Москва, РусКрипто-2018. https://www.ruscrypto.ru/resource/archive/rc2018/files/02_Dmukh_Trifonov_Chukhno.pdf.

6. *Beaulieu R., Shors D., Smith J., et al.* The SIMON and SPECK families of lightweight block ciphers. https://eprint.iacr.org/2013/404.pdf.

UDC 621.391:519.7 DOI 10.17223/2226308X/12/42

A METHOD FOR CONSTRUCTING PERMUTATIONS, INVOLUTIONS AND ORTHOMORPHISMS WITH STRONG CRYPTOGRAPHIC PROPERTIES

R. A. de la Cruz Jiménez

S-Boxes are crucial components in the design of many symmetric ciphers. To construct permutations having strong cryptographic properties is not a trivial task. In this work, we propose a new scheme based on the well-known Lai-Massey structure for generating permutations of dimension $n = 2k$, $k \geqslant 2$. The main cores of our constructions are: the inversion in $\mathrm{GF}(2^k)$, an arbitrary k-bit non-bijective function (which has no pre-image for 0) and any k-bit permutation. Combining these components with the finite field multiplication, we provide new 8-bit permutations without fixed points possessing a very good combination for nonlinearity, differential uniformity and minimum degree — (104; 6; 7) which can be described by a system of polynomial equations with degree 3. Also, we show that our approach can be used for constructing involutions and orthomorphisms with strong cryptographic properties.

Keywords: *S-Box, permutation, Boolean functions.*

Let V_n be n-dimensional vector space over the field $\mathrm{GF}(2)$, by $S(V_n)$ we denote the symmetric group on set of 2^n elements. The finite field of size 2^n is denoted by $\mathrm{GF}(2^n)$, where $\mathrm{GF}(2^n) = \mathrm{GF}(2)[\xi]/g(\xi)$, for some irreducible polynomial $g(\xi)$ of degree n. We use the notation $\mathbb{Z}/2^n$ for the ring of the integers modulo 2^n. There are bijective mappings between $\mathbb{Z}/2^n$, V_n, and $\mathrm{GF}(2^n)$ defined by the correspondences:

$$\left[a_{n-1} \cdot 2^{n-1} + \ldots + a_0\right] \quad \leftrightarrow \quad (a_{n-1}, \ldots, a_0) \quad \leftrightarrow \quad \left[a_{n-1} \cdot \xi^{n-1} + \ldots + a_0\right].$$

Using these mapping in what follows, we make no difference between vectors of V_n and the corresponding elements in $\mathbb{Z}/2^n$ and $\mathrm{GF}(2^n)$.

Throughout the article, we shall use the following operations and notations:

$a \| b$ — concatenation of the vectors a, b of V_l, i.e. a vector from V_{2l};
0 — the null vector of V_l;
$\oplus$ — bitwise eXclusive-OR — addition in $\mathrm{GF}(2^l)$;
$\langle a, b \rangle$ — the scalar product of vectors $a = (a_{l-1}, \ldots, a_0), b = (b_{l-1}, \ldots, b_0)$ of V_l, $\langle a, b \rangle = a_{l-1}b_{l-1} \oplus \ldots \oplus a_0 b_0$;
$\mathrm{w}_H(a)$ — the Hamming weight of a binary vector $a \in V_l$;
$\otimes$ — finite field multiplication;
$\Lambda \circ \Psi$ — a composition of mappings, where Ψ is the first to operate;
Ψ^{-1} — the inverse transformation to some bijective mapping Ψ.

Now, we introduce some basic concepts needed to describe and analyze S-Boxes with respect to linear, differential, and algebraic attacks. For this purpose, we consider an n-bit S-Box Φ as a vector of Boolean functions:

$$\Phi = (f_{n-1}, \ldots, f_0), \ \ f_i : V_n \to V_1, \ \ i = 0, 1, \ldots n-1.$$

For some fixed $i \in \{0, 1, \ldots, n-1\}$, every Boolean function f_i can be written as a sum over V_1 of distinct t-order products of its arguments, $0 \leqslant t \leqslant n-1$; this is called the algebraic normal form of f_i. Functions f_i are called coordinate Boolean functions of the S-Box Φ and it is well known that most of the desirable cryptographic properties of Φ can be defined in terms of their linear combinations (also-called S-Box component Boolean functions).

