تطوير السرية في نظام التشفير الانسيابي اللاخطي من نوعAdder

حميد عبد الكريم يونس

قسم علوم الحاسبات-كلية العلوم-جامعة البصرة-البصرة-العراق.

ISSN-1817-2695

(الاستلام 2005/8/28 ، القبول 2005/11/21)

المستخلص: Abstract

قوة نظام التشفير الانسيابي تعتمد على قوة مولد المفتاح الذي ينتج سلسلة شبة عشوائية. إن المولد يولد سلسلة شبة عشوائية التي تنجح في عدد من الاختبارات. ونظام التشفير الانسيابي اللاخطي الذي يعتمد على الدالة Adder له عدد من نقاط الضعف غير المرغوبة تؤدي به إلى الفشل بمواجهة الاختبارات العشوائية ونجاح نسبي في هجوم الارتباط. في هذا البحث تم تطوير الدالة Adder بإضافة مسجل إزاحة ثالث لتحسين قدرته على تجاوز الاختبارات العشوائية. بالإضافة إلى زيادة التعقيد اللاخطي للسلسلة المتولدة ويكون مقاوماً لكسر الشفرة باستعمال هجوم الارتباط.

الكلمات المفاتيح: Keywords

Stream cipher, Adder generator, Non-linear-feedback shift registers, Correlation attack, Measure of randomness.

1. *المقدمة: Introduction*

تعدّ أنظمة التشفير الانسيابي أحد أنواع أنظمة التشفير الحديثة المهمة جدا التي تستعمل مفتاحاً سرياً في عمليتي التشفير وفك الشفرة[5]. تمتاز هذه الأنظمة بأنها الأكثر شيوعا واستعمالاً في مجال التشفير في الوقت الحاضر لما لها من خصائص مهمة، منها عدم تزايد الأغلاط في حالة وقوعها وسهولة إستعمالها في التطبيقات العملية، فضلاً عن سرعة تنفيذها. إن أمنية نظام التشفير الانسيابي تعتمد على الخوارزمية المستعملة في توليد سلسلة متتابعة المفتاح. وبما أنه توجد خوارزمية محددة لتوليد متتابعة المفتاح ، فتكون هذه السلسلة دوريه، لذلك تكون شبه عشوائية وليست عشوائية تماما[1] .

2. *درجة سرية أنظمة التشفير الانسيابي: Security Degree of Stream Cipher Systems*

بما أن درجة سرية نظام التشفير الانسيابي تعتمد على متتابعة المفتاح ، لذلك فإن هذه المتتابعة يجب أن تتميز ببعض الصفات التي تحقق درجة سرية عالية وهي:

- لها خصائص جيدة، وذلك للقضاء على الخصائص اللغوية التي يمتلكها النص الصريح ويمكن أن تكون مفيدة عند كسر الشفرة، بحيث أن هذه الخصائص لا تنعكس على النص المشفر، واذا كان هناك تكرار في النص الصريح فسوف يختفي في النص المشفر لأنه سيشفر بشكل مختلف باستعمال أجزاء مختلفة من متتابعة المفتاح. لهذا السبب يفضل استعمال التشفير الانسيابي في المجالات التي تشهد تكرارا في البيانات مثل الاتصالات الصوتية[3].
- لها تعقيد خطي كبير ، وهذا يؤدي إلى معرفة جزء من متتابعة المفتاح لا يفيد المهاجم في معرفة بقيتها ، وذلك عند معرفة المهاجم بالنص الصريح المقابل إلى كميه معينة من النص المشفر، لذلك كلما كان التعقيد الخطي كبير حصلنا على درجة سرية أكبر . أما التعقيد الخطي لسلسلة فيعرف على أنه طول أقصر مسجل أزاحه ذو دالة تغذية مرتدة خطية يقوم بتوليد هذه السلسلة.

هذه الخصائص نحصل عليها عندما تكون متتابعة المفتاح عشوائية. لكن متتابعة المفتاح المتولد في نظام التشفير الانسيابي الجيد تكون شبه عشوائية وليست عشوائية تماما لكونها سلسلة دورية, لذلك كلما كان طول الدورة كبير كان أفضل ، ويفضل أن يكون أكبر من طول الرسالة.

