Proposition 2. If $|M^k_{\pi,n}| \neq |M^k_{\rho,n}|$ for some k, then the set of one-to-one functions from $\Delta_{\pi,n}$ is empty.

Theorem 1 means that in order to construct one-to-one functions $F_\pi \in \Delta_{\pi,n}$ we can use bijective maps $\Psi_n : \Theta_{\pi,n} \to \Theta_{\rho,n}$ that satisfy $|\Psi_n(g)| = |g|$, where $g \in \Theta_{\pi,n}$. Then, depending on them, we can construct $F_\pi \in \Delta_{\pi,n}$ such that $\Psi_{F_\pi,n} \equiv \Psi_n$.

Proposition 3. Let $\Psi_n : \Theta_{\pi,n} \to \Theta_{\rho,n}$ satisfy $|\Psi_n(g)| = |g|$ for all $g \in \Theta_{\pi,n}$. Then, for all $k \in \mathbb{N}$, the restriction of Ψ_n on $M^k_{\pi,n}$ is a permutation of $M^k_{\pi,n}$.

Now consider the case $\pi = \rho$. We define $M^k_n = M^k_{\rho,n}$. Consider an one-to-one function Ψ_n which satisfies $|\Psi_n(g)| = |g|$ for all $g \in \Theta_{\pi,n}$. Let us construct function $F_\rho \in \Delta_{\rho,n}$ based on Ψ_n. Let $O \in \Theta_{\rho,n}$ be an orbit of length k. If the value of F_ρ for some $x \in O$ is determined, then the value of F_ρ is determined for all $x \in O$, since $F_\rho(\rho^n(x)) = \rho^{-n}(F_\rho(x))$. Thus, for every $\Psi_{F_\rho,n}$, we are able to construct $\prod\limits_{k\in I_n} k^{|M^k_n|}$ functions, where $I_n = \{z \in \mathbb{N} : z|n\}$, and all of them are pairwise different.

Proposition 4. For any $k \in \mathbb{N}$, $\sum\limits_{\ell\in I_k} \ell \cdot |M^\ell_n| = 2^k$.

This formula allows us to calculate $|M^k_n|$ for every k. There are always only two orbits of length one, so we can calculate $|M^k_n|$ for every prime k. Then we can calculate it for every k. Therefore, we get the number of one-to-one functions from $\Delta_{\rho,n}$:

Theorem 2. The number of one-to-one vectorial Boolean functions in class $\Delta_{\rho,n}$ is equal to $\prod\limits_{k\in I_n} |M^k_n|! \cdot k^{|M^k_n|}$.

UDC 519.7 DOI 10.17223/2226308X/13/13

CRYPTOGRAPHIC PROPERTIES OF A SIMPLE S-BOX CONSTRUCTION BASED ON A BOOLEAN FUNCTION AND A PERMUTATION[1]

D. A. Zyubina, N. N. Tokareva

We propose a simple method of constructing S-boxes using Boolean functions and permutations. Let π be an arbitrary permutation on n elements, f be a Boolean function in n variables. Define a vectorial Boolean function $F_\pi : \mathbb{F}_2^n \to \mathbb{F}_2^n$ as $F_\pi(x) = (f(x), f(\pi(x)), f(\pi^2(x)), \ldots, f(\pi^{n-1}(x)))$. We study cryptographic properties of F_π such as high nonlinearity, balancedness, low differential δ-uniformity in dependence on properties of f and π for small n.

