Antiderivative Functions over $\mathbb{F}_{2^n}$

Valentin SUDER

Seminar CALIN - Paris 13
April 12nd 2016.

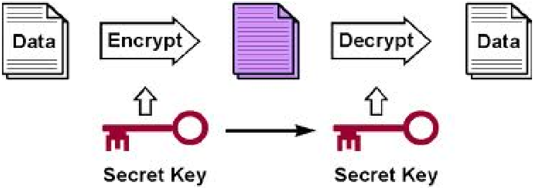
ComSec Lab, University of Waterloo ON, CANADA

Outline

Outline

Design in Symmetric Cryptography

- **Symmetric Cryptography**: Alice and Bob share the same key.



Design in Symmetric Cryptography

- **Symmetric Cryptography**: Alice and Bob share the same key.
- **Primitives**:
  - Block ciphers;
  - Stream ciphers;
  - Hash functions;

Design in Symmetric Cryptography

- **Symmetric Cryptography**: Alice and Bob share the same key.
- **Primitives**:
  - Block ciphers;
  - Stream ciphers;
  - Hash functions;

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 $\mathbb{F}_2^m$.

Design in Symmetric Cryptography

- **Symmetric Cryptography**: Alice and Bob share the same key.
- **Primitives**:
  - Block ciphers;
  - Stream ciphers;
  - Hash functions;

Block Cipher

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

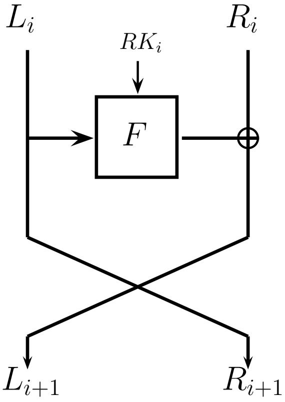
For a fixed key $K \in \mathbb{F}_2^k$,

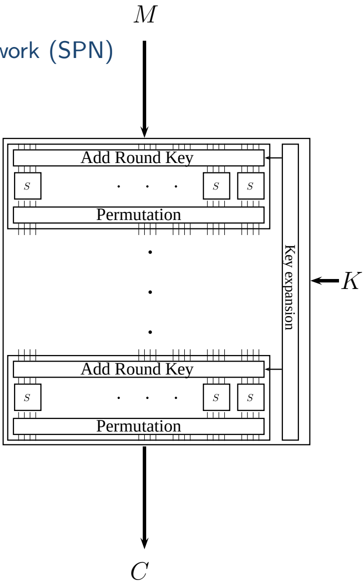
$E_K(M) \mapsto C$, is a permutation of $\mathbb{F}_2^m$.

- **Rounds composed** by smaller functions:
  - Confusion (nonlinear);
  - Diffusion (linear);

Block Ciphers

Feistel Scheme and Substitution Permutation Network (SPN)



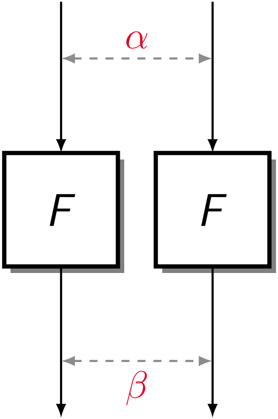


Design in Symmetric Cryptography

- **Symmetric Cryptography**: Alice and Bob share the same key.
- **Primitives**:
  - Block ciphers;
  - Stream ciphers;
  - Hash functions;
- **Rounds composed** by smaller functions:
  - Confusion (nonlinear);
  - Diffusion (linear);
- **Cryptographic requirements** of the confusion part:
  - Differential;
  - Linear;
  - Algebraic;
  - ...

Differential Properties of Sboxes

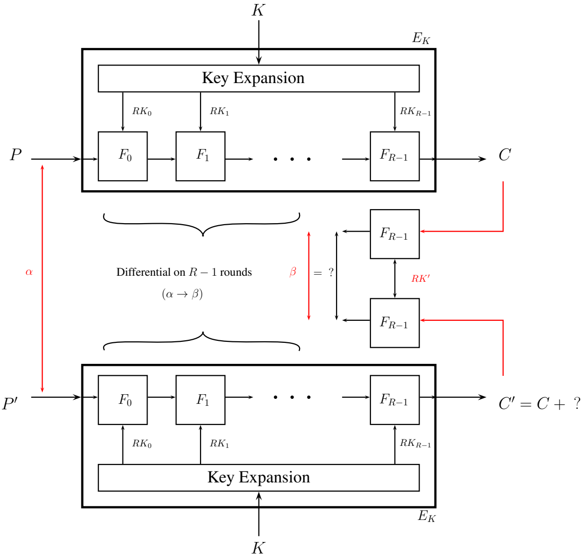
$$F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$$



$$\delta_F(\alpha, \beta) = \#\{x \mid F(x) + F(x + \alpha) = \beta\}$$

The **greater** the value $\delta_F(\alpha, \beta)$, the **more likely** an attacker can find $x \in \mathbb{F}_{2^n}$ such that $F(x) + F(x + \alpha) = \beta$.

Differential Cryptanalysis of the last round



Polynomial representation of the functions $\mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$

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

Definition

The algebraic degree of F is defined as

$$\deg(F) = \max_{0 \le i \le 2^n-1} \{wt(i) \mid c_i \neq 0\}.$$

$wt(i)$ is the binary **Hamming weigth** of the integer i.

- $F(x)$ is said to be a **permutation polynomial** if the associated function F is bijective.
- F is said to be **2-to-1** if the equation $F(x) = c$ has exactly 0 or 2 solutions, for any $c \in \mathbb{F}_{2^n}$.