Definition 1. For $a, b \in V_n$ the Walsh transform $\mathcal{W}_\Phi(a, b)$ of an n-bit S-Box Φ is defined as

$$\mathcal{W}_\Phi(a, b) = \sum_{x \in V_n} (-1)^{\langle b, \Phi(x)\rangle \oplus \langle a, x\rangle}.$$

Definition 2. The nonlinearity of an n-bit S-Box Φ, denoted by $\mathcal{NL}(\Phi)$, is defined as

$$\mathcal{NL}(\Phi) = \min_{a \in V_n \setminus \{0\}} \{\mathcal{NL}(a_{n-1} f_{n-1} \oplus \ldots \oplus a_0 f_0)\},$$

where $\mathcal{NL}(a_{n-1} f_{n-1} \oplus \ldots \oplus a_0 f_0)$ is the nonlinearity of the component Boolean function.

The nonlinearity $\mathcal{NL}(\Phi)$ of an arbitrary n-bit S-Box Φ can be calculated as follows

$$\mathcal{NL}(\Phi) = 2^{n-1} - \frac{1}{2} \max_{a \neq 0, b \in V_n} |\mathcal{W}_\Phi(a, b)|.$$

Definition 3. The differential uniformity of an n-bit S-Box Φ, denoted by δ_Φ, is defined as

$$\delta(\Phi) = \max_{a \neq 0, b \in V_n} \delta_\Phi(a, b),$$

where $\delta_\Phi(a, b) = |\{x \in V_n : \Phi(x \oplus a) \oplus \Phi(x) = b\}|$.

Definition 4. The minimum degree of an S-Box Φ, denoted by $\deg(\Phi)$, is defined as

$$\deg(\Phi) = \min_{a \in V_n \setminus \{0\}} \{\deg(a_{n-1} f_{n-1} \oplus \ldots \oplus a_0 f_0)\}.$$

Definition 5. Let U be a non-empty subset of V_{2n}, then the annihilating set of U is defined as $\{p \in \mathrm{GF}(2)[z_1, \ldots, z_{2n}] : p(U) = 0\}$.

Definition 6. The algebraic immunity of U is defined as

$$\mathcal{AI}(U) = \min\{\deg p : 0 \neq p \in \mathrm{GF}(2)[z_1, \ldots, z_{2n}],\ p(U) = 0\}.$$

Definition 7. The graph algebraic immunity of n-bit S-Box Φ, denoted by $\mathcal{AI}_{\mathrm{gr}}(\Phi)$, is defined as

$$\mathcal{AI}_{\mathrm{gr}}(\Phi) = \min\{\deg p : 0 \neq p \in \mathrm{GF}(2)[z_1, \ldots, z_{2n}],\ p(\mathrm{gr}(\Phi)) = 0\},$$

where $\mathrm{gr}(\Phi) = \{(x, \Phi(x)) : x \in V_n\} \subseteq V_{2n}$.

Thus, we focus on the graph algebraic immunity of S-Box Φ and also on the parameter $r_\Phi^{(\mathcal{AI}_{\mathrm{gr}}(\Phi))}$ referred to as the number of all the independent equations in input and output values of the S-Box Φ, i.e., equations of the form $p(x, \Phi(x)) = 0$, $x \in V_n$.

Definition 8. An element $a \in V_n$ is called a fixed point of an n-bit S-Box Φ if $\Phi(a) = a$.

Definition 9. Two n-bit S-Boxes Φ_1 and Φ_2 are affine/linear equivalent if there exist a pair of invertible affine/linear permutation $A_1(x)$ and $A_2(x)$ such that $\Phi_1(x) = A_2 \circ \Phi_2 \circ$ $\circ A_1(x)$.

