# Sub linear Attack of Classes of Stream ciphers

**Hashim K. Alaraji**
**Dept. of Computer**
**College of Science**
**Babylon University**
**Mohsinabdullah2@yahoo.com**

**Ruma K. Ajeena**
**Dept. of Mathematical**
**College of Education**
**Babylon University**
**ruma_kareem@yahoo.com**

## Abstract:

The cryptanalysis of stream cipher systems by using algebraic methods was took a wide range of interest of researches and studies but it still suffer from weak in solving complex system with high nonlinear because of hardness of translating high nonlinear systems to linear form that the reason why it became fruitless In this paper we improve the current state of above method by partitioning the task into sub parts to facilitate the task. The proposed method present a new approach for translating part of the whole system to linear system of equations defined on GF2 which can be solve by traditional solving techniques Updated approach for solving such system presented here in this study. The method implemented on known classes of stream ciphers such as geffe, bruer, hardmard systems Demonstrated better efficiency compared with other methods in terms of complexity and time . This method is considered one of the ways of partial cryptanalysis of stream ciphers

**Keywords**

**Sub linear attack , cryptanalysis , stream ciphers , linearization ,algebraic attack**

**Linear equations**

## 1. Introduction

The research in cryptology is divided into cryptography and cryptanalysis. Cryptography studies the design of cryptographic systems used to preserve security of information systems. Modern cryptographic systems commonly aim at providing a number of security services, such as confidentiality, integrity, authenticity, and non-repudiation. Confidentiality stands for ensuring that information cannot be accessed by unauthorized entities or processes. Integrity is the assurance that information stays consistent, correct, and accessible. Authenticity means verifying the author of the information, and non-repudiation refers to the concept of ensuring that a contract cannot be later denied by either of the parties involved. The ability to provide these security services is assessed within cryptanalysis. The objective of cryptanalysis is to attempt to circumvent the security of the system being examined. The techniques in cryptography can be further divided into symmetric and asymmetric techniques.
The topic of this paper is new approach on cryptanalysis of stream ciphers, which are symmetric encryption primitives that have recently attracted much attention in the cryptographic community

This paper is about an emergence of a new type of partial cryptanalysis on various types of cipher systems .depend on the relation between the output z and the output of linear feedback shift registers

- Most conventional cryptanalytic methods can be classified as either algebraic or statistical cryptanalysis. In algebraic attacks, the analyst tries to expresses the cipher as a relatively simple system of algebraic equations and then solve it. Algebraic attacks have achieved some attention recently [2, 4, 6, 7]
- Algebraic cryptanalysis of a stream or block cipher consists of two steps. The first is converting a cipher system into a system of equations. The second is solving it. The core accomplishments of my research are efficient methods of solving systems of polynomial or linear equations over the field GF (2) = {0, 1}. The solution to the system of equations, which always exists and is unique, is the secret-key of the cipher, possession of which permits all messages to be read

Algebraic attack is implemented before on : Toyocrypt, LILI-128 (Courtois, Meier : 2003) – Bluetooth key stream generator (Armknecht, Krause : 2003)

## 2. Definitions and Notations:

For m more clearance we need to declare some of useful notations [1],[3],[9] :

- **Monomial:** In mathematics, the word **monomial** can mean two different things in the context of polynomials. The first meaning is a product of powers of variables, or formally any value obtained from 1 by finitely many multiplications by a variable. . If several variables are considered, say, *x*, *y*, *z*, then each can be given an exponent, so that any monomial is of he form $x^a y^b z^c$ with *a*,*b*,*c* nonnegative integers (taking note that any exponent 0 makes the corresponding factor equal to 1)

- **Kerckhoffs´ principle**: Security depends only on secrecy of the secret key (k) i.e
  The enemy cryptanalyst's know all details of the ciphering algorithm
- **algebraic normal form**: A Boolean function can be represented as a multivariate polynomial over F2. When the representation is reduced form, the polynomial is called the *algebraic normal form* (ANF) of *f*.
- **Linearization:** is a process of translation nonlinear equation of d monomial degree to linear equations
- **Nonlinear system :** In mathematics, a nonlinear system is a system which is not linear, i.e. a system which does not satisfy the upper position principle. Less technically, a nonlinear system is any problem where the variable(s) to be solved for cannot be written as a linear sum of independent components. Generally, nonlinear problems are difficult (if possible) to solve and are much less understandable than linear problems. Even if not exactly solvable, the outcome of a linear problem is rather predictable, while the outcome of a nonlinear is inherently not.

