Class of piecewise-monomial mappings: differentially 4-uniform permutations of $\mathbb{F}_{2^8}$ with graph algebraic immunity 3 exist

D.A. Burov, S.V. Kostarev, A.V. Menyachikhin

Definition

A mapping $f: \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is called differentially δ-uniform if the equation $f(x+a)+f(x)=b$ has at most δ solutions for every $a \in \mathbb{F}_{2^n}^*$, $b \in \mathbb{F}_{2^n}$. Minimal δ with this property is called the differential uniformity of f and denoted by $\delta(f)$.

Definition

A nonlinearity of a mapping $f: \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is called a value

$$nl(f) = 2^{n-1} - \frac{1}{2} \max_{u \in \mathbb{F}_{2^n}, v \in \mathbb{F}_{2^n}^*} |W_f(u,v)|,$$

where $W_f(u,v) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{tr_n(f(x)v+xu)}$.

Definition

A value

$$\deg(f) = \min_{\alpha \in \mathbb{F}_{2^n}^*} \deg(tr_n(\alpha f(x))),$$

is called the algebraic degree of a mapping $f: \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ and denoted by $\deg(f)$ where $\deg(tr_n(\alpha f(x)))$ is the degree of the ANF of a boolean function $tr_n(\alpha f(x))$. If $f \in S(\mathbb{F}_{2^n})$ than a value $\overline{\deg}(f) = \min\left\{\deg(f), \deg\left(f^{-1}\right)\right\}$ is called the generalized algebraic degree of a permutation f.

Definition

A graph algebraic immunity of mapping $f: \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is the algebraic immunity of the graph $\Gamma_f = \{(x, f(x)) | x \in \mathbb{F}_{2^n}\}$, and it is denoted by $AI(f)$.

Existing methods constructing of s-boxes

1. Algebraic methods: $x \mapsto x^{-1}$, monomial mappings.
2. Heuristic methods and algorithm optimization.
3. Using lower-dimensional s-boxes: butterfly structure, Feistel scheme, Lai-Massey scheme.

Some classes of permutations in which representatives with low δ-uniformity and high nonlinearity are relatively more common than in $S(V_n)$:

- involutions;
- piecewise-linear permutations;
- monomial permutations.

Definition

The set

$$\mathrm{Aut}(f) = \{\sigma \in AGL_{2n}(2) \,|\sigma(\Gamma_f) = \Gamma_f\}$$

is called the automorphism group of a mapping $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$.

- Involutions

$$(x, y) \mapsto (y, x)$$

- Piecewise-linear mappings

$$(x, y) \mapsto (x\zeta, y\zeta), \langle\zeta\rangle = H < \mathbb{F}_{2^n}^*$$

- Monomial mappings

$$(x, y) \mapsto (x\theta, y\theta^k), \langle\zeta\rangle = \mathbb{F}_{2^n}^*$$

- All well-known lower-dimensional APN-permutations have non-trivial automorphism group (Beierle C., Brinkmann M., Leander G. Linearly self-equivalent APN permutations in small dimension. IEEE Transactions on Information Theory, 2021, v. 67, i. 7, p. 4863-4875)

Empirical distribution of piecewise-linear permutations

$\lvert H\rvert = 3$	δ=2	δ=4	δ=6	δ=8	δ=10	δ=12
$nl = 80$	0	0	0	0	23	39
$nl = 82$	0	0	0	0	66	83
$nl = 84$	0	0	0	1	237	264
$nl = 86$	0	0	0	0	694	774
$nl = 88$	0	0	0	10	1937	2051
$nl = 90$	0	0	0	32	5070	5039
$nl = 92$	0	0	0	89	11301	9935
$nl = 94$	0	0	0	194	17428	13342
$nl = 96$	0	0	0	188	12502	7949
$nl = 98$	0	0	0	45	2040	1008
$nl = 100$	0	0	0	1	15	7
$nl = 102$	0	0	0	0	0	0
$nl = 104$	0	0	0	0	0	0
$nl = 106$	0	0	0	0	0	0
$nl = 108$	0	0	0	0	0	0
$nl = 110$	0	0	0	0	0	0
$nl = 112$	0	0	0	0	0	0