1. Constructing permutations from smaller ones and finite field multiplication

In this section, we present a special algorithmic-algebraic scheme which utilize the Lai-Massey structure for constructing $2k$-bits permutations from smaller ones and finite field multiplication. Our goal is to construct permutations with good cryptographic properties that were enumerated above.

Let $n = 2k$ be a natural number, where $k \geqslant 2$. Choosing

— the permutation polynomial $\mathcal{I} = \mathcal{P}_{2^k-2}(x)$;
— non-bijective k-bit function ψ which has no pre-image for 0;
— arbitrary permutation $h \in S(V_k)$,

we construct the following $2k$-bit vectorial Boolean function $\mathcal{G}$ from V_{2k} to V_{2k} as follows (Fig. 1).

Construction of $\mathcal{G}$

For the input value $(l\|r) \in V_{2k}$, we define the corresponding output value $\mathcal{G}(l\|r) = (l_1\|r_1)$, where
$l_1 = \mathcal{I}(l) \otimes \psi(l \otimes r)$;
$r_1 = h(r \otimes \psi(l \otimes r))$.

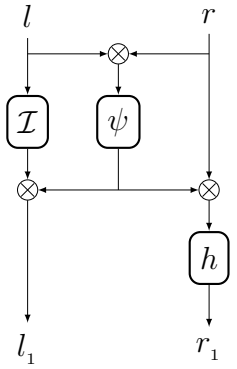

Fig. 1. High level structure of $\mathcal{G}$

The construction of $\mathcal{G}$ share similarities with 1-round of Lai-Massey structure replacing in the latter the XORs by finite field multiplications. The non-bijective k-bit function ψ (which has no pre-image for 0) is chosen in such a way to make invertible the structure of $\mathcal{G}$. Moreover, from the following construction

$$\begin{aligned} \mathcal{G}^{-1}(l_1\|r_1) &= l\|r, \\ l &= h^{-1}(l_1) \otimes \mathcal{I}\big(\psi(h^{-1}(l_1) \otimes \mathcal{I}(r_1))\big), \\ r &= \mathcal{I}\big(r_1 \otimes \mathcal{I}\big(\psi(h^{-1}(l_1) \otimes \mathcal{I}(r_1))\big)\big) \end{aligned}$$

we can easy derive the bijectivity of $\mathcal{G}$ which is a necessary design criterion for SPN ciphers and quite useful for Feistel and Lai-Massey ciphers.

When $n = 8$, in correspondence with the suggested construction of $\mathcal{G}$, we need to construct the 4-bit non-bijective function ψ, the 4-bit permutation $h \in S(V_4)$ and the inversion function $\mathcal{I}$ over the finite field $\mathrm{GF}(2^4) = \mathrm{GF}(2)[\xi]/g(\xi)$, constructing the latter with the irreducible polynomial $g(\xi) = \xi^4 + \xi + 1 \in \mathrm{GF}(2)[\xi]$.

The main advantage offered by construction of $\mathcal{G}$ is that its allows to perform a search based on random generation of 4-bit non-bijective function ψ and 4-bit permutation h for finding 8-bit S-Boxes with actual cryptographic parameters. We have implemented the above construction in SAGE [1] obtaining as a result a lot of affine nonequivalent 8-bit permutations without fixed points with the following parameters:

— minimum degree — 7;
— graph algebraic immunity — 3 (with 441 equations);
— 6 and 8 — uniform;
— nonlinearity in range of 100 up to a value of 104.

1.1. Constructing involutions

In this section, we study how to build involutive S-Boxes with strong cryptographic properties using constructions presented in the previous section. Involutions, i.e. permutations with the property $\Phi \circ \Phi(x) = x$, have an particular interest in cryptography because in the case of lightweight block ciphers, these components are used to decrease the cost of the implementation of decryption process.

Exploring the construction of $\mathcal{G}$, we have found 8-bit involutions having few fixed points with the following properties:

— minimum degree — 7;
— graph algebraic immunity — 3 (with 441 equations);
— 6 and 8 — uniform;
— nonlinearity in range of 100 up to a value of 104.

