On the Interpolation Attacks on Block Ciphers

A.M. Youssef and G. Gong

Center for Applied Cryptographic Research
Department of Combinatorics and Optimization
University of Waterloo, Waterloo, ON N2L 3G1
{a2youssef, ggong}@cacr.math.uwaterloo.ca

Abstract. The complexity of interpolation attacks on block ciphers depends on the degree of the polynomial approximation and/or on the number of terms in the polynomial approximation expression. In some situations, the round function or the S-boxes of the block cipher are expressed explicitly in terms of algebraic function, yet in many other occasions the S-boxes are expressed in terms of their Boolean function representation. In this case, the cryptanalyst has to evaluate the algebraic description of the S-boxes or the round function using the Lagrange interpolation formula. A natural question is what is the effect of the choice of the irreducible polynomial used to construct the finite field on the degree of the resulting polynomial. Another question is whether or not there exists a simple linear transformation on the input or output bits of the S-boxes (or the round function) such that the resulting polynomial has a less degree or smaller number of non-zero coefficients. In this paper we give an answer to these questions. We also present an explicit relation between the Lagrange interpolation formula and the Galois Field Fourier Transform.

Keywords: Block cipher, cryptanalysis, interpolation attack, finite fields, Galois Field Fourier Transform

1 Introduction

Gong and Golomb [7] introduced a new criterion for the S-box design. Because many block ciphers can be viewed as a Non Linear Feedback Shift Register (NLFSR) with input then the S-boxes should not be approximated by a monomial. The reason is that the trace functions $Tr(\zeta_j X^d)$ and $Tr(\lambda X)$ have the same linear span. From the view point of m-sequences [10], both of the sequences $\{Tr(\zeta\alpha^{id})\}_{i\geq 0}$ and $\{Tr(\lambda\alpha^i)\}_{i\geq 0}$ are m-sequences of period 2^n-1. The former can be obtained from the later by decimation d. Gong and Golomb showed that the distance of DES S-boxes approximated by monomial functions has the same distribution as for the S-boxes approximated by linear functions.

In [3] Jakobsen and Knudsen introduced a new attack on block ciphers. This attack is useful for attacking ciphers using simple algebraic functions as S-boxes. The attack is based on the well known Lagrange interpolation formula. Let R be

B. Schneier (Ed.): FSE 2000, LNCS 1978, pp. 109–120, 2001.

a field. Given $2n$ elements $x_1, \ldots, x_n, y_1, \ldots, y_n \in R$, where the x_is are distinct. Define

$$f(x) = \sum_{i=1}^{n} y_i \prod_{1 \le j \le n, j \ne i} \frac{x - x_j}{x_i - x_j}. \quad (1)$$

Then $f(x)$ is the only polynomial over R of degree at most $n-1$ such that $f(x_i) = y_i$ for $i = 1, \ldots, n$. The main result in [3] is that for an iterated block cipher with block size m, if the cipher-text is expressed as a polynomial with $n \le 2^m$ coefficients of the plain-text, then there exists an interpolation attack of time complexity n requiring n known plain-texts encrypted with a secret key K, which finds an algorithm equivalent to encryption (or decryption) with K. This attack can also be extended to a key recovery attack.

In [4] Jakobsen extended this cryptanalysis method to attack block ciphers with probabilistic nonlinear relation of low degree. Using recent results from coding theory (Sudan's algorithm for decoding Reed-Solomon codes beyond the error correction parameter[6]), Jakobsen showed how to break ciphers where the cipher-text is expressible as evaluations of unknown univariate polynomial of low degree m with a typically low probability μ. The known plain-text attack requires $n = 2m/\mu^2$ plain-text/cipher-text pairs. In the same paper, Jakobsen also presented a second attack that needs access to $n = (2m/\mu)^2$ plain-text/cipher-text pairs and its running time is polynomial in n.

