Journal of Emerging Trends in Computer Science and Applications (JETCSA), Volume 1 (Issue 2: May-August, 2025): Pages 17-24; Published on: September 10, 2025.

ISSN: XXXX-XXXX Awaiting for Approval (Online)
Journal of Emerging Trends in Computer Science and Applications(JETCSA)
Contents available at: https://www.swamivivekanandauniversity.ac.in/jetcse/

A Study on Algebraic Attacks over Stream Cipher

Mr. Subrata Nandi[1]

[1]*Department of Computer Science and Engineering, Swami Vivekananda University, Barrackpore-700121, WB, INDIA*

ABSTRACT

There are several known-plaintext attacks(KPA) on Stream cipher. Algebraic Attack is one kind of KPA. In this paper, we study the fundamental aspects of algebraic attack on Stream Cipher. We also study one of the important property related to Algebraic Attack, Algebraic Immunity.

Keyword: Algebraic attack, Stream Cipher, Algebraic Immunity.

I. INTRODUCTION

Stream ciphers play a crucial role in security in wireless communication. To produce the ciphertext bits, it does bitwise-XOR between plaintext bits and the pseudorandom bits(keystream). Stream cipher A5/1 was used in 2G mobile communication, and SNOW 3G, ZUC ciphers[1] are used for 4G and 5G mobile communication to restore confidentiality and integrity. The primary component of the Stream cipher is the keystream generator(KSG). Linear Feedback Shift Register(LFSR) is a very useful KSG. This is because of their low hardware cost, good statistical properties and good periods. Nonlinear Function is used with LFSR to resist the KSG from BMA attack.

Attacks against stream cipher are another threat. Algebraic attack is one of the attacks that Courtois and Meier[2] on EUROCRYPT 2003. There are two fundamental models of stream ciphers: combiner generator and filter generator, where a nonlinear boolean function f takes important roles to generate pseudorandom bits. It can be observed [3] that If a function f or its complement $1 + f$ has low degree annihilators, one can construct equations of degree equal to the

* Authors for Correspondence

degree of the annihilators. So, the designer should not use such boolean functions of having lowdegree annihilators. To resist algebraic attack, algebraic immunity(AI) [4] takes a significant role. AI is nothing but the minimum degree annihilator between f or $1 + f$. Details of the study on algebraic immunity will be discussed in a later section.

A) Literature Survey

Algebraic Attack was ideated by Courtois [2] in 2003. It found vulnerabilities in Toyocrypt, LILI-128 ciphers. This article[5] explains theoretical analysis regarding the algebraic immunity of nonlinear boolean functions. Later, Billet [6] explains the algebraic attacks on the cipher SNOW 2.0 in time complexity 2^{51}. In addition to that, [7] improved the attack with time complexity 2^{291}. Besides, [8] mentions the algebraic attack on the Welch-Gong family of stream ciphers. The article [9] attacks Bluetooth stream cipher E_0 with 2^{79} time complexity using SAT solver, Binary Decision Diagram and Grobner Basis. In this article, we explain the basics of Algebraic Attack.

II. PRE-REQUISITES

Here, we study some definitions and properties of Boolean functions. Weight $wt(x)$ of a vector

2

x in Fn is the number of one count in x. Let f be a n variable boolean function defined as follows f: V$_n$ → F$_2$

where V_n is the domain of n dimensional vector space and F_2 is the binary field of 2 elements. The hamming distance between two boolean functions f and g of n variable is $\mathrm{wt}(\mathrm{f}+\mathrm{g})$. The degree of a Boolean function is defined as the length of the longest monomial in its polynomial representation.

If f is a variable, then a boolean function's algebraic normal form representation is The ring $\mathbb{F}2$ $[x1, x2, \ldots, sn\ ]/< x12 - x1, x22 - x2, \ldots, xn2 - xn >$ can be used to describe boolean functions in the polynomial form over the field $F2$ with n many indeterminates $x1, x2, \ldots, xn, f\ f(x1, x2\ , \ldots , xn\ )\ \ ai\ xi\ \ ai\ xi + \cdots + ai1,\ldots,in\ xi1\ \ldots\ xin{-}1 + a1,\ldots,n\ x1\ \ldots\ xn\ i{=}1\ 1{\leq}i{<}j{\leq}n$ where $a0$, $a1, \ldots , a1,\ldots,n \in \mathbb{F}2$ are called the coefficient of the respective monomials. Boolean functions $f1$ and $f2$ are defined as follows: $d(f1, f2) =|\ \{x \in \mathbb{F}n2\ |f1(x) \neq f2\ (x)|$. The cryptographic boolean function depends on the Walsh coefficient of a vector. This definition applies to any vector u that is a member of