Discrete derivatives

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

Definition

The discrete derivative of F in a **direction** $\alpha \in \mathbb{F}_{2^n}^*$ is defined as

$$\Delta_\alpha F(x) = F(x) + F(x+\alpha).$$

The differential uniformity of F is defined as

$$\delta(F) = \max_{\alpha \neq 0,\ \beta \in \mathbb{F}_{2^n}} \#\{x \mid \Delta_\alpha F(x) = \beta\}.$$

Definition [Lai94]

The *m*-order derivative of F in **directions** $\alpha_0, \ldots, \alpha_{m-1} \in \mathbb{F}_{2^n}$ is:

$$\Delta_{\alpha_0,\ldots,\alpha_{m-1}} F(x) = \Delta_{\alpha_0}\left(\Delta_{\alpha_1,\ldots,\alpha_{m-1}} F(x)\right).$$

Equivalences preserving differential uniformity (but not only ...)

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

EA-equivalence

F and G are Extended Affine (EA) equivalent if there are two **affine**[a] **permutations** $A_0, A_1 : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ and an **affine function** $A_2 : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ such that

$$F = A_0 \circ G \circ A_1 + A_2.$$

[a] of algebraic degree 1.

CCZ-equivalence [Carlet-Charpin-Zinoviev98]

F and G are CCZ-equivalent if their graphs $\{(x, F(x)) \mid x \in \mathbb{F}_{2^n}\}$ and $\{(x, G(x)) \mid x \in \mathbb{F}_{2^n}\}$ are **affine equivalent**, i.e. if there is an **affine permutation** $L = (L_0, L_1) : \mathbb{F}_{2^n} \times \mathbb{F}_{2^n} \to \mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$ such that

$$y = F(x) \Leftrightarrow L_0(x, y) = G(L_1(x, y)), \quad \forall (x, y) \in \mathbb{F}_{2^n}^2.$$

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

- $\alpha \in \mathbb{F}_{2^n}^*$ is a c-**linear structure** of F, $c \in \mathbb{F}_{2^n}$, if $\forall x \in \mathbb{F}_{2^n}$

$$\Delta_\alpha F(x) = F(x) + F(x+\alpha) = c.$$

- F is called **APN** (Almost Perfect Nonlinear) if

$$\delta(F) = \max_{\alpha \neq 0,\ \beta \in \mathbb{F}_{2^n}} \#\{x \mid \Delta_\alpha F(x) = \beta\} = \mathbf{2}.$$

- **EA** and **CCZ-equivalence** preserve **differential uniformity**.
- **EA-equivalence** preserves **algebraic degree**.
- The **discrete derivation** makes the **algebraic degree** decrease:

$$\deg(F) > \deg(\Delta_{\alpha_0} F) > \deg(\Delta_{\alpha_0,\alpha_1} F) > \dots$$

Differences Distribution Table (DDT) $n = 4$

$\alpha \backslash \beta$	.	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
.	16	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
1	.	.	.	2	.	2	.	2	2	.	2	2	2	.	2	.
2	.	.	2	.	.	2	.	6	2	2	.	.	.	.	2	.
3	.	.	4	2	.	.	.	4	.	.	2	.	.	4	.	.
4	.	.	.	.	.	2	2	2	2	2	4	.	.	.	.	2
5	.	4	2	.	2	.	2	.	2	.	.	2	2	.	.	.
6	.	2	.	.	2	4	2	.	.	.	.	2	.	2	.	2
7	2	2	.	2	.	.	4	.	.	2	.	2	.	.	.	2
8	.	.	.	.	.	.	.	.	6	2	.	.	4	.	4	.
9	.	2	2	.	2	.	2	.	.	2	.	2	2	2	.	.
10	2	2	.	.	2	.	2	.	.	2	2	2	.	.	.	2
11	.	.	.	2	.	.	.	2	2	.	2	.	2	.	4	2
12	.	.	.	2	2	2	.	2	2	2	2	.	.	.	.	2
13	.	4	.	2	.	.	.	.	.	.	2	4	.	4	.	.
14	.	.	2	2	2	.	2	2	.	.	2	.	.	.	2	.
15	2	.	4	.	2	.	2	.	.	.	.	2	2	.	.	2

Problem

Build new functions with desirable differential properties.

Classical Solutions

- **Tweak** known APN functions (e.g. switching method);
- Use **correspondence** with relative objects in:
  Coding Theory, *Combinatorics*, *Sequences Theory*, **. . .**
- . . .

New Idea

- **Build** derivatives with **prescribed images**;
- **Gather** them as if they are derivatives of the same **same function**;
- **Retrieve** the said **function**:
  it should have the desired differential properties.

Outline

Derivative as a linear application over $\mathbb{F}_{2^n}^{2^n}$

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

$$\Delta_\alpha F(x) = F(x) + F(x+\alpha) = \sum_i c_i x^i + \sum_i c_i (x+\alpha)^i$$

$$\vdots$$

$$= \sum_j x^j \sum_{i,\, i \succ j} c_i \alpha^{i-j}$$

Derivative as a linear application over $\mathbb{F}_{2^n}^{2^n}$

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

$$\Delta_\alpha F(x) = F(x) + F(x+\alpha) = \sum_i c_i x^i + \sum_i c_i (x+\alpha)^i$$

$$\vdots$$

$$= \sum_j x^j \boxed{\sum_{i,\, i \succ j} c_i \alpha^{i-j}}$$

$$\boxed{\left(a_0^{(j)}, a_1^{(j)}, \ldots, a_{2^n-1}^{(j)}\right) \cdot \left(c_0, c_1, \ldots, c_{2^n-1}\right)^\top}, \quad a_i^{(j)} = \begin{cases} \alpha^{i-j} & \text{if } i \succ j \\ 0 & \text{otherwise.} \end{cases}$$

