A Nonlinear Boolean Function with Good Algebraic Immunity

Ju Young Kim and Hong-Yeop Song

School of Electrical and Electronics Engineering,
Yonsei University, Seoul, Korea

27, September, 2007

What we will discuss

Boolean function used in Cryptosystem

- S-Box in Block Cipher
- Running Key Generator in Stream Cipher

are (Nonlinear) Boolean Functions.

Boolean Function :

$$f : \mathbb{F}_2^n \rightarrow \mathbb{F}_2$$

ANF :

$$f(x_1, \cdots, x_n) = \bigoplus_{u \in \mathbb{F}_2^n} \lambda_u \left(\prod_{i=1}^{n} x_i^{u_i} \right), \lambda_u \in \mathbb{F}_2, u = (u_1, \cdots, u_n). \quad (1)$$

Algebraic Degree : $deg(f) \triangleq d$

- the maximal value of the Hamming weight of u such that $\lambda_u \neq 0$.
- In general $d = n - 1$.

Nonlinearity

The nonlinearity of $f \triangleq \mathcal{NL}(f)$

the minimum Hamming distance between f and all the affine functions

$$\mathcal{NL}(f) = 2^{n-1} - \frac{1}{2}\max_{\mathbf{u}\in\mathbb{F}_2^n} |\hat{f}(\mathbf{u})|,$$

where

$$\hat{f}(\mathbf{u}) = \sum_{\mathbf{x}\in\mathbb{F}_2^n} (-1)^{\mathbf{u}\cdot\mathbf{x}+f(\mathbf{x})}, \qquad \mathbf{u} \in \mathbb{F}_2^n.$$

Algebraic Attack in General

- Given symmetric key of size N, and $d = deg(f)$ the number of equations to solve the system of simultaneous linear equations is [2003, Courtois]

$$\sum_{i=0}^{d} \binom{N}{i} \triangleq T(d)$$

- The computing complexity is $T(d)^{2.8}$[1969, Strassen]
- When $N = 80$ and $d = 15(n = 16)$, the complexity $\approx 2^{148}$
- If we **reduce the number of equations** needed, we can attack target system easily. $\Rightarrow$ Reduce d.

Algebraic Immunity

Annihilator $g(\neq 0)$ of f satisfies

$$f \cdot g \text{ or } (1+f) \cdot g \text{ vanishes.}$$

Algebraic Immunity: $AI(f)$

$$AI(f) = \min_{\substack{fg=0 \text{ or } (1+f)g=0 \\ g \neq 0}} \deg(g). \tag{2}$$

How to Calculate the AI of a Given Boolean Function

f : an n-variable boolean function of degree $> \lceil \frac{n}{2} \rceil \triangleq e$

$G = \{g_i | deg(g_i) \leq e, g_i \neq 0\}$

where, $1 \leq i \leq T(e)$,the number of equation needed.

$H = \{h_i | h_i = f \cdot g_i, g_i \in G\}$

g : defined as one of the linear combination of g_i's

has degree $\max_{g_i \in G} deg(g_i)$

$I = \{f \cdot g | g = \bigoplus_{i=1}^{T(e)} \lambda_i g_i, \forall \lambda = (\lambda_1, \cdots, \lambda_{T(e)}) \in \mathbb{F}_2^{T(e)}\}$

Then, the degree of the minimal degree member of the gröbner basis of I is the $AI(f)$.[2003, Faugere]

Known Bounds

Theorem (Universal Bound, 2003, Courtois)

Let f be a Boolean function with n inputs. Then there is a Boolean function $g \neq 0$ of degree at most $\lceil n/2 \rceil$ such that fg is of degree at most $\lceil n/2 \rceil$.

Theorem (Bound for Boolean inverse function, 2006, Nawaz)

Let $f(x) = Tr_1^n(\beta x^{-1})$ and $g(x) = Tr_1^m(x^r)$. Then

$$deg(f(x)g(x)) = \lfloor \sqrt{n} \rfloor + \lceil \frac{n}{\lfloor \sqrt{n} \rfloor} \rceil - 2.$$

The Numbers of Equations to Attack ($N = 80$)

$\mathbf{n}$	$\mathbf{f}$				$\mathbf{f = inv^{(n)}}$	
	$d = n - 1$	$\mathbf{T(d)}$	$\mathbf{d = AI(f)}$	$\mathbf{T(d)}$	$\mathbf{d = AI(f)}$	$\mathbf{T(d)}$
11	10	2^{41}	6	2^{29}	5	2^{25}
12	11	2^{44}	6	2^{29}	5	2^{25}
13	12	2^{47}	7	2^{32}	6	2^{29}
14	13	2^{50}	7	2^{32}	6	2^{29}
15	14	2^{53}	8	2^{35}	6	2^{29}
16	15	2^{56}	8	2^{35}	6	2^{29}
17	16	2^{59}	9	2^{38}	7	2^{32}
18	17	2^{62}	9	2^{38}	7	2^{32}
19	18	2^{65}	10	2^{41}	7	2^{32}

Boolean Log Function $log_\alpha^{(n)}$

$$\rho : \mathbb{Z}_{2^n} \longrightarrow \mathbb{F}_2^n,$$

$$x = \sum_{i=0}^{n-1} a_i 2^i \rightarrow \rho(x) = (a_{n-1}, a_{n-2}, \cdots, a_1, a_0).$$

$$log_\alpha^{(n)}(\mathbf{x}) = \begin{cases} 1, & \mathbf{x} = (0,0,\cdots,0,1), \\ \rho(LOG_\alpha^{(n)}(\mathbf{x}+1))\&1, & \text{otherwise}, \end{cases} \qquad (3)$$

$\mathbf{x} \in \mathbb{F}_2^n$.