2.1 الاختبارات الإحصائية للعشوائية:Random Tests

إن السلسلة العشوائية تمتلك صفات إحصائية معروفة، مما أدى إلي ظهور عدة اختبارات لفحص العشوائية التي من خلالها يمكننا اختبار مدى عشوائية متتابعة المفتاح .

هنالك العديد من الاختبارات لفحص مدى عشوائية السلسلة الثنائية والتي تسمى اختبارات العشوائية المحلية(Local random tests) لكونها تختبر مقطعاً واحداً (دورة واحدة) من السلسلة الثنائية. في البداية يجب تحديد درجة النجاح والفشل للاختبارات لذلك تم استعمال قيم إحصائية تخصص للسلاسل العشوائية عدت درجة النجاح 95% التي تكون

مساوية إلى%(1- α)=%(100-5) حيث α تسمى المستوى المميز للاختبار ويكون الاختبار ناجحا عندما تكون قيمته أقل أو مساوية إلى قيمة مربع كاي Chi- square حيث يمثل القيمة الجد ولية عند المستوى المميز α % لتوزيع مربع كاي Chi- square . أما الاختبارات العشوائية فهي[1]:

اختبار التردد Frequency test
اختبار التسلسل Serial test
اختبار بوكر Poker test
اختبار الجريان Run test

2.2 هجوم الإرتباط: Correlation Attack

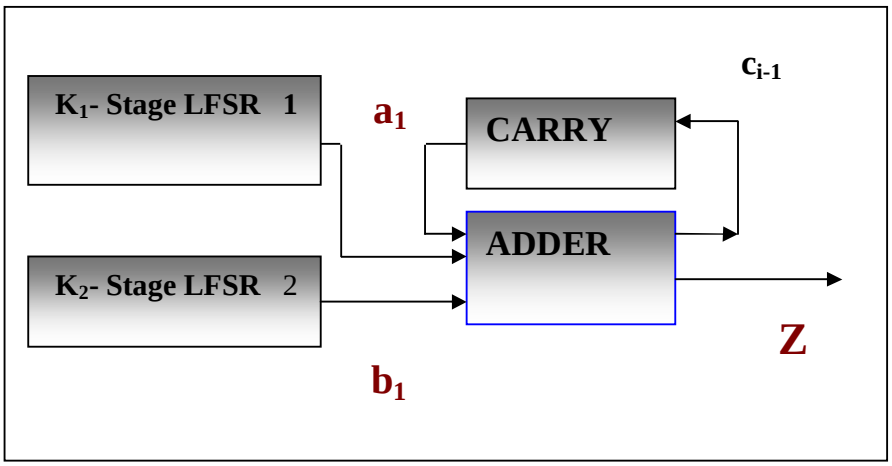
يستعمل هذا الأسلوب لمهاجمة أنظمة التشفير الانسيابي اللاخطية المستندة إلى التوحيد اللاخطي لعدد من مسجلات الإزاحة الخطية, والذي يتطلب معرفة النص المشفر فقط من دون الحاجة إلى معرفة النص المقابل[4].

في عام 1985 أظهرت البحوث وجود نقطة ضعف في هذا النوع من الأنظمة وهي وجود ارتباط بين جزء من مدخلات الدالة اللاخطية(مخرجات مسجلات الإزاحة الخطية) وبين متتابعة المفتاح المتولدة Z. بالاستناد إلى هذا الارتباط أصبح من الممكن معرفة بعض من مسجلات الإزاحة الخطية والتي تعد جزءاً من مفتاح النظام والتي سميت بهجوم الارتباط. وهذا يعني التقليل من عدد المحاولات لإيجاد مفتاح النظام عند وجود ارتباط بين مدخلات ومخرجات الدالة اللاخطية التي استعملت في تجميع مخرجات مسجلات الإزاحة الخطية, حيث يمكن معرفة كل مسجل خطي بشكل مستقل عن بقية المسجلات.

