CRYPTOGRAPHIC PROPERTIES OF BOOLEAN FUNCTIONS

Recent Results on Resilient Functions

D. R. Stinson
Computer Science and Engineering Department
and Center for Communication and Information Science
University of Nebraska
Lincoln, NE 68588-0115, U.S.A.
stinson@bibd.unl.edu

Abstract

Resilient and correlation-immune functions were introduced in the mid-1980's, and have been studied by several researchers. In this paper, we survey the progress that has been made concerning three conjectures on resilient functions.

1 Introduction

The concept of resilient functions was introduced independently in the two papers Chor *et al* [4] and Bennett, Brassard and Robert [1]. Here is the definition. Let $n \geq m \geq 1$ be integers and suppose

$$f : \{0,1\}^n \rightarrow \{0,1\}^m.$$

We will think of f as being a function that accepts n input bits and produces m output bits. Let $t \leq n$ be an integer. Suppose $(x_1, \ldots, x_n) \in \{0,1\}^n$, where the values of t arbitrary input bits are fixed by an opponent, and the remaining $n-t$ input bits are chosen independently at random. Then f is said to be $t-$*resilient* provided that every possible output $m-$tuple is equally likely to occur. More formally, the property can be stated as follows: For every $t-$subset $\{i_1, \ldots, i_t\} \subseteq \{1, \ldots, n\}$, for every choice of $z_j \in \{0,1\}$ $(1 \leq j \leq t)$, and for every $(y_1, \ldots, y_m) \in \{0,1\}^m$, we have

$$p(f(x_1, \ldots, x_n) = (y_1, \ldots, y_m) | x_{i_j} = z_j, 1 \leq j \leq t) = \frac{1}{2^m}.$$

We will refer to such a function f as an $(n, m, t)-$RF.

A closely related concept is that of a correlation-immune function, which was defined by Siegenthaler in [17] and further studied in [16, 11, 3]. A balanced correlation-immune function is the same thing as an $(n, 1, t)-$RF.

Here are some examples of resilient functions from [4] (all addition is in $\mathbf{Z}_2$):

(1) An $(n, 1, n-1)$–RF: Define $f(x_1, \ldots, x_n) = x_1 + \ldots + x_n$.

(2) An $(n, n-1, 1)$–RF: Define $f(x_1, \ldots, x_n) = (x_1 + x_2, x_2 + x_3, \ldots, x_{n-1} + x_n)$.

(3) A $(3h, 2, 2h-1)$–RF: Define

$$f(x_1, \ldots, x_{3h}) = (x_1 + \ldots + x_{2h}, x_{h+1} + \ldots + x_{3h}).$$

Some applications of resilient functions are mentioned in [1] and [4]. One application concerns the generation of shared random strings in the presence of faulty processors. Another involves renewing a partially leaked cryptographic key (one setting in which this would be relevant is quantum cryptography [2]). Correlation-immune functions are used in stream ciphers as combining functions for running-key generators that are resistant to a correlation attack (see, for example, Rueppel [16]).

Interesting results on resilient functions can be found in several papers, e.g. [1, 4, 7, 18, 10, 19]. The basic problem is to maximize t given m and n; or equivalently, to maximize m given n and t. In fact, all three of the examples above are optimal. It is easy to see that $n \geq m + t$, so the first two examples are optimal. The result that $t < \lfloor \frac{2n}{3} \rfloor$ if $m = 2$ is much more difficult; it was first proved in [4].

In this talk, we will survey some recent results on existence and bounds for resilient functions. In particular, we will discuss progress on three conjectures made in papers by Chor *et al* [4] and Bennett *et al* [1].

Our treatment will use an orthogonal array characterization of resilient functions that was given in [18]. An *orthogonal array* $OA_\lambda(t, k, v)$ is a $\lambda v^t \times k$ array of v symbols, such that in any t columns of the array every one of the possible v^t ordered pairs of symbols occurs in exactly λ rows.

