Pitfalls in Designing Substitution Boxes (Extended Abstract)

Jennifer Seberry, Xian-Mo Zhang and Yuliang Zheng

Department of Computer Science
University of Wollongong, Wollongong, NSW 2522, Australia
{jennie, xianmo, yuliang}@cs.uow.edu.au

Abstract. Two significant recent advances in cryptanalysis, namely the differential attack put forward by Biham and Shamir [3] and the linear attack by Matsui [7, 8], have had devastating impact on data encryption algorithms. An eminent problem that researchers are facing is to design S-boxes or substitution boxes so that an encryption algorithm that employs the S-boxes is immune to the attacks. In this paper we present evidence indicating that there are many pitfalls on the road to achieve the goal. In particular, we show that certain types of S-boxes which are seemly very appealing do not exist. We also show that, contrary to previous perception, techniques such as chopping or repeating permutations do *not* yield cryptographically strong S-boxes. In addition, we reveal an important combinatorial structure associated with certain quadratic permutations, namely, the difference distribution table of each differentially 2-uniform quadratic permutation embodies a Hadamard matrix. As an application of this result, we show that chopping a differentially 2-uniform quadratic permutation results in an S-box that is very prone to the differential cryptanalytic attack.

1 Basic Definitions

Denote by V_n the vector space of n tuples of elements from $GF(2)$. Let $\alpha = (a_1, \ldots, a_n)$ and $\beta = (b_1, \ldots, b_n)$ be two vectors in V_n. The scalar product of α and β, denoted by $\langle\alpha, \beta\rangle$, is defined by $\langle\alpha, \beta\rangle = a_1b_1 \oplus \cdots \oplus a_nb_n$, where multiplication and addition are over $GF(2)$. In this paper we consider Boolean functions from V_n to $GF(2)$ (or simply functions on V_n).

Let f be a function on V_n. The $(1,-1)$-sequence defined by $((-1)^{f(\alpha_0)}$, $(-1)^{f(\alpha_1)}$, ..., $(-1)^{f(\alpha_{2^n-1})})$ is called the *sequence* of f, and the $(0,1)$-sequence defined by $(f(\alpha_0)$, $f(\alpha_1)$, ..., $f(\alpha_{2^n-1}))$ is called the *truth table* of f, where $\alpha_0 = (0, \ldots, 0, 0)$, $\alpha_1 = (0, \ldots, 0, 1)$, ..., $\alpha_{2^n-1} = (1, \ldots, 1, 1)$. f is said to be *balanced* if its truth table has 2^{n-1} zeros (ones).

An *affine* function f on V_n is a function that takes the form of $f = a_1x_1 \oplus \cdots \oplus a_nx_n \oplus c$, where $a_j, c \in GF(2)$, $j = 1, 2, \ldots, n$. Furthermore f is called a *linear* function if $c = 0$. The sequence of an affine (or linear) function is called an *affine (or linear) sequence*.

The *Hamming weight* of a vector $\alpha \in V_n$, denoted by $W(\alpha)$, is the number of ones in the vector.

Y.G. Desmedt (Ed.): Advances in Cryptology - CRYPTO '94, LNCS 839, pp. 383-396, 1994.

A $(1,-1)$-matrix H of order m is called a *Hadamard* matrix if $HH^t = mI_m$, where H^t is the transpose of H and I_m is the identity matrix of order m. A *Sylvester-Hadamard matrix* or *Walsh-Hadamard matrix* of order 2^n, denoted by H_n, is generated by the following recursive relation

$$H_0 = 1,\ H_n = \begin{bmatrix} H_{n-1} & H_{n-1} \\ H_{n-1} & -H_{n-1} \end{bmatrix},\ n = 1, 2, \ldots.$$

Now we introduce bent functions, an important combinatorial concept discovered by Rothaus in the mid 1960's, although his pioneering work was not published until some ten years later [14].

Definition 1. A function f on V_n is said to be bent if

$$2^{-\frac{n}{2}} \sum_{x \in V_n} (-1)^{f(x) \oplus \langle \beta, x \rangle} = \pm 1$$

for every $\beta \in V_n$. Here $x = (x_1, \ldots, x_n)$ and $f(x) \oplus \langle \beta, x \rangle$ is considered as a real valued function.

Bent functions can be characterized in various ways. In particular, the following statements are equivalent (see also [6]):

(i) f is bent.

(ii) $\langle \xi, \ell \rangle = \pm 2^{\frac{1}{2}n}$ for any affine sequence ℓ of length 2^n, where ξ is the sequence of f.

(iii) $f(x) \oplus f(x \oplus \alpha)$ is balanced for any non-zero vector $\alpha \in V_n$, where $x = (x_1, \ldots, x_n)$.

An $n \times s$ S-box or substitution box is a mapping from V_n to V_s, where $n \geq s$. Now we consider a nonlinearity criterion that measures the strength of an S-box against differential cryptanalysis [3, 4]. The essence of a differential attack is that it exploits particular entries in the difference distribution tables of S-boxes employed by a block cipher. The difference distribution table of an $n \times s$ S-box is a $2^n \times 2^s$ matrix. The rows of the matrix, indexed by the vectors in V_n, represent the change in the input, while the columns, indexed by the vectors in V_s, represent the change in the output of the S-box. An entry in the table indexed by (α, β) indicates the number of input vectors which, when changed by α (in the sense of bit-wise XOR), result in a change in the output by β (also in the sense of bit-wise XOR).