It is clear that the complexity of such cryptanalytic attacks depends on the degree of the polynomial approximation or on the number of terms in the polynomial approximation expression. In some situations, the round function or the S-boxes of the block cipher are expressed explicitly in terms of algebraic function (For example see [8]), yet in many other occasions the S-boxes are expressed in terms of their Boolean function representation. In this case, the cryptanalyst has to evaluate the algebraic description of the S-boxes or the round function using the Lagrange interpolation formula. A natural question is what is the effect of the choice of the irreducible polynomial used to construct the finite field on the degree of the resulting polynomial. Another question is whether or not there exists a simple linear transformation on the input or output bits of the S-boxes (or the round function) such that the resulting polynomial has a less degree or smaller number of coefficients. In this paper we give explicit answer to these questions. To illustrate the idea, consider the binary mapping from $GF(2)^4$ to $GF(2)^4$ given in the Table 1. If the Lagrange interpolation formula is applied to $GF(2^4)$ where $GF(2^4)$ is defined by the irreducible polynomial $X^4 + X^3 + 1$ then we have $F(X) = X + X^2 + 7X^3 + 15X^4 + 5X^5 + 14X^6 + 14X^8 + 2X^9 + 7X^{10} + 9X^{12}, X \in GF(2^4)$. However, if we use the irreducible polynomial $X^4 + X + 1$ to define $GF(2^4)$ then we have $F(X) = X^3, X \in GF(2^4)$ which is obviously a simpler description.

An interesting observation follows when applying the Lagrange interpolation formula to the DES S-boxes. In this case we consider the DES S-boxes output

x	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$f(x)$	0	1	8	15	12	10	1	1	10	15	15	12	8	10	8	12

Table 1.

coordinates as a mapping from $GF(2^6)$ to $GF(2)$. Let f be the Boolean function resulting from XORing all the output coordinates of the DES S-box number four. When we define $GF(2^6)$ using the irreducible polynomial $X^6 + X^5 + 1$, the polynomial resulting from applying the Lagrange interpolation formula to f has only 39 nonzero coefficient. The Hamming weight of all the exponents corresponding to the nonzero coefficients was ≤ 3. It should be noted that the expected value of the number of nonzero coefficients for a randomly selected function over $GF(2^6)$ is 63. While this observation doesn't have a cryptanalytic significance, it shows the effect of changing the irreducible polynomial when trying to search for a polynomial representation for cipher functions.

2 Mathematical background and definitions

For a background about the general theory of finite fields, the reader is referred to [1] and for a background about finite fields of charachteristic 2, the reader is referred to [2].

Most of the results in this paper can be extended in a straightforward way from $GF(2^n)$ to $GF(q^n)$. Throughout this paper, we use integer labels to present finite field elements. I.e., for any element $X \in GF(2^4)$, $X = \sum_{i=0}^{n-1} x_{i+1}\alpha^i, x_i \in GF(2)$ where α is a root of the irreducible polynomial which defines $GF(2^n)$, we represent X by $\sum_{i=0}^{n-1} x_{i+1}2^i$ as an integer in the range $[0, 2^n - 1]$. The associated addition and multiplication operations of these labels are defined by the finite field structure and have no resemblance to modular integer arithmetic.

Definition 1. A polynomial having the special form

$$L(X) = \sum_{i=0}^{t} \beta_i X^{2^i} \tag{2}$$

with coefficients β_i from $GF(2^n)$ is called a linearized polynomial over $GF(2^n)$.

Definition 2. A cyclotomic coset mod N that contains an integer s is the set

$$C_s = \{s, sq, \ldots, sq^{m-1}\} \pmod{N} \tag{3}$$

where m is the smallest positive integer such that $sq^m \equiv s \pmod{N}$.

Lemma 3. *Let A be a linear mapping over $GF(2^n)$, then $A(X), X \in GF(2^n)$ can be expressed in terms of a linearized polynomial over $GF(2^n)$. I.e., we can express $A(X)$ as*

$$A(X) = \sum_{i=0}^{n-1} \beta_i X^{2^i} \tag{4}$$

Lemma 4. *Let $\alpha_1, \alpha_2, \ldots, \alpha_t$ be elements in $GF(2^n)$. Then*

$$(\alpha_1 + \alpha_2 + \ldots + \alpha_t)^{2^k} = \alpha_1^{2^k} + \alpha_2^{2^k} + \ldots + \alpha_t^{2^k} \tag{5}$$

