Sparse Permutations with Low Differential Uniformity[1]

Valentin Suder (Inria Paris-Rocquencourt)

Joint work with

Pascale Charpin (Inria Paris-rocquencourt) and
Gohar Kyureghyan (Otto-von-Guericke University of Magdeburg)

[1]Published in *Finite Fields and Their Applications* 28 (2014) 214–243 (available online).

Outline

Preliminaries

- Symmetric Cryptography
- APN/AB Functions

Previous works

- Permutations by Switching
- Negative Answers

Main Results

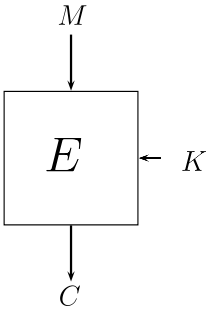
- Compositional Inverses
- $F_{s,1,\gamma}(x) = x^s + \gamma Tr(x)$
- $F(x) = x^{-1} + \gamma Tr(x^t)$

Conclusion

Outline

Block Ciphers

$M \in \mathbb{F}_2^m$: plaintext,
$C \in \mathbb{F}_2^m$: ciphertext,
$K \in \mathbb{F}_2^k$: key.



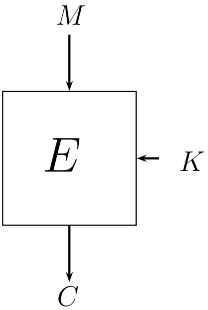
Block Cipher

$$\begin{array}{rccl} E: & \mathbb{F}_2^m \times \mathbb{F}_2^k & \rightarrow & \mathbb{F}_2^m \\ & (M, K) & \mapsto & E(M, K) = C. \end{array}$$

For a fixed key $K \in \mathbb{F}_2^k$,
$E_K(M) \mapsto C$, is a permutation of $\mathbb{F}_2^m$.

Block Ciphers

$M \in \mathbb{F}_2^m$: plaintext,
$C \in \mathbb{F}_2^m$: ciphertext,
$K \in \mathbb{F}_2^k$: key.



Block Cipher

$$\begin{aligned} E: \quad \mathbb{F}_2^m \times \mathbb{F}_2^k &\rightarrow \mathbb{F}_2^m \\ (M, K) &\mapsto E(M, K) = C. \end{aligned}$$

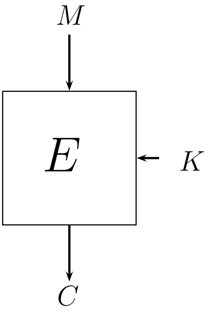
For a fixed key $K \in \mathbb{F}_2^k$,
$E_K(M) \mapsto C$, is a permutation of $\mathbb{F}_2^m$.

Problems? In practice: $m \geq 64$ and $k \geq 80$ (!!!)

- For one key K, E_K permutes 2^{64} elements!

Block Ciphers

$M \in \mathbb{F}_2^m$: plaintext,
$C \in \mathbb{F}_2^m$: ciphertext,
$K \in \mathbb{F}_2^k$: key.



Block Cipher

$$E : \begin{array}{rcl} \mathbb{F}_2^m \times \mathbb{F}_2^k & \to & \mathbb{F}_2^m \\ (M, K) & \mapsto & E(M, K) = C. \end{array}$$

For a fixed key $K \in \mathbb{F}_2^k$,
$E_K(M) \mapsto C$, is a permutation of $\mathbb{F}_2^m$.

Problems? In practice: $m \geq 64$ and $k \geq 80$ (!!!)

- For one key K, E_K permutes 2^{64} elements!
- 2^{80} different permutations!

Substitution Permutation Networks

Add Round Key

$$\begin{aligned} \mathbb{F}_2^m x \mathbb{F}_2^m &\to \mathbb{F}_2^m \\ (M, SubK) &\mapsto M \oplus SubK. \end{aligned}$$

$M = (M_0, \ldots, M_{m/n-1})$, $M_i \in \mathbb{F}_2^n$ (word).

