تطوير السرية في نظام التشفير الانسيابي اللاخطي من نوع J-K

حميد عبد الكريم يونس انور صالح سليمان

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

الملخص

قوة نظام التشفير الانسيابي تعتمد على قوة مولد المفتاح والذي ينتج سلسلة شبة عشوائية ذات خصائص عشوائية. إن مولد التشفير الانسيابي اللاخطي من نوعJ-K فيه العديد من نقـاط الضعف في تجاوز الاختبارات العشوائية وكذلك الدالة اللاخطية J-K ذات درجة غير مناسـبة لمناعة الارتباط عند مهاجمته باستخدام هجوم الارتباط. في هذا البحث تم تطـوير نظـام J-K بإدخال دوال منطقية إضافية إليه لتحسين قدرته على تجاوز الاختبارات العشوائية مما يؤدي إلى زيادة التعقيد اللاخطي للسلسلة المتولدة ويكون مقاوم لكسر الشفرة باستخدام هجوم الارتباط.

الكلمات المفاتيح:

Stream cipher, J-K flip-flops, Non-linear-feedback shift registers, Correlation attack, Measure of randomness.

Develop Security of Non-linear Stream Cipher System Based on J-K flip-flops

Hameed A. Younis and Anwar S. Sleman

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

Abstract

The strong eof stream cipher system depends on the strong of keystream generator. The generator generates pseudo-random-sequence which it passes randomness tests. Non-linear stream cipher based on J-K flip-flops has a number of shortages. This shortage is failure of randomness tests and success of correlation attacks. In this papers, J-K flip-flops is developed by inserting additional logic functions. 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, J-K flip-flops, Non-linear-feedback shift registers, Correlation attack, Measure of randomness.

المقدمة

تعتبر أنظمة التشفير الانسيابي أحد أنواع أنظمة التشفير الحديثة المهمة جدا التي تستخدم مفتاح سري في عمليتي التشفير وفك الشفرة[Stallings W., 2003]. تمتاز هذه الأنظمة بأنها الأنظمة الأكثر شيوعا واستخداما في مجال التشفير في الوقت الحاضر لما لها من خصائص مهمة، منها عدم تزايد الأخطاء في حالة وقوعها وسهولة استخدامها في التطبيقات العملية، بالإضافة إلى سرعة تنفيذها. أن أمنية نظام التشفير الانسيابي تعتمد الخوارزمية المستخدمة في توليد سلسلة متتابعة المفتاح. بما أنه توجد خوارزمية محددة لتوليد متتابعة المفتاح ، تكون هذه السلسلة دوريه، لذلك تكون شبه عشوائية وليست عشوائية تماما.

درجة سرية أنظمة التشفير الانسيابي

Security Degree of Stream Cipher Systems

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

لها خصائص جيدة، وذلك للقضاء على الخصائص اللغوية التي يمتلكها النص الصريح والتي يمكن أن تكون مفيدة عند كسر الشفرة، بحيث أن هذه الخصائص لا تنعكس على النص المشفر، وإذا كان هناك تكرار في النص الصريح سوف يختفي في النص المشفر وذلك لأنه سوف يشفر بشكل مختلف باستخدام أجزاء مختلفة من متتابعة المفتاح . لهذا السبب يفضل استخدام التشفير الانسيابي في المجالات التي تشهد تكرارا في البيانات مثل الاتصالات الصوتية [Schneier B., 1996].

لها تعقيد خطي كبير ، وهذا يؤدي إلي أن معرفة جزء من متتابعة المفتاح لا يفيد المهاجم في معرفة بقيتها ، وذلك عند معرفة المهاجم بالنص الصريح المقابل إلي كميه معينة من النص المشفر، لذلك

كلما كان التعقيد الخطي كبير كلما 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 المتولدة في نظام التشفير الانسيابي الجيد تكون شبه عشوائية وليست عشوائية تماما لكونها سلسلة دورية, لذلك كلما كان طول الدورة كبير كلما كان أفضل ، ويفضل أن يكون أكبر من طول الرسالة.

