On differential uniformity of permutations derived using a generalized construction

Denis Fomin and Maria Kovrizhnykh

National Research University Higher School of Economics, Russia

dfomin@hse.ru, makovrizhnykh@gmail.com

Moscow Region,
June 1-4, 2021

Purpose of the work

The theoretical substantiation of a directed search for 8-bit permutations with given cryptographic properties: differential uniformity and nonlinearity, among vector Boolean functions obtained using a generalized construction.

Motivation

- Vector Boolean functions (S-boxes) are one of the main primitives of modern symmetric ciphers that provide Shannon's confusion.
- Moreover, S-boxes used in modern symmetric ciphers must be bijective.
- S-boxes must have cryptographic properties that guarantee the impossibility of using known methods (in particular, differential and linear methods) of cryptographic analysis.

  Thus, S-boxes with high nonlinearity can ensure the cipher resistance to linear cryptographic analysis. S-boxes with the minimum possible differential uniformity are used for constructing cryptographic algorithms that are resistant to differential analysis.

Motivation

- Construction of $n \geqslant 8$ bits permutations with given cryptographic properties is a difficult and urgent task, which is confirmed by a large number of the latest scientific publications and reports at all-Russian and international conferences dedicated to this theme.
- 8-bit permutations are used, for example, in GOST 34.12-2018 “Kuznyechik”, AES, BelT, and others.

Definitions and Notations

- Let V_n be n-dimensional vector space over the field of two elements $\mathbb{F}_2$, $V_n^{\times} = V_n \setminus \{0\}$.
- The finite field of 2^n elements is denoted by $\mathbb{F}_{2^n}$. The operations of addition and multiplication in the field $\mathbb{F}_{2^n}$ are denoted by the signs "$+$" and "$\cdot$", respectively.
- *Concatenation* of the vectors $a \in V_n$, $b \in V_m$ is denoted by $a\|b \in V_{n+m}$.
- The *dot product* of two vectors $a, b \in V_n$ is an element of the field $\mathbb{F}_2$, calculated by the formula $\langle a, b\rangle = a_{n-1}b_{n-1} + \ldots + a_0b_0$ where addition and multiplication are carried out in the field $\mathbb{F}_2$.
- The vector Boolean (n, m)–function is a mapping $V_n \to V_m$.
- Permutation over V_n is a bijective (n, n)–function.

Monomial permutations of the field $\mathbb{F}_{2^m}$ are permutations of the form x^d, where d is a positive integer such that $\gcd(d, 2^m - 1) = 1$.
In particular, for $m = 4$, monomial permutations are obtained for $d \in \{1, 2, 4, 7, 8, 11, 13, 14\}$.
Moreover, linear monomial permutations of the field $\mathbb{F}_{2^4}$ are x^d for $d \in \{1, 2, 4, 8\}$.

Some cryptographic properties of (n, m)-functions

Definition

The differential uniformity of (n, m)-function F is defined as

$$\delta_F = \max_{a \in V_n^{\times},\, b \in V_m} \delta_F(a, b),$$

where $\delta_F(a, b) = |\{x \in V_n \mid F(x + a) + F(x) = b\}|.$

Definition

The nonlinearity N_F of (n, m)-function F is a value calculated by the formula

$$N_F = 2^{n-1} - \frac{1}{2} \max_{a \in V_n, b \in V_m^{\times}} \left| \sum_{x \in V_n} (-1)^{\langle a, x \rangle + \langle b, F(x) \rangle} \right|.$$

The use of functions with greater nonlinearity and lower differential uniformity in the synthesis of cryptographic algorithms makes it possible to guarantee resistance against the linear and differential methods of cryptographic analysis.

Related works

- **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”, LNCS, Progress in Cryptology — LATINCRYPT 2017, **11368**, eds. T. Lange and O. Dunkelman, Springer Nature, Switzerland AG, 2019, 191–206, https://doi.org/10.1007/978-3-030-25283-0_11

- **De la Cruz Jiménez R.A.**, “On some methods for constructing almost optimal S-Boxes and their resilience against side-channel attacks”, Cryptology ePrint Archive, Report 2018/618. https://eprint.iacr.org/2018/618

- **De la Cruz Jiménez R.A.**, “A method for constructing permutations, involutions and orthomorphisms with strong cryptographic properties”, PDM. Prilozheniye, **12** (2019), 145–151. https://doi.org/10.17223/2226308X/12/42

- **Fomin D.B.**, “New classes of 8-bit permutations based on a butterfly structure”, Mat. Vopr. Kriptogr., **10**:2 (2019), 169–180. https://doi.org/10.4213/mvk294

- **Fomin D.B.**, “Constructing permutations of the space V_{2m} using $(2m, m)$-functions”, Mat. Vopr. Kriptogr., **11**:3 (2020), 121–138.

