Improving the Strict Avalanche Characteristics of Cryptographic Functions *

Jennifer Seberry
Xian-Mo Zhang
Yuliang Zheng

The Centre for Computer Security Research
Department of Computer Science
The University of Wollongong
Wollongong, NSW 2522, AUSTRALIA
E-mail: {jennie,xianmo,yuliang}@cs.uow.edu.au

November 2, 1993

Abstract

This letter presents a simple yet effective method for transforming Boolean functions that do not satisfy the strict avalanche criterion (SAC) into ones that satisfy the criterion. Such a method has a wide range of applications in designing cryptographically strong functions, including substitution boxes (S-boxes) employed by common key block encryption algorithms.

Key Words

cryptography, security in digital systems, strict avalanche criterion (SAC), substitution boxes (S-boxes).

1 The Strict Avalanche Criterion

A (Boolean) function on V_n, where V_n denotes the vector space of n-tuples of elements from $GF(2)$, is said to satisfy the strict avalanche criterion (SAC) if complementing a single bit in its input results in the output of the function being complemented half the time over all the input vectors. The SAC is a very important requirement for cryptographic functions. The formal definition for the SAC seems to appear first in the open literature in 1985 [Web85, WT86]:

*Preprint No. 93-9.

Definition 1 *Let f be a function on V_n. f is said to satisfy the SAC if $f(x) \oplus f(x \oplus \alpha)$ assumes the values zero and one an equal number of times, or simply, $f(x) \oplus f(x \oplus \alpha)$ is balanced, for every $\alpha \in V_n$ with $W(\alpha) = 1$, where $x = (x_1, \ldots, x_n)$ and $W(\alpha)$ denotes the number of ones in (or the Hamming weight of) the vector α.*

A closely related concept is propagation criterion [AT90, PLL+91, PGV91]:

Definition 2 *Let f be a function on V_n. We say that f satisfies*

1. *the* propagation criterion with respect to a non-zero vector α in V_n *if $f(x) \oplus f(x \oplus \alpha)$ is a balanced function.*

2. *the* propagation criterion of degree k *if it satisfies the propagation criterion with respect to all $\alpha \in V_n$ with $1 \leqq W(\alpha) \leqq k$.*

As the SAC is equivalent to the propagation criterion of degree 1, the latter can be viewed as a generalization of the former. In another direction, the SAC has been generalized to higher order SAC. This work is represented by [For89]. In this letter we shall not pursue further the developments in these two directions. Instead we shall focus our attention on how to transform functions which do not satisfy the SAC into ones that satisfy the criterion.

2 Single Functions

First we introduce the following basic theorem.

Theorem 1 *Let f be a function on V_n, and A be a nondegenerate matrix of order n whose entries are from $GF(2)$. Suppose that $f(x) \oplus f(x \oplus \gamma_i)$ is balanced for each row γ_i of A, where $i = 1, \ldots, n$ and $x = (x_1, \ldots, x_n)$. Namely f satisfies the propagation criterion with respect to all rows of A. Then $\psi(x) = f(xA)$ satisfies the SAC.*

Proof. Let δ_i be a vector in V_n whose entries, *except the ith*, are all zero. Note that $W(\delta_i) = 1$ and $\delta_i A = \gamma_i$, $i = 1, \ldots, n$. Then we have $\psi(x) \oplus \psi(x \oplus \delta_i) = f(xA) \oplus f((x \oplus \delta_i)A) = f(u) \oplus f(u \oplus \gamma_i)$, where $u = xA$. Since A is nondegenerate, u runs through V_n while x does. By assumption, $f(u) \oplus f(u \oplus \gamma_i)$ runs through the values zero and one an equal number of times while u runs through V_n. Consequently $\psi(x) \oplus \psi(x \oplus \delta_i)$ runs through the values zero and one an equal number of times while x runs through V_n. That is, $\psi(x)$ satisfies the SAC. □

Note that the algebraic degree, the nonlinearity and the balancedness of a function is unchanged under a nondegenerate linear transformation of coordinates [MS90, SZZ93a]. In addition the number of nonzero vectors with respect to which the function satisfies the propagation criterion is also invariant under the transformation [SZZ93a]. In the case of S-boxes (tuples of functions), the profile of its difference distribution table, which measures the strength against the differential cryptanalysis [BS91, BS93],

also remains invariant under such a transformation [SZZ93c]. Thus Theorem 1 provides us with a very useful tool to improve the strict avalanche characteristics of cryptographic functions. In the following we consider two applications of the theorem.

