Low c-differential uniformity for functions modified on subfields

Marco Calderini
Joint work with: D. Bartoli, C. Riera, P. Stănică

University of Bergen

BFA 2021, Rosendal

Preliminaries

- $\mathbb{F}_{p^n}$ is the finite field with p^n elements.
- Vectorial p-ary (n, m)-functions: $f : \mathbb{F}_{p^n} \to \mathbb{F}_{p^m}$
- (n, n)-function f can be represented uniquely as univariate polynomial of degree at most $p^n - 1$
$$\sum_{i=0}^{p^n-1} a_i x^i.$$
- the **algebraic degree** of f is the largest p-weight of the exponent i, such that $a_i \neq 0$.

Differential uniformity

- Let $f : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$. The function $D_a f(x) = f(x+a) - f(x)$ is called the **derivative** of f in the direction a.
- Let $\Delta_f(a,b) = \#\{x : D_a f(x) = b\}$. The **differential uniformity** f is defined as
$$\delta_f = \max_{a \in \mathbb{F}^\star_{p^n}, b \in \mathbb{F}_{p^n}} \Delta_f(a,b).$$
- Let $\delta = \delta_f$, f is said differentially δ-uniform.

Optimal functions

- f is called **Perfect Nonlinear** (PN) iff $\delta = 1$. (No PN functions in even characteristic)
- f is called **Almost Perfect Nonlinear** (APN) iff $\delta = 2$.

APN functions have the smallest possible differential uniformity for $p = 2$. Indeed, if x is a solution to $f(x + a) - f(x) = b$, so it is $x + a$.

4-uniform bijections

Table: Primarily-constructed differentially 4-uniform over $\mathbb{F}_{2^n}$ (n even) with the best known nonlinearity

Name	F(x)	**deg**	**Conditions**
Gold	x^{2^i+1}	2	$n = 2k,\ k$ odd $\gcd(i, n) = 2$
Kasami	$x^{2^{2i}-2^i+1}$	i+1	$n = 2k,\ k$ odd $\gcd(i, n) = 2$
Inverse	x^{2^n-2}	$n-1$	$n = 2k,\ k \geq 1$
Bracken-Leander	$x^{2^{2k}+2^k+1}$	3	$n = 4k,\ k$ odd
Bracken-Tan-Tan	$\zeta x^{2^i+1} + \zeta^{2^m} x^{2^{-m}+2^{m+i}}$	2	$n = 3m,\ m$ even, $m/2$ odd, $\gcd(n, i) = 2,\ 3 \mid m + i$ and ζ is a primitive element of $\mathbb{F}_{2^n}$

Modifying the inverse function on a subfield

In the recent years, several classes of differentially 4-uniform permutations have been constructed by modifying the inverse function. Some of these are based on modifying the inverse function on a subfield.

Theorem (Sin, K. Kim, R. Kim, Han 2020)

Let $n = sm$ with s even and m odd. Let $f(x)$ be a differentially 4-uniform function over $\mathbb{F}_{2^s}$. Then,

$$F(x) = f(x) + (f(x) + g(x))(x^{2^s} + x)^{2^n - 1} = \begin{cases} f(x) & \text{if } x \in \mathbb{F}_{2^s} \\ x^{-1} & \text{if } x \notin \mathbb{F}_{2^s} \end{cases}$$

is differentially 4-uniform over $\mathbb{F}_{2^n}$.

Modifying other functions on a subfield

Proposition (C. 2021)

Let $n = sm$. Let f be an APN function over $\mathbb{F}_{2^s}$ and $g \in \mathbb{F}_{2^s}[x]$ an APN function over $\mathbb{F}_{2^n}$. Then, the function

$$F(x) = f(x) + (f(x) + g(x))(x^{2^s} + x)^{2^n-1} = \begin{cases} f(x) & \text{if } x \in \mathbb{F}_{2^s} \\ g(x) & \text{if } x \notin \mathbb{F}_{2^s} \end{cases}$$

is a differentially 4-uniform mapping.