$\lvert H\rvert = 5$	δ=2	δ=4	δ=6	δ=8	δ=10	δ=12
$nl = 80$	0	0	0	0	4	2
$nl = 82$	0	0	0	0	9	10
$nl = 84$	0	0	0	3	31	24
$nl = 86$	0	0	0	6	134	40
$nl = 88$	0	0	0	48	566	244
$nl = 90$	0	0	0	186	2048	702
$nl = 92$	0	0	0	658	6073	1915
$nl = 94$	0	0	0	2033	15859	4542
$nl = 96$	0	0	0	4034	25620	6596
$nl = 98$	0	0	0	3283	17077	3643
$nl = 100$	0	0	0	509	1840	320
$nl = 102$	0	0	0	3	8	0
$nl = 104$	0	0	0	0	0	0
$nl = 106$	0	0	0	0	0	0
$nl = 108$	0	0	0	0	0	0
$nl = 110$	0	0	0	0	0	0
$nl = 112$	0	0	0	0	0	0

$\lvert H\rvert = 17$	δ=2	δ=4	δ=6	δ=8	δ=10	δ=12
$nl = 80$	0	0	0	0	1	0
$nl = 82$	0	0	0	0	1	1
$nl = 84$	0	0	0	0	8	7
$nl = 86$	0	0	0	3	43	34
$nl = 88$	0	0	0	26	165	122
$nl = 90$	0	0	0	141	593	290
$nl = 92$	0	0	1	633	1882	684
$nl = 94$	0	0	8	2265	4826	1427
$nl = 96$	0	0	23	6727	10434	2310
$nl = 98$	0	0	86	14401	15198	2406
$nl = 100$	0	0	178	15289	10455	1170
$nl = 102$	0	0	94	4227	1698	116
$nl = 104$	0	0	6	90	13	0
$nl = 106$	0	0	0	0	0	0
$nl = 108$	0	0	0	0	0	0
$nl = 110$	0	0	0	0	0	0
$nl = 112$	0	0	0	0	0	0

$\lvert H\rvert = 51$	δ=2	δ=4	δ=6	δ=8	δ=10	δ=12
$nl = 80$	0	0	0	0	1	0
$nl = 82$	0	0	0	0	0	0
$nl = 84$	0	0	0	0	0	0
$nl = 86$	0	0	0	0	0	0
$nl = 88$	0	0	0	0	0	0
$nl = 90$	0	0	0	0	0	0
$nl = 92$	0	0	0	0	0	0
$nl = 94$	0	0	0	0	0	0
$nl = 96$	0	0	0	0	0	53
$nl = 98$	0	0	0	0	0	0
$nl = 100$	0	0	0	0	0	0
$nl = 102$	0	0	0	0	0	0
$nl = 104$	0	0	0	0	0	0
$nl = 106$	0	0	0	0	0	0
$nl = 108$	0	0	0	0	0	0
$nl = 110$	0	0	0	0	0	0
$nl = 112$	0	0	0	0	0	0

Main Idea

«Good» permutations should be searched in classes with a nontrivial automorphism group.

Let us consider the partitions $\mathbb{F}_{2^n}^* = \bigcup_{i=0}^{r_H-1} H_i = \bigcup_{i=0}^{r_S-1} S_i = \bigcup_{i=0}^{r_D-1} D_i$ of $\mathbb{F}_{2^n}^*$ into cosets of subgroups $H, S, D = \langle H, S \rangle$.

Definition

A mapping $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is called k-piecewise-monomial on $H < \mathbb{F}_{2^n}^*$ if the following properties hold:

1. $f(0) = 0$,
2. there are $A_0, A_1, \ldots, A_{r_H-1} \in \mathbb{F}_{2^n}$ such that for every $x \in H_i$ the equality $f(x) = x^k A_i, i \in \{0, \ldots, r_H - 1\}$, holds.

Denote the set of k-piecewise-monomial on H mappings by $PM_{n,k}(H)$.

Automorphism group of mappings from $PM_{n,k}$ is nontrivial.

