On the Symmetric Property of Homogeneous Boolean Functions

Chengxin Qu, Jennifer Seberry, and Josef Pieprzyk

Centre for Computer Security Research
School of Information Technology and Computer Science
University of Wollongong
Wollongong, NSW 2522, AUSTRALIA
{cxq01,jennie,josef}@cs.uow.edu.au

Abstract. We use combinatorial methods and permutation groups to classify homogeneous boolean functions. The property of symmetry of a boolean function limits the size of the function's class. We exhaustively searched for all boolean functions on V_6. We found two interesting classes of degree 3 homogeneous boolean functions: the first class is degree 3 homogeneous bent boolean functions; and the second is degree 3 homogeneous balanced boolean functions. Both the bent and balanced functions discovered have nice algebraic and combinatorial structures. We note that some structures can be extended to a large boolean space. The application of homogeneous boolean functions for fast implementation on parallel architectures is mooted.

Keywords: S-box Theory, Cryptographically Strong Boolean Functions, Symmetric Functions, Homogeneous Functions.

1 Introduction

The S-box theory emerged quite recently as a part of Cryptology. Shannon [1] established its foundations by formulating the principles for secure product cipher design. To get secure encryption algorithms, it is enough to design two elementary blocks: a permutation block (or P-box) and a substitution block (or S-box). P-boxes provide *diffusion* while S-boxes furnish *confusion*. Encryption algorithms, according to Shannon's concepts, are nothing but a sequence of iterations. Each iteration uses a layer of S-boxes controlled by a secret key. Between two consecutive iterations, a single P-box of known structure is used (the P-box is not keyed).

Shannon's product cipher is easy to implement. If we select building blocks at random (so both P-boxes and S-boxes are random), we can still get with a high probability a strong cipher provided we use "a large enough" number of iterations [2]. The real challenge in the S-box theory is how to design S-boxes so we can reduce the number of iterations without loss of security. Boolean functions are universal tools for S-box design and have received considerable attention over the last decade [4,5]. The cryptographic usefulness of a given boolean function

J. Pieprzyk, R. Safavi-Naini, and J. Seberry (Eds.): ACISP'99, LNCS 1587, pp. 26–35, 1999.

is measured by its cryptographic properties. The collection of these properties includes balance, strict avalanche criterion or SAC, high nonlinearity [10] [9] and higher-degree propagation criteria [3]. If an S-box (or corresponding collection of boolean functions) is implemented as a lookup table, then the length or the form of boolean functions is not important. This is no longer true when the evaluation of the function is done on the fly – this is the case in all MD-type hashing algorithms (MD4, MD5, SHA-1, HAVAL)[15]. It was argued in [13], that symmetric boolean functions can be very efficiently evaluated. Since symmetric boolean functions are composed by a series of homogeneous parts in a boolean space, we study the symmetric properties of boolean functions starting from homogeneous boolean functions.

This work studies homogeneous boolean functions which create subclass of symmetric functions whose terms (in the algebraic normal form) are of the same degree. In particular, we examine symmetric properties of 3-homogeneous bent functions and highly nonlinear balanced ones in V_6.

2 Boolean Functions and Permutation Groups

We first introduce necessary notations. The n-dimension boolean space V_n contains the following 2^n vectors (binary sequences with length n)

$$\alpha_0 = (0, \cdots, 0, 0),\ \alpha_1 = (0, \cdots, 0, 1),\ \cdots,\ \alpha_{2^n-1} = (1, \cdots, 1, 1). \tag{1}$$

Let $\alpha = (a_1, \cdots, a_n),\ a_i \in GF(2)$, be a vector in V_n. Then a single term of a boolean function on a boolean space V_n is written as $x^\alpha = x_1^{a_1} \cdots x_n^{a_n}$. In general, a boolean function can be represented by its algebraic normal form as

$$f(x) = \bigoplus_{\alpha \in V_n} c_\alpha x^\alpha \qquad c_\alpha = 0 \ \text{ or } \ 1. \tag{2}$$

The values of a function form a binary sequence of the length 2^n. For a binary sequence ξ, $wt(\xi)$ denotes its Hamming weight which equals the number of 1s in the sequence. A function, $f(x)$, is called a d-homogeneous if all $\alpha \in V_n$ in the function (2) have the same Hamming weight and equal to d ($wt(\alpha) = d$).