2. نظام المولدAdder:

يعد نظام المولد Adder احد أنظمة التشفير الانسيابي اللاخطي[2] حيث يولد سلسلة شبة عشوائية بالاعتماد على الجامع Adder . يتكون هذا النظام من :

1- مسجلي إزاحة كل واحد منها ذو دالة تغذية مرتدة خطيه تعطي أعظم دورة ذات أطوال K1,K2 بحيث K1<>K2 & GCD(K1,K2)=1.
حيث أن k1=Length(LFSR1) و k2=Length(LFSR2)
2- دالة الربط المستعملة بين مخرجات مسجلي الإزاحة هي دالة الجامع Adder الموضحة في الشكل (1).
3- تكون التكلفة المادية للمولد بسيطة.



شكل (1) خوارزمية الجامع (adder)

من الواضح ويظهر في الشكل أن مولد المفاتيح نوع الجامع (Adder) يتكون من مسجلي إزاحة وبأطوال k1 , k2 على التوالي ، ودالتين تغذيه مرتدة ، و دالة ربط الـ(Adder) ، والـ Carry ويكون ناتج هذا كله هي سلسله شبه عشوائية وهي التي نعني بها (متتابعة المفتاح) Z .

3.1 استراتيجية عمل المولدAdder:

تتمركز إستراتيجية عمل مولد الجامع (Adder) في توليد متتابعة المفتاح (سلسلة شبه عشوائية)، التي هي بطول $(2^{k_1}-1).(2^{k_2}-1)$ ، وتكون ناتجة من إدخال قيمة المسجلين LFSR1, LFSR2 الابتدائية ودوا لهما المرتدة ، وبعد أجراء العديد من العمليات منها التزحيف وعملية الجمع بمعيار 2 (XOR).

المعادلة الرياضية المستعملة في أيجاد السلسلة Z_i من دالة الربط (Adder) هي:

$$Z_i=a_i+b_i+c_{i-1}$$
$$c_i=a_ib_i+(a_i+b_i)\,c_{i-1}$$

إذ أن b_i , a_i هما عنصران تسلسلهما $1<i<(2^{k_1}-1).(2^{k_2}-1)$ في السلسلة b1 , a1 بالتعاقب ومن الواضح انهما معادلات لاخطية، حيث a_i , b_i , c_{i-1} عبارة عن متعددات حدود غير ثابتة.

3.2 مساوئ المولد Adder

يمكن أيجاز مساوئ المولد (Adder) في شيئين هما

1. الأول وهو عدم العشوائية التامة وهذا يمكن عده من المساوئ العامة لنظام التشفير الانسيابي اللاخطي.
2. الثاني وهو إمكانية مهاجمة النظام وكسر الشفرة. وذلك من خلال معرفتنا لجزءاً من السلسلة Z ومنها يمكن معرفة بعض أجزاء مخرجات المسجلين ، ومنها معرفة مسجلي الإزاحة. من هنا جاءت فكرة تطوير المولد Adder والوصول الى مولد جديد قد يتعدى هذا الضعف وهو مولد Adder المطوّر.

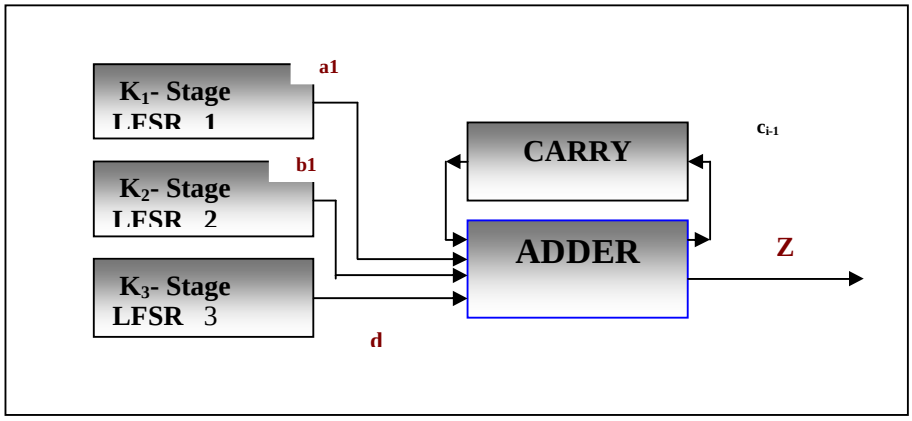
4. نظام المولد Adder المطوّر:

لا يوجد اختلاف كبير في مكونات مولد الجامع ذي ثلاثة مسجلات إزاحة عن السابق ذي المسجلين فقط وانما توجد اختلافات بسيطة منها :

1- يتكون مولد المفاتيح Adder المطور من ثلاثة مسجلات إزاحة كل مسجل لديه داله تغذيه مرتدة خطيه تعطي أعظم دوره وذات أطوال K1, K2 ,k3، وان GCD(K1,K2,k3)= 1

اذ أن k1=Length(LFSR1) و k2=Length(LFSR2) و k3=Length(LFSR3)

2- يتكون أيضا من دالة Adder والCarry كما موضح في الشكل (2).



