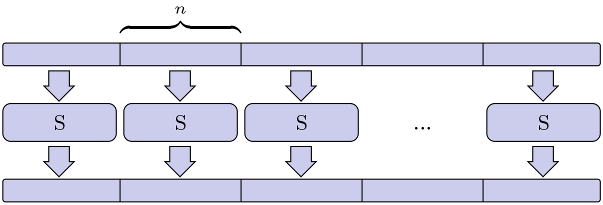
ADAPTED SPECTRAL-DIFFERENTIAL METHOD FOR CONSTRUCTING DIFFERENTIALLY 4-UNIFORM PIECEWISE-LINEAR SUBSTITUTIONS, ORTHOMORPHISMS, INVOLUTIONS OVER THE FIELD $\mathbb{F}_{2^n}$

Menyachikhin Andrey

Shannon's properties[1] are often implemented in modern block ciphers by using three layers in each round:

1. the round key layer,
2. the confusion layer,
3. diffusion layer.

The confusion layer is often realized as a parallel application of nonlinear substitution boxes (S-boxes)



Remark

For computational reasons (n, n)-functions are better used as s-boxes when n is even, the best being when n is a power of 2.

In this report, special attention is paid to the differential uniformity of s-boxes.

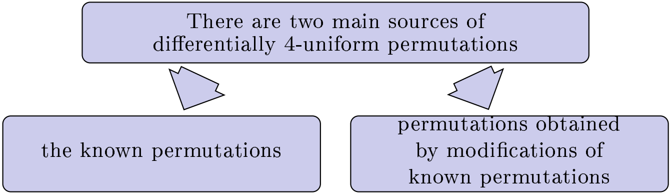
[1] Shannon C. A mathematical theory of cryptography, Tech. Rep. MM 45-110-02, Bell Labs. Tech. Memo., 1945.

Introduction

A mapping is called differentially $\triangle$-uniform[1,2] if for every non-zero input difference and any output difference the number of possible inputs has a uniform upper bound $\triangle$.

Remark

The existence of differentially 2-uniform permutations of $\mathbb{F}_{2^n}$ for even $n > 6$ is an open problem[3]. It is then important to find as many differentially 4-uniform permutations as possible in even dimension.



[1] Nyberg K. Differentially uniform mappings for cryptography. Proceedings of EUROCRYPT 1993, Lecture Notes in Computer Science 765, 1994, pp. 55–64.

[2] Sachkov V.N. Combinatorial properties of differentially 2-uniform substitutions. Mat. Vopr. Kriptogr., 6:1 (2015), pp. 159-179.

[3] Carlet C. Open questions on nonlinearity and on APN functions. Proceedings of Arithmetic of Finite Fields 5th International Workshop, WAIFI 2014, LNCS 9061 (2015), pp. 83-107.

We begin with the known permutations:

1. power functions (for example, the inverse function[1] – $g(x) = x^{2^n-2}$; the Gold function[2] – $g(x) = x^{2^i+1}$, $\gcd(i,n) = 2$, $n \equiv 2 \pmod 4$; the Kasami function[3] – $g(x) = x^{2^{2i}-2^i+1}$, $\gcd(i,n) = 2$; the Dobbertin function[4] – $g(x) = x^{2^{n/2+n/4+1}}$, $4 \mid n$, $8 \nmid n$);
2. polynomial functions (for example, binomial functions[5]

$$\zeta x^{2^s+1} + \zeta^{2^k} x^{2^{-k}+2^{k+s}},$$

where ζ is a primitive field element of $\mathbb{F}_{2^n}$, $n \equiv 3k$, k is even, $k/2$ is odd, $3 \nmid k$, $\gcd(n,s) = 2$, $3 \mid (k+s)$).

[1] Nyberg K. Differentially uniform mappings for cryptography. Proceedings of EUROCRYPT 1993, Lecture Notes in Computer Science 765, 1994, pp. 55–64.

[2] Gold R. Maximal recursive sequences with 3-valued recursive crosscorrelation functions. IEEE Transactions on Information Theory 14, 1968, pp. 154–156.

[3] Kasami T. The weight enumerators for several classes of subcodes of the second order binary Reed–Muller codes. Information and Control 18, 1971, pp. 369–394.

[4] Dobbertin H. One-to-one highly nonlinear power functions on GF(2n). Applicable Algebra in Engineering, Communication and Computing (AAECC), 9:2(1998), pp. 139–152.

[5] Bracken C., Tan C. and Tan Y. Binomial differentially 4 uniform permutations with high nonlinearity. Finite Fields and Their Applications 18:3(2012), pp. 537-546.

We continue with permutations obtained by modifications of known permutations:

1. the switching constructions[1]. These permutations were obtained by adding Boolean functions to the inverse function $g(x) = x^{2^n-2}$ (for example, constructions of the following type
$$g(x) = x^{2^n-2} + tr_n\left(x^2(x+1)^{2^n-2}\right) \text{ и}$$
$$g(x) = x^{2^n-2} + tr_n\left(x^{(2^n-2)d} + \left(x^{2^n-2}+1\right)^d\right),$$
where $d = 3\left(2^t+1\right)$, $2 \le t \le n/2-1$ and other constructions);
2. the Carlet constructions (for example, construction[2] that consist in restricting APN-functions in $n+1$ variables to a linear manifold of dimension $n = 2k$ and its various generalizations[3]; construction of the following type[4]
$$g(x, x') = \begin{cases} \left(x^{2^{n-1}-2}, f(x)\right), & \text{if } x' = 0, \\ \left(cx^{2^{n-1}-2}, f\left(xc^{2^{n-1}-2}+1\right)\right), & \text{if } x' = 1, \end{cases}$$
where $n \ge 6$, n is even, $c \in \mathbb{F}_{2^{n-1}} \setminus \mathbb{F}_2$, $tr_{n-1}(c) = tr_{n-1}\left(c^{2^{n-1}}-2\right) = 1$, $x \in \mathbb{F}_{2^{n-1}}$, $x' \in \mathbb{F}_2$, f is $n-1$ variables Boolean function);

[1] Qu L., Tan Y., Tan C. H., and Li C. Constructing differentially 4-uniform permutations over via the switching method. IEEE Transactions on Information Theory 59:7(2013), pp. 4675–4686.

[2] Carlet C. Boolean functions for cryptography and coding theory. Cambridge University Press, 2020, 574 p.

[3] Davydov S.A., Kruglov I.A. A method of construction of differentially 4-uniform permutations over V_m for even m. Diskr. Mat., 31:2 (2019), pp. 69-76.

[4] Carlet C., Tang D., Tang X., and Liao Q. New construction of differentially 4-uniform bijections. Proceedings of INSCRYPT 2013, LNCScience 8567 (2014), pp. 22–38.

