On one way of constructing unbalanced TU-based permutations

Denis Fomin

HSE University

Definition 1

Walsh-Hadamard transform $W_S(a,b)$ of (n,m)-function S for $a \in \mathbb{F}_2^n$, $b \in \mathbb{F}_2^m$ is defined as follows:

$$W_S^{a,b} = \sum_{x \in \mathbb{F}_2^n} (-1)^{\langle a,x \rangle + \langle b,S(x) \rangle}.$$

Definition 2

The nonlinearity of (n,m)-function S is denote as N_S and defined as follows:

$$N_S = 2^{n-1} - \frac{1}{2} \max_{\substack{a \in \mathbb{F}_2^n, \\ b \in \mathbb{F}_2^m \setminus \theta}} \left| W_S^{a,b} \right|.$$

Definition 3

The algebraic degree (minimum degree) $\deg(S)$ of (n,m)-function S is the minimum degree among all the component functions of S: $\langle a, S(x)\rangle$, $a \in \mathbb{F}_2^m \backslash \theta$:

$$\deg(S) = \min_{a \in \mathbb{F}_2^m \backslash \theta} \deg\left(\langle a, S(x)\rangle\right).$$

Definition 4

The maximum degree of (n,m)-function S is the maximum degree among all the component functions of S: $\langle a, S(x)\rangle$, $a \in \mathbb{F}_2^m \backslash \theta$:

$$\deg_m(S) = \max_{a \in \mathbb{F}_2^m \backslash \theta} \deg\left(\langle a, S(x)\rangle\right).$$

Definition 5

For $a \in \mathbb{F}_2^n \backslash \theta, b \in \mathbb{F}_2^m$ let

$$\delta_S^{a,b} = |\{x \in \mathbb{F}_{2^n} | S(x+a) + S(x) = b\}|.$$

An (n,m)-function S is called differentially δ_S-uniform if

$$\delta_S = \max_{\substack{a \in \mathbb{F}_2^n \backslash \theta, \\ b \in \mathbb{F}_2^m}} \delta_S^{a,b}.$$

Consider the set $\mathcal{G}_k$ of $(n+m,1)$-functions $G(x_1,\ldots,x_n,y_1,\ldots,y_m)$, such that $\deg(G) \leq k$, $k \in \mathbb{N}$ and for each $\overline{x} \in \mathbb{F}_2^n$ if we substitute in place of each variable y_i, $i \in \overline{1,m}$, the value of the corresponding Boolean function $f_i(\overline{x})$, then the value of the function $G(x_1,\ldots,x_n,f_1(\overline{x}),\ldots,f_m(\overline{x}))$ is equals to 0:

$$\mathcal{G}_k = \{G(x_1,\ldots,x_n,y_1,\ldots,y_m)\colon G(x_1,\ldots,x_n,f_1(\overline{x}),\ldots,f_m(\overline{x})) = 0\ \forall \overline{x} \in \mathbb{F}_2^n\}.$$

The set $\mathcal{G}_k$ is a subgroup of the ring of polynomials of degree non above k. Let's denote r_F^k — the basis size of $\mathcal{G}_k$.

Definition 6

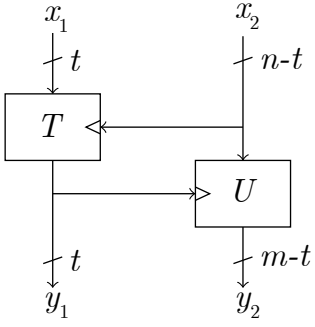
A minimum number k such that $r_F^k \neq 0$, is called graph algebraic immunity of F and denoted by $AI_{gr}(F)$.

Definition 7

Let F be an (n, m)-function, $1 \leq t \leq \min(n, m)$, $x_1,\ y_1 \in \mathbb{F}_2^t$, $x_2 \in \mathbb{F}_2^{n-t}$, $y_2 \in \mathbb{F}_2^{m-t}$, $x \in \mathbb{F}_2^n$, $x = x_1 \| x_2$, $y = y_1 \| y_2$, $T\,(x_1, x_2)$ is a (n, t) function such that if we fix value x_2 by any value from $\mathbb{F}_{2^{n-t}}$ then the function T is a bijection for value x_1, U is any $(n, m-t)$-function. Then if the function F has the following representation:

$$F(x) = F\,(x_1 \| x_2) = (T\,(x_1, x_2)\,, U\,(x_2, T\,(x_1, x_2)))\,, \qquad (1)$$

then such representation of F in the form (1) is called the *TU*-representation.