Theorem (C. 2021)

Let $n = sm$ for some positive integers s and m. Let f and g be two polynomials with coefficients in $\mathbb{F}_{2^s}$, that is $f, g \in \mathbb{F}_{2^s}[x]$, and g permuting $\mathbb{F}_{2^n}$. Suppose that:

(H) *for any $a \in \mathbb{F}_{2^s}^\star$ and $b \in \mathbb{F}_{2^s}$ the equation $g(x) + g(x + a) = b$ has no solution in $\mathbb{F}_{2^n} \setminus \mathbb{F}_{2^s}$.*

Then, the function

$$F(x) = f(x) + (f(x) + g(x))(x^{2^s} + x)^{2^n - 1} = \begin{cases} f(x) & \text{if } x \in \mathbb{F}_{2^s} \\ g(x) & \text{if } x \notin \mathbb{F}_{2^s} \end{cases}$$

is such that

$$\Delta_F(a, b) \leq \begin{cases} \max\{\delta_f, \delta_g\} & \text{if } a \in \mathbb{F}_{2^s} \\ \delta_g + 2 & \text{if } a \notin \mathbb{F}_{2^s}. \end{cases}$$

Gold and Bracken-Leander functions case

Corollary

Let $n = sm$ with s even such that $s/2$ and m are odd. Let k be such that $\gcd(k, n) = 2$ *and* $f \in \mathbb{F}_{2^s}[x]$ *with* $f \sim_{Aff} x^{-1}$*. Then*

$$F(x) = f(x) + (f(x) + x^{2^k+1})(x^{2^s} + x)^{2^n-1} = \begin{cases} f(x) & \text{if } x \in \mathbb{F}_{2^s} \\ x^{2^k+1} & \text{if } x \notin \mathbb{F}_{2^s} \end{cases}$$

is a differentially 6-uniform permutation over $\mathbb{F}_{2^n}$*. Moreover, if* $s > 2$ *then the algebraic degree of* F *is* $n - 1$*.*

Gold and Bracken-Leander functions case

Corollary

Let $n = 4k = sm$ with k, m odd and s even. Let $f \in \mathbb{F}_{2^s}[x]$ with $f \sim_{Aff} x^{-1}$. Then

$$F(x) = f(x) + (f(x) + x^{2^{2k}+2^k+1})(x^{2^s} + x)^{2^n-1} = \begin{cases} f(x) & \text{if } x \in \mathbb{F}_{2^s} \\ x^{2^{2k}+2^k+1} & \text{if } x \notin \mathbb{F}_{2^s} \end{cases}$$

is a differentially 6-uniform permutation over $\mathbb{F}_{2^n}$. Moreover, if $s > 4$ then $\deg(F) = n - 1$.

Other Low uniform functions

When (H) is satisfied

Theorem (Carlet (2021))

Let $n = sm$*, with* m *odd, and let* $f \in \mathbb{F}_{2^s}[x]$ *be an APN function over* $\mathbb{F}_{2^n}$*. Then,* $f(x+a) + f(x) = b$ *does not admit solutions* $x \in \mathbb{F}_{2^n} \setminus \mathbb{F}_{2^s}$*, whenever* $a, b \in \mathbb{F}_{2^s}, a \neq 0$*.*

Theorem (Bartoli, C., Riera, Stănică)

Let $n = sm$*, where* s *and* m *are integers, and let* $f \in \mathbb{F}_{2^s}[x]$ *be a differentially* $2k$*-uniform function over* $\mathbb{F}_{2^n}$*. If* m *is not divisible by any integer* $2 \leq t \leq k$*, then* $f(x+a) + f(x) = b$ *does not admit solutions* $x \in \mathbb{F}_{2^n} \setminus \mathbb{F}_{2^s}$*, whenever* $a, b \in \mathbb{F}_{2^s}, a \neq 0$*.*

Other low uniform functions

Theorem (Bartoli, C., Riera, Stănică)

Let $n = sm$, with s even such that $s/2$ and m are odd. Let k be such that $\gcd(k,n) = 2$ *and let $f \in \mathbb{F}_{2^s}[x]$ with $f \sim_{Aff} x^{-1}$. Then*

$$F(x) = f(x) + (f(x) + x^{2^{2k}-2^k+1})(x^{2^s} + x)^{2^n-1} = \begin{cases} f(x) & \text{if } x \in \mathbb{F}_{2^s} \\ x^{2^{2k}-2^k+1} & \text{if } x \notin \mathbb{F}_{2^s} \end{cases}$$

is a differentially 6-uniform permutation over $\mathbb{F}_{2^n}$. Moreover, if $s > 2$ then the algebraic degree of F is $n-1$. Moreover, the nonlinearity of F is at least $2^{n-1} - 2^{\frac{s}{2}+1} - 2^{\frac{n}{2}}$.

