# استخدام علاقة الارتباط في إيجاد المحتويات الابتدائية والربط لمسجلات الإزاحة الخطية

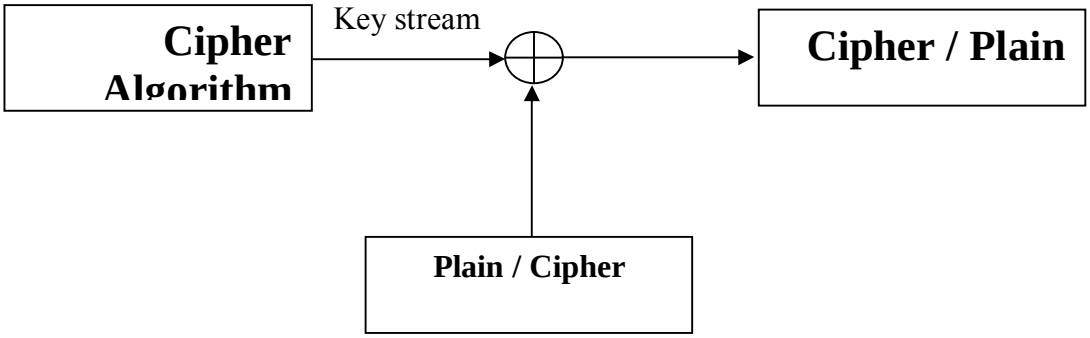
عوني محمد كفطان الجبوري
كلية الادارة والاقتصاد
جامعة تكريت

## ١. تمهيد:

تقسم الانظمة الشفرية الى نوعين: الانظمة الشفرية الكتلية ( Block Cipher systems ) والانظمة الشفرية الانسيابية ( السيلية) ( Stream Cipher System).
الانظمة الكتلية كما يدل اسمها تحتاج الى تقسيم النص الى مقاطع ( كتل ) باطوال ثابتة واستخدام دالة واحدة لتشفير كل مقطع من هذه المقاطع ( هنا يمكننا استخدام دالة مختلفة لكل مقطع ولكن في هذه الحالة تكون عملية ادارة العملية الشفرية صعبة من حيث ادارة المفاتيح ، المساحة الخزنية والزمن ). في حين ان الانظمة الانسيابية يتم فيها التشفير بت بعد بت ( Bit by Bit ) بدالة معينة ( تكون ثابتة لكافة الخطوات في عملية التشفير).

## ٢. انظمة التشفير الانسيابي:

تستخدم الانظمة الشفرية [2] كما موضح بالشكل الاتي:




تستخدم لتشفير النص الواضح ( والذي يمثل بمتتابعة ثنائية Binary ) وذلك بمعالته ( دمجه) باستخدام الجمع (XOR) مع المتتابعة الثنائية ( المتولدة من خوارزمية التشفير Cipher Algorithm التي تغذى بمدخلات اولية ) لنحصل على النص المشفر.
تتصف الانظمة الشفرية الانسيابية بخاصية مهمة وهي عدم تضاعف الاخطاء في حالة حدوثها ( أي عندما يتم استلام واحد من الثنائيات ( Bits) من النص المشفر بشكل خاطيء فانه سيحدث خطأ واحد في احد الثنائيات في النص الواضح).

## ٣. مسجلات الازاحة Shift Registers:

يمكن تعريف مسجل الازاحة بطول ( N) بأنه (N) من الخزانات محتوياتها تمثل بـ(S0,S1, ……Sn-1) وان محتوى هذه الخزانات هي 0و 1 . كما في الشكل:

| ~~S0~~ | ~~S1~~ | S2 | …… | Sn-1 |
|---|---|---|---|---|

## ٤. هدف البحث:

Out put

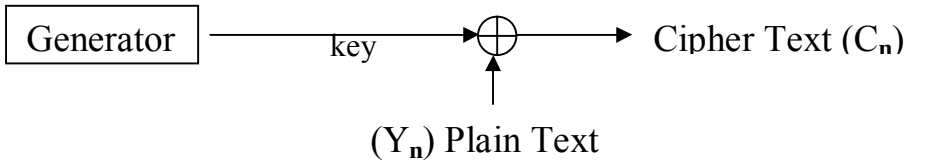
يهدف البحث الى استخدام علاقة الارتباط (Correlation ) بين مخرجات مسجلات الازاحة الخطية (LFSR's ) التي تتألف منها المولدات العشوائية (random generators) وشبه العشوائية ( pseudo random generators ) ) وبين الناتج النهائي (النص المشفر) لمنظومات التشفير لإيجاد المحتويات الابتدائية لمسجلات الازاحة الخطية مع ربطها.

## ٥. الجانب النظري:

### أ.المقدمة:

اولا: تتالف المولدات ذات التشفير الانسيابي من ( s) من الزواحف الخطية (مسجلات الازاحة) (LFSR's) بأطوال $r_i$ (i=1,2,3,….s ) مرتبطة بدالة غير خطية ولكنها معروفة [1].

ثانيا: هذه المولدات افترضت لتستخدم كمولد مفاتيح في التشفير الانسيابي كما في الشكل ادناه:




حيث ان الرمز $\oplus$ يعني عملية الجمع (bit by bit ) على ان يكون الناتج 0 أو 1 (Mod2 ).

