Some cryptographic properties of piecewise–monomial permutations of $\mathbb{F}_{2^n}$

Burov Dmitry, Kostarev Sergei

At the CTCrypt 2023 conference, a class of piecewise–monomial mappings over $\mathbb{F}_{2^n}$ was introduced and investigated. It was also experimentally shown that this class (at n $= 8$) contains permutations with high cryptographic characteristics:

- differential δ-uniformity
- algebraic degree
- nonlinearity
- graph algebraic immunity

D.A. Burov, S.V. Kostarev, A.V. Menyachikhin (CTCrypt 2023)

Using adapted spectral-differential method, we find differentially 4-uniform permutations over $\mathbb{F}_{2^8}$ with graph algebraic immunity 3.

Definition

Let n, δ be positive integers. A function $f\colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ is called differentially δ-uniform if, for every nonzero $a \in \mathbb{F}_2^n$ and every $b \in \mathbb{F}_2^n$, the equation $f(x) + f(x+a) = b$ has at most δ solutions. The minimum of those values δ having such property, that is, the maximum number of solutions of such equations, is denoted by δ_f and called the differential uniformity of f.

Definition

A nonlinearity of a function $f\colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ is called a value

$$nl(f) = 2^{n-1} - \frac{1}{2} \max_{u \in \mathbb{F}_2^n, v \in \mathbb{F}_2^n \setminus \{0\}} |W_f(u,v)|,$$

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

S-boxes with the low differential δ-uniformity and the high nonlinearity increase the resistance of block ciphers against differential and linear cryptanalysis.

Definition

The value

$$\deg(f) = \max_{\alpha \in \mathbb{F}_2^n \setminus \{0\}} \deg(\alpha \cdot f(x)),$$

is called the algebraic degree of a function $f\colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ and denoted by $\deg(f)$ where $\deg(\alpha \cdot f(x))$ is the degree of the ANF of a boolean function $\alpha \cdot f(x) = f_\alpha(x)$. Boolean function $f_\alpha(x)$ is called component function of $f(x)$.

S-boxes with the high generalized algebraic degree increase the resistance of block ciphers against algebraic cryptanalysis.

Definition

A graph algebraic immunity of a function $f\colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ is the algebraic immunity of the graph $\Gamma_f = \{(x, f(x)) | x \in \mathbb{F}_2^n\}$, and it is denoted by $AI(f)$.

S-boxes with the high graph algebraic immunity increase the resistance of block ciphers against XSL-method.

k-piecewise–monomial mappings

The partition $\mathbb{F}_{2^n}^* = \bigcup_{i=0}^{r_H-1} H_i$ of $\mathbb{F}_{2^n}^*$ into cosets of subgroups H is fixed.

Definition

A function $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ 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 functions by $PM_{n,k}(H)$.

Denote the set of piecewise-linear on H functions by $PL_n(H) = PM_{n,1}(H)$.

Cryptographic properties of piecewise-linear permutations were studied by Trishin A. E. and Menyachikhin A. V.

A characteristic feature of this class is that the functions have a non-trivial automorphism group.

Definition

The set

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

is called the automorphism group of a mapping $f : \mathbb{F}_2^n \to \mathbb{F}_2^n$, where $\Gamma_f = \{(x, f(x)) | x \in \mathbb{F}_2^n)\}$.

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.

Main idea

The automorphism group "symmetrizes" the function. Therefore, in some cases cryptographic characteristics can be studied up to the values on the representatives of the orbits of the action of the group $Aut(f)$ on Γ_f.

Such characteristics include:

- differential δ-uniformity
- nonlinearity
- etc.

Every function from $\mathbb{F}_{2^n}$ into $\mathbb{F}_{2^n}$ admits a (unique) representation as a polynomial over $\mathbb{F}_{2^n}$ in one variable and of (univariate) degree at most $2^n - 1$. We described the type of polynomials that define piecewise–monomial mappings over $\mathbb{F}_{2^n}$.

Proposition

A function $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is k-piecewise–monomial on $H < \mathbb{F}_{2^n}^*$, $|H| = l$, if and only if f admits a representation $F(x)$ as a univariate polynomial over $\mathbb{F}_{2^n}$ of the form

$$F(x) = x^k G(x^l)$$

where $G(x) \in \mathbb{F}_{2^n}[x]$, $\deg G(x) \leq r_H - 1$.

