Noname manuscript No.
(will be inserted by the editor)

Generalization of Statistical Criteria for Sboxes

S. M. Dehnavi · A. Mahmoodi Rishakani · M. R. Mirzaee Shamsabad · Einollah Pasha

Received: date / Accepted: date

Abstract Linear and differential cryptanalysis and their generalizations are the most important tools in statistical analysis of symmetric ciphers. These attacks make use of linear and differential properties of Sboxes or component functions of symmetric ciphers. In this article, we investigate generalized statistical properties for Sboxes. We justify the application of linear, differential and differential-linear cryptanalysis from the mathematical viewpoint. We verify some well-known Sboxes and vectorial Boolean functions by the proposed criteria and show that these functions have larger biases compared with previous criteria presented up to now.

Keywords Linear Cryptanalysis · Differential Cryptanalysis · Differential-Linear Cryptanalysis · Nonlinear Cryptanalysis

1 Introduction

Linear and differential cryptanalysis and their generalizations are the most important statistical attacks against symmetric ciphers: various symmetric ciphers have been analyzed by these attacks [3,2,4,6,22,17,21,19,18,11,7]. Statistical attacks like linear and differential cryptanalysis make use of statistical

Kharazmi University
Tehran, Iran
E-mail: std_dehnavism@khu.ac.ir

Shahid Rajaee Teacher Training University
Tehran, Iran

Shahid Bahonar University
Kerman, Iran

Kharazmi University
Tehran, Iran

criteria for component functions of symmetric ciphers and then use these criteria to build a distinguisher for symmetric ciphers or to recover the secret key of them.

Various criteria for designing "good" Sboxes from the viewpoint of a designer have been proposed up to now [8,24,23,20]. Some of these criteria can be used directly to design suitable Sboxes or to mount attacks against symmetric ciphers, while the other are pure mathematical criteria which measure the randomness of ciphers.

In this article, we introduce new generalized criteria for Sboxes. In [9, 10] we have investigated generalized linear, differential and differential-linear criteria for Sboxes. One of the consequences of our general theorems is generalizing the linear criteria to nonlinear criteria which justifies the rationale for "generalized linear cryptanalysis" in [12]. The other result of our general theorems is introducing linear criteria in finite fields with dimensions greater than one and for linear transformations from F_2^n onto its subspaces of dimensions more than one: this is similar to what is stated in [15,14,13]. Justification of generalized differential properties along with differential-linear criteria [1,5, 11] is also amongst the consequences of our theorems. In fact, our theorems justify the application of the criteria used in some papers like [15,14,13,1,5, 11] from the mathematical viewpoint. On the other hand, with the aid of our proposed criteria, we can restrict the input of an Sbox to a subset of the whole space and then, verify the restricted map by generalized linear, differential and differential-linear criteria.

We have verified some well-known Sboxes and vectorial Boolean functions by the proposed criteria: the Sbox of AES (Advanced Encryption Standard) and the inverse map over the field $F_{2^{16}}$ are verified by programming. Our results show that these Sboxes have larger biases in comparison to the largest bias of conventional criteria like linear bias.

In Section 2, we present basic notations and definitions. Section 3 discusses generalized linear criteria in finite stes. In Section 4, we study two-dimensional criteria for Sboxes. Section 5 is the conclusion.

2 Preliminary Notations and Definitions

In this paper, the number of elements or cardinality of a finite set A is denoted by $|A|$. For a function $f : A \to B$, the preimage of an element $b \in B$ is defined as $\{a \in A | f(a) = b\}$ and is denoted by $f^{-1}(b)$. Suppose that $f : A \to A$ is a function. If we have $f(a) = a$ for $a \in A$, then we say that a is a fixed point of f. We denote by F_2^n the Cartesian product of n copies of F_2, the finite field with two elements. The set of all $n \times n$ matrices over a set A is denoted by $\mathcal{M}_n(A)$, the ring of integers modulo 2^n by Z_{2^n} and the finite field with 2^n elements by F_{2^n}. We denote the zero vector of any size by $\mathbf{0}$ and the transpose of a matrix A by A^T. The XOR operation is denoted by $\oplus$ and modular addition by $+$.

Let A and B be two finite sets. The set of all mappings $f : A \to B$ is denoted by $\mathcal{F}(A, B)$ and set of all functions $f : F_2^n \to F_2^m$ is denoted by $\mathcal{B}_{n,m}$.