  linear function (or map) *f*(*x*) is one which satisfies both of the following properties:

  1. Additively: $f(x+y) = f(x) + f(y)$
  2. Homogeneity: $f(\alpha x) = \alpha f(x)$

  An equation written as:

  $$f(x) = C$$

  is called linear if *f*(*x*) is linear (as defined above) and nonlinear otherwise**.**

- **A linear Boolean function:** *L*w(*x* is a Boolean function given by $\oplus$ denotes the Boolean operation 'XOR')
  *L*w(*x*) = *wx* = *w*1*x*1 $\oplus$ *w*2*x*2 $\oplus$ ….. $\oplus$.*wnx*n.

3. **Symmetric ciphers:**

Symmetric encryption ciphers are grouped into two categories,[8].

**Stream ciphers**

A stream cipher is a single-character-in, single-character-out cipher. That is, it does the encryption one character at a time.

**block ciphers:**

A block cipher encrypts whole blocks of data at a time.

We will focus here in this research on the stream_cipher since stream ciphers

**3.1 Stream ciphers:**

Stream ciphers convert plaintext to ciphertext one bit at a time. Refer to Figure 1. In this implementation, the keystream generator outputs a stream of bits: $z_1, z_2, z_3, \ldots, z_i$ . Then this key stream is XORed with a stream of plaintext bits ($p_1, p_2, p_3, \ldots, p_i$) to produce the stream of ciphertext bits. This operation is described by the formula: $c_i = p_i$ xor $z_i$ and Also we have nonlinear function f is mapping from the input linear feedback shift registers

$$\forall t : z_t = f\left(x_t^1, \ldots, x_t^n\right) \qquad \text{----------1}$$

where $x_t^i$ is denotes to linear feedback function of register $i$ so we have, for all t:

$$z_t = f\left(L^t\left(k_1, \ldots, k_n\right)\right) = f\left(L^t\left(K\right)\right) \text{-----------2}$$

where $K$ represents the whole secret key and $L^t$ is the linear function in matrix-form applied t times

To recover the plaintext bits at the decryption end, the ciphertext bits are XORed with an identical keystream. This operation is described by: $p_i = c_i$ xor $z_i$ .

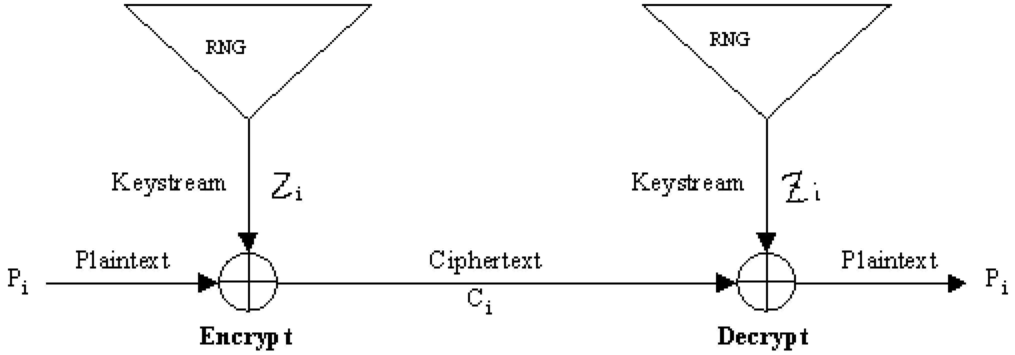

**Figure 1: XOR Stream Cipher**

where RNG denotes to running key generators .which is traditionally build by combining LFSRs of different lengths (i.e. different feedback polynomials), a keystream generator is made. To create a maximal length generator, the lengths of the constituent LFSRs must be relatively prime, and all of the feedback polynomials must be primitive modulo 2. Each time a keystream bit is required, the LFSRs are shifted once and an output bit is produced as a function of the output bits of each LFSR. The keystream generator shown below is the Geffe Generator. This keystream generator uses three LFSRs combined in a nonlinear manner. Refer to Figure 2. Two of the LFSRs are inputs into a multiplexer, and the third LFSR controls the output of the multiplexer. Suppose $a_1$, $a_2$, and $a_3$ are the outputs of the three LFSRs, then the output of the Geffe generator is the following:

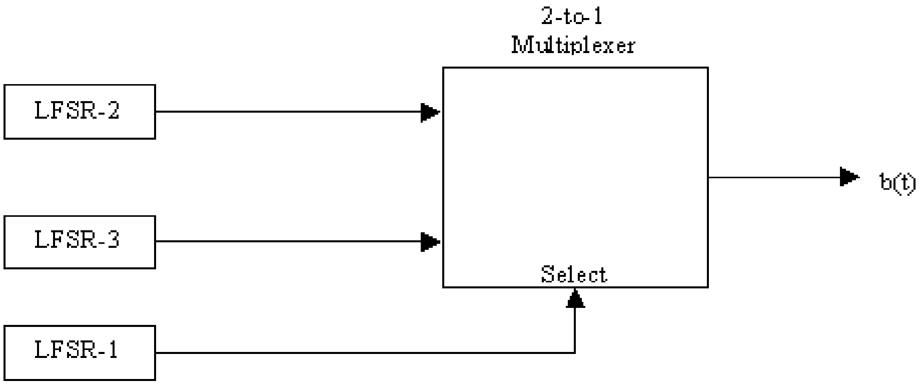

**Figure 2 Geffe generator**

$b = (a_1 \wedge a_2) \text{ xor } ((\sim a_1) \wedge a_3)$

in some resources : b= z=(a1.a2 + ¬a1.a3) mod 2 where a1,a2,a3 Є {0,1}

where ^ represents "AND" □~ represents "NOT"

The period of this combination keystream generator is the least common multiple of the periods of the three generators:

$n = n_1 * n_2 * n_3$

$= 13 * 11 * 8 = 1144$

### 3.2 Feedback Shift Registers

As shown in the diagram above. There are many possibilities for implementing a key stream generator. The one discussed here is a key stream generator based on linear feedback shift registers (LFSRs). The *linear feedback shift register* is made up of two parts: a shift register and a feedback function. The shift register is initialized with n bits (called the key), and each time a key stream bit is required, all of the bits in the register are shifted 1 bit to the right. So the least significant bit is the output bit.

The example implementation shown below uses an 8-bit register with the primitive modulo 2 polynomial $x^8+x^4+x^3+x^2+1$. Therefore, the tap sequence consists of bit 8, bit 4, bit 3, and bit 2. By XORing these bits together, the resultant LFSR will be maximal length, so it will cycle through $2^8$-1 values before repeating. Refer to Figure 3 below.

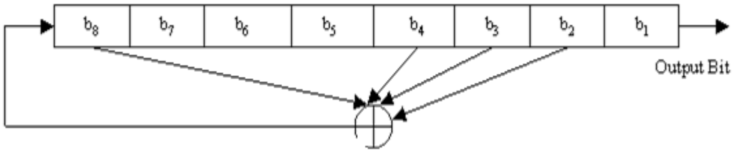

**Figure 3 : 8-bit Long Maximal-Length LFSR**

## 4. Cryptanalytic Methods:

Most conventional cryptanalytic methods can be classified as either algebraic or statistical cryptanalysis. In algebraic attacks, the analyst tries to expresses the cipher as a relatively simple system of algebraic equations and then solve it. Algebraic attacks have achieved some attention recently [7] ,[8]

### 4.1 Stream Ciphers: Attacks:

Several attack method are introduced the potential are*:*

- Key reuse (medieval)
- Time-memory tradeoffs (Babbage, 1995)
- Guess-and-determine (Günther, 1988)
- Correlation (Siegenthaler, 1984)
- Algebraic (Shamir et al., 1999)
- Backtracking (Golic, 1997)
- Binary Decision Diagrams (Krause, 2002)
- Side channel (Kocher et al., 1999)

- Resynchronization (Daemen et al. 1993)
- etc.

### 4.2 Algebraic Attacks:

Algebraic attacks one of the newest and most efficient forms of cryptanalytic attacks, especially with stream ciphers. Algebraic attacks are the fastest known attacks against some ciphers [1, 5, 6, 10]. The major drawback of the linearization approach is that it requires the knowledge of many ($\geq$ m) key stream bits .

