Theorem 1. *Let $F(x) = x^{q^2+q+1} \in \mathbb{F}_{q^4}[x]$, where $q = 2^k$. Then for any nonzero u, v, the second-order*

Proof. Note that for $a \neq 0$ and $\forall u, v \in \mathbb{F}_{2^n}$ with $v \neq 0$, we have

$$\begin{aligned}
W_{D_aF}(u,v) &= \sum_{x\in\mathbb{F}_{2^n}} (-1)^{\mathrm{tr}_1^n(v(D_aF(x))+ux)} \\
&= \sum_{x\in\mathbb{F}_{2^n}} (-1)^{\mathrm{tr}_1^n(v(F(x)+F(x+a))+ux)} \\
&= \sum_{x\in\mathbb{F}_{2^n}} (-1)^{\mathrm{tr}_1^n\left(v\left(x^d+(x+a)^d\right)+ux\right)} \\
&= \sum_{x\in\mathbb{F}_{2^n}} (-1)^{\mathrm{tr}_1^n\left(\left(\left(v^{\frac{1}{d}}x\right)^d+\left(v^{\frac{1}{d}}x+v^{\frac{1}{d}}a\right)^d\right)+ux\right)} \\
&= \sum_{x\in\mathbb{F}_{2^n}} (-1)^{\mathrm{tr}_1^n\left(\left(\left(v^{\frac{1}{d}}x\right)^d+\left(v^{\frac{1}{d}}x+v^{\frac{1}{d}}a\right)^d\right)+uv^{-\frac{1}{d}}v^{\frac{1}{d}}x\right)} \\
&= \sum_{x'\in\mathbb{F}_{2^n}} (-1)^{\mathrm{tr}_1^n\left(\left((x')^d+\left(x'+v^{\frac{1}{d}}a\right)^d\right)+uv^{-\frac{1}{d}}x'\right)} \\
&= W_{D_{a'}F}\left(uv^{-\frac{1}{d}},1\right)
\end{aligned}$$

where $x' = v^{\frac{1}{d}}x$ and $a' = v^{\frac{1}{d}}a$. Then once $W_{D_aF}(u,1)$ is known for all $a, u \in \mathbb{F}_{2^n}$, $W_{D_aF}(u,v)$ will also be determined.

Note that we have $\deg(D_aF) = 2$ since $\deg(F) = 3$, i.e. $D_aF(x)$ is a quadratic function. And the Walsh spectrum of a quadratic Boolean function is completely characterized by the dimension of the kernel of the bilinear form associated to it.

So we consider the bilinear form $\mathcal{B}(x,y)$ associated with $\mathrm{tr}_1^n(D_aF(x))$, and the function $\mathcal{B}(x,y)$ becomes

$$\begin{aligned}
\mathcal{B}(x,y) &= \mathrm{tr}_1^n(D_aF(0)) + \mathrm{tr}_1^n(D_aF(x)) + \mathrm{tr}_1^n(D_aF(y)) + \mathrm{tr}_1^n(D_aF(x+y)) \\
&= \mathrm{tr}_1^n\left(a^d\right) + \mathrm{tr}_1^n\left(x^d+(x+a)^d\right) + \mathrm{tr}_1^n\left(y^d+(y+a)^d\right) + \mathrm{tr}_1^n\left((x+y)^d+(x+y+a)^d\right) \\
&= \mathrm{tr}_1^n\Big(a^qx^{q^2+1} + a^{q^2}x^{q+1} + ax^{q^2+q} + a^qy^{q^2+1} + a^{q^2}y^{q+1} + ay^{q^2+q} + a^q(x+y)^{q^2+1} \\
&\quad + a^{q^2}(x+y)^{q+1} + a(x+y)^{q^2+q}\Big) \\
&= \mathrm{tr}_1^n\left(a^q\left(x^{q^2}y+xy^{q^2}\right) + a^{q^2}\left(x^qy+xy^q\right) + a\left(x^{q^2}y^q+x^qy^{q^2}\right)\right) \\
&= \mathrm{tr}_1^n\left(y\widetilde{f}(x)^q\right).
\end{aligned}$$