Note that an entry in a difference distribution table can only take an even value, the sum of the values in a row is always 2^n, and the first row is always $(2^n, 0, \ldots, 0)$. As entries with higher values in the table are particularly useful to differential cryptanalysis, a necessary condition for an S-box to be immune to differential cryptanalysis is that it does not have large values in its differential distribution table (not counting the first entry in the first row).

Definition 2. Let F be an $n \times s$ S-box, where $n \geq s$. Let δ be the largest value in differential distribution table of the S-box (not counting the first entry in the first row), namely,

$$\delta = \max_{\alpha \in V_n, \alpha \neq 0} \max_{\beta \in V_s} |\{x | F(x) \oplus F(x \oplus \alpha) = \beta\}|.$$

Then F is said to be *differentially δ-uniform*, and accordingly, δ is called the differential uniformity of f.

Obviously the differential uniformity δ of an $n \times s$ S-box is constrained by $2^{n-s} \leq \delta \leq 2^n$. Extensive research has been carried out in constructing differentially δ-uniform S-boxes with a low δ [1, 13, 2, 9, 10, 11, 12]. Some constructions, in particular those based on permutation polynomials on finite fields, are simple and elegant. However, caution must be taken with Definition 2. In particular, it should be noted that low differential uniformity (a small δ) is only a *necessary*, but not a *sufficient* condition for immunity to differential attacks. This is shown by the fact that S-boxes constructed in [1, 9], which have a flat difference distribution table, are extremely weak to differential attacks, despite that they achieve the lowest possible differential uniformity $\delta = 2^{n-s}$ [4, 5, 15]. A more complete measurement that takes into account the number of nonzero entries in the first column of a difference distribution table is the *robustness* introduced in [15].

Definition 3. Let $F = (f_1, \ldots, f_s)$ be an $n \times s$ S-box, where f_i is a function on V_n, $i = 1, \ldots, s$, and $n \geq s$. Denote by L the largest value in the difference distribution table of F, and by N the number of nonzero entries in the first column of the table. In either case the value 2^n in the first row is not counted. Then we say that F is R-robust against differential cryptanalysis, where R is defined by

$$R = (1 - \frac{N}{2^n})(1 - \frac{L}{2^n}).$$

Robustness gives more accurate information about the strength of an S-box against the differential attack than differential uniformity does. However, differential uniformity has an advantage over robustness in that the former is easier to discuss than the latter. For this reason, differential uniformity is employed as the first indicator for the strength of an S-box against the differential attack, while robustness is considered when more complete information about the strength is needed.

An $n \times s$ S-box $F = (f_1, \ldots, f_s)$ is said to be *regular* if F runs through each vector in V_s 2^{n-s} times while x runs through V_n once. S-boxes employed by a block cipher must be regular, since otherwise the cipher would be prone to statistical attacks. For a regular $n \times s$ S-box, its differential uniformity is larger than 2^{n-s} (see also Lemma 2 of [17]). The robustness of the S-box is further determined by the number of nonzero entries in the first column of the table.

We are particularly interested in $n \times s$ S-boxes that have the following property: for any nonzero vector $\alpha \in V_n$, $F(x) \oplus F(x \oplus \alpha)$ runs through half of the vectors in V_s, each 2^{n-s+1} times, but not through the other half of the vectors in V_n. With each row in the difference distribution table of such an S-box, half of its entries contain a value 2^{n-s+1} while the other half contain a value zero. For simplicity, we say such a difference distribution table to be ***uniformly half-occupied***. Clearly an $n \times s$ S-box with a UHODDT or uniformly half-occupied difference distribution table achieves the differential uniformity of 2^{n-s+1}. In Theorem 3 of [17], it has been proved that for quadratic S-boxes, 2^{n-s+1} is the lower bound on differential uniformity.

Note that a differentially 2-uniform permutation is also a permutation with a UHODDT, and vice versa. These permutations have many nice properties [13, 2, 9, 10, 11, 12]. In particular, they achieve the highest possible robustness against the differential attack. The concept of $n \times s$ S-boxes with a UHODDT can be viewed as a generalization of differentially 2-uniform permutations. Hence $n \times s$ S-boxes with a UHODDT are very appealing and have received extensive research (see for instance [2]).

There are two important questions about S-boxes with a UHODDT, namely

(i) Do there exist S-boxes with a UHODDT ? If there do, how to construct them ?
(ii) What is the robustness of an S-box with a UHODDT ?

When $n = s$, the answer to the first question is "yes". It has been shown in [13, 11, 2] that certain permutation polynomials on $GF(2^n)$, n odd, have a UHODDT. So far no result has been known regarding the case of $n > s$. In Section 2, we will partially solve the problem by showing that there exist no quadratic $n \times s$ S-boxes with a UHODDT, if either n or s is even. The second question will be discussed in Section 3. We will prove that the robustness of an S-box with a UHODDT is very low.

Another important question is the synthesis of S-boxes, namely

(iii) How to construct S-boxes from existing ones ?

This question will be discussed in Section 4. We will show that many synthesis methods *which were previously taken for granted*, in fact do ***not*** yield strong S-boxes, even though the starting S-boxes employed are all strong ones. Section 5 is solely devoted to the investigation of combinatorial properties of the differential distribution table of an quadratic permutation. We reveal a result that is very interesting even from the point of view of pure combinatorics, namely, every uniformly half-occupied difference distribution table of a quadratic permutation embodies a Sylvester-Hadamard matrix.