Proposition

Let $H = \langle\zeta\rangle$, $k \in \{0, \ldots, n-1\}$, then $f \in PM_{n,k}(H)$ if and only if mapping $(x, y) \mapsto (x\zeta, y\zeta^k)$, $x, y \in \mathbb{F}_{2^n}$, is an automorphism of f.

Necessary and sufficient condition for a k-piecewise-monomial mapping to be a bijection.

Proposition

Let $f \in PM_{n,k}(H)$, $f(x) = x^k A_i, x \in H_i$, where $H < \mathbb{F}_{2^n}^* = \langle\theta\rangle$, $H_i = H\theta^i$, $A_i = \theta^{a_i}$, $a_i \in \{0, \ldots, 2^n - 2\}$, $i = 0, \ldots, r_H - 1$. Then f is a bijection if and only if $\gcd(k, |H|) = 1$ and the set $\{a_i + ik \,|i \in \{0, \ldots, r_H - 1\}\}$ is a complete set of residues modulo r_H.

Proposition

Let $H < \mathbb{F}_{2^n}^*$, $k, k' \in \mathbb{N}$, then the following conditions are equivalent:

1) $PM_{n,k}(H) \cap PM_{n,k'}(H) \neq \{\mathbb{O}\}$, *where* $\mathbb{O}\colon x \mapsto 0$, $x \in \mathbb{F}_{2^n}$,
2) $|H| \mid k - k'$,
3) $PM_{n,k}(H) = PM_{n,k'}(H)$.

Proposition implies that it is enough to study k-piecewise-monomial mappings when $k \in \{0, \ldots, |H| - 1\}$. Mappings f and $g\colon x \mapsto f(x)^2$ are linear-equivalent and if $f \in PM_{n,k}(H)$ then $g \in PM_{n,2k}(H)$, where index $2k$ is taken modulo r_H. Hence if k, k' belong to the same cyclotomic class modulo $|H|$ then the differential δ-uniformity and the nonlinearity of a function $f \in PM_{n,k}(H)$ equal correspondingly to the differential δ-uniformity and the nonlinearity of an appropriate function $g \in PM_{n,k'}(H)$. Therefore, it is enough to study sets $PM_{n,k}(H)$ up to representatives of cyclotomic class modulo $|H|$.

Expansion of automorphism group I

To expand automorphism group of mappings from $PM_{n,k}(H)$ we search for mappings in the set

$$PM_{n,k}(H) \cap PM_{n,k\prime}(S), \text{ where } H, S < \mathbb{F}_{2^n}.$$

Proposition

Let $H, S < \mathbb{F}_{2^n}^* = \langle\theta\rangle$, $D = \langle H, S\rangle = \langle\psi\rangle$, $\psi = \theta^{r_D}$. *If* $f \in PM_{n,k}(H) \cap PM_{n,k'}(S)$, *then*

$$\langle (x,y) \mapsto (x\psi, y\psi^{ukr_{D,H} + vk'r_{D,S}}) \,|x, y \in \mathbb{F}_{2^n} \rangle < \mathrm{Aut}(f),$$

where u, v *satisfy* $r_D = r_H u + r_S v$.

Class $PM_{n,k}(H) \cap PM_{n,k\prime}(S)$

Here we consider mappings from $PM_{n,k}(H) \cap PM_{n,k'}(S)$. For this reason we use the double numeration for cosets of subgroups $H, S < \mathbb{F}_{2^n}^*$.

Definition

Let $S, H, D = \langle H, S \rangle = \langle \psi \rangle < \mathbb{F}_{2^n}^* = \langle \theta \rangle$, $\psi = \theta^{r_D}$. Let us define the following numeration of cosets:

$$D_i = D\theta^i, \quad i = 0, \ldots, r_D - 1,$$
$$H_{i,j} = H\theta^i\psi^j, \quad i = 0, \ldots, r_D - 1, j = 0, \ldots, r_{D,H} - 1,$$
$$S_{i,j} = S\theta^i\psi^j, \quad i = 0, \ldots, r_D - 1, j = 0, \ldots, r_{D,S} - 1.$$

It's easy to see that

$$D_i = \bigcup_{j=0}^{r_{D,H}-1} H_{i,j} = \bigcup_{j=0}^{r_{D,S}-1} S_{i,j}, \quad i = 0, \ldots, r_D - 1.$$