$i \succ j$: $\mathrm{supp}(i) \supset \mathrm{supp}(j)$

Derivative as a linear application over $\mathbb{F}_{2^n}^{2^n}$

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

$$\Delta_\alpha F(x) = F(x) + F(x+\alpha) = \sum_i c_i x^i + \sum_i c_i (x+\alpha)^i$$

$$\vdots$$

$$= \sum_j x^j \boxed{\sum_{i,\, i \succ j} c_i \alpha^{i-j}}$$

$$\boxed{(a_0^{(j)}, a_1^{(j)}, \dots, a_{2^n-1}^{(j)}) \cdot (c_0, c_1, \dots, c_{2^n-1})^\top}, \quad a_i^{(j)} = \begin{cases} \alpha^{i-j} & \text{if } i \succ j \\ 0 & \text{otherwise.} \end{cases}$$

$$\mathtt{coeffs}(\Delta_\alpha F) = \begin{pmatrix} a_0^{(0)} & \dots & a_{2^n-1}^{(0)} \\ & \ddots & \\ a_0^{(2^n-1)} & \dots & a_{2^n-1}^{(2^n-1)} \end{pmatrix} \cdot \begin{pmatrix} c_0 \\ \vdots \\ c_{2^n-1} \end{pmatrix} = M(\alpha) \begin{pmatrix} c_0 \\ \vdots \\ c_{2^n-1} \end{pmatrix}$$

$i \succ j$: $\mathrm{supp}(i) \supset \mathrm{supp}(j)$

Recursive Construction

$n = 4$

$$M(\alpha)=\begin{pmatrix}
\cdot & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 & \alpha^7 & \alpha^8 & \alpha^9 & \alpha^{10} & \alpha^{11} & \alpha^{12} & \alpha^{13} & \alpha^{14} & \alpha^{15} \\
\cdot & \cdot & \cdot & \alpha^2 & \cdot & \alpha^4 & \cdot & \alpha^6 & \cdot & \alpha^8 & \cdot & \alpha^{10} & \cdot & \alpha^{12} & \cdot & \alpha^{14} \\
\cdot & \cdot & \cdot & \alpha & \cdot & \cdot & \alpha^4 & \alpha^5 & \cdot & \cdot & \alpha^8 & \alpha^9 & \cdot & \cdot & \alpha^{12} & \alpha^{13} \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \alpha^4 & \cdot & \cdot & \cdot & \alpha^8 & \cdot & \cdot & \cdot & \alpha^{12} \\
\cdot & \cdot & \cdot & \cdot & \cdot & \alpha & \alpha^2 & \alpha^3 & \cdot & \cdot & \cdot & \cdot & \alpha^8 & \alpha^9 & \alpha^{10} & \alpha^{11} \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \alpha^2 & \cdot & \cdot & \cdot & \cdot & \cdot & \alpha^8 & \cdot & \alpha^{10} \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \alpha & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \alpha^8 & \alpha^9 \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \alpha^8 \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 & \alpha^7 \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \alpha^2 & \cdot & \alpha^4 & \cdot & \alpha^6 \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \alpha & \cdot & \cdot & \alpha^4 & \alpha^5 \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \alpha^4 \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \alpha & \alpha^2 & \alpha^3 \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \alpha^2 \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \alpha \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot
\end{pmatrix}$$

Correspondence

For $\alpha, \gamma \in \mathbb{F}_{2^n}^*$ and for **any** $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$:

- $M(\alpha) \cdot M(\gamma) = M(\gamma) \cdot M(\alpha) \quad \Leftrightarrow \quad \Delta_{\alpha,\gamma} F(x) = \Delta_{\gamma,\alpha} F(x)$
- $M(\alpha) \cdot M(\gamma) \cdot M(\alpha + \gamma) = 0 \quad \Leftrightarrow \quad \Delta_{\alpha,\gamma,\alpha+\beta} F(x) = 0$
  in particular:

$$M(\alpha) \cdot M(\alpha) = M^2(\alpha) = 0 \quad \Leftrightarrow \quad \Delta_{\alpha,\alpha} F(x) = 0.$$

Derivative Functions

Theorem

For all $\alpha \in \mathbb{F}_{2^n}^*$, we have

$$\mathrm{Im}(M(\alpha)) = \ker(M(\alpha)).$$

Dimension $= 2^{n-1}$.

Let $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$, then

$$\Delta_\alpha f(x) = 0 \quad \Leftrightarrow \quad \exists F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n} \text{ such that } \Delta_\alpha F(x) = f(x).$$

H. Xiong, L. Qu, C. Li and Y. Li,
Some results on the differential functions over finite fields,
AAECC 25(3): 189-195, 2014.

Example: generator matrix of $\ker(M(\alpha))$

$n = 4$

$$
\begin{pmatrix}
1 & . & . & . & . & . & . & . \\
. & 1 & . & . & . & . & . & . \\
. & . & 1 & . & . & . & . & . \\
. & . & . & 1 & . & . & . & . \\
. & . & . & . & 1 & . & . & . \\
. & . & . & . & . & 1 & . & . \\
. & . & . & . & . & . & 1 & . \\
. & . & . & . & . & . & . & 1 \\
. & \alpha^{8} & \alpha^{9} & \alpha^{10} & \alpha^{11} & \alpha^{12} & \alpha^{13} & \alpha^{14} \\
. & . & . & \alpha^{9} & . & \alpha^{11} & . & \alpha^{13} \\
. & . & . & \alpha^{8} & . & . & \alpha^{11} & \alpha^{12} \\
. & . & . & . & . & . & & \alpha^{11} \\
. & . & . & . & . & \alpha^{8} & \alpha^{9} & \alpha^{10} \\
. & . & . & . & . & . & . & \alpha^{9} \\
. & . & . & . & . & . & . & \alpha^{8} \\
. & . & . & . & . & . & . & .
\end{pmatrix}
$$