If $f \in \mathcal{B}_{n,1}$, then we say that f is a Boolean function and if $f \in \mathcal{B}_{n,m}$ with $m > 1$, then we say that f is a Boolean map or an Sbox. Suppose that A and B are two finite sets with $|A| = \mathbf{t}|B|$, $f \in \mathcal{F}(A, B)$ and for every $b \in B$ we have $|f^{-1}(b)| = \mathbf{t}$. In this case, f is called balanced. Suppose that A, B and C are three finite sets such that $|B| = \mathbf{e}|C|$, $f \in \mathcal{F}(B \times A, C)$ and for each $c \in C$ and $a \in A$ we have

$$|\{x \in B | f(x, a) = c\}| = \mathbf{e};$$

then we say that f is parametrically balanced with respect to the second argument. Suppose that A, A' and B are finite sets with $A' \subseteq A$ and $f : A \to B$ is a function. The restriction of f to A' is denoted by $f|_{A'}$.

We know that F_2^n is a linear space. The rank of a linear transformation T in $\mathcal{B}_{n,m}$ is denoted by $r(T)$ and the nullity of T is denoted by $n(T)$. If $r(T) = m$, then we say that T is of full rank. The standard dot product in F_2^n is denoted by ".".

3 Generalized Linear Criteria

Linear bias of an Sbox is a well-known concept in symmetric cryptography. In this section, we lay a mathematical foundation for this concept and also for generalized linear cryptanalysis [12,7,15,14].

Theorem 1 *Suppose that A, A', B and C are nonempty finite sets with $A' \subseteq A$, $|A| = \mathbf{a}$, $|A'| = \mathbf{a}'$, $|B| = \mathbf{b}$, $|C| = \mathbf{c}$ and $\mathbf{b} = \mathbf{ec}$ and suppose that $c \in C$, $f : A' \to A$, $g : B \to B$ and $h : B \times A \to C$ are given. Moreover, suppose that f is an injection, g is a permutation and h is parametrically balanced with respect to the second argument. Now, if $x \in A'$ and $S \in \mathcal{F}(A, B)$ are uniformly distributed, then we have*

$$\mathcal{P}\left(h\left(g(S|_{A'}(x)), f(x)\right) = c\right) = \frac{1}{\mathbf{c}}.$$

Proof Put

$$\mathcal{A} = \{(x, S) | x \in A', S \in \mathcal{F}(A, B), h\left(g(S|_{A'}(x)), f(x)\right) = c\},$$

and

$$\mathcal{A}_x = \{(x, S) | S \in \mathcal{F}(A, B), h\left(g(S|_{A'}(x)), f(x)\right) = c\}, \quad x \in A'.$$

We count the number of elements in $\mathcal{A}_x$ for each x. There are $\mathbf{e}$ choices for $S \in \mathcal{F}(A, B)$ to choose the image of x in order to have $h\left(g(S|_{A'}(x)), f(x)\right) = c$. The image of the remaining elements in A has $\mathbf{b}^{(\mathbf{a}-\mathbf{a}')+(\mathbf{a}'-1)} = \mathbf{b}^{\mathbf{a}-1}$ choices. Therefore,

$$|\mathcal{A}_x| = \mathbf{e}\mathbf{b}^{\mathbf{a}-1};$$

and since $\{\mathcal{A}_x | x \in A'\}$ is a partition of $\mathcal{A}$, we get

$$\mathcal{P}(h\left(g(S|_{A'}(x)), f(x)\right) = c) = \frac{\mathbf{a}'\mathbf{e}\mathbf{b}^{\mathbf{a}-1}}{\mathbf{a}'\mathbf{b}^{\mathbf{a}}} = \frac{\mathbf{e}}{\mathbf{b}} = \frac{1}{\mathbf{c}}.$$

Corollary 1 *Suppose that $x \in F_2^n$ and $S \in \mathcal{B}_{n,m}$ are uniformly distributed. Then for any permutation $f \in \mathcal{B}_{n,n}$ and every fixed nonzero $c_1 \in F_2^n$ and $c_2 \in F_2^m$ we have*

$$\mathcal{P}(c_1 \cdot f(x) \oplus c_2 \cdot S(x) = 0) = \frac{1}{2}.$$

Proof In Theorem 1 put $A = A' = F_2^n$, $B = F_2^m$, $C = F_2$, $f(x) = x$, $g(x) = x$ and $h(x_1, x_2) = c_1 \cdot x_2 \oplus c_2 \cdot x_1$.