2 Nonexistence of Certain Quadratic S-boxes

2.1 On Quadratic S-boxes with a UHODDT

As mentioned in the previous section, an $n \times s$ S-box with a UHODDT or uniformly half-occupied difference distribution table achieves the differential uniformity of 2^{n-s+1}, and for quadratic S-boxes, 2^{n-s+1} is the lower bound on differential uniformity. In the following we show an impossibility result, namely, there exist no quadratic S-boxes that have a UHODDT if either n or s is even.

Assume that $F = (f_1, \ldots, f_s)$ is a quadratic $n \times s$ S-box with a UHODDT, where $n > s$. We prove that neither n nor s can be even.

Recall that a vector $\alpha \in V_n$ is called a *linear structure* of a function f on V_n if $f(x) \oplus f(x \oplus \alpha)$ is a constant. The set of the linear structures of f forms a linear subspace. The dimension of the subspace is called the *linearity dimension* of f. Let $\alpha_1, \ldots, \alpha_{2^n-1}$ be the $2^n - 1$ nonzero vectors in V_n and $g_1, \ldots, g_{2^s-1}$ be the $2^s - 1$ nonzero linear combinations of $f_1, \ldots, f_s$. We construct a bipartite graph whose vertices comprise $\alpha_1, \ldots, \alpha_{2^n-1}$ on one side and $g_1, \ldots, g_{2^s-1}$ on the other side. An edge or link between α_i and g_j exists if and only if α_i is a linear structure of g_j.

Theorem 2 of [17] states that $n - \ell_i$ is even, where ℓ_i is the linearity dimension of g_i. Equivalently, n and ℓ_i must be both even or both odd. Since each g_i is balanced, it can not be bent. By Lemma 5 of [17], a quadratic function is bent if and only if it does not have linear structures. Hence we have $\ell_i \geq 1$. On the other hand, from the proof for Corollary 1 of [17], we have $\ell_i \leq n - 2$. We distinguish the following two cases:

Case 1: n is odd and ℓ_i is $1, 3, 5, \ldots,$ or $n - 2$.

Case 2: n is even and ℓ_i is $2, 4, 6, \ldots,$ or $n - 2$.

First we consider Case 1. Let p_j denote the number of ℓ_i, $1 \leq i \leq 2^n - 1$, such that $\ell_i = j$. Then we have a sequence of numbers $p_1, p_3, p_5, \ldots, p_{n-2}$. Obviously,

$$p_1 + p_3 + p_5 + \cdots + p_{n-2} = 2^s - 1. \tag{1}$$

Since F is a S-box with a UHODDT, for any nonzero vector $\alpha_k \in V_n$

$$F(x) \oplus F(x \oplus \alpha_k) = (f_1(x) \oplus f_1(x \oplus \alpha_k), \ldots, f_s(x) \oplus f_s(x \oplus \alpha_k))$$

is not regular. Thus, by Lemma 6, there exists a linear combination of $f_1(x) \oplus f_1(x \oplus \alpha_k), \ldots, f_s(x) \oplus f_s(x \oplus \alpha_k)$, say $g_j(x) \oplus g_j(x \oplus \alpha_k)$, such that $g_j(x) \oplus g_j(x \oplus \alpha_k)$ is not balanced. Since $g_j(x) \oplus g_j(x \oplus \alpha_k)$ is affine, $g_j(x) \oplus g_j(x \oplus \alpha_k)$ must be constant. This proves that any nonzero vector $\alpha_k \in V_n$ is a linear structure of a g_j, a linear combination of $f_1, \ldots, f_s$. On the other hand, by Theorem 4 of [17], for each α_k, there exists at most one g_j among $g_1, \ldots, g_{2^s-1}$ such that α_k is a linear structure of g_j. By the construction of the bipartite graph, each α_k is linked to a unique g_j. Also each g_i with $\ell_i = j$ has j linearly independent linear structures and $2^j - 1$ nonzero linear structures. Hence we have

$$(2^1 - 1)p_1 + (2^3 - 1)p_3 + (2^5 - 1)p_5 + \cdots + (2^{n-2} - 1)p_{n-2} = 2^n - 1. \tag{2}$$

From (1) and (2) we have

$$(2^1 - 2)p_1 + (2^3 - 2)p_3 + (2^5 - 2)p_5 + \cdots + (2^{n-2} - 2)p_{n-2} = 2^n - 2^s$$

or equivalently

$$(2^2 - 1)p_3 + (2^4 - 1)p_5 + \cdots + (2^{n-3} - 1)p_{n-2} = 2^{s-1}(2^{n-s} - 1) \tag{3}$$

Note that $2^k - 1$ is divisible by 3 if and only $k \geq 2$ is even. Thus the left hand side of (3) is divisible by 3. This implies that the $(2^{n-s} - 1)$ part in the right hand side of the equation is divisible by 3. Hence s must be odd. Thus there exists no quadratic $n \times s$ S-box with a UHODDT if n is odd ($n \geq 5$) and s is even.

We now consider Case 2. Let q_j denote the number of ℓ_i, $1 \leq i \leq 2^n - 1$, such that $\ell_i = j$. Similarly to Case 1, we have a sequence of numbers $q_2, q_4, q_6, \dots, q_{n-2}$, and

$$q_2 + q_4 + q_6 \cdots + q_{n-2} = 2^s - 1,$$
$$(2^2 - 1)q_2 + (2^4 - 1)q_4 + (2^6 - 1)q_6 + \cdots + (2^{n-2} - 1)q_{n-2} = 2^n - 1.$$

By simple deduction,

$$(2^3 - 2)q_4 + (2^5 - 2)q_6 + \cdots + (2^{n-3} - 2)q_{n-2} = 2^{n-1} - 3 \cdot 2^{s-1} + 1. \quad (4)$$

It is not hard to see that the left hand side of (4) is even when $n \geq 4$, while the right hand side of (4) is always odd for $s \geq 2$. From this we can conclude that there exists no quadratic $n \times s$ S-box with a UHODDT if n is even with $n \geq 4$.