شكل(2) مولد المفاتيح ADDER المطوّر

5.التجارب والنتائج: Experiments and Results

أجرينا العديد من التجارب على سلاسل متتابعة المفتاح المتولدة للمولد Adder والمولد Adder المطوّر.

تجربة(1):

أجريت الاختبارات الإحصائية العشوائية على العديد من قيم المفاتيح (القيم الابتدائية للمسجلات ودوال التغذية المرتدة) على المولدين كليهما وحصلنا في المولد Adder على النتائج الآتية: (الجدول (1) يبين النتائج).

الجدول(1) (الاختبارات الإحصائية للعشوائية للسلسلة الناتجة من Adder)

	المفاتيح		خوارزمية Adder			
	القيمة الابتدائية	دالة التغذية	الاختبارات الإحصائية للسلسلة			
			التردد	التسلسل	بوكر	الجريان
1	01	11	1.2	3	3.8	T0=24.2 T1=7.22
	101	11	√	√	√	x
2	101	110	2	1.83	5.93	T0=8.2 T1=24.2
	0011	11	√	√	√	x

فيما حصلنا في المولد Adder المطوّر على النتائج الاتية: (الجدول (2) يبين النتائج).

جدول(2) الاختبارات الإحصائية لعشوائية السلسلة المتولدة من Adder المطوّر

	المفاتيح		خوارزمية Adder المطوّر			
	القيمة الابتدائية	دالة التغذية	الاختبارات الإحصائية للسلسلة			
			التردد	التسلسل	بوكر	الجريان
1	01	11	0.359	1.756	15.689	T0=7.54 T1=4.28
	101	11				
	011	11	√	√	√	√
2	11111	110	0.071	0.054	10.6	T0=1.78 T1=1.04
	111	11				
	11	11	√	√	√	√

يتبين لنا من ملاحظة الجدولين أن اجتياز الاختبارات في نظام Adder المطوّر يكون أفضل من نظام Adder السابق. المولد الأول فشل في اجتياز اختبار الجريان بينما اجتاز المولد المطوّر هذا الاختبار بنجاح.

تجربة(2):

اعتمدت آلية التطوير للمولد Adder على زيادة السرية من خلال زيادة درجة مناعة الارتباط للسلسلة المتولدة من المولد Adder . إذ أن السلسلة الناتجة من تأثير أي من المولدات التي تستعمل تقنية (التوحيد اللاخطي لمسجلات إزاحة خطية)، يكون فيها من الضعف وجود ارتباط أو إعتمادية بين السلسلة المتولد Z وبعض مخرجات مسجلات الإزاحة الخطية. سوف نوضح في هذا المثال سلسله ناتجة من المولد ونتعرف على جزء منها . ومنها نحاول التعرف على بعض مخرجات مسجلي الإزاحة(LFSR1,LFSR2).

ومن الواضح أنه إذا تم التعرف على مخرجات المسجلين يمكن معرفة أطوال المسجلين وقيمتهما، وبهذا نكون قد كسرنا النظام وهاجمناه.

في التجربة الاتية سنوضح بمثال للسلسلة المتولدة من المولد Adder والسلسلة المتولدة من المولد Adder المطوّر وكلا السلسلتين لهما قيم مسجلي ودوال التغذية المرتدة الخطية نفسها وسنوضح قوة السلسلة المتولدة من المولد Adder المطوّر مقارنة مع السلسلة المتولدة من المولد Adder.

أفرض أن القيمة الابتدائية لمسجلي الإزاحة هي على التوالي (111,11)، دوال التغذية لكل مسجل هي

على التوالي $F(S0,S1)=S0 \oplus S1$ ، $F(S0,S1,S2)=S0 \oplus S1$

وأن $\oplus$ تعني دالة الجمع بمعيار 2 (XOR) .

