A New Construction of Boolean Functions with Maximum Algebraic Immunity

National University of Defense Technology
Deshuai Dong
2009-8-26

Outline

- Preliminaries on Boolean functions
- Algebraic attacks and Algebraic immunity
- The recent constructions of Boolean functions with MAI
- The main results of our paper

Preliminaries on Boolean functions

- Boolean functions map n binary inputs to a single binary output

- More formally $f : \mathrm{F}_2^n \to F_2$ map

$$(x_1, \cdots, x_n) \in F_2^n \to x \in F_2$$

Preliminaries on Boolean functions

- It can be represented as a polynomial in the ring

$$F_2[x_1,\cdots,x_n]/<x_1^2-x_1,\cdots,x_n^2-x_n>$$

- This ring is simply a set of all polynomials with binary coefficients in n indeterminates with property that $x_i^2=x_i$

Algebraic Normal Form

- A Boolean function can be formalized further by defining

$$f(x) = \sum_{u \in F_2^n} a_u x^u = \sum_{u \in F_2^n} a_u x_1^{u_1} x_2^{u_2} \cdots x_n^{u_n}, u = (u_1, \cdots, u_n)$$

- This also can be called the algebraic normal form (ANF) of f

Algebraic degree

- Algebraic degree of a Boolean function is defined as maximum length of terms in ANF of f
- The algebraic degree should be large because of Berlekamp-Massey and Ronjom-Helleseth attacks (stream ciphers) and higher differential attack (block ciphers)

Affine and linear functions

- The set of all Boolean functions in n variables is denoted by B_n
- Boolean Functions of degree at most one are called affine

$$A_n = \{a_0 + a_1 x_1 + a_2 x_2 + \cdots + a_n x_n \mid a_i \in F_2, 0 \le i \le n\}$$

- An affine function with $a_0 = 0$ is said to be linear, and all linear functions are denoted by L_n

The Walsh Transform

- The Walsh transform of Boolean functions is defined by

$$\hat{f}(u) = \sum_{x \in F_2^n} (-1)^{f(x)+u \cdot x}$$

- The Hamming distance between two functions:

$$d_H(f, g) = w_H(f+g) = \left|\{x \mid f(x) \neq g(x)\}\right|$$

Nonlinearity definition

- The nonlinearity of a Boolean function is the minimum distance from f to all affine functions i.e.

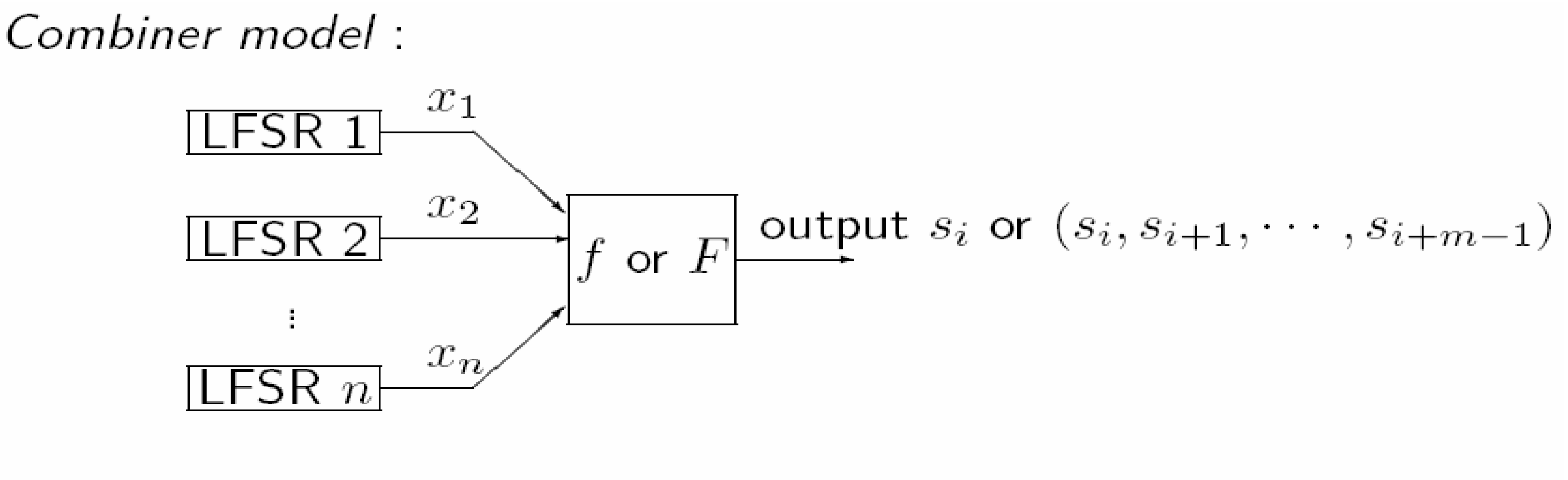
$$N_f = \min_{g \in A_n} d_H(f, g)$$

- The nonlinearity of a Boolean function f also can be represented as:

$$N_f = 2^{n-1} - \frac{1}{2} \max_{a \in F_2^n} \left| \hat{f}(a) \right|$$

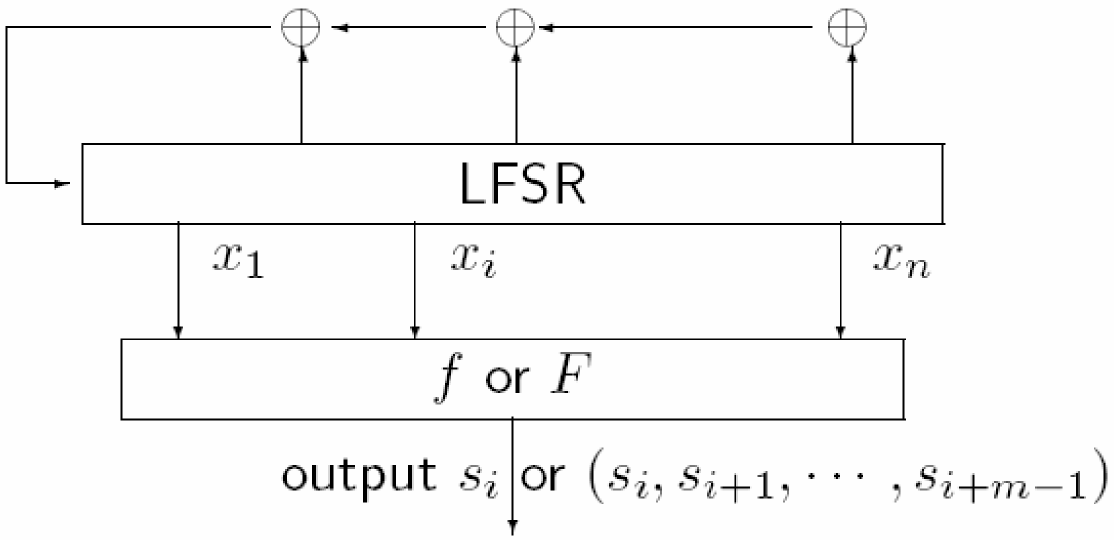
The nonlinearity must be high to prevent the system from fast correlation attacks (stream ciphers) and linear attacks(block ciphers)

The application



The application

Filter model



- Before the introduction of algebraic attacks, balancedness, high algebraic degree and high nonlinearity were considered as roughly sufficient for the filter model of PRG

Outline

- Preliminaries on Boolean functions
- Algebraic attacks and Algebraic immunity

Algebraic attacks principle(Shannon)

- Find equations with the key bits as unknowns
- Solve the system of these equations

- For stream ciphers (combining or filtering Boolean functions):

  - denote by $(s_0, \cdots, s_{N-1})$ the initial state of the linear part of the PRG

  - there exists a linear automorphism L and a linear mapping L' :

$$s_i = f(L' \circ L^i(s_0, s_1, \cdots, s_{N-1}))$$

- For stream ciphers we can have many equations, so we can gain an over-defined system
- One can linearize the system (or use Grőbner bases) to solve it

Problem of algebraic attacks

- However the number of unknowns is too large
- The common ways to solve this system are mostly impossible

Algebraic attacks

- Courtois-Meier 2003: if one can find $g \neq 0$ and h of low degree such that $fg = h$, then the equation $s_i = f(L' \circ L^i(s_0, s_1, \cdots, s_{N-1}))$ implies the following low degree equation:

$$s_i g(L' \circ L^i(s_0, \cdots, s_{N-1})) = h(L' \circ L^i(s_0, \cdots, s_{N-1}))$$

- Then the degree of the original nonlinear system and the unknowns in the related linear system decrease

Algebraic immunity

- Meier-Pasalic-C.C. EUROCRYPY 2004 :

