Research on Fast Algebraic Immunity

Liu Zhang

Department of Computer Science, Shdantou University

May 21, 2020

Outline

Self Instruction

Educational Background

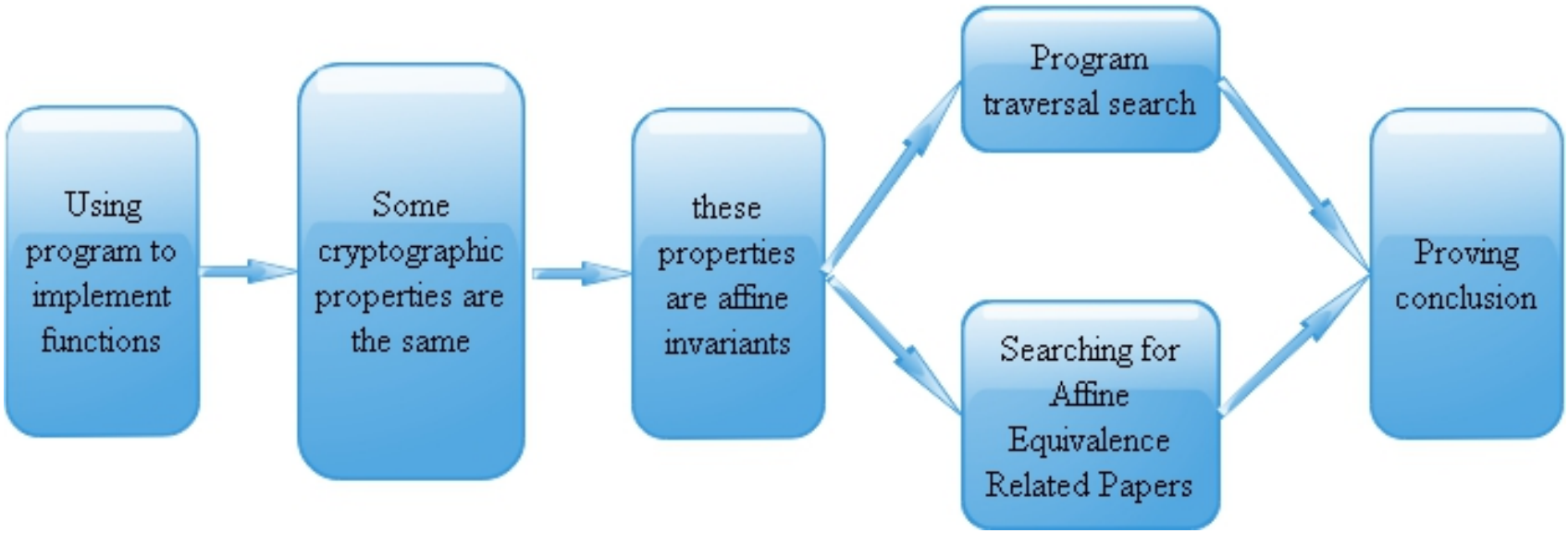
- 2013.9-2017.6 Xinyang Normal University, College of Computer and Information Technology
- 2017.9-now Shantou University, College of Engineering

Academic Research Achievements

- Chen Yindong, **Zhang Liu**, Tang Deng, Cai Weihong. Translation Equivalence of Boolean Functions Expressed by Primitive Element. IEICE Transaction Fundamentals, 2019, 4: 672-675.
- Chen Yindong, **Zhang Liu**, and Xu jianlong, Cai Weihong. A Lower Bound of Fast Algebraic Immunity of A Class of 1-Resilient Boolean Functions. IEEE ACCESS,2019, 12:90145-90151.
- Chen Yindong, **Zhang Liu**, and Guo Fei , Cai Weihong. Fast algebraic immunity of $2^m + 2$ & $2^m + 3$ variables majority function. IEEE ACCESS,2019,12:80733-80736.