$$\mathbb{F}n2\colon \sum_{x\in\mathbb{F}n2} (-1)f(x)\oplus = Wf\ (u) <u,x>$$

A Boolean function $nl(f)$ is said to be nonlinear if

$$nl(f) = \{\min d(f,l)\ |\deg(l) \leq 1\}$$

It can also be defined to walsh coefficient like the following:

$$nl(f) = 2^{n-1} - \frac{1}{2}\max_{u\in\mathbb{F}_2^n}|W_f(u)|$$

A) Algebraic Attack on NLFSR

The section currently available on creating low-degree algebraic equations will be discussed in this section. This algebraic attack is feasible with two fundamental LFSR-based stream cipher models like a nonlinear filter generator and a nonlinear combiner. Assume that a linear update function, represented by k bit LFSRs, is used in the model.

$L\colon \mathbb{F}n2 \rightarrow \quad \mathbb{F}n2$

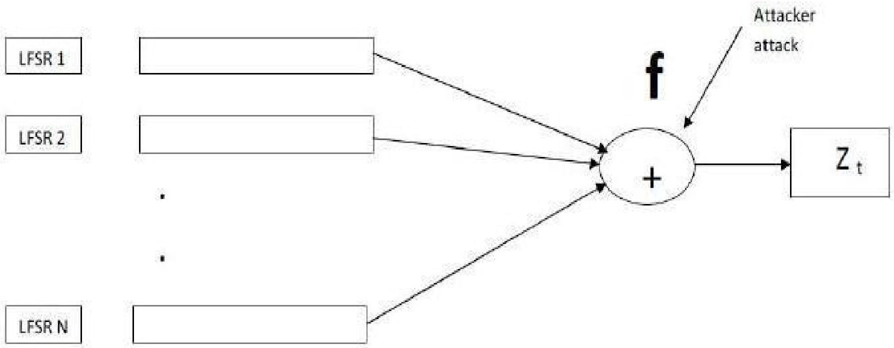


Fig. 1. Nonlinear Combiner Generator

Let $\boldsymbol{S}0 = \{s0, s1, \ldots, sk{-}1\}$ be the initial state. The keystream output will be $zt = f(S\ t\ )$, $t \geq 0$ at the t -th clock, where f is the nonlinear function. The state when the linear function L is applied to the state S 0 t times is shown by the equation $S\ t = Lt\ (S\ 0)$. Restoring the starting state is the issue. $\boldsymbol{S}0$ is equal to $\{s0, s1, \ldots, sk{-}1\}$. Some keystream bits (e.g., $zk1$, $zk2$, …, zkl) are known if an attacker exploits the known plaintext attack. Therefore, it is simpler to create a system of equations with degree equal to deg(f) in the manner described below:

$$f(L_{k1}(S_0)) = z_{k1}$$

$$f(L^{k2}(S^0)) = z_{k2}$$

$$\vdots$$

$$f(L_{kl}(S_0)) = z_{kl}$$

The system of equations will be more challenging to solve in terms of time if the degree of the nonlinear functions f is high. Low-degree equations can be constructed by exploiting a flaw in the fundamental structure of nonlinear functions. We know that $f(Lt\ (S\ 0)) = f(S\ t\ ) = zt$. The fundamental idea [10] is to use low-degree multiples and annihilators of the nonlinear function f to construct a low-degree equation. Therefore, the degree of fg will be minimized by multiplying $f(S\ t)$, which is usually of high degree, by a well chosen function $g(S\ t)$.

1. if $z_t = 1$, any function g in $AN(f)$ leads to $g(L^t(S^0)) \qquad = \qquad 0.$

2. if $z_t = 0$, any function h in $AN(1 \qquad + \qquad f)$ leads to $h(L^t(S^0)) = \qquad 0.$

Thus, if we can collect the relations to all functions of degree at most d (obviously < deg$\boxed{f0}$$(f)$) in $AN(f) + AN(1 + f)$ for known L keystream bits, we can derive a reduced degree equation on n variables $x1$, $x2$, …, xn. Thus, we may recover the bits of the original state by solving the multivariate polynomial problem.

Definition II.1. A Boolean function g over $\mathbb{F}^n{}_2$ is an annihilator $AN(f)$ of a Boolean function f over

$\mathbb{F}^n{}_2$ if

$$fg = 0$$

The degree of the Boolean function g over $\mathbb{F}n2$, where g is a nonzero function of lowest degree such that $fg = 0$ or $(1 + f)g = 0$, is the algebraic immunity $AI(f)$ of a Boolean function f over $\mathbb{F}n2$.

