معالجة جديدة للهجوم باستخدام علاقة الارتباط

م. عوني محمد كفطان
م.م نزار خلف حسين
جامعة تكريت

المستخلص:

قدمنا في هذا البحث بعض المعالجات لعلاقة الارتباط بين المدخلات والمخرجات لأنظمة توليد المفاتيح الشفرية، في المعالجة الأولى، استخدمنا منظومة معالجة تكون مدخلاتها معتمدة على منظومات جزئية من المنظومة الرئيسية ، في المعالجة الثانية، استخدمنا منظومة منفصلة ومستقلة لاتعتمد على أي جزء من المنظومة الرئيسية. حيث يتم معاملة مخرجات منظومة المعالجة (منظومة التوازن) مع مخرجات مولد المفاتيح لنحصل على المخرجات النهائية الجديدة. بينت النتائج أن هذه المعالجة قادتنا إلى تقليل إمكانية المهاجمة باستخدام علاقة الارتباط من (٧٥%) إلى (٢٥%) .

Abstract

In this paper, we present some treatments for the correlation ship between the input and the output of the cryptography keys generators systems, in the first one, we have assumed a system that it's input depends on the other subsystems in the main system. In the second one, we have taken a system which is called (balance system) and it's input is not depending on other subsystems in the main system.

The output of the balance system deals with the output of main system.
The result shows that this treatment led to decreased the correlation ship from (75%) to (25%).

A NEW TREATMENT OF THE ATTACK BY USING CORRELATIONSHIP

AWNEY M. KAFTAN
COLLEGE OF COMPUTERS SCIENCES AND MATHEMATICS

NAZAR K. HUSSAIN
COLLEGE OF COMPUTERS SCIENCES AND MATHEMATICS

1-Abstract

In this paper, we present some treatments for the correlation ship between the input and the output of the cryptography keys generators systems, in the first one, we have assumed a system that it's input depends on the other subsystems in the main system. In the second one, we have taken a system which is called (balance system) and it's input is not depending on other subsystems in the main system.

The output of the balance system deals with the output of main system.
The result shows that this treatment led to decreased the correlation ship from (75%) to (25%).

2-Intoduction

There are three kinds of the cryptographic system: the first one, is transposition system; the second, is the substitution system and the third , is the combination of the first and the second kind[3].

If we design a cipher system, we must be take an attention to the security of the whole system depends on the security of all system element [1].

- cryptographic algorithm
- key generator

It is clear and understandable that if a strong (good) algorithm is applied, but the key generator is a weak random, then an attacker (crypto analyst) will break the system, and he will attacking the system in its weak points.

The basic design philosophy is inspired by some class of encryption algorithms which is called "One-Times-Pad" (O.T.P) [5] which encrypts by XOR'ing the plaintext with a random key. However, the One-Times-Pad impractical for most applications. Instant, stream ciphers expand a given short random key into a pseudo-random key system, which is then XOR'ed with the plaintext to generate the cipher text. Consequently, the design goal for a stream cipher is to efficiently generate pseudo-random bits which are indistinguishable from truly random bits [2],[3].

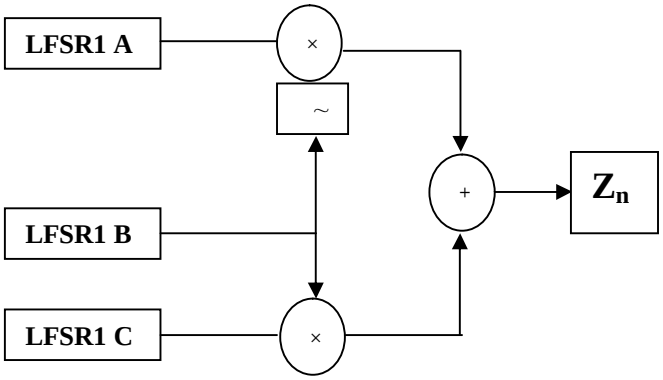
3- Correlation:-

If linear feed back shift register (LFSRs) are combined by function $F(x_1,x_2,\ldots,x_k)$ the highest values of the linear complexity are achieved if the

nonlinear order of the combining function is maximum. But we have to face the individual shift register sequences [2].

For example:-

Geffe- Generator [3] **Fig.(1)**



This generator consists of three shift registers and the operations of this systems are:

1- (AND) between the output of LFSR1 (A) with the negation the output of LFSR2 (B).

2- (XOR) between the output of LFSR2(B) with the output of LFSR3(C).

3- (XOR) between the result of step1 and step2.

Now if we make the truth table of this system as fellow:-

Table(1)

A	B	C	~B	~B×A	B×C	(~B×A)+(B×C)
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

s.t. $Z_n=(\sim B\times A)+(B\times C)$

From the truth table of this key generator we obtain the probability $q_i=p(Z_n=\text{output of LFSRi})$

s.t. $q_1=p(Z_n=\text{output of LFSR1(A)})$

so

$q_1=0.75, \quad q_2=0.5, \quad q_3=0.75$

it is clear that is a strong correlation between Z_n and LFSRi s.t. (i=1,2,3) and we can see a strong correlation in other kinds of key generators like:- (Bruer:threshold-generator) , (Pless-generator) [6].