Also, we have tried to design directly involutions without fixed points using our scheme. To achieve the fulfilment of condition $\Phi \circ \Phi(x) = x$, our strategy was to combine our constructions into two rounds. Choosing two arbitrary k-bit involutions h_1, h_2, the following constructions are able to produce $2k$-bit involutions with strong cryptographic properties (Fig. 2).

Construction of $\mathcal{G}^{\text{invol}}$

For the input value $(l\|r) \in V_{2k}$, we define the corresponding output value

$$\mathcal{G}^{\text{invol}}(l\|r) = \left(\mathcal{G}_2^* \circ \mathcal{G}_1^*\right)(l\|r) = l_1\|r_1, \text{ where}$$

$$\mathcal{G}^*{}_1(l\|r) = h_1(l \otimes \mathcal{I}(\psi(l \otimes r)))\Big\|h_2(l \otimes \psi(l \otimes r));$$

$$\mathcal{G}_2^*(l\|r) = \Big(l \otimes \psi(l \otimes r)\Big)\Big\|\Big(l \otimes \mathcal{I}(\psi(l \otimes r))\Big).$$

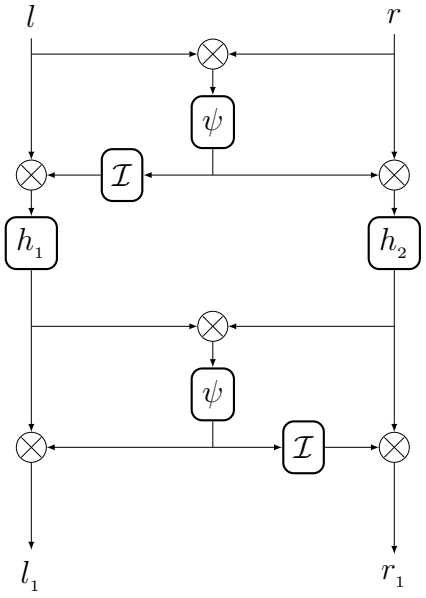

Fig. 2. Structure of $\mathcal{G}^{\text{invol}}$

As we can see from Fig. 2, the construction of $\mathcal{G}^{\text{invol}}$ represents a composition of two functions $\mathcal{G}_2^*$ and $\mathcal{G}_1^*$, each of which has similarities with 1-round of Lai-Massey scheme. The function $\mathcal{G}_2^*$ is chosen in such a way to make the whole structure an involution. In fact, by direct computations, it is not difficult to show that $\mathcal{G}^{\text{invol}} \circ \mathcal{G}^{\text{invol}}(x) = x$ for all $x \in V_{2k}$.

Implementing the construction of $\mathcal{G}^{\text{invol}}$ in SAGE [1], we have obtained affine non-equivalent 8-bit involutions without fixed points (in contrast to the construction of $\mathcal{G}$) with the following parameters:

— minimum degree — 7;

— 8 — uniform;

— graph algebraic immunity — 3 (with 441 equations);

— nonlinearity in range of 100 up to a value of 102.

The possibility of having no fixed points in those involutions constructed under the $\mathcal{G}^{\text{invol}}$ scheme has some significances. In fact, the cryptographic properties related to linear and differential cryptanalysis of involutions based on $\mathcal{G}$-construction are stronger in comparison with those generated by $\mathcal{G}^{\text{invol}}$.

1.2. Searching of highly-nonlinear orthomorphisms

In this section, we study the possibility of using ours methods to find permutations Φ such that $\Phi(x) \oplus x$ are permutations too. In the public literature, these permutations are called orthomorphisms. Orthomorphisms are pertinent to the construction of mutually orthogonal Latin squares and can be used to design check digit systems. In cryptography, applications of orthomorphisms of the group $(V_n, \oplus)$ are found in the construction of block ciphers, stream ciphers and hash functions (in the Lai — Massey scheme most famously in well-known FOX [2] family of block ciphers, Chinese stream cipher LOISS [3] and hash function EDON-R [4]). More recently, orthomorphisms have been used to strengthen the Even-Mansour block cipher against a cryptographic attack which makes the use of the nonuniformity of $\Phi(x) \oplus x$ when Φ is a random permutation [5].

