

Relationships between Boolean Functions and Symmetric Groups

Chengxin Qu, Jennifer Seberry, Josef Pieprzyk
Center for Computer Security Research
School of Information Technology and Computer Science
University of Wollongong
Email: cxq01,jennie,josef@uow.edu.au

Abstract

We study the relations between boolean functions and symmetric groups. We consider elements of a symmetric group as variable transformation operators for boolean functions. Boolean function may be fixed or permuted by these operators. We give some properties relating the symmetric group S_n and boolean functions on V_n .

1 Introduction

The values of a boolean function for each vector in V_n form a binary sequence of length 2^n called the trace of the function. The trace of a boolean function is widely used in communication systems such as *DES* and S-box theory [1, 2]. To protect against cryptographic attacks boolean functions must satisfy some algebraic properties such as nonlinearity, balance, the propagation criteria and correlation immunity. These are called cryptographic properties [6, 8, 11]. In this paper, we use symmetric groups to study boolean functions. The transformation of variables, $x_i \rightarrow x_j$, is called an operation or a variable transformation operator. We consider elements in the symmetric group as a variable exchange operators for boolean functions. We study the conditions under which a boolean function is fixed or transformed by this operation.

2 Background

2.1 Boolean space and boolean functions

The set of n -tuple vectors,

$$V_n = \{\alpha = (a_1, \dots, a_n) \mid a_i \in GF(2), i = 1, \dots, n\},$$

is a *boolean space* if its arithmetic is in a Galois field. A boolean space V_n contains 2^n vectors. Clearly, all the vectors in V_n are binary sequences. A *boolean function* is defined on V_n by the mapping

$$f(x) : V_n \rightarrow V_1$$

where x is a variable vector in V_n .

There are several ways to represent a boolean function: by a polynomial; by a binary sequence; and by a $(-1, 1)$ sequence. Here we use the polynomial representation to discuss boolean functions. Let $x^\alpha = x_1^{a_1} x_2^{a_2} \dots x_n^{a_n}$ denote a monomial on V_n . Then a boolean function on V_n is a linear combination of monomials

$$f(x) = \bigoplus_{\alpha \in V_n} c_\alpha x^\alpha \quad c_\alpha = 0 \text{ or } 1, \quad (1)$$

where the sign \oplus denotes boolean addition (XOR).

For any two binary sequences ξ and η with the same length s , we define their multiplication (\times) and binary addition (\oplus) as follows;

$$\begin{aligned} \xi \times \eta &= (a_1, a_2, \dots, a_s) \times (b_1, b_2, \dots, b_s) \\ &= (a_1 b_1, a_2 b_2, \dots, a_s b_s) \end{aligned} \quad (2)$$

$$\begin{aligned} \xi \oplus \eta &= (a_1, a_2, \dots, a_s) \oplus (b_1, b_2, \dots, b_s) \\ &= (a_1 \oplus b_1, a_2 \oplus b_2, \dots, a_s \oplus b_s). \end{aligned} \quad (3)$$

So $\xi \times \eta$ and $\xi \oplus \eta$ are still binary sequences. If $f(x)$ corresponds to the binary sequence ξ and $g(x)$ corresponds to η , then the functions $f(x)g(x)$ and $f(x) \oplus g(x)$ correspond to formulae (2) and (3) respectively.

We call the number of 1s in a binary sequence, ξ , its *Hamming weight* that is denoted by $wt(\xi)$. A vector in V_n is a binary sequence with length n and the values of a boolean function for each vector in V_n also form a length 2^n binary sequence that we call the *trace* of the function. For any two functions $f(x)$ and $g(x)$, their *Hamming distance* is the number of 1s in the sequence of the function $f(x) \oplus g(x)$. The function (1), with the restriction such that $c_\alpha = 0$ for all α where $wt(\alpha) > 1$, is called an *affine function* and denoted by $\varphi(x)$. Using the dot product we can write affine functions with the form

$$\varphi(x) = \alpha \cdot x \oplus c,$$

where $\alpha \in V_n$, $c = 0, 1$. An affine function is called a *linear function* if $c = 0$ (which corresponds $c_0 = 0$ in the function (1)). The following definitions are the most important cryptographic parameters for a boolean functions in cryptography [3, 9, 10].