ثالثا: اعتبرت الحالة الابتدائية لمسجلات الازاحة الخطية (الزواحف الخطية) والربط (tapping) كجزء مما مطلوب استخراجه بالاضافة الى ذلك يفترض ان يكون ربط مسجلات الازاحة اولي (primitive) لتحقيق اكبر دورة (Maximum period) ممكنة ($2^{ri}$-1) [3].

رابعا:ان عدد الاحتمالات NP هي:

$$NP = R_i\ (2^{ri}\text{-}1\ )$$

حيث ان المقدار $2^{ri}$-1 يمثل طول الدورة ، وان $R_i$ يمثل عدد انواع الربط الممكنة (دالة التغذية المرتدة Feed back) لكل زاحف خطي بما يحقق الشرط اعلاه.

خامسا: ان نقطة الضعف في هذه المولدات ( ربما تكون ) في وجود علاقة الارتباط بين مخرجات الزواحف الخطية وبين الناتج النهائي [5] وبأستخدام هذه العلاقة يتم العمل على كل زاحف على حده للحصول على دالة الربط الخاصة به والمحتويات الابتدائية.

سادسا: ان درجة التعقيد عند استخدام هذه الطريقة ستكون:

$$\sum Ri\ 2^{ri}$$

مع العرض بان الاسلوب التقليدي تكون درجة تعقيده [1] :

$$\prod R_i 2^{ri}$$

وهنا يبدو ان الفرق كبيرا جدا بين الطريقتين.

**ب.النموذج الاحصائي:**

ان احتمالية كون مخرجات الزواحف الخطية 1 تساوي احتمالية كونها 0 أي ان:

$$P\ (X_n^i =0)= P\ (X_n^i =1)= 0.5$$

ان احتمالية كون المخرجات النهائية 1 تساوي احتمالية كونها 0 ، أي ان:

$$P\ (Z_n =0)= P\ (Z_n =1)= 0.5$$

حيث ان $X_n^i$ هي مخرجات الزواحف الخطية لجميع قيم i و n وان $Z_n$ هي المخرجات النهائية.

ان احتمالية تطابق المخرجات النهائية مع مخرجات الزواحف الخطية تكون بالشكل:

$$P\ (X_n^i = Z_n )= q_i$$

هنا يجب علينا ان نختار مقياس او قيمة او نسبة معينة ( Threshold) لمقارنتها مع $q_i$ (هنا مثلا تكون احتمالية التطابق مقبولة عندما تكون نسبتها اكثر من ٦٥%) [7].

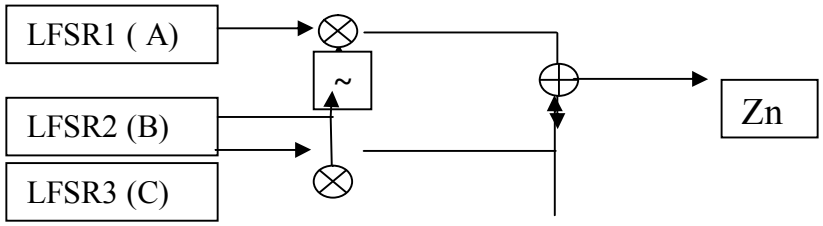
كذلك فأننا نأخذ لكل زاحف خطي جميع دوال الربط الممكنة التي تحقق أطول دورة ( Maximum Period) لحركة الزاحف [1 ].وكما موضح في الامثلة اللاحقة في البند القادم.

**٦. الجانب العملي:**

هنا اخذنا مثالين لتطبيق علاقة الارتباط التي مر ذكرها حيث ان المثال الاول يوضح ظهور احتمالية التطابق بين مخرجات الزواحف الخطية مع الناتج النهائي ( في هذا المثال يمكن ملاحظة التطابق يدويا من خلال بناء جدول الصدق Truth Table ).اما المثال الثاني فقد تم بناء برنامج بلغة باسكال لهذا الغرض ( يمكن للبرنامج ان يكون استخدامه عاما للحصول على دالة الربط والحالة الابتدائية لأي زاحف خطي بعد تزويد البرنامج بالبيانات اللازمة).

مثال(١):

ليكن لدينا المولد ( Pn-generator) وهو ([3] Geffe) الموضح بالشكل:




١. المولد اعلاه مكون من ثلاث زواحف خطية حيث تجمع مخرجات الزاحف الثاني مع مخرجات الزاحف الثالث ( العملية هي عملية AND ) ويؤخذ معكوس مخرجات الزاحف الثاني ايضا مع مخرجات الزاحف الاول (حيث تمثل العملية ~ عملية النفي).

٢. ناتج كل من العمليتين في (١) تجمع معا للحصول على الناتج النهائي Zn ( العملية هي عملية OR ).