[7] For each function f over $\mathbb{F}$, it is known.

In commutative algebra and computational algebraic geometry, solving the system of multivariate algebraic equations is a crucial topic. Even if the basis field is $\mathbb{F}2$ and all the equations are quadratic, the issue is NP-complete. XL, XSL, and Grobner basis algorithms are some of the methods now in use to solve those multivariate equations ($F4$, $F5$).

B) Theoretical Results on Algebraic Immunity

Theorem II.1. [4] Let $f \in B_n$ (set of n variable Boolean functions) and $AI_n(f) > d$. Then

$$\sum_{i=0}^{d} \binom{n}{i} \leq wt(f) \leq \sum_{i=0}^{n-(d+1)}$$

Proof. Let f has an annihilator g of degree d. Let the ANF of g is

$$a^0 + \sum_{i=1}^{10} a_i x_i + \sum_{1\leq i<j\leq n}^{10} a_i x_i + \cdots + a_{i1,\ldots,id}\, x_{i1} \ldots x_{id}$$

where $\mathbb{F}2$ is where the a's are. Since $g \in AN(f)$, we are aware that $f(x) = 1$ implies $g(x) = 0$. The number of homogeneous equations on the a's will be $wt(f)$.

We can identify annihilators g of degree < d on nontrivial solutions by solving the system of homogeneous linear equations. Since we are interested in nonzero g, we are not interested in the trivial case, when all of the a's are equal to zero.

Here, we $\sum_{i=0}^{d} (\ )$ $n\ i$ have number of variables and $wt(f)$ many equations. We shall obtain nontrivial answers if the number of variables surpasses the number of equations. As a result, f has no annihilator g of degree d, suggesting that there are more equations than variables. Therefore, a minimum of $\sum di$=0 (ni) equations must exist, i.e., $wt(f) \geq \sum di$=0 (ni). Likewise, when considering $1 + f$, we get $wt(1 + f) \geq \sum^{d}{}_{i=0}({}^{n}i$). From this we can say, $wt(1 + f) \leq 2^n -$

$\sum_{i=0}^{d} (\ )$ i . $(f) \leq \sum_{i=0}^{n-(d+1)} (\ )$ n n i.e., wt i .

n

It also gives alternative proof [4]$AI\ (f)$ $\leq$ ⌈ ⌉. The inequality in the above theorem will not be $_2$ $_n$ satisfied if d > > $\frac{n-1}{2}$ n − (d + 1) ⇒ d⇒ d ≥ ⌈ ⌉. It is observed that for any f the inequality in $_2$ $_n$ the above theorem will not be satisfied if $AI_n(f)$ > d ≥ ⌈$_2$⌉.

The theorem's opposite isn't always accurate. For instance, the affine functions have linear annihilators but are balanced, meaning their weight is $2(n - 1)$. The following results provide a bound on $wt(f)$ based on the aforementioned theorem, where f of $1 + f$ do not n have annihilators of degree smaller than ⌈ ⌉.

].

2

n

n

Corollary II.1.1. $AI_n(f) = \lceil_2\rceil$ implies

1. f is balanced when n is odd

   n n

   -1 n $-$

2. $\sum_{i=0}^{2} \binom{}{i} \leq wt(f) \leq \sum_{i=0}^{2}$ when n is even.

Theorem II.2. If $nl(f) < \sum^{d}{}_{i=0} (^{n}i)$, then $AI_n(f) \leq d + 1$[4].

Theorem II.3. [11]Let $f \in B_n$ and $AI_n(f) = k$. Then $nl^{(f) \geq 2^{(}n-1) - \sum_{i=k-1}^{n-k} \binom{n-1}{} =_i}$

$2\sum_{i=0}^{n-k} \binom{n-1}{} \; {}_i^{\cdot}$

We derive a number of homogeneous linear equations $wt(f)$ using the a's from the previous description. This system of equations' coefficient matrix will be shown as M. A number of rows in M then contain $wt(f)$.

$\sum_{i=0}^{d} (\;)$ n $n\,i$ $i\,n\,i\,n$ $n\,i$ i

and . The rank(say, r) of the matrix $\min\{wt(f), \sum_{i=0}^{d} (\;)\}$ M, r $\leq$

1. If r, then there is no annihilator of degree $\leq$ d .

$= \sum_{i=0}^{d} (\;)\}$ **2.** If r, then annihilators of degree $\leq d$ exist. Numerous linearly independent annihilators with degree $< d$ will exist.