Lemma 5. *The number of ways of choosing a basis of $GF(2^n)$ over $GF(2)$ is*

$$\prod_{i=0}^{n-1} (2^n - 2^i) \tag{6}$$

3 Lagrange coefficients, Galois Field Fourier Transform and Boolean functions

3.1 Relation between the Galois Field Fourier Transform and the Lagrange coefficients

In this section we give an explicit formula for the relation between the Lagrange Interpolation of F and the Galois Field Fourier Transform of its corresponding sequence. Besides its theoretical interest, the cryptographic significance of this relation stems from the view point of Gong and Golomb [7] where they model many block ciphers as a Non Linear Feedback Shift Register (NLFSR) with input.

Let $\mathbf{v} = (v_0, v_1, \ldots, v_{l-1})$ be a vector over $GF(q)$ whose length l divides $q^m - 1$ for some integer positive m. Let α be an element of order l in $GF(q^m)$. The Galois field Fourier transform (GFFT) [11] of $\mathbf{v}$ is the vector $\mathcal{F}(\mathbf{v}) = \mathbf{V} = (V_0, V_1, \ldots, V_{l-1})$ where $\{V_j\}$ are computed as follows.

$$V_j = \sum_{i=0}^{l-1} \alpha^{-ij} v_i, j = 0, 1, \ldots, l-1. \tag{7}$$

The inverse transform is given by

$$v_i = \frac{1}{l} \sum_{j=0}^{l-1} \alpha^{ij} V_j, i = 0, 1, \ldots, l-1. \tag{8}$$

In the literature, α and α^{-1} are swapped in the equations above. Since α and α^{-1} have the same order, we may use the form presented here. We use this form in order to make it easy to compare with the polynomial representation. For the purpose of our discussion, we will consider the case with $q = 2^n$, $m = 1$ and $l = 2^n - 1$. For a detailed discussion of the general case relation between the Lagrange Interpolation formula and the GFFT, the reader is referred to [13].

Theorem 6. *Let* $F(X) = \sum_{i=0}^{2^n-1} b_i X^i$ *be a function in* $GF(2^n)$ *with the corresponding sequence* $\mathbf{v} = (v_0, v_1, \ldots, v_{2^n-2})$ *where* $v_i = F(\beta^i), i = 0, 1, \ldots, 2^n - 2$ *and* $\beta \in GF(2^n)$ *has order* $2^n - 1$. *If* $F(0) = 0$ *then we have*

$$b_i = \begin{cases} 0 & \text{if } i = 0 \\ V_i & \text{if } 0 < i \leq 2^n - 2, \\ V_0 & \text{if } i = 2^n - 1, \end{cases} \tag{9}$$

Proof: For functions in $GF(2^n)$, the Lagrange interpolation formula can be rewritten as

$$F(X) = \sum_{i=0}^{2^n-1} b_i X^i = \sum_{\beta \in GF(2^n)} F(\beta)(1 + (X + \beta)^{2^n-1}), \tag{10}$$

where

$$b_i = \begin{cases} F(0) & \text{if } i = 0, \\ \sum_{\alpha \in GF(2^n)} F(\alpha)\alpha^{-i} & \text{if } 1 \leq i \leq 2^n - 1 \end{cases} \tag{11}$$

Equation (7) can be written as

$$V_i = \sum_{j=0}^{2^n-2} \beta^{-ij} v_j = \sum_{j=0}^{2^n-2} \beta^{-ij} F(\beta^j) = \sum_{\alpha \in GF^*} \alpha^{-i} F(\alpha), \tag{12}$$

where $GF^* = GF(2^n) - \{0\}$. With the convention $0^t = 1$ for any integer t, if $F(0) = 0$, then

$$\sum_{\alpha \in GF^*} \alpha^{-i} F(\alpha) = \sum_{\alpha \in GF(2^n)} \alpha^{-i} F(\alpha). \tag{13}$$

