$\mathbb{F}_{2^n} \longrightarrow \mathbb{F}_{2^n}$ Functions with Fast Points

Valentin SUDER
(Université Rouen Normandie, France)

The 14th International Conference on Finite Fields and their Applications
Fq14
Vancouver, June 7 2019

Outline

Notations

Finite Field: $\mathbb{F}_{2^n}$ **Vector Space**: $\mathbb{F}_2^n$

Basis: $\langle \beta_1, \beta_2, \ldots, \beta_n \rangle$

$$\mathbb{F}_{2^n} \ni \mu = \mu_1\beta_1 + \mu_2\beta_2 + \cdots + \mu_n\beta_n = (\mu_1, \mu_2, \ldots, \mu_n) \in \mathbb{F}_2^n$$

$$\begin{array}{rccl} F: & \mathbb{F}_{2^n} & \to & \mathbb{F}_{2^n} \\ & x & \mapsto & F(x) \\ & & & = \sum_{i=0}^{2^n-1} c_i x^i \end{array}$$

$$\begin{array}{rccl} F: & \mathbb{F}_2^n & \to & \mathbb{F}_2^n \\ & x = (x_1, \ldots, x_n) & \mapsto & (f_1(x), \ldots, f_n(x)) \end{array}$$

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

$$f_i(x_1, \ldots, x_n) = \mathtt{Tr}(\beta_i^* F(x))$$

Dual Basis: $\langle \beta_1^*, \ldots, \beta_n^* \rangle$ if $\mathtt{Tr}(\beta_i \beta_j^*) = \delta_{i,j}$

Algebraic Degree:

$$\deg(F) = \max\{\mathtt{hw}(i) \mid c_i \neq 0\}$$

$$\deg(F) = \max\{\deg(f_i)\}$$

Differentiation

Let $F, G : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$, $\alpha, \alpha' \in \mathbb{F}_{2^n}^*$, $V = \langle \beta_1, \ldots, \beta_k \rangle$

Discrete Derivatives

$$\begin{array}{rccc} \Delta_\alpha F & : & \mathbb{F}_{2^n} & \to & \mathbb{F}_{2^n} \\ & & x & \mapsto & F(x) + F(x+\alpha) \end{array}$$

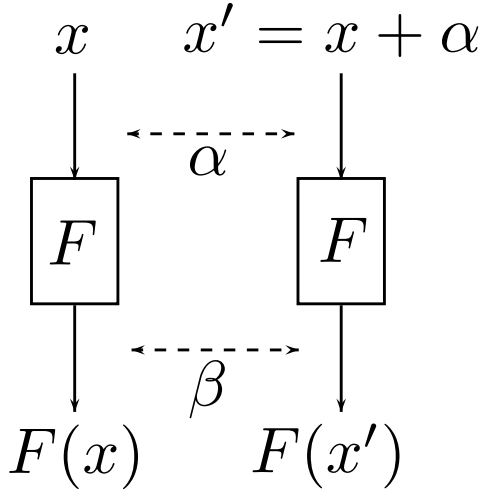
$$\Delta_V F(x) = \Delta_{\beta_1,\ldots,\beta_k} F(x) = \Delta_{\beta_1} \Delta_{\ldots} \Delta_{\beta_k} F(x) = \sum_{v \in V} F(x+v)$$

- $\Delta_\alpha F(x) + \Delta_{\alpha'} F(x) = \Delta_{\alpha+\alpha'} F(x+\alpha)$
- $\Delta_\alpha (F+G)(x) = \Delta_\alpha F(x) + \Delta_\alpha G(x)$

$$\deg(\Delta_\alpha F) < \deg(F)$$

Differential Criteria

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



$$\begin{array}{rccl} \Delta_\alpha F : & \mathbb{F}_{2^n} & \to & \mathbb{F}_{2^n} \\ & x & \mapsto & F(x) + F(x+\alpha) \end{array}$$

Differential Uniformity [Nyberg 94]

$$\delta_F = \max_{\alpha \in \mathbb{F}_{2^n}^*, \beta \in \mathbb{F}_{2^n}} \#\{x \mid \Delta_\alpha F(x) = \beta\}$$

Whenever $\delta_F = 2$ (**minimal** value), the function F is said to be **APN** ('Almost Perfect Nonlinear').