Let $\mathbb{F}_2^n$, $n \geq 6$ is a vector space with elements $v = (v_1, v_2, \ldots, v_n)$.

For each element $v \in \mathbb{F}_2^n$ we put the match the pair (v', v_n), where $v' \in \mathbb{F}_{2^{n-1}}$, $v' = v_{n-1}x^{n-2} + \cdots + v_1$, $\mathbb{F}_{2^{n-1}} = \mathbb{F}_2[x]/f(x)$, $\deg(f) = n - 1$.

This correspondence specifies bijective mapping of the set $\mathbb{F}_2^n$ to $\mathbb{F}_{2^{n-1}} \times \mathbb{F}_2$.

Let $\mathrm{tr}(x)$ be a trace function from the field $\mathbb{F}_{2^{n-1}}$ to $\mathbb{F}_2$.

For any $c \in \mathbb{F}_{2^n-1} \backslash \{0,1\}$ such that $\mathrm{tr}(c) = \mathrm{tr}\left(c^{-1}\right)$, and arbitrary Boolean function g of $n-1$ variables in [1] the function $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ us defined as follows:

$$F(v_1, v_2, \ldots, v_{n-1}, v_n) = \begin{cases} \left(v'^{-1}, g(v')\right), & v_n = 0 \\ \left(c \cdot v'^{-1}, g\left(v' \cdot c^{-1}\right) + 1\right), & v_n = 1 \end{cases}, \tag{2}$$

where $v' \in \mathbb{F}_{2^{n-1}}$, v' is defined by the vector $(v_1, v_2, \ldots, v_{n-1}) \in \mathbb{F}_2^{n-1}$, $0^{-1} = 0$.

F is differentially 4-uniform permutation, that has the maximal algebraic degree equals to $n-1$, and the nonlinearity less or equals to $2^{n-1} - 2\left\lfloor 2^{(n+1)/2} \right\rfloor - 4$.

[1] Claude Carlet, Deng Tang, Xiaohu Tang, and Qunying Liao., "New construction of differentially 4-uniform bijections. In Dongdai Lin, Shouhuai Xu, and Moti Yung, editors, Information Security and Cryptology, pages 22–38, Cham, 2014. Springer International Publishing.".

Proposition 1

Let $x_1 \in \mathbb{F}_2^{n-1}$, $x_2 \in \mathbb{F}_2$,

- $T\colon \mathbb{F}_2^{n-1} \times \mathbb{F}_2 \to \mathbb{F}_2^{n-1}$, $T(x_1, x_2) = x_1^{-1} \cdot c^{x_2}$,
- $U\colon \mathbb{F}_2^1 \times \mathbb{F}_2^{n-1} \to \mathbb{F}_2$, $U(x_2, x_1) = g\left(x_1^{-1}\right) + x_2$.

Then

1. *if we fix* x_2 *by an arbitrary value from* $\mathbb{F}_2$ *then the function* T *is a bijection on the variable* x_1,
2. *if we fix* x_1 *by an arbitrary value from* $\mathbb{F}_2^{n-1}$ *then the function* U *is a bijection on the variable* x_2,
3. *functions* T *and* U *define a* TU*-representation of permutation defined by* (2).