From Equation (11) and (12) we get

$$b_i = V_i, 0 < i \leq 2^n - 2. \tag{14}$$

The result for $i = 2^n - 1$ follows by noting that

$$V_0 = \sum_{\alpha \in GF^*} F(\alpha), \tag{15}$$

and

$$b_{2^n-1} = \sum_{\alpha \in GF(2^n)} F(\alpha)\alpha^{-(2^n-1)} = \sum_{\alpha \in GF(2^n)} F(\alpha) = V_0 \tag{16}$$

which completes the proof. □

If $F(0) \neq 0$, then we can compute its polynomial representation by first computing the polynomial representation of the function G, where $G(X) = 0$ for $X = 0$ and $G(X) = F(X)$ otherwise. If we assume that $F(X) = \sum_{i=0}^{2^n-1} d_i X^i$ and $G(X) = \sum_{i=0}^{2^n-1} b_i X^i$ and by noting that we can express $F(X)$ as

$$F(X) = G(X) + F(0)(1 + X^{2^n-1}), \tag{17}$$

then we have

$$d_i = \begin{cases} F(0) & \text{if } i = 0, \\ b_i & \text{if } 0 < i < 2^n - 1, \\ b_{2^n-1} + F(0) & \text{if } i = 2^n - 1, \end{cases} \tag{18}$$

3.2 Relation between Boolean functions and its Galois filed polynomial representation

Let $F_2 = GF(2)$ and $F_2^{(n)} = \{x_1, \ldots, x_n | x_i \in F_2\}$. Let $f(x_1, \ldots, x_n)$ be a function from F_2^n to $F_2^{(n)}$. Then $f(x_1, \ldots, x_n)$ can be written as $f(x_1, \ldots, x_n) = (y_1, \ldots, y_n)$, where y_j is a Boolean function in n variables, i.e., $y_j = y_j(x_1, \ldots, x_n)$. Since $F_2^{(n)}$ is isomorphic to $GF(2^n)$, then $f(x_1, \ldots, x_n)$ can be regarded as a function F from $GF(2^n)$ to $GF(2^n)$.

It is well known that applying a linear transformation to a function f doesn't change its nonlinear degree. It is also known that the nonlinear degree of the function $f(X) = X^d$ is $wt(d)$. The following theorem illustrates the effect of applying a linear transformation to the output coordinates of f on the coefficients of its corresponding polynomial.

Theorem 7. *Let $F(X) = X^d$ be a function of $GF(2^n)$ which corresponds to the Boolean mapping $f(x_1, \ldots, x_n) = (f_1(x), \ldots, f_n(x))$ over $F_2^{(n)}$. Then the function $G(X)$ corresponding to the Boolean mapping obtained by applying a linear transformation to the output coordinates of $f(x_1, \ldots, x_n)$ can be expressed as $G(X) = \sum_{i=0}^{2^n-1} b_i X^i$, where $b_i = 0 \forall i \notin C_d$ and C_d is the cyclotomic coset* (mod $2^n - 1$) .

Proof: Using Lemma 3, $G(X)$ can be expressed as

$$G(X) = \sum_{i=0}^{n-1} (a_i F(X))^{2^i} = \sum_{i=0}^{n-1} (a_i X^d)^{2^i} = \sum_{i=0}^{n-1} a_i^{2^i} X^{d2^i}. \tag{19}$$

The Theorem follows directly by noting that $X^{d2^i} = X^{(d2^i) mod (2^n-1)}$ for $X \in GF(2^n)$. □

Similarly, one can show that if $F(X) = \sum_{i \in I} a_i X^i$, then $G(X) = \sum_{j \in J} b_j X^j$ where J is the set of cyclotomic cosets modulo $2^n - 1$ corresponding to the set I.

Example 1. Consider the Boolean mapping $f(x)$ in the Table 2. Assuming $GF(2^4)$

x	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$f(x)$	0	1	4	5	9	8	13	12	15	14	11	10	6	7	2	3
$g(x)$	0	2	4	6	10	8	14	12	15	13	11	9	5	7	1	3

Table 2.

is constructed using the irreducible polynomial $X^4 + X^3 + 1$, we have $F(X) = X^2$. Let $g(x)$ be the function obtained from $f(x)$ by swapping the least significant bits of the output. I.e., $g(x_1, x_2, x_3, x_4) = (f_1(x), f_2(x), f_4(x), f_3(x))$, then we have $G(X) = 2X + 10X^2 + 6X^4 + 12X^8$.