c-differential uniformity

Introduced by Ellingsen, Felke, Riera, Stănică, Tkachenko (2020)

- Let $f : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$. The function ${}_cD_a f(x) = f(x+a) - cf(x)$ is called the c-derivative of f in the direction a.
- Let ${}_c\Delta_f(a,b) = \#\{x : {}_cD_a f(x) = b\}$. The c-**differential uniformity** f is defined as

$$\delta_{f,c} = \max_{a \in \mathbb{F}_{p^n}, b \in ff p^n} {}_c\Delta_f(a,b).$$

- $\delta = \delta_{f,c}$, f is said c-differentially δ-uniform.

c-differential uniformity (cont.)

- $\delta_{f,c} = 1$ f is called **Perfect c-Nonlinear** (PcN)
- $\delta_{f,c} = 2$ f is called **Almost Perfect c-Nonlinear** (APcN)

PcN functions have been also independently introduced by Bartoli and Timpanella with the name of β-planar functions.

Results on c-DU:

- power functions with low c-differential uniformity
- APcN and PcN functions constructed from the AGW criterion
- Characterization of quadratic APcN and PcN functions ($c \in \mathbb{F}_p \setminus \{1\}$)
- non existence results for exceptional APcN and PcN functions
- behaviour of c-DU under EA-equivalence
- c-boomerang uniformity
- ...

c-differential uniformity of piece-wise functions

Theorem (Stănică 2020)

Let $n = sm$. Given the Gold function $g(x) = x^{2^k+1}$ with $\gcd(n, k) = 1$, then, for any fixed $\alpha \in \mathbb{F}_{2^s}^{\star}$,

$$G(x) = \begin{cases} x^{2^k+1} + \alpha & \text{if } x \in \mathbb{F}_{2^s} \\ x^{2^k+1} & \text{if } x \notin \mathbb{F}_{2^s}, \end{cases}$$

is such that $\delta_{G,c} \leq 9$, for any $c \in \mathbb{F}_{2^n} \setminus \{1\}$.

Theorem (Bartoli, C., Riera, Stănică)

Let p is a prime, $n > 2$ be an integer, s be a divisor of n, $1 \neq c \in \mathbb{F}_{p^n}$ fixed, and $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ be a p-ary (n, n)-function defined by

$$F(x) = \begin{cases} f(x) & \text{if } x \in \mathbb{F}_{p^s} \\ g(x) & \text{if } x \notin \mathbb{F}_{p^s}, \end{cases}$$

where f is an (s, s)-function of c'-differential uniformity $\delta_{f,c'}$ (for all c') and $g \in \mathbb{F}_{p^n}[x]$ is an (n, n)-function of c'-differential uniformity $\delta_{g,c'}$ (for all c'). Then, the c-differential uniformity of F is

$$\delta_{F,c} \leq \begin{cases} \delta_{f,0} + \delta_{g,0}, & \text{if } c = 0, \\ \max\left\{\delta_{f,c_1} + \delta_{g,c}, \delta_{g,c} + 2p^s\delta_{g,0}\right\}, & \text{if } c \neq 0, \end{cases}$$

where $c = \sum_{i=1}^{m} c_i g_i$, with $c_i \in \mathbb{F}_{p^s}$ and $\{g_1 = 1, g_2, \ldots, g_m\}$ is a basis of the extension $\mathbb{F}_{p^n}$ over $\mathbb{F}_{p^s}$.

Remark

If $g \in \mathbb{F}_{p^s}[x]$, we have that for $c \neq 0$,

$$\delta_{F,c} \leq \max\left\{\delta_{f,c_1} + \delta_{g,c}, \delta_{g,c} + 2\delta_{g,c^{p^s-1}}\right\}.$$

For $g(x) = x^{2^k+1}$, with $\gcd(k,n) = 1$, we have $\delta_{g,c} \leq 3$ for all $c \in \mathbb{F}_{2^n}$. Therefore:

Theorem+Remark $\Rightarrow G(x) = x^{2^k+1} + \alpha + \alpha(x^{2^s} + x)^{2^n-1}$ is such that $\delta_{G,c} \leq 9$.

