^0.5^0.7^1.31^0$, $3^1.5^1.7^0.31^0$,$3^0.5^0.7^0.31^1$, $3^2.5^0.7^1.31^0$)

$= 3^{max(0,1,2)}.5^{max(0,1)}.7^{max(0,1)}.31^{max(0,1)}= 3^2.5^1.7^1.31^1=9765.$

(b). Randomness

For our purposes, a sequence generator is pseudo-random if it has this property: It looks random. This means that it passes all the statistical tests of randomness that we can find [1].

Definition (1) [1]: A random bit generator is a device or algorithm which outputs a sequence of statistically independent and unbiased binary digits.

The sequence that is satisfied the 3-randomness properties called PRS [3]. The randomness criterion depends on LFSR's and CF units, therefore from the important conditions to get Pseudo Random Sequence is, the sequence must be maximal and CF must be balance.

From the truth table of CF of modified Geffe, notice the ratio of number of 0's to the total output of the function = 32 (2^5=32) is 0.5, this mean the number of 0's = 16 and so as number of 1's, that's indicates that this generator can generates random sequence.

The truth table of CF is shown in table (1).

Table (1) Truth table of CF of Modified Geffe generator.

x_1	x_2	x_3	x_4	x_5	F_5
0	0	0	0	0	0
0	0	0	0	1	1
0	0	0	1	0	1
0	0	0	1	1	0
0	0	1	0	0	0
0	0	1	0	1	0
0	0	1	1	0	0
0	0	1	1	1	0
0	0	1	0	0	0
0	1	0	0	1	1
0	1	0	0	0	1
0	1	0	1	1	0
0	1	0	1	0	1
0	1	1	0	1	1
0	1	1	0	0	1
0	1	1	1	1	1
0	1	1	1	0	0
1	0	0	0	1	1
1	0	0	0	0	1
1	0	0	1	1	0
1	0	0	1	0	1
1	0	1	0	1	1
1	0	1	0	0	1
1	0	1	1	1	1
1	0	1	1	0	0
1	1	0	0	1	1
1	1	0	0	0	1
1	1	0	1	1	0
1	1	0	1	0	0
1	1	1	0	1	0
1	1	1	0	0	0
1	1	1	1	1	0
1	1	1	1	0	0
0.5	0.5	0.5	0.5	0.5	0.5
Correlation Probability (CP_i) for each LFSR					Ratio of "0"

Note: the shaded cells means the similarity between x_i and the output of CF.

(c). Linear Complexity

The Linear Complexity is defined as the length, of the shortest LFSR (which is equivalent LFSR) that can mimic the generator output. Any sequence generated by a finite-state machine over a finite field has a finite linear complexity [7].

Let's denotes the Linear Complexity for the generated sequence by LC(S), then it can by calculated by:

$LC(S)= r_1+r_2+r_1r_3+r_2r_3+r_3r_4+r_3r_5$.

Example (3)

Let's use the same information mentioned in example (2), then:

$LC(S)=2+3+2*4+3*4+4*5+4*6 = 69$

(d). Correlation Immunity

Correlation can be defined as the relation between the sequence of $CF=F_n$ from the key generator and the sequences that are combined each other by CF. This relation caused because of the non-linearity of the function F_n. The correlation probability CP(x), in general, represents the ratio between the number of similar binaries of two sequences to the length of the compared part of them. F_n has m^{th} order CI, if the output z of F_n is statistically independent from m output from m-sequences $(x_1,x_2,...,x_m)$, of n combined sequences s.t. $m \leq n$.

Notes from table (1) (from the shaded cells) that the number of similarity between x_i and the output of CF is 16 bits from the total number 32 bits $\forall i$, then the correlation probability (CP_i) can be calculated as:

$CP_i = 16/32 = 0.5$, for $i = 1,2,...,5$.

Let's denotes the Correlation Immunity for the generated sequence by CI(S), then it can by calculated by:

$CI(S) = 5$,

since the number of immune $x_i = 5$.

This indicates that modified Geffe generator is immune and it cannot be attacked by correlation attack or fast correlation attack, while Geffe generator is not immune [8].

4. Constructing A LES for Modified Geffe Generator

Let's have n of SR_{r_j} with length r_j, $j=1,2,\ldots,n$, with feedback vector $C_{0j}=\begin{pmatrix} c_{01j} \\ c_{02j} \\ \\ c_{0r_j j} \end{pmatrix}$, and has unknown initial value vector $A_{0j}=(a_{-1j},\ldots,a_{-rjj})$, so SR_{r_j} has $M_j=(C_{0j}|I_{r_j\times r_j-1})$

By using recurrence equation (4), ...(13)

$C_{ij}=M_j\times C_{i-1,j}$, $i=1,2,\ldots$

by using equation (5):

$A_{0j}\times C_{ij}=s_{ij}$, $i=0,1,\ldots,r-1$ and $S_j=(s_{0j},s_{1j},\ldots,s_{m-1,j})$.