Keywords: *Boolean function, vectorial Boolean function, S-box, high nonlinearity, balancedness, low differential δ-uniformity, high algebraic degree.*

S-boxes play the crucial role for providing resistance of a block cipher to different types of attacks. The major reason for this is that in classical and modern block ciphers the main complicated and nonlinear layer is presented namely by S-boxes. Mathematically, S-box is a vectorial Boolean function that maps n bits to m bits. Usually, n coincides with m. It is well known that some special mathematical properties of S-boxes, such as high nonlinearity, low differential uniformity, high algebraic immunity, etc. make a

[1] The work is supported by Mathematical Center in Akademgorodok under agreement No. 075-15-2019-1613 with the Ministry of Science and Higher Education of the Russian Federation and Laboratory of Cryptography JetBrains Research.

cipher with such S-boxes be resistant to linear, differential, algebraic and other methods of cryptanalysis. The cryptographic properties of a Boolean (vectorial) function contradict to each other [1, 2]. That is why we try to find vectorial Boolean functions that reach a tradeoff between different cryptographic properties and are constructed using mathematical methods (and not a direct computer search) for their constructing.

In the paper, we propose a simple method of constructing S-boxes using Boolean functions. Let π be an arbitrary permutation on n elements, $\pi \in \mathbb{S}_n$. If $x = (x_1, \ldots, x_n)$ is a binary vector, then let $\pi(x)$ be a vector $\pi(x) = (x_{\pi(1)}, \ldots, x_{\pi(n)})$. Let f be a Boolean function in n variables. Define a vectorial Boolean function $F_\pi : \mathbb{F}_2^n \to \mathbb{F}_2^n$ as follows:

$$F_\pi(x) = (f(x), f(\pi(x)), f(\pi^2(x)), \ldots, f(\pi^{n-1}(x))).$$

We would like to study cryptographic properties of the vectorial Boolean function F_π in dependence on properties of the Boolean function f and the permutation π.

Note that this way of constructing vectorial Boolean functions was already mentioned before but only for obtaining some examples. Thus, A. Udovenko proposed a vectorial Boolean function of this type in 5 variables with the maximal possible algebraic immunity 3. It is a unique known solution of the previously unsolved problem from NSUCRYPTO 2016 [3]. So functions F_π can have good crypto properties.

Separately, we consider the special case of a permutation. Let A_n be the set of all full cycle permutations for n elements. For example, A_4 consists of 6 permutations: $(2,3,4,1)$, $(2,4,1,3)$, $(3,1,4,2)$, $(3,4,2,1)$, $(4,1,2,3)$, $(4,3,1,2)$ presented as vectors or (1234), (1243), (1342), (1324), (1432), (1423) in cyclic representation.

Let us recall definitions of several cryptographic properties.

A Boolean function f in n variables is called *balanced* if it takes every value (0 or 1) the same number of times [4]. A vectorial Boolean function $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ is *balanced* if it takes every value of $\mathbb{F}_2^n$ equally often [2] .

Let $\mathcal{A}_n = \{\langle a, x\rangle \oplus b : a \in \mathbb{F}_2^n, b \in \mathbb{F}_2\}$ be the class of all affine Boolean functions in n variables [5]. The *nonlinearity* $\mathrm{nl}(f)$ of a Boolean function f in n variables is the Hamming distance between f and the set of all affine Boolean functions in n variables [5]. The *nonlinearity* $\mathrm{nl}(F)$ of a vectorial Boolean function F is the minimal nonlinearity of all its component Boolean functions:

$$\mathrm{nl}(F) = \min_{v\in\mathbb{F}_2^n\setminus\{0\}} \mathrm{nl}(F_v) = \min_{v\in\mathbb{F}_2^n\setminus\{0\}} \mathrm{d}(\langle v, F\rangle, \mathcal{A}_n) = \min_{v\in\mathbb{F}_2^n\setminus\{0\}} \min_{g\in\mathcal{A}_n} \mathrm{d}(\langle v, F\rangle, g).$$

The *algebraic degree* of a vectorial Boolean function is the maximal algebraic degree of its component functions [2]. Note that for our construction $\deg(F) = \deg(f)$ for any π, since all coordinate functions of F have degree $\deg(f)$.

For a vectorial Boolean function $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ let δ_F denote the maximal number of solutions for the equation $F(x) \oplus F(x \oplus a) = b$ while a, b run through $\mathbb{F}_2^n$ and a is nonzero. Then F is called *differential δ_F-uniform* [2]. Note that the minimal possible value of δ_F, where F maps from $\mathbb{F}_2^n$ to $\mathbb{F}_2^n$, is 2.