- **Fomin D.B.**, “On algebraic degree and differential uniformity of permutations of the space V_{2m}, constructed using $(2m, m)$-functions”, Mat. Vopr. Kriptogr., **11**:4 (2020), 133–149.

Generalized construction

Let $(2m, 2m)$-function $F(x_1, x_2) = y_1 \| y_2$, where $x_1, x_2, y_1, y_2 \in V_m$, be given by the following *generalized construction*, first introduced in [1],

$$y_1 = G_1(x_1, x_2) = \begin{cases} x_1^{\alpha} \cdot x_2^{\beta}, & x_2 \neq 0, \\ \widehat{\pi}_1(x_1), & x_2 = 0, \end{cases}$$
$$y_2 = G_2(x_1, x_2) = \begin{cases} x_1^{\gamma} \cdot x_2^{\delta}, & x_1 \neq 0, \\ \widehat{\pi}_2(x_2), & x_1 = 0, \end{cases} \tag{1}$$

$$\widehat{\pi}_1(0) = 0, \quad \widehat{\pi}_2(0) = 0. \tag{2}$$

Hereinafter, one should go from the vectors of the space V_m to the corresponding elements of the field $\mathbb{F}_{2^m}$ and perform exponentiation and multiplication in the field $\mathbb{F}_{2^m}$. Moreover, in (1), $\widehat{\pi}_1$, $\widehat{\pi}_2$ are permutations over V_m.

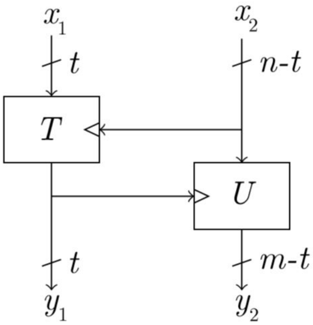
The parameters of the function (1) are the tuple of indexes $(\alpha, \beta, \gamma, \delta)$ of monomial permutations and permutations $\widehat{\pi}_1$, $\widehat{\pi}_2$.

[1] Fomin D.B. "On approaches to constructing low-resource nonlinear transformations", Obozreniye prikladnoy i promyshlennoy matematiki. 25:4 (2018), 379-381, In Russian.

Generalized construction admits TU-decomposition

Statement 1

The construction (1) *admits* TU*-decomposition* [2].



[2] Canteaut A., Perrin L. "On ccz-equivalence, extended-affine equivalence, and function twisting", Cryptology ePrint Archive, Report 2018/713. https://eprint.iacr.org/2018/713.

Two criteria for rejection of vector Boolean functions derived using a generalized construction

1. Let us reject functions (1) for which the differential δ-uniformity is $\delta_F \geqslant 8$ (for $m = 4$).
2. Then we can reject those that are not permutations among the remaining functions.

Partitioning the set of functions (1) into equivalence classes

Lemma 1 [3]

Let $(2m, 2m)$*-function* F *be obtained using the construction* (1)*, and* $a_1, a_2, b_1, b_2 \in V_m$*, then* $\delta_F(a_1 \| a_2, b_1 \| b_2)$ *is greater than or equal to the number of solutions to the system of equations*

$$\begin{cases} (x_1 + a_1)^\alpha \cdot (x_2 + a_2)^\beta + x_1^\alpha \cdot x_2^\beta &= b_1, \\ (x_1 + a_1)^\gamma \cdot (x_2 + a_2)^\delta + x_1^\gamma \cdot x_2^\delta &= b_2, \end{cases} \qquad (3)$$

with the following constraints on the values of the variables x_1 *and* x_2

$$x_2 \neq 0, \quad x_2 \neq a_2, \quad x_1 \neq 0, \quad x_1 \neq a_1. \qquad (4)$$

[3] Fomin D.B., "On algebraic degree and differential uniformity of permutations of the space V_{2m}, constructed using $(2m; m)$-functions", Mat. Vopr. Kriptogr., 11:4 (2020), 133-149, In Russian.