The following theorem illustrates the effect of applying a linear transformation to the input coordinates of a given Boolean function on the coefficients of its corresponding polynomial.

Theorem 8. *Let $F(X) = X^d$ be a function of $GF(2^n)$ which corresponds to the Boolean mapping $f(x_1, \ldots, x_n) = (f_1(x), \ldots, f_n(x))$ over $F_2^{(n)}$. Let $G(x)$ be the function which corresponds to the Boolean mapping obtained by applying a linear transformation to the input coordinates of $x_1, \ldots, x_n$ while fixing $f(x_1, \ldots, x_n)$. Then $G(X)$ can be expressed as $G(X) = \sum_{i=0}^{2^n-1} b_i X^i$, $b_i = 0$ for $wt(i) > wt(d)$, where $wt(d)$ denotes the Hamming weight of d.*

Proof: Using Lemma 3, $G(X)$ can be expressed as

$$G(X) = (\sum_{i=0}^{n-1} c_i X^{2^i})^d \tag{20}$$

Let $d = \sum_{j=0}^{n-1} d_j 2^j$ and let J denote the set $\{j_1, \ldots, j_s\}, s = wt(d)$, for which $d_j = 1$. Then we have

$$G(X) = \prod_{j \in J} (\sum_{i=0}^{n-1} c_i X^{2^{i+j}}) \tag{21}$$

$$= (\sum_{i_1=0}^{n-1} c_{i_1} X^{2^{i_1+j_1}})(\sum_{i_2=0}^{n-1} c_{i_2} X^{2^{i_2+j_2}}) \ldots (\sum_{i_1=0}^{n-1} c_{i_s} X^{2^{i_1+j_s}}) \tag{22}$$

$$= \sum_{i_1, i_2, \ldots, i_s} c_{i_1} c_{i_2} \ldots c_{i_s} X^{2^{i_1+j_1} + 2^{i_2+j_2} + \ldots + 2^{i_s+j_s}} \tag{23}$$

The Theorem follows by noting that $wt(2^{i_1+j_1} + \ldots + 2^{i_s+j_s}) = s \leq wt(d)$. □

Let $W = \max_{i \in I} wt(i)$. Then one can show that if $F(X) = \sum_{i \in I} a_i X^i$, then $G(X) = \sum_{j \in J} b_j X^j$ where J is the set of elements with Hamming weight $\leq W$.

The following theorem illustrates the effect of changing the irreducible polynomial used to construct the finite field on the coefficients resulting polynomial.

Theorem 9. *Let $F(X)$ be a function of $GF(2^n)$ which corresponds to the Boolean mapping $f(x_1, \ldots, x_n) = (f_1(x), \ldots, f_n(x))$ over $F_2^{(n)}$ using irreducible R_1. Then the function $G(x)$ which corresponds to the boolean mapping $f(x_1, \ldots, x_n)$ and constructed using a different irreducible polynomial $R_2 \neq R_1$ can be expressed as*

$$G(X) = L(F(L^{-1}(X))), \tag{24}$$

where L is an invertible linear transformation over $GF(2^n)$.

Proof: Consider the finite field generated by an irreducible polynomial $R_1(X)$. In this case, $GF(2^n) = F_2[X]/(R_1(X)) = \{\sum_{i=0}^{n-1} c_i X^i | c_i \in F_2\}$ where the multiplication is performed by modulus $R_1(X)$. Then every element in the field can be expressed as $\sum_{i=0}^{n-1} a_i \alpha^i$ where $a_i \in GF(2)$ and α is a root of $R_1(X)$. Similarly, if the field was generated using an irreducible polynomial $R_2(X)$. In this case, $GF(2^n) = F_2[X]/(R_2(X)) = \{\sum_{i=0}^{n-1} c_i X^i | c_i \in F_2\}$ where the multiplication is performed by modulus $R_2(X)$. In this case, every element in the field can be expressed as $\sum_{i=0}^{n-1} b_i \beta^i, b_i \in GF(2)$ where β is a root of $R_2(x)$. However, we can express β^i as

$$\beta^i = \sum_{j=0}^{n-1} a_j \alpha^j, a_j \in GF(2), 0 \leq i < n. \tag{25}$$