Let S_n denote a permutation group with n entries and e the unit element of S_n. The the order of the group is $n!$. The minimum number of generators of S_n is $n-1$. For example, the generators can be $(1\ n),\ (1\ n-1),\ \cdots,\ (1\ 2)$. The highest order of the elements of S_n is n. We use the traditional definition of writing $\pi = (i\ j\ \cdots\ k)$ for the permutation

$$\begin{pmatrix} i & j & \cdots & k \\ j & \cdots & \cdots & i \end{pmatrix} \tag{3}$$

Definition 1. *Let π be an element of the permutation group S_n. Assume that permutations from S_n are used to permute n variables of a boolean function. So for a permutation $\pi = (ij) \in S_n$, we can write that*

$$\pi\alpha = (ij)(a_1, \cdots, a_i \cdots, a_j, \cdots, a_n) = (a_1, \cdots, a_j \cdots, a_i, \cdots, a_n). \tag{4}$$

We say that a permutation $\pi \in S_n$ acts on a boolean function $f(x)$ if it permutes the function's variables, i.e.

$$\pi f(x) = \pi \bigoplus_{\alpha \in V_n} c_\alpha x^\alpha = \bigoplus_{\pi\alpha \in V_n} c_{\pi\alpha} x^{\pi\alpha} = \bigoplus_{\beta \in V_n} c_\beta x^\beta \tag{5}$$

where $\pi\alpha = \beta$.

The permutation is a 1-1 transformation for a function $f(x)$. Under the all permutations in S_n, a function $f(x)$ generates a function set $\{\pi f \mid \pi \in S_n\}$. For each boolean function $f(x)$, there exists a minimum subset, denoted by $\mathcal{PG}(f)$, of S_n such that $\{\pi f \mid \pi \in \mathcal{PG}(f)\} = \{\pi f \mid \pi \in S_n\}$.

Lemma 1. *Let π be an element of the permutation group S_n, and $\pi f(x) = g(x)$. Then*

1. *all the functions, $\pi f(x)$ ($\pi \in S_n$), have the same cryptographic properties such as Hamming weight, nonlinearity and SAC [1];*
2. *the set $\{\pi f(x) \mid \pi \in S_n\}$ forms a group if $ef(x) = f(x)$ (e the unit of S_n) is the unite of the set and the group operation "$\circ$" is defined as follows*

$$[\pi_i f(x)] \circ [\pi_j f(x)] = (\pi_i \pi_j) f(x) = \pi_k f(x), \tag{6}$$

where $\circ$ stands for composition of functions or permutations and all $\pi_i,\ \pi_j, \pi_k \in \mathcal{PG}(f)$. The group is denoted by $PG(f)$.

The group operation "$\circ$" on $PG(f)$ is not the operation in S_n. The equality

$$(\pi_i \pi_j) f(x) = \pi_k f(x) \tag{7}$$

does not ensure that $\pi_i\pi_j$ is equal to π_k except $\pi_i\pi_j \in \mathcal{PG}(f)$. For example, suppose $\pi_i\pi_j = \pi_k\pi'_k$ and $\pi'_k f(x) = f(x)$. Then we get the above equality and $\pi_i\pi_j \neq \pi_k$ except $\pi'_k = e$.

Proof. Consider the following two parts of the proof.

1. Since the permutation is a linear 1-1 variable transformation, it preserves all the properties of the function $f(x)$.
2. To be a group, the set with the operation $\circ$ must satisfy the following conditions: (*i*) the unit element must exist; (*ii*) each element must have the inverse in the set and the left inverse is equal to the right inverse; (*iii*) the associative rule must hold for the operation; (*vi*) the set must be closed under the operation.
   The unit element of the set is 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

$$[\pi f(x)] \circ [\pi^{-1} f(x)] = [\pi^{-1} f(x)] \circ [\pi f(x)] = f(x). \tag{8}$$

[1] For the cryptographic desirable properties of boolean functions, see paper [4] [10] [12] [11]

According to the definition of group operation,

$$[\pi_i f(x) \circ \pi_j f(x)] \circ \pi_k f(x) = \pi_i f(x) \circ [\pi_j f(x) \circ \pi_k f(x)] \tag{9}$$

is true. Hence the associative rule holds. The set, $\{\pi f(x) \mid \forall \pi \in S_n\}$, contains all 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.