Algebraic attacks have an important impact on the cryptanalysis of stream ciphers with a linear update function. We present a coherent framework for these attacks, quantify the properties that the stream cipher building blocks should satisfy, present a new and more Efficient algorithm and theoretical bounds . In the following we sum up the steps occurring in an algebraic attack:

1. Set up a system of equations in the unknowns K and $z_t$ , $t \geq 0$
2. Insert the observed key stream bits into the identifiers $z_t$
3. Recover K by solving the resulting equations system

While the second step is obvious, step 1 and 3 require a more careful study. The problems are how to find valid equations and how to solve the resulting system of equations anciently.

## 5. Sub Linear Cryptanalysis:

Sub word here mean this proposed method deal with partially attack of variants of ciphers not full system cause this is an attempt to exploit some weaknesses in this system enable us to reduce the variables of linear equations in previous Algebraic cryptanalysis techniques. 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. Summing up, sub linear algebraic attacks can be described as follows:
our suggested method is also consists of two steps. The first is converting generator system into a system of equations under some conditions . The second is solving it. The core accomplishments of my research are efficient methods of solving systems of polynomial or linear equations over the field GF (2) = {0, 1}. The solution to the system of equations, which always exists and is unique, is the secret-key of the cipher, possession of which permits all messages to be read. The progress in this method is in the translation procedure For example in previous methods the linearization step is done for hole system in this research its reduced to less variables equations systems As follow:
In generators like Geffe system when there is selection between two or more registers one can conclude the following two formulas:
When the out put z=0 then the nonlinear equation become
$Z=a_2 * a_3$
and when Z=1 then we conclude that:
$z =\neg a_2 * \neg a_3$

now the equivalent equations all become of the form :
$a_2 * a_3$
i.e of monomial degree d =2 we note that the variable a1 is Disappear which is in role lessen clearly the complexity of algebraic attack .
The experiment results show the succeed of this attack on geffe , bruer generators

## 6. Conclusions:

In this paper, we introduce a new approach of algebraic attacks on stream ciphers. Algebraic attacks are to find the secret key by solving algebraic equations involving the secret key and output key stream bits. Algebraic attacks are most powerful attacks on stream cipher base on linear feedback shift registers, . LFSR-based stream ciphers might be (potentially) vulnerable to algebraic attacks. We conclude from this research :

- Sub linear attack is potential on stream ciphers that depend on selection procedure to choose the output key z.

- Algebraic attacks one of the newest and most efficient forms of cryptanalytic attacks, especially with stream ciphers
- Correlation attacks less time-consuming, but sub linear algebraic attack need less data.

## References

[1] F. Armknecht and M. Krause, Algebraic attacks on combiners with memory, Advances in Cryptology - Crypto 2003, LNCS 2729, Springer-Verlag, pp. 162–175, 2003.

[2] Frederik Armknecht. Improving fast algebraic attacks. In B. Roy, editor, Fast Software Encryption, FSE 2004, number 3017 in Lecture Notes in Computer Science, pages 65{82. Springer-Verlag, 2004.

[3] Frederik Armknecht, Matthias Krause: Algebraic Attacks on Combiners with Memory,Crypto 2003, LNCS 2729, pp. 162-176, Springer, 2003.

[4] Frederik Armknecht: Improving fast algebraic Attacks, Fast Software Encryption 2004, LNCS3017, pp. 65 - 82, Springer, 2004

[5] Jean-Charles Faug_ere, Gwenole Ars: An algebraic cryptanalysis of nonlinear _lter generators using Gr☐obner bases, 2003. Available at http://www.inria.fr/rrrt/rr-4739.html.

[6] Nicolas Courtois: Higher Order Correlation Attacks, XL Algorithm and Cryptanalysis of Toyocrypt, ICISC 2002, LNCS 2587. An updated version (2002) is available at http://eprint.iacr.org/2002/087/.

[7] Nicolas Courtois, Willi Meier: Algebraic Attacks on Stream Ciphers with Linear Feed-back, Eurocrypt 2003, LNCS 2656, pp. 345-359, Springer, 2003. extended version is available at http://www.minrnak.org/toyolili.pdf

[8] Nicolas Courtois: Higher Order Correlation Attacks, XL algorithm and Cryptanalysis of Toyocrypt, ICISC 2002, LNCS 2587, pp. 182-199, Springer.

[9] R. A. Rueppel. Design and Analysis of Stream Ciphers. Springer–Verlag, 1986.

[10] S. Babbage. A space/time tradeoff in exhaustive search attacks on stream ciphers. In European Convention on Security and Detection, volume 408 of IEE Conference Publication, 1995.