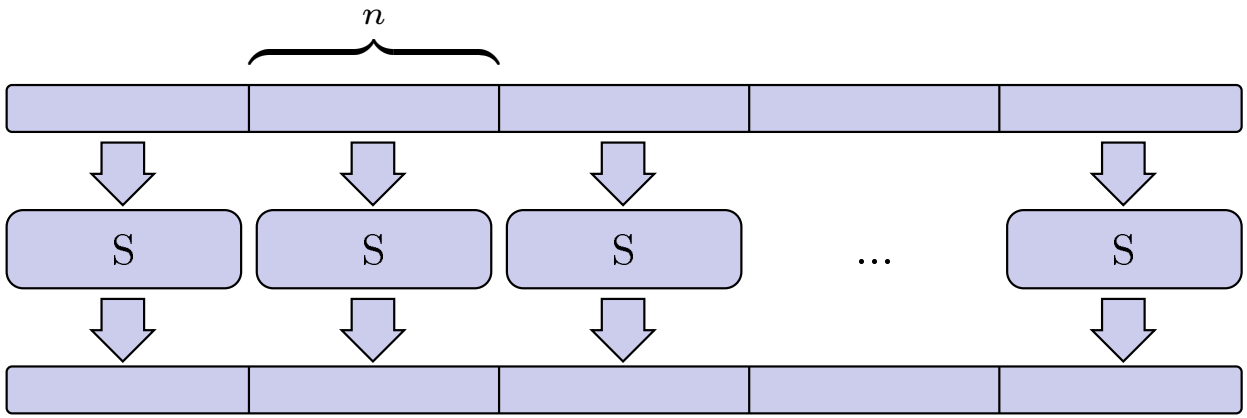
Bounds on the differential uniformity of piecewise-affine permutations over the field $\mathbb{F}_q$

Menyachikhin Andrey, Spiridonov Sergey

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.

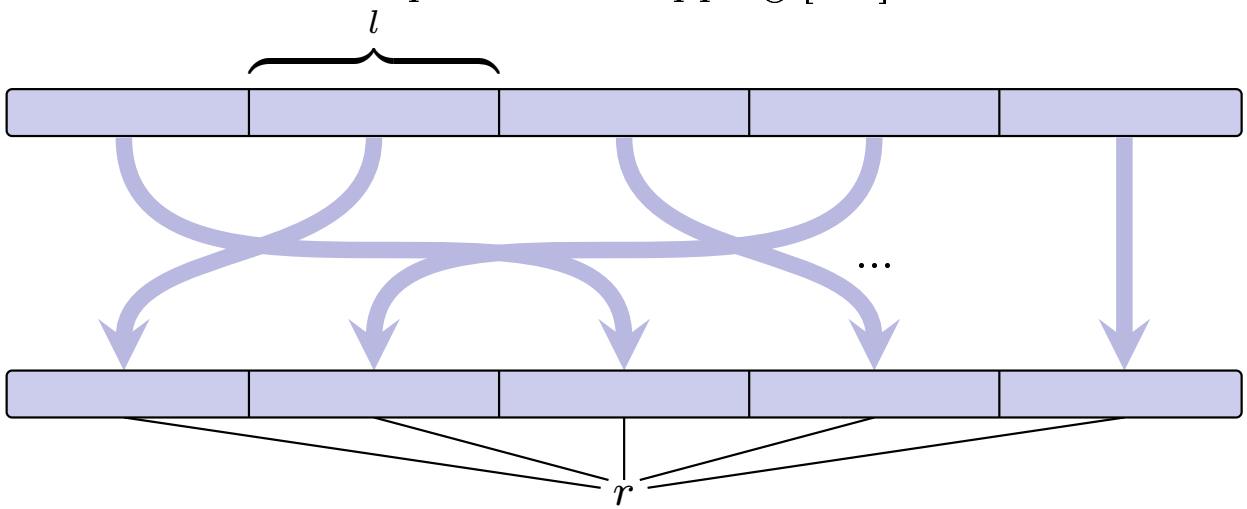
The confusion layer is often realized as a parallel application of nonlinear substitution boxes (S-boxes)



In this report, we give lower and upper bounds on the differential uniformity of piecewise-affine permutations over the field $\mathbb{F}_q$. The indicated permutations are relevant for use as s-boxes in block ciphers.