SBox (substitution)

Nonlinear Permutation:

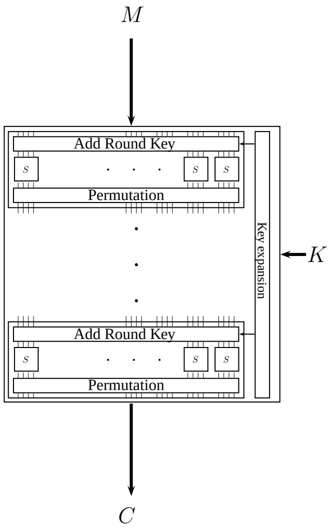
$$\begin{aligned} S: \quad \mathbb{F}_2^n &\to \mathbb{F}_2^n \\ M_i &\mapsto (S_0(M_i), \ldots, S_{n-1}(M_i)). \end{aligned}$$

In practice: $n = 4,\ 8$.

Permutation (diffusion)

Linear Permutation:

$$\mathbb{F}_2^m \to \mathbb{F}_2^m.$$



Unique Univariate Polynomial Representation of an SBox

$$\begin{array}{rccl} F : & \mathbb{F}_{2^n} & \to & \mathbb{F}_{2^n} \\ & x & \mapsto & \sum_{i=0}^{2^n-1} a_i x^i, \qquad a_i \in \mathbb{F}_{2^n}. \end{array}$$

Definition

The component functions of a function F are

$$x \mapsto Tr(\lambda F(x)), \qquad \lambda \in \mathbb{F}_{2^n}^*.$$

$Tr : \mathbb{F}_{2^n} \to \mathbb{F}_2$ is the absolute trace.

Definition

The algebraic degree of a function F is

$$\deg(F) = \max\{wt(i) \mid a_i \neq 0\}.$$

$wt : \mathbb{F}_2^n \to \mathbb{N}$ is the binary Hamming weight.

F is said *sparse* if few of the a_i's are nonzero.

Differential Uniformity

$$F \ : \ \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$$

Definition

The differential uniformity of F is defined as

$$\delta(F) = \max_{a \neq 0,\ b \in \mathbb{F}_{2^n}} \#\{x \mid F(x) + F(x+a) = b\}.$$

F is called **APN** (almost perfect nonlinear) if $\delta(F) = 2$.

Facts about APN functions

APN functions have optimal resistance against *differential attacks*.
Only one APN permutation is known for n even (Dillon's function, $n = 6$).

Nonlinearity

$$F \;:\; \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$$

Definition

The nonlinearity of F is defined as

$$\mathcal{NL}(F) = 2^{n-1} - \max_{\alpha \neq 0, \beta \in \mathbb{F}_{2^n}} \left(2^{n-1} - wt(x \mapsto Tr(\alpha F(x) + \beta x))\right).$$

F is called **AB** (almost bent) if for all $\alpha \neq 0, \beta \in \mathbb{F}_{2^n}$

$$\mathcal{NL}(F) = 2^{n-1} - 2^{\frac{n-1}{2}}.$$

Facts about AB functions

Exist for n odd only!!

AB function have optimal resistance against *linear attacks*.

Any AB function is also APN.

Properties

$$F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$$

Proposition

Differential uniformity and nonlinearity are invariants under:

- compositional inversion (when talking about permutations).
- "Extended Affine"(EA)-equivalence (i.e. $F \sim_{EA} G$ if there exist affine permutations A_0 and A_1 and some affine function A_2 such that $G = A_0 \circ F \circ A_1 + A_2$).

Outline

Permutations by switching

P. Charpin and G. Kyureghyan [SETA08] [FFA09] [AMS10]:

Theorem

Let G be a permutation on $\mathbb{F}_2$, f be any Boolean function on $\mathbb{F}_2$. Then

$$F(x) = G(x) + \gamma f(x),\ \gamma \in \mathbb{F}_{2^n}^*,$$

is a permutation of $\mathbb{F}_{2^n}$ **if and only if**

$$f \circ G^{-1}(x) + f \circ G^{-1}(x+\gamma) = 0 \qquad \text{for all } x \in \mathbb{F}_{2^n}.$$

Let $\lambda \in \mathbb{F}_{2^n}$: $Tr(\lambda F(x)) = Tr(\lambda G(x)) + Tr(\lambda\gamma) f(x)$.