Proposition: F is APN **if and only if**

$\Delta_{\alpha,\alpha'} F(x) = \Delta_\alpha F(x) + \Delta_\alpha F(x+\alpha') \neq 0$ for all $\alpha \neq \alpha' \in \mathbb{F}_{2^n}^*$, $x \in \mathbb{F}_{2^n}$.

Context

APN functions are (very) **useful** but (very) **rare**!

Useful: Cryptography, Coding Theory, Projective Geometry, etc...

Rare (Up to CCZ-equivalence): Mostly monomials or quadratics, (very) few are bijectives (n even, only one for $n = 6$)

CCZ-Equivalence (preserves the differential uniformity)

$F \sim_{CCZ} G$ **if and only if** there is $\mathcal{A}$ an affine permutation such that

$$\{(u, F(u)) \mid u \in \mathbb{F}_{2^n}\} = \{\mathcal{A}(u, G(u)) \mid u \in \mathbb{F}_{2^n}\}$$

Challenges

Big APN Problem:

Find a bijective APN function for $n > 6$ **even**.

K. A. Browning, J. F. Dillon, M. T. McQuistan and A. J. Wolfe,
An APN Permutation in Dimension Six,
Fq9 (Selected Papers), Contemporary Mathematics, 2010.

Plan of action:

- Construct **new** (CCZ-**in**equivalent) APN functions.
- Check if they are **CCZ-equivalent** to a bijection.

A. Canteaut and L. Perrin,
On CCZ-Equivalence, Extended-Affine Equivalence, and Function Twisting,
Finite Fields and their Applications 26, March 2019.

Outline

Definitions

Fast Point

A Fast Point for a Boolean function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ is a **direction** $\alpha \in \mathbb{F}_2^n \backslash \{0\}$ such that

$$\deg(\Delta_\alpha f(x)) < \deg(f) - 1.$$

M. Duan and X. Lai,
Higher order differential cryptanalysis framework and its applications,
ICIST, 2011.

Faster Point

A Fast Point of order ℓ for a Boolean function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ is a **direction** $\alpha \in \mathbb{F}_2^n \backslash \{0\}$ such that

$$\deg(\Delta_\alpha f(x)) = \deg(f) - \ell.$$

A. Sălăgean and F.Özbudak,
Counting Boolean Functions with Faster Points,
WCC, 2019.

Higher order differential cryptanalyses

L. R. Knudsen,
Truncated and Higher-order Differentials,
Fast Software Encryption, 1994.

M. Vielhaber,
Breaking one.fivium by aida an algebraic iv differential attack,
https://eprint.iacr.org/2007/413, 2007.

I. Dinur and A. Shamir,
Cube attacks on tweakable black box polynomials,
EUROCRYPT, 2009.

Definition

Fast Point

A Fast Point for a **Vectorial** Boolean function $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ is a **direction** $\alpha \in \mathbb{F}_2^n \backslash \{0\}$ such that

$$\deg(\Delta_\alpha F(x)) < \deg(F) - 1.$$

Set of Fast Points

$$\mathbb{FP}_F = \{\alpha \in \mathbb{F}_2^n \mid \deg(\Delta_\alpha F) < \deg(F) - 1\} \cup \{0\}$$

Proposition: $\mathbb{FP}_F$ is a (proper) subspace of $\mathbb{F}_2^n$.