where $\widetilde{f}(x) = (a^q + a)\, x^{q^2} + \left(a^{q^2} + a\right) x^q + \left(a^q + a^{q^2}\right) x$ and the kernel of $\mathcal{B}(x, y)$ is equal to $\mathcal{E} = \left\{ x \in \mathbb{F}_{2^n} \middle| \widetilde{f}(x) = 0 \right\}$.

When the coefficient of x^{q^2} in $\widetilde{f}(x)$ is zero, we have $a^q + a = 0$, i.e. $a \in \mathbb{F}_q$, resulting in the coefficients of x^q and x both are 0, which means that the kernel of $\mathcal{B}(x, y)$ is $\mathbb{F}_{2^n}$ for $a \in \mathbb{F}_q$, that is, the dimension of the kernel is n.

When $a^q + a \neq 0$, i.e. $a \in \mathbb{F}_{2^n} \setminus \mathbb{F}_q$, $\widetilde{f}(x)$ is a linearized polynomial and we can transform it into

$$\begin{aligned}
\widetilde{f}(x) &= (a^q + a)\, x^{q^2} + \left(a^{q^2} + a\right) x^q + \left(a^q + a^{q^2}\right) x \\
&= (a^q + a)\, x^{q^2} + \left(a^q + a^{q^2} + a^q + a\right) x^q + \left(a^q + a^{q^2}\right) x \\
&= (a^q + a) \left(x^{q^2} + x^q\right) + \left(a^q + a^{q^2}\right) (x^q + x) \\
&= (a^q + a)\, (x^q + x)^q + (a + a^q)^q\, (x^q + x)\,.
\end{aligned}$$

Note that $a^q + a \neq 0$, then $\widetilde{f}(x) = 0$ implies that $(x^q + x)^q + (a + a^q)^{q-1} (x^q + x) = 0$. Clearly all elements of $\mathbb{F}_q$ are solutions of $\widetilde{f}(x) = 0$, meanwhile, for $x \in \mathbb{F}_{q^4} \setminus \mathbb{F}_q$, $\widetilde{f}(x) = 0$ can get

$$(a + a^q)\, (x^q + x) \left((x^q + x)^{q-1} + (a + a^q)^{q-1}\right) = 0,$$

implying that

$$\left(\frac{x^q + x}{a^q + a}\right)^{q-1} = 1.$$

In other words, $x \in \mathbb{F}_{q^4} \setminus \mathbb{F}_q$ is a solution of $\widetilde{f}(x) = 0$ if and only if $\frac{x^q + x}{a^q + a} \in \mathbb{F}_q^*$. Therefore assume $\theta = \frac{x^q + x}{a^q + a} \in \mathbb{F}_q^*$, then we have $x^q + x + \theta(a^q + a) = x^q + x + (\theta a)^q + \theta a = (x + \theta a)^q + (x + \theta a) = 0$, which is equivalent to $x + \theta a \in \mathbb{F}_q$. Thus we have $x \in \theta a + \mathbb{F}_q$ and the number of solutions $x \in \mathbb{F}_{q^4} \setminus \mathbb{F}_q$ of $\widetilde{f}(x) = 0$ is $q(q-1)$ for $a \in \mathbb{F}_{q^4} \setminus \mathbb{F}_q$.