3. constructions that implement multiplication by cycles (for example, permutation[1] obtained from the inverse function $g(x) = x^{2^n-2}$ by swapping its values at two different points $x_1, x_2 \in \mathbb{F}_{2^n}^{\times}$, $tr_n\left(x_1 x_2^{-1}\right) tr_n\left(x_1^{-1} x_2\right) = 1$; permutations[2] obtained from the inverse function by cyclically shifting the images of the function over some subset

$$g(x) = (\pi_i(x))^{2^n-2},$$

where $\pi_i = \left(i, c_i, c_i^{-1}\right)$, $c_i \in \mathbb{F}_{2^{n-1}} \setminus \mathbb{F}_2$, $tr_n(c_i) = tr_n\left((c_i+1)^{-1}\right) = 1$, $i \in \{0,1\}$, $tr_n\left((c_1+1)^{-3}\right) = 0$, $tr_n\left(c_1^{-1}\right) = 1$; and other constructions);

4. permutations obtained by applying affine transformations to an inverse function on some subfields of $\mathbb{F}_{2^n}$ (for example, construction of the following type[3]

$$g(x) = \begin{cases} c_0 x^{2^n-2} + c_1, & \text{if } x^{2^m} = x, \\ x^{2^n-2}, & \text{if } x^{2^m} \neq x, \end{cases}$$

where $c_0, c_1 \in \mathbb{F}_{2^m}$, $n = mk$, $x \in \mathbb{F}_{2^n}$);

[1] Yu Y., Wang M., Li Y. Constructing low differential uniformity functions from known ones. Chinese Journal of Electronics, 22:3 (2013), pp. 495-499.

[2] Fu S. and Feng X. Involutory differentially 4-uniform permutations from known constructions. Designs, Codes and Cryptography 87:1(2018), pp. 31–56.

[3] Zha Z., Hu L., and Sun S. Constructing new differentially 4-uniform permutations from the inverse function. Finite Fields and Their Applications 25 (2014), pp. 64–78.

6. the butterfly construction[1] and its various generalizations[2,3] (for example, construction of the following type[4]

$$g\left(x,x'\right)=\left(f\left(x,x'\right),f\left(x',x\right)\right) \text{ and } g\left(x,x'\right)=\left(f\left(f^{-1}\left(x,x'\right),x'\right),f^{-1}\left(x,x'\right)\right),$$

where $x,x' \in \mathbb{F}_{2^{n/2}}$, $n=4k+2$, $k\geq 1$, $f\left(x,x'\right)=\left(x+c_1x'\right)^3+c_2x'^3$, $c_1,c_2\in\mathbb{F}_{2^{n/2}}$, $c_2\neq\left(1+c_1\right)^3$.

The main idea of this report

Combining an algebraic and heuristic approaches to construction s-boxes with low differential uniformity.

[1] Perrin L., Udovenko A., and Biryukov A.. Cryptanalysis of a theorem: decomposing the only known solution to the big APN problem. Proceedings of CRYPTO 2016, Lecture Notes in Computer Science 9815, part II, 2016, pp. 93–122.

[2] De La Cruz Jimenez R.A. Constructing 8-bit permutations, 8-bit involutions and 8-bit orthomorphisms with almost optimal cryptographic parameters. Mat. Vopr. Kriptogr., 12:3 (2021), pp. 89-124.

[3] Fomin D.B. New classes of 8-bit permutations based on butterfly structure. Mat. Vopr. Kriptogr., 10:2 (2019), pp. 169-180.

[4] Canteaut A., Duval S., and Perrin L. A generalisation of Dillon's APN permutation with the best known differential and nonlinear properties for all fields of size 24k+2. IEEE Transactions on Information Theory 63:11 (2017), pp. 7575–7591.

Let $H < \mathbb{F}_{2^n}^{\times}$ be the subgroup of order l of the multiplicative group of the field $\mathbb{F}_{2^n}$, $0 < l < 2^n - 1$, $2^n - 1 = l \cdot r$, where $r \in \mathbb{N}$, ζ is a primitive field element of $\mathbb{F}_{2^n}$, $H = \langle \zeta^r \rangle$. The group $\mathbb{F}_{2^n}^{\times}$ is partitioned into cosets of H:

$$\mathbb{F}_{2^n}^{\times} = \bigcup_{i=0}^{r-1} H_i, H_i = \zeta^i H, i = 0, ..., r-1.$$

Definition 1

Piecewise-linear function[1–5] $g \colon \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is defined as

$$g(x) = \begin{cases} 0, & \text{if } x = 0, \\ \zeta^{a_i} x, & \text{if } x \in H_i, \end{cases}$$

where $a_i \in \{0, ..., 2^n - 2\}$, $i = 0, ..., r-1$.

It is well known[2,3] that function g is bijective if and only if bijective function $\pi \colon \mathbb{Z}_r \to \mathbb{Z}_r$,

$$\pi(i) = (a_i + i) \bmod r, i = 0, ..., r-1$$

Let $L_r(\mathbb{F}_{2^n})$ be the set of all piecewise-linear permutations satisfying conditions of definition 1.

For all $n > 1$ we have

$$|L_r(\mathbb{F}_{2^n})| = l^r r!.$$

[1] Wells C. Groups of permutation polynomials. Monatshefte für Mathematik, 71 (1967), pp. 248-262.

[2] Evans A. Orthomorphisms graphs and groups. Springer-Verlag, Berlin, 1992, 114 p.

[3] Trishin A.E. The nonlinearity index for a piecewise-linear substitution of the additive group of the field $\mathbb{F}_{2^n}$. Prikl. Diskr. Mat., 4:30 (2015), pp. 32-42.

[4] Bugrov A.D. Piecewise-affine permutations of finite fields. Prikl. Diskr. Mat., 4:30 (2015), pp. 5-23.

[5] Pogorelov B.A., Pudovkina M.A. Classes of piecewise quasiaffine transformations on the dihedral, the quasidihedral and the modular maximal-cyclic 2-group. Diskr. Mat., 34:1 (2022), pp. 103-125.

Let $g\colon \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ be a function from a set $\mathbb{F}_{2^n}$ to a set $\mathbb{F}_{2^n}$. If a set M is a subset of $\mathbb{F}_{2^n}$, then the *restriction of g to M* is the function $g_M\colon M \to \mathbb{F}_{2^n}$.

Definition 2

The differential uniformity p_{g_M} of the mapping g_M is defined as

$$p_{g_M} = \max_{\alpha \in \mathbb{F}_{2^n}^{\times}, \beta \in \mathbb{F}_{2^n}} p_{\alpha,\beta}^{g_M},$$

where

$$p_{\alpha,\beta}^{g_M} = \left| \left\{ x \in M \,|\, x + \alpha \in M, g(x+\alpha) + g(x) = \beta \right\} \right|.$$

If M is a proper subset of $\mathbb{F}_{2^n}$, then the p_{g_M} parameter is called *the partial differential uniformity* of the function g over the set M.

Remarks

1. Notice that $M \subset \mathbb{F}_{2^n}$ may be not closed under operation $+$ in the field $\mathbb{F}_{2^n}$.
2. The introduced definition is consistent with the known formulation if the set $M \subset \mathbb{F}_{2^n}$ is closed under operation $+$ in the field $\mathbb{F}_{2^n}$.
3. For a chain of subsets $M_0 \subseteq M_1 \subseteq \ldots \subseteq M_{s-1} \subseteq \mathbb{F}_{2^n}$ we have

$$p_{g_{M_0}} \le p_{g_{M_1}} \le \ldots \le p_{g_{M_{s-1}}} \le p_g.$$

The difference distribution table $P(g_M)$ of the mapping g_M counts the number of cases when the input difference of a pair is α and the output difference is β.

