A study of Algebraic Attack and proposed developed clock control stream cipher

Sattar B. Sadkhan **Rafeef M. Hamza**
University of Babylon/Computer science department

Abstract

Stream cipher is one of the efficient cryptographic primitives to provide confidentiality of electronically transmitted data. Where it is widely used in practice (e.g., in mobile phones, internet). Researches are interested with different types of attacking on stream ciphers. This paper provide classification for types of attacks on stream cipher and concentrate on the algebraic attack, since it represent the most important among them. Also the paper presents proposed developed clock control keystream generator based on combiner, that has an increase in the complexity of the structure. The Algebraic cryptanalysis was applied for comparing the resistant of proposed generator with LILI keystream generator.

الخلاصة

يعتبر التشفير الانسيابي من أساسيات التشفير الأكثر كفاءة في توفير السرية المطلوبة للبيانات المنقولة الكترونيا.حيث انه يستخدم وبصوره شائعة في الحياة العملية اليومية (مثل استخدام الموبايل والانترنيت) , لذلك فمن الطبيعي أن تتوفر العديد من الأبحاث التي تتناول طرق الهجوم على هذا النوع من طرق التشفير.والتي سوف يتم تصنيفها في هذا البحث وتركيز الاهتمام على نوع معين منها وهو الهجوم الجبري وذلك لأنه يعتبر الأداة الأكثر كفاءة في كشف المفتاح السري لنظم التشفير خصوصاً بعدما اثبت نجاحه ضد العديد من خوارزميات التشفير الانسيابي سواء المعتمدة على تقنية التوحيد او الترشيح او تقنية السيطرة على الوقت.كذلك سوف نقترح في هذا البحث مولد جديد يعتمد على تقنية السيطرة على الوقت المبني على التوحيد ومقارنة نتائجه مع مولد LILI وذلك لان فكرة المولد المقترح مستمدة منة.

1. Introduction

Cryptanalysis is the study of methods for obtaining the meaning of encrypted information, without known to the secret information(such as the used key for encryption) that is normally required to do so. Typically, this involves knowing how the system works and finding a secret key. Cryptanalysis is also routinely done by a system's designer, and by others, attempting to evaluate whether a system is secure or not. This is a normal part of the design process in cryptography. Nearly all cryptographic algorithms and protocols undergo this process and are carefully examined. The methods and techniques of cryptanalysis have changed drastically through the history of cryptography. An Attack is a successful or unsuccessful attempt at breaking part or all of a cryptosystem[E. Conrad 2007]. The types of attacks are different depending the cryptanalyst's knowledge or the methods that used for attacking or the goal from the attacking .Also the method and strategies of attacking are different depending on the type of primitive of encryption algorithm. Stream cipher one of efficient cryptographic primitives to provide confidentiality of electronically transmitted data. Stream ciphers are widely used in practice (e.g., in mobile phones, internet). Therefore the researches are interested with attacking of stream cipher [S.Kumar2010][F.Armknecht2004].From these attacking methods, the algebraic attack that also divide in to two types: ordinary algebraic attacks that based on three steps(convert the system to system of equations, insert the keystream, and solve the system to known the secret key),while the second type of algebraic attack is a fast algebraic attacks, where the idea is that before starting to solve the system of equations, the equations are linearly combined to get new equations with a lower degree[F. Armknecht 2004].

The main interested of this paper based on the ordinary algebraic attacks. The aim from this paper was to provide classification for types of attacks and provide main

interest with in the algebraic attack, since it represent the most important among them. Algebraic attacks has powerful cryptanalytic tool for re-covering the keys, spatially after it's proofing a successful against several types of nonlinear stream cipher algorithms (filtering, combiner and clock control). Also the paper presents proposed developed clock control keystream generator based on combiner, that has an increase in the complexity of the structure. Algebraic cryptanalysis was applied for comparing the resistant of proposed generator with LILI keystream generator.

The rest of the paper is organized as follows: Section 2 presents literatures review related with main purpose of the paper (algebraic attack on stream cipher). Section 3 discuses the proposed key stream generator. Section 4, applied an algebraic attack on it. Section 5 appears the result of comparison. Section6 contain the conclusion and future work.

2. Literature review

An attack could be classified depending on several criteria, where there are several types of attack that depends on what the knowledge that the attacker are know, such as cipher text only attack, chosen plain text attack, chosen cipher text attack, and in the standard assumption in cryptanalysis is that the attacker has access to certain amount of cipher text together with the corresponding plaintext and an attack that assumes such a scenario is called a known plaintext attack [E. Conrad2007]. Each of these attacks finally accessed to the keystream. With access to the keystream, any technique that can be applied to extract the secret key (initial value of the key generator, which represents the challenges), such as divide and conquered, correlation attacks, algebraic attack, and others [J.Mattson2006] The task of attacker in all of these types may be classified to the following:

- Key recovery: A method to recover the key, such as exhaustive key search, dictionary attack [M.Hafeez2009].
- Distinguish the keystream from a random sequence [M.Hafeez2009].