Definition 1 Let $f(x)$ be a function on V_n . If, as x runs through all vectors in V_n , $f(x) = 1$ is true 2^{n-1} times $f(x) = 1$, then the function $f(x)$ is said to be *balanced*.

Definition 2 Let $f(x)$ be a function on V_n . The *nonlinearity* (denoted by N_f) of the function $f(x)$ is defined by the minimum Hamming distance from $f(x)$ to all affine functions over V_n i.e.

$$N_f = \min\{wt(f \oplus \varphi) \mid \text{for all } \varphi \text{ on } v_n\}.$$

Definition 3 Let $f(x)$ be a boolean function on V_n . If for a vector $\alpha \in V_n$ the function $f(x) \oplus f(x \oplus \alpha)$ is balanced, then the function $f(x)$ is said to have *propagation criteria with respect to the vector α* . If $f(x)$ has propagation criteria with respect to all vectors with $0 < wt(\alpha) \leq k$, then $f(x)$ has propagation criteria of degree k denoted by $PC(k)$. If $k = 1$, the function is said to satisfy the *strict avalanche criteria (SAC)*.

Definition 4 Let $0 \leq k \leq n$. The function $f(x)$ on V_n is *k -th order correlation immune* if the following equation

$$\sum_{x \in V_n} (-1)^{f(x) \oplus \alpha \cdot x} = 0, \quad \text{for } 1 \leq wt(\alpha) \leq k,$$

is satisfied, where $wt(\alpha)$ is the Hamming weight of a vector $\alpha \in V_n$.

2.2 Symmetric group

For an n -tuple vector, $\alpha = (a_1, a_2, \dots, a_n) \in V_n$, we consider an operation on the vector which permutes the positions of a_i and a_j . Then the vector becomes

$$(a_1, \dots, a_j, \dots, a_i, \dots, a_n).$$

We denote the operation of permuting the positions of a_i and a_j by the operator $\pi = (ij)$ and then we write

$$\pi(a_1, a_2, \dots, a_n) = (a_1, \dots, a_j, \dots, a_i, \dots, a_n).$$

The permutations for an n -tuple vector in V_n may apply to more than two entries. Thus the operation $\pi = (ijk \dots)$ is defined by the i th entry goes to j th position, the j th entry goes to k th position, and so on. Thus the operator $\pi = (ij \dots k)$, acting on the vector α , for example, gives the vector

$$(a_1, \dots, a_{i-1}, a_k, a_{i+1}, \dots, a_{j-1}, a_i, a_{j+1}, \dots, a_n).$$

Let π_i and π_j be any two operators for a vector $\alpha \in V_n$. Then the combination of the operators is defined by $\pi = \pi_i \pi_j$ such that

$$\pi \alpha = (\pi_i \pi_j) \alpha = \pi_i (\pi_j \alpha).$$

The inverse of an operator exists. For $\pi = (ij \dots k)$, $\pi^{-1} = (k \dots ji)$ is its inverse because $\pi \pi^{-1} = \pi^{-1} \pi = e$, the unit permutation.

Definition 5 For an n -tuple vector (a_1, a_2, \dots, a_n) in the boolean space V_n , we consider operations π that permute the positions of the n -tuple. Then all possible operations on the n -tuple form a group which is called the *symmetric group defined on V_n and denoted by S_n (or permutation group)*.

If a subset of S_n forms a group under the same laws of combination used in S_n , then the group is called *subgroup* of S_n . Any group has at least two trivial subgroups: the group containing only one element $\{e\}$; and the group itself. For a symmetric group S_n , the following properties hold.

