Ex 12 INF240 KENNETH FOSSEN

(1) Let α be a primitive element of $\mathbb{F}_{2^4}$ and consider a $(4,4)$ n,m function

$$F(x) = x^9 + \alpha x$$

Univariate of $F(x)$, $a \in \mathbb{F}_{2^4}$ $0,1,2,4,8$ $0\,1\,2\,3$

$$D_a F(x) = (x+a)^9 + \alpha(x+a) + x^9 + \alpha x$$

$$D_a F(x) = (x+a)^8(x+a) + x^9 + \alpha(x+a) + \alpha x$$

$$= (x^8 + a^8)(x+a) + x^9 + \alpha x + \alpha a + \alpha x$$

$$= x^9 + x^8 a + a^8 x + a^9 + x^9 + \alpha a$$

$$D_a F(x) = x^8 a + a^8 x + a^9 + \alpha a$$

2. $D_b D_a F(x)$, $b \in \mathbb{F}_{2^4}$

$D_a F(x) = x^8 a + a^8 x + a^9 + \alpha a$

$D_b D_a F(x) = D_a F(x+b) + D_a F(x)$

$= a(x+b)^8 + a^8(x+b) + a^9 + \alpha a$

$+ x^8 a + a^8 x + a^9 + \alpha a$

$= a(x+b)^4(x+b)^4 + a^8 x + a^8 b + x^8 a + a^8 x$

$= a(x^4+b^4)(x^4+b^4) + a^8 b + x^8 a$

$= a(x^8 + x^4 b^4 + b^4 x^4 + b^8) + a^8 b + x^8 a$

$= ax^8 + ab^8 + a^8 b + x^8 a$

$= ab^8 + a^8 b$

3. Algebraic degree

F = $x^1 \Rightarrow 9 = 1001 = 2$
$x \Rightarrow 1 = 1 = 1$ } 2

$D_a F$ = $x^0 \Rightarrow 8 = 1000 = 1$
$x^1 \Rightarrow 1 = 1 = 1$ } 1

$D_b D_a F$ = there are no x
hence 0 degree. 0

② TT for (3,3) power function

$b \in \mathbb{F}_2^3$

Number of solutions to

$F(a+x) + F(x) = b$, $a = (0,0,1)$

What is the differential uniformity of this function

x	F(x)
0 0 0	0 0 0
0 0 1	1 0 1
0 1 0	1 1 0
0 1 1	1 1 1
1 0 0	1 0 0
1 0 1	0 1 1
1 1 0	0 0 1
1 1 1	0 1 0

(3) Gold function

$G(x) = x^{2^i+1}$ are APN

for (n,n) for any n

with $\gcd(i,n) = 1$

Show that the gold function for $i = 1$, $\Rightarrow G = x^3$ is APN for any n.

1. Calculate $D_a F(x)$, $a \neq 0$

$$D_a F(x) = (x+a)^3 + x^3 \quad , a = 1$$

$$= a^3\underbrace{\left(\left(\frac{x}{a}+1\right)^3 + \left(\frac{x}{a}\right)^3\right)}_{F(x+a)+F(x)}$$

$$= a^3 D_1 F\left(\frac{x}{a}\right) \curvearrowleft$$

2. APN over $\mathbb{F}_{2^n}$ when $\gcd(3,n)=1$

when

$$F(x+a)+F(x)=F(a)$$

has only 2 solutions for any $a \neq 0$.

$$G(x)=x^{2^i+1}, \quad i=1 \Rightarrow x^3$$

$F(x+1)+F(x)$, for $G(x)$

$=(x+1)^3+x^3$

$=x^3+1+x^3$

$=1$

(4) (2.1) Function f

TT

x	f(x)
0 0	1
0 1	0
1 0	1
1 1	1

Compact its nonlinearity

Basis (0,1)
(1,0)

1. 2.

x	l_1	l_2	l_3	l_4	a_1	a_2	a_3	a_4
0 0	0	0	0	0	1	1	1	1
0 1	0	0	1	1	1	1	0	0
1 0	0	1	0	1	1	0	1	0
1 1	0	1	1	0	1	0	0	1

3.

	$l(x)$	$f(x)$	Hamming
$l_1(x)$	0 0 0 0		3
$l_2(x)$	0 0 1 1		1
$l_3(x)$	0 1 0 1		3
$l_4(x)$	0 1 1 0	1 0 1 1	3
$a_1(x)$	1 1 1 1		1
$a_2(x)$	1 1 0 0		3
$a_3(x)$	1 0 1 0		1
$a_4(x)$	1 0 0 1		1

(5) consider all (7,7) functions

1. Converging radius

$m = 7, n = 7$

$$N_f \leq 2^{n-1} - 2^{\frac{n}{2}-1}$$

$$2^6 - 2^{\frac{7}{2}-1}$$

$$2^6 - 5.6569$$

$$N_f \leq 58.3431$$

2. SCV bound

$n = 7, m = 7$

$$N_f \leq 2^{n-1} - \frac{1}{2}\sqrt{3 \cdot 2^n - 2 - 2\frac{(2^n-1)(2^{n-1}-1)}{2^m-1}}$$

$$\leq 2^6 - \frac{1}{2}\sqrt{3 \cdot 2^7 - 2 - 2\frac{(2^7-1)(2^6-1)}{(2^7-1)}}$$

$$\leq 2^6 - \frac{1}{2}16 \Rightarrow 2^6 - 8 = \underline{56}$$

3. Deduce the Nonlinearity

Walsh Transformation

4. algebraic degree is upper bounded by:

$$\deg(F) = \frac{n+1}{2}$$

since $n = 7$

$$\deg(F) = \frac{7+1}{2} = 4$$

(6) $(n,i) = 7$

$i = \{0, \ldots, 6\}$

$f_i(x) = x^{10}$ $\quad n=7 \Rightarrow 2^n = 128$

$d = 2^i e \ \text{mcd}(2^n - 1)$

used magma to solve

this gives for i

$0 \quad 1 \quad 2 \quad 3 \quad 4 \quad 5 \quad 6$

$\{1, 20, 40, 80, 33, 66, 5\}$

since $10 \text{mcd} 127 = 1 \Rightarrow$

$10 \ \text{mcd}^{-1}(127) = 89$

$0 \quad 1 \quad 2 \quad 3 \quad 4 \quad 5 \quad 6$

$\Rightarrow \{89, 51, 102, 77, 27, 54, 108\}$

$f_2(x) = x^{23}$

$\Rightarrow$

$\{23, 46, 92, 57, 114, 101, 75\}$

inverse $= 116$

$\{116, 105, 83, 39, 78, 29, 58\}$

$f_8(x) = x^{25}$

{25, 50, 100, 73, 19, 38, 76}

inverse 61

{61, 122, 117, 107, 87, 47, 94}

$f_4(x) = x^{40}$

{40, 80, 33, 66, 5, 10, 20}

inverse = 54

{54, 108, 89, 51, 102, 77, 27}

$f_5(x) = x^{101}$

{101, 75, 23, 46, 92, 57, 114}

inverse 83

{83, 39, 78, 29, 58, 116, 105}

$f_2(x) = x^{23}$

$f_7(x) = x^{100}$

are cyclotomatic

$f_1(x) = x^{10}$

$f_4(x) = x^{40}$

are cyclotomatic