Journal of Universal Computer Science, vol. 1, no. 5 (1995), 320-337
submitted: 8/10/95, accepted: 10/5/95, appeared: 28/5/95, ©Springer Pub. Co.

GAC — the Criterion for Global Avalanche Characteristics of Cryptographic Functions

Xian-Mo Zhang
(The University of Wollongong, Wollongong, NSW 2522, Australia
xianmo@cs.uow.edu.au)

Yuliang Zheng
(Monash University, Melbourne, VIC 3199, Australia
yzheng@fcit.monash.edu.au)

Abstract: We show that some widely accepted criteria for cryptographic functions, including the strict avalanche criterion (SAC) and the propagation criterion, have various limitations in capturing properties of vital importance to cryptographic algorithms, and propose a new criterion called GAC to measure the global avalanche characteristics of cryptographic functions. We also introduce two indicators related to the new criterion, one forecasts the *sum-of-squares* while the other the *absolute* avalanche characteristics of a function. Lower and upper bounds on the two indicators are derived, and two methods are presented to construct cryptographic functions that achieve nearly optimal global avalanche characteristics.

Category: E.3

1 Why the GAC

In 1985, Webster and Tavares introduced the concept of the *strict avalanche criterion (SAC)* when searching for principles for designing DES-like data encryption algorithms [Web85, WT86]. A function is said to satisfy the SAC if complementing a single bit results in the output of the function being complemented with a probability of a half. More formally, let V_n denote the vector space of n tuples of elements from GF(2), a function f on V_n, a mapping from V_n into GF(2), is said to satisfy the SAC if for any n-bit vector α with $W(\alpha) = 1$, where $W(\cdot)$ denotes the Hamming weight, $f(x) \oplus f(x \oplus \alpha)$ assumes the values zero and one an equal number of times, namely $f(x) \oplus f(x \oplus \alpha)$ is a *balanced* function on V_n, where $\oplus$ denotes the addition in GF(2).

The SAC was generalized in one direction by Forré in [For89]. Forré defines that a function f satisfies the SAC of order k if a partial function obtained by keeping any k input bits to f constant still satisfies the SAC. Enumerating functions satisfying the higher order SAC is an interesting combinatorial problem and various results on this topic have been obtained over the past years (see for instance [Llo90, Llo92, Mit90]). In another direction, the SAC has been generalized by Adams and Tavares [AT90] and independently by Preneel et al [PLL+91] to what is now called the *propagation criterion.* A function f on V_n is said to satisfy the propagation criterion with respect to a vector $\alpha \in V_n$ if $f(x) \oplus f(x \oplus \alpha)$ is balanced, and to satisfy the propagation criterion of degree k if it satisfies the propagation criterion with respect to all nonzero vectors whose Hamming weight is at most k. In informal terms, f satisfies the propagation criterion of degree k if complementing k or less bits results in the output of f being complemented with a probability of a half. We note that functions satisfying the propagation criterion of degree n coincide with *bent functions*, an important combinatorial structure discovered by Rothaus [Rot76]. A combination of the two generalizations has also been studied in [PLL$^+$91, PGV91].

The SAC and its various generalizations are very important concepts in designing cryptographic functions employed by data encryption algorithms and one-way hashing functions. As is shown below, however, these concepts all have their limitations in capturing some of the vital characteristics required by a cryptographically strong function. The following concept of *linear structure* will be useful in our discussions. Given a function f on V_n and a vector $\alpha \in V_n$, the vector is said to be a linear structure of f if $f(x) \oplus f(x \oplus \alpha)$ is a constant. An affine function $f(x) = a_1x_1 \oplus \cdots \oplus a_nx_n \oplus c$, where $a_j, c \in GF(2)$, $j = 1, 2, \ldots, n$, has all the vectors in V_n as its linear structures. Hence having linear structures is generally regarded as an unwelcome property in cryptographic practice.

First we can see that the SAC is an indicator with a very strong local flavor, as it guarantees good avalanche characteristics with respect only to the vectors of Hamming weight one. A function that satisfies the SAC can have a large number of vectors of Hamming weight larger than one as its linear structures. Such functions, if employed in certain cryptographic algorithms or systems, can result in a potential security risk.

Next we consider generalizations of the SAC. The higher order SAC suggested by Forré in [For89] has not been widely accepted by the research community as a criterion of cryptographic significance, although the concept itself seems interesting from a combinatorial point of view. In contrast, the other generalization of the SAC, namely the propagation criterion, has well established its position in cryptographic design. This can be seen from work represented by [AT90, PLL$^+$91, PGV91, DT93, SZZ94b, SZZ95]. A function satisfying the propagation criterion of degree k shows the perfect avalanche characteristic with respect to vectors of Hamming weight not larger than k. This property, however, does not rule out the possibility that the function can have vectors of Hamming weight larger than k as its linear structures. For instance, all currently known methods for constructing functions satisfying higher degree propagation criteria, including those presented in [PGV91, DT93, SZZ94b, SZZ95], yield functions having undesirable linear structures. Therefore the propagation criterion, though being an extension of the SAC, is merely another indicator for local properties. On the other hand, the criterion is too strict in the sense that it requires that $f(x) \oplus f(x \oplus \alpha)$ be 100% balanced. This leads to the situation where a function satisfying the propagation criterion of the largest possible degree becomes bent. Although bent functions have nice properties, they are not balanced and hence can hardly be directly employed in practice.

In designing a cryptographic algorithm, we often need functions that satisfy a number of crucial cryptographic requirements such as balance, high nonlinearity, high algebraic degree and good avalanche characteristics. A function can be considered to have good avalanche characteristics if it does not have a nonzero linear structure and satisfies the propagation criterion with respect to the majority of the vectors.

These discussions show a necessity to search for a new criterion for cryptographic functions. The new criterion should overcome the shortcomings of the SAC or its generalizations, and be able to forecast the overall avalanche characteristic of a cryptographic function. The main aim of this paper is to put forward two closely related indicators that forecast the GAC or *global avalanche charac-*

teristic of a cryptographic function. We also present methods for constructing functions that have promising overall avalanche characteristics.

The rest of the paper is organized as follows: The two new indicators, one is called the *sum-of-squares* indicator and the other the *absolute* indicator, are introduced in Section 2, and the lower and upper bounds on the two indicators are discussed in Sections 3 and 4 respectively. Finally, Section 5 presents two methods, one for even and the other for odd dimensional spaces, for constructing cryptographic functions that have excellent nonlinear characteristics, including GACs, nonlinearity and balance.

2 Introducing the GAC

A *function* on V_n is a mapping from V_n into GF(2). The *truth table* of f is a $(0,1)$-sequence defined by $(f(\alpha_0), f(\alpha_1), \ldots, f(\alpha_{2^n-1}))$, where $\alpha_0 = (0,\ldots,0,0)$, $\alpha_1 = (0,\ldots,0,1)$, …, $\alpha_{2^{n-1}-1} = (1,\ldots,1,1)$. The *sequence* of f is a $(1,-1)$-sequence defined by $((-1)^{f(\alpha_0)}, (-1)^{f(\alpha_1)}, \ldots, (-1)^{f(\alpha_{2^n-1})})$, where each exponent is regarded as being real-valued.

f is said to show the perfect avalanche effect with respect to a vector $\alpha \in V_n$ if it satisfies the propagation criterion with respect to the vector, namely, $f(x) \oplus f(x \oplus \alpha)$ is balanced. We note that $f(x) \oplus f(x \oplus \alpha)$ is also called the directional derivative of f in the direction α. To broaden our observation, we say that f shows good avalanche effect with respect to α if $f(x) \oplus f(x \oplus \alpha)$ is almost balanced. By imposing certain conditions on α, we have the notion of the SAC as well as that of the propagation criterion. As shown in the previous section, this approach introduces various limitations in capturing the GAC or global avalanche characteristic of a cryptographic function. To get around the problem, we will not impose restrictions on α. Instead, we will let it be a free vector, which allows us to examine the overall avalanche characteristic of a function. The following are a few notations used in further discussions.