Application 1 Our first application shows that a SAC-fulfilling function on a higher dimensional space can be easily obtained from a SAC-fulfilling function on a lower dimensional space.

Let $g(y_1, \ldots, y_s)$ be a function on V_s that satisfies the SAC. Adding t dummy-coordinates $x_1, \ldots, x_t$ into g, we obtain a function f on V_{s+t}, namely,

$$f(y_1, \ldots, y_s, x_1, \ldots, x_t) = g(y_1, \ldots, y_s)$$

The t newly added coordinates have no influence on the output of f. Hence f does not satisfy the SAC.

Let A be a nondegenerate matrix of order $s+t$. Assume that each row γ_i of A can be written as $\gamma_i = (\beta_i, \alpha_i)$, where $W(\beta_i) = 1$, $\beta_i \in V_s$ and $\alpha_i \in V_t$. Let $x = (x_1, \ldots, x_t)$, $y = (y_1, \ldots, y_s)$ and $z = (y, x)$. Then we have $f(z) \oplus f(z \oplus \gamma_i) = g(y) \oplus g(y \oplus \beta_i)$. This shows that $f(z) \oplus f(z \oplus \gamma_i)$ is balanced for γ_i, $i = 1, \ldots, s+t$. By Theorem 1, $\psi(z) = f(zA)$ satisfies the SAC.

An example of the matrices that satisfy the requirements is as follows:

$$A = \begin{bmatrix} I_s & 0_{s\times t} \\ Q_{t\times s} & I_t \end{bmatrix} \tag{1}$$

where I denotes the identity matrix, 0 denotes the zero matrix, and Q is a matrix that contains precisely an one in each of its rows.

ψ and f have the same nonlinearity, algebraic degree, and balancedness as $f(z)$ does. The two functions also have the same number of nonzero vectors with respect which they satisfy the propagation criterion. The net gain of ψ over f is the SAC. However, it should be pointed out that for this particular example, the resulting function ψ does not satisfy the propagation criterion with respect to vectors whose entries are zeros except in the first and the $(s+j)$th, where $1 \leqq j \leqq t$. This property might be undesirable in certain applications. We can get around the problem by selecting a nondegenerate matrix A that introduces more inter-dependencies among the coordinates. Here is such a matrix:

$$\begin{aligned} A &= \begin{bmatrix} I_s & 0_{s\times t} \\ Q_{t\times s} & I_t \end{bmatrix} \begin{bmatrix} I_s & B_{s\times t} \\ 0_{t\times s} & I_t \end{bmatrix} \\ &= \begin{bmatrix} I_s & B_{s\times t} \\ Q_{t\times s} & Q_{t\times s}B_{s\times t} \oplus I_t \end{bmatrix} \end{aligned} \tag{2}$$

where B is an arbitrary matrix whose entries are taken from $GF(2)$.

Application 2 Let g_0 and g_1 be functions on V_t. Then $f(y_1, x_1, \ldots, x_n) = (1 \oplus y_1)g_0(x_1, \ldots, x_t) \oplus y_1 g_1(x_1, \ldots, x_t)$ is a function on V_{t+1}. The truth table of f can be

obtained by *concatenating* the truth tables of g_0 and g_1. For this reason, we say that f is the concatenation of g_0 and g_1. Similarly, we can define the concatenation of 2^s functions on V_t. The result is a function on V_{t+s}. To simplify the representation of the concatenation of 2^s functions, we introduce the following notation.

For each vector $\delta = (i_1, \ldots, i_s) \in V_s$, we define a function D_δ on V_s by

$$D_\delta(y) = (y_1 \oplus \bar{i_1}) \ldots (y_s \oplus \bar{i_s})$$

where $y = (y_1, \ldots, y_s)$ and $\bar{i}$ denotes the binary complement of i, namely, $\bar{i} = 1 \oplus i$. For instance, when $s = 2$ we have $D_{0,0}(y_1, y_2) = (y_1 \oplus 1)(y_2 \oplus 1)$, and when $s = 3$ we have $D_{1,0,1}(y_1, y_2, y_3) = y_1(y_2 \oplus 1)y_3$. Note that $D_\delta(y) = 1$ if and only if $y = \delta$.