Exploring and exploiting the construction of $\mathcal{G}$, we have found highly-nonlinear orthomorphisms with the following parameters:

— minimum degree — 7;

— 8 — uniform;

— graph algebraic immunity — 3 (with 441 equations);

— nonlinearity in range of 100 up to a value of 102.

1.3. Some examples

We include in Table some permutations generated by our method, one ordinary permutation with the best founded cryptographic parameters, two involutions and one orthomophism.

Some constructed 8-bit S-Boxes

S-Box $\mathcal{G}_1$															
$\mathcal{NL}(\mathcal{G}_1) = 104$, $\delta(\mathcal{G}_1) = 6$, $\deg(\mathcal{G}_1) = 7$, $\mathcal{AI}_{\text{gr}}(\mathcal{G}_1) = 3$, $r^{(3)}_{\mathcal{G}_1} = 441$															
6e	e8	5f	a8	32	24	a7	0e	1d	64	87	14	c3	6f	95	92
fb	4c	82	99	3d	19	ac	45	9f	fe	de	15	b9	f9	e2	8a
ec	f5	0d	ea	3a	77	47	12	11	01	97	c5	13	10	81	9d
ed	75	88	68	fa	a4	c0	ca	ba	b2	3b	61	ae	0a	6c	65
d5	42	5d	dc	f2	85	9b	a6	67	50	63	91	c7	34	80	d7
96	1b	8e	5e	94	2f	b1	ad	a0	93	2c	52	d0	29	07	c8
8d	7f	49	6b	36	2e	d9	e0	37	cd	83	af	6d	57	ce	b3
5c	c6	60	d8	3f	e4	4f	ab	56	a1	72	e7	69	f1	dd	9c
84	90	25	4b	76	5a	6a	da	f0	e5	53	5b	7e	2a	2b	d3
35	a3	1c	a2	28	9e	30	a9	b4	06	0b	ef	aa	43	e9	7d
e1	3e	31	44	54	db	79	c9	41	fc	f7	66	7a	b7	51	38
df	62	40	bb	26	09	f3	cf	d2	1a	20	0c	04	16	33	22
4e	a5	58	9a	d6	02	e6	cb	be	eb	86	7b	bd	d1	03	f6
ee	8f	0f	55	8b	4a	7c	23	2d	b6	1f	c2	17	bf	73	08
cc	70	1e	59	46	e3	27	ff	78	b8	18	21	d4	bc	98	f4
c1	c4	74	39	89	f8	fd	48	71	4d	b0	3c	00	8c	b5	05

Involution $\mathcal{G}_2$															
$\mathcal{NL}(\mathcal{G}_2) = 104$, $\delta(\mathcal{G}_2) = 6$, $\deg(\mathcal{G}_2) = 7$, $\mathcal{AI}_{\mathrm{gr}}(\mathcal{G}_2) = 3$, $r^{(3)}_{\mathcal{G}_2} = 441$															
00	10	90	e0	d0	b0	70	60	f0	20	c0	50	a0	40	30	80
01	11	19	85	2f	2c	8b	f5	2e	12	fa	9a	8c	98	fb	93
09	2d	4e	3c	47	d5	36	dc	3b	29	db	46	15	21	18	14
0e	b3	b8	64	b4	81	26	3f	86	6b	89	28	23	65	3e	3
0d	87	8a	63	6c	9c	2b	24	66	4f	96	9b	83	4d	22	49
0b	ad	62	be	61	5c	b7	a8	69	b2	a3	5b	55	ed	e1	e9
07	54	52	43	33	3d	48	67	c2	58	6e	39	44	cc	6a	cb
06	bd	bf	7c	aa	e2	76	df	a5	b9	dd	e4	73	ee	de	a9
0f	35	c6	4c	c3	13	38	41	c8	3a	42	16	1c	8e	8d	8f
02	94	92	1f	91	d7	4a	e7	1d	d3	1b	4b	45	d6	ea	e5
0c	c1	c9	5a	cd	78	ab	f9	57	7f	74	a6	ac	51	fd	ff
05	c4	59	31	34	b5	cf	56	32	79	bb	ba	ce	71	53	72
0a	a1	68	84	b1	c7	82	c5	88	a2	ca	6f	6d	a4	bc	b6
04	f6	d8	99	d4	25	9d	95	d2	fc	fe	2a	27	7a	7e	77
03	5e	75	e3	7b	9f	e8	97	e6	5f	9e	f1	f2	5d	7d	f7
08	eb	ec	f4	f3	17	d1	ef	f8	a7	1a	1e	d9	ae	da	af