This means that we can write $G(X) = L(F(L^{-1}(X))$ where $L(.)$ is the linear transformation used to convert between the α and the β basis. □

From the theorem above changing the irreducible polynomial is equivalent to applying a linear transformation to both the input and the output coordinates, and hence we have the following corollary

Corollary 10. *Let $F(X) = \sum_{i \in I} a_i X^i$ be a function of $GF(2^n)$ which corresponds to the Boolean mapping $f(x_1, \ldots, x_n) = (f_1(x), \ldots, f_n(x))$ over $F_2^{(n)}$ using irreducible R_1. Let the $W = \max_{i \in I} wt(i)$. Then the function $G(x)$ corresponds to the boolean mapping $f(x_1, \ldots, x_n)$ and constructed using a different irreducible polynomial $R_2 \neq R_1$ can be expressed as*

$$G(X) = \sum_{j \in J} b_j X^j, \tag{26}$$

where J is the set of elements with Hamming weight $\leq W$.

Example 2. Consider the Boolean function described in Table 3.

x	0	1	2	3	4	5	6	7
$f(x)$	0	1	3	4	5	6	7	2

Table 3.

Using the irreducible polynomial $X^3 + X^2 + 1$ with root β, we have $F(X) = 2X + 2X^2 + 3X^3 + 4X^4 + X^5 + 7X^6$. Now, consider the irreducible polynomial $X^3 + X + 1$ with root α. One can prove that $\beta = \alpha^3$. Thus we have the following linear transformation

$$\begin{pmatrix} 1 \\ \beta \\ \beta^2 \end{pmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix} \begin{pmatrix} 1 \\ \alpha \\ \alpha^2 \end{pmatrix} \tag{27}$$

Applying this linear transformation to both the input and the output of the truth table we get $L^{-1}(x) and L(f(x))$ in Table 4. Interpolating the relation between $L^{-1}(x)$ and $L(f(x))$, we get $L(F(X)) = (L^{-1}(X))^3$.

x	0	1	2	3	4	5	6	7
$L^{-1}(x)$	0	1	3	2	5	4	6	7
$f(x)$	0	1	3	4	5	6	7	2
$L(f(x))$	0	1	2	5	4	6	7	3

Table 4.

To summarize the results in this section, a linear transformation on the output coordinates affects only the coefficients of the exponents that belong to the same cyclotomic cosets of the exponent in the original function representation. A linear transformation on the input coordinates or changing the irreducible polynomial affect only the coefficients of the exponents with Hamming weight less than or equal to the maximum Hamming weight of the exponents in original function representation.

4 Checking algebraic expressions for trap doors

In [5] the authors presented a method to construct trap door block ciphers which contains some hidden structures known only to the cipher designers. The sample trapdoor cipher in [5] was broken [12] and designing practical trape door S-boxes is still an intersting topic. In this section we discuss how to check if the S-boxes or the round function has a simple algebraic structure. In particular, we consider the case where we can represent the round function or the S-boxes by a monomial. The number of invertible linear transformations grows exponentially with n. Using exhaustive search to check if applying an invertible linear transformation to the output and/or the input coordinates of the Boolean function $f(x_1, \ldots, x_n) = (f_1(x), \ldots, f_n(x))$ leads to a simpler polynomial representation becomes computationally infeasible even for small values of n. In this section we show how to check for the existence of such simple description. Note that we only consider the case of polynomials over $GF(2^n)$. S-boxes with a complex algebraic expression over $GF(2^n)$ may have a simpler description over other fields.