The group $PG(f)$ is a homomorphism to symmetric group S_n. Consider a relation between the groups $PG(f)$ and S_n. There exists subgroups of S_n, say $H(f)$, such that $\pi_i f(x) = f(x)$ for some $\pi_i \in S_n$. For any given boolean function $f(x)$ on V_n, there is at least one subgroup $H(f)$ of S_n which is the subgroup containing the unit element $\{e\}$. By convention, for a given boolean function $f(x)$ we denote $H(f)$ is the biggest subgroup of S_n. Since $PG(f) = \mathcal{P}G(f)f(x)$, then

$$S_n = H(f) + \pi_1 H(f) + \pi_2 H(f) + \cdots \qquad \pi_i \in \mathcal{P}G(f) \tag{10}$$

where "+" denotes the union of sets. Equation (10) is true, since all the intersection sets, $\pi_i H(f) \cap \pi_j H(f)$, where $\pi_i, \pi_j \in \mathcal{P}G(f)$, are empty. Therefore the order of the group $H(f)$ is $|H(f)| = n!/|PG(f)|$.

For a boolean space V_n, there are 2^{2^n} different boolean functions and the size of the permutation group is $n!$. Since $2^{2^n} \gg n!$, it is impossible to discuss all $PG(f)$. However, we can use the permutation group to discuss homogeneous boolean functions in which some of them have nice combinatorial structures. The study of the group $H(f)$ is more important than the group $PG(f)$. For example, the function $f(x) = x_i$ has the group $H(f)$ with order $(n-1)!$ and $f(x) = x_i x_j$ has the group $H(f)$ with order $2(n-2)!$.

Throughout the paper, the boolean function containing all terms of degree d over V_n is denoted by $P_n^{(d)}(x)$. Clearly the group $H(P_n^{(d)}) = S_n$. For the sake of simplicity, we use the natural numbers to encode the terms. For example, 123 stands for $x_1x_2x_3$. Thus a function

$$\begin{aligned} f(x) = {} & x_1x_2x_3 \oplus x_1x_2x_4 \oplus x_1x_2x_5 \oplus x_1x_2x_6 \oplus x_1x_3x_4 \oplus x_1x_3x_5 \oplus \\ & x_1x_4x_6 \oplus x_1x_5x_6 \oplus x_2x_3x_4 \oplus x_2x_3x_6 \oplus x_2x_4x_5 \oplus x_2x_5x_6 \oplus \\ & x_3x_4x_5 \oplus x_3x_4x_6 \oplus x_3x_5x_6 \oplus x_4x_5x_6 \end{aligned}$$

can be equivalently represented as

$$f(x) = P_6^{(3)}(x) \oplus x_1x_3x_6 \oplus x_1x_4x_5 \oplus x_2x_3x_5 \oplus x_2x_4x_6 \tag{11}$$

or

$$\begin{aligned} f(x) &= 123 \oplus 124 \oplus 125 \oplus 126 \oplus 134 \oplus 135 \oplus 146 \oplus 156 \oplus \\ &\quad 234 \oplus 236 \oplus 245 \oplus 256 \oplus 345 \oplus 346 \oplus 356 \oplus 456. \\ &= P_6^{(3)}(x) \oplus 136 \oplus 145 \oplus 235 \oplus 246. \end{aligned}$$

Combinatorial parameters are useful to discuss homogeneous boolean functions allowing easy determination of in-equivalence. We take each single term as a block so that $x_1x_2x_3$ is the block 123.

We will use the concept of BIBD [17]. BIBD stands for balanced incomplete block design which is a block design within ν varieties and has parameters κ the number of varieties in block, β the number of blocks in the design and $r_1, \cdots, r_\nu$ the numbers of repetitions of varieties respectively. Sometimes we use the parameters $\lambda_1, \lambda_2, \cdots$ to stand for the numbers of repetitions of pairs in the block design. Let ν stand for the space dimension, κ for the order of the function, β for the number of terms in the function and let $r_1, \cdots, r_\nu$ be the numbers of repetitions for variables $x_1, \ldots, x_\nu$ in the function, respectively. Then the structure of a d-homogeneous boolean function can be considered as a BIBD with parameters $\{\nu, \kappa, \beta, r_1, \cdots, r_\nu\}$.