Let $\tilde{a} = (a_1, \cdots, a_m)$ and $\tilde{b} = (b_1, \cdots, b_m)$ be two vectors (or sequences), the *scalar product* of $\tilde{a}$ and $\tilde{b}$, denoted by $\langle \tilde{a}, \tilde{b} \rangle$, is defined as the sum of the component-wise multiplications. In particular, when $\tilde{a}$ and $\tilde{b}$ are from V_m, $\langle \tilde{a}, \tilde{b} \rangle = a_1 b_1 \oplus \cdots \oplus a_m b_m$, where the addition and multiplication are over $GF(2)$, and when $\tilde{a}$ and $\tilde{b}$ are $(1,-1)$-sequences, $\langle \tilde{a}, \tilde{b} \rangle = \sum_{i=1}^{m} a_i b_i$, where the addition and multiplication are over the reals.

Given a function f on V_n and a vector $\alpha \in V_n$, we denote by $\xi(\alpha)$ the sequence of $f(x \oplus \alpha)$. Note that $\xi(0)$ is identical to the sequence of f. In addition, $\xi(0) * \xi(\alpha)$, the component-wise multiplication of the two sequences, is the sequence of $f(x) \oplus f(x \oplus \alpha)$. Set $\Delta_f(\alpha) = \langle \xi(0), \xi(\alpha) \rangle$. $\Delta_f(\alpha)$ is called the *auto-correlation* of f with a shift α. To further simplify our discussions, $\Delta_f(\alpha)$ will be written as $\Delta(\alpha)$ if the function under consideration is clear. Obviously, $\Delta(\alpha) = 0$ if and only if $f(x) \oplus f(x \oplus \alpha)$ is balanced, and $|\Delta(\alpha)| = 2^n$ if and only if $f(x) \oplus f(x \oplus \alpha)$ is a constant, namely, α is a linear structure of f. More generally, we have

Lemma 1. *Let f be a function on V_n. Then the Hamming weight of the truth table of $f(x) \oplus f(x \oplus \alpha)$ is equal to $2^{n-1} - \frac{1}{2}\Delta(\alpha)$.*

Let e_+ and e_- denote the number of ones and minus ones in $\xi(0) * \xi(\alpha)$ respectively. Thus $e_+ - e_- = \Delta(\alpha)$, $(2^n - e_-) - e_- = \Delta(\alpha)$ and hence $e_- =$

$2^{n-1} - \frac{1}{2}\Delta(\alpha)$. As e_- is also the number of ones in the truth table of $f(x) \oplus f(x \oplus \alpha)$, the lemma holds.

The overall avalanche characteristic of a function f can be measured by examining $|\Delta(\alpha)|$ for all nonzero vectors α. We can say that a function has a good GAC or global avalanche characteristic if for most nonzero α, $|\Delta(\alpha)|$ is zero or very close to zero. Again only bent functions that are unbalanced satisfy the criterion perfectly ! In designing cryptographic algorithms, however, we are mainly interested in balanced functions.

Although simple, the concept of GAC introduces a number of problems to be resolved. These include

1. How to measure precisely the GAC of a function.
2. How to compare the GACs of two different functions.
3. What is the best GAC of a *balanced* function and how to construct balanced functions that achieve the best GAC.

To solve the various problems, we propose the following two indicators:

Definition 2. Let f be a function on V_n. Then the *sum-of-squares* indicator for the avalanche characteristic of f is defined by

$$\sigma_f = \sum_{\alpha \in V_n} \Delta^2(\alpha)$$

and the *absolute* indicator for the characteristic is defined by

$$\Delta_f = \max_{\alpha \in V_n, \alpha \neq 0} |\Delta(\alpha)|.$$

The smaller σ_f and Δ_f, the better the GAC of a function. Like many other nonlinearity characteristics of a function including nonlinearity, algebraic degree and the profile of difference distribution tables, the two indicators for the GAC are invariant under nonsingular linear transforms on the input coordinates.

3 The Sum-of-Squares Indicator σ_f

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 of order 2^n, denoted by H_n, is defined by the following recursive relation

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

Let ℓ_i be the ith row of H_n. By Lemma 2 of [SZZ94b], ℓ_i is the sequence of a linear function defined by $\varphi_i(x) = \langle \alpha_i, x \rangle = a_1x_1 \oplus a_2x_2 \oplus \cdots \oplus a_nx_n$, where $x = (x_1, x_2, \ldots, x_n)$ and $\alpha_i = (a_1, a_2, \ldots, a_n)$ is the ith vector in V_n in the ascending alphabetical order.

Definition 3. Let f be a function on V_n. The Walsh-Hadamard transform of f is defined as

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

where $\alpha = (a_1, \ldots, a_n) \in V_n$, $x = (x_1, \ldots, x_n)$ and $\langle \alpha, x \rangle = \bigoplus_{i=1}^n a_i x_i$, and $f(x) \oplus \langle \alpha, x \rangle$ is regarded as a real-valued function.

The Walsh-Hadamard transform has numerous applications in areas ranging from physical science to communications engineering. It appears in several slightly different forms [Rot76, MS77, Dil72]. The above definition follows the first formula in [Rot76]. It can be equivalently written as

$$(\hat{f}(\alpha_0), \hat{f}(\alpha_1), \ldots, \hat{f}(\alpha_{2^n-1})) = 2^{-\frac{n}{2}} \xi H_n$$

where α_i is the ith vector in V_n according to the ascending order, ξ is the sequence of f and H_n is the Sylvester-Hadamard matrix of order 2^n. More information regarding the transform can be found in [MS77, Dil72]. In addition, Beauchamp's book [Bea84] is a good source of information on other related orthogonal transforms with their applications.

We now introduce the concept of bent functions.

Definition 4. A function f on V_n is called a *bent* function if its Walsh-Hadamard transform satisfies

$$\hat{f}(\alpha) = \pm 1$$

for all $\alpha \in V_n$.

From [Dil72, AT90, SMZ93, YH89] we know that the following four statements are equivalent

(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 $x = (x_1, x_2, \ldots, x_n)$.

(iv) $M = ((-1)^{f(\alpha_i \oplus \alpha_j)})$, $0 \le i, j \le 2^n - 1$, which is called the matrix of f is a Hadamard matrix.