Example We have verified the inverse Sbox

$$S : F_{2^{16}} \to F_{2^{16}},$$

$$S(x) = x^{-1},$$

over $F_{2^{16}}$ defined by irreducible polynomial $x^{16} + x^5 + x^3 + x^2 + 1$. We have explored S with the aid of the criterion in Corollary 1 and have found some masks by programming: for example for $c_1 = 0x59b$, $c_2 = 0x6205$ and

$$f(x) = 4x^2 + x + 1 \ mod\ 65536,$$

we have:

$$P\left(c_1 \cdot f(x) = c_2 \cdot S(x)\right) = \frac{1}{2} - \frac{686}{65536}.$$

We note that the bias $\frac{686}{65536}$ is quite larger than the largest linear bias of S, i.e. $\frac{256}{65536}$.

Corollary 2 *Suppose that $x \in F_2^n$ and $S \in \mathcal{B}_{2n,2n}$ are uniformly distributed. Then for any fixed nonzero $c_1 \in F_2^{2n}$ and $c_2 \in F_2^n$ we have*

$$\mathcal{P}(c_1 \cdot x \oplus (\mathbf{0}, c_2) \cdot S(\mathbf{0}, x) = 0) = \frac{1}{2}.$$

Here, $(0, x)$ is a vector of length $2n$ whose n least significant bits are equal to x and its n most significant bits are zero.

Proof In Theorem 1 put $A = F_2^{2n}$, $A' = \{\mathbf{0}\} \times F_2^n$, $B = F_2^{2n}$, $C = F_2$, $f(x) = (\mathbf{0}, x)$, $g(x) = x$ and $h(x_1, x_2) = c_1 \cdot x_1 \oplus (\mathbf{0}, c_2) \cdot x_2$.

One of the results of Theorem 1 is the criteria used in conventional linear cryptanalysis.

Theorem 2 *Suppose that $x \in F_2^n$ and $S \in \mathcal{B}_{n,m}$ are uniformly distributed. Then for any fixed $a \in F_2^n$ and every fixed nonzero $b \in F_2^m$, we have*

$$\mathcal{P}(a \cdot x \oplus b \cdot S(x) = 0) = \frac{1}{2}.$$

Proof In Theorem 1 put $A = A' = F_2^n$, $B = F_2^m$, $C = F_2$, $f(x) = x$, $g(x) = x$ and $h(x_1, x_2) = b \cdot x_1 \oplus a \cdot x_2$.

Now, we have a result which is a generalization for the concept of linear bias that is used in linear cryptanalysis. This theorem resembles [12].

Theorem 3 *If $x \in F_2^n$ and $S \in \mathcal{B}_{n,m}$ are uniformly distributed, then for each given Boolean function $\phi \in \mathcal{B}_{n,1}$ and every given balanced Boolean function $\psi \in \mathcal{B}_{m,1}$, we have*

$$\mathcal{P}(\phi(x) \oplus \psi(S(x)) = 0) = \frac{1}{2}.$$

Proof In Theorem 1 put $A = A' = F_2^n$, $B = F_2^m$, $C = F_2$, $f(x) = x$, $g(x) = x$ and $h(x_1, x_2) = \psi(x_1) \oplus \phi(x_2)$.

Theorem 4, in some sense, is presented in [1].

Theorem 4 *Suppose that $x \in F_2^n$ and $S \in \mathcal{B}_{n,m}$ are uniformly distributed, $n = kt$ and $m = st$. Then for any fixed $a_i \in F_{2^t}$, $0 \leq i < k$, and every fixed $b_i \in F_{2^t}$, $0 \leq i < s$, such that all of b_i's are not zero simultaneously, and each given $c \in F_{2^t}$ we have*

$$\mathcal{P}\left(\bigoplus_{i=0}^{k-1}(a_i \bullet x_i) \oplus \bigoplus_{j=0}^{s-1}(b_j \bullet S(x)_j) = c\right) = \frac{1}{2^t}.$$

Here, "$\bullet$" is the operator of multiplication in F_{2^t}, and

$$S(x) = (S(x)_{s-1}, \ldots, S(x)_0),$$

with $S(x)_i \in F_{2^t}$, $0 \leq i < s$.