4.1 Undoing the effect of a linear transformation on the output coordinates

First, we will consider the case of a function $G(X)$ obtained by applying a linear transformation of the output coordinates of a monomial function X^d. The

algebraic description of such a function will have nonzero coefficients only for exponents $\in C_d \pmod{2^n - 1}$. Thus $G(X)$ is expressed as

$$G(X) = \sum_{i=0}^{2^n-1} b_i X^{2^i d}, \tag{28}$$

$b_i = 0$ if $i \notin C_d$. A linear transformation of the output coordinates of $G(X)$ can be expressed as

$$L(G(X)) = \sum_{j=0}^{n-1} a_j \Big(\sum_{i=0}^{2^n-1} b_i X^{2^i d} \Big)^{2^j} \tag{29}$$

$$= \sum_{j=0}^{n-1} a_j \sum_{i=0}^{2^n-1} {b_i}^{2^j} X^{(2^{i+j})d} \tag{30}$$

By equating the coefficients of X^i to zero except for $i = d$, the above equation forms a system of $n \times n$ linear equations (with unknowns $a_i's \in GF(2^n)$) which can be checked for the existence of a solution using simple linear algebra.

Example 3. Let $G(X) = 2X + 10X^2 + 6X^4 + 12X^8, X \in GF(2^4)$ constructed using the irreducible polynomial $X^4 + X^3 + 1$, Suppose we want to check if there exists a linear transformation on the output coordinates of $G(X), L(G(X))$ such that the resulting polynomial has only one term with degree 2. Using the theorem above, form the set of 4×4 linear equations over $GF(2^4)$ we get:

$$\begin{bmatrix} b_0 & b_3^2 & b_2^4 & b_1^8 \\ b_1 & b_0^2 & b_3^4 & b_2^8 \\ b_2 & b_1^2 & b_0^4 & b_3^8 \\ b_3 & b_2^2 & b_1^4 & b_0^8 \end{bmatrix} \begin{pmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \tag{31}$$

For $G(X)$ above we have $b_0 = 2, b_1 = 10, b_2 = 6, b_3 = 12$. Thus

$$\begin{bmatrix} 2 & 6 & 7 & 11 \\ 10 & 4 & 13 & 12 \\ 6 & 11 & 9 & 7 \\ 12 & 13 & 10 & 14 \end{bmatrix} \begin{pmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} \tag{32}$$

Solving for a_i's we get

$$\begin{pmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \end{pmatrix} = \begin{pmatrix} 10 \\ 6 \\ 12 \\ 2 \end{pmatrix} \tag{33}$$

and $L(G(X)) = 10G(X) + 6G(X)^2 + 12G(X)^4 + 2G(X)^8 = X^2$

4.2 Undoing the effect of a linear transformation on the input coordinates

Consider a function $G(X)$ obtained by applying a linear transformation to the input coordinates of a monomial function X^d. The algebraic description of such a function will have zero coefficients for all exponents with Hamming weight $> d$. Thus $G(X)$ is expressed as

$$G(X) = \sum_{i=0}^{2^n-1} b_i X^i, \tag{34}$$

$b_i = 0$ if $wt(i) > d$

A linear transformation of the input coordinates of $G(X)$ can be expressed as

$$L(G(X)) = \sum_{i=0}^{2^n-1} b_i \sum_{j=0}^{n-1} (a_j X^{2^j})^i \tag{35}$$

If one tries to evaluate the above expression and equate the coefficients to the coefficients of a monomial, then one has to solve a set of non linear equations with unknowns $a_j, j = 0, 1, \ldots, n-1$.

To overcome this problem, we will reduce the problem of undoing the effect of a linear transformation on the input coordinates to undoing the effect of a linear transformation on the output coordinates.

Consider $G(X)$ obtained by a linear transformation on the input coordinates of $F(X)$. Then $G(X) = F(L(X))$. Thus we have $G^{-1}(X) = L^{-1}(F^{-1}(X))$. If $F(X)$ is a monomial, then $F^{-1}(X)$ is also a monomial and our problem is reduced to finding the linear transformation L^{-1} on the output coordinates of $F^{-1}(X)$ which is equivalent to solving a system of linear equations in n variables.