Permutations by switching

P. Charpin and G. Kyureghyan [SETA08] [FFA09] [AMS10]:

Theorem

Let G be a permutation on $\mathbb{F}_2$, f be any Boolean function on $\mathbb{F}_2$. Then

$$F(x) = G(x) + \gamma f(x),\ \gamma \in \mathbb{F}_{2^n}^*,$$

is a permutation of $\mathbb{F}_{2^n}$ **if and only if**

$$f \circ G^{-1}(x) + f \circ G^{-1}(x+\gamma) = 0 \qquad \text{for all } x \in \mathbb{F}_{2^n}.$$

Let $\lambda \in \mathbb{F}_{2^n}$: $Tr(\lambda F(x)) = Tr(\lambda G(x)) + Tr(\lambda\gamma) f(x)$.

Proposition

Let $\delta(G) = \rho$, then $\delta(F) \leq 2\rho$.

Particular case with monomials

Definition

Let $1 \leq s, t \leq 2^n - 2$ and $\gamma \in \mathbb{F}_{2^n}^*$.

$$F_{s,t,\gamma}(x) = x^s + \gamma\, Tr(x^t).$$

Theorem

$F_{s,t,\gamma}$ is a permutation on $\mathbb{F}_{2^n}$ *if and only if*

$$\gcd(s, 2^n - 1) = 1,$$

$$t \equiv 2^j(2^i+1)s \pmod{2^n-1} \quad \text{for some } 0 \leq i, j \leq n-1,\ i \neq n/2,$$

and either **(a)** or **(b)** holds:

(a) $i = 0$ and $Tr(\gamma) = 0$.

(b) $i > 0$ and $\gamma \in \mathbb{F}_{2^{\gcd(2i,n)}}$ with $Tr(\gamma^{2^i+1}) = 0$.

Properties

$$F_{s,t,\gamma}(x) = x^s + \gamma\, Tr(x^t).$$

Fact: $x \mapsto x^s$ is APN $\Rightarrow \gcd(s, 2^n - 1) = 3$ if n is even and 1 otherwise.

Proposition

- If n is *even* and $x \mapsto x^s$ is APN then F is not a permutation.
- If n is *odd* and $t = s(2^i + 1)$ where $\gcd(i, n) = 1$. Then F is not a permutation. It is a $2 - to - 1$ function when $\gcd(s, 2^n - 1) = 1$ and $\gamma = 1$.

Proposition

There is no permutation on $\mathbb{F}_{2^n}$ of the shape

$$F(x) = x^{2^j+1} + \gamma\, Tr(x^{(2^i+1)(2^j+1)}),$$

with $\gcd(i, n) = 1$ and $\gcd(j, n) = 1$.

Outline

Compositional inverses

$$F(x) = G(x) + \gamma f(x),\ \gamma \in \mathbb{F}_{2^n}^*.$$

Theorem

If F is a permutation on $\mathbb{F}_{2^n}$ (i.e. $f \circ G^{-1}(x) + f \circ G^{-1}(x+\gamma) = 0$), then

$$F^{-1} = G^{-1} \circ Q,$$

where $Q(x) = x + \gamma f \circ G^{-1}(x)$.

Because

$$F = Q \circ G \qquad \text{and} \qquad Q = Q^{-1}.$$

Compositional inverses

$$F_{s,t,\gamma}(x) = x^s + \gamma\, Tr(x^t).$$

Theorem

Let $F_{s,t,\gamma}$ be a permutation on $\mathbb{F}_{2^n}$ with $t = s(2^i + 1)$ for some i. Let $\sigma = s^{-1} \pmod{2^n - 1}$. Then,

$$\begin{aligned} F^{-1}_{s,t,\gamma}(x) &= (x + \gamma\, Tr(x^{2^i+1}))^\sigma \\ &= x^\sigma + \left(\sum_{j \prec \sigma} x^j \gamma^{\sigma - j} \right) Tr(x^{2^i+1}). \end{aligned}$$

Definition: Let $a = \sum a_i 2^i$ and $b = \sum b_i 2^i$. If $a_i \geq b_i$ for all i then

$$b \preceq a \qquad \text{and } b \prec a \text{ if } a \neq b.$$

Special case when $t = 1$

$$F_{s,1,\gamma}(x) = x^s + \gamma Tr(x)$$

Theorem

$F_{s,1,\gamma}$ is a permutation on $\mathbb{F}_{2^n}$ *if and only if*

1. $s = \frac{2^j}{2^i+1} \pmod{2^n-1}^\dagger$ for some $i > 0$ and $j \geq 0$; **AND**
2. $\gcd(i,n) = \gcd(2i,n)$; **AND**
3. $\gamma \in \mathbb{F}_{2^{\gcd(i,n)}}$ such that $Tr(\gamma^{2^i+1}) = 0$.

