Aalto University
School of Science
and Technology

Master's Thesis Presentation
On the Properties of S-boxes

Léo Perrin (perrin.leo@gmail.com)
Supervisor: Céline Blondeau

Department of Information and Computer Science
Aalto University, School of Science and Technology

March 18, 2013

Table of contents

Table of Contents

Purpose of Cryptography

- Use of electronic communications is *huge*.
  - HTTP
  - Mail
  - *Cloud computing*
- Communication through unsecure channel requires protection.
- Electronic data must be protected too.
  - Thumb drive
  - Computer HDD

Cryptographic Primitives

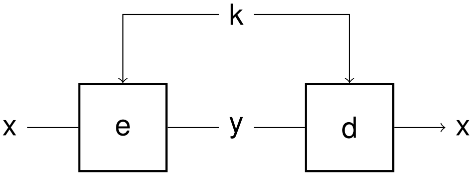
Protection: cryptographic primitives

- Read only by the recipient: Ciphers.
- No tampering: Hash functions, MAC.
- Authentication: Electronic Signatures.

Asymmetric vs. Symmetric

Today: Symmetric cryptography.

Block Cipher

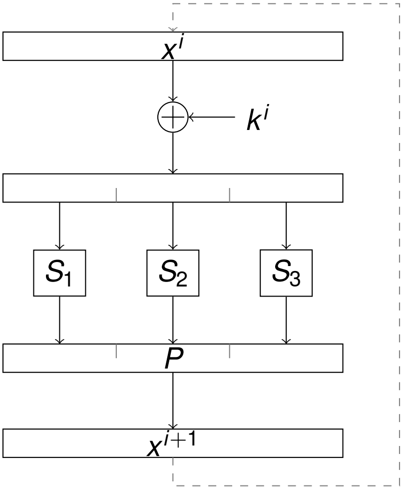


Claude Shannon's construction (ciphers): multiple iteration of confusion and diffusion.

Diffusion Small modification in input $\Longrightarrow$ Great modification in output.

Confusion No simple relation between input and output.

Substitution-Permutation Network



Attack Models

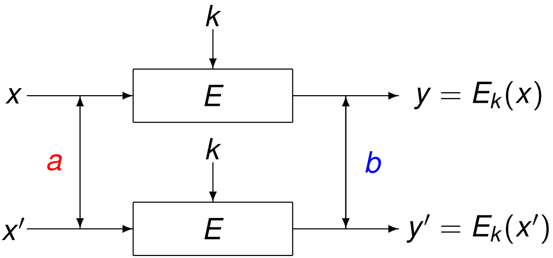
Attack (Cryptanalysis) The action of trying to extract useful data from a ciphertext without any previous knowledge of the key.

Chosen plaintext attack The attacker has a black-box `cipher + key` and can encrypt any plaintext with it.

Statistical attack Uses the fact that the distribution of ciphertext has some statistical bias.

...

Differential Cryptanalysis (1/2)



Differential cryptanalysis relies on the existence of (a, b) such that $E_k(x + a) + E_k(x) = b$ for many plaintexts x.

Differential Cryptanalysis (2/2)

Idea: look at pairs (a, b) called differentials that have a high probability for a fixed k.

Definition (Propagation ratio)

$$
\begin{aligned}
R_p(a, b) &= \mathbf{Pr}[\ E_k(x + a) + E_k(x) = b\ ] \\
&= \frac{\delta(a, b)}{2^n}
\end{aligned}
$$

where $\delta(a, b)$ is the number of plaintexts x such that $E_k(x + a) + E_k(x) = b$

S-boxes

S-boxes are key components of most ciphers (SPN and Feistel).

- $S : \{0,1\}^n \mapsto \{0,1\}^m$
- S-boxes should be non-linear (confusion).
- Monomials ($x \mapsto x^d$) imply “easy” study and “easy” hardware implementation.