The classification of different attacks can be shown in the Figure(1), where its appear how classified types of attacks depending on the knowledge that the attacker have, or depending on the methods that used for attacking ,or depending on the goal of the attack, is it for distinguishing the keystream from the random bits? ,or for recovering the secret key from given keystream segment .The dotted line refers to relation between the classes of attacks, such that when the attacker used algebraic method must have segment of plain text with corresponding cipher text(know plain text attack) for recovering the secret key(key recovers attacks) .

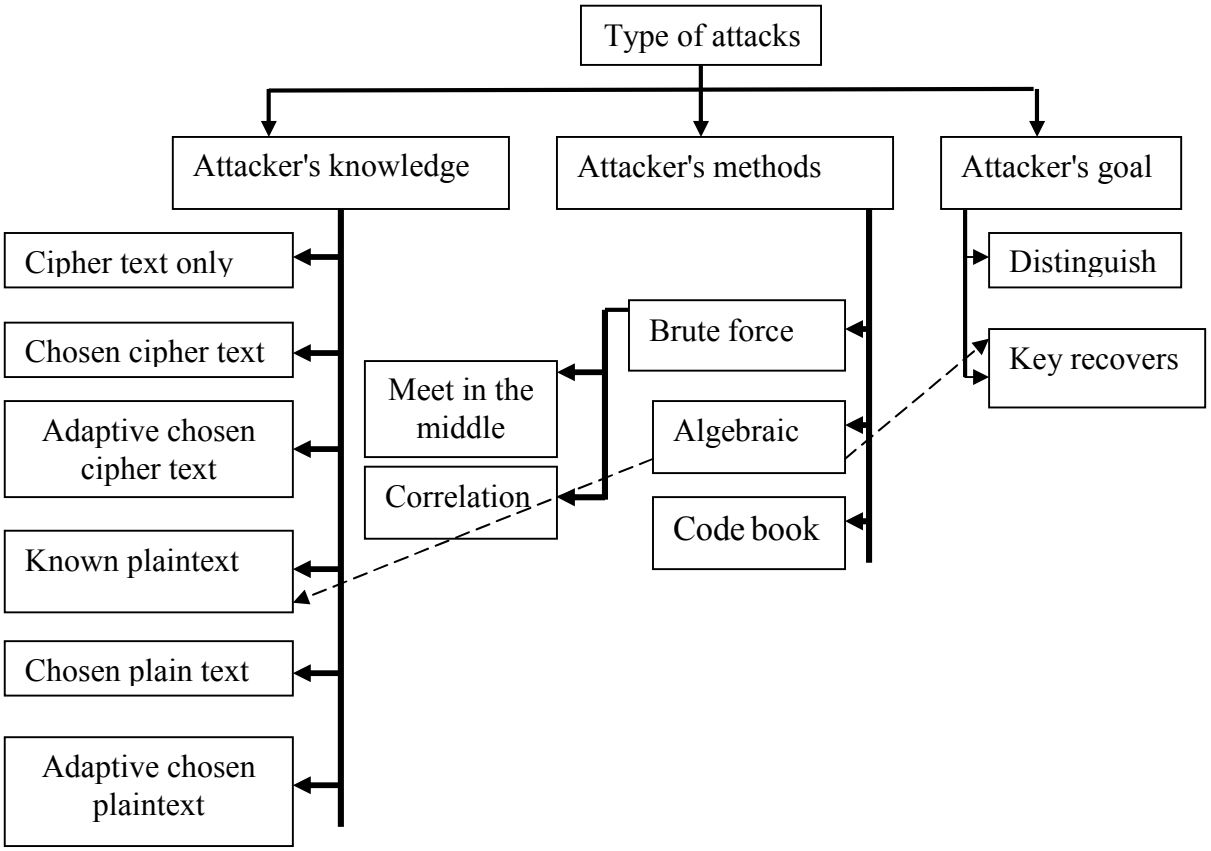
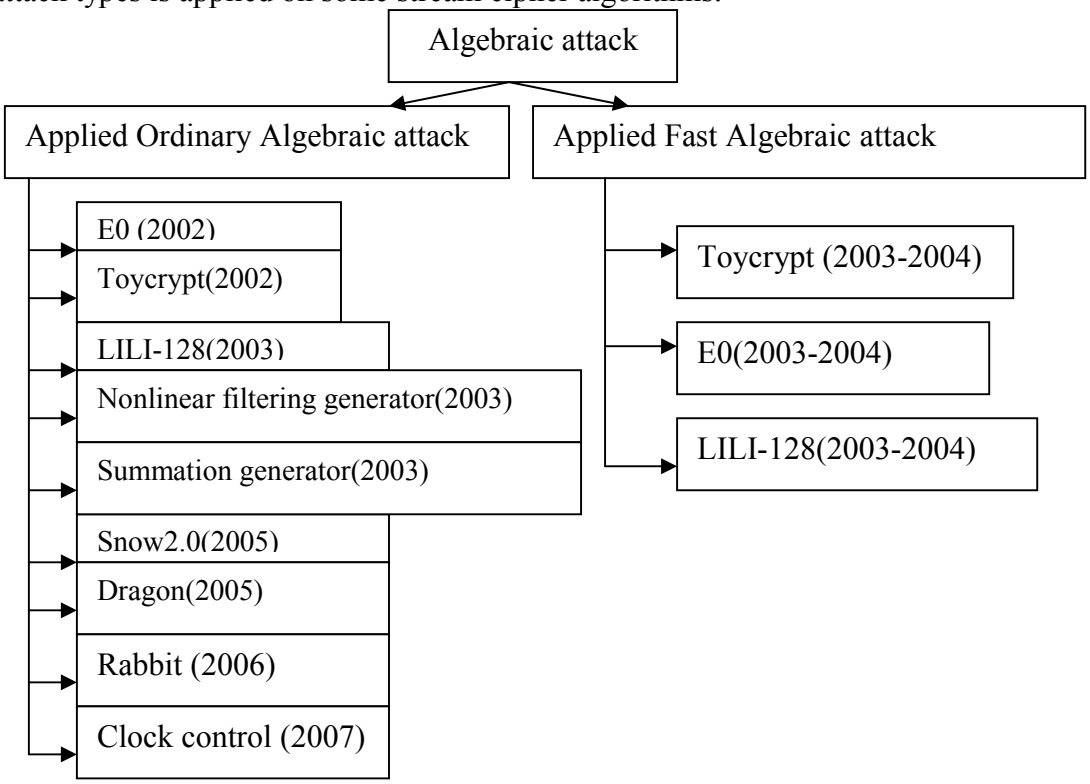