Theorem (Bartoli, C., Riera, Stănică)

Let p be a prime, $n > 2$ be an integer, s be a divisor of n, $1 \neq c \in \mathbb{F}_{p^s}$ fixed, and $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ be a p-ary (n, n)-function defined by

$$F(x) = \begin{cases} f(x) & \text{if } x \in \mathbb{F}_{p^s} \\ g(x) & \text{if } x \notin \mathbb{F}_{p^s}, \end{cases}$$

where f is an (s, s)-function of c-differential uniformity $\delta_{f,c}$ and $g \in \mathbb{F}_{p^s}[x]$ is an (n, n)-function of c-differential uniformity, $\delta_{g,c}$. Suppose that:

(H1) *for any $a \in \mathbb{F}_{p^s}^{\star}$ and $b \in \mathbb{F}_{p^s}$ the equation $g(x + a) - g(x) = b$ has no solution in $\mathbb{F}_{p^n} \setminus \mathbb{F}_{p^s}$.*

(H2) *for any $a \in \mathbb{F}_{p^s}$ and $b \in \mathbb{F}_{p^s}$ the equation $g(x + a) - cg(x) = b$ has no solution in $\mathbb{F}_{p^n} \setminus \mathbb{F}_{p^s}$.*

Then,

$${}_c\Delta_F(a, b) \leq \begin{cases} \max\{\delta_{f,c}, \delta_{g,c}\} & \text{if } a \in \mathbb{F}_{p^s} \\ \delta_{g,c} + 2 \cdot \delta_{g,0} & \text{if } a \notin \mathbb{F}_{p^s}, \end{cases}$$

Remark

We can note that if we remove condition (H2), we would obtain that

$$ {}_c\Delta_F(a,b) \leq \begin{cases} \delta_{f,c} + \delta_{g,c} & \text{if } a \in \mathbb{F}_{p^s} \\ \delta_{g,c} + 2 \cdot \delta_{g,0} & \text{if } a \notin \mathbb{F}_{p^s}. \end{cases} $$

Moreover, if g permutes $\mathbb{F}_{p^n}$ then we have also that $\delta_{g,0} = 1$.

Functions satisfying (H2)

Theorem (Bartoli, C., Riera, Stănică)

Let $n = sm$, where s and m are integers. Let $c \in \mathbb{F}_{p^s} \setminus \{1\}$ and let $f \in \mathbb{F}_{p^s}[x]$ be a c-differentially k-uniform function over $\mathbb{F}_{p^n}$. If m is not divisible by any integer $2 \leq t \leq k$, then $f(x+a) - cf(x) = b$ does not admit solutions $x \in \mathbb{F}_{p^n} \setminus \mathbb{F}_{p^s}$, whenever $a, b \in \mathbb{F}_{p^s}$.

Theorem (Bartoli, C., Riera, Stănică)

Let $n = sm$, with n/s odd. For a Gold-like function $g(x) = x^{2^k+1}$, with $\gcd(n, k) = t$ *such that* $\mathbb{F}_{2^t} \subset \mathbb{F}_{2^s}$*, and n/t odd. Then, for any fixed* $\alpha \in \mathbb{F}_{2^s}^\star$,

$$G(x) = \begin{cases} x^{2^k+1} + \alpha & \text{if } x \in \mathbb{F}_{2^s} \\ x^{2^k+1} & \text{if } x \notin \mathbb{F}_{2^s}, \end{cases}$$

is such that $\delta_{G,c} \leq 3$, for any $c \in \mathbb{F}_{2^t} \setminus \{1\}$.

Theorem (Bartoli, C., Riera, Stănică)

Let $n = sm$, with n odd. Given the Gold function $g(x) = x^{2^k+1}$ with $\gcd(n, k) = 1$, *then, for any fixed* $\alpha \in \mathbb{F}_{2^s}^\star$,

$$G(x) = \begin{cases} x^{2^k+1} + \alpha & \text{if } x \in \mathbb{F}_{2^s} \\ x^{2^k+1} & \text{if } x \notin \mathbb{F}_{2^s}, \end{cases}$$

is such that $\delta_{G,c} \le 6$, *for any* $c \in \mathbb{F}_{2^s} \setminus \{1\}$.
Moreover, if $3 \nmid m$ *we have* $\delta_{G,c} \le 5$.

Thanks for your attention!