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

A piecewise mapping [1-9]



[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] Menyachikhin A.V. Adapted spectral-differential method for constructing differentially 4-uniform piecewise-linear substitutions, orthomorphisms, involutions over the field $\mathbb{F}_{2^n}$. Diskr. Mat., 35:2 (2023), pp. 42-47.

[6] Menyachikhin A.V. The differential uniformity of piecewise-linear substitutions over the field $\mathbb{F}_{2^n}$. Diskr. Mat., 35:4 (2023), pp. 58-68.

[7] Burov D., Kostarev S., Menyachikhin A. Class of piecewise-monomial mappings: differentially 4-uniform permutations of $\mathbb{F}_{2^8}$ with graph algebraic immunity 3 exist. In: Pre-proceedings of CTCrypt'23-Volgograd, Russia, (2023), pp. 219-235.

[8] 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.

[9] Pogorelov B.A., Pudovkina M.A. Classes of piecewise quasiaffine transformations on generalized quaternion group of order 2^m. Diskr. Mat., 34:2 (2022), pp. 50-66.

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

$$\mathbb{F}_q = \coprod_{i=0}^{r-1} H_{u_i,v_i} \sqcup \{v_r\}, \tag{1}$$

where $H_{u_i,v_i} = \zeta^{u_i} H + v_i, u_i \in \{0, ..., r-1\}$, $v_i, v_r \in \mathbb{F}_q$, $i = 0, ..., r-1$.

The partition (1) can be represented by a pair of vectors $\vec{u} = (u_0, ..., u_{r-1})$ and $\vec{v} = (v_0, ..., v_r)$.

Remark

Let $u_i = i$ for any $i = 0, ..., r-1$ and $v_i = 0$ for any $i = 0, ..., r$. Then $\mathbb{F}_q$ is partitioned into cosets of H:

$$\mathbb{F}_q = \bigsqcup_{i=0}^{r-1} H_{i,0} \sqcup \{0\}, i = 0, ..., r-1.$$

The existence of other partitions of the field $\mathbb{F}_q$ is studied, for example, in [1].

Let pairs of vectors $(\vec{u}, \vec{v})$ and $(\vec{u}', \vec{v}')$ is define two (not necessarily different) partitions $\bigsqcup_{i=0}^{r-1} H_{u_i,v_i} \sqcup \{v_r\}$ and $\bigsqcup_{i=0}^{r-1} H_{u'_i,v'_i} \sqcup \{v'_r\}$ of the field $\mathbb{F}_q$.

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

Definition 1

Piecewise-affine function[1] $g\colon \mathbb{F}_q \to \mathbb{F}_q$ is defined as

$$g(x) = \begin{cases} v'_r, & \text{if } x = v_r, \\ \zeta^{a_i}(x - v_i) + v'_{\pi(i)}, & \text{if } x \in H_{u_i, v_i}, \end{cases}$$

where $a_i = rk_i + u'_{\pi(i)} - u_i$, $k_i \in \{0, ..., l-1\}$, $i = 0, ..., r-1$, $\pi\colon \mathbb{Z}_r \to \mathbb{Z}_r$.

It's easy to see that function g is bijective if and only if bijective function $\pi\colon \mathbb{Z}_r \to \mathbb{Z}_r$.