Proof In Theorem 1 put $A = A' = F_2^n$, $B = F_2^m$, $C = F_{2^t}$, $f(x) = x$, $g(x) = x$ and $h(x_1, x_2) = \psi(x_1) \oplus \phi(x_2)$ with

$$\phi(x) = f(x_{k-1}, \ldots, x_0) = \bigoplus_{i=0}^{k-1}(a_i \bullet x_i),$$

$$\psi(x) = f(x_{s-1}, \ldots, x_0) = \bigoplus_{j=0}^{s-1}(b_j \bullet x_j).$$

Theorem 4 introduced a generalized linear criterion. Now, we present a generalized nonlinear criterion.

Theorem 5 *Suppose that $x \in F_2^n$ and $S \in \mathcal{B}_{n,m}$ are uniformly distributed and $1 \leq t \leq \min\{m, n\}$. Then for each given Boolean map $\phi \in \mathcal{B}_{n,t}$ and every given balanced $\psi \in \mathcal{B}_{m,t}$ and for each fixed $c \in F_2^t$, we have*

$$\mathcal{P}(\phi(x) \oplus \psi(S(x)) = c) = \frac{1}{2^t}.$$

Proof In Theorem 1 put $A = A' = F_2^n$, $B = F_2^m$, $C = F_2^t$ and $h(x_1, x_2) = \psi(x_1) \oplus \phi(x_2)$.

In Lemma 1, we use theorem 2 of Section 3.1 in [16].

Lemma 1 *Any linear transformation T in $\mathcal{B}_{n,t}$ with $n \geq t$ and $r(T) = t$ is balanced.*

Proof We know that $n(T) = n - t$ and the null space of T is a subspace F_2^n; so $|T^{-1}(0)| = 2^{n-t}$, and for any $y \in F_2^t$ we have

$$|T^{-1}(y)| = |T^{-1}(0)| = 2^{n-t}.$$

The following theorem is, in some sense, a generalization of Theorem 4.

Theorem 6 *If $x \in F_2^n$ and $S \in \mathcal{B}_{n,m}$ are uniformly distributed and $1 \leq t \leq \min\{n, m\}$, then for any given linear transformation T in $\mathcal{B}_{n,t}$ and every given full rank linear transformation R in $\mathcal{B}_{m,t}$ and for each fixed $c \in F_2^t$, we have*

$$\mathcal{P}(T(x) \oplus R(S(x)) = c) = \frac{1}{2^t}.$$

Proof See Theorem 5 and Lemma 1.

4 Generalized Differential-Linear and (Nonlinear) Two-Dimensional Criteria

In this section, we introduce some kind of differential-linear criteria and also we present two-dimensional (nonlinear) properties for Sboxes. The next theorem justifies the reasoning for criteria presented in [1,5].

Theorem 7 *Suppose that $(G_1, *)$ and $(G_2, \bullet)$ are two finite Abelian groups and $a \in G_1$ and $b \in G_2$ are given such that a is not the identity of G_1. If $x \in G_1$ and $S \in \mathcal{F}(G_1, G_2)$ are uniformly distributed, then we have*

$$\mathcal{P}(S(x) \bullet S(x * a) = b) = \frac{1}{|G_2|}.$$

Proof Put

$$\mathcal{A} = \{(x, S) | x \in G_1, S \in \mathcal{F}(G_1, G_2), S(x) \bullet S(x * a) = b\},$$

and

$$\mathcal{A}_x = \{(x, S) | S \in \mathcal{F}(G_1, G_2), S(x) \bullet S(x * a) = b\}, \quad x \in G_1.$$

We count the number of elements in $\mathcal{A}_x$ for each x. There are $|G_2|$ choices for $S \in \mathcal{F}(G_1, G_2)$ to choose the image of the fixed element $x \in \mathcal{A}$, or equivalently, to choose $S(x)$; since we should have

$$S(x) \bullet S(x * a) = b,$$

the image of $S(x * a)$ is uniquely determined. The image of the remaining elements in A, has $|G_2|^{|G_1|-2}$ choices. Therefore,

$$|A_x| = |G_2||G_2|^{|G_1|-2} = |G_2|^{|G_1|-1};$$

and since $\{\mathcal{A}_x | x \in A\}$ is a partition of $\mathcal{A}$, we get,

$$\mathcal{P}(S(x) \bullet S(x * a) = b) = \frac{|\mathcal{A}|}{|G_1||G_2|^{|G_1|}} = \frac{|G_1||G_2|^{|G_1|-1}}{|G_1||G_2|^{|G_1|}} = \frac{1}{|G_2|}.$$

If we consider the groups $(F_2^n, \oplus)$, $(Z_{2^n}, +)$, $(F_2^m, \oplus)$ and $(Z_{2^m}, +)$, then the next corollary is a direct result of Theorem 7.