Example 4. Consider the function $G(X) = 8X^2 + 9X^3 + X^4 + 11X^5 + 14X^6 + X^7 + 12X^8 + 2X^9 + 9X^{10} + 4X^{11} + 11X^{12} + 14X^{13} + 14X^{14} \in GF(2^4)$ where $GF(2^4)$ is constructed using the irreducible polynomial $X^4 + X^3 + 1$. In this case, we have $G(X)^{-1} = 5X^7 + 5X^{11} + 11X^{13} + 15X^{14}$. In this case, we have 60 linear transformations on the output coordinates of $G^{-1}(X)$ that will map it to a monomial of exponent with weight 3. Out of these 60 transformations, we have 15 linear transformations such that $L(G^{-1}(X)) = aX^{13}, a \in GF(2^4)$. In particular, the linear mapping $L(X) = X + 14X^2 + 9X^4 + 14X^8$ on the output bits of $G^{-1}(X)$ reduces $G^{-1}(X)$ to X^{13}, i.e., $L(G^{-1}(X)) = X^{13}$ and hence $G(X) = (L(X))^7$.

Undoing the effect of changing the irreducible polynomial corresponds to undoing the effect of a linear transformation on both the input and the output coordinates which seems to be a hard problem. The number of irreducible polynomials of degree n over a finite field with q elements is given by

$$I_n = \frac{1}{n} \sum_{d|n} \mu(d) q^{n/d}, \tag{36}$$

where $\mu(d)$ is defined by

$$\mu(d) = \begin{cases} 1 & \text{if } d = 1, \\ (-1)^k & \text{if } d \text{ is the product of } k \text{ distinct primes,} \\ 0 & \text{if } d \text{ is divisible by the square of a prime.} \end{cases} \quad (37)$$

Since the dominant term in I_n occurs for $d = 1$, we get the estimate

$$I_n \approx \frac{q^n}{n} \quad (38)$$

Thus for typical S-box sizes, exhaustive search through all the set of $(2^n/n)$ irreducible polynomials seems to be a feasible task.

References

1. R. Lidl and H. Niederreiter, *Finite Fields (Encyclopedia of Mathematics and its Applications)* , Addison Wesley. Reading, MA. 1983.
2. R. J. McEliece, *Finite Fields For Computer Scientists and Engineers* , Kluwer Academic Publishers. Dordrecht. 1987.
3. T. Jakobsen and L. Knudsen, *The Interpolation Attack on Block Ciphers, LNCS 1267*, Fast Software Encryption. pp. 28-40. 1997.
4. T. Jakobsen, *Cryptanalysis of Block Ciphers with Probabilistic Non-linear Relations of Low Degree*, Proceedings of Crypto'99. LNCS 1462. pp. 213-222. 1999.
5. V. Rijmen and B. Preneel, *A family of trapdoor ciphers*, Proceedings of Fast Software Encryption. LNCS 1267. pp. 139-148. 1997.
6. M. Sudan, *Decoding Reed Solomon Codes beyond the error-correction bound*, Journal of Complexity. Vol. 13. no 1. pp180-193. March, 1997.
7. G. Gong and S. W. Golomb, *Transform Domain Analysis of DES*, IEEE transactions on Information Theory. Vol. 45. no. 6. pp. 2065-2073. September, 1999.
8. K. Nyberg and L. Knudsen, *Provable Security Against a Differential Attack*, Journal of Cryptology. Vol. 8. no. 1. 1995.
9. K. Aoki, *Efficient Evaluation of Security against Generalized Interpolation Attack*, Sixth Annual Workshop on Selected Areas in cryptography SAC'99. Workshop record. pp. 154-165. 1999.
10. S.W. Golomb,*Shift Register Sequences*, Aegean Park Press. Laguna Hills, California. 1982.
11. R.E. Blahut, *Theory and Practice of Error Control Codes*, Addison-Wesley. Reading, MA. 1990.
12. H. Wu, F. Bao, R. Deng and Q. Ye *Cryptanalysis of Rijmen-Preneel Trapdoor Ciphers, LNCS 1514*, Asiacrypt'98. pp. 126-132. 1998.
13. G. Gong and A.M. Youssef, *Lagrange Interpolation Formula and Discrete Fourier Transform* , Technical Report. Center for Applied Cryptographic Research. University of Waterloo. 1999.