3.1 Bounds on σ_f

McFarland, when studying Walsh-Hadamard transform of functions, obtained the following result (see also Theorem 3.3 of [Dil72]):

$$M = 2^{-n} H_n \operatorname{diag}(\langle \xi, \ell_0 \rangle, \cdots, \langle \xi, \ell_{2^n-1} \rangle) H_n,$$

where f is a function on V_n, ξ is the sequence of f, $M = ((-1)^{f(\alpha_i \oplus \alpha_j)})$, $0 \le i, j \le 2^n - 1$, and ℓ_i is the ith row of H_n. Thus

$$MM^T = 2^{-n} H_n \operatorname{diag}(\langle \xi, \ell_0 \rangle^2, \cdots, \langle \xi, \ell_{2^n-1} \rangle^2) H_n.$$

The first row of MM^T is

$$(\Delta(\alpha_0), \Delta(\alpha_1), \cdots, \Delta(\alpha_{2^n-1}))$$

while the first row of $2^{-n} H_n \operatorname{diag}(\langle \xi, \ell_0 \rangle^2, \cdots, \langle \xi, \ell_{2^n-1} \rangle^2) H_n$ can be expressed as

$$2^{-n}(\langle \xi^*, \ell_0 \rangle, \cdots, \langle \xi^*, \ell_{2^n-1} \rangle) = 2^{-n} \xi^* H_n$$

where

$$\xi^* = (\langle \xi, \ell_0 \rangle^2, \cdots, \langle \xi, \ell_{2^n-1} \rangle^2).$$

Hence

$$(\Delta(\alpha_0), \Delta(\alpha_1), \cdots, \Delta(\alpha_{2^n-1})) = 2^{-n}(\langle \xi, \ell_0 \rangle^2, \cdots, \langle \xi, \ell_{2^n-1} \rangle^2) H_n.$$

Thus we have proved:

Theorem 5. *Let ξ be the sequence of a function f on V_n. Then*

$$(\Delta(\alpha_0), \Delta(\alpha_1), \cdots, \Delta(\alpha_{2^n-1})) H_n = (\langle \xi, \ell_0 \rangle^2, \cdots, \langle \xi, \ell_{2^n-1} \rangle^2).$$

This theorem is in fact a special form of a more general result, the Wiener-Khintchine Theorem [Bea84]. Now write $\eta = (\Delta(\alpha_0), \Delta(\alpha_1), \cdots, \Delta(\alpha_{2^n-1}))$. Since

$$\langle \xi^*, \xi^* \rangle = \langle \eta H_n, \eta H_n \rangle = \eta H_n H_n^T \eta^T = 2^n \langle \eta, \eta \rangle,$$

we have

$$\sum_{j=0}^{2^n-1} \langle \xi, \ell_j \rangle^4 = 2^n \sum_{\alpha \in V_n} \Delta^2(\alpha).$$

Thus the following result holds:

$$\sigma_f = \sum_{\alpha \in V_n} \Delta^2(\alpha) = 2^{-n} \sum_{j=0}^{2^n-1} \langle \xi, \ell_j \rangle^4. \tag{1}$$

A closely related equation is

$$\sum_{j=0}^{2^n-1} \langle \xi, \ell_j \rangle^2 = 2^{2n} \tag{2}$$

(See also p.416, [MS77]). Both (1) and (2) are special forms of a general equation attributed to Parseval [Bea84].

The *nonlinearity* of a function f on V_n, commonly denoted by N_f, is defined as the minimum Hamming distance between f and all the affine functions on V_n. On the other hand, the distance between two functions g_1 and g_2 on V_n, namely the number of disagreeing positions in the truth tables or sequences of the two functions, can be calculated by

$$d(g_1, g_2) = 2^{n-1} - \frac{1}{2} \langle \eta_1, \eta_2 \rangle$$

where η_i, $i = 1, 2$, are the sequences of g_1 and g_2 (see for instance Lemma 4 of [SZZ94b]). Hence for any f on V_n, we have

$$N_f = 2^{n-1} - \frac{1}{2}\max\{|\langle \xi, \ell_i \rangle|, 0 \le i \le 2^n - 1\}$$

where ξ is the sequence of f and $\ell_0, \ldots, \ell_{2^n-1}$ are the rows of H_n, namely, the sequences of the linear functions on V_n. Now considering Theorem 5, Lemma 1 and in particular, the equation (1), we can see that the nonlinearity of a function is closely related to the sum-of-squares avalanche characteristic of the function. In general, the larger the nonlinearity, the smaller (i.e., better) the sum-of-squares avalanche characteristic.

Theorem 6. *Let f be a function on V_n. Then*

(i) $2^{2n} \le \sigma_f \le 2^{3n}$,
(ii) $\sigma_f = 2^{2n}$ *if and only if f is a bent function,*
(iii) $\sigma_f = 2^{3n}$ *if and only if f is an affine function.*

Proof. (i) Note that $\Delta(0) = 2^n$. Hence

$$\sigma_f = \sum_{\alpha \in V_n} \Delta^2(\alpha) \ge \Delta^2(0) = 2^{2n}. \tag{3}$$

On the other hand, by Parseval's equation (2), we have

$$\sum_{j=0}^{2^n-1} \langle \xi, \ell_j \rangle^2 = 2^{2n}.$$

Thus

$$\sigma_f = 2^{-n} \sum_{j=0}^{2^n-1} \langle \xi, \ell_j \rangle^4 \le 2^{-n} (\sum_{j=0}^{2^n-1} \langle \xi, \ell_j \rangle^2)^2 = 2^{-n} 2^{4n} = 2^{3n}.$$

(ii) $\sigma_f = 2^{2n}$ if and only if $\Delta(\alpha) = 0$ for all $\alpha \neq 0$, namely, f is bent.

(iii) Set $b_j = \langle \xi, \ell_j \rangle^2$. Again by Parseval's equation (2), $\sum_{j=0}^{2^n-1} b_j = 2^n$. Now we have the following reasoning:
$\sigma_f = 2^{3n}$ if and only if
$2^{-n} \sum_{j=0}^{2^n-1} b_j^2 = 2^{3n}$ if and only if
$\sum_{j=0}^{2^n-1} b_j^2 = 2^{4n}$ if and only if
$\sum_{j=0}^{2^n-1} b_j^2 = (\sum_{j=0}^{2^n-1} b_j)^2$ if and only if
$b_i b_j = 0$ for $j \neq i$ if and only if
there exists a j_0 such that $b_{j_0} = 2^{2n}$ and $b_j = 0$ for $j \neq j_0$ if and only if
there exists a j_0 such that $\langle \xi, \ell_{j_0} \rangle = \pm 2^n$ and $\langle \xi, \ell_j \rangle = 0$ for $j \neq j_0$ if and only if
there exists a j_0 such that $\xi = \pm \ell_{j_0}$, i.e., f is an affine function. □

A more important topic is to find a lower bound on σ_f for balanced functions f. This is left as a problem for future research.

3.2 σ_f of Some Highly Nonlinear Functions

Now we discuss the sum-of-squares avalanche characteristics of some highly nonlinear functions.

The structure of a function f on V_n that satisfies the propagation criterion with respect to all but a subset $\Re$ of vectors in V_n, has been studied in [SZZ94d]. We note that $\Re$ always contains the zero vector in V_n. It has been shown in [SZZ94d] that

1. if $|\Re| = 2$ then n is odd, the nonlinearity of f satisfies $N_f = 2^{n-1} - 2^{\frac{1}{2}(n-1)}$ and in addition, there exists a nonsingular matrix of order n over GF(2), say A, such that $g(x) = f(Ax)$ can be written as
$$g(x) = cx_n \oplus h(x_1, \ldots, x_{n-1})$$
where c is a constant in GF(2) and h is a bent function on V_{n-1};
2. if $|\Re| = 4$ then n must be even, the nonlinearity of f satisfies $N_f = 2^{n-1} - 2^{\frac{1}{2}n}$ and there exists a nonsingular matrix of order n over GF(2), say B, such that $g(x) = f(Bx)$ can be written as
$$g(x) = c_1 x_{n-1} \oplus c_2 x_n \oplus h(x_1, \ldots, x_{n-2})$$
where c_1 and c_2 are constants in GF(2), and h is a bent function on V_{n-2};
3. in both cases, all vectors in $\Re$ are linear structures of f.