Corollary 3 *Suppose that $a \in F_2^n - \{\mathbf{0}\}$ and $b \in F_2^m$ are given. If $x \in F_2^n$ and $S \in \mathcal{B}_{n,m}$ are uniformly distributed, then we have*

$$\mathcal{P}(S(x) \oplus S((x+a) \mod 2^n) = b) = \frac{1}{2^m},$$

$$\mathcal{P}(S(x) + S((x+a) \mod 2^n) \mod 2^m = b) = \frac{1}{2^m},$$

$$\mathcal{P}(S(x) + S(x \oplus a) \mod 2^m = b) = \frac{1}{2^m}.$$

The following corollary which is also a direct result of Theorem 7, justifies the application of conventional differential cryptanalysis, from the mathematical viewpoint.

Corollary 4 *Suppose that $a \in F_2^n - \{\mathbf{0}\}$ and $b \in F_2^m$ are given. If $x \in F_2^n$ and $S \in \mathcal{B}_{n,m}$ are uniformly distributed, then we have*

$$\mathcal{P}(S(x) \oplus S(x \oplus a) = b) = \frac{1}{2^m}.$$

Theorem 8 *Suppose that A, A', B and C with $|A| = \mathbf{a}$, $|A'| = \mathbf{a}'$, $|B| = \mathbf{b}$ and $|C| = \mathbf{c}$ are finite sets such that $\mathbf{b}^2 = \mathbf{ec}$ and $c \in C$, $f : A' \to A'$ and $g : B \times B \to C$ are given. Moreover, suppose that f is a permutation which does not have any fixed points and g is a balanced map. Now, if $x \in A'$ and $S \in \mathcal{F}(A, B)$ are uniformly distributed, then we have*

$$\mathcal{P}\left(g\left(S|_{A'}(x), S|_{A'}(f(x))\right) = c\right) = \frac{1}{\mathbf{c}}.$$

Proof Put

$$\mathcal{A} = \{(x, S) | x \in A', S \in \mathcal{F}(A, B), g\left(S|_{A'}(x), S|_{A'}(f(x))\right) = c\},$$

and

$$\mathcal{A}_x = \{(x, S) | S \in \mathcal{F}(A, B), g\left(S|_{A'}(x), S|_{A'}(f(x))\right) = c\}, \quad x \in A'.$$

We count the number of elements in $\mathcal{A}_x$ for each x. There are $\mathbf{e}$ choices for $S \in \mathcal{F}(A, B)$ to choose the images of the distinct fixed elements $x \in A'$ and $f(x) \in A'$ in order to have $g\left(S|_{A'}(x), S|_{A'}(f(x))\right) = c$. The image of the remaining elements in A has $\mathbf{b}^{\mathbf{a}-2}$ choices. Therefore,

$$|\mathcal{A}_x| = \mathbf{eb}^{\mathbf{a}-2};$$

and since $\{\mathcal{A}_x | x \in A'\}$ is a partition of $\mathcal{A}$, we get

$$\mathcal{P}(g\left(S|_{A'}(x), S|_{A'}(f(x))\right) = c) = \frac{\mathbf{a}'\mathbf{eb}^{\mathbf{a}-2}}{\mathbf{a}'\mathbf{b}^{\mathbf{a}}} = \frac{\mathbf{e}}{\mathbf{b}^2} = \frac{1}{\mathbf{c}}.$$

We note that, in Theorem 8, if we put $A = A' = G_1$, $B = G_2$, $C = G_2$, $f(x) = x * a$ and $g(x, y) = x \bullet y$, then Theorem 7 is concluded. Next corollary, introduces some kind of differential-linear criteria.