Outline

Instruction



Preliminaries

- The sequence $\{s_t\}$ obey the recursion $\sum_{j=0}^{n} m_j s_{t+j} = 0, m_j \in F_2$
- $m(x) = 1 + m_1 x + \cdots + m_{n-1} x^{n-1} + x^n$
- The generator matrix of the sequence

$$M = \begin{pmatrix} 0 & 1 & \cdots & 0 & 0 \\ 0 & 0 & \cdots & 0 & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & 0 & 1 \\ m_0 & m_1 & \cdots & m_{n-2} & m_{n-1} \end{pmatrix}.$$

- $(s_{t+1}, s_{t+2}, ..., s_{t+n})^T = M(s_t, s_{t+1}, ..., s_{t+n-1})^T = M^{t+1}(s_0, s_1, ..., s_{n-1})^T$
- If the initial state of the register is b, $S = (b, Mb, ..., M^{q-2}b)$.
- Let $b_0 = (1, 0, ..., 0)^T$, $S_k = (M^k b_0, M^{k+1} b_0, ..., M^{k+q-2} b_0)$, where $0 \le k \le q-2$.
- $1_f = \{M_j^{i_1} b_0, M_j^{i_2} b_0, ..., M_j^{i_w} b_0\}$, where $0 \le i_1 < i_2 < ... < i_w \le q-2$.

Translation equivalence relation of support of C-F function

Construction (1)

[1] Let n be an integer greater than 1 and α be a primitive element of F_{2^n}. If f is an n-variable Boolean function whose support is

$$\{\mathbf{0}, \alpha^s, \alpha^{s+1}, ..., \alpha^{s+2^{n-1}-2}\},$$

where $0 \leq s < 2^n - 1$ is an integer, then f has optimal algebraic immunity $\lceil n/2 \rceil$.

Construction (2)

[2] Let n be an integer greater than 1 and $\underline{s} = (s_t)_{t \geq 0}$ be an m-sequence of order n. If an n-variable Boolean function f whose support is

$$\{\mathbf{0}\} \cup \{s_t, s_{t+1}, ..., s_{t+n-1} | 0 \leq t \leq 2^{n-1} - 2\},$$

where $\mathbf{0}$ denotes the all-zero vector in F_2^n, then f has optimal algebraic immunity $\lceil n/2 \rceil$.

Translation equivalence relation of support of C-F function

Lemma (1)

[3] Let n be an integer greater than 1 and $m(x)$ be a primitive polynomial of degree n over F_2. If $\alpha \in F_{2^n}$ is a root of $m(x)$ and $\underline{s} = (s_t)_{t\geq 0} \in G(m(x))$ is a nonzero sequence, then there exists a basis $\{\beta_0, \beta_1, ..., \beta_{n-1}\}$ of F_{2^n} such that

$$s_t\beta_0 \oplus s_{t+1}\beta_1 \oplus \cdots \oplus s_{t+n-1}\beta_{n-1} = \alpha^t, t \geq 0.$$

Lemma (2)

[4] Let $f \in Bn$ and

$$1_f = \{M_1^{k_1+i_1}b_0, M_1^{k_1+i_2}b_0, ..., M_1^{k_1+i_w}b_0\},$$

where M_1 is the generator matrix of the sequence and $0 \leq i_1 < i_2 < ... < i_w \leq q-2$. Clearly, any $g \sim f$ can be represented by

$$1_g = \{M_j^{k_2+i_1}b_0, M_j^{k_2+i_2}b_0, ..., M_j^{k_2+i_w}b_0\},$$

where $1 \leq j \leq \phi(q-1)/n$, M_j is a generator matrix and $0 \leq k_2 \leq q-2$.

Translation equivalence relation of support of C-F function

Theorem (1)

Let n be an integer greater than 1 and α be a primitive element of F_{2^n}. If f is an n-variable Boolean function whose support is

$$\{0, \alpha^s, \alpha^{s+1}, ..., \alpha^{s+2^{n-1}-2}\},$$

where $0 \leq s < 2^n - 1$ is an integer. When s takes different values, Boolean functions obtained are affine equivalent.