1. The order of S_n (the number of all elements) is $n!$ i.e. $|S_n| = n!$.
2. We take some elements in S_n as the generators of the group, if any element in S_n can be equivalently expressed by those generators. Then the minimum set of generators for S_n is of size $n - 1$. Let $\{(12), (13), \dots, (1n)\}$ be a set of generators of S_n . Then the element $(123 \dots n)$, for example, is equal to $(1n) \dots (13)(12)$.
3. The transitive relations of symmetric groups S_1, S_2, \dots, S_n are as follows;

$$S_1 \subset S_2 \subset \dots \subset S_{n-1} \subset S_n.$$

The following statements from group theory will be used later. Let G and G' be any two groups and elements g and g' be elements with $g \in G$ and $g' \in G'$.

1. (*Homomorphism*). If there is a mapping $G \rightarrow G'$ and the laws of combination for the two groups are preserved, i.e.

$$\left. \begin{array}{l} g_i \rightarrow g'_i \\ g_j \rightarrow g'_j \end{array} \right\} \Rightarrow (g_i g_j) \rightarrow (g'_i g'_j),$$

then the two groups, G and G' , are said to be homomorphic.

2. (*Isomorphism*). For two homomorphic groups, G and G' , if the mapping is invertible, then the two groups are said to be isomorphic.
3. (*Kernel*). For the homomorphic mapping of G and G' , the unit element in G maps to a subset H_e in G' . The subset H_e in G' corresponding to the unit element e in G is called the kernel of the homomorphic mapping.
4. (Lagrange's theorem). The order of a subgroup of a finite group is a divisor of the order of the group.

5. (Cayley's theorem). Any group with order n is isomorphic with a subgroup of S_n .

For a boolean space V_n , we say that the symmetric group S_n is defined on the space, if each element in S_n just permutes the vectors in V_n . Let V_m and V_n be subspaces of V_{m+n} . Let S_m be the symmetric group for the space V_m and S_n for the space V_n . Then for any elements $\pi \in S_m$ and $\pi' \in S_n$, it is obviously that $\pi\pi' = \pi'\pi$. We say that the two groups are commutative (both the two groups are subgroups of S_{m+n} and S_{m+n} is on V_{m+n}). Obviously, the set, $\{\pi\pi' \mid \pi \in S_m, \pi' \in S_n\}$ denoted by $S_m \times S_n$ (*direct product*), is a subgroup of S_{m+n} with order $m! \times n!$.

Let H be a subgroup of S_n . Then the subset πH , $\pi \in S_n$, $\pi \notin H$, is called the (left) *coset* associated with H in S_n . The subgroup H is called a *normal subgroup* (or invariant subgroup) of S_n if $\pi H \pi^{-1} = H$ for any $\pi \in S_n$. For any subgroup H of S_n , there exists $|S_n|/|H|$ elements g_i , ($g_i \notin H$, $g_i \in S_n$) such that

$$S_n = H \cup (g_1 H) \cup \dots \cup (g_{s-1} H), \quad (4)$$

where $s = |S_n|/|H|$. In the above formula, if H is a normal subgroup, the set, $\{H, g_1 H, \dots, g_{s-1} H\}$, forms a group (called *quotient group or factor group of S_n*) with order $n!/|H|$. For more detail about group theory, one can refer the books [7][5].

3 Relationships between symmetric group and boolean functions

Now we turn our discussion to the relationships between the symmetric group and boolean functions on finite boolean spaces V_n . We highlight features of a boolean function under the operations of a symmetric group.

Definition 6 Let π denote an element of the symmetric group S_n . We take all the elements of S_n as permuting operators on a vector α in V_n . We say that a permuting operator acts on a func-

tion on V_n as follows

$$\begin{aligned}\pi f(x) &= \pi \left(\bigoplus_{\alpha \in V_n} c_\alpha x^\alpha \right) \\ &= \bigoplus_{\pi\alpha \in V_n} c_{\pi\alpha} x^{\pi\alpha} \\ &= \bigoplus_{\beta \in V_n} c_\beta x^\beta\end{aligned}$$

where $\pi\alpha = \beta$ and $c_\alpha = c_\beta \in GF(2)$.