Example: generator matrix of $\ker(M(\alpha))$

$n = 4$

$$
\begin{pmatrix}
1 & . & . & . & . & . & . & . \\
. & 1 & . & . & . & . & . & . \\
. & . & 1 & . & . & . & . & . \\
. & . & . & 1 & . & . & . & . \\
. & . & . & . & 1 & . & . & . \\
. & . & . & . & . & 1 & . & . \\
. & . & . & . & . & . & 1 & . \\
. & . & . & . & . & . & . & 1 \\
. & \alpha^{8} & \alpha^{9} & \alpha^{10} & \alpha^{11} & \alpha^{12} & \alpha^{13} & \alpha^{14} \\
. & . & . & \alpha^{9} & . & \alpha^{11} & . & \alpha^{13} \\
. & . & . & \alpha^{8} & . & . & \alpha^{11} & \alpha^{12} \\
. & . & . & . & . & . & & \alpha^{11} \\
. & . & . & . & . & \alpha^{8} & \alpha^{9} & \alpha^{10} \\
. & . & . & . & . & . & . & \alpha^{9} \\
. & . & . & . & . & . & . & \alpha^{8} \\
. & . & . & . & . & . & . & .
\end{pmatrix}
\cdot
\begin{pmatrix}
a_0 \\ a_1 \\ a_2 \\ a_3 \\ a_4 \\ a_5 \\ a_6 \\ a_7
\end{pmatrix}
=
\begin{pmatrix}
d_0 \\ d_1 \\ d_2 \\ d_3 \\ d_4 \\ d_5 \\ d_6 \\ d_7 \\ d_8 \\ d_9 \\ d_{10} \\ d_{11} \\ d_{12} \\ d_{13} \\ d_{14} \\ d_{15}
\end{pmatrix}
$$

Example: generator matrix of $\ker(M(\alpha))$

$n = 4$

$$\begin{pmatrix}
1 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\
\cdot & 1 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\
\cdot & \cdot & 1 & \cdot & \cdot & \cdot & \cdot & \cdot \\
\cdot & \cdot & \cdot & 1 & \cdot & \cdot & \cdot & \cdot \\
\cdot & \cdot & \cdot & \cdot & 1 & \cdot & \cdot & \cdot \\
\cdot & \cdot & \cdot & \cdot & \cdot & 1 & \cdot & \cdot \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 1 & \cdot \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 1 \\
\cdot & \alpha^8 & \alpha^9 & \alpha^{10} & \alpha^{11} & \alpha^{12} & \alpha^{13} & \alpha^{14} \\
\cdot & \cdot & \cdot & \alpha^9 & \cdot & \alpha^{11} & \cdot & \alpha^{13} \\
\cdot & \cdot & \cdot & \alpha^8 & \cdot & \cdot & \alpha^{11} & \alpha^{12} \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & & \alpha^{11} \\
\cdot & \cdot & \cdot & \cdot & \cdot & \alpha^8 & \alpha^9 & \alpha^{10} \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \alpha^9 \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \alpha^8 \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot
\end{pmatrix}
\cdot
\begin{pmatrix} a_0 \\ a_1 \\ a_2 \\ \cdot \\ a_4 \\ \cdot \\ \cdot \\ \cdot \end{pmatrix}
=
\begin{pmatrix} d_0 \\ d_1 \\ d_2 \\ \cdot \\ d_4 \\ \cdot \\ \cdot \\ \cdot \\ d_8 \\ \cdot \\ \cdot \\ \cdot \\ \cdot \\ \cdot \\ \cdot \\ \cdot \end{pmatrix}$$

Higher-order Derivative Functions (I)

Let $\alpha_0, \ldots, \alpha_{m-1} \in \mathbb{F}_{2^n}^*$ be $\mathbb{F}_2$-linearly independent

Theorem

$$\mathrm{Im}\left(\prod_{0 \le i \le m-1} M(\alpha_i)\right) = \bigcap_{0 \le i \le m-1} \ker(M(\alpha_i)).$$

Dimension $= 2^{n-m}$.

Higher-order Derivative Functions (I)

Let $\alpha_0, \dots, \alpha_{m-1} \in \mathbb{F}_{2^n}^*$ be $\mathbb{F}_2$-linearly independent

Theorem

$$\mathrm{Im}\left(\prod_{0\le i\le m-1} M(\alpha_i)\right) = \bigcap_{0\le i\le m-1} \ker(M(\alpha_i)).$$

Dimension $= 2^{n-m}$.

Let $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$.
There is a function $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ such that

$\Delta_{\alpha_0,\dots,\alpha_{m-1}} F(x) = f(x)$ **if and only if** $\Delta_{\alpha_i} f(x) = 0,\ 0 \le i \le m-1.$

($\Rightarrow$ **easy**, $\Leftarrow$ **not easy**)

Sketch of proof (I)

$\mathrm{Im}\left(\prod_{0\leq i\leq m-1} M(\alpha_i)\right) = \bigcap_{0\leq i\leq m-1} \ker(M(\alpha_i))$

By induction:

We have

$$\mathrm{Im}\,(M(\alpha_0)M(\alpha_1)) = \{M(\alpha_0)\nu \mid \nu \in \mathrm{Im}(M(\alpha_1))\} = \mathrm{Im}(M(\alpha_0)_{|\mathrm{Im}(M(\alpha_1))}),$$

and $M(\alpha_0)$ **commutes** with $M(\alpha_1)$, so

$$\mathrm{Im}(M(\alpha_0)_{|\mathrm{Im}(M(\alpha_1))}) = \mathrm{Im}(M(\alpha_1)_{|\mathrm{Im}(M(\alpha_0))}) \subset \mathrm{Im}(M(\alpha_1)).$$

Thus,

$$\begin{aligned}\mathrm{Im}(M(\alpha_0)_{|\mathrm{Im}(M(\alpha_1))}) &= \ker(M(\alpha_0)_{|\mathrm{Im}(M(\alpha_1))}) \\ &= \ker(M(\alpha_0)) \cap \mathrm{Im}(M(\alpha_1)) \\ &= \ker(M(\alpha_0)) \cap \ker(M(\alpha_1)).\end{aligned}$$