Using this notation, the concatenation of 2^s functions on V_t, $g_{0,\ldots,0}$, $g_{0,\ldots,1}$, $\ldots$, $g_{1,\ldots,1}$, can be written as

$$f(y, x) = \bigoplus_{\delta \in V_s} [D_\delta(y) g_\delta(x)] \tag{3}$$

where $x = (x_1, \ldots, x_t)$. Note that each g_δ is a function on V_t and is indexed by a vector in V_s. Of particular interest is the concatenation of linear functions on V_t. In Theorems 4 and 5 of [SZZ93b], the following result is proved:

Lemma 1 *When $t \geqq s$ and all g_δ, $\delta \in V_s$, are distinct nonzero linear functions on V_t, the function f constructed by (3) is highly nonlinear and balanced. In addition, f satisfies the propagation criterion with respect to all $\gamma = (\beta, \alpha)$, where β is a nonzero vector in V_s and α is an arbitrary vector in V_t.*

Let A be a nondegenerate matrix of order $s + t$. Suppose that the ith row γ_i of A can be written as $\gamma_i = (\beta_i, \alpha_i)$ with $\beta_i \neq 0$, where $\beta_i \in V_s$ and $\alpha_i \in V_t$. From Lemma 1 we know that f satisfies the propagation criterion with respect to all rows of A. By Theorem 1, $\psi(z) = f(zA)$ satisfies the SAC. Note that the matrix A defined by (1) or (2) satisfies the requirements.

These discussions also hold for the more general case where f is defined by

$$f(y, x) = \bigoplus_{\delta \in V_s} [D_\delta(y) g_\delta(x)] \oplus r(y)$$

where r is an arbitrary function on V_s.

3 A Set of Functions

In computer security practice, such as the design of S-boxes, we often consider a set of functions. It is desirable that all component functions in a set simultaneously satisfy the SAC. From Theorem 1 we can see that given a set of functions on V_n, $\{f_1, \ldots, f_m\}$, if A is a nondegenerate matrix of order n such that $f_i(x) \oplus f_i(x \oplus \gamma_j)$ is balanced for every function f_i and every row γ_j in A, then $g_1(x) = f_1(xA)$, $\ldots$, $g_m(x) = f_m(xA)$ all satisfy the SAC. The following theorem gives a sufficient condition for the existence of such a nondegenerate matrix.

Theorem 2 *Let f_1, ..., f_m be functions on V_n. Denote by B the set of nonzero vectors γ in V_n such that $f_j(x) \oplus f_j(x \oplus \gamma)$ is* not *balanced for some $1 \leqq j \leqq m$, and by $|B|$ the number of vectors in B. If $|B| < 2^{n-1}$, then there exists a nondegenerate matrix A of order n with entries from $GF(2)$ such that each $\psi_j(x) = f_j(xA)$ satisfies the SAC.*

Proof. We show how to construct a nondegenerate matrix A of order n, under the condition that $|B| < 2^{n-1}$. Denote by $S_{\alpha_1,\ldots,\alpha_k}$ the set of vectors consisting of all the linear combinations of vectors $\alpha_1, \ldots, \alpha_k$.

The first row of A, γ_1, is selected from V_n excluding those in B and the zero vector, i.e., from the vector set $V_n - B - S_0$. There are $2^n - |B| - 2^0$ different choices for γ_1. The second row of A, γ_2, is selected from the vector set $V_n - B - S_{\gamma_1}$. This guarantees that γ_2 is linearly independent of γ_1. We have $2^n - |B| - 2^1$ different choices for γ_2.

In general, once the first $k-1$ linearly independent rows γ_1, ..., γ_{k-1} of A are selected, the kth row γ_k, $k \leqq n$, will be selected from the vector set $V_n - B - S_{\gamma_1,\ldots,\gamma_{k-1}}$. This process ensures that γ_1, ..., γ_k are all linearly independent.

The number of choices for the last row γ_n is $2^n - |B| - 2^{n-1} = 2^{n-1} - |B| > 0$. Therefore, we can always find a nondegenerate matrix A such that $f_i(x) \oplus f_i(x \oplus \gamma_j)$ is balanced for every $1 \leqq i \leqq m$ and $1 \leqq j \leqq n$. By Theorem 1, $\psi_1(x) = f_1(xA)$, ..., $\psi_m(x) = f_m(xA)$ all satisfy the SAC. □

As is discussed in Section 2, the transformation technique does not affect the nonlinearity, the algebraic degree and the balancedness of the component functions of an S-box. The profile of the difference distribution table of the S-box, and the number of nonzero vectors with respect to which the component functions satisfy the propagation criterion are not altered either. This technique has been successfully applied in [SZZ93c] to design S-boxes that possess many desirable cryptographic properties, which include the high nonlinearity, the SAC, the balancedness and the robustness against differential cryptanalysis. As is shown below, the technique can also be applied to other approaches to the construction of S-boxes.