Main definitions and notations

For the mapping g_M and each number $i = 0, 1, ..., |M|$, we define the set

$$D_{g_M,i} = \left\{ (\alpha, \beta) \in \mathbb{F}_{2^n}^{\times} \times \mathbb{F}_{2^n} \left| p_{\alpha,\beta}^{g_M} = i \right. \right\}.$$

Definition 3

The differential spectrum of the mapping g_M is defined as
$$\vec{D}_{g_M} = \left(|D_{g_M,0}|, |D_{g_M,1}|, |D_{g_M,2}|, ..., |D_{g_M,|M|}| \right).$$

Definition 4

The nonlinearity nl_g of the function $g\colon \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is defined as

$$nl_g = 2^{n-1} - \frac{1}{2} \max_{\alpha \in \mathbb{F}_{2^n}, \beta \in \mathbb{F}_{2^n}^{\times}} w_{g_\beta}(\alpha),$$

where $w_{g_\beta}(\alpha) = \sum\limits_{x \in \mathbb{F}_{2^n}} (-1)^{tr_n(\beta g(x) + \alpha x)}$ is a Walsh transform of a Boolean function $g_\beta \colon \mathbb{F}_{2^n} \to \mathbb{F}_2$ as follows $g_\beta(x) = tr_n(\beta g(x))$.

For the function $g\colon \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ and each number $i = 0, 1, ..., 2^{n-1} - 2^{\frac{n}{2}-1}$, we define the set

$$L_{g,i} = \left\{ (\alpha, \beta) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^n}^{\times} \left| w_{g_\beta}(\alpha) = i \right. \right\}.$$

Definition 5

The linear spectrum of the function g is defined as
$$\vec{L}_g = \left(|L_{g,0}|, |L_{g,1}|, |L_{g,2}|, ..., |L_{g,2^{n-1}-2^{\frac{n}{2}-1}}| \right).$$

Definition 6

The generalized algebraic degree $\overline{\lambda_g}$ of the permutation $g \in S\left(\mathbb{F}_{2^n}\right)$ is defined as

$$\overline{\lambda_g} = \min\left\{\lambda_g, \lambda_{g^{-1}}\right\},$$

where
$$\lambda_g = \min_{\alpha \in \mathbb{F}_{2^n}^{\times}} \deg\left(tr\left(ag\left(x\right)\right)\right), \lambda_{g^{-1}} = \min_{\alpha \in \mathbb{F}_{2^n}^{\times}} \deg\left(tr\left(ag^{-1}\left(x\right)\right)\right),$$

and deg denotes the algebraic degree of the Zhegalkin polynomial of Boolean function.

Definition 7

Two permutations $g, h \in S\left(\mathbb{F}_{2^n}\right)$ are *linear equivalent* ($g \overset{L}{\sim} h$) if there exist linear permutations $L_1, L_2\colon \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ such that

$$L_2 \circ g \circ L_1 = h.$$

The set of all *fixed point* of a permutation $g \in S\left(\mathbb{F}_{2^n}\right)$ is denoted by F_g.

Proposition 1

Let $g \in L_r\left(\mathbb{F}_{2^n}\right)$ and ζ is a primitive field element of $\mathbb{F}_{2^n}$. Then $x_0 \in \mathbb{F}_{2^n}$ is a solution to equation $g\left(x+\alpha_0\right)+g\left(x\right)=\beta_0$, $\alpha_0, \beta_0 \in \mathbb{F}_{2^n}$ if and only if $x_j = x_0\zeta^{rj}$ is a solution to equation $g\left(x+\alpha_j\right)+g\left(x\right)=\beta_j$, $\alpha_j = \alpha_0\zeta^{rj}$, $\beta_j = \beta_0\zeta^{rj}$, $j = 1, 2, ..., l-1$.

Corollary

For $g \in L_r\left(\mathbb{F}_{2^n}\right)$ and any number $i = 0, 1, ..., 2^{n-1}$ we have $\left|D_{g,i}\right| \equiv 0 \pmod{l}$.

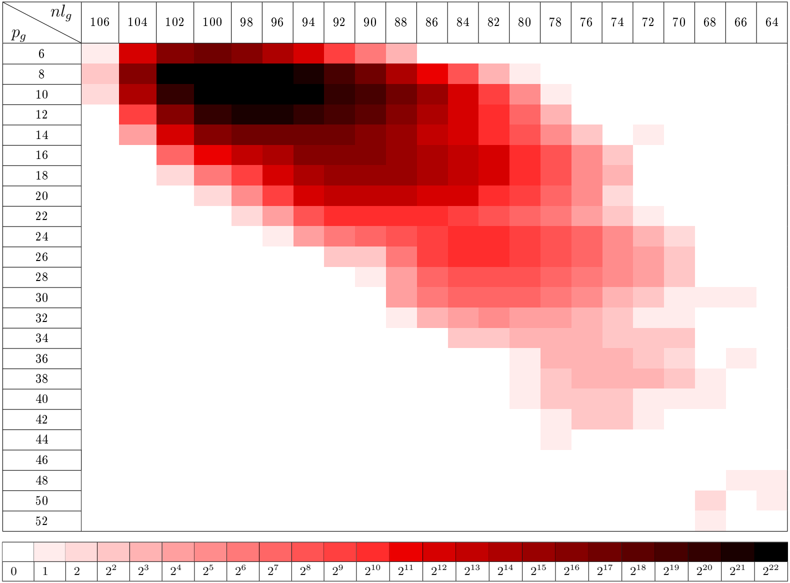
Proposition 2

Let $g \in L_r\left(\mathbb{F}_{2^n}\right)$ and ζ is a primitive field element of $\mathbb{F}_{2^n}$. Then $x_0 \in \mathbb{F}_{2^n}$ is a solution to equation $tr_n\left(x \cdot \alpha_0\right) = tr_n\left(g\left(x\right) \cdot \beta_0\right)$, $\alpha_0, \beta_0 \in \mathbb{F}_{2^n}$ if and only if $x_j = x_0\zeta^{rj}$ is a solution to equation $tr_n\left(x \cdot \alpha_j\right) = tr_n\left(g\left(x\right) \cdot \beta_j\right)$, $\alpha_j = \alpha_0\zeta^{r(l-i)}$, $\beta_j = \beta_0\zeta^{r(l-j)}$, $j = 1, 2, ..., l-1$.