Figure (1): Classification of attacks

Types of algebraic attack can be classified as shown in figure(2), each one from these attack types is applied on some stream cipher algorithms.



Figure(2): Types of Algebraic Attack

In the following we will explain briefly how applied each types on different algorithms depending on time.

-The linearization method(method for convert the system of nonlinear equations to system of linear equations) on the equations of E0 algorithm that used on the Bluetooth keystream generator, with $2^{70.341}$ operations [F. Armknecht 2002].

-Algebraic attack applied on the toycrypt stream cipher using XL algorithm, where such attack required 2^{92} CPU clock for 128 bit LFSR [N.Courtois 2002].

-Algebraic attack applied on the stream cipher (toy crypt and lili128),where the complexity of this attack reduced for square root with multiplying the system of equations with well chosen polynomial [N. Courtois &W.Meier 2003].

-Method to reduce the complexity of the algebraic attack on toycrypt,lili128,E0 stream cipher by applying the fast algebraic attacks, with providing consecutive bit of keystream [N. Courtois 2003] .

-Algebraic attack applied on nonlinear filter generator and explanation theoretically and practically the nonlinear function of degree D behave from algebraic attack point as low degree function d<D, and could be found the secret key from O (L^d) keystream bits, where d< (k+1/2), k is the number of variables that input to the nonlinear filter function [J. Charles 2003].

- Algebraic attack was applied on summation generator and it was found that such attack provide results much less than that of upper bound given by previous results[D. Hoon Lee2003].

- The algebraic attack and it's developed fast algebraic attack explained and illustrated how applying them on the toy cipher practically, and theoretically on the E0. It was show the problem of this type that based on the degree of the system of equation, and the complexity of solving that system [F. Armknecht 2004].

- The resistant of stream cipher SNOW 2.0 against algebraic attack as explained .This type of attack considered as an efficient type of attack against a closed variant of SNOW 2.0. It was claimed that the key search problem for the actual SNOW 2.0 was shown to be reducible to the solving of an over determined system of quadratic equations. The complexity of which remains unknown nowadays [O.Billet2005].

- A survey about applied an algebraic attacks on the stream cipher that based on LFSR and how to apply it on some type of stream ciphers like (E0,LILI128, Toy crypt, summation). It was claimed a foundation of new stream cipher that based on Non-LFSR. and such type is hard analysis its characteristic using previous ways [D.Hoon Lee 2005].

-Algebraic attacks was applied on Dragon (word base)stream cipher, but could not have a success, because of the increase of it's nonlinearity due to use the Non-LFSR[K.Chen2005].

- The analyses of the application of algebraic attack on the Rabbit stream cipher algorithm, and proving it's infeasibility, because the large of it's nonlinearity for updated state and the complexity of g-function (number of monomials), and so on. Those made the system very complex and its sequence like random [Cryptico A/S 2006].

- Algebraic cryptanalysis of Grain that is aimed toward used nonlinear feedback shift register(NLFSR) based stream cipher was describe. The effort to recovering the initial state by solving the vary degree equations, with some guessed bit using Grobner bases technique, where they are succeed in recover 1/2 of the internal state bits of Grain -1 and other half was Guessed, while only 1/4 from the internal state bit obtained in the Grain -128 [M. Afzal 2006].