Piecewise affine transformations were described and the form of a polynomial defining piecewise affine transformations was given. (Bugrov A. D., "Piecewise affine transformations of finite field", 2015)

The type of polynomial of piecewise-monomial functions were previously mentioned in the literature

- Hou X.D., "Permutations polynomials over finite fields — a survey of resent advances", 2015.
- Jeong J., Kim C.H., Koo N., KwonS., Lee S., "On cryptographic parameters of permutation polynomials of the form $x^r h(x^{\frac{q-1}{d}})$", 2022.
- Zhu X., Zeng X., Chen Y., "Some binomial and trinomial differentially 4–uniform permutation polynomials", 2015.

The algebraic degree of a function $f\colon \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ can be evaluated from its univariate representation $F(x) = \sum_{i=0}^{2^n-1} \delta_i x^i$:

$$\deg f = \max_{\substack{i=0,1,\ldots,2^n-1:\\ \delta_i \neq 0}} \omega_2(i),$$

where $\omega_2(j)$ is binary weight of j.

Therefore, describing $\deg f$, $f \in PM_{n,k}(H)$, is equal to describing the spectrum of binary weights of the degrees of the monomes:

$$\{k + ls | s = 0, 1 \ldots, r_H - 1\},$$

where $2^n - 1 = r_H l$.

It is not difficult to specify some classes of k-piecewise-monomial mappings containing mappings with algebraic degree $n-1$ (the maximum possible value for permutations). To do this, it is sufficient to consider the degrees of the monomials of the univariate polynomial over $\mathbb{F}_{2^n}$ which represents $f \in PM_{n,k}(H)$, $|H| = l$:

$$\{k + ls | s = 0, 1, \ldots, r_H - 1\}$$

and specify the cases when in a given set of degrees there is a number d whose binary weight is $\omega_2(d) = n - 1$.

Table: Some classes $PM_{n,k}(H)$ in which the maximum algebraic degree for permutations is achieved

n	k	$\lvert H\rvert$	The maximum algebraic degree in the class
$2m$	1	2^m+1	$n-1$
$2m$, $m \underset{(2)}{\equiv} 1$	1	2^b-1, $b \mid m$	$n-1$
$2m$	$2+2^3+\ldots 2^{2v-1}$, $v \geq 1$	$r_H = 3$	$m+v$

Table: The spectrum of algebraic degree of k-piecewise–monomial mappings $PM_{8,k}(H)$ over $\mathbb{F}_{2^8}$

$\lvert H\rvert$	k	deg	$\lvert H\rvert$	k	deg
3	1	1,2,3,4,5,6,7	85	1	1,4,5
5	1	1,2,3,4,5,6,7		3	2,3,5
15	1	1,2,3,4,5		5	2,4,6
	3	2,3,4,5,6		7	3,4
	5	2,3,4,5,6		9	2,5
	7	3,4,5,6,7		13	3,6
17	1	1,2,3,4,5,6,7		15	3,4,5
	3	2,3,4,5,6		17	2,4,6
51	1	1,3,4,5		21	3,4,7
	3	2,4,6		29	4,5
	5	2,3,4,5		37	3,5,6
	9	2,3,4,5,6			
	11	3,4,5,6			
	17	2,4,6			
	19	3,4,5,7			

Let $M \subset \mathbb{F}_{2^n}$. Define $(M)_{\mathbb{F}_2}$ as linear span of the set M over $\mathbb{F}_2$.

Theorem

If $f \in PM_{n,k}(H)$, $gcd(k, |H|) = 1$ *and* $(H)_{\mathbb{F}_2} = \mathbb{F}_{2^n}$, *then*

$$\min_{\lambda \in \mathbb{F}_{2^n}^*} \deg f_\lambda = \max_{\lambda \in \mathbb{F}_{2^n}^*} \deg f_\lambda.$$

Theorem

Let $n, r_H, l \in \mathbb{N}$, $2^n - 1 = r_H l$, θ — *primitive element of the field* $\mathbb{F}_{2^n}$, $H = \langle \theta^{r_H} \rangle$ *is subgroup of* $\mathbb{F}_{2^n}^*$, $|H| = l$, $f \in PM_{n,k}(H)$ *and* $A_j = \theta^{a_j}$, $j = 0, \ldots, r_H - 1$, $3 \leq r_H \leq \frac{\sqrt{2^n}+1}{k}$.

1. *If* k *belongs to the same cyclotomic class as* 1 *modulo* l *and the elements* $a_j \in \{0, 1, \ldots, 2^n - 2\}$, $j = 0, \ldots, r_H - 1$ *are all distinct, then*
$$nl(f) \geq \frac{\sqrt{2^n}(r_H - 1)(\sqrt{2^n} - r_H + 1)}{2r_H}.$$
2. *If* k *does not belong to the same cyclotomic class as* 1 *modulo* l, *then*
$$nl(f) \geq \frac{1}{2}\left(2^n - (r_H k' - 1)\sqrt{2^n}\right),$$
where k' *is the minimum element of a cyclotomic class modulo* l *with a representative* k.