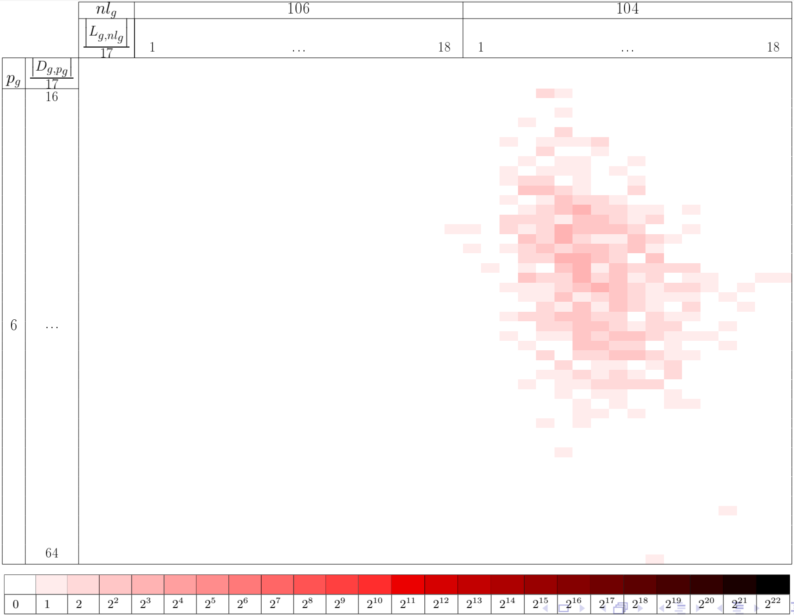
Corollary

For $g \in L_r\left(\mathbb{F}_{2^n}\right)$ and any number $i = 0, 1, ..., 2^{n-1} - 2^{\frac{n}{2}-1}$ we have $\left|L_{g,i}\right| \equiv 0 \pmod{l}$.

The joint distribution of parameters p_g and nl_g for 10^8 randomly generated permutations $g \in L_{15}(\mathbb{F}_{2^8})$



The joint distribution of parameters p_g and nl_g for 10^8 randomly generated permutations $g \in L_{15}(\mathbb{F}_{2^8})$



We define mapping $\psi\colon \mathbb{F}_{2^n}^{\times} \to \left\{1, \zeta, \zeta^2, ..., \zeta^{r-1}\right\}$ as follows $\psi\left(x\right) = \zeta^i$ if $x \in H_i$, $i \in \{0, ..., r-1\}$, and for any $x \in \mathbb{F}_{2^n}^{\times}$ we define the permutation $\sigma_x \in S\left(\mathbb{F}_{2^n}\right)$ as follows $\sigma_x\left(y\right) = yx^{-1}\psi\left(x\right)$.

Proposition 1 allows us to associate any row of the matrix P_g

$$\left(p^g_{\alpha,0}, p^g_{\alpha,1}, p^g_{\alpha,\zeta}, ..., p^g_{\alpha,\zeta^{2^n-2}}\right)$$

with the row

$$\left(p^g_{\psi(\alpha),0}, p^g_{\psi(\alpha),1}, p^g_{\psi(\alpha),\zeta}, ..., p^g_{\psi(\alpha),\zeta^{2^n-2}}\right) = \\ = \left(p^g_{\alpha,\sigma_\alpha(0)}, p^g_{\alpha,\sigma_\alpha(1)}, p^g_{\alpha,\sigma_\alpha(\zeta)}, ..., p^g_{\alpha,\sigma_\alpha\left(\zeta^{2^n-2}\right)}\right)$$

of the same matrix. Hence, the matrix P_g of the permutation $g \in L_r\left(\mathbb{F}_{2^n}\right)$ has at most r unique rows.

Example 1

Let H is the subgroup of order 5 of $\mathbb{F}_{2^4} = \mathbb{F}_2[x]/x^4+x+1$ and $\zeta = 2$ is a primitive field element of $\mathbb{F}_{2^4}$. The group $\mathbb{F}_{2^4}^{\times}$ is partitioned into cosets of H:

$$\mathbb{F}_{2^4}^{\times} = \underbrace{\{8, c, a, f, 1\}}_{H_0} \cup \underbrace{\{3, b, 7, d, 2\}}_{H_1} \cup \underbrace{\{6, 5, e, 9, 4\}}_{H_2}.$$

Permutation $g \in L_3(\mathbb{F}_{2^4})$															
0	9	7	d	f	8	1	3	4	a	5	2	6	b	c	e

The difference distribution table $P(g)$ of the permutation g																
α \ β	0	1	2	4	8	3	6	c	b	5	a	7	e	f	d	9
1	**0**	**0**	**4**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**2**	**4**	**2**	**0**	**2**	**2**
2	**0**	**2**	**0**	**2**	**2**	**0**	**0**	**0**	**2**	**2**	**2**	**2**	**2**	**0**	**0**	**0**
4	**0**	**4**	**2**	**0**	**0**	**0**	**2**	**2**	**0**	**0**	**0**	**0**	**2**	**2**	**0**	**2**
8	0	0	2	2	0	4	0	0	0	0	0	0	0	2	4	2
3	0	0	0	0	2	0	2	2	0	0	0	2	2	2	2	2
6	0	2	0	2	4	2	0	0	0	2	2	0	0	0	0	2
c	0	2	4	2	0	2	2	0	4	0	0	0	0	0	0	0
b	0	2	2	2	0	0	0	2	0	2	2	0	0	0	2	2
5	0	0	0	2	2	0	2	4	2	0	0	0	2	2	0	0
a	0	0	0	0	2	4	2	0	2	2	0	4	0	0	0	0
7	0	0	2	2	2	2	2	0	0	0	2	0	2	2	0	0
e	0	2	0	0	0	0	2	2	0	2	4	2	0	0	0	2
f	0	0	0	0	0	0	0	2	4	2	0	2	2	0	4	0
d	0	2	0	0	0	2	2	2	2	2	0	0	0	2	0	2
9	0	0	0	2	2	0	0	0	0	2	2	0	2	4	2	0

Efficient computation of the differential spectrum of piecewise-linear substitutions

Denote by $H_{(i_0,\dots,i_{s-1})} = \bigcup_{j=0}^{s-1} H_{i_j} \cup \{0\}$, where $s \in \{1,\dots,r\}$. Consider the mapping $g_{H_{(i_0,\dots,i_{s-1})}} : H_{(i_0,\dots,i_{s-1})} \to \mathbb{F}_{2^n}$, which is the restriction of the permutation $g \in L_r(\mathbb{F}_{2^n})$ to the set $H_{(i_0,\dots,i_{s-1})}$. Proposition 1 gives us the following algorithm for calculating the differential spectrum of the mapping $g_{H_{(i_0,\dots,i_{s-1})}} : H_{(i_0,\dots,i_{s-1})} \to \mathbb{F}_{2^n}$ (see Fig. 1).

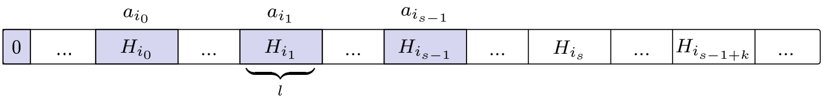


Figure 1. The idea of algorithm 1

Proposition 3

Differential spectrum $\vec{D}_{g_{H_{(i_0,\dots,i_{s-1})}}}$ of the mapping $g_{H_{(i_0,\dots,i_{s-1})}}$, $s \in \{1,\dots,r\}$, can be calculated using algorithm 1 with complexity t,

$$t \le cls^2, c = const.$$

Remark

For $s = r$ the complexity of algorithm 1 is l times lower than the complexity of the classical approach.