Corollary 5 *Suppose that $a \in F_2^n - \{\mathbf{0}\}$ and $c \in F_2^m - \{\mathbf{0}\}$ are given. If $x \in F_2^n$ and $S \in \mathcal{B}_{n,m}$ are uniformly distributed, then we have*

$$\mathcal{P}\left(c \cdot (S(x) \oplus S(x \oplus a)) = 0\right) = \frac{1}{2}.$$

Proof In Theorem 8, put $A = A' = F_2^n$, $B = F_2^m$ and $C = F_2$ and let $g(x_1, x_2) = c \cdot (x_1 \oplus x_2)$ and $f(x) = x \oplus a$. Satisfaction of the conditions of Theorem 8 are obvious.

Proof of the next two corollaries is not hard.

Corollary 6 *Suppose that $a \in F_2^n - \{\mathbf{0}\}$ and $c_1, c_2 \in F_2^m - \{\mathbf{0}\}$ are given. If $x \in F_2^n$ and $S \in \mathcal{B}_{n,m}$ are uniformly distributed, then we have*

$$\mathcal{P}\left(c_1 \cdot S(x) = c_2 \cdot S(x \oplus a)\right) = \frac{1}{2}.$$

Corollary 7 *Suppose that $a \in Z_{2^n} - \{\mathbf{0}\}$ and $c_1, c_2 \in F_2^m - \{\mathbf{0}\}$ are given. If $x \in F_2^n$ and $S \in \mathcal{B}_{n,m}$ are uniformly distributed, then we have*

$$\mathcal{P}\left(c_1 \cdot S(x) = c_2 \cdot S(x + a \mod 2^n)\right) = \frac{1}{2}.$$

Example We have verified the Sbox of AES which we call S here with the aid of the criterion in Corollary 7 . We have found some masks yielding the maximum bias by programming: for example for $c_1 = 0x5f$, $c_2 = 0xce$ and $a = 0x87$ we have:

$$\mathcal{P}\left(c_1 \cdot S(x) = c_2 \cdot S(x + a \mod 256)\right) = \frac{1}{2} - \frac{42}{256}.$$

We note that the bias $\frac{42}{256}$ is almost three times larger the largest linear bias of S, i.e. $\frac{16}{256}$.
Example We have verified the inverse Sbox

$$S : F_{2^{16}} \to F_{2^{16}},$$

$$S(x) = x^{-1},$$

over $F_{2^{16}}$ defined by irreducible polynomial $x^{16} + x^5 + x^3 + x^2 + 1$. We have explored S with the aid of the criterion in Corollary 7 and have found some masks by programming: for example for $c_1 = 0x9d29$, $c_2 = 0xea61$ and $a = 0xe734$ we have:

$$\mathcal{P}\left(c_1 \cdot S(x) = c_2 \cdot S(x + a \mod 65536)\right) = \frac{1}{2} + \frac{636}{256}.$$

We note that $\frac{636}{65536}$ is quite larger than the largest linear bias of S, i.e. $\frac{256}{65536}$.

Corollary 8 *Suppose that $a \in F_2^n - \{\mathbf{0}\}$ and $B_1, B_2 \in \mathcal{M}_m(F_2)$ are given. Let B_1 and B_2 be nonsingular. Now, if $x \in F_2^n$ and $S \in \mathcal{B}_{n,m}$ are uniformly distributed, then for each $c \in F_2^m$ we have*

$$\mathcal{P}\left(B_1(S(x))^T \oplus B_2(S(x \oplus a))^T = c\right) = \frac{1}{2^m}.$$

Proof In Theorem 8, put $A = A' = F_2^n$, $B = F_2^m$ and $C = F_2^m$ and let $f(x, y) = x \oplus a$ and g be the linear transformation corresponding to the matrix

$$\left(B_1 \ B_2\right),$$

or $g(x_1, x_2) = B_1 x_1^T \oplus B_2 x_2^T$.

We know that every linear map in F_{2^n} is also linear in F_2^n; so we have:

Corollary 9 *Suppose that $\alpha \in F_{2^n}$ and $\beta_1, \beta_2 \in F_{2^m}$ are given nonzero elements. If $x \in F_2^n$ and $S \in \mathcal{B}_{n,m}$ are uniformly distributed, then for each fixed $c \in F_{2^m}$ we have*

$$\mathcal{P}\left(\beta_1 S(x) \oplus \beta_2 S(x \oplus \alpha)) = c\right) = \frac{1}{2^m}.$$