$$M^t b_0\beta_0 \oplus M^{t+1} b_0\beta_1 \oplus \cdots \oplus M^{t+n-1} b_0\beta_{n-1} = \alpha^t, t \geq 0.$$

$$1_f = \{0\} \cup \{M_1^{i+s} b_0 | i = 0, 1, ..., 2^{n-1} - 2, 0 \leq s < 2^n - 1\}.$$

$$1_{f_1} = \{M_1^i b_0 | i = 0, 1, ..., 2^{n-1} - 1\}.$$

$$1_g = \{M_1^{s+i} b_0 | i = 0, 1, ..., 2^{n-1} - 1\}$$

Translation equivalence relation of support of Tu-Deng function and T-C-T function

Theorem (2)

Let $n = 2k$ and α be a primitive element of F_{2^k}. The Boolean function $g : F_{2^k} \to F_2$ is defined as

$$supp(g) = \{1 = \alpha^s, \alpha^{s+1}, ..., \alpha^{2^{k-1}+s-1}\}.$$

Let Boolean function $f : F_{2^k} \times F_{2^k} \to F_2$ be defined as

$$f(x, y) = g(x/y).$$

the support of Boolean function f can be written

$$supp(f) = \{\beta^{(2^k+1)(i+s)} + \beta^{2^k-1} \cdot \beta^{(2^k+1)j}\},$$

where $i \in (0, 2^k), j \in (0, 2^k), (i-j) \pmod{2^k-1} \in (0, 2^{k-1}-1), 0 \leq s < 2^k - 1$ is an integer.

Translation equivalence relation of support of Tu-Deng function and T-C-T function

Theorem (3)

Let $n = 2k > 4$. Let α be a primitive element of the finite field F_{2^k}. Set $\Delta = \{\alpha^s, ..., \alpha^{2^{k-1}+s-1}\}$ where $0 \leq s < 2^k - 1$ is an integer. Then Boolean function $f \in B_n$ as follows:

$$f(x, y) = g(xy),$$

where the support of Boolean function g is Δ.the support of Boolean function f can be written

$$supp(f) = \{\beta^{(2^k+1)(i+s)} + \beta^{2^k-1} \cdot \beta^{(2^k+1)j}\},$$

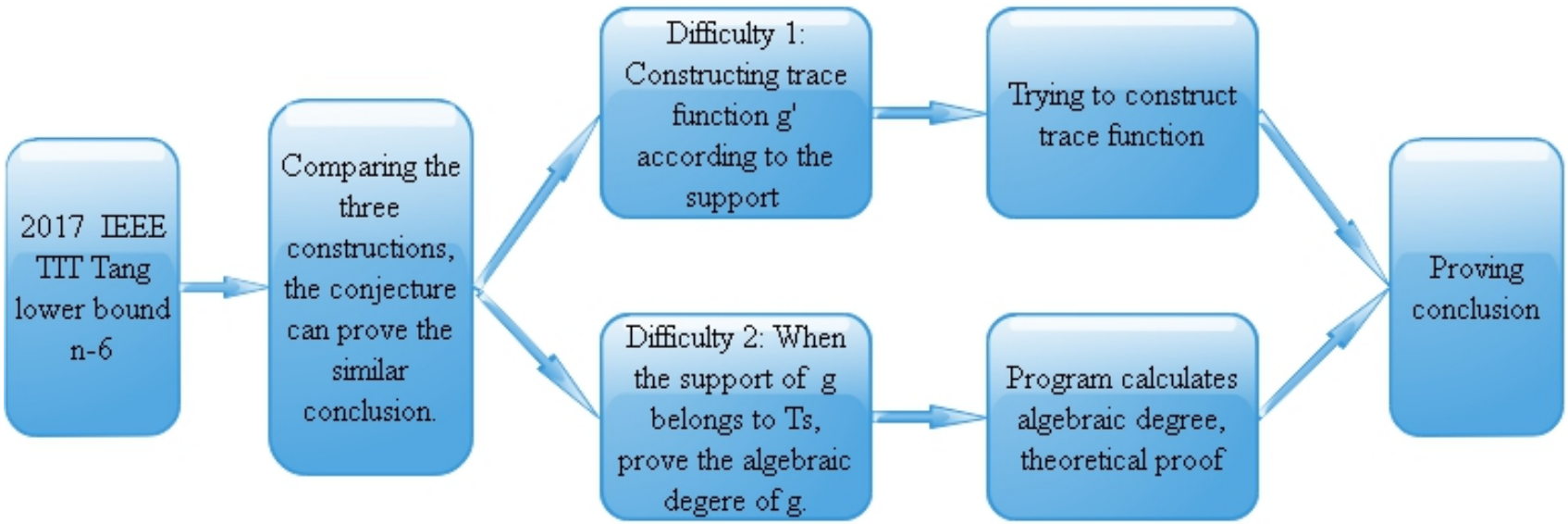
where $i \in (0, 2^k), j \in (0, 2^k), (i + j) \pmod{2^k - 1} \in (0, 2^{k-1} - 1), 0 \leq s < 2^k - 1$ is an integer.