Let $A^{\vec{u},\vec{v}}_{\vec{u}',\vec{v}'}(\mathbb{F}_q)$ be the set of all piecewise-affine permutations satisfying conditions of definition 1 and $\tilde{A}^{\vec{u},\vec{v}}_{\vec{u}',\vec{v}'}(\mathbb{F}_q)$ be the set of piecewise-affine permutations from $A^{\vec{u},\vec{v}}_{\vec{u}',\vec{v}'}(\mathbb{F}_q)$ having pairwise distinct elements a_i, $i = 0, ..., r-1$.

Remark

If $u_i = u'_i = i$ for any $i = 0, ..., r-1$ and $v_i = v'_i = 0$ for any $i = 0, ..., r$, then we have definition of *piecewise-linear function*

Definition 2

The differential uniformity p_g of the mapping $g\colon \mathbb{F}_q \to \mathbb{F}_q$ is defined as

$$p_g = \max_{\alpha \in \mathbb{F}_q^\times, \beta \in \mathbb{F}_q} p^g_{\alpha,\beta},$$

where

$$p^g_{\alpha,\beta} = |\{x \in \mathbb{F}_q \,|\, g(x+\alpha) - g(x) = \beta\}|.$$

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

Bounds on the differential uniformity of piecewise-affine permutations over the field $\mathbb{F}_q$

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

Lemma 1

Let $n, r \in \mathbb{N}$, p is a prime number, $q = p^n$, $r|q-1$, ζ is a primitive field element of $\mathbb{F}_q$, $g \in \tilde{A}^{\vec{u},\vec{v}}_{\vec{u}',\vec{v}'}(\mathbb{F}_q)$. Then the difference equation

$$g(x+\alpha) - g(x) = \beta, \alpha, \beta \in \mathbb{F}_q^\times$$

for any $i \neq j$ has at most one solution $x_1 \in H_{u_i,v_i}$ satisfying the condition $x_1 + \alpha \in H_{u_j,v_j}$ (fig. 1).

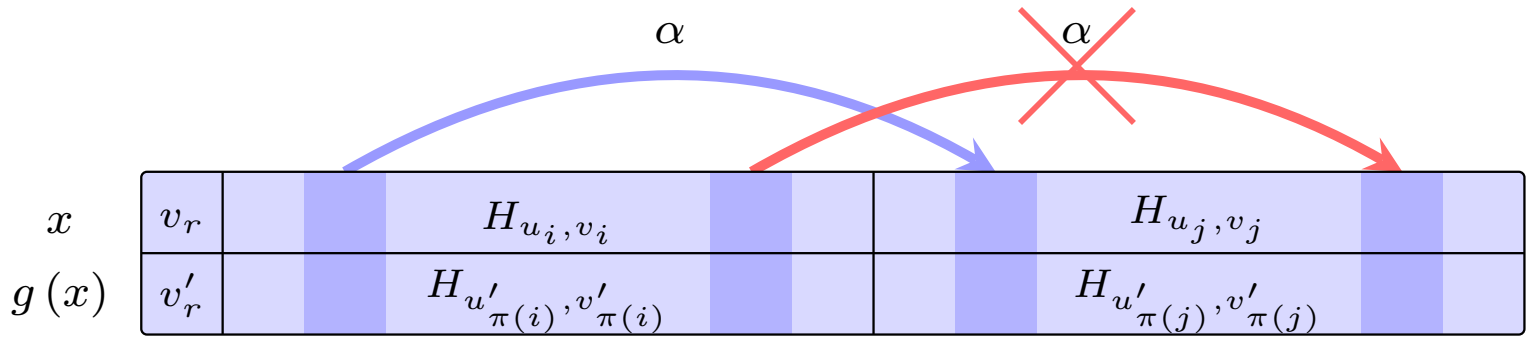


Figure 1

Lemma 2

Let $n, r \in \mathbb{N}$, p is a prime number, $q = p^n$, $r|q-1$, ζ is a primitive field element of $\mathbb{F}_q$, $g \in \tilde{A}^{\vec{u},\vec{v}}_{\vec{u}',\vec{v}'}(\mathbb{F}_q)$. Let, in addition, the difference equation