Now the sum-of-squares avalanche characteristics for the two cases can be determined.

1. if $|\Re| = 2$ then $n = 2k + 1$ and
$$\sigma_f = \sum_{\alpha \in V_{2k+1}} \Delta^2(\alpha) = \Delta^2(0) + \Delta^2(\alpha_1) = 2 \cdot 2^{4k+2} = 2^{4k+3},$$
where α_1 is the nonzero vector in $\Re$;
2. if $|\Re| = 4$ then $n = 2k$ and
$$\sigma_f = \sum_{\alpha \in V_{2k}} \Delta^2(\alpha) = \Delta^2(0) + \sum_{j=1}^{3} \Delta^2(\alpha_j) = 4 \cdot 2^{4k} = 2^{4k+2}$$
where α_i, $i = 1, 2, 3$, are the nonzero vectors in $\Re$.

Functions f on V_n with $|\Re| = 5$ are also studied in [SZZ94d], where it is shown that $N_f = 2^{n-1} - 2^{\frac{1}{2}(n-1)}$, n is odd and that $|\Delta(\alpha_i)| = 2^{n-1}$ for all the four nonzero vectors, α_1, α_1, α_3 and α_4, in the set $\Re$. Thus, the sum-of-squares avalanche characteristic of f with $\Re = 5$ is
$$\sigma_f = \sum_{\alpha \in V_{2k+1}} \Delta^2(\alpha) = \Delta^2(0) + \sum_{j=1}^{4} \Delta^2(\alpha_j) = 2^{4k+2} + 4 \cdot 2^{4k} = 2^{4k+3}.$$
This value is the same as that for the case when $|\Re| = 2$.

It is also shown in [SZZ94d] that functions with $|\Re| = 3$ or 6 do not exist.

4 The Absolute Indicator Δ_f

Let f be a function on V_n. Recall that Δ_f is defined as the maximum among all $\Delta(\alpha)$, $\alpha \neq 0$, and that $\Delta(\alpha) = \pm 2^n$ if and only if α is a linear structure of f. Thus the following result is straightforward.

Lemma 7. *Let f be a function on V_n. Then $0 \leq \Delta_f \leq 2^n$. Moreover, $\Delta_f = 0$ if and only if f is bent, and $\Delta_f = 2^n$ if and only if f has a nonzero linear structure.*

In particular, for any quadratic non-bent function f, we have $\Delta_f = 2^n$. Next we focus on functions whose algebraic degrees are at least three.

Now set $g(x) = f(x) \oplus f(x \oplus \alpha)$. Then the algebraic degree of g is one less than that of f. As $g(x) \oplus g(x \oplus \alpha) = 0$, g cannot be bent. Thus we have the following simple yet helpful lemma.

Lemma 8. *Let f be a function on V_n. Then for any nonzero vector $\alpha \in V_n$, $f(x) \oplus f(x \oplus \alpha)$ is not bent and its algebraic degree is one less than that of f.*

Recall that by Lemma 1, $\Delta_f(\alpha)$ and the Hamming weight $W(g)$ of $g(x) = f(x) \oplus f(x \oplus \alpha)$ are related by $W(g) = 2^{n-1} - \frac{1}{2}\Delta_f(\alpha)$, or equivalently, $\Delta_f(\alpha) = 2(2^{n-1} - W(g))$. Therefore, assume that f is a function on V_n of algebraic degree k, the problem of finding Δ_f is reduced to that of finding the minimum Hamming weight of functions on V_n of algebraic degree $k-1$ which are *integrable* in the sense that they can be expressed as $f(x) \oplus f(x \oplus \alpha)$ with α a nonzero vector in V_n.

For a function f on V_n of algebraic degree $k \geq 3$, Δ_f is to some extent connected to the weight distribution of the $(k-1)$st order binary Reed-Muller code $\mathrm{RM}(k-1, n)$. Here $\mathrm{RM}(r, n)$ is defined as the collection of *all* functions on V_n, whose algebraic degrees are at most r. The minimum Hamming weight of $\mathrm{RM}(r, n)$, i.e., the minimum Hamming weight of functions on V_n of algebraic degree r, is known to be 2^{n-r} (see Theorem 3, p.375 of [MS77]). Now the connection between Δ_f of a function f on V_n of algebraic degree k and $\mathrm{RM}(k-1, n)$ can be precisely stated as

$$\Delta_f \geq 2(2^{n-1} - 2^{n-k+1}) = 2^n - 2^{n-k+2}$$

where 2^{n-k+1} is the minimum Hamming weight of $\mathrm{RM}(k-1, n)$. This lower bound on Δ_f, however, is very rough and not satisfactory. The reason is that 2^{n-k+1} is the minimum Hamming weight of *all* functions on V_n, whose algebraic degrees are $k-1$, including those which are *not integrable*. Hence it is one of our aims to find a lower bound on Δ_f that is smaller (i.e., better) than the value $2^n - 2^{n-k+2}$.

On the other hand, in designing cryptographic algorithms we are more concerned with balanced nonlinear functions than non-balanced ones. Therefore it is an important issue to know how small the absolute indicator Δ_f can be, for a balanced nonlinear function f on V_n. In the rest of the section we report the result we have obtained on the lower bound of Δ_f of cubic functions. This result can be regarded as the first step towards fully answering the question about Δ_f.

The following two results (see for instance Lemma 9 of [SMZ93] and Lemma 5 of [SZZ94c] respectively), will be employed in the discussions of cubic functions.

Lemma 9. *$f(x_1, \ldots, x_n) = \psi(x_1, \ldots, x_r) \oplus h(x_{r+1}, \ldots, x_n)$ is balanced on V_n if ψ is balanced on V_r or h is balanced on V_{n-r}.*

Lemma 10. *If f is a quadratic function and does not have nonzero linear structures, then it is bent.*

According to Lemma 10, a quadratic non-bent function f must have at least one linear structure. Hence the lower bound on Δ_f for such a function is (trivially) equal to 2^n. For cubic functions, we have a result described in the following theorem.

Theorem 11. *Let f be a non-bent cubic function on V_n. Then $\Delta_f \geq 2^{\frac{1}{2}(n+1)}$.*

Proof. Since f is not bent, there exists a nonzero vector in V_n, say α, such that $f(x) \oplus f(x \oplus \alpha)$ is not balanced. We set $g(x) = f(x) \oplus f(x \oplus \alpha)$ and want to find out the Hamming weight of the truth table of g from which we can find out $\Delta(\alpha)$ and hence the lower bound on Δ_f.