We denote by H_f a subgroup of S_n associated with the boolean function $f(x)$ over V_n . Then the subgroup H_f is described by the following lemma.

Lemma 1 *Let H_f denote the subset that contains all the elements $\pi \in S_n$ such that $\pi f(x) = f(x)$. Then H_f is a subgroup of S_n .*

Proof. For the subset H_f to be a group, we only need to show the set is closed under the laws of group combination of S_n . In fact if π_i and π_j are in the set H_f , then $\pi_i\pi_j$ and $\pi_j\pi_i$ are also in H_f , because

$$\pi_i\pi_j f(x) = \pi_i(\pi_j f(x)) = \pi_i f(x) = f(x).$$

The set H_f is closed. Therefore it is a subgroup of S_n . \square

Associated with the function $f(x)$ on V_n and the symmetric group S_n , we have another group, denoted by G_f , which is described by the following lemma.

Lemma 2 *If $ef(x) = f(x)$ (e the unit of S_n) is the unit of the set $\{\pi f(x) \mid \pi \in S_n\}$, then the set of functions forms a group, denoted by G_f , where the group operation “ \circ ”, stands for composition of functions, defined as follows*

$$[\pi_i f(x)] \circ [\pi_j f(x)] = (\pi_i \pi_j) f(x) = \pi_k f(x). \quad (5)$$

Proof. To be a group, the set G_f with the operation \circ must satisfy the following conditions: (i) the unit element must exist; (ii) each element must have an inverse in the set and the left inverse must be equal to the right inverse; (iii) the associative rule must hold for the operation; (vi) the set must be closed under the group operation. The unit

element of the set is defined by the function itself $f(x)$. Let $\pi_i f(x)$ be an element of the set. Then the element has its inverse $\pi_j f(x)$, such as $\pi_j = \pi_i^{-1}$, in the set, since

$$\begin{aligned}[\pi_i f(x)] \circ [\pi_j f(x)] &= [\pi_j^{-1} f(x)] \circ [\pi_i f(x)] \\ &= f(x).\end{aligned} \quad (6)$$

According to the definition of the group operation,

$$\begin{aligned}[\pi_i f(x) \circ \pi_j f(x)] \circ \pi_k f(x) &= \\ \pi_i f(x) \circ [\pi_j f(x) \circ \pi_k f(x)] &\end{aligned} \quad (7)$$

holds. Hence the associative law holds. The set, $G_f = \{\pi f(x) \mid \forall \pi \in S_n\}$, contains all the different boolean functions generated by permutations in S_n . Therefore, the set is closed. So we have proved that the set, $\{\pi f(x) \mid \pi \in S_n\}$, with composition \circ is a group. \square

The group operation “ \circ ” on G_f is not the group operation of S_n . The equality

$$(\pi_i \pi_j) f(x) = \pi_k f(x) \quad (8)$$

does not restrict $\pi_i \pi_j$ to equal π_k , because any element in $H_{\pi_k f}$ will leave the function $\pi_k f(x)$ unchanged. For convenience, we use the element $\pi_k = \pi_i \pi_j$ to identity the function $\pi_k f$. The group G_f is a set of polynomials on a finite boolean space, which is generated by a boolean function $f(x)$ on V_n and the symmetric group S_n . Each element, $\pi f(x)$, in G_f corresponds to a subgroup, $H_{\pi f}$, of S_n . Then for the function $f(x)$, we have the left coset πH_f and right coset $H_{\pi f} \pi$ that give the function $\pi f(x)$. Therefore among the elements in G_f , the following lemma holds.