Table of Contents

Math Reminder and Notations (1/2)

- $\mathbb{F}_{2^n}$ is the field of characteristic 2 of size 2^n.
- Frobenius automorphism:

$$(a+b)^{2^i} = a^{2^i} + b^{2^i}.$$

- The absolute trace over $\mathbb{F}_{2^n}$ is:

$$\mathbf{Tr}(x) = \sum_{i=0}^{n-1} x^{2^i},\ \mathbf{Tr}(x) \in \{0,1\}$$

Math Reminder and Notations (2/2)

- We denote:
  - $\mathcal{F} = \mathbb{F}_{2^n} \backslash \{0, 1\}$
  - and $\mathcal{F}_c = \{x \in \mathcal{F}, \mathbf{Tr}(x) = c\}$
- The derivative of $F : \mathbb{F}_{2^n} \mapsto \mathbb{F}_{2^m}$ with respect to $a \in \mathbb{F}_{2^n}^*$ is:

$$\mathbb{D}_a F(x) = F(x + a) + F(x)$$

Differential Uniformity

Resistance against differential cryptanalysis depends on the differential uniformity (introduced by Nyberg):
Let $F : \mathbb{F}_{2^n} \mapsto \mathbb{F}_{2^m}$. Then:

$$\delta(a, b) = |\{x \in \mathbb{F}_{2^n},\ \mathbb{D}_a F(x) = b\}|$$

Definition

The differential uniformity of F is $u(F)$ with:

$$u(F) = \max_{a \neq 0,\ b \in \mathbb{F}_{2^n}} \delta(a, b)$$

Functions F such that $u(F) = 2$ are called Almost-Perfect Non-linear (APN).

Differential Spectrum

For monomials, studying $\delta(1, b)$ is enough:

$$(x+a)^d + x^d = b \Leftrightarrow \; a^d\Big((\frac{x}{a}+1)^d + (\frac{x}{a})^d \Big) = b$$

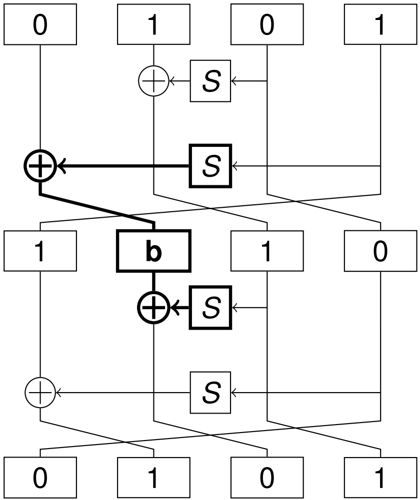
Let $\delta(b) = \delta(1, b)$.

Definition

Let $\omega_i = |\{b \in \mathbb{F}_{2^n}, \delta(b) = i\}|$. The differential spectrum of a monomial F is:

$$\mathbb{S} = \{\omega_0, \omega_2, ..., \omega_{u(F)}\}$$

Cryptographic Relevance of the Spectrum



Studied differential:
$\big((0,1,0,1),(0,1,0,1)\big)$.

$$\begin{aligned}\mathbf{Pr}[(a,b)] &= \sum_{b\in\mathbb{F}_{2^n}} \mathbf{Pr}[S: 1 \mapsto b]^2 \\ &= \frac{1}{2^{2n}} \sum_{k=0}^{u(S)} \omega_k \cdot k^2 \\ &= \frac{\ell_S}{2^{2n}}\end{aligned}$$