Algorithm 1 can be easily modified for the case when it is necessary to calculate the differential spectrum $\vec{D}_{g_{H_{(i_0,\dots,i_{s-1+k})}}}$ of the mapping $g_{H_{(i_0,\dots,i_{s-1+k})}}$ from the known mapping $g_{H_{(i_0,\dots,i_{s-1})}}$, difference distribution table $P_{g_{H_{(i_0,\dots,i_{s-1})}}}$ and differential spectrum $\vec{D}_{g_{H_{(i_0,\dots,i_{s-1})}}}$ (see Fig. 2).

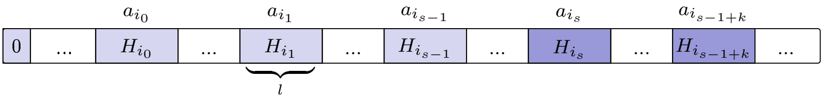


Figure 2. The idea of algorithm 2

Proposition 4

Differential spectrum $\vec{D}_{g_{H_{(i_0,\dots,i_{s-1+k})}}}$ of the mapping $g_{H_{(i_0,\dots,i_{s-1+k})}}$, $s \in \{1,\dots,r-1\}$, can be calculated from the differential spectrum $\vec{D}_{g_{H_{(i_0,\dots,i_{s-1})}}}$ and the submatrix $P_{g_{H_{(i_0,\dots,i_{s-1})}}}\begin{pmatrix} 1, \zeta, \zeta^2, \dots, \zeta^{r-1} \\ 0, 1, \zeta, \dots, \zeta^{2^n-2} \end{pmatrix}$ of the matrix $P_{g_{H_{(i_0,\dots,i_{s-1})}}}$ of the mapping $g_{H_{(i_0,\dots,i_{s-1})}}$ using algorithm 2 with t complexity,

$$t \leq cls, c = const.$$

[1] Menyachikhin A.V. The change in linear and differential characteristics of substitution after the multiplication by transposition. Mat. Vopr. Kriptogr., 11:2 (2020), pp. 111-123.

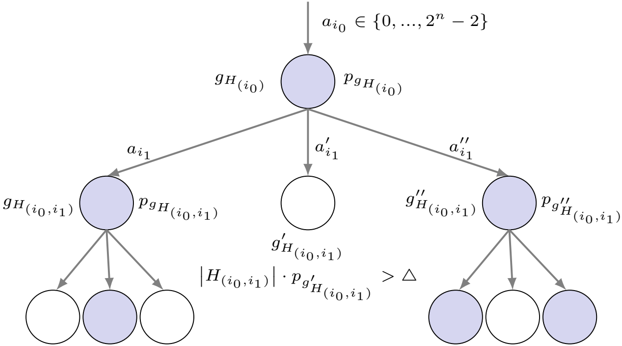


Figure 3. The main idea of algorithm 3 implementing the adapted spectral-differential method

Proposition 5

For $n, r, w \in \mathbb{N}$, $r \mid 2^n - 1$ we have the following complexity t of algorithm 3:

$$t \leq cw2^n\,(r-1)\left(2^{n-1} + n + \log w + {}^r\!/_2\right), \text{ where } c = const.$$

[1] Menyachikhin A.V. Spectral-linear and spectral-differential methods for generating s-boxes having almost optimal cryptographic parameters. Mat. Vopr. Kriptogr., 8:2 (2017), pp. 97-116.

Examples of differentially 4-uniform piecewise-linear permutations $g \in L_{15}(\mathbb{F}_{2^8})$ constructed using algorithm 3

Let $\mathbb{F}_{2^8} = \mathbb{F}_2[x]/_{x^8+x^4+x^3+x+1}$, $\zeta = 3$ is a primitive field element of $\mathbb{F}_{2^8}$

$\vec{a}_g = (a_0, a_1, \ldots, a_{14})$															p_g	$\lvert D_{g,p_g}\rvert$	nl_g	$\lvert L_{g,nl_g}\rvert$	$\overline{\lambda_g}$
ef	e1	11	b4	35	44	ea	9a	f2	d1	46	9c	18	56	80	4	3825	102	34	7
ef	e1	25	5	42	73	ab	82	cd	29	d3	17	ae	9f	e0	4	4029	106	102	7
ef	dd	3c	52	88	83	a8	59	29	6d	84	d9	4e	3a	f9	4	4029	102	17	7
ef	dd	79	86	2	9b	3f	2b	2d	70	4e	83	d5	e7	2a	4	4131	104	68	7
ef	de	9a	44	5	2	ab	73	8e	10	eb	5f	42	60	ae	4	4182	102	17	7
ef	de	34	70	10	c5	cd	83	22	ed	23	c0	ca	b8	cf	4	4233	104	17	7
ef	dd	43	86	16	73	df	3	bc	b8	ce	57	7e	7f	44	4	4233	104	34	7
ef	dd	3e	91	7c	e3	d6	da	b2	2	8f	33	17	fb	5c	4	4233	102	17	7
ef	dd	f9	c6	1b	5f	c0	7e	81	49	c1	d	b7	7f	6e	4	4233	102	34	7
ef	e1	be	14	20	f8	57	8a	52	d0	1f	db	16	22	a0	4	4233	100	17	7
ef	e3	23	a	15	83	d1	91	f	84	4c	94	bb	3e	d0	4	4284	106	102	7
ef	de	12	51	d8	c6	f	c3	91	f8	6a	a6	7b	d5	f5	4	4284	104	17	7
ef	de	63	bd	d6	f	6a	2c	16	62	78	70	fc	f3	41	4	4284	104	68	7
ef	e1	a	5c	e4	c7	5a	f3	45	e5	32	e8	74	8d	a2	4	4335	106	204	7
ef	dd	f8	ab	57	15	a4	2e	94	55	5f	7e	46	2d	31	4	4335	104	17	7
ef	e1	ac	63	8e	ed	b4	3c	46	f4	19	68	74	d4	6e	4	4335	104	34	7

Definition 8

A substitution $g \in S(\mathbb{F}_{2^n})$ is called *involutive* if for all $x \in \mathbb{F}_{2^n}$ we have $g(g(x)) = x$.

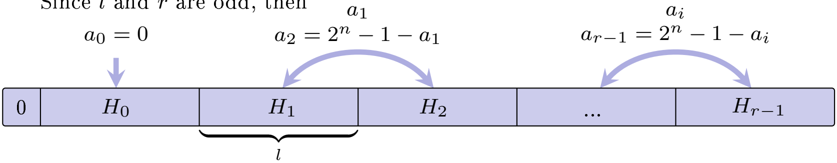
It is easy to see that function $g \in L_r(\mathbb{F}_{2^n})$ is involutive if and only if for any elements $i = 0, ..., r-1$ we have

$$a_i + a_{\pi(i)} \equiv 0 \bmod r,$$

where $\pi\colon \mathbb{Z}_r \to \mathbb{Z}_r$, $\pi(i) = (a_i + i) \mod r$, $i = 0, ..., r-1$.