Class $PM_{n,k}(H) \cap PM_{n,k'}(S)$

Theorem

Let $H, S, D = \langle H, S \rangle < \mathbb{F}_{2^n}^* = \langle \theta \rangle$, and the numeration of cosets is defined. Let $f \in PM_{n,k}(H)$, $f\colon x \mapsto x^k A_{i,j}, x \in H_{i,j}$, $f \neq \mathbb{O}$, $\gamma_{H,S} = r_{D,S}^{-1} \mod r_{D,H}$. Then $f \in PM_{n,k'}(S)$, $f\colon x \mapsto x^{k'} B_{i,j}$, $x \in S_{i,j}$, if and only if $|H \cap S|$ divides $k' - k$ and for all $j_1, j_2 \in \{0, \ldots, r_{D,H} - 1\}$ the following equality holds

$$A_{i,j_1} = \theta^{r_S(k'-k)(j_1-j_2)\gamma_{H,S}} A_{i,j_2}, i \in \{0, \ldots, r_D - 1\}. \quad (1)$$

If the theorem's conditions are satisfied then the set of elements

$$\{B_{i,j} \,|i \in \{0, \ldots, r_D - 1\}, j \in \{0, \ldots, r_{D,S} - 1\}\}$$

is uniquely defined and can be obtained by the formula

$$B_{i,j} = \theta^{(k-k')(i-r_S j \gamma_{H,S})} A_{i,0}.$$

Properties of class $PM_{n,k}(H) \cap PM_{n,k'}(S)$

Proposition

1. *A mapping* $f \in PM_{n,k}(H) \cap PM_{n,k'}(S)$, $f\colon x \mapsto x^k A_{i,j}$, $x \in H_{i,j}$, $A_{i,j} = \theta^{a_{i,j}}$, $i = \{0, \ldots, r_D - 1\}$, $j = \{0, \ldots, r_{D,H} - 1\}$ *is a bijection if and only if* $\gcd(k, |H|) = 1$, $\gcd(r_D(k' - k + 1), r_H) = r_D$ *and the set* $\{a_{i,0} + ki \,|\, i \in \{0, \ldots, r_D - 1\}\}$ *is a complete set of residues modulo* r_D.
2. *Let* $H, S, D = \langle H, S \rangle < \mathbb{F}_{2^n}^*$, *then*

$$|PM_{n,k}(H) \cap PM_{n,k'}(S)| = \begin{cases} 2^{nr_D} & \text{if } |H \cap S| \mid k' - k, \\ 1 & \text{otherwise.} \end{cases}$$

$$|PM_{n,k}(H) \cap PM_{n,k'}(S) \cap S(\mathbb{F}_{2^n})| =$$

$$= \begin{cases} r_D! |D|^{r_D} & \text{if } |H \cap S| \mid k' - k, GCD(r_D(k' - k + 1), r_H) = r_D, \\ & GCD(k, |H|) = 1, \\ 0 & \text{otherwise.} \end{cases}$$

Expansion of automorphism group II

By $\sigma_m : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ we define an automorphism $x \mapsto x^{2^m}$ of the field $\mathbb{F}_{2^n}$.

Definition

Define the set $RS_{n,m}$, $m \mid n$ as a set of all mappings of a field $\mathbb{F}_{2^n}$ satisfying the following equality

$$f(\sigma_m(x)) = \sigma_m\left(f(x)\right), x \in \mathbb{F}_{2^n}.$$

Expansion of automorphism group II

Let $f \in PM_{n,k}(H)$, $f\colon x \mapsto x^k A_i$, $A_i \in \mathbb{F}_{2^n}$, $i = 0, \ldots, r_H - 1$. Let us describe necessary and sufficient conditions for $A_0, \ldots, A_{r_H-1}$ which imply that f belongs to $RS_{n,m}$.