Sketch of proof (II)

$\mathrm{Im}\left(\prod_{0\leq i\leq m-1} M(\alpha_i)\right) = \bigcap_{0\leq i\leq m-1} \ker(M(\alpha_i))$

Lemma

$$\dim(\ker(H\cdot G)) = \dim(\ker(H)) + \dim(\ker(H)\cap \mathrm{Im}(G)).$$

By induction:

$$\dim\left(\ker\left(\prod_{i=1}^{m} M(\alpha_i)\right)\right) = \sum_{k=1}^{m}\dim\left(\bigcap_{i=1}^{k}\ker(M(\alpha_i))\right).$$

With the **rank-nullity Theorem**, we have:

$$\dim\left(\ker\left(\prod_{i=1}^{m} M(\alpha_i)\right)\right) + \dim\left(\mathrm{Im}\left(\prod_{i=1}^{m} M(\alpha_i)\right)\right) = 2^n$$

Sketch of proof (II)

$\mathrm{Im}\left(\prod_{0\le i\le m-1} M(\alpha_i)\right) = \bigcap_{0\le i\le m-1} \ker(M(\alpha_i))$

Lemma

$$\dim(\ker(H\cdot G)) = \dim(\ker(H)) + \dim(\ker(H)\cap \mathrm{Im}(G)).$$

By induction:

$$\dim\left(\ker\left(\prod_{i=1}^{m} M(\alpha_i)\right)\right) = \sum_{k=1}^{m}\dim\left(\bigcap_{i=1}^{k}\ker(M(\alpha_i))\right).$$

With the **rank-nullity Theorem**, we have:

$$\sum_{k=1}^{m}\dim\left(\bigcap_{i=1}^{k}\ker(M(\alpha_i))\right) + \dim\left(\bigcap_{i=1}^{m}\ker(M(\alpha_i))\right) = 2^n$$

Sketch of proof (II)

$\mathrm{Im}\left(\prod_{0\leq i\leq m-1} M(\alpha_i)\right) = \bigcap_{0\leq i\leq m-1} \ker(M(\alpha_i))$

Lemma

$$\dim(\ker(H \cdot G)) = \dim(\ker(H)) + \dim(\ker(H) \cap \mathrm{Im}(G)).$$

By induction:

$$\dim\left(\ker\left(\prod_{i=1}^{m} M(\alpha_i)\right)\right) = \sum_{k=1}^{m} \dim\left(\bigcap_{i=1}^{k} \ker(M(\alpha_i))\right).$$

With the **rank-nullity Theorem**, we have:

$$\sum_{k=1}^{m} \dim\left(\bigcap_{i=1}^{k} \ker(M(\alpha_i))\right) = 2^n - 2^{n-m} \Rightarrow \dim\left(\bigcap_{i=1}^{m} \ker(M(\alpha_i))\right) = 2^{n-m}$$

(reminder: $\dim(\ker(M(\alpha))) = 2^{n-1}$)

Higher-order Derivative Functions (II)

Let $\alpha_0, \ldots, \alpha_{m-1} \in \mathbb{F}_{2^n}^*$ be $\mathbb{F}_2$-linearly independent

Theorem

$$\ker\left(\prod_{0\le i\le m-1} M(\alpha_i)\right) = \sum_{0\le i\le m-1} \ker(M(\alpha_i)).$$

Dimension $= 2^n - 2^{n-m}$.

Higher-order Derivative Functions (II)

Let $\alpha_0, \ldots, \alpha_{m-1} \in \mathbb{F}_{2^n}^*$ be $\mathbb{F}_2$-linearly independent

Theorem

$$\ker\left(\prod_{0\leq i\leq m-1} M(\alpha_i)\right) = \sum_{0\leq i\leq m-1} \ker(M(\alpha_i)).$$

Dimension $= 2^n - 2^{n-m}$.

Let $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$. Then,

$\Delta_{\alpha_0,\ldots,\alpha_{m-1}} F(x) = 0$ **if and only if** $F(x) = F_0(x) + \cdots + F_{m-1}(x)$,

where $\Delta_{\alpha_i} F_i(x) = 0$, $0 \leq i \leq m-1$.
($\Leftarrow$ **easy**, $\Rightarrow$ **not easy**)

Sketch of proof (I)

$\ker\left(\prod_{0\leq i\leq m-1} M(\alpha_i)\right) = \sum_{0\leq i\leq m-1} \ker(M(\alpha_i))$

We have $$\ker\left(\prod_{0\leq i\leq m-1} M(\alpha_i)\right) \supseteq \sum_{0\leq i\leq m-1} \ker(M(\alpha_i))$$ **and**

$$\dim\left(\ker\left(\prod_{i=1}^{m} M(\alpha_i)\right)\right) = 2^n - 2^{n-m}.$$

Also, for any $\beta \in \mathbb{F}_{2^n}$ $\mathbb{F}_2$-**linearly independent** from the α_i's,

$$M(\beta)\left(\sum_{1\leq i\leq m} M(\alpha_i)\right) = \sum_{1\leq i\leq m} (M(\alpha_i)M(\beta))$$

$$\Downarrow$$

$$\ker(M(\beta)) \cap \left(\sum_{1\leq i\leq m} \ker(M(\alpha_i))\right) = \sum_{1\leq i\leq m} \left(\ker(M(\alpha_i)) \cap \ker(M(\beta))\right).$$

Sketch of proof (II)

Inclusion-Exclusion principle

Proposition[Inclusion-Exclusion]

$$\dim\left(\sum_{i=1}^{m}\ker(M(\alpha_i))\right)$$

$$=\sum_{k=1}^{m}(-1)^{k+1}\left(\sum_{1\leq i_1\leq\cdots\leq i_k\leq m}\dim\left(\ker(M(\alpha_{i_1}))\cap\cdots\cap\ker(M(\alpha_{i_k}))\right)\right)$$

Sketch of proof (II)

Inclusion-Exclusion principle

Proposition[Inclusion-Exclusion]

$$\dim\left(\sum_{i=1}^{m}\ker(M(\alpha_i))\right)$$

$$=\sum_{k=1}^{m}(-1)^{k+1}\left(\sum_{1\le i_1\le\cdots\le i_k\le m}\dim\left(\ker(M(\alpha_{i_1}))\cap\cdots\cap\ker(M(\alpha_{i_k}))\right)\right)$$

Hence,

$$\dim\left(\sum_{1\le i\le m}\ker(M(\alpha_i))\right)=\sum_{1\le k\le m}(-1)^{k+1}\binom{m}{k}2^{n-k}$$

$$=2^n-2^{n-m}$$ **by induction** on m.