- Algebraic attack on combiner was applied and constructed its system in details and explained the closely connected between the efficiently of algebraic attack and the degree of equation and the method for solving this equations [F. Armknecht 2006].
- Algebraic attack on clock control generator using stop-and- go clocking was describe and appear that it's very efficient attack on Beth-piper, alternating step and, Golleman stop and go generator while not efficient attack on pomaranch cipher. Also it was appear that such attack is very powerful attack against (p, q) clocking generator such as step1/step2 and self decimated, while a difficult way to apply algebraic attack on mutual clocking control generator A5/1,Micky [S.Zayid 2007].
- The algebraic cryptanalysis was used as a tool for assessing the resistance of the stream cipher. It show the structure of some type of stream cipher(grain, trivium, Micky), since the structure of the system effects on the efficiency. They found that Grain-128 and Micky have more resistance than Grain-1 and trivium [M. Afzal2008].
- A proposed an efficient type of attack (algebraic attack) against modern model of Alternating Step Generator(ASG) that was called ASG(r; s).where the designer of the ASG(r; s) claimed that the structure is more secure than the original ASG. They proved that it's security is not more than the original ASG, and need for less complexity than other types of previous known attacks [M. Hassan2008].
- Analyses of the algebraic attack on the RC4, which is a family of word base stream cipher that based on look up table. They were contended it's infeasibility, that return to it's operations (state extraction, word addition, and state permutation). Each one from these operations needed to build system of equation exclusive to it, that make the attack very difficult [K. Koon 2010].
- Algebraic cryptanalysis on the A5/2 type clock control generator was describe and using Groebner method for solving the system of equations [A. Mihaita2010].
- Several modified types of alternating step generators was described such as the More Generalized Clock-Controlled Alternating Step Generator MGASG, Modified Clock-Controlled Alternating Step Generator (MASG), Alternating _*k*-generators, Step*(D,K)* Generator and applied algebraic attack that satisfy all types for reduce the complexity of attacks [S.Mehdi 2011].

3. A proposed Developed Clock Control Keystream Generator

The structure of the proposed generator consists from two parts as shown in figure(3):

1-Sub generator : Clock Control Register.

2-Data Generating Registers (combiner generator).

- The first part represents the clock control. Consists form LFSR used primitive polynomial to produce a sequence with large period, and (k) fixed positions from the LFSR will be selected. The content of this K position will be connected at each step using selected integer filtering function to generate the controlled sequence(c(t)), where each integer number in this sequence will control the clocking of the registers in the second part (combiner's registers). In this proposed system we assume k=2, and choose (x_2, x_4) to generate c(t) using eq(1) as:

$$c(t) = 2x_2 + x_4 + 1 \qquad \text{eq(1)}$$

That make c (t) $\in \{1, \ldots, 2^k\}$.(note, this function depends on the designer's choice).

-The second part, represents nonlinear combiner generator, consists of (m) LFSRs each one use a primitive polynomial. This combiner generator generates the output bits of the keystream after c(t)time of clocking the LFSRs.

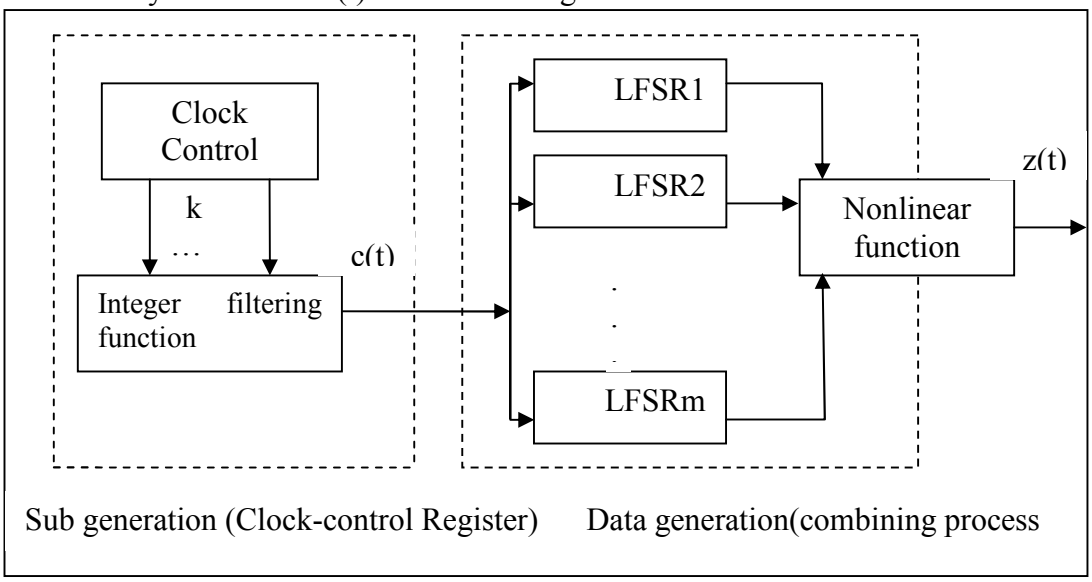


Figure (3): A proposed Clock control based on combiner generator.