Proposition

Let $\mathbb{F}_{2^n}^* = \bigcup_{i=0}^{r_H-1} H_i$ *— a partition of* $\mathbb{F}_{2^n}^*$ *into the cosets of subgroup* $H < \mathbb{F}_{2^n}^* = \langle\theta\rangle$, $H_i = H\theta^i$, $i = 0, \ldots, r_H - 1$, $f \in PM_{n,k}(H)$, $f\colon x \mapsto x^k A_i$, $x \in H_i$, $A_i \in \mathbb{F}_{2^n}$, $i = 0, \ldots, r_H - 1$. *Then* $f \in RS_{n,m}$ *if and only if for all* $i \in \{0, \ldots, r_H - 1\}$ *the equality* $A_i^{2^m} = A_{i2^m}$ *holds.*

Examples of differential 4-uniform piecewise monomial permutations with graph algebraic immunity equals to 3

Permutations $f \in PM_{8,k}(H)$, $|H| = 51$,
vector $\vec{a}_g \in \{0, ..., 2^8 - 2\}^5$ is written in hex-notation

k	$\vec{a}_g = (a_0, a_1, ..., a_4)$					$nl(f)$	$\overline{\deg}(f)$
7	3b	f1	7f	fa	26	104	5
	3b	ee	57	fb	50	104	5
	3b	a2	2e	32	b7	104	5
	3b	d5	46	b	84	100	5
	3b	e9	d7	e7	f2	104	5
	3b	2f	9c	12	f0	104	5
	3b	76	8d	c5	4b	104	5

Permutation $f \in PM_{8,k}(H)$, $|H| = 85$,
vector $\vec{a}_g \in \{0, ..., 2^8 - 2\}^3$ is written in hex-notation

k	a_0, a_1, a_2			$nl(f)$	$\overline{\deg}(f)$
3	f7	b0	4b	104	5

Examples of differential 4-uniform piecewise monomial permutations with graph algebraic immunity equals to 2

Permutations $f \in PM_{8,2}(H) \cap PM_{8,1}(S)$, $|H| = 17$, $|S| = 5$,
vector $\vec{a}_g \in \{0, ..., 2^8 - 2\}^{15}$ is written in hex-notation

k	$\vec{a}_g = (a_0, a_1, ..., a_{14})$															$nl(f)$	$\overline{\deg}(f)$
2	0	0	fc	39	39	36	72	72	6f	ab	ab	a8	e4	e4	e1	106	7
	0	bd	7b	39	f6	b4	72	30	ed	ab	69	27	e4	a2	60	112	7

Permutations $f \in PM_{8,2}(H) \cap PM_{8,1}(S)$, $|H| = 17$, $|S| = 3$,
vector $\vec{a}_g \in \{0, ..., 2^8 - 2\}^{15}$ is written in hex-notation

k	$\vec{a}_g = (a_0, a_1, ..., a_{14})$															$nl(f)$	$\overline{\deg}(f)$
2	0	fe	e4	89	d8	55	54	3a	de	2e	aa	a9	8f	34	83	102	7
	0	e	da	ad	6e	55	63	30	3	c3	aa	b8	85	58	19	106	7
	0	22	44	11	dd	55	77	99	66	33	aa	cc	ee	bb	88	104	5
	0	1	11	62	8b	55	56	66	b7	e0	aa	ab	bb	d	36	104	7
	0	1	34	ad	b3	55	56	89	3	9	aa	ab	de	58	5e	100	7
	0	1	84	e4	63	55	56	d9	3a	b8	aa	ab	2f	8f	e	104	7
	0	6	39	44	7c	55	5b	8e	99	d1	aa	b0	e3	ee	27	98	7
	0	dd	bb	99	77	55	33	11	ee	cc	aa	88	66	44	22	112	7
	0	0	e7	c9	c9	b1	93	93	7b	5d	5d	45	27	27	f	106	7

Examples of differential 4-uniform piecewise monomial permutations with graph algebraic immunity equals to 2

Permutations $f \in PM_{8,1}(H) \cap RS_{8,2}$, $|H| = 17$,
vector $\vec{a}_g \in \left\{0, ..., 2^8 - 2\right\}^{15}$ is written in hex-notation

k	$\vec{a}_g = (a_0, a_1, ..., a_{14})$															$nl(f)$	$\overline{\deg}(f)$
2	0	ee	dd	cc	bb	aa	99	88	77	66	55	44	33	22	11	112	7
	0	11	22	dd	44	aa	bb	cc	88	ee	55	66	77	33	99	108	7
	0	dd	bb	44	77	aa	88	66	ee	22	55	33	11	99	cc	104	5
	0	44	88	dd	11	aa	bb	66	22	ee	55	33	77	99	cc	104	6