  A necessary and sufficient condition for existence $g \neq 0$ and h of low degree such that $fg = h$:

  there exist $g \neq 0$ of low degree such that

  $f \cdot g = 0$ or $(1 + f) \cdot g = 0$

Algebraic immunity

- Given $f \in B_n$, a nonzero function g is called an annihilator of f if $f \cdot g = 0$. By $AN(f)$ we mean the set of annihilators of f
- The algebraic immunity of f, denoted by $AI(f) = \deg(g)$, where $g \in B_n$ is the minimum degree nonzero function such that $f \cdot g = 0$ either $(1+f) \cdot g = 0$

Algebraic immunity

- It is easy to prove that $AI(f) \le \deg(f)$ and $AI(f) \le \lceil n/2 \rceil$
- If the AI of a Boolean function in n-variable equals $\lceil n/2 \rceil$, we call it a maximum algebraic immunity (MAI) function.
- In practical situation, $AI(f)$ should be greater than or equal to 7
- So we need $n \ge 13$

Algebraic immunity and nonlinearity

- Lobanov (IACR e-print archive) given a tight bound between nonlinearity and algebraic immunity:

$$N_f \geq 2 \sum_{i=0}^{AI(f)-2} \binom{n-1}{i}$$

- This tight bound does not guarantee that an maximum algebraic immunity implies a good enough nonlinearity

Design criteria

- High algebraic degree
- High nonlinearity
- Resiliency (for certain applications)
- High algebraic immunity

Outline

- Preliminaries on Boolean functions
- Algebraic attacks and Algebraic immunity
- The recent constructions of Boolean functions with MAI

Three Recent constructions

- Construction based support-inclusion
- Construction based basis-exchange technique
- Construction based finite field expression

Construction based support-inclusion

- Dalai, Basic theory in construction of MAI functions, 2005
- Lemma 1. Let f, f_1, f_2 in B_n, and

(1) f_1, f_2 both have no nonzero annihilators degree less than $\left\lceil \frac{n}{2} \right\rceil$;

(2) $Supp(f) \supseteq Supp(f_1), Supp(f+1) \supseteq Supp(f_2)$ Then

$$AI(f) = \left\lceil \frac{n}{2} \right\rceil$$

Construction based support-inclusion (Cont.)

- Theorem 1. Let f in B_n, if n is odd, let

$$f(x)=\begin{cases}0, & wt(x)<\left\lceil \frac{n}{2}\right\rceil\\ 1, & wt(x)\geq\left\lceil \frac{n}{2}\right\rceil\end{cases}$$

if n is even, let

$$f(x)=\begin{cases}0, & wt(x)<\left\lceil \frac{n}{2}\right\rceil\\ 1, & wt(x)>\left\lceil \frac{n}{2}\right\rceil\\ b\in\{0,1\}, & wt(x)=\left\lceil \frac{n}{2}\right\rceil\end{cases}$$

Then $AI(f)=\left\lceil \frac{n}{2}\right\rceil$

Construction based basis-exchange technique

- Longjiang Qu, Na Li, et al., On MAI functions: construction and a lower bound of the count, 2005.
- Idea of basis-exchange technique:

Construction based basis-exchange technique (Cont.)

- Lemma 2 Let U be an m-dimension vector space, $\alpha_1, \alpha_2, \cdots, \alpha_m$ and $\beta_1, \beta_2, \cdots, \beta_m$ be two bases of U, then for any integer $1 \le k \le m$, for any k integers $1 \le i_1 < i_2 < \cdots < i_k \le m$, there exist k integers $1 \le j_1 < j_2 < \cdots < j_k \le m$ such that

$$\{\alpha_1, \alpha_2, \cdots, \alpha_m\} \cup \{\beta_{j_1}, \cdots, \beta_{j_k}\} \setminus \{\alpha_{i_1}, \cdots, \alpha_{i_k}\}$$

and

$$\{\beta_1, \beta_2, \cdots, \beta_m\} \cup \{\alpha_{i_1}, \cdots, \alpha_{i_k}\} \setminus \{\beta_{j_1}, \cdots, \beta_{j_k}\}$$

are two new bases of U.

Construction based finite field expression

- C. Carlet, K. Feng, An infinite class of balanced functions with optimal AI, good immunity to fast algebraic attacks, 2008.

Construction based finite field expression (Cont.)

Theorem 3 Let n be any integer such that $n \geqslant 2$ and α a primitive element of the field F_2^n. Let f be the Boolean function on F_2^n whose support is $\{0,1,\alpha,\alpha^2,\cdots,\alpha^{2^{n-1}-2}\}$. Then f has optimal algebraic immunity $\left\lceil \frac{n}{2} \right\rceil$.