(as for Boolean functions)

Characterization

Theorem

Any (nonzero) $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ such that $\mathbb{FP}_F \neq \{0\}$ can be written as

$$F(x) = G(x) + H(x)$$

where $G, H : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ such that:

1. $\deg(H) < \deg(G) = \deg(F)$
2. $\deg(H) = \min\{\deg(\Delta_\alpha F) \mid \alpha \in \mathbb{F}_{2^n}^*\} + 1$
3. $\mathbb{FP}_G = \mathbb{FP}_F$ and $\mathbb{FP}_H \cap \mathbb{FP}_F = \{0\}$
4. $\Delta_v G(x) = 0, \ \forall v \in V$ for some $\{0\} \subset V \subseteq \mathbb{FP}_F$

Proposition: $\deg(F) \leq n - \dim(\mathbb{FP}_F)$

(as for Boolean functions)

An example

Let's build a function $F : \mathbb{F}_{2^8} \to \mathbb{F}_{2^8}$ with $\deg(F) = 4$ and with some **affine** and **quadratic** derivatives.
Let $\mathbb{F}_{2^8}^* = \langle z \rangle$,

$$F(x) = \Delta_{1,z,z^2}\left(\left(x^{255} + (x + z^3)^{255}\right) + x^{63}\right) + x^3$$

Now, $\alpha \neq 0$,

$$\deg(\Delta_\alpha F) = \begin{cases} 1 & \text{when } \alpha \in \langle 1, z, z^2 \rangle, \\ 2 & \text{when } \alpha \in z^3 + \langle 1, z, z^2 \rangle \\ 3 & \text{otherwise.} \end{cases}$$

But Why?

Quadratic APN functions are still "manageable".

What if we had an APN function for which *most* (but not all) *of* the derivatives were **affine**?

Example of an APN function with Fast Points

Y. Edel and A. Pott,

A New Almost Perfect Nonlinear Function Which is not Quadratic,

Adv. in Math. of Comm. 3(1), 2009.

Theorem [Edel-Pott 09]

Let $\mathbb{F}_{2^6}^* = \langle z \rangle$, the $\mathbb{F}_{2^6} \to \mathbb{F}_{2^6}$ function

$$E(x) = x^3 + z^{17}(x^{17} + x^{18} + x^{20} + x^{24}) + z^{14}\mathtt{Tr}(z^{52}x^3 + z^6x^5 + z^{19}x^7 + z^{28}x^{11} + z^2x^{13} + z^2x^9 + x^{21})$$

is APN, is cubic and CCZ-**in**equivalent to a quadratic.

$\Delta_v E(x)$ is **affine** for any $v \in$

$$\left\{ \begin{array}{llll} 1+ & z^2 & & z^5, \\ & z^2+ & z^3+ & \\ & & z^4 & \\ 1+ & z^2+ & z^4 & \\ 1+ & & z^3+ & z^5, \\ 1+ & & z^3+ & z^4+ \quad z^5, \\ & z^2+ & z^3+ & z^4+ \quad z^5 \end{array} \right\}$$

Outline

The Switching construction

$$E(x) = x^3 + z^{17}(x^{17} + x^{18} + x^{20} + x^{24}) + z^{14}\mathtt{Tr}(z^{52}x^3 + z^6x^5 + z^{19}x^7 + z^{28}x^{11} + z^2x^{13} + z^2x^9 + x^{21})$$

Idea: $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$, choose $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ and $u \in \mathbb{F}_{2^n}^*$ such that

$$F(x) + uf(x) \text{ has a } \textit{desirable} \text{ property .}$$

In our case: F is APN, we want

$$\Delta_{\alpha,\alpha'} f(x) = 0, \text{ for any } \alpha, \alpha', x \in \mathbb{F}_{2^n} \text{ such that } \Delta_{\alpha,\alpha'} F(x) = u.$$

Therefore $F(x) + uf(x)$ is APN.

(e.g. $x^3 + \mathtt{Tr}(x^9)$)

Now with Fast Points

$$E(x) = x^3 + z^{17}(x^{17} + x^{18} + x^{20} + x^{24}) + z^{14}\mathrm{Tr}(z^{52}x^3 + z^6x^5 + z^{19}x^7 + z^{28}x^{11} + z^2x^{13} + z^2x^9 + x^{21})$$

$\Delta_v E(x)$ is **affine** for any $v \in V =$

$$\left\{ \begin{array}{llll} 1+ & z^2 & & z^5, \\ & z^2+ & z^3+ & \\ & & z^4 & , \\ 1+ & z^2+ & z^4 & , \\ 1+ & & z^3+ & z^5, \\ 1+ & & z^3+ & z^4+ \quad z^5, \\ & z^2+ & z^3+ & z^4+ \quad z^5 \end{array} \right\}$$

We can thus write

$$E(x) = C(x) + Q(x) \quad (= \Delta_V G(x) + Q(x)),$$

where $\deg(C) = 3$ and $\deg(Q) = 2$.