Influence of the Differential Spectrum

$u(F_d)$	d	Differential Spectrum of F_d	ℓ_{F_d}
4	511	$\omega_0 = 513,\ \omega_2 = 510,\ \omega_4 = 1$	2056
	84	$\omega_0 = 572,\ \omega_2 = 392,\ \omega_4 = 60$	2528
	103	$\omega_0 = 588,\ \omega_2 = 360,\ \omega_4 = 76$	2656
	87	$\omega_0 = 632,\ \omega_2 = 272,\ \omega_4 = 120$	3008
	160	$\omega_0 = 768,\ \omega_2 = 0,\ \omega_4 = 256$	4096
6	147	$\omega_0 = 597,\ \omega_2 = 347,\ \omega_4 = 75,\ \omega_6 = 5$	2768
	122	$\omega_0 = 608,\ \omega_2 = 330,\ \omega_4 = 76,\ \omega_6 = 10$	2896
	152	$\omega_0 = 628,\ \omega_2 = 300,\ \omega_4 = 76,\ \omega_6 = 20$	3136
	118	$\omega_0 = 623,\ \omega_2 = 315,\ \omega_4 = 61,\ \omega_6 = 25$	3136
	7	$\boldsymbol{\omega_0 = 583},\ \boldsymbol{\omega_2 = 405},\ \boldsymbol{\omega_4 = 1},\ \boldsymbol{\omega_6 = 35}$	2896
	54	$\omega_0 = 667,\ \omega_2 = 242,\ \omega_4 = 75,\ \omega_6 = 40$	3608
	167	$\omega_0 = 688,\ \omega_2 = 210,\ \omega_4 = 76,\ \omega_6 = 50$	3856

Properties of the Differential Spectrum

$\mathbb{S} = \{\omega_0, \omega_2, ..., \omega_{\delta(F)}\}$: differential spectrum of a monomial F.

$$\sum_{i=0}^{\delta(F)} \omega_i = 2^n \ , \quad \sum_{i=0}^{\delta(F)} i \cdot \omega_i = 2^n$$

Lemma

If $e \equiv 2^k \cdot d \mod (2^n - 1)$ *or if* $e \equiv d^{-1} \mod (2^n - 1)$ *then* F_e *has the same spectrum as* F_d*.*

Theorem

Let $G_t(x) = x^{2^t - 1}$ *and* $s = n - t + 1$*. Then* G_t *and* G_s *have the same restricted differential spectrum.*

Differential Spectra of $x \mapsto x^{2^t-1}$ for $n = 14$

t	$\delta(0), \delta(1)$	restricted spectrum
2	2 , 2	0 [8192] 2 [8190]
3	0 , 4	0 [9578] 2 [6111] 6 [693]
4	2 , 2	0 [9548] 2 [6216] 6 [588] 14 [30]
5	0 , 4	0 [9578] 2 [6111] 6 [693]
6	2 , 2	0 [9548] 2 [6216] 6 [588] 14 [30]
7	126 , 4	0 [8255] 2 [8127]
8	2 , 128	0 [8255] 2 [8127]
9	0 , 4	0 [9548] 2 [6216] 6 [588] 14 [30]
10	2 , 2	0 [9578] 2 [6111] 6 [693]
11	0 , 4	0 [9548] 2 [6216] 6 [588] 14 [30]
12	2 , 2	0 [9578] 2 [6111] 6 [693]
13	0 , 4	0 [8192] 2 [8190]

On the 2,4 Differentially Uniform Functions

Differentially 2 and 4-uniform monomials are well known.

name	exponent
quadratic	$2^{t} + 1$
Kasami	$2^{2t} - 2^{t} + 1$
Bracken-Leander	$2^{2t} + 2^{t} + 1$
Inverse	$2^{n-1} - 1$

Conjecture: All differentially 4-uniform are in this table.

Table of Contents

Kloosterman's Sum

It is denoted $K(1)$:

$$\begin{aligned} K(1) &= \sum_{x \in \mathbb{F}_{2^n}} (-1)^{\mathbf{Tr}(x+x^{-1})} \\ &= 2^n - |\{x \in \mathbb{F}_{2^n}, \mathbf{Tr}(x + x^{-1}) = 1\}| \\ &= 1 + \frac{(-1)^{n-1}}{2^{n-1}} \sum_{i=0}^{\lfloor \frac{n}{2} \rfloor} (-1)^i \binom{n}{2i} 7^i, \end{aligned}$$

with $(-1)^{\mathbf{Tr}(x^{-1})} = 1$ when $x = 0$.