Summarizing Case 1 and Case 2, we have

Theorem 4. *For $n \geq 4$, there exists no quadratic $n \times s$ S-box with a UHODDT if either n or s is even.*

Theorem 4 can be viewed as an extension of Corollary 2 in [17], which states that there exists no differentially 2-uniform quadratic permutation on an even dimensional vector space.

By Theorem 4, $n \times s$ S-boxes with a UHODDT do not exist if either n or s is even. When n is odd and $n = s$, as mentioned before, we do have differentially 2-uniform quadratic permutation [13, 2, 11]. Thus a problem that is left open is whether there are quadratic S-boxes with a UHODDT for $n > s$, both n and s odd. It should be pointed out that an S-box which has an odd number of input bits and also an odd number of output bits may not be very useful in practice.

2.2 An Extension

The result in the previous subsection can be extended to a special kind of differentially 2^{n-s+t}-uniform quadratic S-boxes. Let F be a $n \times s$ S-box such that for any nonzero vector $\alpha \in V_n$, $F(x) \oplus F(x \oplus \alpha)$ runs through 2^{s-t} vectors in V_s, each 2^{n-s+t} times, but not through the remaining $2^s - 2^{s-t}$ vectors in V_s, where $t \geq 1$. The case when $t = 1$ has been discussed in the previous subsection. In the following we present a nonexistence result on the case when $t > 1$.

Theorem 5. *If n is odd and t is even, there exists no quadratic $n \times s$ S-boxes such that for any nonzero vector $\alpha \in V_n$, $F(x) \oplus F(x \oplus \alpha)$ runs through 2^{s-t} vectors in V_s, each 2^{n-s+t} times, but not through the remaining vectors in V_s.*

The proof will be provided in the full version.

3 Columns of a UHODDT

In the previous section we proved that there does not exist a quadratic $n \times s$ S-box with a UHODDT if either n or s is even. It is not clear whether or not higher degree S-boxes with a UHODDT exist. If there do exist such S-boxes, we would like to know whether or not they satisfy a more stringent requirement, namely high robustness. Results to be shown below give a negative answer to the question.

The following lemma is exactly the same as Theorem 1 of [17].

Lemma 6. *Let $F = (f_1, \ldots, f_s)$ be a mapping from V_n to V_s, where each f_j is a function on V_n. Then F is regular if and only if each nonzero linear combination of $f_1, \ldots, f_s$ is balanced.*

It is easy to show that the profile of the difference distribution table of an S-box is not changed by a nonsingular linear transformation on input coordinates (see for instance [2, 17]). In particular we have

Lemma 7. *Let $F = (f_1, \ldots, f_s)$ be a regular S-box with a UHODDT or uniformly half-occupied difference distribution table. Let A be a nonsingular matrix of order n and B a nonsingular matrix of order s over $GF(2)$. Then both Let $G(x) = F(xA) = (f_1(xA), \ldots, f_n(xA))$ and $H(x) = F(x)B = (f_1(x), \ldots, f_n(x))B$ are regular S-boxes with a UHODDT.*

By definition, each row in a uniformly half-occupied difference distribution table, except the first, contains an equal number of zero and nonzero entries. The following lemma shows that a similar result holds with columns in the table.

Lemma 8. *Let F be a regular $n \times s$ S-box with a UHODDT. Then each column, except the first, in the difference distribution table contains an equal number of zero and nonzero entries.*

Proof. We prove that for each nonzero $\beta \in V_s$, there exist 2^{n-1} nonzero $\alpha \in V_n$ such that $F(x) \oplus F(x \oplus \alpha) = \beta$ has solutions for x.

Fix $x_0 \in V_n$. Since the difference distribution table of F is uniformly half-occupied, $F(x_0) \oplus F(x_0 \oplus \alpha)$ runs through each nonzero $\beta \in V_s$ 2^{n-s} times while α runs through V_n. As x_0 is arbitrary, for each nonzero $\beta \in V_s$, there exist $2^n \cdot 2^{n-s}$ pairs (x, α) such that $F(x) \oplus F(x \oplus \alpha) = \beta$, where $\alpha \neq 0$. On the other hand, since the difference distribution table of F is uniformly half-occupied, $F(x) \oplus F(x \oplus \alpha) = \beta$ either has 2^{n-s+1} solutions or has no solution for x. Thus for each nonzero $\beta \in V_s$ there exist $2^n \cdot 2^{n-s}/2^{n-s+1} = 2^{n-1}$ nonzero vectors $\alpha \in V_n$ such that $F(x) \oplus F(x \oplus \alpha) = \beta$ has solutions for x.

Recall that the robustness of an S-box is determined by the largest value in the difference distribution table of the S-box, and also by the number of nonzero entries in the first column of the table. The lemma described below gives the precise number of nonzero entries in the first column of a uniformly half-occupied difference distribution table.

Lemma 9. *Let F be a regular $n \times s$ S-box with a UHODDT. Then there are $2^{n-1} - 2^{s-1}$ nonzero entries in the first column of the difference distribution table (excluding the first entry).*

As an immediate consequence of Lemma 9, we obtain the robustness of an S-box with a UHODDT:

$$R = [1 - (2^{n-1} - 2^{s-1})/2^n](1 - 2^{n-s+1}/2^n) = (1/2 + 2^{-n+s-1})(1 - 2^{-s+1}).$$

When $n = s$, we have $R = 1 - 2^{-n+1}$, which is the highest possible value for robustness. However, when s is relatively smaller than n, say $n - s > 3$, R is very close to $1/2$. For comparison, we note that the robustness of S-boxes constructed in [15] is at least $7/8$.