Let $IL_r(\mathbb{F}_{2^n})$ be the set of all involutive piecewise-linear permutations from the set $L_r(\mathbb{F}_{2^n})$.

Since l and r are odd, then



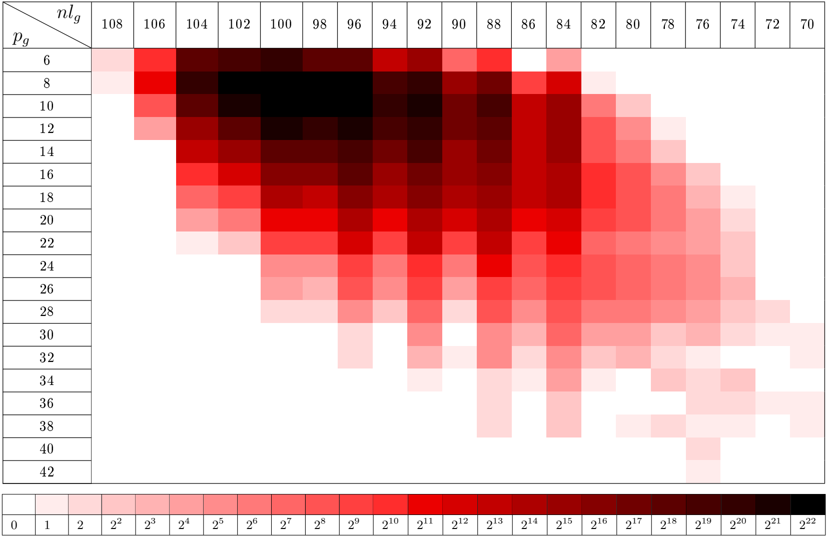
Proposition 6

For all $n > 1$ we have

$$|IL_r(\mathbb{F}_{2^n})| = 1 + \sum_{i=0}^{\frac{r-3}{2}} C_r^{2i+1} l^{\frac{r-2i-1}{2}} (r-2i-2)!!.$$

$$|\{g \in IL_r(\mathbb{F}_{2^n}) \,|\, |F(g)| = l+1\}| = \left(1 + l^{\frac{r-1}{2}} r!!\right) << l^r r! = |L_r(\mathbb{F}_{2^n})|.$$

The joint distribution of parameters p_g and nl_g for 10^8 randomly generated involutive permutations $g \in IL_{15}(\mathbb{F}_{2^8})$



Examples of differentially 4-uniform piecewise-linear involutions $g \in IL_{15}\left(\mathbb{F}_{2^8}\right)$ constructed using algorithm 3

Let $\mathbb{F}_{2^8} = {}^{\mathbb{F}_2[x]}/_{x^8+x^4+x^3+x+1}$, $\zeta = 3$ is a primitive field element of $\mathbb{F}_{2^8}$

$\vec{a}_g = (a_0, a_1, ..., a_{14})$															p_g	$\lvert D_{g,p_g}\rvert$	nl_g	$\lvert L_{g,nl_g}\rvert$	$\overline{\lambda_g}$
0	ee	dd	cc	bb	aa	99	88	77	66	55	44	33	22	11	4	255	112	1275	7
0	d3	2c	f3	c4	3b	c	25	12	1	fe	ed	2e	d1	da	4	3774	106	68	7
0	45	4d	15	b2	c5	d9	3a	6d	ea	ba	3f	92	26	c0	4	3876	104	51	7
0	27	74	79	86	25	88	77	15	c5	d8	3a	da	8b	ea	4	4029	104	17	7
0	b0	44	f6	d6	b6	62	49	29	9	bb	2	4f	fd	9d	4	4080	100	17	7
0	d	be	e9	5	21	a6	59	de	fa	7b	16	41	84	f2	4	4131	104	136	6
0	72	dd	8b	a0	51	ab	74	10	ef	8d	ae	54	22	5f	4	4131	102	34	7
0	e3	51	1c	21	db	d8	de	ae	f2	8a	d	27	75	24	4	4182	106	238	7
0	31	fb	7f	af	ce	d7	d4	d6	2b	80	28	29	4	50	4	4233	104	17	7
0	e2	1d	98	d8	67	3e	aa	c1	2	27	fd	55	1f	e0	4	4284	106	102	7
0	da	5	c4	3b	9b	7	fa	ba	25	64	88	77	f8	45	4	4335	108	646	7
0	d6	e9	7d	5c	29	a3	a9	82	14	16	56	79	86	eb	4	4386	104	119	7
0	af	c6	63	64	39	7f	6b	f2	94	d	50	9c	80	9b	4	4386	106	170	7
0	b0	93	c5	70	3a	2f	8d	d0	1	fe	8f	4f	72	6c	4	4437	104	187	6
0	4f	46	26	82	b0	5b	a4	50	a6	59	d9	b9	af	7d	4	4488	106	204	7
0	f7	dc	9c	f1	e	6a	95	8	63	40	6b	23	94	bf	4	4539	102	34	7

Definition 9

A permutation $g \in S(\mathbb{F}_{2^n})$ is called an *orthomorphism*[1–4] of the group $\mathbb{F}_{2^n}^+$ if the mapping $g' \colon \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ defined by the rule $g'(x) = x + g(x)$ is a permutation from $S(\mathbb{F}_{2^n})$.

It is well known[4] that function g is an orthomorphism if and only if $a_i \neq 0$ for all $i = 0, ..., r-1$ and bijective function $\pi' \colon \mathbb{Z}_r \to \mathbb{Z}_r$,

$$\pi'(i) = \left(\log_\zeta(\zeta^{a_i} + 1) + i\right) \bmod r, i = 0, ..., r-1.$$

Let $\mathrm{Orth}(\mathbb{F}_{2^n})$ be the set of all orthomorphisms of the group $\mathbb{F}_{2^n}^+$ and let $OL_r(\mathbb{F}_{2^n})$ be the set of all orthomorphisms from the set $L_r(\mathbb{F}_{2^n})$.

For $r = 1$ we have $|OL_1(\mathbb{F}_{2^n})| = 2^n - 2$.

For $r = 2^n - 1$ we have $|OL_{2^n-1}(\mathbb{F}_{2^n})| = \frac{|\mathrm{Orth}(\mathbb{F}_{2^n})|}{2^n}$.

Calculating $|\mathrm{Orth}(\mathbb{F}_{2^n})|$ for sufficiently large $n \in \mathbb{N}$ is an open problem.

1 Mann H. B. On orthogonal Latin squares. Bulletin of the American Mathematical Society, 1944, Vol. 50, Pp. 249–257.

2 Sachkov V. N. Deficiencies of finite group permutations. Tr. Diskr. Mat., 2003, T. 7, Pp. 156–175.

3 Niederreiter H. and Robinson K. Complete mappings of finite fields. Australian Mathematical Society, 1982, Vol. 33, Issue. 2, Pp. 197–212.