Differential Spectrum of $x \mapsto x^7$

Blondeau, Canteaut and Charpin (**BCC11**): the spectrum of $x \mapsto x^7$ (and of $x \mapsto x^{2^{n-2}-1}$) is:

- If n is odd, then:

$$\omega_6 = \frac{2^{n-2}+1}{6} - \frac{K(1)}{8},\ \omega_4 = 0$$
$$\omega_2 = 2^{n-1} - 3\omega_6,\ \omega_0 = 2^{n-1} + 2\omega_6 + 1$$

- If n is even, then:

$$\omega_6 = \frac{2^{n-2}-4}{6} + \frac{K(1)}{8},\ \omega_4 = 1$$
$$\omega_2 = 2^{n-1} - 3\omega_6 - 2,\ \omega_0 = 2^{n-1} + 2\omega_6 + 1$$

Blondeau's Conjectures

Conjecture 8.9. *La fonction* $G_t(x) = x^{2^t-1}$ *avec* $t = (n-1)/2$ *a le même spectre différentiel que la fonction* $G_3 = x^7$.

Conjecture 8.10. *Soient* n *et* k *tel que* $n \equiv k \mod 3$ *et* $k = 1$ *ou* 2 *alors le spectre différentiel privé de* $\delta(0)$ *et* $\delta(1)$ *de* $G_{\frac{n+k}{3}}$ *est le même que celui de* $G_3(x) = x^7$.

Conjecture

$G_t(x) = x^{2^t-1}$ *with* $t = (n-1)/2$ *has the same spectrum as* $G_3(x) = x^7$.

Conjecture

Let n *and* k *be such that* $n \equiv k \mod (3)$ *and* $k = 1$ *or* 2*; then the differential spectrum minus* $\delta(0)$ *and* $\delta(1)$ *of* $G_{(n+k)/3}$ *is the same as that of* $G_3(x) = x^7$.

Outline of the Proof in BCC11

1. $\delta(0)$ and $\delta(1)$ are computed independently.
2. Re-write $(x+1)^7 + x^7 = b$:

$$\begin{cases} \ell_\beta(y) & = 0 \\ \mathbf{Tr}(y) & = 0, \end{cases} \qquad \ell_\beta = y^3 + y + \beta.$$

3. Aim: to compute $\omega_0 = \#\{\beta \mid \text{system has no solution}\}$.
   - A theorem gives the number of roots of ℓ_β depending on β.
   - Explain why when ℓ_β has 3 roots, exactly 1 or 3 satisfy the trace condition.
   - Use Kloosterman's sum $K(1)$ when ℓ_β has 1 root.
4. Compute the rest of the spectrum using $\sum \omega_i = 2^n$ and $\sum i \cdot \omega_i = 2^n$.

Outline of our PROOFS

1. $\delta(0)$ and $\delta(1)$ are computed independently.
2. Re-write $(x+1)^{2^t-1} + x^{2^t-1} = b$:

$$\begin{cases} \mathcal{L}_\beta(v) & = 0 \\ \mathbf{Tr}(v^q) & = c, \end{cases} \quad \mathcal{L}_\beta(v) = v^{2^t+1} + v + \beta$$

3. Aim: to compute $\omega_0 = \#\{\beta \mid \text{system has no solution}\}$.
   - Use a theorem to find number of roots of $\mathcal{L}_\beta$.
   - Explain why when $\mathcal{L}_\beta$ has 3 roots, exactly 1 or 3 satisfy the trace condition.
   - Involve the Kloosterman's sum $K(1)$ when $\mathcal{L}_\beta$ has 1 root.
4. Compute the rest of the spectrum using $\sum \omega_i = 2^n$ and $\sum i \cdot \omega_i = 2^n$.