Lemma 2. *Let f be a homogeneous boolean function on V_n. If the element $(ij) \in S_n$ belongs to the group $H(f)$, the repetitions of x_i and x_j must be equal i.e. $r_i = r_j$.*

Proof. By contradiction. Suppose $r_i \neq r_j$, then $(ij)f(x) \neq f(x)$. Then we have $(ij) \notin H(f)$ which is a contradiction.

3 3-Homogeneous Boolean Functions

We conducted an exhaustive computer search of all 3-homogeneous function on V_6 and found the complete set of bent[2] and balanced 3-homogeneous boolean functions which exist on V_6. These are used as the basis on which we discuss 3-homogeneous boolean functions.

Definition 2. *Let $f(x)$ be a d-homogeneous boolean function on V_n. Then the homogeneous complement of $f(x)$ is defined by*

$$f_c(x) = P_n^{(d)} \oplus f(x) \tag{12}$$

It is clear that a given homogeneous function $f(x)$ can be equivalently represented by the terms it contains (i.e. the function $f(x)$) or the terms it does not contain (i.e. the function $f_c(x)$). The function $f_c(x)$ preserves all symmetric properties of the function $f(x)$. We use the shorter, $f(x)$ or $f_c(x)$, representation.

3.1 3-Homogeneous Bent Functions

We know that the function

$$\begin{aligned} f(x) &= 124 \oplus 125 \oplus 126 \oplus 134 \oplus 135 \oplus 136 \oplus 146 \oplus 156 \oplus \\ &\quad 234 \oplus 235 \oplus 236 \oplus 245 \oplus 256 \oplus 345 \oplus 346 \oplus 456 \\ &= P_6^{(3)}(x) \oplus 123 \oplus 145 \oplus 246 \oplus 356 = P_6^{(3)}(x) \oplus f_c(x) \end{aligned}$$

[2] For the definition of bent function see the papers, for example, [6], [7], [8].

is bent on V_6, where $f_c(x)$ is the homogeneous complement of $f(x)$,

$$f_c(x) = 123 \oplus 145 \oplus 246 \oplus 356 = P_6^{(3)}(x) \oplus f(x) \tag{13}$$

The function $f_c(x)$ can be seen as a combinatorial design with parameters as follows,

$$\{\nu, \kappa, \beta, r_1, r_2, r_3, r_4, r_5, r_6\} = \{6, 3, 4, 2, 2, 2, 2, 2, 2\}. \tag{14}$$

This is a BIBD(v, b, k, r, λ) = BIBD$(4, 6, 3, 2, 1)$ in which the parameters $v = \beta$, $b = \nu$, $k = \kappa$. The group $H(f)$ is generated by the elements (12)(56), (13)(46) and (24)(35). The elements $(12), (13), (14)$ are 3 generators of S_4. If we take the mapping

$$(12) \leftrightarrow (12)(56),\ (13) \leftrightarrow (13)(46),\ (14) \leftrightarrow (24)(35), \tag{15}$$

we find that $H(f)$ is isomorphic with S_4, i.e. $H(f) \simeq S_4$. Hence the order of $PG(f) = 6!/4! = 30$, which means that there are only 30 bent functions of this kind on V_6. Let $Z_2 = \{e,\ (16)(34)\}$, $Z_2' = \{e,\ (16)(25)\}$ and

$$S_3' = \{e,\ (12)(56),\ (13)(46),\ (23)(45),\ (123)(465),\ (132)(456)\}.$$

Then the group can be expressed as

$$H(f) = Z_2 \times Z_2' \times S_3'. \tag{16}$$

There are many ways to represent the groups $H(f)$ and $PG(f)$. The explicit forms of the two groups are as follows.