By Lemma 8, g is not bent. Note that g is quadratic. By Lemma 10, g has nonzero linear structures. it is easy to see [Nyb93] that all the linear structures of a function on V_n form a linear subspace of V_n. Denote by W the linear subspace formed by the linear structures of g, and by r the dimension of W. From [SZZ94c], there exists a nonsingular matrix A of order n on GF(2) such that $g^*(x) = g(xA)$ can be expressed as

$$g^*(x_1, \ldots, x_n) = \psi(x_1, \ldots, x_r) \oplus h(x_{r+1}, \ldots, x_n)$$

where ψ is a linear function on W while h is a function on V_{n-r} that does not have nonzero linear structures. Note that the truth tables of g^* and g have the same Hamming weight. Now suppose that ψ is a nonzero linear function. Then ψ is balanced. By Lemma 9, g^* is balanced, which contradicts the fact that g is not balanced. Consequently ψ must be equal to zero and hence

$$g(x_1, \ldots, x_n) = h(x_{r+1}, \ldots, x_n). \tag{4}$$

As h does not have nonzero linear structures, by Lemma 10, it is a bent function on V_{n-r} (which implies that $n-r$ must be even). Thus the Hamming weight of the truth table of h is $2^{n-r-1} + c2^{\frac{1}{2}(n-r)-1}$, where $c = \pm 1$, and the Hamming weight of the truth table of g^*, a function on V_n, is $2^r(2^{n-r-1} + c2^{\frac{1}{2}(n-r)-1}) = 2^{n-1} + c2^{\frac{1}{2}(n+r)-1}$. Equivalently, the Hamming weight of the truth table of $f(x) \oplus f(x \oplus \alpha)$ is $2^{n-1} + c2^{\frac{1}{2}(n+r)-1}$. Applying Lemma 1 to the function f, we have $\Delta(\alpha) = c2^{\frac{1}{2}(n+r)}$. Thus we have proved that there exists a nonzero vector $\alpha \in V_n$ such that $|\Delta(\alpha)| = 2^{\frac{1}{2}(n+r)}$. As r, the dimension of W, is at least 1, we have $\Delta_f \geq |\Delta(\alpha)| \geq 2^{\frac{1}{2}(n+1)}$. □

We stress that the bound $2^{\frac{1}{2}(n+1)}$ in Theorem 11 is satisfied by any non-bent cubic function, be it balanced or non-balanced. The bound, however, is clearly not satisfied by functions of algebraic degree larger than three. For instance, complementing a single bit in the truth table of a bent function f on V_n results in a non-bent, non-balanced function g with $\Delta_g(\alpha) = \pm 2$ for all nonzero $\alpha \in V_n$ (hence $\Delta_g = 2$, and by Theorem 11, g can *not* be cubic.) Nevertheless, we believe that the lower bound $2^{\frac{1}{2}(n+1)}$ is also satisfied by *balanced* functions of algebraic degree larger than three. This leads to the following conjecture:

Conjecture 1 *Let f be a balanced function on V_n, whose algebraic degree is at least three. Then $\Delta_f \geq 2^{\frac{1}{2}(n+1)}$.*

5 Constructing Balanced Functions with Good GAC

Having discussed various bounds of the two indicators σ_f and Δ_f, we now turn our attention to constructing cryptographic functions that have good GACs or global avalanche characteristics measured in terms of the two indicators. A remarkable property of the functions to be constructed is that they are balanced and do not have a nonzero linear structure.

5.1 On V_{2k}

For $z \in V_{2k}$, write $z = (y, x)$ where $y \in V_k$ and $x \in V_k$. Let ω be a permutation on the set of nonzero vectors in V_k, i.e., $V_k - \{0\} = \{\alpha_1, \ldots, \alpha_{2^k-1}\}$, where α_j is the ith vector in V_k in the ascending alphabetical order. Set

$$f(z) = f(y, x) = \begin{cases} \langle \alpha_{j_0}, x \rangle & \text{if } y = 0 \\ \langle \omega(y), x \rangle & \text{if } y \neq 0 \end{cases} \tag{5}$$

where $\langle \cdot, \cdot \rangle$ denotes the scalar product and α_{j_0} is a fixed nonzero vector in V_k. Equivalently (5) can be expressed as

$$f(z) = (1 \oplus y_1)(1 \oplus y_2) \cdots (1 \oplus y_k) \langle \alpha_{j_0}, x \rangle \oplus [1 \oplus (1 \oplus y_1)(1 \oplus y_2) \cdots (1 \oplus y_k)] \langle \omega(y), x \rangle$$

where $y = (y_1, y_2, \ldots, y_k)$.

First we examine the sequence of the function f. Given a vector $\alpha_i \in V_k$, denote by ℓ_i the sequence of a linear function on V_k defined by $\langle \alpha_i, x \rangle$. By Lemma 2 of [SMZ93], ℓ_i is the ith row of H_k, $i = 0, 1, \ldots, 2^k - 1$. Since α_j corresponds to the binary representation of integer j, w can be regarded as a permutation on $\{1, \ldots, 2^k - 1\}$. In particular, $\omega(\alpha_j) = \alpha_i$ can be equivalently written as $\omega(j) = i$. By Lemma 1 of [SMZ93], the sequence of f defined by (5) is

$$\xi = (\ell_{j_0}, \ell_{\omega(1)}, \ldots, \ell_{\omega(2^k-1)}).$$

We can view ξ in the following way: Concatenating the rows in H_k together, we have $(\ell_0, \ell_1, \ldots, \ell_{2^k-1})$. Replacing ℓ_0 by ℓ_{j_0} gives us $(\ell_{j_0}, \ell_1, \ell_2, \ldots, \ell_{2^k-1})$. Finally reordering $\ell_1, \ldots, \ell_{2^k-1}$ according to the permutation ω results in the sequence ξ. As each ℓ_i, $1 \leq i \leq 2^k - 1$, contains an equal number of ones and minus ones, their concatenation ξ has the same property. Thus we have

Lemma 12. *f defined by (5) is a balanced function on V_{2k}.*

We proceed to the discussion of the absolute indicator Δ_f. Let $\gamma = (\beta, \alpha)$ be a nonzero vector in V_{2k}, where $\beta, \alpha \in V_k$. By definition,

$$\Delta(\gamma) = \sum_{y \in V_k} \sum_{x \in V_k} (-1)^{f(y,x) \oplus f(y \oplus \beta, x \oplus \alpha)}.$$

We discuss $\Delta(\gamma)$ in two separate cases: $\beta \neq 0$ and $\beta = 0$.

First we consider Case 1 where $\beta \neq 0$. In this case $\Delta(\gamma)$ can be written as

$$\Delta(\gamma) = \sum_{y=0,\beta} \sum_{x \in V_k} (-1)^{f(y,x)\oplus f(y\oplus\beta, x\oplus\alpha)} + \sum_{y\neq 0,\beta} \sum_{x \in V_k} (-1)^{f(y,x)\oplus f(y\oplus\beta, x\oplus\alpha)}.$$

When $y = 0$, the exponent $f(y,x) \oplus f(y \oplus \beta, x \oplus \alpha)$ becomes

$$f(0,x) \oplus f(\beta, x\oplus\alpha) = \langle \alpha_{j_0}, x\rangle \oplus \langle \omega(\beta), x\oplus\alpha\rangle = \langle \alpha_{j_0} \oplus \omega(\beta), x\rangle \oplus \langle \omega(\beta), \alpha\rangle \quad (6)$$

and when $y = \beta$, it becomes

$$f(\beta,x) \oplus f(0, x\oplus\alpha) = \langle \omega(\beta), x\rangle \oplus \langle \alpha_{j_0}, x\oplus\alpha\rangle = \langle \alpha_{j_0} \oplus \omega(\beta), x\rangle \oplus \langle \alpha_{j_0}, \alpha\rangle \quad (7)$$

Otherwise when $y \neq 0$ or β, the exponent becomes

$$\begin{aligned} f(y,x) \oplus f(y\oplus\beta, x\oplus\alpha) &= \langle \omega(y), x\rangle \oplus \langle \omega(y\oplus\beta), x\oplus\alpha\rangle && (8)\\ &= \langle \omega(y) \oplus \omega(y\oplus\beta), x\rangle \oplus \langle \omega(y\oplus\beta), \alpha\rangle. && (9)\end{aligned}$$

To find out the value of $\Delta(\gamma)$, we distinguish between the cases of $\omega(\beta) = \alpha_{j_0}$ and $\omega(\beta) \neq \alpha_{j_0}$.