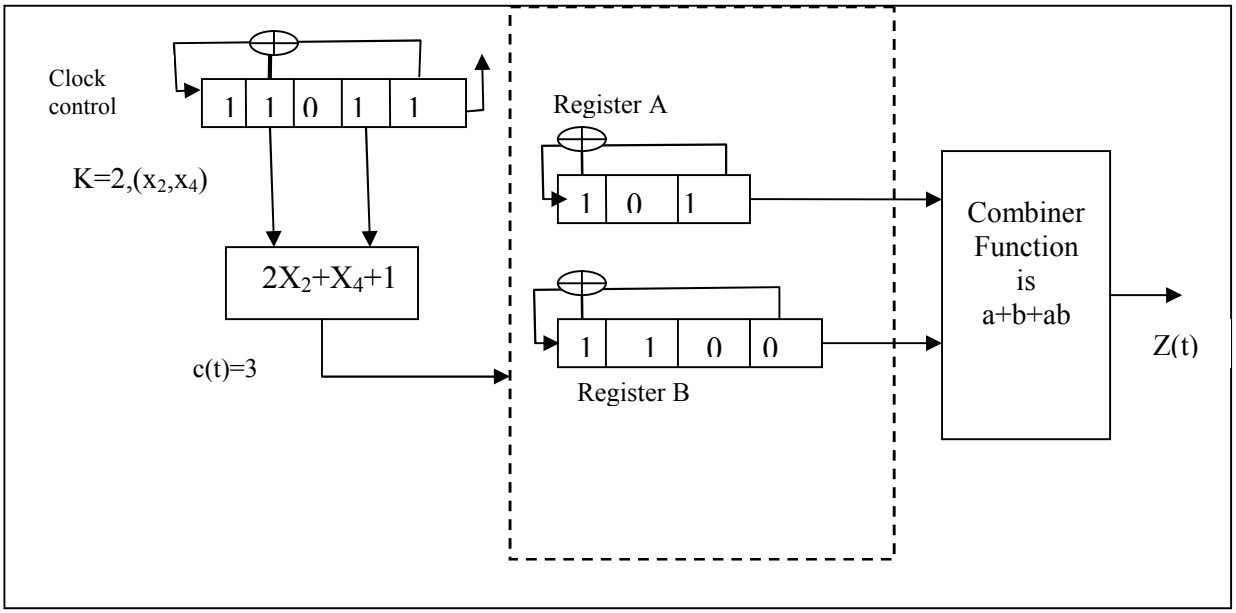
Example1: let (1 1 0 1 1) is the initial value for clock control register that used (x_5+x_2+1) as the primitive polynomial. The (1 0 1), (1 1 0 0), are the initial values for the two LFSRs(A,B) of combiner, that used (a_3+a_1+1), (b_4+b_1+1) as primitive polynomials respectively, and integer filtering function that used for clock control register as in eq(1),with using the nonlinear combiner function (a+b+ab), will generate the key stream Z={1,1,1,…}, as illustrated in table(1).

Table (1) generate keystream depending on clock control based combiner generator

T	Clock control	c(t)	I	A	outA	B	outB	Z
	(1 1 0 1 1)			(1 0 1)		(1 1 0 0)		
1	(0 1 1 0 1)	3	1	(0 1 0)	1	(1 1 1 0)	0	
			2	(0 0 1)	0	(1 1 1 1)	0	
			3	(1 0 0)	1	(0 1 1 1)	1	1
2	(0 0 1 1 0)	2	1	(1 1 0)	0	(1 0 1 1)	1	
			2	(1 1 1)	0	(0 1 0 1)	1	1
3	(0 0 0 1 1)	2	1	(0 1 1)	1	(1 0 1 0)	1	
			2	(1 0 1)	1	(1 1 0 1)	0	1

In table(1), T represents the time for the clock control register, c(t) represents the number of time that LFSRs on the combiner must be clocked before generating the output bit(z) using nonlinear combiner function. The structure of this example can be explained in figure(4).

When we look to the proposed structure it is clear that it is similar to the structure of LILI generator but with a changes the second part to combiner, where the idea of this generator derived from the LILI structure[X. Huang2005]. There for in the final we will compare the results of proposed generator with LILI 128 to explain which one is better.



figure(4):explanation to the work of example1.

4.Application of the Algebraic Attack

The algebraic attack, converts the problem from finding the secret key (initial value) to solve multivariable system of algebraic equations, where an algebraic equation relating the initial key bits and the output keystream bits. And then solved through linearization techniques or any other proper techniques. Where the initial value represents the solution of the system [D.Hoon Lee 2003][C. McDonald 2010] .
The scenario of the working of algebraic attacks is as follow:
1- Find a system of equations which relate the initial value that represent the secret key (unknown) with the keystream (known) . If the system have n unknown variables, and the degree for the system of equation d, such system requires at least $\sum_{i=0}^{d}\binom{n}{i}$ independent algebraic relations(equations), since the system of n unknown variable has $\binom{n}{i}$ monomials of degree i, that make the total system has $\sum_{i=0}^{d}\binom{n}{i}$ items from linear to nonlinear.
2 - Have sufficient amount of keystream as much as the number of terms that appear in the system (Substitute the keystream into the system of equations).
3 - Solve the system to recover the unknown variables.
When we want to construct the system of equations for clock control based combiner generator, that like the construction system of equations for combiner generator but with irregular clocking. The keystream equivalent to the function with input variables $z_i = f(x_{i1}, x_{i2}, \ldots, x_{in})$,where x_{ij} is typically a linear function (Li)of the initial states S applied i times for j^{th} register .
For each observed keystream symbol we get an equation .