Theorem (4)

When s takes different values, T-C-T functions are affine equivalent. Meanwhile, Tu-Deng function are also affine equivalent.

Outline

Instruction



Preliminaries

Definition (1)

[5] The algebraic immunity of a Boolean function $f \in \mathcal{B}_n$, expressed by $AI(f)$, is defined as $AI(f) = \min\{\deg(g) | fg = 0 \ or \ (f+1)g = 0, g \neq 0 \in \mathcal{B}_n\}$.

Definition (2)

[6] The fast algebraic immunity of a Boolean function $f \in \mathcal{B}_n$, expressed by $FAI(f)$, is defined as $FAI(f) = \min\{2AI(f), \min\{\deg(g) + \deg(fg) | 1 \leq \deg(g) < AI(f)\}\}$.

A lower bound of fast algebraic immunity of a class of 1-resilient Boolean functions

Construction (1)

[7] Let $n = 2k \geq 10$, α *be a primitive element of the finite field* $\mathbb{F}_{2^k}$. *Let* $\Delta_s = \{s, s+1, \cdots, s+2^{k-1}-1\}$ *and* $\overline{\Delta_s} = \mathbb{Z}_{2^k-1} \backslash \Delta_s$ *where* $0 \leq s < 2^{k-1}-1$. *Boolean Function* $f_s \in \mathcal{B}_n$ *can be defined as:*

$$f_s(x,y) = b_s(x,y) + u_s(x,y) \tag{1}$$

where $b_s(x,y) \in \mathcal{B}_n$ *belongs to (2) and* $supp(u_s)$ *includes the following three parts:*

- $\{(\alpha^i, \alpha^{s+2^{k-1}-i-1}) \mid i \in \{0, \cdots, s+2^{k-1}-1\}\} \cup \{(\alpha^i, \alpha^{s-i-1}) \mid s > i \in \overline{\Delta_s}\}$
- $\{(0, \alpha^i) \mid i \in \Delta_s\}$
- $\{(\alpha^i, 0) \mid i \in \Delta_s\}$

Theorem (1)

[7] Let $n = 2k$, f_s *be the* n*-variable Boolean function in Construction 1. Then algebraic immunity of Boolean function* f_s *is* k, *i.e.,* $AI(f_s) = k$.

A class of Boolean functions with almost optimal algebraic immunity

Construction (2)

[8] Let $n = 2k \geq 4$, α *be a primitive element of the finite field* $\mathbb{F}_{2^k}$ *and* $\Delta_s = \{s, s+1, \cdots, s+2^{k-1}-1\}$ *where* $0 \leq s < 2^k - 1$. *Boolean function* $b_s(x,y) \in \mathcal{B}_n$ *can be defined as:*

$$b_s(x,y) = g_s(xy) \tag{2}$$

where g_s *is defined on* $\mathbb{F}_{2^k}$ *with* $supp(g_s) = \{\alpha^i \mid i \in \Delta_s\}$.

Proposition (1)

[8] The n*-variable Boolean function* $b_s(x,y)$ *in Construction 2 includes the four cryptographic properties where* $0 \leq s < 2^k - 1$*:*
1) $AI(b_s) = k$*;*
2) $FAI(b_s) \geq n - 2$.

A lower bound of fast algebraic immunity of a class of 1-resilient Boolean functions

Theorem (2)

Let $n = 2k > 10$, $0 \leq s < 2^{k-1} - 1$, then the FAI of f_s in Construction 1 is at least $n - 6$.

Proof.