Moreover (when $j = 0$),

$$F^{-1}_{s,1,\gamma}(x) = x^{2^i+1} + (\gamma^{2^i+1} + \gamma^{2^i} x + \gamma x^{2^i})\, Tr(x^{2^i+1}).$$

In this case,

$$\delta(F_{s,1,\gamma}) = 2^{\gcd(i,n)}, \qquad \mathcal{NL}(F_{s,1,\gamma}) = 2^{n-1} - 2^{(n+\gcd(i,n)-2)/2},$$

and $$\deg(F_{s,1,\gamma}) = \frac{n-\gcd(i,n)+2}{2}^\dagger, \qquad \deg(F^{-1}_{s,1,\gamma}) = 3.$$

† (On inversion in $\mathbb{Z}_{2^n-1}$ [KS13])

Specific Classes

$$F_{s,1,\gamma}(x) = x^s + \gamma Tr(x)$$

Let $n = 2m$, with m odd. Take

1. $\gcd(i, n) = 2$;
2. $s = \frac{1}{2^i+1}$;
3. $\gamma \in \mathbb{F}_{2^2}^*$ such that $Tr(\gamma^{2^i+1}) = 0$ (i.e. $\gamma = 1$).

Then

$$F_{s,1,\gamma}(x) = x^{\frac{1}{2^i+1}} + Tr(x)$$

is a permutation on $\mathbb{F}_{2^n}$. Moreover

$$\delta(F_{s,1,\gamma}) = 4, \qquad \mathcal{NL}(F_{s,1,\gamma}) = 2^{n-1} - 2^m \quad \text{and} \quad \deg(F_{s,1,\gamma}) = m.$$

Its *compositional inverse* is

$$F^{-1}_{s,1,\gamma}(x) = x^{2^i+1} + (1 + x + x^{2^i+1})\, Tr(x^{2^i+1}).$$

With the multiplicative inverse function

Before getting started . . .

Lemma

Let $F(x) = x^{-1} + \gamma f(x)$ where f is any boolean function on $\mathbb{F}_{2^n}$. Then

$$\delta(F) \in \begin{cases} \{2,4\} & \text{when } n \text{ is odd,} \\ \{4,6\} & \text{when } n \text{ is even.} \end{cases}$$

It is worth noticing that

for n even $, \forall f, \quad \forall \gamma,$ $\underline{F \text{ can not be } APN}$.

Specific Classes

$$F(x) = x^{-1} + \gamma Tr(x^t)$$

Proposition

Let $1 \leq i \leq n$ with $i \neq n/2$, $\gamma \in \mathbb{F}_2^{\gcd(2i,n)}$ such that $Tr(\gamma^{2^i+1}) = 0$, and

$$F_{i,\gamma}(x) = x^{-1} + \gamma Tr(x^{2^{n-1}-2^{i-1}-1}).$$

Then $F_{i,\gamma}(x)$ is a permutation on $\mathbb{F}_{2^n}$ with

$$\delta(F_{i,\gamma}) \in \begin{cases} \{2,4\} \text{ when } n \text{ is odd,} \\ \{4,6\} \text{ when } n \text{ is even.} \end{cases}$$

Remark: when $Tr(\gamma^{2^i+1}) = 1$, $F_{i,\gamma}(x)$ is $2 - to - 1$, with the same differential uniformity.

Outline

Conclusion and Perspectives

- Little is known about the *nonlinearity* of the functions $F_{s,t,\gamma}$;
- Although we have a *good upper bound* on diffrential uniformity, it is generally *difficult* to get general result;
- Other classes of functions remain to be studied:
  - $x^{2^{2k}-2^k+1} + \gamma Tr(x^{2^{3i}+1})$,
  - $x^s + \gamma Tr(x^t + x^r)$,
  - $\vdots$

Thank you!