Correlation Attacks

A good running key generator must produce a key system that has a long period , a high linear complexity and good statistical properties in order to make the key system unpredictable. But that is not enough , in fact, we must assume that the cryptanalyst (Attacker) know the structure of the generator and with this knowledge he may attack some of its internal components rather the key system itself [2].This kind of attacker is call (Correlation Attack).

Many almost stream cipher are based on the linear feedback shift register (LFSRs).A number of correlation attacks, such as [35,23,5,19,17,29], have been developed to analyze them. In 1996 Golic devised the linear cryptanalysis of streem ciphers. That technique could be applied to wide range of streem cipher[1].

Solution to the correlation problem

Now, we suggest to solve the correlation problem:-

1- **Independent balance system (I.B.S)**

In this case we use a linear feedback shift register and we fill its contains directly the output of the balance system deals with the final output of the main system (with Z) fig.(1).

The truth table below show the use of (I.B.S.)

Table(2)

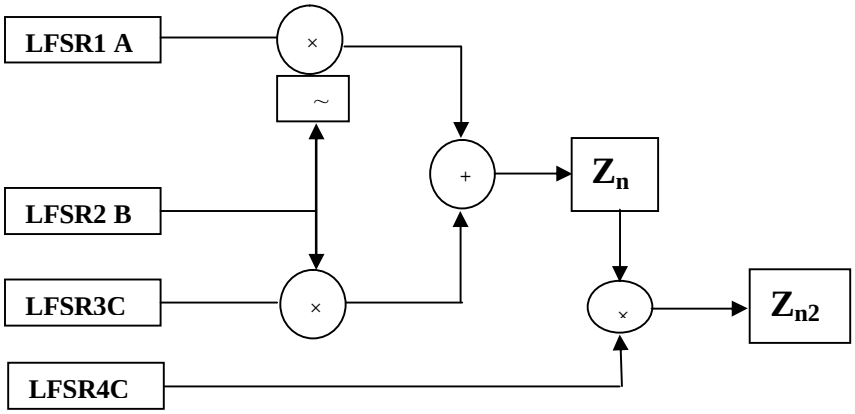
A	B	C	D	~B	B×C	~B×A	Z_n	~ D + Z_n
0	0	0	0	1	0	0	0	1
0	0	1	0	1	0	0	0	1
0	1	0	0	0	0	0	0	1
0	1	1	0	0	1	0	1	0
1	0	0	1	1	0	1	1	0
1	0	1	0	1	0	1	1	0
1	1	0	1	0	0	0	0	0
1	1	1	0	0	1	0	1	0

From this truth table we can see the probability q_i become q_1=0.125, q_2=0.375, q_3=0.375 and it is easy to see the correlation ship is weak.

2- Dependent Balance System (D.B.S.)

Now, we use a linear feedback shift register which it is contains by using the output of other components in the main system (i.e. this shift register is the subsystem of main system). As shows in the fig.(2)

Fig.(2)



The truth table of this system is :

Table(3)

A	B	C	B+C	~(B+C)	~B	~B×A	B×C	D	Z_n
0	0	0	0	1	1	0	0	0	1
0	0	1	1	0	1	0	0	0	1
0	1	0	1	0	0	0	0	0	1
0	1	1	1	0	0	0	1	0	0
1	0	0	0	1	1	1	0	1	1
1	0	1	1	0	1	1	0	0	0
1	1	0	1	0	0	0	0	0	1
1	1	1	1	0	0	0	1	0	0

s.t. $D=\sim(B+C)\times A$ and $Z_n=D+ \sim[(\sim B\times A)+(B\times C)]$

From this table we obtain the fellow probability qi

q 1=3/8 q 2=3/8 q 3=1/8

it is clear to note the correlation ship between the output of shifts registers (A , B and C) and the final output are weak .

Conclusion

From this work we can reduce the correlation ship between the initial contents of the shift registers of the system (key generator system) with the final output of the system (the final key which it is used as the key deals with plane text to obtain the cipher text).

In the future, the researchers can check: if we use this treatments, the system has Maximum Correlation Immunity, but also has Minimum Complexity.

References :

1- Prof. Dr. Golec (key generator system) Rotary Institute , Beograd , Jan. 2002 .

2- (Omnisec 's Solution to the correlation problem in Bruer : threshold – generator and pless-generator) Omnisec company for cryptography Equipments . 1994 .

3- Prof. Brainier Keskenovic and Prof. Miladin Dabic, (Roots of stream Cipher) , Bill Export-Import, Beograde, Yugoslavia 2001.

4- Hongjun Wu, (A New Stream Cipher HC-256) , Institute of Infocmm Research , Singapore, April ,2004.

5-Martin B., and, Mette V. and others, (Rabbit: A New High – performance Stream Cipher) CRYPTICO A/S, Copenhagen, Denmark 2001.

٦. عوني محمد كفطان، (استخدام علاقة الارتباط في ايجاد المحتويات الابتدائية والربط لمسجلات الازاحة الخطية) مجلة تكريت للعلوم الادارية والاقتصادية، المجلد١، العدد الاول لسنة ٢٠٠٥).

This document was created with Win2PDF available at http://www.win2pdf.com.
The unregistered version of Win2PDF is for evaluation or non-commercial use only.
This page will not be added after purchasing Win2PDF.