Assume $\deg(g) + \deg(f_s g) \leq n - 7$.

$$f_s g = (b_s + u_s) g \tag{3}$$

- $supp(g) \subseteq T_s$
- $supp(g) \nsubseteq T_s$,$g'(x, y) = tr_1^k(z' \alpha^{2^{k-1} - s} xy + r' \alpha^{2^k - s} xy)$

$$f_s g g' = (b_s + u_s) g g' = (b_s + u_s) g' g = b_s g g'$$

g' is a nonzero annihilator of u_s.

$$\deg(gg') + \deg(f_s gg') = \deg(gg') + \deg(b_s gg') \leq FAI(f_s) + 4 \leq n - 3.$$

□

A lower bound of fast algebraic immunity of a class of 1-resilient Boolean functions

Lemma (1)

Let $n = 2k \geq 10$, α *be a primitive element of the finite filed* $\mathbb{F}_{2^k}$. *Let* $T_s = \{(x, 0) \mid x \in F_{2^k}\} \cup \{(0, y) \mid y \in \mathbb{F}_{2^k}\} \cup \{(z, \alpha^{s+2^{k-1}-1} z^{2^k-2}) \mid z \in \mathbb{F}_{2^k}^*\} \cup \{(z, \alpha^{s-1} z^{2^k-2}) \mid z \in \mathbb{F}_{2^k}^*\}$ *where* $0 \leq s < 2^{k-1} - 1$. *When* $g \in \mathcal{B}_n$ *has* $supp(g) \subseteq T_s$, $\deg(g) \geq k - 1$.

Construction (2)

Let $n = 2k \geq 4$, α *be a primitive element of the finite field* $\mathbb{F}_{2^k}$. *Let* $\Delta_m = \{m + 2, m + 3, \cdots, m + 2^{k-1} - 1\}$ *where* $0 \leq m < 2^k - 1$. *Boolean function* $b_m(x, y) \in \mathcal{B}_n$ *can be defined as:*

$$b_m(x, y) = g_m(xy) \tag{4}$$

where g_m *is defined on* $\mathbb{F}_{2^k}$ *with* $supp(g_m) = \{\alpha^j \mid j \in \Delta_m\}$.

Theorem (3)

Let f *be the* $2k$*-variable Boolean function in Construction 2. Then,* $AI(f)$ *is* $k - 1$.

A class of Boolean functions with almost optimal algebraic immunity

Lemma (2)

[9] For $k \geq 3,\ 1 \leq t \leq 2^k - 2$, *let*

$$M_{\leq k-1,\ t} = \left\{ \begin{array}{c} 0 \leq a, b \leq 2^k - 2, \\ (a,b) \in \mathbb{Z}^2 \,|\, a - b \equiv t \pmod{2^k - 1}, \\ wt(\bar{a}) + wt(\bar{b}) \leq k - 1 \end{array} \right\}.$$

Then $|M_{\leq k-1,\ t}| \leq 2^{k-1} - 1$.

Lemma (3)

For $k \geq 3,\ 1 \leq t \leq 2^k - 2$, *let*

$$M_{k-1,\ t} = \left\{ \begin{array}{c} 0 \leq a, b \leq 2^k - 2, \\ (a,b) \in \mathbb{Z}^2 \,|\, a - b \equiv t \pmod{2^k - 1}, \\ wt(\bar{a}) + wt(\bar{b}) = k - 1 \end{array} \right\}.$$

Then $|M_{k-1,\ t}| \geq 1$.

A class of Boolean functions with almost optimal algebraic immunity

Lemma (4)

For $k \geq 3,\ 1 \leq t \leq 2^k - 2$, *let*

$$M_{\leq k-2,\ t} = \left\{ \begin{array}{c} 0 \leq a, b \leq 2^k - 2, \\ (a,b) \in \mathbb{Z}^2 \,|\, a - b \equiv t \pmod{2^k - 1}, \\ wt(\bar{a}) + wt(\bar{b}) \leq k - 2 \end{array} \right\}.$$

Then $|M_{\leq k-2,\ t}| \leq 2^{k-1} - 2$.