Following theorem, presents a two-dimensional (nonlinear) criterion. We note that for every odd element $a \in Z_{2^n}$, the map

$$f : Z_{2^n} \to Z_{2^n},$$

$$f(x) = ax \ \ mod \ 2^n,$$

is a bijection and for nonzaro element $a \in Z_{2^n}$, the map

$$f : Z_{2^n} \to Z_{2^n},$$

$$f(x) = x + a \ \ mod \ 2^n,$$

has no fixed points. Now, in Theorem 8, if we put $A = A' = Z_{2^n}$, $B = Z_{2^m}$ and $C = Z_{2^m}$, and

$$f : Z_{2^n} \to Z_{2^n},$$

$$f(x) = x + a \ \ mod \ 2^n,$$

and

$$g : Z_{2^m} \times Z_{2^m} \to Z_{2^m},$$

$$g(x_1, x_2) = b(x_1 + x_2) \ \ mod \ 2^m,$$

then we have:

Corollary 10 *Suppose that $a \in Z_{2^n}$ is nonzero and $b \in Z_{2^m}$ is odd. Now, if $x \in F_2^n$ and $S \in \mathcal{B}_{n,m}$ are uniformly distributed, then for each fixed $c \in Z_{2^m}$ we have*

$$\mathcal{P}\left(b(S(x) + S(x + a \ \ mod \ 2^n)) \ \ mod \ 2^m = c\right) = \frac{1}{2^m}.$$

Corollary 10 introduces a nonlinear two-dimensional criteria. The following corollary, introduces a two-dimensional linear criterion.

Corollary 11 *Suppose that $a \in F_2^n$ and $B \in \mathcal{M}_m(F_2)$ are given. Also, suppose that a is nonzero and B is nonsingular. Now, if $x \in F_2^n$ and $S \in \mathcal{B}_{n,m}$ are uniformly distributed, then for each given $c \in F_2^m$ we have*

$$\mathcal{P}\left(B(S(x) \oplus S(x \oplus a))^T = c\right) = \frac{1}{2^m}.$$

Proof In Theorem 8, put $A = A' = F_2^n$, $B = F_2^m$ and $C = F_2^m$ and let $f(x) = x \oplus a$ and g be the linear transformation corresponding to the matrix

$$\left(B\ B\right),$$

or $g(x_1, x_2) = Bx_1^T \oplus Bx_2^T$.

Corollary 12 *Suppose that $\alpha \in F_{2^n}$ and $\beta \in F_{2^m}$, are given nonzero elements. If $x \in F_2^n$ and $S \in \mathcal{B}_{n,m}$ are uniformly distributed, then for each given $c \in F_{2^m}$ we have,*

$$\mathcal{P}\left(\beta(S(x) \oplus S(x \oplus \alpha)) = c\right) = \frac{1}{2^m}.$$

5 Conclusion

Linear and differential cryptanalysis and their generalizations, are the most important statistical attaks against symmetric ciphers. These attacks make use of linear and differential properties of Sboxes or component functions of symmetric ciphers.

In this paper, we investigated generalized statistical properties for Sboxes. We justified the application of linear, differential and differential-linear cryptanalysis from the mathematical viewpoint. We verified some well-known Sboxes and vectorial Boolean functions by the proposed criteria.

We believe that the generalized criteria presented in this paper, can be used for defining new generalized parameters for Sboxes and also in attacking symmetric ciphers or devising new statistical tests with the help of these new generalized criteria.

References

1. Thomas Baigneres, Quantitative Security of Block Ciphers: Design and Cryptanalysis Tools, ECOLE POLYTECHNIQUE FEDERALE DE LAUSANNE, Phd Thesis, Suisse, 2008.
2. E. Biham and A. Shamir, "Differential Cryptanalysis of DES-like Cryptosystems", Journal of Cryptology, vol. 4, no. 1, pp. 3-72, 1991.
3. E. Biham and A. Shamir, Differential Cryptanalysis of the Data Encryption Standard, Springer-Verlag, 1993.