We consider cryptographic properties of F_π for small n in relation to f and π. All of the following propositions are obtained via computer search.

1. Case $n = 2$

- For any permutation $\pi \in \mathbb{S}_2$ there exists a Boolean function f in 2 variables such that $\delta_{F_\pi} = 2$. Moreover, such Boolean functions are constructed as $f(x) = x_1x_2 \oplus a_1x_1 \oplus a_2x_2 \oplus a_0$, where $a_0, a_1, a_2 \in \mathbb{F}_2$.

2. Case $n = 3$

For any Boolean function f in 3 variables $\mathrm{nl}(f) \leqslant 2$.

• For any permutation $\pi \in A_3$ there exists a balanced Boolean function f in 3 variables such that vectorial Boolean function F_π is balanced.

• For any permutation $\pi \in A_3$ it holds $\mathrm{nl}(F_\pi) = \mathrm{nl}(f)$. Note that if $\mathrm{nl}(F_\pi) = 2$, i.e., is maximal, then $\delta_{F_\pi} = 2$, i.e., is minimal possible. The number of such funstions f is 48.

• For an arbitary permutation $\pi \notin A_3$ and Boolean function f in 3 variables $\delta_{F_\pi} \geqslant 4$.

3. Case $n = 4$

Let us introduce the notation for permutations from the set A_4: $\pi_1 = (2,3,4,1)$, $\pi_2 = (4,1,2,3)$, $\pi_3 = (2,4,1,3)$, $\pi_4 = (3,1,4,2)$, $\pi_5 = (3,4,2,1)$, $\pi_6 = (4,3,1,2)$. Note that $\pi_1^{-1} = \pi_2$, $\pi_3^{-1} = \pi_4$, $\pi_5^{-1} = \pi_6$.

• For any permutation $\pi \in A_4^1$ and a balanced Boolean function f in 4 variables such that $\delta_{F_\pi} = 2$, F_π is not balanced.

• For any permutation $\pi \in A_4^1$ there exists a Boolean function f in 4 variables such that if $\delta_{F_\pi} = 2$ and nonlinearity of f and F_π are the same, then $\delta_{F_{\pi^{-1}}} = 2$. Moreover, nonlinearity of $F_{\pi^{-1}}$ and f coincide.

• For any permutation $\pi \notin A_4^1$ for an arbitary Boolean function f in 4 variables $\delta_{F_\pi} \geqslant 4$.

Based on the results, we suppose that it is possible to construct vectorial Boolean functions in the arbitrary number of variables with cryptographic properties good enough using our simple construction for necessary Booleans functions and permutations.

We plan to use our program for studying vectorial Boolean functions with larger number of variables, now this work is in progress.

REFERENCES

1. *Cusick T. W. and Stănică P.* Cryptographic Boolean Functions and Applications. USA, Acad. Press, Elsevier, 2009.
2. *Carlet C.* Vectorial Boolean functions for cryptography. Y. Crama and P. Hammer (eds.) Boolean Models and Methods in Mathematics, Computer Science, and Engineering. Cambridge, Cambridge University Press, 2010, pp. 398–470.
3. *Tokareva N., Gorodilova A., Agievich S., et al.* Mathematical methods in solutions of the problems presented at the Third International Students' Olympiad in Cryptography. Prikladnaya Diskretnaya Matematika, 2018, no. 40, pp. 34–58.
4. *Carlet C.* Boolean functions for cryptography and error-correcting codes. Y. Crama and P. Hammer (eds.) Boolean Models and Methods in Mathematics, Computer Science, and Engineering. Cambridge, Cambridge University Press, 2010, pp. 257–397.
5. *Logachev O. A., Salnikov A. A., Smyshlyaev S. V., and Yaschenko V. V.* Bulevy funktsii v teorii kodirovaniya i kriptologii [Boolean Functions in Coding Theory and Cryptology]. Moscow, MCCME Publ., 2012. 584 p. (in Russian)