Lemma (5)

For $k \geq 3,\ t = 0$, *let*

$$M_{\leq k-2,\ 0} = \left\{ \begin{array}{c} 0 \leq a, b \leq 2^k - 2, \\ (a,b) \in \mathbb{Z}^2 \,|\, a - b \equiv t \pmod{2^k - 1}, \\ wt(\bar{a}) + wt(\bar{b}) \leq k - 2 \end{array} \right\}.$$

Then $|M_{\leq k-2,\ 0}| \leq 2^{k-1} - 2$.

A class of Boolean functions with almost optimal algebraic immunity

Lemma (6)

For $k \geq 3,\ 0 \leq t \leq 2^k - 2$, *let*

$$M_{\leq k-2,\ t} = \left\{ \begin{array}{c} 0 \leq a, b \leq 2^k - 2, \\ (a,b) \in \mathbb{Z}^2 \,|\, a - b \equiv t \pmod{2^k - 1}, \\ wt(\bar{a}) + wt(\bar{b}) \leq k - 2 \end{array} \right\}.$$

Then $|M_{\leq k-2,\ t}| \leq 2^{k-1} - 2$.

Lemma (7)

Let $n = 2k$, α *be a primitive element of* $\mathbb{F}_{2^k}$. *Let* $T_s = \{(0,y) \mid y \in \mathbb{F}_{2^k}\} \cup \{(x,0) \mid x \in \mathbb{F}_{2^k}\} \cup \{(\gamma, \alpha^{s+2^{k-1}-1}\gamma^{2^k-2}) \mid \gamma \in \mathbb{F}_{2^k}^*\} \cup \{(\gamma, \alpha^{s-1}\gamma^{2^k-2}) \mid \gamma \in \mathbb{F}_{2^k}^*\}$ *where* $0 \leq s < 2^{k-1} - 1$ *and* $U' = \{z \in \mathbb{F}_{2^k}^* \mid tr_1^k(z) = 0\}$. *For* $0 \leq s < 2^{k-1} - 1$, *if an arbitary element* $(a,b) \in \mathbb{F}_{2^k} \times \mathbb{F}_{2^k} \backslash T_s$, *there are* $2(2^{k-2}(2^{k-2} - 1))$ *pair* (z', r') *where* $z', r' \in U'$ *such that* $g'(x,y) = tr_1^k(z'\alpha^{2^{k-1}-s}xy + r'\alpha^{2^k-s}xy)$ *equals* 1 *if* $(x,y) = (a,b)$.

A lower bound of fast algebraic immunity of a class of 1-resilient Boolean functions

Theorem (2)

Let $n = 2k > 10$, $0 \leq s < 2^{k-1} - 1$, then the FAI of f_s in Construction 1 is at least $n - 6$.

Proof.

Assume $\deg(g) + \deg(f_s g) \leq n - 7$.

$$f_s g = (b_s + u_s) g \tag{3}$$

- $supp(g) \subseteq T_s$
- $supp(g) \nsubseteq T_s$,$g'(x, y) = tr_1^k(z' \alpha^{2^{k-1} - s} xy + r' \alpha^{2^k - s} xy)$