4. J. Borst, B. Preneel, and J. Vandewalle, Linear Cryptanalysis of RC5 and RC6, In Lars R. Knudsen, editor, Fast Software Encryption, 6th International Workshop, FSE99, Rome, Italy, March 24-26, 1999, volume 1636 of Lecture Notes in Computer Science, pages 16-30, Berlin, 1999. Springer-Verlag.
5. Claude Carleta, Cunsheng Ding, "Highly nonlinear mappings", Journal of Complexity, 20(2-3): 205-244 (2004)
6. J. Y. Cho and Pieprzyk. Distinguishing attack on Sober-128 with linear masking. In Information Security and Privacy 2006, volume 4058 of Lecture Notes in Computer Science, pages 29-39. Springer-Verlag, 2006a.
7. J. Y. Cho, M. Hermelin, and K. Nyberg. A New Technique for Multidimensional Linear Cryptanalysis with Applications on Reduced Round Serpent. In ICISC, pages 383398, 2008.
8. M.H. Dawson and S.E. Tavares. An expanded set of S-box design critena based on information theory and its relation to differential attacks. Advances in Cryptology: Pruc. of EUROCRYPT '91. Springer-Verlag. pp. 352-365, 1992.
9. S. M. Dehnavi, A. Mahmoodi Rishakani, M. R. Mirzaee Shamsabad and Einollah Pasha, "Generalization of Statistical Criteria for Sboxes", 9th International Conference on Information Security and Cryptology (ISCISC'12), University of Tabriz, Tabriz, Iran, 2012
10. S. M. Dehnavi, A. Mahmoodi Rishakani, M. R. Mirzaee Shamsabad and Einollah Pasha, "Generalization of Differential Criteria for Sboxes", 11th International Conference on Information Security and Cryptology (ISCISC'14), University of Tehran, Tehran, Iran, 2014
11. Orr Dunkelman, Sebastiaan Indesteege, and Nathan Keller. A Differential-Linear Attack on 12-Round Serpent. In D. R. Chowdhury, V. Rijmen, and A. Das, editors, INDOCRYPT, volume 5365 of LNCS, pages 308-321. Springer, 2008.
12. C. Harpes, G. Kramer, and J.L. Massey. A generalization of linear cryptanalysis and the applicability of Matsuis piling-up lemma. In Advances in Cryptology EUROCRYPT95, volume 921 of LNCS, pages 24-38. Springer-Verlag, 1995.
13. Miia Hermelin, Kaisa Nyberg: Dependent Linear Approximations: The Algorithm of Biryukov and Others Revisited. CT-RSA 2010: 318-333
14. Miia Hermelin, Joo Yeon Cho, Kaisa Nyberg: Multidimensional Extension of Matsui's Algorithm 2. FSE 2009: 209-227
15. Miia Hermelin, Kaisa Nyberg: Multidimensional linear distinguishing attacks and Boolean functions. Cryptography and Communications 4(1): 47-64 (2012)
16. K. H. Hoffman and R. Kunze. Linear Algebra, 2nd ed. Prentice-Hall, Upper Saddle River, NJ, 1971.
17. Jovan Dj. Golic, Vittorio Bagini, and Gugliemo Morgari, Linear Cryptanalysis of Bluetooth Stream Cipher, EUROCRYPT'02, pages 238-255 (2002)
18. L. Knudsen and M.J.B. Robshaw, "Nonlinear Approximations in Linear Cryptanalysis", Advances in Cryptology - EUROCRYPT 96 (Lecture Notes in Computer Science no. 1070), Springer-Verlag, pp. 224-236, 1996.
19. L.R. Knudsen, "Truncated and Higher Order Differentials", Fast Software Encryption (Lecture Notes in Computer Science no. 1008), Springer-Verlag, pp. 196-211, 1995.
20. Yuan Li, Thomas W. Cusick: Strict avalanche criterion over finite fields. J. Mathematical Cryptology 1(1): 65-78 (2007)
21. Mitsuru Matsui, Linear cryptanalysis method for DES cipher, EUROCRYPT93, volume 765 of Lecture Notes in Computer Science, pages 386-397, Springer (1993)
22. K. Nyberg and J. Wallen, "Improved linear distinguishers for SNOW 2.0", In Fast Software Encryption 2006, volume 4047 of Lecture Notes in Computer Science, pages 144-162. Springer-Verlag 2006.
23. M.G. Parker, "Generalised S-Box Nonlinearity", NESSIE Public Document - NES/DOC/UIB/WP5/020/A, https://www.cosic.esat. kuleuven.ac.be/nessie/reports/phase2/SBoxLin.pdf 11 Feb, 2003.
24. A.M. Youssef and S.E. Tavares. Information leakage of randornly selected boolean functions. Information Theory and Applications II, 4th Canadiun Workshop On Information Theory. May 1995, LNCS 1133, pp. 41 -52, Springer-Verlag, 1996.