So the number of solutions of $\widetilde{f}(x) = 0$ is q^4 and $q + q(q-1) = q^2$ for $a \in \mathbb{F}_q$ and $a \in \mathbb{F}_{q^4} \setminus \mathbb{F}_q$, respectively. Thus,

$$\dim_{\mathbb{F}_2} \mathcal{E} = \begin{cases} 2k, & \text{if } a \in \mathbb{F}_{q^4} \setminus \mathbb{F}_q \\ 4k, & \text{if } a \in \mathbb{F}_q. \end{cases}$$

Therefore, we have

$$\max_{u \in \mathbb{F}_{q^4}} |W_{D_a F}(u, 1)| = \begin{cases} 2^{3k}, & \text{if } a \in \mathbb{F}_{q^4} \setminus \mathbb{F}_q \\ 2^{4k}, & \text{if } a \in \mathbb{F}_q \end{cases}$$

□

Theorem 2 (name of the theorem)**.** *Let* $F(x) = x^{2^{2i}-2^i+1} \in \mathbb{F}_{2^n}[x]$*, where* $\gcd(i, n) = 1$*. Then for any* γ, η, ω *we have*

$$\mathcal{N}_F(\gamma, \eta, \omega) = \#\left\{x \in \mathbb{F}_{2^n} : F(x) + F(x+\gamma) + F(x+\eta) + F(x+\gamma+\eta) = \omega\right\}$$

and the distribution of $\mathcal{N}_F(\gamma, \eta, \omega)$ *is*

Let $d = 2^{2i} - 2^i + 1 = 2^{i+i-1} + 2^{i+i-2} + \cdots + 2^i + 1$, note that the exponents of 2 are all distinct and we assume a set D associated with d such that

$$D = \{0, i, i+1, \ldots, i-2, i-1\},$$

then we can partition D into two disjoint sets J, K such that $J \cap K = \emptyset$ and $J \cup K = D$. Therefore we can rewrite $(x+\gamma)^d$ as

$$(x+\gamma)^d = \sum_{\substack{J \cap K = \emptyset \\ J \cup K = D}} x^J \gamma^K,$$

where we denote $\prod_{j \in J} x^j$ by x^J.

To Be Conituned. We calculate the equation

$$F(x) + F(x+\gamma) + F(x+\eta) + F(x+\gamma+\eta) = \omega.$$

After calculation we have

$$\sum_{\substack{J \cap K = \emptyset \\ J \cup K = D \\ 1 \le |J| \le i-1}} y^J \left[(1+\theta)^K + 1 + \theta^K\right] = \omega',$$

where $\theta = \frac{b}{a}$, $y = \frac{x}{a}$ and $\omega' = \omega + cons$ with $cons$ is the function of γ, η and we can omit it since ω ranges over $\mathbb{F}_{2^n}$.

For $i = 3$, we □

Let μ_d be the d-th roots of unity and $q = 2^{2m}$ with $d \mid (q-1)$, where d and m are positive integers. The unit circle of $\mathbb{F}_q$ is defined by

$$\mu_{2^m+1} = \left\{x \in \mathbb{F}_q : x^{2^m+1} = x\overline{x} = 1\right\}.$$

Theorem 3 (permutation polynomials like P.L. Sharma)**.** *The polynomial* $f(x) = x^b h(x^{2^m-1})$ *is a permutation polynomial over* $\mathbb{F}_q$*, where* $h(x) = 1 + x^a + x^b$*,* $b = 2^i + 2^j, a = 2^j$ *and* $i > j$ *with satisfying the system*

$$\begin{cases} \gcd(2^m + 1, 2^i - 2^j - 1) = 1 \\ \gcd(m, i-j) = \gcd(2m, i-j) = \gcd(m, 2(i-j)) \end{cases} \tag{1}$$

We will use Lemma below to prove the theorem.

Lemma 1. *Let $d, r > 0$ with $d \mid (q-1)$ and $h(x) \in \mathbb{F}_q[x]$. Then $f(x) = x^r h(x^{\frac{q-1}{d}})$ permute $\mathbb{F}_q$ iff the following two conditions hold:*

(1) $\gcd(r, (q-1)/d) = 1$,

(2) $x^r h(x)^{(q-1)/d}$ *permutes* μ_d.