$$f_s g g' = (b_s + u_s) g g' = (b_s + u_s) g' g = b_s g g'$$

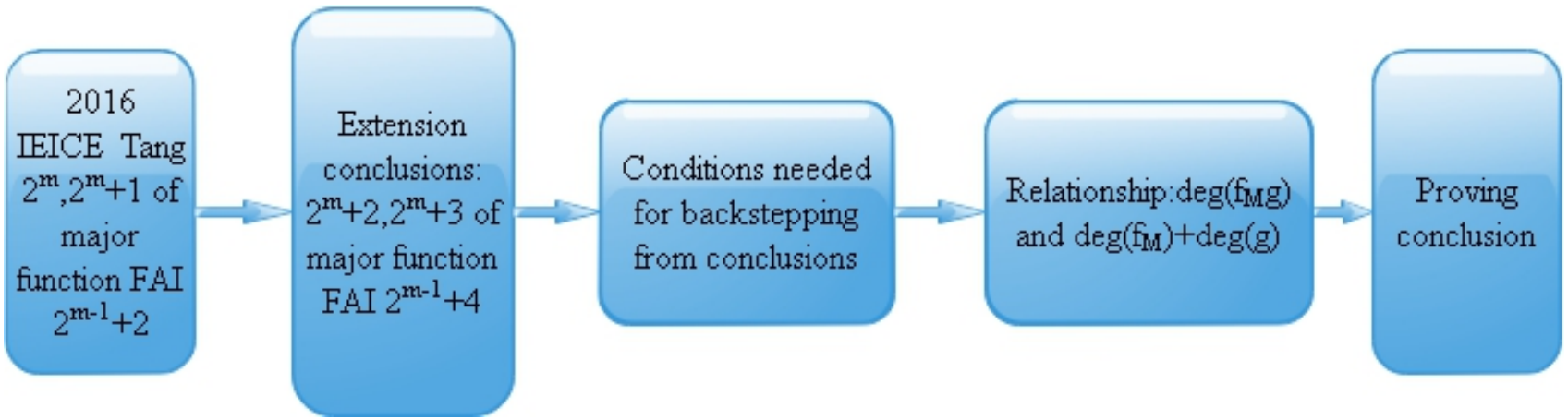
g' is a nonzero annihilator of u_s.

$$\deg(gg') + \deg(f_s gg') = \deg(gg') + \deg(b_s gg') \leq FAI(f_s) + 4 \leq n - 3.$$

□

Outline

Instruction



Preliminaries

Definition (1)

[11] The majority function is defined as

$$f_M(x) = \begin{cases} 1, & wt(x) \geq \lceil \frac{n}{2} \rceil \\ 0, & \text{otherwise.} \end{cases}$$

Lemma (1)

[12] Let $f_M \in \mathcal{SB}_n$ be the majority function, then

i) $\deg(f_M) = 2^{\lfloor \log_2 n \rfloor}$;

ii) $AI(f_M) = \lceil \frac{n}{2} \rceil$.

Main Result

Theorem (1)

Let $f_M \in \mathcal{SB}_n$ be the majority function with $n \in \{2^m + 2, 2^m + 3\}$ where $m \geq 2$. Then $FAI(f_M) = 2^{m-1} + 4$.

Lemma (2)

[13] Let $n \geq 2$, f_M is the n-variable majority function . There are Boolean Functions g and h so that $f_M g = h$ with $d = \deg(h) = \lfloor n/2 \rfloor + 1$ and $e = \deg(g) = d - 2^j$ where j is the maximum number ensure that $e > 0$.

Lemma (3)

Let $f_M \in \mathcal{SB}_n$ be the majority function with $2^m + 2 \leq n < 2^{m+1}$ where $m \geq 2$. Then $FAI(f_M) \geq \lfloor \frac{n}{2} \rfloor + 3$.

Main Result

Lemma (4)

Let $2^m + 2 \leq n < 2^{m+1}$ with $m \geq 2$ and $f_M \in \mathcal{SB}_n$ be the majority function. Let $A = \min\{\deg(h) | 0 \neq h \in Ann(f_M)\}$. Then $FAI(f_M) \geq A + 2 \geq AI(f_M) + 2$.

Proof.

$$\min_{1 \leq \deg(g) < AI(f_M+1)} \{\deg(g) + \deg((f_M + 1)g)\} \geq A + 2 \geq AI(f_M) + 2 \quad (1)$$

□

Main Result

Lemma (5)

Let $2^m + 2 \leq n < 2^{m+1}$ with $m \geq 2$ and $f_M \in \mathcal{SB}_n$ be the majority function. For any n-variable Boolean function g with $\deg(g) = 1$, then $\deg(f_M g) = \deg(f_M) + 1$.

Theorem (1)

Let $f_M \in \mathcal{SB}_n$ be the majority function with $n \in \{2^m + 2, 2^m + 3\}$ where $m \geq 2$. Then $FAI(f_M) = 2^{m-1} + 4$.