Same structure as in **BCC11**...

But!

$t = 3 \implies$ small and constant degree of the polynomial (ℓ_β vs. $\mathcal{L}_\beta$). Here...

No.

More complicated. Lots of non-trivial computations not shown here.

Theorem 1 of Helleseth and Kholosha's Paper (08)

We define polynomial $\mathcal{L}_a$ by

$$\mathcal{L}_a(x) = x^{2^t+1} + x + a.$$

- Let $t \leq n$ and $\gcd(t, n) = 1$. For any $a \in \mathbb{F}_{2^n}^*$, $\mathcal{L}_a$ has either 0,1 or 3 roots in $\mathbb{F}_{2^n}$.
- $\mathcal{L}_a$ has exactly one root $x_0 \in \mathbb{F}_{2^n}^*$ if and only if $\mathbf{Tr}\left((1 + x_0^{-1})^\tau\right) = 1$ where $\tau \equiv (2^t - 1)^{-1} \mod (2^n - 1)$.
- Let $M_i = \#\{a \in \mathbb{F}_{2^n}^*, \mathcal{L}_a \text{ has } i \text{ roots}\}$.

For n odd, $\quad M_0 = \dfrac{2^n + 1}{3}, \quad M_1 = 2^{n-1} - 1, \quad M_3 = \dfrac{2^{n-1} - 1}{3}.$

For n even, $\quad M_0 = \dfrac{2^n - 1}{3}, \quad M_1 = 2^{n-1}, \quad M_3 = \dfrac{2^{n-1} - 2}{3}.$

Table of Contents

t=(kn+1/3)

Wanted to study $t = (n + k)/3$, but...

- If $k = 1$, $t = (n + 1)/3$.
- If $k = 2$, $s = (2n + 1)/3$, $(s = n - t + 1)$.
- $2^{(kn+1)/3} - 1$ is invertible modulo $2^n - 1$.

We studied $t = (kn + 1)/3$ with $2 \equiv n/k \mod 3$ instead.

Base Problem

BCC11: the number of solutions of $(x+1)^{2^t-1} + x^{2^t-1} = b$ is the number of roots of

$$P_b(x) = x^{2^t} + bx^2 + (b+1)x$$

and half that of

$$\begin{cases} Q_b(y) & = & by \\ \mathbf{Tr}(y) & = & 0 \end{cases}, \; Q_b(y) = \sum_{i=0}^{t-1} y^{2^i}.$$

Rewriting the Problem (1/3)

An interesting observation:

$$Q_b(y)^{2^t} = \sum_{i=0}^{t-1} y^{2^{i+t}} = \sum_{i=t}^{2t-1} y^{2^i}$$

$$Q_b(y)^{2^{2t}} = \sum_{i=0}^{t-1} y^{2^{i+2t}} = \sum_{i=2t}^{3t-1} y^{2^i}.$$

Where $3t - 1 = (kn + 1) - 1$. Thus:

$$Q_b(y) + Q_b(y)^{2^t} + Q_b(y)^{2^{2t}} = k \cdot \mathbf{Tr}(y) + y^{2^{kn}} = y.$$

Rewriting the Problem (2/3)

Furthermore:

$$L_1(u) = u + u^{2^t} + u^{2^{2t}}$$

has a unique root, 0.