Previous result

Trishin A.E., "The nonlinearity index for a piecewise-linear substitution of the additive group of the field $\mathbb{F}_{2^n}$", 2015.

Table: Lower bounds for the nonlinearity of k-piecewise–monomial mappings over $\mathbb{F}_{2^8}$ obtained using the theorem

r_H	k	Lower bound for $nl(f)$
3	1	75
	3	64
	5	16
15	1	15
5	1	77
	3	16

Table: The actual lower values of the nonlinearity of k-piecewise–monomial mappings over $\mathbb{F}_{2^8}$ obtained as a result of brute force search

r_H	k	Lower values for $nl(f)$
3	1	80
	3	96
	5	86

When constructing cryptographically strong S-box, we want to guarantee the high nonlinearity nl and the low differential δ-uniformity.

Note that in general case, low differential δ-uniformity doesn't imply high nonlinearity. Also high nonlinearity doesn't imply low differential δ-uniformity.

Only in the case of APN permutations is it possible to prove the lower bound of $nl(f) > 0$, but nothing more consistent can be said.

Beierle C., Leander G., 2020

There are differential 4-uniform permutations with null nonlinearity.

In the special case when $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$, $f(x) = x^k$, $gcd(k, 2^n - 1)$, we can prove that $nl(f) \geq 2^{n-1} - 2^{\frac{3n-4}{4}} \sqrt[4]{\delta}$.

We have generalized this fact to the case of $PM_{n,k}(H)$.

Proposition

If $f \in PM_{n,k}(H)$, $|H| = l$, $2^n - 1 = lr_H$, $gcd(k, l) = 1$ *and* $\delta_f = \delta$, *then*

$$nl(f) \geq 2^{n-1} - 2^{\frac{3n-4}{4}} \sqrt[4]{r_H \delta}.$$

As a consequence, we obtain a previously proven result.

Corollary (Charpin P., Peng J.(2019))

If $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$, $f(x) = x^k$ *and* $gcd(k, 2^n - 1) = 1$, *then*

$$nl(f) \geq 2^{n-1} - 2^{\frac{3n-4}{4}} \sqrt[4]{\delta}.$$

Table: A lower bound on the nonlinearity of k-piecewise–monomial permutations with a given δ-uniformity

δ	r_H	Lower bound for $nl(f)$
4	3	69
	5	61
	15	39
	17	37

δ	r_H	Lower bound for $nl(f)$
6	3	63
	5	54
	15	30
	17	27

To every Boolean function on $\mathbb{F}_2^n \times \mathbb{F}_2^n$ of multivariate degree ≤ 2 corresponds a function $g(x, y)$ over $\mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$:

1. If n is even, $n = 2m$, then

$$g(x,y) = tr_{2m}(v_0 x + b_0 y) + \sum_{1 \leq k \leq m-1} tr_{2m}(v_k x^{2^k+1} + b_k y^{2^k+1}) +$$

$$+ tr_m(v_m x^{2^m+1} + b_m y^{2^m+1}) + tr_{2m}(y \cdot (c_0 x^{2^0} + c_1 x^{2^1} + \cdots + c_{n-1} x^{2^{n-1}})) + v,$$

where

$$v \in \mathbb{F}_2, v_0, \ldots, v_{m-1}, b_0, \ldots, b_{m-1}, c_0, \ldots, c_{n-1} \in \mathbb{F}_{2^{2m}}, v_m, b_m \in \mathbb{F}_{2^m}.$$

2. If n is odd, $n = 2m + 1$, then

$$g(x,y) = tr_n(v_0 x + b_0 y) + \sum_{1 \leq k \leq m} tr_n(v_k x^{2^k+1} + b_k y^{2^k+1}) +$$

$$+ tr_n(y \cdot (c_0 x^{2^0} + c_1 x^{2^1} + \cdots + c_{n-1} x^{2^{n-1}})) + v,$$

where

$$v \in \mathbb{F}_2, v_0, \ldots, v_{m-1}, b_0, \ldots, b_{m-1}, c_0, \ldots, c_{n-1} \in \mathbb{F}_{2^n}.$$

Definition

A function $g(x, y)$ on $\mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$ of multivariate degree ≤ 2 is called quadratic relation for the function $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ if

$$g(x, f(x)) = 0, \ \forall x \in \mathbb{F}_{2^n}.$$

If the function f has a quadratic relation $g(x, y)$ then $AI(f) \leq 2$.