When $\omega(\beta) = \alpha_{j_0}$, (6) becomes a constant $\langle \omega(\beta), \alpha\rangle$, (7) also becomes a constant $\langle \alpha_{j_0}, \alpha\rangle$ and (9) is a nonzero linear function of x for any fixed y and hence balanced. Thus we have

$$\Delta(\gamma) = \sum_{x\in V_k} [(-1)^{\langle \alpha_{j_0}, \alpha\rangle} + (-1)^{\langle \alpha_{j_0}, \alpha\rangle}] = 2 \cdot 2^k \cdot c = 2^{k+1} c$$

where $c = (-1)^{\langle \alpha_{j_0}, \alpha\rangle} = \pm 1$.

On the other hand, when $\omega(\beta) \neq \alpha_{j_0}$, (6), (7) and (9) are all nonzero linear functions and hence balanced. This results in $\Delta(\gamma) = 0$.

Next we consider Case 2 where $\beta = 0$. In this case, it is necessary for α to be nonzero. Thus (5) specializes to

$$\Delta(\gamma) = \sum_{x\in V_k} (-1)^{f(0,x)\oplus f(0,x\oplus\alpha)} + \sum_{y\neq 0} \sum_{x\in V_k} (-1)^{f(y,x)\oplus f(y,x\oplus\alpha)}.$$

When $y = 0$, the exponent $f(y,x) \oplus f(y, x\oplus\alpha)$ becomes

$$f(0,x) \oplus f(0, x\oplus\alpha) = \langle \alpha_{j_0}, x\rangle \oplus \langle \alpha_{j_0}, x\oplus\alpha\rangle = \langle \alpha_{j_0}, \alpha\rangle. \quad (10)$$

Otherwise, when $y \neq 0$, it becomes

$$\begin{aligned} f(y,x) \oplus f(y, x\oplus\alpha) &= \langle \omega(y), x\rangle \oplus \langle \omega(y), x\oplus\alpha\rangle && (11)\\ &= \langle \omega(y), \alpha\rangle. && (12)\end{aligned}$$

Now $\Delta(\gamma)$ can be calculated by

$$\begin{aligned} \Delta(\gamma) &= \sum_{x\in V_k} (-1)^{\langle \alpha_{j_0}, \alpha\rangle} + \sum_{y\neq 0} \sum_{x\in V_k} (-1)^{\langle \omega(y), \alpha\rangle}\\ &= \sum_{x\in V_k} (-1)^{\langle \alpha_{j_0}, \alpha\rangle} + \sum_{u\neq 0} \sum_{x\in V_k} (-1)^{\langle u, \alpha\rangle}\end{aligned}$$

where $u = \omega(y)$. Since ω is a permutation on $V_k - \{0\}$, $u = \omega(y) \neq 0$. Thus we can continue our calculation of $\Delta(\gamma)$:

$$\Delta(\gamma) = \sum_{x \in V_k} (-1)^{\langle \alpha_{j_0}, \alpha \rangle} + \sum_{v \in V_k} \sum_{x \in V_k} (-1)^{\langle v, \alpha \rangle} - \sum_{x \in V_k} (-1)^{\langle 0, \alpha \rangle}.$$

Note that $\langle v, \alpha \rangle$ is a nonzero linear function of v and hence balanced. Thus we have

$$\begin{aligned}
\Delta(\gamma) &= \sum_{x \in V_k} (-1)^{\langle \alpha_{j_0}, \alpha \rangle} - \sum_{x \in V_k} (-1)^{\langle 0, \alpha \rangle} \\
&= \sum_{x \in V_k} [(-1)^{\langle \alpha_{j_0}, \alpha \rangle} - 1] \\
&= \begin{cases} 0 & \text{if } \langle \alpha_{j_0}, \alpha \rangle = 0 \\ 2^{k+1} & \text{if } \langle \alpha_{j_0}, \alpha \rangle = 1 \end{cases}
\end{aligned}$$

Summarizing the above discussions on Cases 1 and 2, we conclude that $|\Delta(\gamma)| \leq 2^{k+1}$ for any nonzero vector $\gamma \in V_{2k}$. This proves the following lemma:

Lemma 13. *Let f be the function on V_{2k} defined by (5). Then $\Delta_f \leq 2^{k+1}$.*

Now we count the vectors with respect to which the function f satisfies the propagation criterion. We have seen in the above discussions that $\Delta(\gamma) = 0$ in two cases: (1) $\Delta(\gamma) = 0$, $\beta \neq 0$, $\omega(\beta) \neq$ or α_{j_0} and α is arbitrary. (2) $\Delta(\gamma) = 0$, $\beta = 0$ and α satisfies $\alpha \neq 0$ and $\langle \alpha_{j_0}, \alpha \rangle = 0$. For the first case there are $(2^k - 2)2^k = 2^{2k} - 2^{k+1}$ choices, while for the second case there are $2^{k-1} - 1$ choices for $\gamma = (\beta, \alpha)$. Hence there exist $2^{2k} - 2^{k+1} + 2^{k-1} - 1$ vectors $\gamma = (\beta, \alpha)$ such that $\Delta(\gamma) = 0$. This proves

Lemma 14. *The function f defined by (5) satisfies the propagation criterion with respect to $2^{2k} - 2^{k+1} + 2^{k-1} - 1$ vectors in V_{2k}.*

Next we examine the sum-of-squares avalanche characteristic of the function f. Recall that the sequence of f is

$$\xi = (\ell_{j_0}, \ell_{\omega(1)}, \ell_{\omega(2)}, \ldots, \ell_{\omega(2^k-1)})$$

where ℓ_i is the sequence of a linear function on V_k defined by $\langle \alpha_i, x \rangle$.

Let L be a row of H_{2k}. By Lemma 2 of [SMZ93], L is a linear sequence of length 2^{2k}. Since $H_{2k} = H_k \times H_k$, L can be rewritten as $L = \ell_p \times \ell_q$ for some p and q satisfying $0 \leq p, q, \leq 2^k - 1$. Write $\ell_p = (c_0, c_1, \ldots, c_{2^k-1})$. Then we have $L = (c_0\ell_q, c_1\ell_q, \ldots, c_{2^k-1}\ell_q)$.

As H_k is a Hadamard matrix, $\langle \ell_i, \ell_j \rangle = 0$ when $j \neq i$. Also note that as ω is a permutation on $V_k - \{0\}$, $\omega(\alpha_j)$ runs through the nonzero vectors in V_k while j runs through $1, 2, \ldots, 2^k - 1$. So there exists a unique j^* such that $\omega(\alpha_{j^*}) = \alpha_{j_0}$. Thus we have

$$\langle \xi, L \rangle = \begin{cases} (c_0 + c_{j^*})\langle \ell_{j_0}, \ell_{j_0} \rangle) = (c_0 + c_{j^*})2^k & \text{if } \alpha_q = \alpha_{j_0} \\ \pm 2^k & \text{if } \alpha_q \neq \alpha_{j_0}, 0 \\ 0 & \text{if } q = 0 \end{cases}$$

Here $c_0 = 1$ and $c_{j^*} = \pm 1$.

There exist 2^{k-1} linear sequences ℓ_p such that $c_1 = 1$. Hence there exist 2^{k-1} linear sequences L such that $L = \ell_p \times \ell_q$ with $c_{j^*} = 1$ and $\alpha_q = \alpha_{j_0}$. For these sequences we have $\langle \xi, L \rangle = 2^{k+1}$.