4 On Methods for Synthesizing S-boxes

This section is concerned with methods for constructing S-boxes from existing ones. We show that a number of techniques which were previously taken for granted do not yield good S-boxes.

4.1 Chopping Permutations

Chopping permutations which are cryptographically strong has been conceived as a promising method to construct S-boxes for DES-like encryption algorithms. For this reason, many researchers have focused their attention on permutations, especially those on a finite field [2, 9, 10, 11, 12]. Results to be present in this subsection indicate that, contrary to the common perception, this practice does not produce good S-boxes.

First we prove the following:

Theorem 10. *Let $F = (f_1, \dots, f_s)$ be a regular $n \times s$ S-box with a UHODDT, where $n \geq s$ and each f_j is a function on V_n. The following two statements hold:*

(i) Let $1 \leq t \leq s-1$ and let G be an S-box obtained by dropping $s-t$ component functions from F, say $G = (f_1, \dots, f_t)$. Then the difference distribution table of G is not uniformly half-occupied.

(ii) Let $n \geq t \geq s+1$ and let H be an S-box obtained by adding $t-s$ component functions to F, say $H = (f_1, \dots, f_s, f_{s+1}, \dots, f_t)$, where $f_{s+1}, \dots, f_t$ are newly added. Then the difference distribution table of H is not uniformly half-occupied.

Proof. (i) Since F has a UHODDT, for any nonzero $\alpha \neq 0$, $F(x) \oplus F(x \oplus \alpha)$ runs through 2^{s-1} vectors in V_s, each 2^{n-s+1} times, but not through the other 2^{s-1} vectors in V_s, while α runs through V_n. Fix a nonzero vector, say $\gamma = (0, \beta) \in V_s$, where 0 is the zero vector in V_t and β is a nonzero vector in V_{s-t}. By Lemma 8 there exist 2^{n-1} nonzero vector α such that $F(x) \oplus F(x \oplus \alpha) = \gamma$ has solutions for x. Thus there exist 2^{n-1} nonzero vector α such that $G(x) \oplus G(x \oplus \alpha) = 0$, where

0 is the zero vector in V_t, has solutions for x. It is easy to show that G is not uniformly half-occupied. Since G is regular there exist $2^{n-1}-2^{t-1}$ nonzero vector α such that $G(x) \oplus G(x \oplus \alpha) = 0$ (see Lemma 8) if G is uniformly half-occupied.

(ii) follows (i).

From Theorem 10 chopping a regular S-box with a UHODDT does not yield a regular S-box with a UHODDT. In particular, chopping a differentially 2-uniform permutation on V_n does not produce an S-box with a UHODDT.

As quadratic permutations with a UHODDT or differentially 2-uniform quadratic permutations have been studied very extensively, an important problem is about the structure of the difference distribution table of an S-box obtained by chopping such a permutation. We will devote a single section, Section 5, to this topic.

In addition to chopping permutations, other techniques, such as linear transforms or modulo operations on inputs or outputs of differentially 2-uniform permutations, and repeating differentially 2-uniform permutations, are also conceived as possible S-box synthesis methods. In the following we show that none of these methods generates an S-box with a UHODDT.

4.2 Linear Transforms Applied on Inputs

Let F be a differentially 2-uniform permutation on V_s, B a matrix of order $n \times s$ $(n > s)$ over $GF(2)$. Set $G(y) = F(yB)$ where $y \in V_n$. Since the rank of B is s, yB runs through 2^s vectors in V_s each 2^{n-s} times while y runs through V_n. Since F is a permutation on V_s, $G(y)$ is a regular $n \times s$ S-box.

Unfortunately the difference distribution table of $G(y)$ is not uniformly half-occupied. The reason is described in the following. Since $n > s$ there exists a nonzero vector, say β, such that $\beta B = 0$, where 0 is the zero vector in V_s. Note that $G(y) \oplus G(y \oplus \beta) = F(yB) \oplus F((y \oplus \beta)B) = F(yB) \oplus F(yB \oplus \beta B) = F(yB) \oplus F(yB) = 0$, where 0 is the zero vector in V_s, for every $y \in V_n$.

4.3 Linear Transforms Applied on Outputs

Let F be a differentially 2-uniform permutation on V_s, and B a matrix of order $n \times s$ $(n > s)$ over $GF(2)$. Set $G(x) = F(x)B$. Note that the rank of B is s. Hence yB runs through 2^s vectors in V_s each 2^{n-s} times while y runs through V_n. As F is a permutation on V_n, G is a regular $n \times s$ S-box.

Since $n > s$, there exists a matrix of order $n \times (n-s)$, say D, such that the matrix $A = [BD]$ of order n is nonsingular. Set $\Psi(x) = F(x)A$. By Lemma 7, Ψ is a also a differentially 2-uniform permutation. By Theorem 10, G is not an S-box with a UHODDT.

4.4 Connecting Permutations in Parallel

Let F be a differentially 2-uniform permutation on V_s. Set

$$G(y) = (1 \oplus x_{s+1})F(x) \oplus x_{s+1}F(x \oplus \alpha)$$

where $x = (x_1, \ldots, x_s)$, $y = (x_1, \ldots, x_s, x_{s+1})$, $\alpha \in V_s$. Note that $G(x, 0) = F(x)$, $G(x, 1) = F(x \oplus \alpha)$. Since F is permutation on V_s G is a regular $(s+1) \times s$ S-box.