Lemma 3 *Let $\pi_i f(x)$ and $\pi_j f(x)$ be any two elements in G_f associated with the function $f(x)$ over V_n . Then*

- (i) $|H_f| = |H_{\pi_i f}| = |H_{\pi_j f}| = \dots;$
- (ii) *There exists a subset of elements $\{e, \pi_1, \pi_2, \dots\}$, called representative set of S_n , denoted by C_f , such that*

$$S_n = H_f \cup \pi_1 H_f \cup \pi_2 H_f \dots; \quad (9)$$

- (iii) *Let π_i and π_j belong to C_f . If $\pi_i \neq \pi_j$, then $\pi_i f(x) \neq \pi_j f(x)$ and $C_f f(x) = G_f$.*

Proof. The group $H_{\pi f}$ is the group of the function $\pi f(x)$. So $H_{\pi f}$ contains all the elements in S_n such that $\pi_j(\pi f(x)) = \pi f(x)$. The left coset, πH_f , acting on the function $f(x)$, also produces the function $\pi f(x)$. So $|\pi H_f| \leq |H_{\pi f}|$. On the other hand, πH_f contains all elements in S_n such that $(\pi \pi_i)f(x) = \pi f(x)$ for each $\pi_i \in H_f$. Thus we have $|\pi H_f| \geq |H_{\pi f}|$. Therefore $|H_f| = |H_{\pi f}|$ which proves (i).

Since the intersection of distinct cosets is empty and all cosets contain $|S_n|$ elements, then (ii) holds.

The part (iii) is obvious. According to the definition of G_f , each function is uniquely generated by the function $f(x)$. The set of functions, $C_f f(x)$, contains all the different functions. Therefore $C_f f(x) = G_f$ \square

The subset C_f is not the only subset. We can choose one representative from each group $H_{\pi f}$ to form a subset C_f . But the group G_f is unique. Any C_f in S_n generates the group G_f and so may be used as the identity set for the function $f(x)$. Each element π in the identity set may be used as the identity element for the function $\pi f(x)$. Note that the class C_f may not contain the unit element.

It is clear that an operator acting on a function $f(x)$ is equivalent to a one-to-one linear transformation. The functions $f(x)$ and $\pi f(x)$ in G_f have many properties in common.

Lemma 4 *Let $f(x)$ be a boolean function on V_n . Then the all functions in G_f have the same (1) Hamming weight, (2) nonlinearity, (3) propagation criteria $PC(k)$ and (4) correlation immunity.*

Proof. Since each function in G_f relates to another by a one-to-one linear transformation, they have the same Hamming weight $wt(f)$ and nonlinearity N_f .

Let $f(x)$ on V_n have k -th order propagation criteria. According to definition 3, $f(x) \oplus f(x \oplus \alpha)$ is balanced for all $0 < wt(\alpha) \leq k$. The function $\pi f(x) = f(\pi x)$ and then

$$f(\pi x) \oplus f(\pi x \oplus \pi \alpha) = f(x') \oplus f(x' \oplus \beta)$$

Of course $wt(\pi \alpha) = wt(\beta)$. As α runs through all vectors such that $1 \leq wt(\alpha) \leq k$, β runs through

all vectors with $1 \leq wt(\beta) \leq k$.

According to definition 4, the if f has k -th order correlation immunity, then it satisfies

$$\sum_{x \in V_n} (-1)^{f(x) \oplus \alpha \cdot x} = 0, \quad \text{for all } 1 \leq wt(\alpha) \leq k.$$

Let $\pi f(x)$ be a function in G_f . Since the map from $f(x)$ to $\pi f(x)$ is a one-to-one linear transform and the vector α has been chosen for such that $1 \leq wt(\alpha) \leq k$, $\pi f(x)$ has the same correlation immunity as $f(x)$ has. \square

Lemma 5 *Let the $f(x)$ be a boolean function on V_n and r_i the number of x_i occurs in the function. (i) The numbers of repetitions of each variable of the x_{i_1}, \dots, x_{i_k} in $f(x)$ being equal (i.e. $r_{i_1} = \dots = r_{i_k}$), is a necessary condition for the group S_k associated with variables x_{i_1}, \dots, x_{i_k} to be a subgroup of H_f . (ii) The order of G_f is greater than or equal to the number of all different patterns of (r_1, \dots, r_n) .*

Proof. We prove the lemma by contradiction. By the lemma 1 the element in H_f operating on the function $f(x)$ does not change the function itself. Suppose $r_i \neq r_j$. After the operation, x_j in the function $\pi f(x)$ is transformed to x_i . Obviously, the number of repetitions of x_i in $\pi f(x)$ is r_j that induces $\pi f(x) \neq f(x)$. Therefore $\pi \notin H_f$.

