UDC 519.7 DOI 10.17223/2226308X/13/12

ON ONE-TO-ONE PROPERTY OF A VECTORIAL BOOLEAN FUNCTION OF THE SPECIAL TYPE[1]

M. M. Zapolskiy, N. N. Tokareva

S-boxes are widely used in cryptography. In particular, they form important components of SP and Feistel networks. Mathematically, S-box is a vectorial Boolean function $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ that should satisfy several cryptographic properties. Usually $n = m$. We study one-to-one property of a vectorial Boolean function constructed in a special way on the base of a Boolean function and a permutation on n elements. The number of all one-to-one functions of this type is calculated.

Keywords: *Boolean function, vectorial Boolean function, S-box.*

Let $\pi \in S_n$ be a permutation such that $\pi^n(x) = x$. Consider some $x \in \mathbb{F}_2^n$, $x = (x_1, \ldots, x_n)$, define $\pi(x) = (x_{\pi(1)}, \ldots, x_{\pi(n)})$. Let f be a Boolean function in n variables, we construct vectorial Boolean function $F_\pi : \mathbb{F}_2^n \to \mathbb{F}_2^n$ by the following rule:

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

Let $\Delta_{\pi,n}$ be the set of all these functions. Define $\rho(x) = (x_n, x_1, x_2, \ldots, x_{n-1})$, i.e., $\rho = (n, 1, 2, \ldots, n-1)$.

Proposition 1. Let $\pi \in S_n$ be such that $\pi^n(x) = x$, $F_\pi \in \Delta_{\pi,n}$. Then $F_\pi(\pi(x)) = \rho^{-1}(F_\pi(x))$ for all $x \in \mathbb{F}_2^n$.

We define action of π on $\mathbb{F}_2^n$ by the rule: if $x \in \mathbb{F}_2^n$, then $x \circ \pi = \pi(x)$. This action splits $\mathbb{F}_2^n$ into orbits with respect to π. If x is in some orbit o, we call x *a generator of* o. We call $O_\pi(x)$ *the orbit with respect to the action of* π.

Example 1. For $n = 4$, the set $\mathbb{F}_2^n$ is divided into six orbits with respect to the permutation ρ:

$O_\rho((0,0,0,0))$	$(0,0,0,0)$
$O_\rho((1,0,0,0))$	$(1,0,0,0), (0,1,0,0), (0,0,1,0), (0,0,0,1)$
$O_\rho((1,0,1,0))$	$(1,0,1,0), (0,1,0,1)$
$O_\rho((1,0,0,1))$	$(1,0,0,1), (1,1,0,0), (0,1,1,0), (0,0,1,1)$
$O_\rho((0,1,1,1))$	$(0,1,1,1), (1,0,1,1), (1,1,0,1), (1,1,1,0)$
$O_\rho((1,1,1,1))$	$(1,1,1,1)$

We denote by $\Theta_{\pi,n}$ the set of all orbits with respect to the action of π on $\mathbb{F}_2^n$. Proposition 1 implies that, for arbitrary $F_\pi \in \Delta_{\pi,n}$, values of elements of some π-orbit $g \in \Theta_{\pi,n}$ are elements of some ρ-orbit $q \in \Theta_{\rho,n}$, since $F_\pi(\pi^i(x)) = \rho^{-i}(F_\pi(x))$. Let $M^k_{\pi,n} = \{g \in \Theta_{\pi,n} : |g| = k\}$.

Let $\Psi_{F_\pi,n} : \Theta_{\pi,n} \to \Theta_{\rho,n}$ be a mapping defined by the rule $\Psi_{F_\pi,n}(O_\pi(x)) = O_\rho(F_\pi(x))$. Now we can formulate conditions for F_π to be one-to-one in terms of $\Psi_{F_\pi,n}$.

Theorem 1. $F_\pi \in \Delta_{\pi,n}$ is an one-to-one function if and only if $\Psi_{F_\pi,n}$ is one-to-one. If $\Psi_{F_\pi,n}$ is one-to-one, then $|\Psi_{F_\pi,n}(g)| = |g|$, for all $g \in \Theta_{\pi,n}$.

As a corollary of Theorem 1, we obtain the following result.

[1]The work was carried out within the framework of the state contract of the Sobolev Institute of Mathematics (project no. 0314-2019-0017) and supported by RFBR (project no. 18-07-01394) and Laboratory of Cryptography JetBrains Research.

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.