Let $\beta = (\alpha, 1)$. Clearly $G(y \oplus \beta) = G(y)$ for every $y \in V_{s+1}$. Thus $G(y) \oplus G(y \oplus \beta) = 0$, where 0 is the zero vector in V_s, for every $y \in V_n$. Thus the difference distribution is very bad in this case, and $G(y)$ is not an S-box with a UHODDT.

The above discussions can be extended to the general case where F is repeated 2^k times, $k \geq 1$.

4.5 Enlarging Inputs or Reducing Outputs by Modulo Operations

Let $\alpha = (a_1, \ldots, a_n) \in V_n$. Rewrite α as $\alpha = a_1 \oplus a_2 x \oplus \cdots \oplus a_n x^{n-1}$. Thus V_n and the set of polynomials of degree at most $n-1$ over $GF(2)$ have a one-to-one correspondence. Let $\sigma(x)$ be a primitive polynomial of degree s $(s < n)$. For any $\alpha \in V_n$, we have

$$\alpha = h\sigma \oplus \overline{\alpha}$$

where the degree of h is less than or equal to $n - s - 1$, the degree of $\overline{\alpha}$ is less than s. Thus we have defined a mapping from V_n to V_s: $\alpha \rightarrow \overline{\alpha}$.

Now let ξ be a vector in V_n and $\overline{\xi}$ a vector in V_s. Let $F(\overline{\xi})$ be a differentially 2-uniform permutation on V_s. Set $G(\xi) = F(\overline{\xi})$. This gives an $n \times s$ S-box. Note that $\overline{\xi \oplus \eta} = \overline{\xi} \oplus \overline{\eta}$. This means that the mapping from V_n to V_s, $\alpha \rightarrow \overline{\alpha}$, is linear. Hence $G(\xi)$ is not an S-box with a UHODDT, although it is regular (see Subsection 5.1).

Now let $\Phi(\xi)$ be a differentially 2-uniform permutation on V_n. Set $\Psi(\xi) = \overline{\Phi(\xi)}$. Ψ is an $n \times s$ S-box. A similar argument shows that the difference distribution table of $\Psi(\xi)$ is not uniformly half-occupied.

5 Hadamard Matrices Embodied in Difference Distribution Table

In this section we reveal a very important combinatorial property of differentially 2-uniform quadratic permutations, namely, every differentially 2-uniform quadratic permutation is associated with a Sylvester-Hadamard matrix. As an application of the result, we show that chopping a differentially 2-uniform quadratic permutation results in an S-box whose difference distribution table is nearly flat. Such an S-box is very weak to the differential attack.

5.1 Difference Distribution Tables and Incidence Functions

Let $F = (f_1, \ldots, f_n)$ be a differentially 2-uniform quadratic permutation on V_n, namely, a quadratic permutation with a UHODDT or uniformly half-occupied difference distribution table. Let W_α be the set of vectors $F(x) \oplus F(x \oplus \alpha)$ runs through when x runs through V_n, namely,

$$W_\alpha = \{F(x) \oplus F(x \oplus \alpha) | x \in V_n\} \tag{5}$$

Obviously if $\alpha = 0$ then $W_\alpha = \{0\}$. Since each f_j is quadratic $f_j(x) \oplus f_j(x \oplus \alpha)$ is an affine function.

Write $f_j \oplus f_j(x \oplus \alpha) = c_{1j}x_1 \oplus \cdots \oplus c_{nj}x_n \oplus d_j$, $j = 1, \ldots, n$. Set $C_\alpha = (c_{ij})$, $\sigma_\alpha = (d_1, \ldots, d_n)$. Thus $F(x) \oplus F(x \oplus \alpha) = xC_\alpha \oplus \sigma_\alpha$ and $W_\alpha = \{F(x) \oplus F(x \oplus \alpha) | x \in V_n\} = \{xC_\alpha \oplus \sigma_\alpha | x \in V_n\}$.

Now let $\alpha \neq 0$. Since F is a permutation, $F(x) \oplus F(x \oplus \alpha) \neq 0$ for any $x \in V_n$. Hence $0 \notin W_\alpha$. Since $F(0) \oplus F(\alpha) = \sigma_\alpha$, we have $\sigma_\alpha \neq 0$. And by the definition of a UHODDT, $|W_\alpha| = 2^{n-1}$ and hence $rank(C_\alpha) = n - 1$. Thus we have

Lemma 11. *Let F be a differentially 2-uniform quadratic permutation on V_n. If $\alpha \neq 0$ then*
(i) $0 \notin W_\alpha$, (ii) $\sigma_\alpha \neq 0$, (iii) $|W_\alpha| = 2^{n-1}$, and (iv) $rank(C_\alpha) = n - 1$.

Now set $W_\alpha^0 = \{xC_\alpha | x \in V_n\}$. Then we have

Lemma 12. *Let F be a differentially 2-uniform quadratic permutation on V_n. If $\alpha \neq 0$ then $V_n = W_\alpha \cup W_\alpha^0$ and $W_\alpha \cap W_\alpha^0 = \phi$.*

Lemma 13. *Let F be a differentially 2-uniform quadratic permutation on V_n. Let $\alpha \neq 0$. Then the following statements hold:*

(i) If β, $\beta' \in W_\alpha$ then $\beta \oplus \beta' \in W_\alpha^0$,
(ii) if $\beta \in W_\alpha$, $\beta' \in W_\alpha^0$ then $\beta \oplus \beta' \in W_\alpha$,
(iii) if β, $\beta' \in W_\alpha^0$ then $\beta \oplus \beta' \in W_\alpha^0$.