Partitioning the set of functions (1) into equivalence classes

Statement 2

The system (3) *with a tuple of parameters* $(\alpha, \beta, \gamma, \delta)$*, where* x^{α}*,* x^{β}*,* x^{γ}*, and* x^{δ} *define monomial permutations, has the maximum number of solutions* (x_1, x_2)*,* $x_1, x_2 \in \mathbb{F}_{2^m}$*, satisfying the conditions* (4)*, for* $a_1, a_2, b_1, b_2 \in \mathbb{F}_{2^m}$ *(*a_1 *and* a_2 *do not vanish simultaneously), that is coincide with the maximum number of solutions of systems of the form* (3) *under constraints* (4) *with the following tuples of parameters*

$$(\alpha \cdot d_1,\ \beta \cdot d_1,\ \gamma \cdot d_2,\ \delta \cdot d_2) \mod 2^m - 1,$$

$$(\alpha \cdot d_1,\ \beta \cdot d_2,\ \gamma \cdot d_1,\ \delta \cdot d_2) \mod 2^m - 1,$$

$$(\gamma,\ \delta,\ \alpha,\ \beta), \qquad (\beta,\ \alpha,\ \delta,\ \gamma), \qquad (\delta,\ \gamma,\ \beta,\ \alpha),$$

where x^{d_1}*,* x^{d_2} *define linear permutations.*

Partitioning the set of functions (1) into equivalence classes

Remark 1

Note that the sets $\{1, 2, 4, 8\}$ *and* $\{7, 11, 13, 14\}$ *are closed under multiplication by* $d \in \{1, 2, 4, 8\}$ *modulo 15. Then, by virtue of Statement 2, we obtain that* $8^4 = 2^{12} = 4096$ *of all possible parameter tuples* $(\alpha, \beta, \gamma, \delta)$ *of the functions from the family* (1) *are split into disjoint equivalence classes with the same maximum number of solutions of the system* (3) *under the constraints* (4) *in each class. A distinct equivalence class can be obtained from one of its representatives* $(\alpha, \beta, \gamma, \delta)$*, by composing different tuples from the following ones*

$$\begin{aligned}
&(\alpha \cdot d_1 \cdot d_3, \quad \beta \cdot d_1 \cdot d_4, \quad \gamma \cdot d_2 \cdot d_3, \quad \delta \cdot d_2 \cdot d_4) \mod 2^m - 1,\\
&(\gamma \cdot d_1 \cdot d_3, \quad \delta \cdot d_1 \cdot d_4, \quad \alpha \cdot d_2 \cdot d_3, \quad \beta \cdot d_2 \cdot d_4) \mod 2^m - 1,\\
&(\beta \cdot d_1 \cdot d_3, \quad \alpha \cdot d_1 \cdot d_4, \quad \delta \cdot d_2 \cdot d_3, \quad \gamma \cdot d_2 \cdot d_4) \mod 2^m - 1,\\
&(\delta \cdot d_1 \cdot d_3, \quad \gamma \cdot d_1 \cdot d_4, \quad \beta \cdot d_2 \cdot d_3, \quad \alpha \cdot d_2 \cdot d_4) \mod 2^m - 1,
\end{aligned}$$

where $m = 4, \quad d_1, d_2, d_3, d_4 \in \{1, 2, 4, 8\}$.

Justification of the first criterion for rejecting functions (1)

Propositions 1, 2

Let F be a $(2m, 2m)$-function given by the construction (1).

1. *If x^{α}, x^{γ} define linear permutations, then $\delta_F \geqslant 2^m - 2$.*
2. *If $\alpha = \beta = \gamma = \delta$, then $\delta_F \geqslant 2^m - 2$.*

Propositions 3, 4

Let F be a $(8, 8)$-function given by the construction (1).

3. *If $\alpha = 11$, $\beta = \gamma = 1$, $\delta = 13$, then $\delta_F \geqslant 14$.*
4. *If $\alpha = 7$, $\beta = \gamma = 1$, $\delta = 7$, then $\delta_F \geqslant 14$.*

Justification of the second criterion for rejecting functions (1)

Statement 3

Let F be a $(2m, 2m)$-function given by the construction (1) with a tuple of parameters $(\alpha, \beta, \gamma, \delta)$, where x^α, x^β, x^γ, and x^δ define monomial permutations. If F is not a bijection for any values of the permutations $\widehat{\pi}_i(x_i)$, $i \in \{0, 1\}$, then any $(2m, 2m)$-function from the family (1) with the following tuples of parameters

$$(\alpha \cdot d_1,\ \beta \cdot d_1,\ \gamma \cdot d_2,\ \delta \cdot d_2) \mod 2^m - 1,$$

$$(\alpha \cdot d_1,\ \beta \cdot d_2,\ \gamma \cdot d_1,\ \delta \cdot d_2) \mod 2^m - 1,$$

$$(\gamma,\ \delta,\ \alpha,\ \beta), \qquad (\beta,\ \alpha,\ \delta,\ \gamma), \qquad (\delta,\ \gamma,\ \beta,\ \alpha),$$

where x^{d_1}, x^{d_2} define a linear permutation, is also not a bijection for any values of the permutations $\widehat{\pi}_i(x_i)$, $i \in \{0, 1\}$.