Assume that $r_i \neq r_j$ for all $i \neq j$, $1 \leq i, j \leq n$. Any operation from S_n will change the representation of the function $f(x)$. So $G_f = S_n$. For all $r_i \neq r_j$ we have $\pi_i f(x) \neq \pi_j f(x)$. Therefore we have proved (ii). \square

Lemma 6 *Let $f(x)$ and $g(x)$ be any two boolean functions on V_n and H_f and H_g be their groups respectively. Then in the group $H_{f \oplus g}$ formed by the function $f(x) \oplus g(x)$, at least the intersection of H_f and H_g is a subgroup i.e. $H_f \cap H_g \subseteq H_{f \oplus g}$.*

Proof. Since the intersection set is a subset of S_n , all the laws of combination for S_n are preserved. The first we prove the intersection $H_f \cap H_g$ is a subset of $H_{f \oplus g}$. Let $\pi_i, \pi_j \in H_f$ and $\pi_i, \pi_j \in H_g$. Then π_i, π_j are in the intersection set $H_f \cap H_g$. Because

$$\begin{aligned} \pi_i \pi_j (f(x) \oplus g(x)) &= \pi_i (f(x) \oplus g(x)) \\ &= f(x) \oplus g(x), \end{aligned}$$

the elements π_i, π_j and $\pi_i\pi_j$ are in the group $H_{f\oplus g}$. Therefore $H_f \cap H_g \subset H_{f\oplus g}$. The unit element is in $H_f \cap H_g$. So to prove $H_f \cap H_g$ is a group, it is enough to show it is self closed under the laws of combination that are used in S_n . The above formula shows that the element $\pi_i\pi_j$ is in $H_{f\oplus g}$ and also in $H_f \cap H_g$. So $H_f \cap H_g$ is self closed. Therefore it is a group. Because the elements in $H_{f\oplus g}$ are all elements in S_n that leave the function $f(x) \oplus g(x)$ unchanged, $H_f \cap H_g$ is a subgroup of $H_{f\oplus g}$ for the function $f(x) \oplus g(x)$. \square

Note: The groups $H_{f\oplus g}$ and $H_f \cap H_g$ may equal, since the function $f(x) \oplus g(x)$ may increase the symmetric properties but also may reduce the properties. If $f(x) \oplus g(x) = 0$, $H_{f\oplus g} = S_n$ and $H_f \cap H_g$ is a subgroup. If $f(x)$ and $g(x)$ do not contain any common term, then $H_{f\oplus g} = H_f \cap H_g$.

The following are a few trivial facts for some boolean functions

1. Let k be an integer with $0 \leq k \leq n$. Then the function

$$h_k(x) = \bigoplus_{\forall \alpha \in V_n, \& wt(\alpha)=k} x^\alpha$$

has group S_n , i.e. $H_h = S_n$.

2. Let $\{i_1, i_2, \dots\}$ be a subset of $\{1, 2, \dots, n\}$. Based on lemma 6, for the function

$$h(x) = h_{i_1}(x) \oplus h_{i_2}(x) \oplus \dots, \quad (10)$$

the group H_h is S_n .

3. Let H_f be the group for the function $f(x)$ on V_n . Then H_f is also the group for the function $f(x) \oplus h(x)$, where $h(x)$ is the function (10) over V_n .
4. Let $\{i_1, i_2, \dots, i_d\}$ be a subset of $\{1, 2, \dots, n\}$ and

$$f(x) = x_{i_1}x_{i_2} \dots x_{i_d}$$

be an algebraic degree d boolean function on V_n . Then the group $H_f = S_d \times S_{n-d}$, where S_d is the symmetric group associated with the subset and S_{n-d} is the group associated with the subset $\{1, 2, \dots, n\} \setminus \{i_1, i_2, \dots, i_d\}$.