بعد تنفيذ كلا المولدين لإنتاج السلاسل تبين ماياتي:

---- في المولد Adder السلسلة المتولدة هي

Z= 011001011000101011011

وبطول $(2^2-1)(2^3-1)$ = **21**

وبعد تطبيق

$Q_r=0, Q_{r+1}=0 \longrightarrow a_{r+1}=0$
$Q_r=0, Q_{r+1}=1 \longrightarrow a_{r+1}=1$
$Q_r=0, Q_{r+1}=0 \longrightarrow b_{r+1}=0$
$Q_r=0, Q_{r+1}=1 \longrightarrow b_{r+1}=0$

يمكننا معرفة بعض من مخرجات مسجلي الإزاحة. وبهذا تكون مهاجمته ممكنة و يؤدي إلى كسر النظام وكسر الشفرة.

--- في المولد Adder المطوّر

بإضافة مسجل ثالث (11111) ذي دالة تغذية مرتدة $F(S0,S1,S2,S3,S4)=S0 \oplus S1 \oplus S3$

كانت السلسلة المتولدة هي

Z=00101100101101100100 1……

وبطول **651=** $(2^2-1)(2^3-1)(2^5-1)$

وبتطبيق

$Q_r=0, Q_{r+1}=0 \longrightarrow a_{r+1}=0$
$Q_r=0, Q_{r+1}=1 \longrightarrow a_{r+1}=1$
$Q_r=0, Q_{r+1}=0 \longrightarrow b_{r+1}=0$
$Q_r=0, Q_{r+1}=1 \longrightarrow b_{r+1}=0$

لا يمكننا ببساطة اكتشاف مخرجات مسجلي الإزاحة ولا بعضها وذلك للتعقيد الخطي الذي أجريناه على المولد(Adder). مما زاد في تعقيد السلسلة .(هذا يعني تغير في سلوكيات المولد Adder) كما وضحنا سابقا.

يتبين لنا من هذة التجربة إن هجوم الارتباط قد فشل في الحصول على متسلسلة المفتاح وكسر الشفرة في نظام Adder المطوّر مقارنة نظام Adder السابق.

6.الاستنتاج: *Conclusion*

في هذا البحث تم تطوير فكرة المولد Adder والوصول إلى مولد مطوّر يتعدى الضعف الموجود في المولد السابق ويجعلة ذا سرية اكبر ومقاومة قوية أمام المهاجمين. وقد كان ذلك في تجاوز الاختبارات العشوائية للمولد وكذلك زيادة مناعة الارتباط. وتم تطبيق العديد من السلاسل على نظام Adder المطوّر وتم الحصول على نتائج جيدة.

المصادر: *References*

1. **Carter G.**, "***Statistical Tests for Randomness***", EISS, England,1989.
2. **Ruppel R. A.**, "***Analysis and Design of Stream Ciphers***", Springer-Verlay, Berlin, Heidelberg, 1986.
3. **Schneier B.**, "***Applied Cryptography Second Edition: Protocols, Algorithms, and Source Code in C***", John Wiley and Sons, Inc., USA, 1996.
4. **Staffelbach O.**, "***Correlation Attacks on Stream Cipher***", GRETAG aktiengesellschaft althardstr. 70, CH-8105, Regensdorf, Switzerland, 1985.
5. **Stallings W.**, "***Cryptography and Network Security***", Pearson Edition, Inc., USA, 2003.

Develop Security of Non-linear Stream Cipher System Based on Adder

H. A. Younis

Dept. of Computer Science, College of Science, University of Basrah, Basrah, Iraq.

Abstract

The strength of stream cipher system depends on the strength of keystream generator. The generator generates pseudo-random-sequence which passes randomness tests. Non-linear stream cipher based on Adder has a number of shortages. This weakness is failure of randomness tests and success of correlation attacks. In this paper, Adder is developed by inserting a third shift register. It leads to improve the generator to pass randomness tests. Also, the non-linear complexity is increased and correlation attack is faced.

Keywords: Stream cipher, Adder generator , Non-linear-feedback shift registers, Correlation attack, Measure of randomness.