S_j represents the output vector of SR_{r_j}, which of course, is unknown too.

m represents the number of variables produced from the LFSR's with consider to CF, in the same time its represents the number of equations which are be needed to solve the LES. Of course, there is n of LES (one LES for each SR_{r_j} with unknown absolute values).

Now, let A_0 be the extended vector for m variables, which consists of initial values from all LFSR's and C is the matrix of C_i vectors considering the CF, C_i represents the extended vector of all feedback vectors C_{ij}, then $A_0\times C=S$.

From CF the number of variables (m) are:

$m= r_1+r_2+r_1r_3+r_2r_3+r_3r_4+r_3r_5$.

The initial value is:

$$A_0=A_{01}+A_{02}+A_{01}A_{03}+A_{02}A_{03}+A_{03}A_{04}+A_{03}A_{05}=(x_0,x_1,\ldots,x_{m-1}),$$

s.t. $x_0=a_{-11}$, $x_1=a_{-21},\ldots,x_{m-1}=a_{-r_4,4}a_{-r_5,5}$

(this arrangement is not standard so it can be changed according to the researcher requirements).

For simplicity let's denote the unknowns of $LFSR_1$ by 'a', $LFSR_2$ by 'b', and so on, let's denote the unknowns of SR_5 by 'e', and so on, therefore:

$$x_0=a_1,\ x_1=a_2,\ldots,x_{m-1}=d_{r4}e_{r5} \quad \ldots(14)$$

In the same way, equation (14) can be applied on the feedback vector C_{ij}:

$$C_i=C_{i1}+C_{i2}+C_{i1}C_{i3}+C_{i2}C_{i3}+C_{i3}C_{i4}+C_{i3}C_{i5}$$

And the sequence S will be:

$$S=S_1+S_2+S_1S_3+S_2S_3+S_3S_4+S_3S_5,$$

s.t. $s_i=s_{i1}+s_{i2}+s_{i1}s_{i3}+s_{i2}s_{i3}+s_{i3}s_{i4}+s_{i3}s_{i5}$,

where s_i is the element i of S.

So the LES can be obtained by equation (6).

Figure (3) shows the block diagram of Modified Geffe Generator.

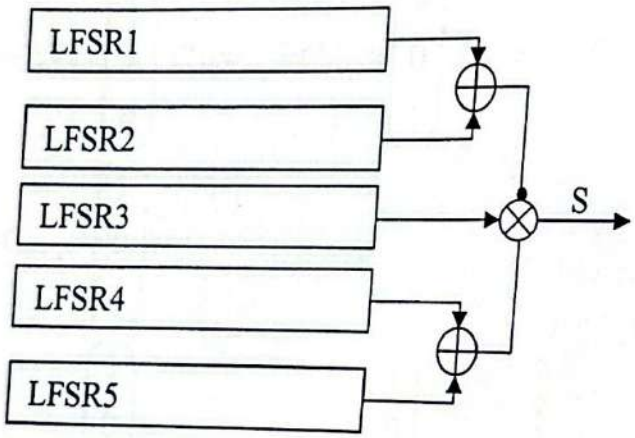

Figure (3) Block diagram Modified Geffe generator.

Example (4)

Let's have the following feedback vectors for 5 LFSR's with lengths 2,3,4,5 and 6:

$C_{01}=\begin{pmatrix}1\\1\end{pmatrix}$, $C_{02}=\begin{pmatrix}1\\0\\1\end{pmatrix}$, $C_{03}=\begin{pmatrix}1\\0\\0\\1\end{pmatrix}$, $C_{04}=\begin{pmatrix}0\\1\\0\\0\\1\end{pmatrix}$, $C_{05}=\begin{pmatrix}1\\0\\0\\0\\0\\1\end{pmatrix}$ then m=69.

Let the output sequences be:

S=(0,1,0,1,0,0,1,1,1,0,1,…,0,0,0,0,0,0,1,1,0,1,1,0,0),

$C_{01}=C_{31}=\ldots=C_{65,1}=C_{68,1}=\begin{pmatrix}1\\1\end{pmatrix}$, $C_{11}=C_{41}=\ldots=C_{63,1}=C_{66,1}=\begin{pmatrix}0\\1\end{pmatrix}$

$C_{21}=C_{51}=\ldots=C_{64,1}=C_{67,1}=\begin{pmatrix}1\\0\end{pmatrix}$.