Sketch of proof (II)

Inclusion-Exclusion principle

Proposition[Inclusion-Exclusion]

$$\dim\left(\sum_{i=1}^{m}\ker(M(\alpha_i))\right)$$

$$=\sum_{k=1}^{m}(-1)^{k+1}\left(\sum_{1\le i_1\le\cdots\le i_k\le m}\dim\left(\ker(M(\alpha_{i_1}))\cap\cdots\cap\ker(M(\alpha_{i_k}))\right)\right)$$

Hence,

$$\dim\left(\sum_{1\le i\le m}\ker(M(\alpha_i))\right)=\sum_{1\le k\le m}(-1)^{k+1}\binom{m}{k}2^{n-k}$$

$$=2^n-2^{n-m}$$ **by induction** on m.

Thus $\ker\left(\prod_{0\le i\le m-1}M(\alpha_i)\right)\supseteq\sum_{0\le i\le m-1}\ker(M(\alpha_i))$

Sketch of proof (II)

Inclusion-Exclusion principle

Proposition[Inclusion-Exclusion]

$$\dim\left(\sum_{i=1}^{m} \ker(M(\alpha_i))\right)$$

$$= \sum_{k=1}^{m} (-1)^{k+1} \left(\sum_{1 \le i_1 \le \cdots \le i_k \le m} \dim\left(\ker(M(\alpha_{i_1})) \cap \cdots \cap \ker(M(\alpha_{i_k}))\right)\right)$$

Hence,

$$\dim\left(\sum_{1\le i\le m} \ker(M(\alpha_i))\right) = \sum_{1\le k\le m} (-1)^{k+1} \binom{m}{k} 2^{n-k}$$

$$= 2^n - 2^{n-m}$$ **by induction** on m.

Thus $\ker\left(\prod_{0\le i\le m-1} M(\alpha_i)\right) = \sum_{0\le i\le m-1} \ker(M(\alpha_i))$

Antiderivatives

Theorem

Let $\alpha_0, \ldots, \alpha_{m-1} \in \mathbb{F}_{2^n}^*$ be $\mathbb{F}_2$-*linearly independent*.
Let $f_i : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ be such that $\Delta_{\alpha_i} f_i(x) = 0$, $0 \le i \le m-1$. Then,

$$\exists F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n} \quad \text{such that} \quad \Delta_{\alpha_i} F(x) = f_i(x)$$

if and only if

$$\Delta_{\alpha_i} f_j(x) = \Delta_{\alpha_j} f_i(x),$$

for all $0 \le i, j \le m-1$.

Due to the **structure** of the $M(\alpha_i)$'s, it is possible to **build** efficiently $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ from a compatible set of functions f_i.

Algorithm

Antiderivative: $\{(f_i, \alpha_i) \mid 0 \leq i \leq m-1\}$ verifying conditions of consistency

1. $G \leftarrow$ generating matrix of $\ker(M(\alpha_0))$;
2. $sol \leftarrow 0_{\mathbb{F}_{2^n}^{2^n}}$;
3. $F_0 \leftarrow$ a solution of $M(\alpha_0) \cdot F_0 = f_0$;
4. **for** i **from** 1 **to** $m-1$ **do**:
5. $\quad F_i \leftarrow$ a solution of $M(\alpha_i) \cdot F_i = f_i$;
6. $\quad \kappa \leftarrow$ generating matrix of $\ker(M(\alpha_i)G)$;
7. $\quad tmp \leftarrow$ a solution of $M(\alpha_i)G \cdot tmp = M(\alpha_i) \cdot (F_0 + F_i + sol)$;
8. $\quad sol \leftarrow tmp$;
9. $\quad G \leftarrow G \cdot \kappa$;
10. **return** $sol + F_0$

A new equivalence

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

Definition $F \sim_V G$

F and G are said differentially equivalent w.r.t. a subspace $V \subseteq \mathbb{F}_{2^n}$ if

$$\Delta_v F(x) = \Delta_v G(x), \qquad \text{for all } v \in V.$$

Proposition

$$F \sim_V G \quad \Leftrightarrow \quad \texttt{coeffs}(F+G) \in \bigcap_{v \in V} \ker\left(M(v)\right)$$

Furthermore,

$$n - \dim(V) \geq \deg(F+G).$$

Differential equivalence is different from **CCZ**-equivalence!