Table: Quadratic relations for mappings from $PL_n(H)$

n	Conditions	The lower bound for the number of quadratic relations	The type of quadratic relations
$2m$	$\lvert H\rvert = 2^s + 1$, $s \neq m$, $4n > r_H$	$2^{4n-r_H} - 1$	$tr_n(v_s x^{2^s+1} + b_s y^{2^s+1} + c_s y x^{2^s} + c_{n-s} y x^{2^{n-s}})$

n	$\lvert H\rvert$	The lower bound for the number of quadratic relations of the specified type	
		for mapping from $PL_n(H)$	for arbitrary mapping over $\mathbb{F}_{2^n}$
4	3	$2^{11} - 1$	0
6	3	$2^3 - 1$	0

Table: Quadratic relations for mappings from $PL_n(H)$

n	Conditions	The lower bound for the number of quadratic relations	The type of quadratic relations
$2m$	$\lvert H\rvert = 2^m + 1$, $4m > 2^m - 1$	$2^{4m-2^m+1} - 1$	$tr_m(v_m x^{2^m+1} + b_m y^{2^m+1}) + tr_{2m}(c_m y x^{2^m})$

n	$\lvert H\rvert$	The lower bound for the number of quadratic relations of the specified type	
		for mapping from $PL_n(H)$	for arbitrary mapping over $\mathbb{F}_{2^n}$
4	5	$2^5 - 1$	0
6	9	$2^5 - 1$	0
8	17	1	0

All piecewise–linear mappings on the index 3 subgroup have graph algebraic immunity equal to 2.

Table: Quadratic relations $g_k(x, y)$ for mappings from $PL_{2m}(H)$ in case $r_H = 3$

k	The lower bound for the number of quadratic relations $g_k(x, y)$	The type of quadratic relations $g_k(x, y)$
$1 \le k \le m-1$	$2^{2m}-1$	$tr_{2m}(v_k x^{2^k+1} + b_k y^{2^k+1} + c_k y x^{2^k} + c_{2m-k} y x^{2^{2m-k}})$
$k = m$	2^m-1	$tr_m(v_m x^{2^m+1} + b_m y^{2^m+1}) + tr_{2m}(c_m y x^{2^m+1})$

Table: Quadratic relations for mappings from $PM_{2m,k}(H)$ in case $r_H = 3$

Conditions	The lower bound for the number of quadratic relations	The type of quadratic relations
$\exists d \in \mathbb{N}$: $d < m$, $d \mid m$, $\frac{2^m-1}{2^d-1} \mid k$	$2^{2m} - 1$	$tr_m(\gamma y^{2^m+1})$
$\exists t \in \mathbb{N}$: $2^m + 1 \mid 2^t + k$	$2^m - 1$	$tr_m(\gamma y x^{2^t})$

When studying classes of discrete maps, the classical question is to describe a group of transformations that stabilizes this class as a set.

- Resilient functions (Hou X.D., 2003)
- Bent-functions (Tokareva N., N., 2010)
- Galois-closed subalgebras of the Sheffer algebra (Tarasov A. V., 2015)
- etc.

The paper studies the subgroup $Stab_{GL_n(2)\times GL_n(2)}(PM_{n,k}(H))$ of $GL_n(2) \times GL_n(2)$, stabilizing the set of k-piecewise–monomial mappings, i.e.

$$Stab_{GL_n(2)\times GL_n(2)}(PM_{n,k}(H)) =$$
$$= \left\{(L_1, L_2) \in GL_n(2) \times GL_n(2) \,\middle|\, L_1^{-1} PM_{n,k}(H) L_2 = PM_{n,k}(H) \right\}.$$

Theorem

If $H < \mathbb{F}_{2^n}^*$ and $\mathbb{F}_{2^m}$ is the minimal subfield of $\mathbb{F}_{2^n}^*$ containing the group H, $gcd(k, |H|) = 1$, then

$$\{((g,\varphi),(h,\psi)) \in (GL_d(2^m) \rtimes Aut(\mathbb{F}_{2^m})) \times (GL_d(2^m) \rtimes Aut(\mathbb{F}_{2^m})) \mid \psi = \varphi\} < Stab_{GL_n(2)\times GL_n(2)}(PM_{n,k}(H)),$$

where $d = \frac{n}{m}$.

It has been experimentally verified that for all subgroups $H < \mathbb{F}_{2^4}^*$ and $gcd(k, |H|) = 1$, $Stab_{GL_4(2)\times GL_4(2)}(PM_{4,k}(H))$ coincides with the described subgroup.

Thank you for your attention!