$$z1 = f(X1(s)) \quad (2)$$
$$z2 = f(X2(s)) \quad (3)$$
.
.
$$z_m=f(X_m(s)) \quad (4)$$

where $m = \prod_{i=1}^{n} 2^{ki} - 1$ is the period of sequence produced by the combiner, k_i is the length of register i, z represent keystream bit [J. Mattson2006].
The initial value for the clock control register must be specified firstly to generate the control sequence c(t), which selects the equation required for building the final system of equations with it's keystream. And finally the system of equations must be solved using Gaussian elimination method based on binary matrix[A.Bogdanov 2005].
Example(2): Suppose the clock control based combiner generator consists of clock control register(5bit), with initial value (1 1 0 1 1), primitive polynomial (x_5+x_2+1) to follow the algebraic attacks application. Table2 will give a brief review to the mentioned stages of the attack

Table(2):steps of clocking the registers of combiner

T	First register	Second register	Third register
	(a1,a2,a3)	(b1,b2,b3,b4)	(c1,c2,c3,c4,c5,c6,c7)
1	(a1+a3,a1,a2)	(b1+b4,b1,b2,b3)	(c3+c7, c1,c2,c3,c4,c5,c6)
2	(a1+a2+a3,a1 +a3,a1)	(b1+b3+b4,b1+b4,b1,b2)	(c2+c6,c3+c7, c1,c2,c3,c4,c5)
3	(a2+a3,a1+a2 +a3,a1+a3)	(b1+b2+b3+b4,b1+b3+b 4, b1+b4,b1)	(c1+c5,c2+c6,c3+c7, c1,c2,c3,c4)
4	(a1+a2,a2+a3, a1+a2+a3)	(b2+b3+b4,b1+b2+b3+b 4, b1+b3+b4, b1+b4)	(c3+c4+c7,c1+c5,c2+c6,c3+c7, c1,c2,c3)
5	(a3,a1+a2,a2+ a3)	(b1+b2+b3,b2+b3+b4, b1+b2+b3+b4, b1+b3+b4)	(c2+c3+c6,c3+c4+c7,c1+c5,c2+c6 ,c3+c7, c1,c2)
6	(a2,a3,a1+a2)	(b2+b4,b1+b2+b3,b2+b3 +b4, b1+b2+b3+b4)	(c1+c2+c5,c2+c3+c6,c3+c4+c7,c1 +c5,c2+c6,c3+c7, c1)
7	(a1,a2,a3)	(b1+b3,b2+b4,b1+b2+b3 ,b2+b3+b4)	(c1+c3+c4+c7,c1+c2+c5,c2+c3+c 6,c3+c4+c7,c1+c5,c2+c6,c3+c7)
8	(a1+a3,a1,a2)	(b1+b2+b4,b1+b3,b2+b4 ,b1+b2+b3)	(c2+c6+c7,c1+c3+c4+c7,c1+c2+c 5,c2+c3+c6,c3+c4+c7,c1+c5,c2+c 6)
9	(a1+a2+a3,a1 +a3,a1)	(b3+b4,b1+b2+b4,b1+b3 ,b2+b4)	(c1+c5+c6,c2+c6+c7,c1+c3+c4+c 7,c1+c2+c5,c2+c3+c6,c3+c4+c7,c 1+c5)
10	(a2+a3,a1+a2 +a3,a1+a3)	(b2+b3,b3+b4,b1+b2+b4 ,b1+b3)	(c3+c4+c5+c7,c1+c5+c6,c2+c6+c 7,c1+c3+c4+c7,c1+c2+c5,c2+c3+ c6,c3+c4+c7)

Using eq(1) to generate controlled sequence c(t)={3,2,2,1,3,3,4,….}. And $(x_3+x_1+1),)(x_4+x_1+1),(x_7+x_3+1)$ used as primitive polynomials for three registers on combiner generator with $(x_1+x_2+x_3+x_2x_3)$ as nonlinear combining function to generate system of equation. Firstly let us represent the initial values for the three registers using variables and applied the primitive polynomials on it at each step as describe in table(2), and when we applied the nonlinear combiner function on the selected row, this will generate system of equations for the second part. Then it will be easy find the initial value for the second part of the generator whenever insert the sub keystream that generated from these values.

After applying nonlinear combining function on the variables that results from the three registers on the shading rows, this will generate the following equations for only five steps, where the shading rows in the table(2) dedicated using controlled sequence

1- a1+b2+c5+b2c5
2- a1+a2+a3+b1+b4+c3+b1c3+b4c3
3- a1+a2+b1+b2+b3+b4+c1+b1c1+b2c1+b3c1+b4c1
4- a3+b2+b3+b4+c3+c7+b2c3+b3c3+b4c3+b2c7+b3c7+b4c7.

This equations will generate continuously until provide the number of equations that we need for finding the solution. Then we will apply linearization to convert the nonlinear system of equation to linear of system equations and solved the final system using Gaussian elimination method to find the secret key for the second part.