$$g(x+\alpha) - g(x) = \beta, \alpha, \beta \in \mathbb{F}_q^{\times}, \tag{2}$$

have solutions $x_1 \in H_{u_i,v_i} \cup \{v_r\}$ satisfying the condition $x_1 + \alpha \in H_{u_i,v_i} \cup \{v_r\}$. Then for any $j \neq i$ equation (2) has no solutions $x_2 \in H_{u_j,v_j}$ satisfying the condition $x_2 + \alpha \in H_{u_j,v_j}$ (fig. 2).

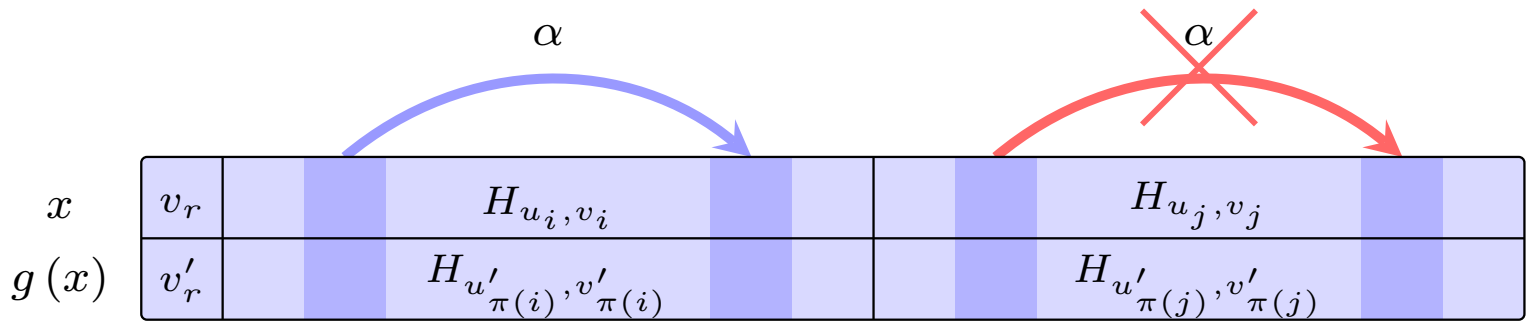


Figure 2

Bounds on the differential uniformity of piecewise-affine permutations over the field $\mathbb{F}_q$

Theorem

Let $n, r, l \in \mathbb{N}$, p is a prime number, $q = p^n$, $q - 1 = rl$, ζ is a primitive field element of $\mathbb{F}_q$, $H = \langle \zeta^r \rangle$ is the subgroup of order l of $\mathbb{F}_q^\times$, $g \in \tilde{A}^{\vec{u},\vec{v}}_{\vec{u}',\vec{v}'}(\mathbb{F}_q)$. Then we have lower and upper bounds on the differential uniformity of g:

$$\max\left\{2, \left\lceil \frac{l-1}{r} \right\rceil\right\} \leq$$

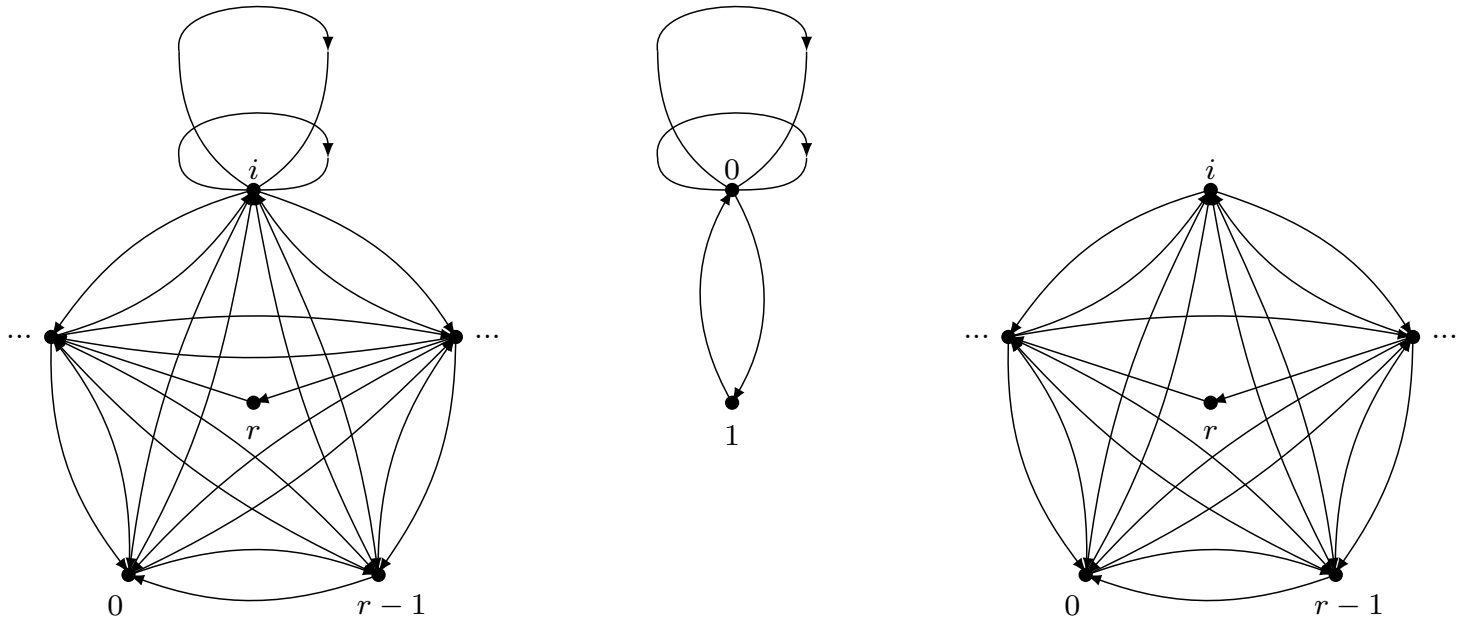
$$\leq p_g \leq$$

$$\leq (r-1)\min\{l, r-1\} + 2 + l - I_r(1) - I_{\min\{l,r-1\}}(l),$$

where $I_x(y) = \begin{cases} 1, & \text{if } x = y \\ 0, & \text{if } x \neq y \end{cases}$.

Let us consider the oriented pseudograph $\Gamma_{\alpha,\beta}$ in order to estimate from above the number of solutions of the difference equation $g(x+\alpha)-g(x)=\beta$.

$$\Gamma_{\alpha,\beta}=\left(\left\{0,...,r\right\},\left\{(i,j),i,j\in\{0,...,r\}\,\middle|\, g(x+\alpha)-g(x)=\beta, x\in H_{u_i,v_i}, x+\alpha\in H_{u_j,v_j}\right\}\right)$$



(a) $r\neq 1, r<l+1$ (b) $r=1$ (c) $r\neq 1, r\geq l+1$

Figure 3

The reachability of the lower and upper bounds on the differential uniformity of piecewise-affine permutations

The reachability of lower and upper bounds is related to the study of the properties of partitions over the field $\mathbb{F}_q$.