For the function F that has a TU-representation given by equation (1), denote

- for $a \in \mathbb{F}_2^t$ the value $\delta_{T,a}$ is equal to δ if permutation T with fixed $x_2 = a$ is differentially δ-uniform,
- for $a \in \mathbb{F}_2^t$, $\alpha_1,\ \beta_1 \in \mathbb{F}_2^{n-t}$, $\alpha_2 \in \mathbb{F}_2^t \backslash \theta$, the value $\Delta_{T,a}^{\alpha_1,\alpha_2,\beta_1}$ is the number of solutions to the equation:

$$T(x_1, a) + T(x_1 + \alpha_1, a + \alpha_2) = \beta_1.$$

Theorem 8

Let $n, t \in \mathbb{N}$, $1 \leq t \leq n-1$, $x_1 \in \mathbb{F}_2^{n-t}$, $x_2 \in \mathbb{F}_2^t$,

- *function $T\colon \mathbb{F}_2^{n-t} \times \mathbb{F}_2^t \to \mathbb{F}_2^{n-1}$ such that fixation x_2 by arbitrary value from $\mathbb{F}_2^t$ the function $T(x_1, x_2)$ is the permutation on the variable x_1,*
- *function $U\colon \mathbb{F}_2^t \times \mathbb{F}_2^{n-t} \to \mathbb{F}_2^t$ such that fixation x_1 by arbitrary value from $\mathbb{F}_2^{n-t}$ the function $U(x_2, x_1)$ is the permutation on the variable x_2.*

Then the permutation F, defined by (1) *is differentially δ-uniform, where*

$$\delta \leq 2^t \cdot \max \left\{ \max_{a \in \mathbb{F}_2^t} \left(\delta_{T,a}\right), \max_{\substack{\alpha_1, \beta_1 \in \mathbb{F}_2^{n-t}, \\ a \in \mathbb{F}_2^t,\ \alpha_2 \in \mathbb{F}_2^t \setminus \theta}} \left(\Delta_{T,a}^{\alpha_1, \alpha_2, \beta_1}\right) \right\}. \tag{3}$$

Corollary 9

In the conditions of theorem 8 let $t = 1$, $\delta_{T,a} \leq \delta$, $a \in \mathbb{F}_2$, *then the permutation* F, *defined by* (1) *is differentially* 2δ*-uniform* $\max\limits_{\alpha_1,\, \beta_1 \in \mathbb{F}_2^{n-1}} \Delta_{T,0}^{\alpha_1,1,\beta_1} \leq \delta$.

According to the corollary in order to construct a differentially 4-uniform permutation F one must take two differential 2-uniform permutations π_1 and π_2 of the space $\mathbb{F}_2^{n-1}$. And if $T(x_1, 0) = \pi_1$ and $T(x_1, 1) = \pi_2$, then it remains to check that the number of solutions of following equations:

$$\pi_1(x) + \pi_2(x + \alpha_1) = \beta_1$$

for all possible values of $\alpha_1, \beta_1 \in \mathbb{F}_2^{n-1}$ are not greater than 2.

Proposition 2

Let $x_1 \in \mathbb{F}_2^{n-1}$, n be an even number, $x_2 \in \mathbb{F}_2$, f be an arbitrary Boolean function of $n-1$ variables, $c \in \mathbb{F}_{2^{n-1}} \setminus \{\theta, 1\}$,

- $T\colon \mathbb{F}_2^{n-1} \times \mathbb{F}_2 \to \mathbb{F}_2^{n-1}$, $T(x_1, x_2) = x_1^{-1} \cdot c^{x_2}$,
- $U\colon \mathbb{F}_2^1 \times \mathbb{F}_2^{n-1} \to \mathbb{F}_2$, $U(x_2, x_1) = f(x_1) + x_2$.

Then equation (1) *defines the permutation F, and at the same time*

1. *if* $\mathrm{tr}(c) = \mathrm{tr}\left(c^{-1}\right) = 1$, *then* $\delta_F = 4$,
2. *otherwise* — $\delta_F = 6$.

Remark 1

The proof of point 1 of the previous proposition was previously published in [2].

[2] Claude Carlet, Deng Tang, Xiaohu Tang, and Qunying Liao., "New construction of differentially 4-uniform bijections. In Dongdai Lin, Shouhuai Xu, and Moti Yung, editors, Information Security and Cryptology, pages 22–38, Cham, 2014. Springer International Publishing.".