Involution $\mathcal{G}_3^{\mathrm{invol}}$															
$\mathcal{NL}(\mathcal{G}_3^{\mathrm{invol}}) = 100$, $\delta(\mathcal{G}_3^{\mathrm{invol}}) = 8$, $\deg(\mathcal{G}_3^{\mathrm{invol}}) = 7$, $\mathcal{AI}_{\mathrm{gr}}(\mathcal{G}_3^{\mathrm{invol}}) = 3$, $r^{(3)}_{\mathcal{G}_3^{\mathrm{invol}}} = 441$															
a0	af	61	7b	5e	2f	12	27	be	38	b6	6a	76	33	71	36
80	67	06	a4	e4	59	17	16	9d	6e	d5	51	de	ec	a7	93
40	37	78	9e	d9	fa	ff	07	58	3e	9c	b1	b2	3f	d6	05
90	6c	e9	0d	a1	75	0f	21	09	74	b7	69	ea	bc	29	2d
20	a3	f1	ed	b3	db	c4	fc	df	8e	bf	e7	c2	8f	a5	8d
70	1b	62	cf	bd	f4	89	cc	28	15	87	f8	f3	63	04	b8
d0	02	52	5d	86	ce	77	11	83	3b	0b	aa	31	a8	19	cb
50	0e	96	7c	39	35	0c	66	22	88	9f	03	73	da	8c	d7
10	e2	c6	68	fd	cd	64	5a	79	56	eb	f5	7e	4f	49	4d
30	c7	ca	1f	c5	a9	72	9b	f2	f6	ad	97	2a	18	23	7a
00	34	c9	41	13	4e	e6	1e	6d	95	6b	e8	e3	9a	c3	01
e0	2b	2c	44	c1	d4	0a	3a	5f	c8	d2	d8	3d	54	08	4a
f0	b4	4c	ae	46	94	82	91	b9	a2	92	6f	57	85	65	53
60	d3	ba	d1	b5	1a	2e	7f	bb	24	7d	45	e1	e5	1c	48
b0	dc	81	ac	14	dd	a6	4b	ab	32	3c	8a	1d	43	fe	f7
c0	42	98	5c	55	8b	99	ef	5b	fb	25	f9	47	84	ee	26

Orthomorphism $\mathcal{G}_4$															
$\mathcal{NL}(\mathcal{G}_4) = 102$, $\delta(\mathcal{G}_4) = 8$, $\deg(\mathcal{G}_4) = 7$, $\mathcal{AI}_{\mathrm{gr}}(\mathcal{G}_4) = 3$, $r^{(3)}_{\mathcal{G}_4} = 441$															
a1	f9	70	7e	a7	c2	12	d2	88	ed	62	d5	2a	2e	08	79
c6	fc	b0	90	ba	de	cc	66	58	c1	5b	00	15	e0	64	25
37	f8	9e	28	83	4e	17	7d	16	a2	67	2b	7a	29	57	a9
31	f7	e2	b6	21	98	6a	d1	92	71	74	97	85	8d	0a	e3
18	f4	be	a0	1b	32	39	27	80	db	6e	0e	d4	d6	5e	61
65	f5	ce	a6	6d	50	5c	6c	4b	36	19	0b	02	eb	c4	8b
33	f2	82	e1	ec	ab	13	c7	9a	73	b7	8a	a3	9d	89	45
72	fb	b8	35	3b	c8	d9	1e	48	d0	68	e4	30	c3	1a	24
8e	f1	46	9c	2c	01	07	cd	b5	3d	03	54	ac	bb	43	8c
51	f3	6b	40	26	bd	e8	b2	05	76	0d	4c	11	e6	b3	86
c5	f6	b4	94	dc	60	55	56	44	47	cb	69	53	7c	38	84
52	fa	e7	81	2d	42	1d	dd	ea	96	ee	87	ad	0c	20	93
3a	fe	3c	78	77	ca	23	da	a4	22	b9	e9	91	ae	5a	a8
d8	f0	9b	5d	14	c9	aa	3e	49	10	d7	09	34	7b	59	1c
6f	ff	8f	2f	3f	0f	cf	5f	ef	1f	4f	9f	df	af	bf	7f
4a	fd	06	95	d3	b1	63	99	c0	75	4d	bc	a5	e5	41	04