- **الاختبارات الإحصائية للعشوائية**:Random Tests

إن السلسلة العشوائية تمتلك صفات إحصائية معروفة، مما أدى إلي ظهور عـدة اختبـارات لفحص العشوائية التي من خلالها يمكننا اختبار مدى عشوائية متتابعة المفتاح .
هنالك العديد من الاختبارات لفحص مدى عشوائية السلسلة الثنائية والتـي تسـمى اختبـارات العشوائية المحلية(Local random tests) لكونها تختبر مقطع واحـد (دورة واحـدة) مـن السلسلة الثنائية. في البداية يجب تحديد درجة النجاح والفشل للاختبارات لذلك تم استخدام قـيم إحصائية تخصص للسلاسل العشوائية اعتبرت درجة النجاح على أنهـا 95% والتـي تكـون مساوية إلى
%(1-α)=%(100-5) حيث α تسمى المستوى المميز للاختبار . يكون الاختبار ناجحا عندما تكون قيمته أقل أو مساوية إلى قيمة مربع كاي Chi- square حيث يمثل القيمة الجـد وليـة عند المستوى المميز α % لتوزيع مربع كاي Chi- square . أما الاختبـارات العشـوائية فهي[Carter G., 1989]:

اختبار التردد Frequency test
اختبار التسلسل Serial test
اختبار بوكر Poker test
اختبار التطابق الذاتي Auto correlation test

- **هجوم الارتباط:** Correlation Attack

يستخدم هذا الأسلوب لمهاجمة أنظمة التشفير الانسيابي اللاخطية المستندة علـى التوحيـد اللاخطي لعدد من مسجلات الإزاحة الخطية, والذي يتطلب معرفة الـنص المشـفر فقـط دون الحاجة إلى معرفة النص المقابل[Staffelbach O.,1985].

في عام 1985 أظهرت البحوث وجود نقطة ضعف في هذا النوع من الأنظمة وهي وجود ارتباط بين جزء من مدخلات الدالة اللاخطية(مخرجات مسجلات الإزاحـة الخطيـة) وبـين متتابعة المفتاح المتولدة Z. بالاستناد على هذا الارتباط أصبح من الممكن معرفة بعـض مـن مسجلات الإزاحة الخطية والتي تعتبر جزء من مفتاح النظام والتي سميت بهجـوم الارتبـاط. وهذا يعني التقليل من عدد المحاولات لإيجاد مفتاح النظام عند وجود ارتبـاط بـين مـدخلات ومخرجات الدالة اللاخطية التي استخدمت في تجميع مخرجات مسجلات الإزاحة الخطية, حيث يمكن معرفة كل مسجل خطي بشكل مستقل عن بقية المسجلات.

نظام المولد J-K

يتكون هذا النظام من [Rubin F.,1979]

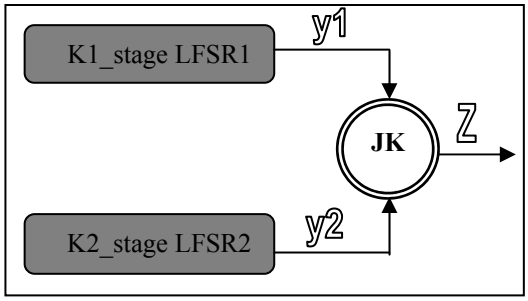
1- مسجلي إزاحة كل واحد منها ذو دالة تغذية مرتدة خطيه تعطي أعظم دورة وذات أطـوال K1,K2 بحيث K1<>K2 & GCD(K1,K2)=1.

حيث أن:

k1=Length(LFSR2) و k1=Length(LFSR1)

2- دالة الربط المستخدمة بين مخرجات مسجلي الإزاحة هي الدالة J-K كما في الشكل (1).

الجدول (1) يوضح جدول الحقيقة لهذه الدالة.



شكل(1)

Y_1	Y_2	Q_n
0	0	Q_{n-1}
0	1	0
1	0	1
1	1	Q_{n-1}

جدول (1)

جدول الحقيقة للنطاط(J-K)

خوارزمية النطاط (J-K)

فأن المولد يتكون من مسجلي إزاحة وبأطوال k1 , k2 على التـوالي ، ودالتـين تغذيه مرتدة ، دالة ربط (J-K) ، ويكون ناتج كل هذا هي سلسله شبه عشوائية والتي نعنـي بها (متتابعة المفتاح) Z.