5.The results

A)The result of attacking on clock based filtering generator as describe in simulation for LILI keystream generator as follow

1- The following keystream is inserted

1 0 0 1 0 1 1 1 1 1 0 0 0 0 0 0 0 1 1 1 0 0 1 0 1 1 0 1 1 0 1 0 1 0 0 0 0 1 0 0 1 1 0 1 1 0
1 0 1 1 0 1 1 1 0 1 1 1 1 1 0 0 1 1 0 1 1 1 1 0 0 0 1 1 1 1 1 1 1 1 1 1 0 0 0 0 1 1 1 0 0 0
1 1 0 1 1 1 1 1 1 1 1 1 0 0 1 0 0 0 0

This will be taken 6.3118s to recover the initial value and they will be as follow

- Initial value of clock control register is [1 1 1 1 1].
- Initial value of the filtering register is [1 1 1 1 1 1 1 1 1 1 1 1 1 1 1].

2- If the inserted key stream is

0 1 0 1 0 1 0 0 1 0 0 0 1 0 0 0 0 0 0 0 0 0 0 1 1 0 0 0 1 0 1 0 1 0 0 1 1 0 0 1 0 1 0 0 1 1 1
0 1 0 1 1 1 0 1 0 0 1 0 0 1 1 1 1 0 0 1 0 0 0 1 0 0 0 1 1 0 0 1 0 1 1 1 0 0 0 1 1 1 1 0 0 1
1 1 0 0 0 1 1 1 1 0 0 0 1 1 0 0 1 0 1 0 1 0 0 1 1 0 1 0 1

This will be taken 5.4558s to recover the initial value and they will be as follow

- Initial value of clock control register is [1 1 0 1 1].
- Initial value of the filtering register is [1 0 1 1 1 0 1 1 1 1 0 0 0 0].

B)The results of attacking on the clock control based combiner generator.

1- If the keystream inserted as in follows:

0 1 0 0 1 0 1 0 1 0 0 1 1 1 0 0 1 0 0 1 0 1 0 0 1 0 0 1 0 0 1 1 1 1 1 0 1 1 0 0
1 0 1 0 0 1 1 0 1 0 0 0 1 0 1 0 1 1 0 0 0 0 1 0 1 0 1 0 1 0 1 0 1 1 1 1 1 1 0 0
0 1 0 1 0 0 0 1

This will be taken 3.6353s to recover the initial value and they will be as follow

- Initial value of clock control register is [1 1 0 1 1]
- Initial value for the first register on the combiner is [1 0 1].
- Initial value for the second register on the combiner is [1 1 0 1].
- Initial value for the first register on the combiner is [1 1 1 0 0 0 0].

2- If the inserted key stream is

1 1 0 1 0 0 1 1 0 1 1 0 0 0 1 1 1 1 0 0 0 1 0 1 1 0 1 0 1 1 0 1 0 0 1 0 0 0 1
1 0 0 0 1 0 0 0 1 1 1 1 1 1 1 0 1 0 0 1 1 1 1 1 0 0 0 0 1 1 1 0 1 0 0 0 1 1 0 1
0 0 0 1 1 0 1

This will be taken 4.1819s to recover the initial value and they will be as follow

- Initial value of clock control register is [1 1 1 1 1]
- Initial value for the first register on the combiner is [1 1 1].
- Initial value for the second register on the combiner is [1 1 1 1].

- Initial value for the first register on the combiner is [1 1 1 1 1 1 1].

From the above results and what mentioned in the above structure, we can recognize the different between the two generators with the table(3).

Table(3) the difference between two clock control generators

	Based on filtering	Based on combiner
1- The length of keystream, with the clock control register have length L1	- 2^{L1}-1*2^{L2}-1, where L2 is the length of the filtering register.	-(2^{L1}-1)*(2^{k1}-1)*(2^{k2}-1) *(2^{k3}-1), where k1,k2,k3 are the length of the three register that used on the combiner respectively, where k1+k2+k3=L2.
2- The Time will need for generating the keystream	-Needed large time since the length of the keystream generated large than that generated from clock control based combiner.	-Lease than time will need for clock control based filtering generator.
3- The number of variables that will be appear on the system of equation is	N= $\sum_{i=1}^{d} \binom{n}{i}$. Where **n** is the length of the filtering register and, **d** is the degree of the nonlinear filtering function.	N= $\left[\sum_{i=1}^{d}\binom{n}{i}\right]-\left[\sum_{j=1}^{m}\binom{Lj}{d}\right]$ where **d**, is the degree of nonlinear combiner function, **n** is the summation of the length of total registers that used in the combiner, **m** is the number of registers, $\mathbf{L_j}$ is the length of $LFSR_j$ in the combiner .
4-The time of attack depending on the initial values spatial of the clock control.	In all cases it take time large than taken in the combiner based register.	In all cases it take time lease than taken in the filtering based register.

5.Conclusion

This paper showed the different types of attacks could be classified depending on several criteria(available information, methods, goals from attack). Algebraic attack represents the most important method against stream ciphers. The proposed key stream generator (clock control based combiner generator) increasing the complexity of the structure, and the results appear when we used algebraic cryptanalysis to compare between it and LILI 128 key stream generator , that using clock control based filtering generator more secure than clock control based combiner. In the future could be introduce developed clock control based hypered generator and applied algebraic cryptanalysis to compare among them.