$C_{02}=\ldots=C_{63,2}=\begin{pmatrix}1\\0\\1\end{pmatrix}$, $C_{12}=\ldots=C_{69,2}=\begin{pmatrix}1\\1\\1\end{pmatrix}$, $C_{22}=\ldots=C_{64,2}=\begin{pmatrix}0\\1\\1\end{pmatrix}$,

$C_{32}=\ldots=C_{65,2}=\begin{pmatrix}1\\1\\0\end{pmatrix}$, $C_{42}=\ldots=C_{66,2}=\begin{pmatrix}0\\0\\1\end{pmatrix}$, $C_{52}=\ldots=C_{67,2}=\begin{pmatrix}0\\1\\0\end{pmatrix}$,

$C_{62}=\ldots=C_{68,2}=\begin{pmatrix}1\\0\\0\end{pmatrix}$.

$C_{03}=\ldots=C_{65,3}=\begin{pmatrix}1\\0\\0\\1\end{pmatrix}$, $C_{13}=\ldots=C_{66,3}=\begin{pmatrix}1\\0\\1\\1\end{pmatrix}$, $C_{23}=\ldots=C_{67,3}=\begin{pmatrix}1\\1\\1\\1\end{pmatrix}$,

$C_{33}=\ldots=C_{68,3}=\begin{pmatrix}0\\1\\1\\1\end{pmatrix}$,

And so on until we get:

$$C_{12,3}=\ldots=C_{57,3}=\begin{pmatrix}0\\0\\1\\0\end{pmatrix},\ C_{13,3}=\ldots=C_{58,3}=\begin{pmatrix}0\\1\\0\\0\end{pmatrix},C_{14,3}=\ldots=C_{59,3}=\begin{pmatrix}1\\0\\0\\0\end{pmatrix}.$$

In the same process we get C_{i4} and C_{i5}, for $i=1,2,\ldots,69$.

by applying equation (4), $C_0{}^T$ will be:

$C_0{}^T=(1,1,1,0,1,1,0,0,1,0,0,0,0,1,0,0,1,\ldots,0,0,0,0,0,0,0,1,0,0,0,0,1)$.

Therefore,

$$Y=\begin{pmatrix}1\,1\,1\,0\,1\,1\,0\,0\ldots0\,0\,1\,0\,0\,0\,0\,1\,|\,0\\1\,0\,0\,1\,0\,1\,0\,0\ldots1\,1\,1\,0\,0\,0\,1\,1\,|\,1\\ \vdots\\1\,0\,0\,1\,1\,1\,1\,1\ldots0\,0\,1\,1\,1\,1\,1\,1\,|\,0\\0\,1\,1\,1\,1\,0\,0\,0\ldots1\,1\,0\,1\,1\,1\,1\,1\,|\,0\end{pmatrix} \qquad \ldots(15)$$

5. Test The Uniquness of The Solution of LES

Since the system of m variables, then there are 2^m-1 equations, but only m independent equations are needed to solve the system. If the system contains dependent equations, then the system has no unique solution. So first it should test the uniqueness of solution of the system by many ways like calculating the rank of the system matrix ($r(\mathbf{C}^T)$) or by finding the determinant of the matrix. If the rank equal the matrix degree ($deg(\mathbf{C}^T)$), then the system has unique solution, else ($r(\mathbf{C}^T)< deg(\mathbf{C}^T)$) the system has no unique solution.

In order to calculate the $r(\mathbf{C}^T)$ it has to use the elementary operations to convert the $\mathbf{C}^T$ matrix to a simplest matrix by making, as many as possible of, the matrix elements zero's. The elementary operations should be applied in the rows and columns of the matrix $\mathbf{C}^T$, if it converts to Identity matrix then $r(\mathbf{C}^T)=deg(\mathbf{C}^T)=m$, then we can judge that $\mathbf{C}^T$ has unique solution [9].

Example (5)

Let's have the matrix $C^T=\begin{pmatrix}0&0&1&1\\0&1&1&0\\1&1&0&0\\1&0&1&1\end{pmatrix}$, by using the elementary operations, the matrix can be converted to the matrix $C^{T*}=\begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&1\end{pmatrix}$, this matrix has rank =4=deg(C^T) then the matrix has unique solution.

For modified Geffe generator, we obtain that the LES has unique solution; of course we have to choose 69 independent equations not all are in sequence order.

6. Solving The LES

After be sure that the LES has unique solution, the LES can be solved by using one of the most common classical methods, its Gauss Elimination method. This method chosen since it has lower complexity than other methods. As known, this method depending in two main stages, first, converting the matrix Y to up triangular matrix, and the second one, is finding the converse solution [8]. Example (6) shows the solving of a single LES for one LFSR.