Proposition

Let $n \in \mathbb{N}$, p is prime number, $p > 2$, $q = p^n$, pairs of vectors $(\vec{u}, \vec{v}), (\vec{u}', \vec{v}') \in \{0, ..., q-2\}^{q-1} \times \mathbb{F}_q^q$ is define two (not necessarily different) partitions of the field $\mathbb{F}_q$. Let, in addition, the components of each of the vectors $\vec{u}$ and $\vec{u}'$ are pairwise different. Then we have

$$\left| \tilde{A}_{\vec{u}',\vec{v}'}^{\vec{u},\vec{v}}(\mathbb{F}_q) \right| = 0.$$

Let $p = 3$, $n = 3$, $p^n - 1 = rl$, $r, l \in \mathbb{N}$, ζ is a primitive field element of $\mathbb{F}_{3^3} = \mathbb{F}_3[x]/x^3 + 2x + 1$, $H = \langle \zeta^r \rangle$ is the subgroup of order l of $\mathbb{F}_{3^3}^{\times}$. The following table for different values of $l \in \{1, 2, 13, 26\}$ contains the best and worst values of p_g for permutations $g \in \tilde{A}_{\vec{u}',\vec{v}'}^{\vec{u},\vec{v}}(\mathbb{F}_q)$. The table also contains the lower and upper bounds obtained in the theorem for the values p_g.

Table 1.

l	A lower bound on p_g	A best case example $A_{\vec{u}',\vec{v}'}^{\vec{u},\vec{v}}(\mathbb{F}_{3^3})$	A worst case example $\tilde{A}_{\vec{u}',\vec{v}'}^{\vec{u},\vec{v}}(\mathbb{F}_{3^3})$	An upper bound on p_g
1	2	3	13	27
2	2	3	27	27
13	6	7	7	16
26	25	27	27	27

Let $p = 3$, $n = 4$, $p^n - 1 = rl$, $r, l \in \mathbb{N}$, ζ is a primitive field element of $\mathbb{F}_{3^4} = \mathbb{F}_3[x]/x^4 + x + 2$, $H = \langle \zeta^r \rangle$ is the subgroup of order l of $\mathbb{F}_{3^4}^{\times}$. The following table for different values of $l \in \{1, 2, 4, 5, 8, 10, 16, 20, 40, 80\}$ contains the best and worst known values of p_g for permutations $g \in \tilde{A}_{\vec{u}', \vec{v}'}^{\vec{u}, \vec{v}}(\mathbb{F}_q)$. The table also contains the lower and upper bounds obtained in the theorem for the values p_g.

Table 2.

l	A lower bound on p_g	A best case example $A_{\vec{u}', \vec{v}'}^{\vec{u}, \vec{v}}(\mathbb{F}_{3^4})$	A worst case example $\tilde{A}_{\vec{u}', \vec{v}'}^{\vec{u}, \vec{v}}(\mathbb{F}_{3^4})$	An upper bound on p_g
1	2	3	13	81
2	2	5	81	81
4	2	4	47	81
5	2	3	32	81
8	2	7	81	81
10	2	3	24	61
16	3	9	21	34
20	5	6	12	31
40	20	21	21	43
80	79	81	81	81

Let $p = 3$, $n = 5$, $p^n - 1 = rl$, $r, l \in \mathbb{N}$, ζ is a primitive field element of $\mathbb{F}_{3^5} = \mathbb{F}_3[x]/x^5 + 2x + 1$, $H = \langle \zeta^r \rangle$ is the subgroup of order l of $\mathbb{F}_{3^5}^{\times}$. The following table for different values of $l \in \{1, 2, 11, 22, 121, 242\}$ contains the best and worst values of p_g for permutations $g \in \tilde{A}_{\vec{u}', \vec{v}'}^{\vec{u}, \vec{v}}(\mathbb{F}_q)$. The table also contains the lower and upper bounds obtained in the theorem for the values p_g.

Table 3.

l	A lower bound on p_g	A best case example $A_{\vec{u}', \vec{v}'}^{\vec{u}, \vec{v}}(\mathbb{F}_{3^5})$	A worst case example $\tilde{A}_{\vec{u}', \vec{v}'}^{\vec{u}, \vec{v}}(\mathbb{F}_{3^5})$	An upper bound on p_g
1	2	4	12	243
2	2	6	77	243
11	2	4	45	243
22	2	6	34	124
121	60	61	61	124
242	241	243	243	243

Thanks for attention