4 Evans A. Orthomorphisms graphs and groups. Springer-Verlag, Berlin, 1992, 114 p.

Examples of differentially 4-uniform piecewise-linear orthomorphisms $g \in OL_{15}(\mathbb{F}_{2^8})$ constructed using algorithm 3

Let $\mathbb{F}_{2^8} = {}^{\mathbb{F}_2[x]}/_{x^8+x^4+x^3+x+1}$, $\zeta = 3$ is a primitive field element of $\mathbb{F}_{2^8}$

$\vec{a}_g = (a_0, a_1, ..., a_{14})$															p_g	$\lvert D_{g,p_g} \rvert$	nl_g	$\lvert L_{g,nl_g} \rvert$	$\overline{\lambda_g}$
36	8e	b1	5c	3	ec	b0	50	a7	a	23	dc	a6	6e	84	4	4743	102	17	7
26	ee	f8	fa	3d	b8	d	63	ac	81	89	ec	fe	80	21	4	4845	104	34	7
b7	99	bb	85	2b	20	3e	16	89	15	6b	19	88	d	42	4	4998	102	17	7

Proposition 7

Let $g, g' \in L_r(\mathbb{F}_{2^n})$ given by the vectors $(a_0, a_1, ..., a_{r-1})$ and $(a'_0, a'_1, ..., a'_{r-1})$ respectively, $a_i, a'_i \in \{0, ..., 2^n - 2\}$, $i = 0, ..., r-1$, ζ is a primitive field element of $\mathbb{F}_{2^n}$. Then $g \overset{L}{\sim} g'$ if there exists such $j \in \{0, ..., 2^n - 2\}$ that for any $i = 0, ..., r-1$ we have

$$a'_i = (a_i + j) \bmod 2^n - 1.$$

Proposition 8

Let $g, g' \in L_r(\mathbb{F}_{2^n})$ given by the vectors $(a_0, a_1, ..., a_{r-1})$ and $(a'_0, a'_1, ..., a'_{r-1})$ respectively, $a_i, a'_i \in \{0, ..., 2^n - 2\}$, $i = 0, ..., r-1$, ζ is a primitive field element of $\mathbb{F}_{2^n}$. Then $g \overset{L}{\sim} g'$ if there exists such $j \in \{0, ..., r-1\}$ that for any $i = 0, ..., r-1$ we have

$$a'_i = a_{i+j \bmod r}.$$

Corollary

If under the conditions of proposition g is an involutive permutation, then g' is also an involutive permutation.

Corollary

If under the conditions of proposition g is an orthomorphism, then g' is also an orthomorphism.

Proposition 9

Let $g, g' \in L_r(\mathbb{F}_{2^n})$ given by the vectors $(a_0, a_1, ..., a_{r-1})$ and $\left(a'_0, a'_1, ..., a'_{r-1}\right)$ respectively, $a_i, a'_i \in \{0, ..., 2^n - 2\}$, $i = 0, ..., r-1$, ζ is a primitive field element of $\mathbb{F}_{2^n}$. Then $g \overset{L}{\sim} g'$ if there exists such $j \in \{1, ..., n-1\}$ that for any $i = 0, ..., r-1$ we have

$$a'_i = 2^{n-j} \cdot a_{i \cdot 2^j \bmod r} \bmod 2^n - 1.$$

Corollary

If under the conditions of proposition g is an involutive permutation, then g' is also an involutive permutation.

Corollary

If under the conditions of proposition g is an orthomorphism, then g' is also an orthomorphism.

The problem of checking linear equivalence between two partially given piecewise-linear permutations

Piecewise-linear permutation $g \in L_r(\mathbb{F}_{2^n})$ can be defined by the vector

$$\vec{a}_g = (a_0, a_1, ..., a_{r-1}),$$

where $a_i \in \{0, ..., 2^n - 2\}$, $i = 0, ..., r-1$.

We define mappings $\tau_1, \tau_2, \tau_3 \colon \{0, ..., 2^n - 2\}^r \to \{0, ..., 2^n - 2\}^r$ as follows

$$\tau_1(a_0, ..., a_{r-1}) = ((a_0 + 1) \bmod 2^n - 1, ..., (a_{r-1} + 1) \bmod 2^n - 1);$$

$$\tau_2(a_0, a_1, ..., a_{r-1}) = (a_1, a_2, ..., a_0);$$

$$\tau_3(a_0, ..., a_{r-1}) = \left(2^{n-1} \cdot a_0 \bmod 2^n - 1, ..., 2^{n-1} \cdot a_{r-1} \bmod 2^n - 1\right).$$

Let us associate the partially defined permutation $g \in L_r(\mathbb{F}_{2^n})$ with the vector

$$\vec{a}_g = \left(*, ..., *, a_{i_0}, *, ..., *, a_{i_1}, *, ..., *, a_{i_{d-1}}, *, ..., *\right),$$

where the symbol $*$ denotes undefined positions of the vector (the permutation g on the elements of the corresponding cosets is not defined). Two partially given vectors $\vec{a}_g$ и $\vec{a}_h$ are called linearly equivalent if there exist such $j_1 \in \{0, ..., 2^n - 2\}$, $j_2 \in \{0, ..., r-1\}$, $j_3 \in \{0, ..., n-1\}$ that we have

$$\vec{a}_h = \tau_3^{j_3}\left(\tau_2^{j_2}\left(\tau_1^{j_1}(\vec{a}_g)\right)\right).$$

Remark

Linear equivalence of vectors $\vec{a}_g$ and $\vec{a}_h$ can be checked when $d \mid r$ and for any $j = 0, ..., d-1$ we have $i_j \equiv c \bmod \frac{r}{d}$, $c = const$.

Example 2

Let $\mathbb{F}_{2^6} = \mathbb{F}_2[x] / _{x^6+x+1}$, $\zeta = 2$ is a primitive field element of $\mathbb{F}_{2^6}$. It is easy to see that the partially given vector $\vec{a}_g = (3c, *, *, 20, *, *, 21, *, *)$ linear equivalent to any partially given vector $\vec{a}_h$ from the following table.

j_1	j_2	j_3	$\vec{a}_h$								
6	3	3	3c	*	*	34	*	*	18	*	*
7	6	3	3c	*	*	20	*	*	5	*	*
18	0	4	3c	*	*	b	*	*	f	*	*
18	6	2	3c	*	*	33	*	*	2c	*	*
19	3	2	3c	*	*	d	*	*	4	*	*
24	3	1	3c	*	*	1c	*	*	2a	*	*
25	6	1	3c	*	*	b	*	*	1d	*	*
27	6	0	3c	*	*	18	*	*	3b	*	*
28	3	0	3c	*	*	3d	*	*	19	*	*
33	0	5	3c	*	*	6	*	*	4	*	*
42	0	3	3c	*	*	21	*	*	19	*	*
45	6	4	3c	*	*	2a	*	*	38	*	*
46	3	4	3c	*	*	1	*	*	2e	*	*
54	0	2	3c	*	*	35	*	*	6	*	*
60	0	1	3c	*	*	f	*	*	2e	*	*
60	3	5	3c	*	*	3a	*	*	33	*	*
61	6	5	3c	*	*	35	*	*	3e	*	*

Bounds on the differential uniformity of piecewise-linear permutations over the field $\mathbb{F}_{2^n}$

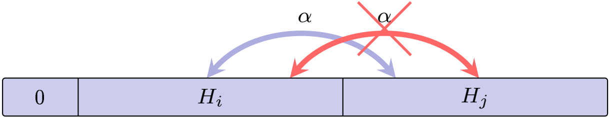
Obtaining bounds on the differential uniformity of piecewise-linear permutations is related to the study of the additive properties of multiplicative subgroups $\mathbb{F}_{2^n}^{\times}$.