For $c_{j^*} = -1$, we have $\langle \xi, L \rangle = 0$. It is easy to see that there exits $2^k \cdot (2^k - 2)$ linear sequences L such that $L = \ell_p \times \ell_q$ with $\alpha_q \neq 0$ or α_{j_0}. With these sequences we have $\langle \xi, L \rangle = \pm 2^k$.

In summary, we have

$$\begin{aligned}\sigma_f &= 2^{-2k} \sum_{s=0}^{2^{2k}-1} \langle \xi, L_s \rangle^4 = 2^{k-1} \cdot 2^{4(k+1)} + 2^k \cdot (2^k - 2) \cdot 2^{4k} \\ &= 2^{4k} + 2^{3k+3} - 2^{3k+1}.\end{aligned}$$

This proves the following conclusion:

Lemma 15. *The sum-of-squares avalanche characteristic of f, a function on V_{2k} defined by (5), satisfies $\sigma_f = 2^{4k} + 2^{3k+3} - 2^{3k+1}$.*

Recall that for a function on V_{2k}, its sum-of-squares indicator is bounded between 2^{4k} and 2^{6k}, with the lower bound 2^{4k} being achieved only when the function is bent. We conjecture that the function f defined by (5) with $\sigma_f = 2^{4k} + 2^{3k+3} - 2^{3k+1}$ achieves nearly optimal sum-of-squares avalanche characteristic of balanced functions on V_{2k}.

From the above discussions, it becomes clear that $|\langle \xi, L_s \rangle| \leq 2^{k+1}$ for any L_s that is a linear sequence of length 2^{2k}. By Lemma 3 of [SMZ93], the nonlinearity of f satisfies $N_f \geq 2^{2k-1} - 2^k$.

Putting the above discussions together, we have

Theorem 16. *Let f be the function on V_{2k} defined by (5). Then*

(i) f is balanced,
(ii) the nonlinearity of f satisfies $N_f \geq 2^{2k-1} - 2^{2k}$,
(iii) f satisfies the propagation criterion with respect to $2^{2k} - 2^{k+1} + 2^{k-1} - 1$ nonzero vectors,
(iv) the sum-of-squares avalanche characteristic of f satisfies $\sigma_f = 2^{4k} + 2^{3k+3} - 2^{3k+1}$,
(v) the absolute avalanche characteristic of f satisfies $\Delta_f \leq 2^{k+1}$.

A final remark is about the strict avalanche characteristic of the function f. The number of vectors with respect to which f satisfies the propagation criterion is $2^{2k} - 2^{k+1} + 2^{k-1} - 1$ which is larger than 2^{2k-1}. Hence these vectors contain at least $2k$ linear independent ones. Let A be the matrix with the $2k$ linear independent vectors as its rows. Then A is nonsingular and of order $2k$. By Theorem 3 of [SZZ94a], $f(zA)$ satisfies the SAC. All the properties described in Theorem 16 are affected by the nonsingular transform A.

5.2 On V_{2k+1}

To construct functions on V_{2k+1} with good avalanche characteristics, we need a permutation $m(u)$ on V_k with a special property that $u \oplus m(u)$ is also a permutation on V_k, namely, $u \oplus m(u)$ runs through the vectors in V_k while u runs V_k. As is shown in the following, such functions can be obtained from maximal length shift register sequences or m-sequences [Gol82]. In a different context, Nyberg showed that m-sequences are useful in constructing cryptographic substitution boxes with the maximum nonlinearity [Nyb91]. (It should be noted, however, that such substitution boxes have been identified to be prone to the differential cryptanalytic attack [BS93, BKPS93].)

Let $(s_0, s_1, \ldots, s_{2^k-2})$ be a m-sequence of length $2^k - 1$, where each s_i is from GF(2). A k-gram is one of the $2^k - 1$ subsequences of length k of the form

$$r_t = (s_{t \bmod (2^k-1)}, s_{(t+1) \bmod (2^k-1)}, \ldots, s_{(t+k-1) \bmod (2^k-1)}),$$

where $t = 0, 1, 2, \ldots, 2^k - 2$. Note that a k-gram can also be viewed as a vector in V_k. Thus we have an ordered list of 2^k-1 nonzero vectors in V_k $(r_0, r_1, \ldots, r_{2^k-2})$. Adding to the beginning of the list the zero vector 0 in V_k results in an extended ordered list $(0, r_0, r_1, \ldots, r_{2^k-2})$. The extended list contains all vectors in V_k. Rotating cyclically to the left the nonzero vectors in the list by one position we get $(0, r_1, r_2, \ldots, r_{2^k-2}, r_0)$. Now we have two ordered vector lists:

$$(0, r_0, r_1, \ldots, r_{2^k-2})$$

and

$$(0, r_1, r_2, \ldots, r_{2^k-2}, r_0).$$

Define a mapping $m(u)$ that maps the ith vector in the first list to the corresponding vector in the second list, namely, 0 to 0, r_0 to r_1, r_1 to r_2, …, and r_{2^k-2} to r_0. By properties of m-sequences, the mapping $m(u)$ is a permutation with the special property that $u \oplus m(u)$ is also a permutation.

Now write $W_1 = \{(0, u) | u \in V_k\}$, $W_2 = \{(1, u) | u \in V_k\}$, where $0, 1 \in GF(2)$. Obviously, $V_{k+1} = W_1 \cup W_2$. For any $y \in V_{k+1}$, write $y = (y_1, u)$ where $y_1 \in GF(2)$ and $u \in V_k$. For $z \in V_{2k+1}$, write $z = (y, x)$ where $y \in V_{k+1}$ and $x \in V_k$.

Then the following is our construction for the case of V_{2k+1}:

$$f(z) = f(y, x) = \begin{cases} 1 \oplus \langle u, x \rangle \text{ if } y \in W_1 \\ \langle m(u), x \rangle \text{ if } y \in W_2 \end{cases} \tag{13}$$

where $m(u)$ is a permutation on V_k with the property that $u \oplus m(u)$ is also a permutation on V_k. Note that (13) can be equivalently written as $f(z) = (1 \oplus y_1)\langle u, x \rangle \oplus y_1 \langle m(u), x \rangle$.

Since α_j is the binary representation of integer j, m can be regarded as a permutation on $\{0, 1, \ldots, 2^k - 1\}$ and hence $\omega(\alpha_j) = \alpha_i$ can be equivalently written as $\omega(j) = i$. Let ξ be the sequence of f. Then the first half of ξ is specified by $1 \oplus \langle u, x \rangle$, while the second half by $\langle m(u), x \rangle$. To be more precise, the first half is (the concatenation of) $-\ell_0, -\ell_1, \ldots, -\ell_{2^k-1}$, where each ℓ_i is the ith row in H_k and $-\ell_i$ means multiplying each component of ℓ_i by -1. And the second half is $\ell_{m(0)}, \ell_{m(1)}, \ldots, \ell_{m(2^k-1)}$, a reordered version of $\ell_0, \ell_1, \ldots, \ell_{2^k-1}$ according to the permutation m on V_k. Thus the sequence of f takes the form of

$$\xi = (-\ell_0, -\ell_1, \ldots, -\ell_{2^k-1}, \ell_{m(0)}, \ell_{m(1)}, \ldots, \ell_{m(2^k-1)}).$$

Obviously ξ contains an equal number of ones and minus ones. Hence f is a balanced function on V_{2k+1}. Using very similar arguments to those for the function f on V_{2k} defined by (5) with attention to the fact that both $m(u)$ and $u \oplus m(u)$ are permutations, we can find out other properties of the function f on V_{2k+1} defined by (13). In particular, we have

Theorem 17. *Let f be the function on V_{2k+1} defined in (13). Then*

(i) f is balanced,
(ii) the nonlinearity of f satisfies $N_f \geq 2^{2k} - 2^k$,
(iii) f satisfies the propagation criterion with respect to $2^{2k} - 1$ nonzero vectors,
(iv) the sum-of-squares avalanche characteristic of f satisfies $\sigma_f = 2^{4k+3}$,
(v) the absolute avalanche characteristic of f satisfies $\Delta_f \leq 2^{k+1}$.