Outline

Example

$z \in \mathbb{F}_{16},\ z^4 = z + 1$

$\alpha \backslash \beta$	.	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
.	16	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
1	.	.	.	2	.	2	.	2	2	.	2	2	2	.	2	.
2	.	.	2	.	.	2	.	6	2	2	.	.	.	.	2	.
3	.	.	4	2	.	.	.	4	.	.	2	.	.	4	.	.
4	.	.	.	.	.	2	2	2	2	2	4	.	.	.	.	2
5	.	4	2	.	2	.	2	.	2	.	.	2	2	.	.	.
6	.	2	.	.	2	4	2	.	.	.	.	2	.	2	.	2
7	2	2	.	2	.	.	4	.	.	2	.	2	.	.	.	2
8	.	.	.	.	.	.	.	.	6	2	.	.	4	.	4	.
9	.	2	2	.	2	.	2	.	.	2	.	2	2	2	.	.
10	2	2	.	.	2	.	2	.	.	2	2	2	.	.	.	2
11	.	.	.	2	.	.	.	2	2	.	2	.	2	.	4	2
12	.	.	.	2	2	2	.	2	2	2	2	.	.	.	.	2
13	.	4	.	2	.	.	.	.	.	.	2	4	.	4	.	.
14	.	.	2	2	2	.	2	2	.	.	2	.	.	.	2	.
15	2	.	4	.	2	.	2	.	.	.	.	2	2	.	.	2

Example

$z \in \mathbb{F}_{16},\ z^4 = z + 1$

$\alpha \backslash \beta$	.	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
.	16	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
1	.	.	.	2	.	2	.	2	2	.	2	2	2	.	2	.
3	.	.	4	2	.	.	.	4	.	.	2	.	.	4	.	.
4	.	.	.	.	.	2	2	2	2	2	4	.	.	.	.	2
5	.	4	2	.	2	.	2	.	2	.	.	2	2	.	.	.
6	.	2	.	.	2	4	2	.	.	.	.	2	.	2	.	2
7	2	2	.	2	.	.	4	.	.	2	.	2	.	.	.	2
9	.	2	2	.	2	.	2	.	.	2	.	2	2	2	.	.
10	2	2	.	.	2	.	2	.	.	2	2	2	.	.	.	2
11	.	.	.	2	.	.	.	2	2	.	2	.	2	.	4	2
12	.	.	.	2	2	2	.	2	2	2	2	.	.	.	.	2
13	.	4	.	2	.	.	.	.	.	.	2	4	.	4	.	.
14	.	.	2	2	2	.	2	2	.	.	2	.	.	.	2	.
15	2	.	4	.	2	.	2	.	.	.	.	2	2	.	.	2

Example

$z \in \mathbb{F}_{16},\ z^4 = z + 1$

$\alpha \backslash \beta$	.	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
.	16	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
1	.	.	.	2	.	2	.	2	2	.	2	2	2	.	2	.
3	.	.	4	2	.	.	.	4	.	.	2	.	.	4	.	.
4	.	.	.	.	.	2	2	2	2	2	4	.	.	.	.	2
5	.	4	2	.	2	.	2	.	2	.	.	2	2	.	.	.
6	.	2	.	.	2	4	2	.	.	.	.	2	.	2	.	2
7	2	2	.	2	.	.	4	.	.	2	.	2	.	.	.	2
9	.	2	2	.	2	.	2	.	.	2	.	2	2	2	.	.
10	2	2	.	.	2	.	2	.	.	2	2	2	.	.	.	2
11	.	.	.	2	.	.	.	2	2	.	2	.	2	.	4	2
12	.	.	.	2	2	2	.	2	2	2	2	.	.	.	.	2
13	.	4	.	2	.	.	.	.	.	.	2	4	.	4	.	.
14	.	.	2	2	2	.	2	2	.	.	2	.	.	.	2	.
15	2	.	4	.	2	.	2	.	.	.	.	2	2	.	.	2

Example

$z \in \mathbb{F}_{16},\ z^4 = z + 1$

$\alpha \backslash \beta$	.	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
.	16	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
1	.	.	.	2	.	2	.	2	2	.	2	2	2	.	2	.
4	.	.	.	.	.	2	2	2	2	2	4	.	.	.	.	2
5	.	4	2	.	2	.	2	.	2	.	.	2	2	.	.	.
6	.	2	.	.	2	4	2	.	.	.	.	2	.	2	.	2
7	2	2	.	2	.	.	4	.	.	2	.	2	.	.	.	2
9	.	2	2	.	2	.	2	.	.	2	.	2	2	2	.	.
10	2	2	.	.	2	.	2	.	.	2	2	2	.	.	.	2
11	.	.	.	2	.	.	.	2	2	.	2	.	2	.	4	2
12	.	.	.	2	2	2	.	2	2	2	2	.	.	.	.	2
13	.	4	.	2	.	.	.	.	.	.	2	4	.	4	.	.
14	.	.	2	2	2	.	2	2	.	.	2	.	.	.	2	.
15	2	.	4	.	2	.	2	.	.	.	.	2	2	.	.	2

Example $z \in \mathbb{F}_{16},\ z^4 = z + 1$

$$F(x) = z^{12}x^{15} + zx^{14} + z^{12}x^{13} + z^{12}x^{12} + z^{8}x^{11} + z^{14}x^{10} + x^{9} + x^{8} + z^{2}x^{7} + z^{5}x^{6} + z^{14}x^{5} + z^{4}x^{4} + z^{9}x^{3} + z^{4}x^{2} + x + z^{2}$$

Let $V = \{0, \mathbf{1}, \mathbf{z}, z^4\}$.

Example $z \in \mathbb{F}_{16},\ z^4 = z + 1$

$$F(x) = z^{12}x^{15} + zx^{14} + z^{12}x^{13} + z^{12}x^{12} + z^8x^{11} + z^{14}x^{10} + x^9 + x^8 + z^2x^7 + z^5x^6 + z^{14}x^5 + z^4x^4 + z^9x^3 + z^4x^2 + x + z^2$$

Let $V = \{0, \mathbf{1}, \mathbf{z}, z^4\}$. We want $G : \mathbb{F}_{16} \to \mathbb{F}_{16}$ such that:

$$F \sim_V G \qquad \text{and} \qquad \delta(G) < \delta(F) = 6.$$

Example

$z \in \mathbb{F}_{16},\ z^4 = z + 1$

$$F(x) = z^{12}x^{15} + zx^{14} + z^{12}x^{13} + z^{12}x^{12} + z^{8}x^{11} + z^{14}x^{10} + x^{9} + x^{8} + z^{2}x^{7} + z^{5}x^{6} + z^{14}x^{5} + z^{4}x^{4} + z^{9}x^{3} + z^{4}x^{2} + x + z^{2}$$

Let $V = \{0, \mathbf{1}, \mathbf{z}, z^4\}$. We want $G : \mathbb{F}_{16} \to \mathbb{F}_{16}$ such that:

$$F \sim_V G \qquad \text{and} \qquad \delta(G) < \delta(F) = 6.$$

We pick $h : \mathbb{F}_{16} \to \mathbb{F}_{16}$ with $\texttt{coeffs}(h) \in \ker(M(z^2)) \cap \ker(M(z^3))$.