$$H(f) = \left\{ \begin{array}{llll} e, & (12)(56), & (13)(46), & (14)(36), \\ (15)(26), & (23)(45), & (24)(35), & (16)(34), \\ (16)(25), & (34)(25), & (25)(1364), & (25)(1463), \\ (34)(1562), & (34)(1265), & (16)(2453), & (16)(2354), \\ (123)(465), & (132)(456), & (124)(365), & (142)(356), \\ (263)(145), & (154)(236), & (135)(264), & (153)(246) \end{array} \right\} \tag{17}$$

$$PG(f) = \left\{ \begin{array}{llll} f, & (45)f, & (56)f, & (465)f, \\ (456)f, & (46)f, & (34)f, & (345)f, \\ (34)(56)f, & (3465)f, & (3456)f, & (346)f, \\ (354)f, & (35)f, & (3564)f, & (35)(46)f, \\ (356)f, & (3546)f, & (3654)f, & (365)f, \\ (364)f, & (3645)f, & (36)f, & (36)(45)f, \\ (26)(35)f, & (26)(354)f, & (26)(345)f, & (26)(34)f, \\ (25)(45)f, & (26)f. & & \end{array} \right\} \tag{18}$$

For any bent function on V_n, its nonlinearity is

$$N_f = 2^{n-1} - 2^{\frac{n}{2}-1}. \tag{19}$$

So on V_6, $N_f = 28$.

3.2 3-Homogeneous Balanced Functions

We found two classes of balanced functions on V_6. One class contains functions with 14 terms. The other class includes functions with 15 terms. All the boolean functions in the two classes have the nonlinearity $N_f = 24$. Comparing with other balanced boolean functions, it is not lower (for bent $N_f = 28$). There exist more classes of homogeneous balanced boolean functions on the boolean space with $n > 6$. The maximum nonlinearities are 52 on V_7 (maximum for all boolean functions is 56) and 112 on V_8 (for bent function, it is 128).

(A) A 14-term 3-homogeneous boolean function

$$f(x) = P_6^{(3)} \oplus 126 \oplus 136 \oplus 145 \oplus 234 \oplus 235 \oplus 456 \tag{20}$$

is balanced and its complement $f_c(x)$ can be characterised by its combinatorial parameters,

$$\{\nu, \kappa, \beta, r_1, r_2, r_3, r_4, r_5, r_6\} = \{6, 3, 6, 3, 3, 3, 3, 3, 3\} \tag{21}$$

which is also a BIBD$(v, b, k, \lambda_1, \lambda_2)$ = BIBD$(6, 6, 3, 2, 1)$. Under the permutation operations $\{(16),\ (23),\ (45)\}$, the function f does not change. Also, the set of permutations

$$\{(124635),\ (125634),\ (134625),\ (135624)\} \tag{22}$$

leaves the function unchanged. The set

$$\left\{ \begin{array}{llll} e, & (16), & (23), & (45), \\ (16)(23), & (16)(45), & (23)(45), & (16)(23)(45), \\ (124635), & (125634), & (134625), & (135624), \\ (124)(356), & (125)(346), & (134)(256), & (135)(246), \\ (142)(365), & (152)(364), & (153)(264), & (143)(265), \\ (153642), & (143652), & (152643), & (142653) \end{array} \right\} \tag{23}$$

forms a group $H(f)$. We point out that the group $H(f)$ is not isomorphic to the symmetric group S_4, since S_4 does not contain any element of order 6. The group $H(f)$ is isomorphic to the group

$$A \cap C_1 \cap C_2 \cap C_3 \cap C_4 \tag{24}$$

where $A = Z_2 \times Z_2 \times Z_2$ is an Abelian group, and C_1, C_2, C_3, C_4 are four cyclic groups of order 6 which are generated by elements

$$(124635), (125634), (134625), (135624),$$

respectively.
The balanced function $f(x)$ can also be expressed as

$$f(x) = P_6^{(3)}(x) \oplus \bigoplus_{h=0}^{5} \pi^h(x_1 x_2 x_6) \tag{25}$$

where π is an element of order 6 in $H(f)$. Since the order of the group is 24, we have

$$|PG(f)| = \frac{|S_6|}{24} = \frac{6!}{24} = 30, \tag{26}$$

which says that there are 30 3-homogeneous balanced functions with exactly 14 terms only.