Example (6)

Let's use the matrix Y of equation (9), after applying the elementary operations, and then the up triangular matrix is:

$$Y' = \left[\begin{array}{cccc|c}1&1&0&0&0\\0&1&1&0&0\\0&0&1&1&1\\0&0&0&1&1\end{array}\right]$$

Now applying the backward solution to get the initial value vector:

$A_0=(0,0,0,1)$.

The LES of 5_LFSR's is more complicated than LES of a single LFSR, specially, if the CF is high order (non-linear) function. First, it should solve the variables which are consists of multiplying more than one initial variable bits of the combined LFSR's.

As an example of modified Geffe generator, its going to solve the variables d_k, $1\le k\le m-1$, then solving the initial values a_{-ij} since x_k is represented by multiplying three initial bits in 10 terms, and four initial bits in 5 terms. In another word, every system has its own LES system because of the CF, so it has own solving method.

As an example to find the variables a_{-ij} of modified Geffe generator, after solving the LES we found that 91 variables (x_k) equal (1) from the whole number of variables, s.t.:

$x_0=x_2=x_3=0$, $x_1=x_4=x_{12}=x_{24}=x_{44}=x_{68}=1$.

From equation (14), we know that every x_k is consists from product of (3) or (4) unknowns, where a_i,b_j,c_k,d_l,e_n are initial values the five LFSR's contribute in 5-modified Geffe generator s.t. i=1,2,3,4,5. The LES system Y which mentioned in example (4) will be solved in the next example.

Example (7)

$x_0=a_1=0$, $x_1=a_2=1$, $x_2=b_1=0$, $x_3=b_2=0$, $x_4=b_3=1$, and $x_{24}=c_4*d_5=1$, this means $c_4=d_5=1$ and so on until we found all the initial values of all LFSR's contribute the modified Geffe generator. After applying the above process we get:

- $A_{01}=(a_1,a_2)=(a_{-11},a_{-21})=(0,1)$.
- $A_{02}=(b_1,b_2,b_3)=(a_{-12},a_{-22},a_{-32})=(0,0,1)$.
- $A_{03}=(c_1,c_2,c_3,c_4)=(a_{-13},a_{-23},a_{-33},a_{-43})=(0,0,0,1)$.
- $A_{04}=(d_1,d_2,d_3,d_4,d_5)=(a_{-14},a_{-24},a_{-34},a_{-44},a_{-54})=(0,0,0,0,1)$.
- $A_{05}=(e_1,e_2,e_3,e_4,e_5,e_6)=(a_{-15},a_{-25},a_{-35},a_{-45},a_{-55},a_{-65})=(0,0,0,0,0,1)$.

7. Conclusions

1. If we change our attack from known plain attack to cipher attack only, which means, changing in the sequence S (non-pure absolute values), so we shall find a new technique to isolate the right equations in order to solve the LES.
2. It is not hard to construct a LES of any other LFSR systems; of course, we have to know all the necessary information (CF, the number of combined LFSR's and their lengths and tapping).
3. Notice that m(=69) is may larger because of the non-linearity of the combining function CF (majority function), and because of changing the non-linear variables to new variables, so we think that it can keep m as number of non-linear variables and solving the non-linear system by using direct methods after applying the suitable modifying.

References

[1]. Schneier, B., "***Applied Cryptography (Protocol, Algorithms and Source Code in C***", Second Edition, John Wiley & Sons Inc. 1997.

[2]. Victor Shoup, "***A Computational Introduction to Number Theory and Algebra***", (Version 1), Cambridge University Press, 2005.

[3]. Golomb, S.W., "***Shift Register Sequences***" San Francisco: Holden Day 1967, Reprinted by Aegean Park Press in 1982.

[4]. Papoulis, A. "***Probability Random Variables, and Stochastic Process***", McGraw-Hill College, October, 2001.

[5]. Geffe, P. R., "***How to Protect Data with Ciphers that are Really Hard to Break***", Electronics pp. 99-101, Jan. 4, 1973.

[6]. Al-Shammari, A. G., "***Mathematical Modeling and Analysis Technique of Stream Cipher Cryptosystems***", Ph. D. Thesis, University of Technology, Applied Sciences, 2009.

[7]. Massey, J. L., "***Cryptography and System Theory***", Proceedings of the 24th Allerton Conference on Communication, Control, and Computers, 1-3 Oct. 1986.

[8]. Siegenthaler, T., "***Correlation-Immunity of Nonlinear Combining Functions for Cryptographic Applications***", IEEE Transactions on Information Theory, v. IT-30, n. 5, pp. 776-780, Sep. 1984.

[9]. Jaan Kiusalaas, "***Numerical Methods in Engineering with MATLAB***", Cambridge University Press, 2005.