2. Conclusion and Future Work

In this work, we have presented a new algorithmic-algebraic scheme based in the Lai — Massey structure for constructing permutations of dimension $n = 2k$, $k \geqslant 2$. For the common case $k = 8$, we have obtained new cryptographically strong 8-bit permutations having better resistance to algebraic attacks in comparison with the inversion function in $\mathrm{GF}(2^8)$ which so far has the best-known values for nonlinearity and differential uniformity. Compared to the best nonlinearity (108, for $k = 4$) offered by the construction presented in [6] and later generalized in [7], the nonlinearity for the permutations obtained by our scheme slightly decrease up to 104, but to the best of our knowledge the schemes presented in [6, 7] can not produce involutions and orthomorphisms with strong cryptographic properties, so we can conclude that the new structure presented in this work is more powerful and attractive due to the diversity of permutations that can be constructed. Interestingly, the involutions and orthomorphisms founded in this work have comparable classical cryptographic properties like those constructed by using spectral-linear and spectral-difference methods [8]. The main advantage of our 8-bit permutations is that they can be constructed using smaller 4-bit components which could be useful for the implementation of the S-Box in hardware or using a bit-sliced approach. We only presented a new scheme that can help to find permutations, involutions and orthomophisms with rather good cryptographic properties. There are several questions (theoretical results, hardware and bit-sliced implementations, efficient methods of masking) about the construction suggested in this work which are left as future work.

REFERENCES

1. `http://www.sagemath.org`. Sage Mathematics Software (Version 8.1). 2018.
2. *Vaudenay S. and Junod P.* Fox, a New Family of Block Ciphers. `http://crypto.junod.info/sac04a.pdf`. 2004.
3. *Feng D., Feng X., Zhang W., et al.* Loiss: a byte oriented stream cipher. LNCS, 2011, vol. 6639, pp. 109–125.
4. *Gligoroski D., Odegard R. S., Mihova M., et al.* Cryptographic hash function Edon-R. Proc. IWSCN, Trondheim, 2009, pp. 1–9.
5. *Gilboa Sh. and Gueron Sh.* Balanced Permutations Even-Mansour Ciphers. Cryptology ePrint Archive, Report 2014.
6. *De la Cruz Jiménez R. A.* Generation of 8-bit S-Boxes Having Almost Optimal Cryptographic Properties Using Smaller 4-bit S-Boxes and Finite Field Multiplication. 2017. `www.cs.haifa.ac.il/orrd/LC17/paper60.pdf`.
7. *Fomin D.* New classes of 8-bit permutations based on a butterfly structure. Pre-proc. CTCrypt'18-Suzdal, 2016, pp. 199–211.
8. *Menyachikhin A.* Spectral-linear and spectral-difference methods for generating cryptographically strong S-Boxes. Pre-proc. CTCrypt'16-Yaroslavl, 2016, pp. 232–252.

UDC 621.391:519.7 DOI 10.17223/2226308X/12/43

SOME PROPERTIES OF THE OUTPUT SEQUENCES OF COMBINED GENERATOR OVER FINITE FIELDS

Aulet R. Rodriguez

The sequences are an important part of the cryptography and analysis of their properties is of great interest. In this paper, the following characteristics of combined