$LOG_\alpha^{(n)} : \mathbb{F}_2^n \backslash \{(0,0,\cdots,0,1)\} \rightarrow \{0,1,2,\cdots,2^n-2\}$,

$\alpha^{LOG_\alpha^{(n)}(\mathbf{x}+1)} = \mathbf{x}+1 = \alpha^\omega$, $\omega \in \{0,1,2,\cdots,2^n-2\}$,

α: primitive element of $\mathbb{F}_{2^n}$.

$\&1$: choosing right most bit.

Example of Boolean Log Function: $n = 3$

i	α^i	$LOG_\alpha^{(3)}$	$log_\alpha^{(3)}$
-	000	000	0
0	001	-	1
1	010	011	1
2	100	110	0
3	011	001	1
4	110	101	1
5	111	100	0
6	101	010	0

α is a primitive element of $\mathbb{F}_{2^3}$, and $\alpha^3 + \alpha + 1 = 0$.

Example of Boolean Log Function: $n = 3$

Truth table in order

i	α^i	$LOG_\alpha^{(3)}$	$log_\alpha^{(3)}$						λ_u
-	000	000	0		0		0		0
0	001	-	1		1		1		1
1	010	011	1		1		1		1
3	011	001	1	$\Rightarrow$	0	$\Rightarrow$	1	$\Rightarrow$	1
2	100	110	0		0		0		0
6	101	010	0		0		0		1
4	110	101	1		1		1		0
5	111	100	0		1		1		0

$$log_\alpha^{(3)}(x_1, x_2, x_3) = x_1x_3 + x_2x_3 + x_2 + x_1.$$

Boolean Log Function $log_{\alpha}^{(n)}$: ANF

n	$\mathbf{log}_{\alpha}^{(\mathbf{n})}$
4	$x_1x_3x_4 + x_1x_2x_4 + x_1x_2x_3 + x_3x_4 + x_2x_4 + x_1x_3 + x_1$
5	$x_1x_2x_4x_5 + x_1x_2x_3x_5 + x_1x_2x_3x_4 + x_3x_4x_5 + x_1x_4x_5$ $+x_2x_3x_5 + x_1x_3x_5 + x_1x_2x_5 + x_2x_3x_4 + x_1x_2x_4$ $+x_1x_2x_3 + x_3x_5 + x_2x_5 + x_1x_5 + x_1x_4 + x_4 + x_3 + x_1$

Boolean Log Function $log_{\alpha}^{(n)}$: ANF

n	the number of monomials of every order in ANF of $\log^{(n)}$
6	1, 8, 11, 10, 5
7	3, 13, 17, 21, 12, 6
8	4, 14, 24, 42, 31, 14, 5
9	5, 14, 39, 61, 66, 37, 29, 5
10	3, 26, 62, 107, 132, 97, 50, 26, 7
11	7, 26, 94, 151, 235, 224, 172, 85, 36, 9
12	7, 30, 106, 256, 395, 466, 396, 220, 109, 26, 9
13	7, 33, 145, 360, 619, 831, 851, 598, 362, 131, 44, 11
14	12, 50, 182, 492, 1005, 1494, 1720, 1432, 1036, 465, 203, 62, 11
15	5, 54, 252, 682, 1492, 2467, 3259, 3190, 2499, 1460, 663, 241, 70, 14
16	10, 63, 285, 877, 2177, 3959, 5710, 6328, 5776, 3982, 2237, 907, 277, 69, 12
17	5, 66, 334, 1185, 3091, 6265, 9722, 12282, 12087, 9703, 6185, 3160, 1133, 351, 73, 14

Boolean Log Function: Nonlinearity

n	$\mathbf{log}^{(\mathbf{n})}$		$\mathbf{inv}^{(\mathbf{n})}$		**Upper Bound**
	$\mathcal{NL}(\mathbf{log}^{(\mathbf{n})})$	**sec**	$\mathcal{NL}(\mathbf{inv}^{(\mathbf{n})})$	**sec**	
8	112	< 1	112	< 1	120
9	232	< 1	234	< 1	248
10	478	< 1	480	< 1	496
11	980	< 1	980	< 1	1008
12	1984	< 1	1984	< 1	2016
13	3988	1	4006	1	4064
14	8034	4	8064	7	8128
15	16212	19	16204	31	16320
16	32530	80	32512	136	32640
17	65210	349	65174	579	65408
18	130478	1442	130560	2471	130816
19	261428	6012	261420	10519	261888

Boolean Log Function: Algebraic Immunity

n	$\log^{(n)}$		$\mathrm{inv}^{(n)}$		Universal Upper Bound
	$AI(\log^{(n)})$	sec	$AI(\mathrm{inv}^{(n)})$	sec	
8	4	< 1	4	< 1	4
9	**5**	< 1	**4**	< 1	**5**
10	5	< 1	5	< 1	5
11	**6**	3	**5**	3	**6**
12	6	6	5	7	6
13	7	35	6	44	7
14	7	92	6	124	7
15	**8**	469	**6**	231	**8**
16	8	1532	6	654	8
17	9	15906	7	5661	9

Concluding Remarks - Open Problems

Conjecture (1)

$f(x) = log_{\alpha}^{(n)}(x)$ attains the universal bound on AI. It is True for $n \leq 17$. Is this first such one? Is this the only such one?

Conjecture (2)

$f(x) = log_{\alpha}^{(n)}(x)$ has larger $\mathcal{NL}$ than the boolean inverse function for $n > n_0$. If so, find the minimum n_0. Is it true that $n_0 = 18$?