Proposition 3

Let $x_1 \in \mathbb{F}_2^{n-1}$, *n be an even number,* $x_2 \in \mathbb{F}_2$, *f be an arbitrary Boolean function of* $n-1$ *variables,* $c \in \mathbb{F}_{2^{n-1}} \setminus \{\theta, 1\}$,

- $T\colon \mathbb{F}_2^{n-1} \times \mathbb{F}_2 \to \mathbb{F}_2^{n-1}$, $T(x_1, x_2) = x_1^3 \cdot c^{x_2}$,
- $U\colon \mathbb{F}_2^1 \times \mathbb{F}_2^{n-1} \to \mathbb{F}_2$, $U(x_2, x_1) = f(x_1) + x_2$.

Then equation (1) *defines the permutation F, and* $\delta_F = 6$.

Proposition 4

Let $x_1 \in \mathbb{F}_2^{n-1}$, *n be an even number,* $x_2 \in \mathbb{F}_2$, $a, b \in \mathbb{F}_{2^{n-1}}$, $T\colon \mathbb{F}_2^{n-1} \times \mathbb{F}_2 \to \mathbb{F}_2^{n-1}$

- $T(x_1, 0) = x_1^3$,
- $T(x_1, 1) = x_1^3 + a \cdot x_1^2 + b \cdot x_1$.

Then either $\alpha_1 \in \mathbb{F}_{2^{n-1}}$ *and* $\beta_1 \in \mathbb{F}_{2^{n-1}}$ *exist such that the number of solutions to the equation*

$$T(x_1 + \alpha_1, 0) + T(x_1, 1) = \beta_1$$

will equal to 2^{n-1} *or* $T(x_1, 1)$ *is not a permutation.*

Proposition 5

Let $x_1 \in \mathbb{F}_2^{n-1}$, n e an even number, $x_2 \in \mathbb{F}_2$, f be an arbitrary Booleann function of $n-1$ variables, $c \in \mathbb{F}_{2^{n-1}} \setminus \{\theta, 1\}$,

- $T\colon \mathbb{F}_2^{n-1} \times \mathbb{F}_2 \to \mathbb{F}_2^{n-1}$, $T(x_1, 0) = x_1^3$, $T(x_1, 0) = x_1^{-1}$,
- $U\colon \mathbb{F}_2^1 \times \mathbb{F}_2^{n-1} \to \mathbb{F}_2$, $U(x_2, x_1) = f(x_1) + x_2$.

Then the equation (1) *specifies differentially 8-uniform permutation.*

Proposition 6

Let $t = 2$, $x_1 \in \mathbb{F}_2^{n-t}$, $x_2 \in \mathbb{F}_2^t$,

- $T\colon \mathbb{F}_2^{n-t} \times \mathbb{F}_2^t \to \mathbb{F}_2^{n-1}$, *when fixing an arbitrary x_2 function $T(x_1, x_2) = x_1^{-1} \cdot c^{x_2}$,*
- $U\colon \mathbb{F}_2^t \times \mathbb{F}_2^{n-t} \to \mathbb{F}_2^t$, *when fixing an arbitrary x_1 function $U(x_2, x_1)$ is a permutation on the variable x_2.*

Then there exist such c_y, $y \in \mathbb{F}_{2^2}$, $c_{y_1} \neq c_{y_2}$ if $y_1 \neq y_2$, that the permutation F, given by equation (1) *is a differentially 8-uniform permutation.*

Proposition 7

Let $x_1 \in \mathbb{F}_2^{n-1}$, $n \in \mathbb{N}$ *be an even number,* $i \in \mathbb{N}$, $i \leq 2^{n-1} - 2$, $x_2 \in \mathbb{F}_2$, $c \in \mathbb{F}_{2^{n-1}} \setminus \{\theta, 1\}$, $T \colon \mathbb{F}_2^{n-1} \times \mathbb{F}_2 \to \mathbb{F}_2^{n-1}$, $T(x_1, x_2) = x_1^i \cdot c^{x_2}$, *then* $\deg T = |i| + 1$.

Remark 2

If in statements of propositions 2 and 3 the function f has an algebraic degree equal to 1, then the entire permutation F will also have an algebraic degree equal to 1.

Proposition 8

Under the conditions of propositions 2 and 3, the permutation F will have the graph algebraic immunity equals to 2.