4 Discussion

For a fixed boolean space V_n , there are 2^{2^n} boolean functions and the size of the permutation group is $n!$. Although this is very large, we can use the permutation groups to discuss boolean functions. The boolean functions in the group G_f share the same cryptographic properties such as Hamming weight, nonlinearity, propagation criteria and correlation immunity. For a group G_f , there exist subsets, $\aleph = \{f | f \in G_f\}$, of functions such that \aleph is a additive group (f, \oplus) if we add the zero to the subset and regard the zero as the unit element. There are trivial additive groups, for example, $\{0, \pi_i f(x)\}$ (since $\pi_i f \oplus \pi_i f = 0$). If such a subset contains m functions (of course $m \leq |G_f|$), the additive group is a S-box design $n \times m$ (note the group order is $m+1$). Good S-box designs need to satisfy some cryptographic properties such as (1) any nonzero linear combination $c_1 f_1 \oplus \dots \oplus c_m f_m$ is balanced, (2) any nonzero linear combination has high nonlinearity, (3) any nonzero linear combination satisfies the same and good propagation criteria, (4) the mapping of the S-box is regular i.e. each vector in V_m corresponds to 2^{n-m} vectors in V_n as x runs through all vectors in V_n once, and (5) the S-box has good differential distribution [1, 2, 4, 12]. If all components of an S-box are in an additive group \aleph and G_f at the same time, then the discussion of the S-box concerns the one function $f(x)$ on V_n only.

References

- [1] E. Biham and A. Shamir. Differential cryptanalysis of DES-like cryptosystems. *Journal of Cryptology*, 4.1:3–72, 1991.
- [2] E. F. Brickell, J. H. Moore, and M. R. Purtil. Structures in S-boxes of the DES. *Advances in Cryptology – CRYPTO’86, Lecture Notes in Computer Science, Springer-Verlag, Berlin Heidelberg New York Tokyo*, pages 3–8, 1987.
- [3] P. Camion, C. Carlet, P. Charpin, and N. Sendrier. On correlation-immune functions. *Advances in Cryptology – CRYPTO’91, Lecture Notes in Computer*

*Science, Springer-Verlag, Berlin Heidelberg
New York Toyko, 576:86–100, 1991.*

- [4] J. H. Cheon, S. Chee, and C. Park. S-boxes with controllable nonlinearity. *Advances in Cryptology – EUROCRYPT’99, Lecture Note in Computer Science, Springer-Verlag, Berlin Heidelberg New York, 1592:286–294, 1999.*
- [5] M. Hamermesh. *Group Theory and Its Application to Physical Problems.* Reading, Mass., Addison-Wesley, 1962.
- [6] L. O’Connor and A. Klapper. Algebraic nonlinearity and its applications to cryptography. *Journal of Cryptology, 7:213–227, 1994.*
- [7] B. E. Sagan. *The Symmetric Group; Representations, Combinatorial Algorithms, and Symmetric Functions.* Pacific Grove, Calif., Wadosworth & Books, 1991.
- [8] J. Seberry, X. Zhang, and Y. Zheng. Nonlinearity and propagation characteristics of balanced boolean functions. *Information and Computation, Academic Press, 119, No.1:1–13, 1995.*
- [9] T. Siegenthaler. Correlation-immunity of nonlinear combining functions for cryptographic applications. *IEEE Transaction on Information Theory, 30.5:776–779, 1984.*
- [10] G. Xiao and J. L. Massey. A spectral characterization of correlation-immune combining functions. *IEEE Transactions on Information Theory, 34:3, May 1988.*
- [11] X. Zhang and Y. Zheng. Auto-correlations and new bounds on the nonlinearity of boolean functions. *Advances in Cryptology – EUROCRYPT’96, Lecture Notes in Computer Science, Springer-Verlag, Berlin Heidelberg New York, 1070:294–306, 1996.*
- [12] X. Zhang, Y. Zheng, and H. Imai. Relating differential distribution tables to other properties of substitution boxes. *Designs, Codes and Cryptography, 19:45–63, 2000.*