Examples of differential 4-uniform piecewise monomial permutations with graph algebraic immunity equals to 3

Substitutions $f \in PM_{8,k}(H)$, $|H| = 17$,
vector $\vec{a}_g \in \{0, ..., 2^8 - 2\}^{15}$ is written in hex-notation

k	$\vec{a}_g = (a_0, a_1, ..., a_{14})$															$nl(f)$	$\overline{\deg}(f)$
3	7d	d3	92	f1	f6	3d	12	8f	86	0	36	cf	d7	c1	88	104	6
	6e	d0	7	ba	c0	ac	77	a7	1b	fd	e4	10	f8	b7	c2	100	6
	97	a7	f2	3a	1b	6	25	80	f4	f6	a9	8f	1a	8a	b7	104	6
	99	1	2	f5	da	f6	9	28	17	10	96	62	e2	4b	76	108	6
	c1	5b	7d	4b	9c	51	df	1d	1	a8	71	e	da	3	dc	104	6
	22	d4	9d	6f	a1	a	54	f8	35	95	45	4b	1e	f7	be	104	6
	9b	d3	b4	52	b5	1e	50	57	50	1e	45	25	92	fd	95	104	6
5	cb	eb	e	66	ba	80	16	3b	83	3e	d7	4e	e2	54	28	100	6
	5	f7	f3	5c	8a	ab	d9	b8	e1	3f	90	f5	bf	c2	92	104	6
	48	28	53	e6	54	1	5b	f3	63	ae	cf	1e	fd	a6	48	104	6
	e1	53	22	f3	b	94	a9	34	be	89	51	3b	70	79	4b	104	6
7	2	a6	3e	ba	60	2d	6c	36	7b	31	1e	f4	27	46	f1	104	6
	d3	d0	b0	c	46	48	de	af	2	da	ea	2b	58	56	67	104	6
	66	91	e5	79	c3	c2	40	64	d1	ab	fb	3f	7a	1d	5a	104	6
	df	76	82	8d	64	8c	bb	7b	8c	c3	7d	de	53	dc	58	104	6
	66	af	eb	b1	0	af	91	60	f3	8a	a0	ba	af	4b	a8	100	6
	2	67	8e	fa	46	8f	98	8a	9d	6a	c2	df	4c	82	e5	104	6
	7c	31	8e	7a	40	18	22	9f	56	60	3e	94	29	63	af	100	6
11	5	55	72	8b	4	49	43	e8	e5	b9	25	c2	59	2	f	104	6
	45	17	3c	e6	88	2	28	b	4	92	df	dc	9	3e	64	100	6
	f3	c6	f8	6e	bb	55	3a	82	c3	2d	50	f	5	fe	d9	104	6
	3f	6	8b	fb	2f	b1	31	98	56	7c	4e	b8	c3	16	4d	104	6
	b7	90	de	ef	df	5d	3	d	35	5c	fb	7e	3e	20	7c	100	6
	95	66	a4	db	9b	b9	e5	e	5	71	78	6	a6	8a	14	104	6
	a	b1	73	7c	4b	7a	2a	83	94	f0	2c	23	e4	e9	d3	104	6

Examples of differential 4-uniform piecewise monomial permutations with graph algebraic immunity equals to 3

Permutations $f \in PM_{8,k}(H)$, $|H| = 15$,
vector $\vec{a}_g \in \{0, ..., 2^8 - 2\}^{17}$ is written in hex-notation

k	$\vec{a}_g = (a_0, a_1, ..., a_{16})$																	$nl(f)$	$\overline{\deg}(f)$
7	c7	d9	46	88	ac	3a	ef	7f	55	c	40	a	fd	b6	1f	fc	89	102	7
	13	b	78	99	64	d2	46	98	e9	f9	4f	bd	c8	35	91	88	39	104	7