- **إستراتيجية عمل المولد J-K**

تتمحور إستراتيجية عمل المولد (J-K) في توليد متتابعة المفتاح (سلسلة شبه عشوائية) ، والذي هو بطول (2k1-1)(2k2-1)، والذي هو ناتج عن من إدخال قيمة المسجلين الابتدائية ودوا لهما المرتدة ، وبعد أجراء العديد من العمليات منها التزحيف وعملية الجمع بمعيار 2 (Xor).

المعادلة الرياضية المستخدمة في أيجاد السلسلة Z والتي هي Qn من دالة الربط (J-K) هي:

$$Q_n=(a_n \oplus b_n \oplus 1)Q_{n-1} \oplus a_n$$

حيث أن an، bn هما عنصران تسلسلهما n في السلسلة y1، y2 بالتعاقب ، وأن $\oplus$ تعني دالة الجمع بمعيار 2 (XOR) .

$$Q_0=a_0 \oplus \oplus \oplus$$

$$Q_1=(a_1 \oplus b_1 \oplus 1)a_0 \oplus a_1 \oplus \oplus \oplus$$

$$Q_2=(a_2 \quad b_2 \quad 1)[(a_1 \quad b_1 \quad 1)a_0 \quad a_1] \quad a_2$$

والتي من الواضح أنها معادلات لا خطية.

- **مساؤي المولد J-K**

يمكن أيجاز مساؤي المولد(J-K) في شيئين هما

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

- **نظام مولد J-K المطوّر**

يتكون هذا النظام من:

1- مسجلي إزاحة كل واحد منهما ذو داله تغذيه مرتدة خطيه تعطي أعظم دوره وذات أط ـ وال

GCD(K1,K2)= 1 ، K1 , K2

2- حيث أن k1=length(LFSR1) و k1=length(LFSR2)

3- دالة الربط الأولى(F): وهي عبارة عن دالة النطاط J-K كما موضح سابقاً في شكل (1).

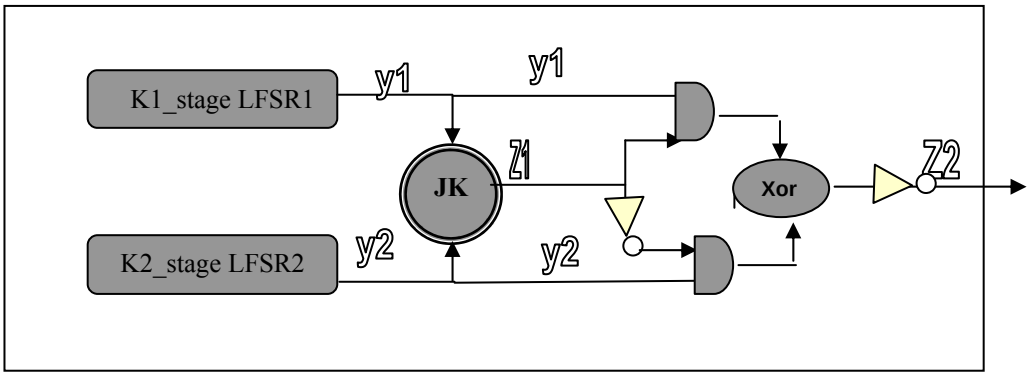
4- دالة بوليا نية تتكون من:

- دالتي الربط (AND).

- دالتي النفي المكمل (NOT) .

- دالة الجمع بمعيار 2 (XOR).

والشكل (2) يوضح دالة الربط في المولد J-K المطوّر



شكل(2) مولد المفاتيح J-K المطوّر

*** لاحظ عملية التوليد المرحلي للسلسلة Z1 ثم السلسلة Z2.

التجارب والنتائج: Experiments and Results

لقد أجرينا العديد من التجارب على سلاسل متتابعة المفتاح المتولدة للمولد J-K والمولد J-K المطوّر.

تجربة(1):

أجريت الاختبارات الإحصائية العشوائية على العديد من قيم المفاتيح (القيم الابتدائية للمسجلات ودوال التغذية المرتدة) على كلا المولدين وحصلنا في المولد J-K على النتائج التالية: (الجدول (2) يبين النتائج).