Let F be a differentially 2-uniform quadratic permutation on V_n and let W_α be the same as (5). For each $\alpha \in V_n$ we define an *incidence function* φ_α as follows:

$$\varphi_\alpha(\beta) = \begin{cases} 0 \text{ if } \alpha = 0 \\ \\ 1 \text{ if } \alpha \neq 0 \text{ and } \beta \in W_\alpha \\ 0 \text{ if } \alpha \neq 0 \text{ and } \beta \notin W_\alpha \end{cases} \tag{6}$$

As is to be proved below, each φ_α is in fact a linear function on V_n.

Lemma 14. *Let F be a differentially 2-uniform quadratic permutation on V_n. Then φ_α, defined in (6), is a linear function on V_n for every vector $\alpha \in V_n$.*

Lemma 15. *Let F be a differentially 2-uniform quadratic permutation on V_n. If $\alpha \neq \alpha'$, then $\varphi_\alpha \neq \varphi_{\alpha'}$.*

5.2 Hadamard Matrices in Difference Distribution Tables

Lemma 14 states that each row of the differential distribution table is associated with a linear function on V_n, while Lemma 15 indicates that these linear functions are all different. Hence we have

Theorem 16. *Let F be a differentially 2-uniform quadratic permutation on V_n. Then φ_α runs through all linear functions on V_n while α runs through the vectors in V_n.*

Recall that $\alpha_0, \alpha_1, \ldots, \alpha_{2^n-1}$ are all the vectors in V_n, with $\alpha_0 = (0, \ldots, 0)$, $\ldots$, $\alpha_{2^n-1} = (1, \ldots, 1)$. Let $M = (m_{ij})$ be a $(1, -1)$-matrix defined by

$$m_{ij} = (-1)^{\varphi_{\alpha_i}(\alpha_j)} \tag{7}$$

M is called the *difference trait matrix* of F. Essentially, M is a matrix obtained from the difference distribution table of the S-box by replacing each zero entry by 1 and each nonzero entry by -1, with an exception that the first entry in the first row is replaced by 1.

Theorem 17. *Let F be a differentially 2-uniform quadratic permutation on V_n. Then M, the difference trait matrix of F, is a Sylvester-Hadamard matrix if the row-order is ignored.*

Proof. From Theorem 16, the 2^n rows of M comprise all the linear sequences of length 2^n. By Lemma 1 of [16], each linear sequence of length 2^n is a row of H_n. Thus M can be changed to H_n by re-ordering its rows.

Obviously, W_α, φ_α and M can be defined for any permutation on V_n, not restricted to quadratic ones.

Theorem 18. *Let F be a differentially 2-uniform quadratic permutation on V_n and M be the difference trait matrix of F. Then the inverse of F is also a differentially 2-uniform permutation, whose difference trait matrix is the transpose of M.*

Note that for a differentially 2-uniform quadratic permutation F based on a cubic polynomial on $GF(2^n)$, n odd, the algebraic degree of F^{-1} is larger than $(n+1)/2$. By Theorem 18, both the difference trait matrix of F and that of F^{-1} are Sylvester-Hadamard matrices (subject to re-ordering their rows).

5.3 Chopping Quadratic Permutations

Let $F = (f_1, \ldots, f_n)$ be a differentially 2-uniform permutation on V_n. Let G be an S-box obtained by chopping a component function of F, say $G = (f_2, \ldots, f_n)$. Similarly to W_α, φ and M corresponding to F (see (5), (6) and (7)), we can define

$$U_\alpha = \{G(x) \oplus G(x \oplus \alpha) | x \in V_n\},$$

where $\alpha \in V_n$, and the incidence function

$$\psi_\alpha(\beta) = \begin{cases} 0 \text{ if } \alpha = 0 \\ \\ 1 \text{ if } \alpha \neq 0 \text{ and } \beta \in U_\alpha \\ 0 \text{ if } \alpha \neq 0 \text{ and } \beta \notin U_\alpha \end{cases}$$

where $\beta \in V_{n-1}$.

Let $\alpha_0, \alpha_1, \cdots, \alpha_{2^n-1}$ be the ordered vectors in V_n and $\beta_0, \beta_1, \cdots, \beta_{2^{n-1}-1}$ the ordered vectors in V_{n-1}. Define a $2^n \times 2^{n-1}$ (1, -1)-matrix, say $N = (n_{ij})$, where $n_{ij} = (-1)^{\psi_{\beta_i}(\beta_j)}$.

Write $M = [M_1 M_2]$ where each M_j is of order $2^n \times 2^{n-1}$, $M_1 = (m_{ij})$, and $M_2 = (m_{ij+2^{n-1}})$. It is easy to see that $\psi_\alpha(\beta) = 1$ if and only if $\varphi_\alpha(0, \beta) = 1$ or $\varphi_\alpha(1, \beta) = 1$. In other words, $n_{ij} = -1$ if and only if $m_{ij} = -1$ or $m_{ij+2^{n-1}} = -1$.