Example $z \in \mathbb{F}_{16},\ z^4 = z + 1$

$$F(x) = z^{12}x^{15} + zx^{14} + z^{12}x^{13} + z^{12}x^{12} + z^{8}x^{11} + z^{14}x^{10} + x^{9} + x^{8} + z^{2}x^{7} + z^{5}x^{6} + z^{14}x^{5} + z^{4}x^{4} + z^{9}x^{3} + z^{4}x^{2} + x + z^{2}$$

Let $V = \left\{0, \mathbf{1}, \mathbf{z}, z^4\right\}$. We want $G : \mathbb{F}_{16} \to \mathbb{F}_{16}$ such that:

$$F \sim_V G \qquad \text{and} \qquad \delta(G) < \delta(F) = 6.$$

We pick $h : \mathbb{F}_{16} \to \mathbb{F}_{16}$ with $\texttt{coeffs}(h) \in \ker(M(z^2)) \cap \ker(M(z^3))$.

For instance:

$$\texttt{coeffs}(h) = (z^{10}, z^{13}, z^{7}, z^{12}, z^{3}, z^{7}, z^{2}, 0, z^{11}, z^{2}, z^{7}, 0, z^{12}, 0, 0, 0)$$

$$\delta(F + h) = 4$$

Example

$F : \mathbb{F}_{16} \to \mathbb{F}_{16}$

$\alpha \backslash \beta$	.	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
.	16	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
1	.	.	.	2	.	2	.	2	2	.	2	2	2	.	2	.
2	.	.	2	.	.	2	.	6	2	2	.	.	.	.	2	.
3	.	.	4	2	.	.	.	4	.	.	2	.	.	4	.	.
4	.	.	.	.	.	2	2	2	2	2	4	.	.	.	.	2
5	.	4	2	.	2	.	2	.	2	.	.	2	2	.	.	.
6	.	2	.	.	2	4	2	.	.	.	.	2	.	2	.	2
7	2	2	.	2	.	.	4	.	.	2	.	2	.	.	.	2
8	.	.	.	.	.	.	.	.	6	2	.	.	4	.	4	.
9	.	2	2	.	2	.	2	.	.	2	.	2	2	2	.	.
10	2	2	.	.	2	.	2	.	.	2	2	2	.	.	.	2
11	.	.	.	2	.	.	.	2	2	.	2	.	2	.	4	2
12	.	.	.	2	2	2	.	2	2	2	2	.	.	.	.	2
13	.	4	.	2	.	.	.	.	.	.	2	4	.	4	.	.
14	.	.	2	2	2	.	2	2	.	.	2	.	.	.	2	.
15	2	.	4	.	2	.	2	.	.	.	.	2	2	.	.	2

Example $F + h : \mathbb{F}_{16} \to \mathbb{F}_{16}$

$\alpha \backslash \beta$	.	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
.	16	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
1	.	.	.	2	.	2	.	2	2	.	2	2	2	.	2	.
2	.	.	.	.	2	.	.	2	2	2	2	**4**	2	.	.	.
3	.	.	.	2	2	.	2	2	2	.	2	2	2	.	.	.
4	.	.	.	.	.	2	2	2	2	2	**4**	.	.	.	.	2
5	2	2	.	.	.	2	**4**	2	.	.	.	.	.	.	.	**4**
6	2	.	.	2	.	.	2	**4**	2	.	.	.	2	.	.	2
7	2	.	2	2	.	.	.	.	.	.	.	.	2	2	**4**	2
8	2	.	2	.	.	.	2	**4**	.	**4**	2	.	.	.	.	.
9	2	.	2	.	.	.	2	.	.	2	2	2	.	2	2	.
10	2	**4**	2	.	.	.	2	.	2	.	.	.	2	2	.	.
11	.	2	2	.	2	.	.	.	2	2	2	.	2	2	.	.
12	.	.	.	.	2	2	2	2	.	2	2	**4**	.	.	.	.
13	2	.	2	2	2	.	.	2	2	.	.	.	2	.	.	2
14	2	.	.	2	.	.	.	2	.	2	2	.	**4**	.	.	2
15	2	.	**4**	.	2	.	2	.	.	.	.	2	2	.	.	2

Correspondence with previous works

Proposition

A function is quadratic **if and only if** all its derivatives are affines.

1. **Choose** 2-to-1 affine derivatives that are **compatible**
2. **Verify** that the $\mathbb{F}_2$-linear combinations are **again** 2-to-1
3. **Apply** the **algorithm** to find a quadratic APN function

G. Weng, Y. Tan and G. Gong,
On Quadratic Almost Perfect Nonlinear Functions and their Related Algebraic Object,
WCC 2013.

Y. Yu, M. Wang and Y. Li,
A matrix approach for constructing quadratic APN functions,
WCC 2013.

Outline

Perspectives and open problems

- **Characterize** 2-to-1 functions/derivatives;
- **Understand** when the sum of two of them is again 2-to-1;
- **How many** APN functions in a same differential coset?
- Is it possible to **preserve** bijectivity?
- What are the **possible shapes** for DDT of APN functions?
- Extend to $\mathbb{F}_{p^n}$, with p an odd prime.