٣. بعد ذلك نقوم بحساب احتمالية تطابق الناتج النهائي Zn مع كل زاحف وهي عملية احتسابqi في العلاقات السابقة، وتكون النتائج كما في الجدول الآتي الذي يوضح بصورة مفصلة آلية عمل هذا المولد:

| A | B | C | ~ B | ~ BxA | B x C | Zn |
|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 1 | 0 | 0 | 0 |
| 0 | 0 | 1 | 1 | 0 | 0 | 0 |
| 0 | 1 | 0 | 0 | 0 | 0 | 0 |
| 0 | 1 | 1 | 0 | 0 | 1 | 1 |
| 1 | 0 | 0 | 1 | 1 | 0 | 1 |

| | | | | | | |
|---|---|---|---|---|---|---|
| 1 | 0 | 1 | 1 | 1 | 0 | 1 |
| 1 | 1 | 0 | 0 | 0 | 0 | 0 |
| 1 | 1 | 1 | 0 | 0 | 1 | 1 |

حيث ان

$$Zn = (\sim B x \oplus \quad (x C)$$

نلاحظ من جدول النتائج اعلاه ما يلي:

احتمالية تطابق الناتج النهائي Zn مع A ( أي احتمالية Pi ) هي

$$Pi_A = 6/8 = 0.75$$

احتمالية تطابق Zn مع B هي

$$Pi_B = 4/8 = 0.5$$

احتمالية تطابق Zn مع C هي

$$Pi_C = 6/8 = 0.75$$

وهذا يعني ان تطابق كلا من A و C اعلى من تطابق B مع الناتج النهائي ( أي ان تطابق B ضعيف ولا يمكن من خلاله مهاجمة المنظومة).

مثال ٢:

في هذا المثال تمكنا من الحصول على دالة الربط المستخدمة والحالة الابتدائية لزاحف خطي بطول ( ٥ ) وذلك بتجربة كل الاحتمالات الممكنة لدالة الربط والحالة الابتدائية، حيث اخذنا دوال الربط التالية:

[ 3 , 5 ]
[ 1,3,4 5 ]
[ 2,3,4,5 ]
[ 1,2,4,5 ]
[ 4 , 5 ]

وان دوال الربط هذه هي التي تحقق اطول دورة ( Maximum Period) وطول الدورة هنا هو

( $2^5 - 1 = 31$).

بعد ان استخدمنا البرنامج الخاص بهذه الطريقة وجدنا ان اعلى قيمة نتجت من حساب علاقة الارتباط هي ( ٢٣٦ ) والتي تقابل الحالة الابتدائية (١٠١٠٠ ) للزاحف الخطي بطول خمسة وان دالة الربط المناظرة لهذه الحالة هي ( 5 , 3 ).

وفيما يلي عرض للنظام البرامجي المستخدم:

```
PROGRAM CORRELATION;
        USES CRT;
          TYPE
             TYP1 = ARRAY [1..11 ] OF 0..1;
           VAR
              PLN_TEXT , CIP_ TEXT     : ARRAY [1..30000 ] OF
0..1;
              SR                                : ARRAY [1..5,1..11 ]
OF 0..1;
               LEN , LENST                      : ARRAY [1..5 ] OF
BYTE;
```

```
                ST                          : ARRAY [1..5 , 1..6 ]
OF BYTE;
                 FUNC                       : ARRAY [1..31 ] OF
0..1;
                ONE                         : ARRAY [0..1, 1..5] OF
LONGINT;
                INITIAL                     : ARRAY [1..5 ] OF
STRING;
                 LEN_PLAIN, NO_SR           :INTEGER:
  (*************************************)
 PROCEDURE    DEC_TO_  BIN(DEC,NO_BIT: INTEGER; VAR
BIT:TYP1);
        (*************************************)
 PROCEDURE  BIN_TO_ DEC(BIT: TYP1; NO_BIT: INTEGER; VAR
DEC :INTEGER);
  (*************************************)
  PROCEDURE READ_ PLAIN;
  (*************************************)
    PROCEDURE  MAKE_ SYSTEM;
   (*************************************)
  PROCEDURE  MAKE_ CIPHER;
 (*************************************)
   PROCEDURE  WRITE _ SR;
   (*************************************)
    PROCEDURE  FIND_ SR;
   (*************************************)
BEGIN
   MAKE_SYSTEM;
   READ_PLAIN;
   MAKE_CIPHER;
   WRITE_SR;
    FIND_SR;
END.
```

## REFRENCES المصادر


1.Bruce Schneier, Applied Cryptography. (1996).

2.Piper & Beaker, Cipher System, (1982).

3. Carl H. & Stephan M. , Cryptography, A guide for the design and implementation of secure systems, (1982).

4. Dorthy Elizabeth R. D. , Cryptography and Data Security, (1982).

5. T. Siegenthaler, Decrypting a class of stream cipher using ciphertext only. IEEE, Transaction Computers, Vol. C-34, No.1 ; Jan. 1985.

٦.علي محمد كاظم، دراسة تحليلية لاختبارات العشوائية لمتتابعات انظمة التشفير الانسيابي، رسالة ماجستير، الجامعة التكنولوجية/ قسم علوم الحاسبات،١٩٩٢.
٧. مدخل لدراسة النماذج الاحتمالية، ترجمة الدكتور فاضل محسن الربيعي، الجامعة المستنصرية، ١٩٩٣.