We deduce that $Q_b(y) + by = 0$ and $\mathbf{Tr}(y) = 0$ is equivalent to:

$$\begin{cases} Q_b(y) + by + \big(Q_b(y) + by\big)^{2^t} + \big(Q_b(y) + by\big)^{2^{2t}} = 0 \\ \mathbf{Tr}(y) = 0 \end{cases}$$

Rewriting the Problem (3/3)

Thus, if we let $z = by$ and $\beta = 1 + b^{-1}$:

$$\begin{cases} z^{2^{2t}} + z^{2^t} + \beta z = 0 \\ \mathbf{Tr}(z) = 0 \end{cases}$$

At last, let $v = z^{2^t - 1}$ and $\tau = (2^t - 1)^{-1} \mod (2^n - 1)$:

Theorem

The differential spectrum of G_t for $t = (kn + 1)/3$ is given by the number of solutions of the following system:

$$\begin{cases} \mathcal{L}_\beta(v) = v^{2^t + 1} + v + \beta = 0 \\ \mathbf{Tr}(v^\tau) = 0 \end{cases}$$

Counting Solutions (1/2)

We want to know when the system has no solutions. We know that:

- $\mathcal{L}_\beta(v) = 0$ has 0, 1 or 3 solutions.
- If v_1, v_2, v_3 are solutions, then v_1^τ, v_2^τ and v_3^τ are solutions of a linear polynomial, so $v_1^\tau + v_2^\tau + v_3^\tau = 0$.Thus, either

$$\mathbf{Tr}(v_1^\tau) = \mathbf{Tr}(v_2^\tau) = \mathbf{Tr}(v_3^\tau) = 0$$

or

$$\mathbf{Tr}(v_1^\tau) = \mathbf{Tr}(v_2^\tau) = 1, \; \mathbf{Tr}(v_3^\tau) = 0$$

So exactly 1 or 3 satisfy the trace condition.

Counting Solutions (2/2)

- $\mathcal{L}_\beta(v) = 0$ has no solutions in $M_0 = \frac{2^n - (-1)^n}{3}$ cases.
- $\mathcal{L}_\beta(v) = 0$ has a unique solution v_0 if and only if $\mathbf{Tr}\big((1 + v_0^{-1})^\tau\big) = 1$.

Let $\mathcal{B}_1$ be defined by:

$$\mathcal{B}_1 = \{v \in \mathcal{F}, \mathbf{Tr}(v^\tau) \neq 0, \mathbf{Tr}\big((1 + v^{-1})^\tau\big) = 1\}$$

then the ω_0 is:

$$\omega_0 = \frac{2^n - (-1)^n}{3} + |\mathcal{B}_1|$$

and so:

$$\omega_0 = \frac{2^n - (-1)^n}{3} + 2^{n-2} + (-1)^n \frac{K(1)}{4}$$

Conclusion for $t = (kn+1)/3$

Theorem

Let $t = \frac{kn+1}{3}$ and $k = 1$ or 2 such that $kn \equiv -1 \mod 3$. G_t is differentially 6-uniform. Its differential spectrum is:

$$\text{if } n \equiv \pm 1 \bmod 6, \quad \omega_6 = \frac{2^{n-2}+1}{6} - \frac{K(1)}{8}, \quad \omega_4 = 0,$$
$$\text{if } n \equiv \pm 2 \bmod 6, \quad \omega_6 = \frac{2^{n-2}-4}{6} + \frac{K(1)}{8}, \quad \omega_4 = 1,$$

$$\omega_2 = 2^{n-1} - 3\omega_6 - 2\omega_4 \text{ and } \omega_0 = 2^{n-1} + 2\omega_6 + \omega_4.$$

CQFD.

Table of Contents

A New Approach

- Study $t = (n-1)/2$ for odd n.
- $x \mapsto x^{2^t-1}$ is a permutation and $\tau = (2^t - 1)^{-1} \equiv -2 - 2^{t+1}$ mod $(2^n - 1)$.
- $3 \times \frac{n-1}{2} \not\equiv 1 \mod n$, so we can't do as before...

Idea!

Lemma (from **BCC11**)

The differential spectrum of a function is the same as that of its inverse.

A New Equation...

Number of solutions of:

$$(x+1)^{\tau} + x^{\tau} = b$$

After computations, this equation is equivalent to:

$$c(x^2+x)^{2^t+1} + x^{2^t} + x + 1 = 0$$

where $c = b^{2^{n-1}}$.