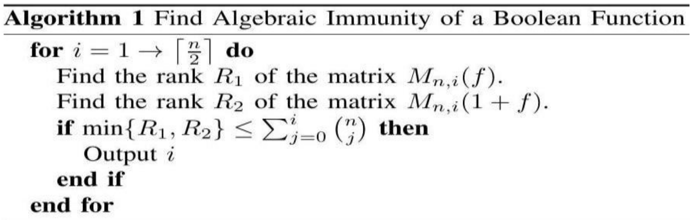
$< \sum_{i=0}^{d} (\;)\}$ The number of annihilators and linearly independent annihilators for any Boolean function f are $2wt(1+f)$ $\sum_{i=0}^{d} (\;) -$ $-$ 1

and $wt(1 + f)$. It is assumed that $Mn.d\ (f)$ is the matrix representation of the boolean function f with n variables and algebraic degree d. The row and column count of the matrix are $wt(f)$. and

$\sum_{i=0}^{d} (\;)$ n

i respectively. An algorithm for Algebraic Immunity (AI) of Boolean function f

is given below.



Algorithm 1 Find Algebraic Immunity of a Boolean Function

```
for $i = 1 \to \lceil \frac{n}{2} \rceil$ do
  Find the rank $R_1$ of the matrix $M_{n,i}(f)$.
  Find the rank $R_2$ of the matrix $M_{n,i}(1 + f)$.
  if $\min\{R_1, R_2\} \leq \sum_{j=0}^{i} \binom{n}{j}$ then
    Output $i$
  end if
end for
```

If f is a balanced boolean function, the time complexity of the above algorithm is approximately $(2n-2)3$.

III. CONCLUSION

This article examines the Algebraic Immunity trait and Algebraic assaults on Stream Cipher. We know that low algebraic degree Boolean functions are vulnerable to cryptanalysis. It might be a better problem to provide an efficient algorithm than the current one because the algorithm described above, which finds algebraic immunity of the Boolean function, is exponential.

REFERENCES

[1] A. Mufeed, "A different algebraic analysis of the zuc stream cipher," *Proceedings of the 4th international conference on Security of information and networks, Brisbane, Australia*, pp. 191–198, 2011.

[2] T. Nicolas, Courtois, and M. Willi, "Algebraic attacks on stream ciphers with linear feedback," *In Advances in Cryptology*

- *Eurocrypt 2003, number 2656 in Lecture Notes in Computer Science*, pp. 345– 359, 2003.

[3] W. Meier and O. Staffelbach, "Nonlinearity criteria for cryptographic functions," in *Proceedings of the Workshop on the Theory and Application of Cryptographic Techniques on Advances in Cryptology*, ser. EUROCRYPT '89. New York, NY, USA: Springer-Verlag New York, Inc., 1990, pp. 549–562. [Online]. Available: http://dl.acm.org/citation.cfm?id=111563.111614

[4] D. K. Dalai, "On boolean functions to resist algebraic attacks: Some necessary conditions," Vdm Verlag Dr. Miller, 2010.

[5] D. K. Dalai, K. C. Gupta, and S. Maitra, "Cryptographically significant boolean functions: Construction and analysis in terms of algebraic immunity," in *International Workshop on Fast Software Encryption*. Springer, 2005, pp. 98–111.

[6] O. Billet and H. Gilbert, "Resistance of snow 2.0 against algebraic attacks," in *Topics in Cryptology–CT-RSA 2005: The Cryptographers' Track at the RSA Conference 2005, San Francisco, CA, USA, February 14-18, 2005. Proceedings*. Springer, 2005, pp. 19–28.

[7] N. T. Courtois and B. Debraize, "Algebraic description and simultaneous linear approximations of addition in snow 2.0." in *Information and Communications Security: 10th International Conference, ICICS 2008 Birmingham, UK, October 20-22, 2008 Proceedings 10*. Springer, 2008, pp. 328–344.

[8] S. Rønjom, "Improving algebraic attacks on stream ciphers based on linear feedback shift register over f 2ˆ k f 2 k,"

[9] *Designs, Codes and Cryptography*, vol. 82, pp. 27–41, 2017.

[10] R. La Scala, S. Polese, S. K. Tiwari, and A. Visconti, “An algebraic attack to the bluetooth stream cipher e0,” *Finite Fields and Their Applications*, vol. 84, p. 102102, 2022. [11] G. M., R. and J. D., *Computers and Intractability*. W H Freeman publisher, 1999.

[12] L. Mikhail, “Tight bounds between algebraic immunity and nonlinearities of high orders,” Cryptology ePrint Archive, Report 2007/444, 2007, http://eprint.iacr.org/.