(B) A representative of the balanced 3-homogeneous boolean functions with 15 terms

$$\begin{aligned} f(x) &= P_6^{(3)}(x) \oplus x_1x_4x_6 \oplus x_1x_5x_6 \oplus x_2x_3x_5 \oplus x_2x_4x_5 \oplus x_3x_4x_5 \\ &= P_6^{(3)}(x) \oplus 146 \oplus 156 \oplus 235 \oplus 245 \oplus 345. \end{aligned}$$

is invariant under the permutation operations $\{e, (16), (23), (16)(23)\}$. Therefore, $H(f) = \{e, (16), (23), (16)(23)\}$ and $PG(f)$ has order 180. Among all 15-term 3-homogeneous boolean functions, there are 4 functions with the same symmetry. We can see the functions

$$\begin{aligned} f_{c1}(x) &= 146 + 156 + 235 + 245 + 345 \\ f_{c2}(x) &= 146 + 156 + 234 + 245 + 345 \\ f_{c3}(x) &= 145 + 146 + 234 + 235 + 456 \\ f_{c4}(x) &= 145 + 156 + 234 + 235 + 456 \end{aligned} \tag{27}$$

share the same symmetry under the subgroup

$$H(f) = \{e, (16), (23), (16)(23)\}.$$

The four functions also have the relations

$$f_1(x) = (45)f_2 = (12)(36)f_3(x) = (12)(36)(45)f_4(x). \tag{28}$$

The combinatorial parameters of the complementary function of the function are

$$\{\nu, \kappa, \beta, r_1, r_2, r_3, r_4, r_5, r_6\} = \{6, 3, 5, 2, 2, 2, 3, 4, 2\}. \tag{29}$$

4 Discussion

Let V_m and V_n be two boolean spaces. If $m < n$, then V_m is a subspace of V_n, $(V_m \subset V_n)$. If a function is balanced on V_m, the function is balanced on V_n. For $n \leq 5$, there is no 3-homogeneous boolean function which is either balanced or bent. The above discussion can be directly extended to the boolean spaces V_{6n} [14]. 3-homogeneous balanced boolean functions may exist in any boolean space V_n $(n > 5)$. For example,

$$\begin{aligned} &x_1x_2x_3 \oplus x_1x_2x_4 \oplus x_1x_2x_5 \oplus x_1x_2x_6 \oplus x_1x_2x_7 \oplus x_1x_3x_4 \oplus x_1x_3x_5 \oplus \\ &x_1x_3x_6 \oplus x_1x_3x_7 \oplus x_1x_4x_5 \oplus x_1x_4x_6 \oplus x_1x_4x_7 \oplus x_1x_5x_6 \oplus x_2x_3x_4 \oplus \\ &x_2x_3x_5 \oplus x_2x_3x_6 \oplus x_2x_3x_7 \oplus x_2x_4x_5 \oplus x_2x_4x_6 \oplus x_2x_5x_7 \oplus x_2x_6x_7 \oplus \\ &x_3x_4x_7 \oplus x_3x_5x_7 \oplus x_3x_6x_7 \oplus x_4x_5x_6 \oplus x_4x_5x_7 \oplus x_4x_6x_7 \oplus x_5x_6x_7 \end{aligned}$$

is a balanced on V_7 and

$$x_1x_2x_3 \oplus x_1x_2x_4 \oplus x_1x_2x_5 \oplus x_1x_2x_6 \oplus x_1x_2x_7 \oplus x_1x_2x_8 \oplus x_1x_3x_4 \oplus x_1x_3x_5 \oplus x_1x_3x_6 \oplus x_1x_3x_7 \oplus x_1x_3x_8 \oplus x_1x_4x_5 \oplus x_1x_4x_6 \oplus x_1x_4x_7 \oplus x_1x_4x_8 \oplus x_1x_5x_7 \oplus x_1x_5x_8 \oplus x_1x_6x_7 \oplus x_1x_6x_8 \oplus x_2x_3x_5 \oplus x_2x_3x_6 \oplus x_2x_3x_7 \oplus x_2x_3x_8 \oplus x_2x_4x_5 \oplus x_2x_4x_7 \oplus x_2x_6x_8 \oplus x_2x_7x_8 \oplus x_3x_4x_5 \oplus x_3x_4x_7 \oplus x_3x_5x_6 \oplus x_3x_5x_7 \oplus x_3x_5x_8 \oplus x_3x_7x_8 \oplus x_4x_5x_8 \oplus x_4x_6x_8 \oplus x_4x_7x_8 \oplus x_5x_6x_7 \oplus x_5x_6x_8 \oplus x_5x_7x_8 \oplus x_6x_7x_8$$