Proof of Theorem. The polynomial $f(x)$ can be written as $f(x) = x^b h\left(x^{2^m-1}\right)$, where $h(x) = 1 + x^a + x^b \in \mathbb{F}_{2^{2^m}}[x]$. Note that

$$\gcd(b, (q-1)/d) = \gcd(2^i + 2^j, 2^m - 1) = \gcd(2^{i-j} + 1, 2^m - 1) = 1$$

since $\gcd(i-j, m) = \gcd(2(i-j), m)$, and then $f(x)$ permutes $\mathbb{F}_q$ iff the polynomial $g(x) = x^b h(x)^{2^m-1}$ permutes μ_{2^m+1} by Lemma 1.

The inexistence of roots of polynomial $h(x)$ in μ_{2^m+1} can be decuced in the following steps:

(1) Rasing $h(x)$ to the 2^m-power and multiplying it by x^b will give us $1 + x^{b-a} + x^b$,

(2) Sum of $h(x)$ and $1 + x^{b-a} + x^b$ leads to $x^{b-a} + x^a = 0 \Leftrightarrow x \in \mathbb{F}^*_{b-2a}$,

(3) Condition $\gcd(2^m+1, 2^i - 2^j - 1) = 1$ means that $x \in \mathbb{F}^*_{b-2a} \cap \mu_{2^m+1}$ is equivalent to $x = 1$.

(4) $x = 1$ is not the roots of $h(x)$.

The polynomial $h(x)$ has no roots in μ_{2^m+1}, implying that $h : \mu_{2^m+1} \longrightarrow \mathbb{F}^*_q$, and hence $g(\mu_{2^m+1}) \subseteq \mu_{2^m+1}$. So the permutation of $f(x)$ on μ_{2^m+1} can be determined by the injective of $g(x)$ over μ_{2^m+1}.

So assume $g(x)$ is not injective over μ_{2^m+1}, i.e. there exist $x \neq y \in \mu_{2^m+1}$ such that $g(x) = g(y)$. Therefore we have

$$g(x) = x^b(1 + x^a + x^b)^{2^m-1} = \frac{x^b(1 + x^{2^m a} + x^{2^m b})}{1 + x^a + x^b} = \frac{x^b + x^{b-a} + 1}{x^b + x^a + 1}.$$

So $g(x) = g(y)$ is equal to

$$g(x) + 1 = g(y) + 1 \Leftrightarrow \frac{x^a + x^{b-a}}{x^b + x^a + 1} = \frac{y^a + y^{b-a}}{y^b + y^a + 1},$$

then it comes to

$$\begin{aligned}
&x^a + y^a + x^a y^a (x^{b-a} + y^{b-a}) + x^{b-a} y^{b-a} (x^a + y^a) \\
&+ x^a y^{b-a} + x^{b-a} y^a + x^{b-a} + y^{b-a} \\
=&(1 + x^{b-a} y^{b-a})(x^a + y^a) + (1 + x^a y^a)(x^{b-a} + y^{b-a}) + x^a y^{b-a} + x^{b-a} y^a \qquad (2) \\
=&(1 + xy)^{2^n} (x + y)^{2^k} + (1 + xy)^{2^k} (x + y)^{2^n} + x^{2^k} y^{2^n} + x^{2^n} y^{2^k} \\
=&0.
\end{aligned}$$

We first consider the special situation, that is, when $xy = 1$, equation (2) becomes

$$x^{2^n - 2^k} + y^{2^n - 2^k} = 0,$$

which implies $\frac{y}{x} \in \mathbb{F}_{2^{n-k}}$. Since $\gcd(m, n-k) = \gcd(2m, n-k)$, we are sure that $\frac{y}{x} \in \mathbb{F}_{2^{n-k}} \cap \mu_{2^m+1} \Leftrightarrow y = x$, a contradiction.