References

Afzal , M.and, A. Masood, 2006,"Algebraic Cryptanalysis of A NLFSR Based Stream Cipher", IEEE.

Afzal , M.and, A. Masood, 2008, " Resistance of Stream Ciphers to Algebraic Recovery of Internal Secret States", Third 2008 International Conference on Convergence and Hybrid Information Technology, IEEE.

Albrecht, M. 2008, "Algebraic Attacks on the Courtois Toy Cipher", Cryptologia, 32: 3, 220 — 276, Copyright©Taylor & Francis Group, LLC,URL: http://dx.doi.org/10.1080/01611190802058139.

Armknecht , F. 2002 ,"linearization attack on Bluetooth key stream generator", Available on http://eprint.iacr.org/2002/191/.

Armknecht , F.2006, "Algebraic Attack on Certain Stream Ciphers" , thesis for university of Mannheim.

Armknecht, F. 2004," Algebraic Attack on Stream Ciphers", European Congress on Computational Methods in Applied Sciences and Engineering (ECCOMAS),http://th.informatik.unimannheim.de/people/armknecht.

Billet, O. and H. Gilbert 2005," Resistance of SNOW 2.0 against Algebraic Attacks", Springer-Verlag Berlin Heidelberg, CT-RSA 2005, LNCS 3376, pp. 19–28.

Bogdanov, A. M.C. Mertens, C. Paar, J. Pelzl and, A. Rupp, 2005," SMITH- A Parallel Hardware Architecture for fast Gaussian Elimination over GF(2)", Ruhr University Bochum, Germany.

Charles , J.2003," An Algebraic Cryptanalysis of Nonlinear Filter Generators using Grobner bases" , Institute National de Recherche Informatique et en Automatique(INRIA).

Chen ,K. M. Henricksen, W. Millan, J. Fuller, L. Simpson, E. Dawson, H. Lee, and S. Moon, 2005, "Dragon: A Fast Word Based Stream Cipher", available at cr.yp.to/streamciphers/dragon-128/desc.pdf.

Conrad , E.2007, "Types of Cryptographic Attacks", Cryptography, www.giac.org/cissp-papers/57.pdf .

Courtois, N. 2002, "Higher Order Correlation Attacks, XL Algorithm and Cryptanalysis of Toy crypt", Cryptography research, *ICISC 2002*, LNCS 2587, Springer-Verlag, pp. 182-199,http://eprint.iacr.org/2002/087.pdf.

Courtois, N. 2003," Fast Algebraic Attacks on Stream Ciphers with Linear Feedback", Springer, Crypto 2003, LNCS 2729, pp. 177-194.

Courtois, N. and W. Meier 2003," Algebraic Attacks on Stream Ciphers with Linear Feedback", http://www.minrank.org/toyolili.pdf .

Cryptico A/S 2006," Algebraic Analysis of Rabbit", White Paper, Version 1.1.

Hafeez, M. 2009," Attacks on Stream Cipher System" http://www.articlesbase.com/authors/mohammed-hafeez-mk/112928.

Hassan zadeh, M. and Tor Helleseth 2008," Algebraic Attack on the Alternating Step(r,s) Generator ", Norwegian Research Council.

Hoon Lee D., 2005, "Algebraic Attack on Stream Ciphers (Survey)", Information Center for Mathematical Sciences, Volume 8, Number 1, Pages 133-143.

Hoon Lee, D. J. Kim, J. Hong, J. Woo Han, and D. Moon, 2003, "Algebraic Attacks on Summation Generators", National Security Research Institute.

Huang, X. W. Huang, X. Liu, C. Wang, Z. Wang and, T. Wang, 2005, "Reconstructing the Nonlinear Filter Function of LILI-128 Stream Cipher Based on Complexity", Cornell university, http://arxiv.org/abs/cs/0702128.

Koon, K.G. Carter and, E. Dawson, 2010, " An Analysis of the RC4 Family of Stream Ciphers against Algebraic Attacks", Australasian Information Security Conference (AISC).

Kumar Bishoi, S. 2010, " Efficient Solution of Large Sparse Linear Equations over GF2 for Algebraic Attacks On Stream Ciphers", Supercomputer Education and Research Centre, Indian Institute of Science, Bangalore - 560 01.

Mattson , J.2006, "Stream Cipher Design" , KTH computer science and communication.

McDonald, C.2010," Analysis of Modern Cryptographic Primitives" thesis submitted to Macquarie University

Mehdi , S.2011," Cryptanalysis of Cryptographic Primitives and Related Topics", Selmer center, department of informatics, university of Bergen.

Mihaita, A. 2010, " Some Results on Algebraic Cryptanalysis of A5/2 Algorithm", Faculty of Mathematics and Computer Science, University of Bucharest Bucharest, ROMANIA.

Zayid Mohammed AL Hinai, S. 2007," Algebraic Attacks on Clock-Controlled Stream Ciphers", information security institution , Faculty of information Technology and, Queensland University of technology.