Justification of the second criterion for rejecting functions (1)

Proposition 5

$(8,8)$-function F given by the construction (1) with the parameters $(\alpha,\beta,\gamma,\delta)$ from the list below

- $(7,7,7,13)$
- $(1,7,7,7)$
- $(4,7,7,7)$
- $(7,7,2,2)$
- $(1,1,7,13)$
- $(2,7,7,7)$
- $(7,2,2,7)$

is not a bijection for any values of the permutations $\widehat{\pi}_i(x_i)$, $i \in \{0,1\}$.

Summary table of the equivalence classes for $m = 4$

№	The representative of the equivalence class	The number of elements in the equivalence class	The reason for rejection
1	Generalized representative: $(\alpha, \beta, \gamma, \delta)$, where $\alpha, \gamma \in \{1, 2, 4, 8\}$	1792	$\delta_F \geqslant 14$, according to Statement 1
2	(7,7,7,7)	64	$\delta_F \geqslant 14$, according to Statement 2
3	(11,1,1,13)	128	$\delta_F \geqslant 14$, according to Statement 3
4	(7,1,1,7)	128	$\delta_F \geqslant 14$, according to Statement 4
5	(7,7,7,13)	64	are not permutations, according to Statement 5
6	(1,7,7,7)	256	
7	(4,7,7,7)	256	
8	(7,7,2,2)	128	
9	(1,1,7,13)	128	
10	(2,7,7,7)	256	
11	(7,2,2,7)	128	
12	(1,1,7,11)	256	are not rejected
13	(1,7,7,11)	256	
14	(1,7,7,2)	128	
15	(7,7,7,11)	128	

On the selection of auxiliary 4-bit permutations in the generalized construction

It remains to learn how to choose the auxiliary permutations $\widehat{\pi}_1$ and $\widehat{\pi}_2$ so that the resulting 8-bit permutation F (1) has $\delta_F = 6$, $N_F = 108$.

A heuristic approach that uses the ideas of spectral-linear and spectral-differential methods [4] is proposed:

1. initial randomly generated 4-bit permutations $\widehat{\pi}_i$ are iteratively multiplied by transpositions;
2. the best ones in terms of nonlinearity, differential uniformity and the corresponding values in the linear and differential spectra among the obtained 8-bit permutations are selected;
3. if the specified properties $\delta_F \leqslant 6$ and $N_F \geqslant 108$ are reached, exit;
4. 4-bit permutations $\widehat{\pi}_i$ corresponding to the best in step 2, are iteratively multiplied by transpositions, go to step 2;

[4] Menyachikhin A.V., “Spectral-linear and spectral-differential methods for generating S-boxes having almost optimal cryptographic parameters”, Mat. Vopr. Kriptogr., 8:2 (2017), 97–116, https://doi.org/10.4213/mvk227.

On the selection of auxiliary 4-bit permutations in the generalized construction

The possibility of optimizing the calculation of cryptographic properties at each iteration of the algorithm is investigated following [5].

The practical applicability of the algorithm is shown experimentally: 8-bit 6-uniform permutations with nonlinearity 108 and algebraic degree 7 are obtained.

[5] Menyachikhin A., "The change in linear and differential characteristics of substitution multiplied by transposition", The VIIIth Workshop on Current Trends in Cryptology (CTCrypt 2019), 2019, https://ctcrypt.ru/files/files/2019/materials/15_Menyachikhin.pdf

Summary

- We proposed the principle of partitioning the set of $(8, 8)$-functions derived using a generalized construction (1) into equivalence classes. It is shown how to obtain the entire equivalence class from one of its representatives.

- We have proved statements that allow us to reject $(2m, 2m)$-functions given by the construction (1), either by the high differential uniformity or by the fact that they are not permutations. Moreover, the conclusion about all functions from the equivalence class is based on the analysis of only one of its representatives.

Summary

- The statements proved in the work justify the rejection of 3328 tuples of parameters $(\alpha, \beta, \gamma, \delta)$ of $(8, 8)$-functions F defined by the construction (1) due to the value $\delta_F \geqslant 14$ or because F is not a bijection. The 768 tuples of parameters $(\alpha, \beta, \gamma, \delta)$ remained unrejected, which are split by Statement 2 and Remark 1 into 4 equivalence classes with representatives $(1, 1, 7, 11)$, $(1, 7, 7, 11)$ with 256 tuples in each class, $(1, 7, 7, 2)$, $(7, 7, 7, 11)$ with 128 tuples in each class (see table 1).

- A heuristic algorithm for finding auxiliary 4-bit permutations in a generalized construction is proposed. The ideas of spectral-linear, and spectral-differential methods are used. 8-bit 6-uniform permutations with nonlinearity 108 and algebraic degree 7 are experimentally obtained.

Thank you for your attention!