Sequential Studies

n	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
degree	2	2	4	4	4	4	8	8	8	8	8	8	8	8	16	16	16	16	16	16	16	16
A(F)	2	2	3	3	4	4	5	5	6	6	7	7	8	8	9	9	10	10	11	11	12	12
A(F+1)	1	2	2	3	3	4	4	5	5	6	6	7	7	8	8	9	9	10	10	11	11	12
FAI		3	4	4	6	6	6	6	8	8	10	10	10	10	10	10	12	12	14	14	16	16
n	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45
degree	16	16	16	16	16	16	16	16	32	32	32	32	32	32	32	32	32	32	32	32	32	32
A(F)	13	13	14	14	15	15	16	16	17	17	18	18	19	19	20	20	21	21	22	22	23	23
A(F+1)	12	13	13	14	14	15	15	16	16	17	17	18	18	19	19	20	20	21	21	22	22	23
FAI	18	18	18	18	18	18	18	18	18	18	20	20	22	22	24	24	26	26	28	28	30	30

Figure: Research process

Outline

Research Plan

- Theoretical proof of the fast algebraic immunity of some special Boolean functions.
- Security evaluation of block cipher for differential and linear cryptanalysis(MILP).
- Sagemath

Outline

[1] C.Carlet, K.Feng, An Infinite Class of Balanced Functions with Optimal Algebraic Immunity, Good Immunity to Fast Algebraic Attacks and Good Nonlinearity[C]// International Conference on the Theory and Application of Cryptology and Information Security: Advances in Cryptology. Springer-Verlag, 2008:425-440.

[2] Q.Wang, J.Peng, H.Kan, Constructions of Cryptographically Significant Boolean Functions Using Primitive Polynomials[J]. IEEE Transactions on Information Theory, 2010, 56(6):3048-3053.

[3] H.Chen, T.Tian, W.Qi, On the affine equivalence relation between two classes of Boolean functions with optimal algebraic immunity[J]. Designs Codes Cryptography, 2013, 67(2):175-185.

[4] Q.Wang, T.Johansson, On Equivalence Classes of Boolean Functions[M] Information Security and Cryptology - ICISC 2010. Springer Berlin Heidelberg, 2010:311-324.

[5] W. Meier, E. Pasalic, C. Carlet, ”Algebraic attacks and decomposition of Boolean functions,” International Conference on the Theory and Applications of Cryptographic Techniques, pp. 474-491, 2004.

[6] M. Liu, D. Lin, ”Fast algebraic attacks and decomposition of symmetric Boolean functions,” IEEE Trans. Inf. Theory, vol. 57, no. 7, pp. 4817-4821, 2011.

[7] D. Tang, C. Carlet, X. Tang, ”A class of 1-resilient Boolean functions with optimal algebraic immunity and good behavior against fast algebraic attacks,” International Journal of Foundations of Computer Science, vol. 25, no. 6, pp. 763-780, 2014.

[8] D. Tang, C. Carlet, X. Tang, "Highly nonlinear Boolean functions with optimal algebraic immunity and good behavior against fast algebraic attacks," IEEE Trans. Inf. Theory, vol. 59, no. 1, pp. 653-664, 2013.

[9] Q. Jin, Z. Liu, B. Wu, "1-resilient Boolean function with optimal algebraic immunity," Cryptology ePrint Archive, Report 2011/549, http://eprint.iacr.org/.v

[10] D. Tang, R. Luo, and X. Du, "The exact fast algebraic immunity of two subclasses of the majority function," IEICE Trans. Fundamentals, vol. E99-A, no. 11, pp. 2084-2088, Nov. 2016.

[11] C. Ding, G. Xiao, and W. Shan, "The stability theory of stream ciphers," (Lecture Notes in Computer Science), vol. 561, Springer Berlin Heidelberg, Berlin, Heidelberg, 1991.

[12] D.K. Dalai, S. Maitra, and S. Sarkar, "Basic theory in construction of Boolean functions with maximum possible annihilator immunity," Designs, Codes and Cryptography, vol. 40, no. 1, pp. 41-58, Jul. 2006.

[13] F. Armknecht, C. Carlet, P. Gaborit, S. Künzli, W.Meier, and O. Ruatta, "Efficient computation of algebraic immunity for algebraic and fast algebraic attacks," in Advances in Cryptology-EUROCRYPT, (Lecture Notes in Computer Science), vol. 4004, pp. 147-164, Springer Berlin Heidelberg, Berlin, Heidelberg, 2006.