Lemma 1

Let $n, r, l \in \mathbb{N}$, $2^n - 1 = rl$, ζ is a primitive field element of $\mathbb{F}_{2^n}$, $H = \langle \zeta^r \rangle$ is the subgroup of order l of $\mathbb{F}_{2^n}^{\times}$, $H_i = \zeta^i H$, $i = 0, ..., r-1$, $g \in L_r(\mathbb{F}_{2^n})$ is a permutation given by the set of pairwise distinct numbers $(a_0, a_1, ..., a_{r-1})$. Then the difference equation

$$g(x) + g(x + \alpha) = \beta, \alpha, \beta \in \mathbb{F}_{2^n}^{\times}$$

for any $i \neq j$ has at most one solution $x_1 \in H_i$ satisfying the condition $x_1 + \alpha \in H_j$.

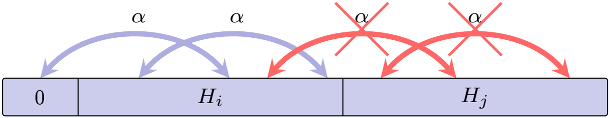


Lemma 2

Let $n, r, l \in \mathbb{N}$, $2^n - 1 = rl$, ζ is a primitive field element of $\mathbb{F}_{2^n}$, $H = \langle \zeta^r \rangle$ is the subgroup of order l of $\mathbb{F}_{2^n}^{\times}$, $H_i = \zeta^i H$, $i = 0, ..., r-1$, $g \in L_r(\mathbb{F}_{2^n})$ is a permutation given by the set of pairwise distinct numbers $(a_0, a_1, ..., a_{r-1})$. Let, in addition, the difference equation

$$g(x) + g(x+\alpha) = \beta, \alpha, \beta \in \mathbb{F}_{2^n}^{\times} \ (*)$$

have solutions $x_1, x_1 + \alpha \in H_i \cup \{0\}$. Then for any $j \neq i$ equation $(*)$ has no solutions $x_2 \in H_j$ satisfying the condition $x_2 + \alpha \in H_i \cup H_j$.



Bounds on the differential uniformity of piecewise-linear permutations over the field $\mathbb{F}_{2^n}$

Theorem

Let $n, r, l \in \mathbb{N}$, $2^n - 1 = rl$, ζ is a primitive field element of $\mathbb{F}_{2^n}$, $H = \langle \zeta^r \rangle$ is the subgroup of order l of $\mathbb{F}_{2^n}^{\times}$, $g \in L_r(\mathbb{F}_{2^n})$ is a permutation given by the set of pairwise distinct numbers $(a_0, a_1, ..., a_{r-1})$. Then we have lower and upper bounds on the differential uniformity of g:

$$\max\left\{\sum_{s=1}^{t}(-1)^{s+1}\sum_{n_1\le\ldots\le n_s}2^{\gcd(n_1,n_2,\ldots,n_s)}, 2\left\lfloor\frac{l+1}{2r}\right\rfloor\right\}\le$$

$$\le p_g \le$$

$$\le 2\max\left\{\lfloor\varphi(r,l)\rfloor, \varphi(r-1,l)+\right.$$

$$\left.+\max\left\{\lfloor\varphi(l/m_{n_t}, m_{n_t})\rfloor, \frac{m_{n_t}+1}{2}+\varphi(l/m_{n_t}-1, m_{n_t})\right\}\right\},$$

where $m_{n_1} < m_{n_2} < ... < m_{n_t}$ is the complete list of divisors of l of the form $m_{n_k} = 2^{n_k} - 1$, $k = 1, ..., t$, $\varphi\colon \mathbb{R}^2 \to \mathbb{R}$, $\varphi(x, y) = \frac{x \cdot \min\{x-1, y\}}{2}$.

Remark

The lower and upper bounds proved in the theorem for $r = 2^n - 1$ are also valid in the case when the numbers from the set $(a_0, a_1, ..., a_{r-1})$ are not pairwise distinct.

Theorem gives us necessary conditions for the existence of APN substitutions.

Corollary

If $g \in S(\mathbb{F}_{2^6})$, $p_g = 2$, $g(0) = 0$, then $g \in L_r(\mathbb{F}_{2^6})$, where $r \notin \{1, 3, 7, 9, 21\}$.

Corollary

If there is a permutation $g \in S(\mathbb{F}_{2^8})$ such that $p_g = 2$, $g(0) = 0$, then $g \in L_r(\mathbb{F}_{2^8})$, where $r \notin \{1, 3, 5, 17, 85\}$.

Remark

An upper bound for p_g is not always trivial for $r \geq 2^{n/2} + 1$. For example, if $g \in L_r(\mathbb{F}_{2^{12}})$, where $r \in \{91, 117, 195, 455\}$, then we have

$$p_g \leq 4094.$$

Let $n = 6$, $2^6 - 1 = rl$, $r, l \in \mathbb{N}$, ζ is a primitive field element of $\mathbb{F}_{2^6}$, $H = \langle \zeta^r \rangle$ is the subgroup of order l of $\mathbb{F}_{2^6}^{\times}$. The following table for different values of $l \in \{1, 3, 7, 9, 21, 63\}$ contains the minimum and maximum values of p_g among all permutations $g \in L_r(\mathbb{F}_{2^6})$. The table also contains the lower and upper bounds obtained in the theorem for the values p_g.

$\lvert H \rvert$	A lower bound on p_g	$\min\limits_{g \in L_r(\mathbb{F}_{2^6})} p_g$	$\max\limits_{g \in L_r(\mathbb{F}_{2^6})} p_g$	An upper bound on p_g
1	2	2	64	64
3	4	4	64	64
7	8	8	64	64
9	4	4	22	42
21	10	10	12	12
63	64	64	64	64

Let $n = 8$, $2^8 - 1 = rl$, $r, l \in \mathbb{N}$, ζ is a primitive field element of $\mathbb{F}_{2^8}$, $H = \langle \zeta^r \rangle$ is the subgroup of order l of $\mathbb{F}_{2^8}^{\times}$. The following table for different values of $l \in \{1, 3, 5, 15, 17, 51, 85, 255\}$ contains the best and worst known values of p_g for permutations $g \in L_r(\mathbb{F}_{2^8})$. The table also contains the lower and upper bounds obtained in the theorem for the values p_g.

$\lvert H \rvert$	A lower bound on p_g	Best-known example	A worst case example	An upper bound on p_g
1	2	4	256	256
3	4	4	256	256
5	2	4	216	256
15	16	16	256	256
17	2	4	56	210
51	12	12	20	64
85	30	30	32	88
255	256	256	256	256

Thanks for attention