on V_8. So far, we have not found any 3-homogeneous bent functions in V_8 or V_{10}. Since the functions we discuss are homogeneous, every single term in a function has the same properties on the boolean space. Therefore, the repetitions of variables and pairs of variables directly affect the properties of the boolean function. Further study will be undertaken to try to construct boolean functions that satisfy the cryptographic desirable properties through the study of repetitions of variables and pairs.

Acknowledgement

The authors wish to thank Dr Xian-mo Zhang, Dr Chris Charnes, Mr Tianbing Xia and anonymous referees for their help and critical comments during this project.

References

1. C. E. Shannon, *Communication theory of secrecy system*, Bell System Technical Journal, 28: 656-715, 1976
2. L. O'Connor, *On the distribution of characteristics in bijective mappings*, Journal of Cryptology, 8: 67-86, 1995.
3. B. Preneel, W. V. Leekwijck, L. V. Linden, R. Govaerts and J. Vandewalle, *Propagation characteristics of boolean functions*, In Advances in Cryptology – EUROCRYPT'90, Lecture Notes in Computer Science, 473, Springer-Verlag, 161-173, 1991.
4. A. F. Webster and S. E. Tavares, *On the design of S-box*, In Advances in Cryptology – CRYPTO'85, Lecture Notes in Computer Science, 219, Springer-Verlag, 523-534, 1986.
5. X. M. Zhang, Y. Zheng, H. Imai, *Differential distribution and other properties of substitution boxes*, Proceedings of JW-ISC'97, Session 1 / Block cipher, 19-29, 1997.
6. O. S. Rothaus, *On "bent" functions*, Journal of Combinatorial Theory (A), Academic Press, Inc., 20:300-305, 1976.
7. J. F. Dillon, *Elementary Hadamard difference set*, PhD Dissertation, University of Maryland, 1976.
8. Kaisa Nyberg, *Construction of bent functions and difference sets*, In Advances in Cryptology – EUROCRYPT'90, Lecture Notes in Computer Science, 473, Springer-Verlag, 151-160, 1991.

9. Josef Pieprzyk, Zhong Li, Jennifer Seberry and Xian Mo Zhang, *Fast-H: A family of fast and strong hashing algorithms*, (preprint) 1997.
10. Carlisle Adams and Stafford Tavares, *The structured design of cryptographically good S-boxes*, Journal of Cryptology, 3:27-41, 1990.
11. Willi Meier and Othmar Staffelbach, *Nonlinearity criteria for cryptographic functions*, Lecture Notes in Computer Science, EUROCRYPT'89, 549-562, 1989.
12. J. Seberry and X.M. Zhang and Y. Zheng, *Highly nonlinear 0-1 balanced functions satisfying strict avalanche criterion*, Advances in Cryptology - AUSCRYPT'92, Lecture Notes in Computer Science, 718, Springer-Verlag, 145-155, 1993.
13. Josef Pieprzyk and Chengxin Qu, *Rotation-symmetric functions and fast hashing*, Information Security and Privacy, ACISP'98, Lecture Notes in Computer Science, 1438, Springer-Verlag, 169-180, 1998.
14. Chengxin Qu, Jennifer Seberry and Josef Pieprzyk, *Homogeneous bent functions*, (preprint), 1998.
15. Alfred J. Menezes, Paul C. Van Oorschot and Scott A. Vanstone, "Handbook of Applied Cryptography", CRC Press, Boca Raton, 1996.
16. Bruce E. Sagan, "The Symmetric Group; Representations, Combinatorial Algorithms, and Symmetric Functions", Wadsworth & Books, Pacific Grove, Calif., 1991.
17. Anne Penfold Street and Deborah J. Street, "Combinatorics of Experimental Design", Oxford Science Publications, Oxford, 1987.