Application 3 S-boxes based on permutation polynomials are studied in [Pie91, NK92, Nyb92, Nyb93, BD93]. In general, these permutations do not satisfy the SAC. Employing the transformation technique discussed above, the strict avalanche characteristics of these permutations can be improved. In particular, with the permutations constructed by the "cubing" method [Pie91, NK92, Nyb93], each component function f_j satisfies the propagation criterion with respect to all but one nonzero vectors in V_n, where $n \geqq 3$ is odd. Note that $|B| \leqq n$. A component function fails to satisfy the SAC if the Hamming weight of the nonzero vector with respect to which the propagation criterion is not satisfied is one. If this is the case, by Theorem 2 we can use a nondegenerate matrix to transform the component functions of such a permutation so that they all satisfy the SAC.

4 A Final Remark

In [SZZ93a], we have constructed highly nonlinear balanced functions on V_{2k+1} that satisfy the propagation criterion of degree $2k$, and highly nonlinear balanced functions on V_{2k} that satisfy the propagation criterion of degree $\frac{4}{3}k$. A transformation technique similar to that presented in this letter has played an important role in the constructions.

Acknowledgments

The authors would like to thank the anonymous referee for his or her helpful comments. The first author was supported in part by the Australian Research Council under the reference numbers A49130102, A9030136, A49131885 and A49232172, the second author by A49130102, and the third author by A49232172.

References

[AT90] C. M. Adams and S. E. Tavares. The use of bent sequences to achieve higher-order strict avalanche criterion. Technical Report, TR 90-013, Department of Electrical Engineering, Queen's University, 1990.

[BD93] T. Beth and C. Ding. On permutations against differential cryptanalysis. In *Advances in Cryptology - EUROCRYPT'93*. Springer-Verlag, Berlin, Heidelberg, New York, 1993. to appear.

[BS91] E. Biham and A. Shamir. Differential cryptanalysis of DES-like cryptosystems. *Journal of Cryptology*, Vol. 4, No. 1:3–72, 1991.

[BS93] E. Biham and A. Shamir. *Differential Cryptanalysis of the Data Encryption Standard*. Springer-Verlag, New York, Berlin, Heidelberg, London, Paris, Tokyo, Hong Kong, Barcelona, Budapest, 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.

[MS90] W. Meier and O. Staffelbach. Nonlinearity criteria for cryptographic functions. In *Advances in Cryptology - EUROCRYPT'89*, volume 434, Lecture Notes in Computer Science, pages 549–562. Springer-Verlag, Berlin, Heidelberg, New York, 1990.

[NK92] K. Nyberg and L. R. Knudsen. Provable security against differential cryptanalysis. In *Advances in Cryptology - CRYPTO'92*, volume Lecture Notes in Computer Science. Springer-Verlag, Berlin, Heidelberg, New York, 1992. to appear.

[Nyb92] K. Nyberg. On the construction of highly nonlinear permutations. In *Advances in Cryptology - EUROCRYPT'92*. Springer-Verlag, Berlin, Heidelberg, New York, 1992. to appear.

[Nyb93] K. Nyberg. Differentially uniform mappings for cryptography. In *Advances in Cryptology - EUROCRYPT'93*. Springer-Verlag, Berlin, Heidelberg, New York, 1993. to appear.

[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.

[Pie91] J. Pieprzyk. Bent permutations. In *Proceeding of the International Conference on Finite Fields, Coding Theory, and Advances in Communications and Computing*, Las Vegas, 1991.

[PLL+91] B. Preneel, W. V. Leekwick, 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.

[SZZ93a] J. Seberry, X. M. Zhang, and Y. Zheng. Nonlinearly balanced boolean functions and their propagation characteristics. In *Advances in Cryptology - CRYPTO'93*. Springer-Verlag, Berlin, Heidelberg, New York, 1993. to appear.

[SZZ93b] J. Seberry, X. M. Zhang, and Y. Zheng. On constructions and nonlinearity of correlation immune functions. In *Advances in Cryptology - EUROCRYPT'93*. Springer-Verlag, Berlin, Heidelberg, New York, 1993. to appear.

[SZZ93c] J. Seberry, X. M. Zhang, and Y. Zheng. Systematic generation of cryptographically robust S-boxes. In *Proceedings of the First ACM Conference on Computer and Communications Security*, November 1993. to appear.

[Web85] A. F. Webster. *Plaintext/Ciphertext Bit Dependencies in Cryptographic System*. Master's Thesis, Department of Electrical Engineering, Queen's University, 1985.

[WT86] A. F. Webster and S. E. Tavares. On the designs 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.