Outline

- Preliminaries on Boolean functions
- Algebraic attacks and Algebraic immunity
- The recent constructions of Boolean functions with MAI
- The main results of our paper

Main idea

- We will use a specific order on elements of F_2^n. More precisely an element $X=(x_1,\cdots,x_n)$ are associated to the integer $\sum_{i=1}^{n} x_i 2^{i-1}$.
- This identification allows us to compare elements in F_2^n .
- We index from Y_0 to Y_k the elements in F_2^n of weight $\leq \lceil n/2 \rceil - 1$ arranged in increasing order .

Two lemmas

Lemma 2 [A.Canteaut WCC2005]:

Let n be odd, and $f \in B_n$ be balanced. Then $AI(f) = \lceil n/2 \rceil$ if and only if f does not have a nonzero annihilator of degree $\leq \lceil n/2 \rceil - 1$.

Two lemmas

Lemma 3[M.C. Liu Chinacrypt 2008]:

Let n be even, $f \in B_n$, and its weight equals $\sum_{i=0}^{n/2-1} \binom{n}{i}$. Then $AI(f) = \lceil n/2 \rceil$ if and only if f does not have a nonzero annihilator of degree $\leq \lceil n/2 \rceil - 1$

Main idea

Lemma 4: Given a monomial $x_1^{y_1} x_2^{y_2} \cdots x_n^{y_n}$ of degree d, then it is 1 on $X = (x_1, \cdots, x_n) \in F_2^n$ if and only if $\mathrm{supp}(Y) \subseteq \mathrm{supp}(X)$ which means $Y = (y_1, \cdots, y_n) \subset X$. Moreover, this function is equal to zero on the interval $[0, \mathrm{Y})$, and is equal to 1 on the interval $[\mathrm{Y}, \mathrm{Y}^{'})$ where $\mathrm{Y}^{'}$ is the first point in F_2^n greater than Y of weight $\leq d$

Algorithm 1

Step 1: From i=0 to k-1, choose element X_i in $[Y_i, Y_{i+1})$;

Step 2: if i=k, choose X_k such that $Y_k \subset X_k$;

Step 3: Construct $f \in B_n$ such that $\mathrm{supp}(f) = \bigcup_{i=0}^{k} \{X_i\}$;

Step 4: Output f, then $AI(f) = \lceil n/2 \rceil$.

- It is obvious that when n is even the constructed functions are not balanced
- So we give another algorithm for n is even so that the constructed functions are also balanced

Algorithm 2

Step 1: From i=0 to k-1, choose element X_i in $[Y_i,\ Y_{i+1})$ and $wt(X_i) \le n/2$;

Step 2: if i=k, choose X_k such that $Y_k \subset X_k$ and $wt(X_k) \le n/2$;

Step 3: From i=k+1 to $2^{n-1}-1$, choose any $X_i \notin \bigcup_{j=0}^{i-1}\{X_j\}$ and $wt(X_i) \le n/2$;

Step 4: Construct $f \in B_n$ such that $\mathrm{supp}(f) = \bigcup_{i=0}^{2^{n-1}-1}\{X_i\}$;

Step 5: Output f, then $AI(f) = n/2$.

The enumeration

Theorem 3: Let $c = \lceil n/2 \rceil - 1$, then the number of *n-variable* Boolean functions with MAI in Algorithm 1 is

$$2^{n-c} \prod_{d=3}^{n} \prod_{t=\max\{1,c+3-d}^{\min\{c,n-d+1\}} 2^{(t+d-2-c)\binom{n-d}{t-1}}$$

The enumeration

- Different from Algorithm 1, the accurate number of constructed functions in Algorithm 2 is hard to calculate.
- We just give a bound of this case during Theorem 4, and we will not introduce it here.

The algebraic degree

- Based on Theorem 5, we can modify the two algorithms so that the degree of the constructed n-variable function is n-1.
- Lastly, we give an example.

An example ($n=5$)

- By using Algorithm 1, we choose $\bigcup_{i=0}^{15}\{X_i\}$ = {(00000), (10000), (01000), (11000), (00100), (10100), (11100), (00010), (10010), (11010), (11110), (00001), (10001), (11001), (11101), (00011)}
- The AI of the constructed function is 3, and its degree is 4.

Conclusions

- We give a new simple method to construct Boolean functions with maximum algebraic immunity.
- However, whether the constructed functions against FAA and have good nonlinearity need to be further studied.

Thank you!