Let $y = x + x^2$:

$$A(y) = cy^{2^t+1} + \sum_{i=0}^{t-1} y^{2^i} + 1 = 0$$

... And a New System

This system has half as many solutions as $(x+1)^\tau + x^\tau = b$.

$$\begin{cases} A(y) = cy^{2^t+1} + \sum_{i=0}^{t-1} y^{2^i} + 1 = 0 \\ \mathbf{Tr}(y) = 0 \end{cases}$$

Sort of ugly...

But!

$$A(y) + A(y)^{2^{t+1}} = \mathbf{Tr}(y) + y^{2^t}\left(c^{2^{t+1}} y^{2^t+1} + cy + 1\right)$$

This system has exactly the same solutions as:

$$\begin{cases} c^{2^{t+1}} y^{2^t+1} + cy + 1 = 0 \\ \mathbf{Tr}(cy^{2^t+1}) = 1 \end{cases}$$

Obtaining the Base System

Let $v = yc^{2-2^{t}+1}$. Then the previous system becomes:

$$\begin{cases} \mathcal{L}_\beta(v) = v^{2^t+1} + v + \beta = 0 \\ \mathbf{Tr}(v) = 1 + \mathbf{Tr}(\beta) \end{cases}$$

where $\mathbf{Tr}(v) = 1 + \mathbf{Tr}(\beta)$ is the same as $\mathbf{Tr}(v^{2^t+1}) = 1$.

Good...
But not a great trace condition.

$\implies$ We need another idea

An Expression of Triple Solutions

Lemma

Define $\Lambda : \mathcal{F}_0 \to \mathcal{F}$ *by*

$$\Lambda(\ell) = \sum_{i=1}^{t} \ell^{2^i - 1}.$$

Then:

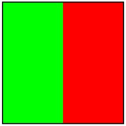
$$\{x \mid \mathcal{L}_\beta(x) = 0 \text{ and } \mathcal{L}_\beta \text{ has 3 roots}\} \;=\; Im_\Lambda(\mathcal{F}_0)$$

- Λ is an injection over $\mathcal{F}_0$.
- So is $l \mapsto 1/\Lambda(l)$.
- It holds that $\mathrm{Im}_\Lambda(\mathcal{F}_0) \cap \mathrm{Im}_{1/\Lambda}(\mathcal{F}_0) = \emptyset$.

An Expression of Unique Solutions

$\mathcal{F}$

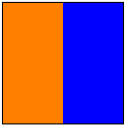
$\mathrm{Im}_\Lambda(\mathcal{F}_0)$



$\overline{\mathrm{Im}_\Lambda(\mathcal{F}_0)}$
$= \mathrm{Im}_{1/\Lambda}(\mathcal{F}_0)$

Every $x \in \mathbb{F}_{2^n}$ is a root of some $\mathcal{L}_\beta$ having exactly 1 or 3 roots.
There is $2^{n-1} - 1$ of each (Theorem 1):

Roots of $\mathcal{L}_\beta$
($\mathcal{L}_\beta$ has 3 roots)



Roots of $\mathcal{L}_\beta$
($\mathcal{L}_\beta$ has 1 roots)

$$\{x \mid x \text{ is the unique root of } \mathcal{L}_\beta\} = \mathrm{Im}_{1/\Lambda}(\mathcal{F}_0)$$

Counting Solutions (1/2)

We want now to compute ω_0 using the expressions we found.

- $\mathcal{L}_\beta(v) = 0$ has 0, 1 or 3 solutions.
- If v_1, v_2, v_3 are solutions, then they yield:
  - $v_3^\tau = v_1^\tau + v_2^\tau$.
  - $v_1^{-1} + v_2^{-1} + v_3^{-1} = 1$.

$\Longrightarrow$ Exactly one or three satisfy the trace condition.