Then dividing $(x + y)^{2^n + 2^k}$ on the both sides of equation (2) leads to

$$\frac{(1 + xy)^{2^n}}{(x + y)^{2^n}} + \frac{(1 + xy)^{2^k}}{(x + y)^{2^k}} + \frac{x^{2^k} y^{2^n} + x^{2^n} y^{2^k}}{(x + y)^{2^n + 2^k}} = 0. \qquad (3)$$

□

Cryptographic algorithm are vulnerable to side-channel attacks. A popular approach is to make the intermediate results of algorithm being excuted independent of the secret key. This can be done at the level of algorithm. They are in common that they require the use of random values in order to mask data that is being processed. A common feature of those approaches is that the introduction of additional random values in order to mask the intermediate results computed by the circuits.

Glitches can leak information:

Firstly, consider AND gate with x, y are inputs and z is output. Assume a glitch occurs in x. If input y is 1, then $z = x$ AND $y = x$, and the glitch in x will change the state temporarily. But when $y = 0$, the glitch in x will not affect the output. Consequently, the glitch in x depends on the value of y.

Secondly, consider the traditional masked AND gate. The masked inputs are $\widetilde{x} = a \oplus x$, a, $\widetilde{y} = b \oplus y$, and the random value c to mask the output $z = x$ AND y, then we have

$$\widetilde{z} = (\widetilde{x} \oplus a)(\widetilde{y} \oplus b) \oplus c = \widetilde{x}\widetilde{y} \oplus \widetilde{x}b \oplus \widetilde{y}a \oplus ab \oplus c.$$

Now if a glitch occurs in $\widetilde{x}$, then the number of affected gate depends on the values

of b and $\widetilde{y}$, the results are listed in the following table:

$$\begin{cases} 0,0, \text{ if } b=\widetilde{y}=0, \\ 1,1, \text{ if } b=0,\widetilde{y}=1, \\ 1,2, \text{ if } b=1,\widetilde{y}=0, \\ 2,2, \text{ if } b=\widetilde{y}=1. \end{cases} \tag{4}$$

A s-share of $x \in \mathbb{F}_{2^n}$ is a tuple $\underline{x}=(x_1,x_2,\ldots,x_s) \in \mathbb{F}_{2^n}^s$ over $\mathbb{F}_{2^n}$ such that

$$x=\sum_{i=1}^{s} x_i.$$

Of course,

Intuitively, if a share z_i doesn't depend on the valus of inputs share x_i, then z_i cannot be correlated with x, which means that the computation of z_i won't leak information about the values of x. Therefore, we have the following properties:

Definition 1 (Non-completeness)**.** *Let $z=f(x)=(f_1(x),f_2(x),\ldots,f_m(x))$ denote a function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^m}$ which is not linear over $\mathbb{F}_2$. The non-completeness is satisfied if each share is absent from at least one coordinate function.*

1 The second-order Threshold Implementation

For the first-order Threshold Implementation, the authors gave a general $t+2$-shares construction for the permutation with degree at most $t+1$. The method they used is below, that is, to decompose the $F(\sum_{i=1}^{t+2} x_i)$ into the sum of several partial sum of the shares within t:

Lemma 2. *Let $F:\mathbb{F}_2^n \to \mathbb{F}_2^m$ be of algebraic degree at most $t \geq 1$ and let $s \geq t$. Then for every $x_1,x_2,...,x_s \in \mathbb{F}_2^n$, we have that*

$$F\left(\sum_{i=1}^{s} x_i\right)=\sum_{j=0}^{t} \mu_{s,t}(j) \sum_{I \in \mathcal{I}_s,|I|=j} F\left(\sum_{i \in I} x_i\right).$$