وكانت الاختبارات التي فحصت السلسلة هي:-

1- اختبار التردد Frequency test
2- اختبار التسلسل Serial test
3- اختبار بوكر Poker test
4- اختبار التطابق Auto correlation test

	المفاتيح		خوارزمية J-K			
	القيمة الابتدائية	دالة التغذية	الاختبارات الإحصائية للسلسلة			
			التردد	**التسلسل**	***بوكر***	**التطابق الذاتي**
1	0101	011	2.1428	4.087	327	9
	111	110	√	√	x	x
2	110	110	4.761	3.152	30	3
	10	11	x	√	√	√

الجدول(2) (الاختبارات الإحصائية للعشوائية للسلسلة الناتجة من J-K)

فيما حصلنا في المولد J-K المطوّر على النتائج التالية: (الجدول (3) يبين النتائج).

	المفاتيح	خوارزمية J-K المطوّر

	القيمة الابتدائية	دالة التغذية	الاختبارات الإحصائية للسلسلة			
			التردد	التسلسل	بوكر	التطابق الذاتي
1	0101	011	2.1428	4.087	283	2
	111	110	√	√	√	√
2	110	110	1.6095	5.005	109	2
	10	11	√	√	√	√

جدول(3) الاختبارات الإحصائية لعشوائية السلسلة المتولدة من J-K المطوّر

يتبين لنا من ملاحظة الجدولين إن اجتياز الاختبارات في نظام J-K المطوّر يكون أفضل من نظام J-K السابق.

تجربة(2):

اعتمدت آلية التطوير للمولد J-K على زيادة السرية من خلال زيادة درجة مناعة الارتباط للسلسلة المتولدة من المولد J-K . حيث أن السلسلة الناتجة من تأثير أي من المولدات التي تستخدم 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 التالية سوف نوضح بمثال للسلسلة متولدة من المولد J-K والسلسلة متولدة من المولد J-K المطوّر.

وكلا السلسلتين لهما نفس قيم مسجلي ودوال التغذية المرتدة الخطية، وسوف نوضح قوة السلسلة المتولدة من المولد J-K المطوّر مقارنة مع السلسلة المتولدة من المولد J-K.

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

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

بعد تنفيذ كلا المولدين لإنتاج السلاسل تبين مايلي:

---- في المولد J-K السلسلة المتولدة هي

Z= 011001011000101011011

وبطول 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 والذي يؤدي إلى كسر النظام وكسر الشفرة.

--- في المولد J-K المطوّر

كانت السلسلة المتولدة هي

Z=001011001011011001001

وبتطبيق

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

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

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

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

الاستنتاج: Conclusion

قوة نظام التشفير الانسيابي تعتمد على قوة مولد المفتاح والذي ينتج سلسلة شبة عشوائية ذات خصائص عشوائية. في هذا البحث تم تطوير فكرة المولد J-K والوصول إلى مولـد مطـوّر يتعدى الضعف الموجود في المولد السابق ويجعلة ذو سرية اكبر ومقاومة قوية أمام المهـاجمين. كان ذلك بإدخال بوابات منطقية أضافية (بوابـات XOR , NOT , AND) بحيـث تجـاوز الاختبارات العشوائية للمولد J-K (اختبار التردد, اختبار التسلسل, اختبار بوكر، اختبر التطابق) وتحقيق النجاح فيها. كذلك زيادة مناعة الارتباط حيث إن المهاجم لا يسـتطيع تطبيـق هجـوم الارتباط على السلاسل المتولدة Z لتحديد قيمة مسجلات الإزاحة الخطية التي ولدت السلسـلة Z مما قاد إلى زيادة التعقيد الخطي للسلسلة Z وأدى ذلك تغير في سلوكيات المولد J-K وبـذلك فشل هجوم الارتباط لتحليل النظام وكسر الشفرة. تم تطبيق العديد من السلاسل (بقـيم ابتدائيـة للمسجلات ودوال تغذية مرتدة مختلفة) على نظام J-K المطوّر وتم الحصول على نتائج جيدة.

المصادر

1. **Carter G.**, "***Statistical Tests for Randomness***", EISS, England,1989.

2. **Rubin F**, "***Decryption a Stream Cipher Based on J-K Flip-flops***", IEEE Trans. On Computers, vol. c-28, No. 7, July 1979, pp. 483-487.

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.