Counting Solutions (2/2)

- $\mathcal{L}_\beta(v) = 0$ has no solutions in $M_0 = \frac{2^n - (-1)^n}{3}$ cases.
- $\mathcal{L}_\beta(v) = 0$ has a unique solution v_0 if and only if there is $l \in \mathcal{F}_0$ such that $v_0 = 1/\Lambda(l)$.

Let $\mathcal{B}_1$ be defined by:

$$\mathcal{B}_1 = \{v \in \mathcal{F}, \mathbf{Tr}(v^{2^t+1}) \neq 1, \exists l \in \mathcal{F}_0, v = 1/\Lambda(l)\}$$

then ω_0 is:

$$\frac{2^n - 1}{3} + |\mathcal{B}_1|$$

Again: $|\mathcal{B}_1| = 2^{n-2} + (-1)^n K(1)/4$.

Conclusion for $t = (n-1)/2$

We obtain (almost) the same result!

Theorem

Let n odd and $t = (n-1)/2$. The functions G_t is locally differentially 6-uniform. Its differential spectrum is:

$$\text{if } n \equiv \pm 1 \bmod 6, \quad \omega_8 = 0, \quad \omega_6 = \frac{2^{n-2}+1}{6} - \frac{K(1)}{8},$$

$$\text{if } n \equiv 3 \bmod 6, \quad \omega_8 = 1, \quad \omega_6 = \frac{2^{n-2}-8}{6} - \frac{K(1)}{8},$$

$$\omega_4 = 0, \omega_2 = 2^{n-1} - 3\omega_6 - 4\omega_8 \text{ and } \omega_0 = 2^{n-1} + 2\omega_6 + 3\omega_8.$$

CQFD.

Table of Contents

Dickson Polynomials (1/2)

Dickson polynomials $D_n(x, y)$:

$$D_n(x + y, xy) = x^n + y^n.$$

Definition of differential spectrum: number of roots of

$$(x + 1)^d + x^d = b$$
$$\Leftrightarrow D_n(1, x^2 + x) = b.$$

Hou. *et al.* (2009) introduced reversed Dickson polynomial

$$RD_d(y) = D_d(1, y).$$

Dickson Polynomials (2/2)

Equivalent definition of the differential spectrum:

$$\omega_{2k} = |\{b \in \mathbb{F}_{2^n},\ RD_d(y) = b \text{ has } k \text{ solutions in } \mathcal{F}_0\}|$$

Recall result from **BCC11**: for $d = 2^t - 1$,

$$\omega_{2k} = |\{b \in \mathbb{F}_{2^n},\ \sum_{i=0}^{t-1} y^{2^i} = by \text{ has } k \text{ solutions in } \mathcal{F}_0\}|$$

It turns out (**Göl12**) that

$$RD_{2^t-1}(y) = \sum_{i=0}^{t-1} y^{2^i-1}.$$

Resilience Against other Attacks

Linear Attacks Depends on non-linearity. We know no general fomula.

Experiments:

- No pattern for the value of the non-linearity.
- Value of non-linearity for small n: not bad.

Algebraic Attacks Depends on algebraic degree, i.e. Hamming weight of exponent.

- Algebraic degree: always t (or s).
- Inverse also matters.
- $t = \frac{kn+1}{3}$ (and corresponding s): very bad.
- $s = \frac{n+3}{2}$ is pretty good.

Conclusion

All locally differentially 6-uniform monomials have exponent $2^t - 1$ with:

- $t = 3$ or $n - 2$.
- $t = \frac{n-1}{2}$ or $s = \frac{n+3}{2}$.
- $t = \frac{kn+1}{3}$ or $s = \frac{(3-k)n+2}{3}$.
- Conjecture: $t = \frac{n}{3}$ or $s = \frac{2n}{3} + 1$.
- Conjecture: $t = \frac{n}{3} + 1$ or $s = \frac{2n}{3}$.

Thank you!