In fact, they deduce higher order derivates of F to obtain the key parts:

$$D_{x_1,x_2,\ldots,x_{t+1}}F(x)=F(x)+F(x+x_1)+F(x+x_2)+\cdots+F\left(x+\sum_{i=1}^{t+1} x_i\right)=0$$

since the algebraic degree of F is at most t. And then subsititude $x = x_{t+1}$ into above equation to get

$$F(x_{t+1}) + F(x_{t+1} + x_1) + \cdots + F\left(x_{t+1} + \sum_{i=1}^{t} x_i\right) + \cdots + F\left(x_{t+1} + \sum_{i=1}^{t+1} x_i\right) = 0.$$

Therefore assume $x_{t+1} = x_{t+1} + x_{t+2}$, we conclude that

$$F\left(\sum_{i=1}^{t+2} x_i\right) = F(x_{t+1} + x_{t+2}) + F(x_{t+1} + x_{t+2} + x_1) + \cdots + F\left(\sum_{i=1}^{t} x_i\right). \tag{5}$$

Furthermore, we can divide the right parts of equation (5) into several parts:

$$\begin{aligned}
&F\left(\sum_{i=1}^{t+2} x_i\right) \\
=&\sum_{I\in\mathcal{I}_t} F\left(\sum_{i\in I} x_i\right) \\
&+ \sum_{I\in\mathcal{I}_0} F\left(\sum_{i\in I} x_i + \sum_{i=2}^{t+2} x_i\right) \\
&+ \sum_{I\in\mathcal{I}_1} F\left(\sum_{i\in I} x_i + \sum_{i=3}^{t+2} x_i\right) \\
&+ \cdots + \\
&+ \sum_{I\in\mathcal{I}_{t-1}} F\left(\sum_{i\in I} x_i + \sum_{i=t+1}^{t+2} x_i\right)
\end{aligned}$$

Actually the sum can be listed in below:

$$
\begin{array}{|cccccccc|}
\hline
0 & x_2 & x_3 & x_4 & \cdots & x_{t-1} & x_t & x_{t+1} & x_{t+2} \\
\hline
0 & 0 & x_3 & x_4 & \cdots & x_{t-1} & x_t & x_{t+1} & x_{t+2} \\
x_1 & 0 & x_3 & x_4 & \cdots & x_{t-1} & x_t & x_{t+1} & x_{t+2} \\
\hline
0 & 0 & 0 & x_4 & \cdots & x_{t-1} & x_t & x_{t+1} & x_{t+2} \\
0 & x_2 & 0 & x_4 & \cdots & x_{t-1} & x_t & x_{t+1} & x_{t+2} \\
x_1 & 0 & 0 & x_4 & \cdots & x_{t-1} & x_t & x_{t+1} & x_{t+2} \\
x_1 & x_2 & 0 & x_4 & \cdots & x_{t-1} & x_t & x_{t+1} & x_{t+2} \\
\hline
0 & 0 & 0 & 0 & \cdots & x_{t-1} & x_t & x_{t+1} & x_{t+2} \\
0 & 0 & x_3 & 0 & \cdots & x_{t-1} & x_t & x_{t+1} & x_{t+2} \\
0 & x_2 & 0 & 0 & \cdots & x_{t-1} & x_t & x_{t+1} & x_{t+2} \\
0 & x_2 & x_3 & 0 & \cdots & x_{t-1} & x_t & x_{t+1} & x_{t+2} \\
x_1 & 0 & 0 & 0 & \cdots & x_{t-1} & x_t & x_{t+1} & x_{t+2} \\
x_1 & 0 & x_3 & 0 & \cdots & x_{t-1} & x_t & x_{t+1} & x_{t+2} \\
\hline
\vdots & \vdots & \vdots & \vdots & & \vdots & \vdots & \vdots & \vdots \\
0 & 0 & 0 & 0 & \cdots & 0 & 0 & x_{t+1} & x_{t+2} \\
0 & 0 & 0 & 0 & \cdots & x_{t-1} & 0 & x_{t+1} & x_{t+2}
\end{array}
$$