An important property of f is that Δ_f matches the lower bound we conjectured at the end of Section 4. Comparing $\sigma_f = 2^{4k+3} = 2 \cdot 2^{4k+2}$ with 2^{4k+2} and 2^{6k+3}, the upper and upper bounds respectively (see also Theorem 6), we can see that the sum-of-squares avalanche characteristic of the function is also extremely good. Again we conjecture that it achieves the lowest possible value for balanced functions on V_{2k+1}.

It should be noted that since the total number of nonzero vectors with respect to which f satisfies the propagation criterion is $2^{2k} - 1$, there are at most $2k$ linearly independent ones among the vectors. Therefore, unlike the case on V_{2k}, the function f on V_{2k+1} constructed by (13) can not be transformed into an SAC-fulfilling one.

Acknowledgments

The authors would like to thank the anonymous referees for their comments that have helped in improving the presentation of this paper. This work was supported in part by the Australian Research Council (ARC) under the reference number A49232172 and by the Australian Telecommunications and Electronics Research Board (ATERB) under the reference numbers C010/058 and N069/412.

References

[AT90] C. M. Adams and S. E. Tavares. Generating and counting binary bent sequences. *IEEE Transactions on Information Theory*, IT-36 No. 5:1170–1173, 1990.

[Bea84] K. G. Beauchamp. *Applications of Walsh and Related Functions with an Introduction to Sequency Functions.* Microelectronics and Signal Processing. Academic Press, London, New York, Tokyo, 1984.

[BKPS93] L. Brown, M. Kwan, J. Pieprzyk, and J. Seberry. Improving resistance to differential cryptanalysis and the redesign of LOKI. In *Advances in Cryptology - ASIACRYPT'91*, volume 739, Lecture Notes in Computer Science, pages 36–50. Springer-Verlag, Berlin, Heidelberg, New York, 1993.

[BS93] E. Biham and A. Shamir. *Differential Cryptanalysis of the Data Encryption Standard.* Springer-Verlag, New York, Heidelberg, Tokyo, 1993.

[Dil72] J. F. Dillon. A survey of bent functions. *The NSA Technical Journal*, pages 191–215, 1972. (unclassified).

[DT93] J. Detombe and S. Tavares. Constructing large cryptographically strong S-boxes. In *Advances in Cryptology - AUSCRYPT'92*, volume 718, Lecture Notes in Computer Science, pages 165–181. Springer-Verlag, Berlin, Heidelberg, New York, 1993.

[For89] R. Forré. The strict avalanche criterion: Special properties of boolean functions and extended definition. In *Advances in Cryptology - CRYPTO'88*, volume 403, Lecture Notes in Computer Science, pages 450–468. Springer-Verlag, Berlin, Heidelberg, New York, 1989.

[Gol82] S. W. Golomb. *Shift Register Sequences.* Laguna Hills, CA: Aegean Park, 1982.

[Llo90] S. Lloyd. Counting functions satisfying a higher order strict avalanche criterion. In *Advances in Cryptology - EUROCRYPT'89*, volume 434, Lecture Notes in Computer Science, pages 64–74. Springer-Verlag, Berlin, Heidelberg, New York, 1990.

[Llo92] S. Lloyd. Counting binary functions with certain cryptographic properties. *Journal of Cryptology*, 5(2):107–132, 1992.

[Mit90] C. Mitchell. Enumerating boolean functions of cryptographic significance. *Journal of Cryptology*, 2(3):155–170, 1990.

[MS77] F. J. MacWilliams and N. J. A. Sloane. *The Theory of Error-Correcting Codes.* North-Holland, Amsterdam, New York, Oxford, 1977.

[Nyb91] K. Nyberg. Perfect nonlinear S-boxes. In *Advances in Cryptology - EUROCRYPT'91*, volume 547, Lecture Notes in Computer Science, pages 378–386. Springer-Verlag, Berlin, Heidelberg, New York, 1991.

[Nyb93] K. Nyberg. On the construction of highly nonlinear permutations. In *Advances in Cryptology - EUROCRYPT'92*, volume 658, Lecture Notes in Computer Science, pages 92–98. Springer-Verlag, Berlin, Heidelberg, New York, 1993.

[PGV91] B. Preneel, R. Govaerts, and J. Vandewalle. Boolean functions satisfying higher order propagation criteria. In *Advances in Cryptology - EUROCRYPT'91*, volume 547, Lecture Notes in Computer Science, pages 141–152. Springer-Verlag, Berlin, Heidelberg, New York, 1991.

[PLL+91] B. Preneel, W. V. Leekwijck, L. V. Linden, R. Govaerts, and J. Vandewalle. Propagation characteristics of boolean functions. In *Advances in Cryptology - EUROCRYPT'90*, volume 437, Lecture Notes in Computer Science, pages 155–165. Springer-Verlag, Berlin, Heidelberg, New York, 1991.

[Rot76] O. S. Rothaus. On "bent" functions. *Journal of Combinatorial Theory*, Ser. A, 20:300–305, 1976.

[SMZ93] J. Seberry, X. M., and Y. Zhang. Highly nonlinear 0-1 balanced functions satisfying strict avalanche criterion. In *Advances in Cryptology - AUSCRYPT'92*, volume 718, Lecture Notes in Computer Science, pages 145–155. Springer-Verlag, Berlin, Heidelberg, New York, 1993.

[SZZ94a] J. Seberry, X. M. Zhang, and Y. Zheng. Improving the strict avalanche characteristics of cryptographic functions. *Information Processing Letters*, 50:37–41, 1994.

[SZZ94b] J. Seberry, X. M. Zhang, and Y. Zheng. Nonlinearly balanced boolean functions and their propagation characteristics. In *Advances in Cryptology - CRYPTO'93*, volume 773, Lecture Notes in Computer Science, pages 49–60. Springer-Verlag, Berlin, Heidelberg, New York, 1994.

[SZZ94c] J. Seberry, X. M. Zhang, and Y. Zheng. Relationships among nonlinearity criteria. Presented at *EUROCRYPT'94*, 1994.

[SZZ94d] J. Seberry, X. M. Zhang, and Y. Zheng. Structures of cryptographic functions with strong avalanche characteristics. Asiacrypt'94, December 1994.

[SZZ95] J. Seberry, X. M. Zhang, and Y. Zheng. Nonlinearity and propagation characteristics of balanced boolean functions. To appear in *Information and Computation*, 1995.

[Web85] A. F. Webster. Plaintext/ciphertext bit dependencies in cryptographic system. Master's Thesis, Department of Electrical Engineering, Queen's University, Ontario, Cannada, 1985.

[WT86] A. F. Webster and S. E. Tavares. On the design of S-boxes. In *Advances in Cryptology - CRYPTO'85*, volume 219, Lecture Notes in Computer Science, pages 523–534. Springer-Verlag, Berlin, Heidelberg, New York, 1986.

[YH89] R. Yarlagadda and J. E. Hershey. Analysis and synthesis of bent sequences. *IEE Proceedings (Part E)*, 136:112–123, 1989.