Since F is a differentially 2-uniform quadratic permutation, by Theorem 17, each row of M is a row of H_n. Now recall that $H_n = \begin{bmatrix} H_{n-1} & H_{n-1} \\ H_{n-1} & -H_{n-1} \end{bmatrix}$. Write $H_n = (h_{ij})$, $i, j = 1, \ldots, 2^n$. We can see that $-h_{ij} = h_{ij+2^{n-1}}$ if $i > 2^{n-1}$. This implies that $h_{ij} = -1$ or $m_{ij+2^{n-1}} = -1$, if $i > 2^{n-1}$. Note that M and H_n have the same set of rows. This proves that there exists 2^{n-1} nonzero $\alpha \in V_n$ such that ψ_α is constant 1. In this case $G(x) \oplus G(x \oplus \alpha)$ runs through every vector (including the zero vector) in V_{n-1}, for some 2^{n-1} nonzero vectors $\alpha \in V_n$ and hence the robustness of G is less than $\frac{1}{2}$.

To summarize the above discussions, the difference distribution table of an S-box obtained by chopping a component function of a differentially 2-uniform quadratic permutation has the following profile: it can be viewed as a folded (right to left) version of the uniformly half-occupied table of the original permutation, with half of the rows containing a value 2 in all their entries, and the remaining rows, not counting the first row, containing an equal number of 0s and 4s. Similarly, chopping two component functions from a permutation results in an S-box whose difference distribution table is almost flat: it can be viewed as a twice-folded (right to left) version of the uniformly half-occupied table of the original permutation, and three quarters of the rows contain a value 4 in all their entries, while the remaining rows, not counting the first row, have an equal number of 0s and 8s. This observation can be extended to the case when three or more component functions are chopped.

In conclusion, S-boxes obtained by chopping differentially 2-uniform quadratic permutations have an almost flat difference distribution table, which renders a DES-like encryption algorithm that employs such S-boxes very prone to the differential attack.

Acknowledgments The first author was supported in part by the Australian Research Council under the reference numbers A49130102, A49131885 and A49232172, the second author by A49130102, and the third author by A49232172. All authors were supported by a University of Wollongong Research Program grant and the first two by ATERB C010/058. The authors would like to thank the anonymous referees for Crypto'94 for their helpful comments.

References

1. Adams, C. M.: On immunity against Biham and Shamir's "differential cryptanalysis". Information Processing Letters **41** (1992) 77–80

2. Beth, T., Ding, C.: On permutations against differential cryptanalysis. In Advances in Cryptology - EUROCRYPT'93 (1994) vol. 765, Lecture Notes in Computer Science Springer-Verlag, Berlin, Heidelberg, New York pp. 65–76
3. Biham, E., Shamir, A.: Differential cryptanalysis of DES-like cryptosystems. Journal of Cryptology **Vol. 4, No. 1** (1991) 3–72
4. Biham, E., Shamir, A.: Differential Cryptanalysis of the Data Encryption Standard. Springer-Verlag New York, Heidelberg, Tokyo 1993
5. Brown, L., Kwan, M., Pieprzyk, J., Seberry, J.: Improving resistance to differential cryptanalysis and the redesign of LOKI. In Advances in Cryptology - ASIACRYPT'91 (1993) vol. 739, Lecture Notes in Computer Science Springer-Verlag, Berlin, Heidelberg, New York pp. 36–50
6. Dillon, J. F.: A survey of bent functions. The NSA Technical Journal (1972) 191–215
7. Matsui, M.: Linear cryptanalysis method for DES cipher. In Advances in Cryptology - EUROCRYPT'93 (1994) vol. 765, Lecture Notes in Computer Science Springer-Verlag, Berlin, Heidelberg, New York pp. 386–397
8. Matsui, M.: Linear cryptanalysis method for DES cipher (II). In Proceedings of 1994 Symposium on Cryptography and Information Security (Japan, 1994)
9. Nyberg, K.: Perfect nonlinear S-boxes. In Advances in Cryptology - EUROCRYPT'91 (1991) vol. 547, Lecture Notes in Computer Science Springer-Verlag, Berlin, Heidelberg, New York pp. 378–386
10. Nyberg, K.: On the construction of highly nonlinear permutations. In Advances in Cryptology - EUROCRYPT'92 (1993) vol. 658, Lecture Notes in Computer Science Springer-Verlag, Berlin, Heidelberg, New York pp. 92–98
11. Nyberg, K.: Differentially uniform mappings for cryptography. In Advances in Cryptology - EUROCRYPT'93 (1994) vol. 765, Lecture Notes in Computer Science Springer-Verlag, Berlin, Heidelberg, New York pp. 55–65
12. Nyberg, K., Knudsen, L. R.: Provable security against differential cryptanalysis. In Advances in Cryptology - CRYPTO'92 (1993) vol. 740, Lecture Notes in Computer Science Springer-Verlag, Berlin, Heidelberg, New York pp. 566–574
13. Pieprzyk, J.: Bent permutations. In Proceeding of the International Conference on Finite Fields, Coding Theory, and Advances in Communications and Computing (Las Vegas, 1991)
14. Rothaus, O. S.: On "bent" functions. Journal of Combinatorial Theory **Ser. A, 20** (1976) 300–305
15. Seberry, J., Zhang, X. M., Zheng, Y.: Systematic generation of cryptographically robust S-boxes. In Proceedings of the first ACM Conference on Computer and Communications Security (1993) The Association for Computing Machinery, New York pp. 172 - 182
16. Seberry, J., Zhang, X. M., Zheng, Y.: Nonlinearly balanced boolean functions and their propagation characteristics. In Advances in Cryptology - CRYPTO'93 (1994) vol. 773, Lecture Notes in Computer Science Springer-Verlag, Berlin, Heidelberg, New York pp. 49–60
17. Seberry, J., Zhang, X. M., Zheng, Y.: Relationships among nonlinearity criteria. Presented at *EUROCRYPT'94*, 1994