Remark 1: Q is not APN.

Remark 2: $\Delta_v Q(x)$ for $v \in V$ are not 2-to-1 (but others are).

Outline

With the same idea

$F(x) = C(x) + Q(x) \quad (= \Delta_V G(x) + Q(x))$

Let $Q : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ be a quadratic APN.
Let $\mathbb{F}_{2^n} = V \oplus W$

$$\deg(C) = 3$$

$F(x) = C(x) + Q(x)$ is APN **if and only if**
for all $\omega \neq \omega' \in W \backslash \{0\}$ and for all $x \in \mathbb{F}_{2^n}$

$$\Delta_{\omega,\omega'} C(x) \notin \left\{ \Delta_{\omega+v,\omega'+v'} Q \mid v, v' \in V \right\}$$

Constructing the system

$C(x) = \Delta_V G(x)$ and $\dim(V) = n - 3$ and $\mathbb{F}_{2^n} = V \oplus W$

For all $\omega \neq \omega' \in W \backslash \{0\}$

$$\Delta_{\omega,\omega'} C(x) = \gamma \mathrm{Tr}(\mu x) + c_{\omega,\omega'},$$

where $\gamma = \Delta_W C(x)$ and $\mu = \omega''^*$ when $W = \langle \omega, \omega', \omega'' \rangle$.

$F(x) = C(x) + Q(x)$ is APN **if and only if**
for all $\omega \neq \omega' \in W \backslash \{0\}$ and for all $x \in \mathbb{F}_{2^n}$

$$c_{\omega,\omega'}, c_{\omega,\omega'} + \gamma \notin \left\{ \Delta_{\omega+v,\omega'+v'} Q \mid v, v' \in V \right\}$$

Algorithm

- **Choose** $Q : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ a quadratic APN
- **Choose** $V \oplus W = \mathbb{F}_{2^n}$ with $\dim(V) = n - 3$
- For all (7 possibilities) $\omega \neq \omega' \in W \backslash \{0\}$, **compute** the sets

$$S_{\omega,\omega'} = \mathbb{F}_{2^n} \backslash \left\{ \Delta_{\omega+v,\omega'+v'} Q \mid v, v' \in V \right\}$$

- **Find** (actually only 3 of them, linearly independent)

$$c_{\omega,\omega'} \in S_{\omega,\omega'}$$

so that there is $\gamma \in \mathbb{F}_{2^n}^*$ such that

$$c_{\omega,\omega'} + \gamma \in S_{\omega,\omega'}$$

- **Recover** $C : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ from

$$\Delta_{\omega,\omega'} C(x) = \gamma \mathrm{Tr}(\mu x) + c_{\omega,\omega'}$$

V. S,
Antiderivative Functions over $\mathbb{F}_{2^n}$,
DCC (82), 2017.

$$\Rightarrow \quad F(x) = C(x) + Q(x) \text{ is a } \textbf{cubic } \textbf{APN}.$$

Observation after some Computation

$n = 6$

- Not all the quadratic APN functions can be **extended** to a cubic one (by this method)

Observation after some Computation

$n = 6$

- Not all the quadratic APN functions can be **extended** to a cubic one (by this method)
- All the cubic APN functions found were CCZ-**in**equivalent to a quadratic, but...

Observation after some Computation

$n = 6$

- Not all the quadratic APN functions can be **extended** to a cubic one (by this method)
- All the cubic APN functions found were CCZ-**in**equivalent to a quadratic, but...
- ...There were also all CCZ-equivalent to the **Edel-Pott** function!

Outline

Closing Remarks

- What's the *clever* choice for $V \oplus W = \mathbb{F}_{2^n}$?
- $\deg(C) = 3$ and $\dim(W) = 4$?
- $\deg(C) = 4$ (and still $\deg(H) = 2$)?