An orthogonal array is said to be *simple* if no two rows are identical. A *large set* of orthogonal arrays $OA_\lambda(t, k, v)$ is defined to be a set of v^{k-t}/λ simple arrays $OA_\lambda(t, k, v)$ such that every possible k–tuple of symbols occurs in exactly one of the OA's in the set. (An equivalent statement is that the union of the OA's forms an $OA_1(k, k, v)$.)

Here is the characterization proved in [18].

Theorem 1.1 *An (n, m, t)–resilient function is equivalent to a large set of orthogonal arrays $OA_{2^{n-m-t}}(t, n, 2)$.*

The correspondence between resilient functions and orthogonal arrays is this: for any k–tuple $(y_1, \ldots, y_k)$, the inverse image $f^{-1}(y_1, \ldots, y_k)$ of an (n, k, t)–RF, f, is an orthogonal array $OA_{2^{n-k-t}}(t, n, 2)$; and the 2^k OA's thus obtained comprise a large set.

We should mention another related cryptographic application of OA's, namely the *perfect local randomizers* of Maurer and Massey [14]. A perfect local randomizer turns out to be equivalent to a single orthogonal array, whereas a resilient function requires a large set.

2 Non-linear resilient functions

The most important construction for resilient functions uses linear error-correcting codes. Recall that a (linear) $[n, k, d]$ code is a $k-$dimensional subspace $\mathcal{C}$ of $(\mathbf{Z}_2)^n$ such that any two distinct vectors (codewords) in $\mathcal{C}$ have Hamming distance at least d. If M is a $k \times n$ matrix whose rows form a basis for $\mathcal{C}$, then M is called a *generating matrix* for $\mathcal{C}$.

A *linear* $(n, m, t)-$RF is one where every output bit is a linear function of the input bits.

Theorem 2.1 *[1, 4] The existence of an $[n, k, d]$ code is equivalent to the existence of a linear $(n, k, d-1)-RF$.*

In [1], it was conjectured that if there exists an $(n, m, t)-$RF, then there exists a linear $(n, m, t)-$RF. Recently, Stinson and Massey constructed an infinite class of counterexamples to this conjecture using the (non-linear) Kerdock codes. The smallest counterexample in the class is a non-linear $(16, 8, 5)-$RF which is constucted from the famous Nordstrom-Robinson code.

The result is based on constructing a non-linear resilient function from a non-linear systematic code. We will use the notation (n, K, d) code to denote a binary code $\mathcal{C}$ (not necessarily linear), where $\mathcal{C} \subseteq \{0,1\}^n$, $|\mathcal{C}| = K$, and any two codewords have Hamming distance at least d. (Thus, an $[n, k, d]$ code is also an $(n, 2^k, d)$ code.) Suppose $\mathcal{C}$ is an (n, K, d) code in which there exist k co-ordinates such that every possible $k-$tuple occurs in exactly one codeword within the k specified co-ordinates (of course, this implies $K = 2^k$). Then $\mathcal{C}$ is said to be *systematic*.

The following result was proved in [19].

Theorem 2.2 *If there exists a systematic (n, K, d) code, $\mathcal{C}$, having dual distance d', then there is an $(n, n-k, d'-1)-RF$, where $K = 2^k$.*

Note that the value of the distance, d, is irrelevant in this theorem. Further, this result subsumes Theorem 2.1, since the dual code of an $[n, k, d]$ code is a systematic $(n, 2^{n-k}, d^*)$ code (for some d^*) having dual distance d.

Theorem 2.2 was applied to the well-known Preparata codes [15] and Kerdock codes [12]. The properties of these codes are also discussed in [13], where the following results are proved.

Theorem 2.3 *Let $r \geq 3$ be odd. The Preparata code $\mathcal{P}(r+1)$ is a non-linear, systematic $(2^{r+1}, 2^{2^{r+1}-2r-2}, 6)$ code having dual distance $d' = 2^r - 2^{(r-1)/2}$. The Kerdock code $\mathcal{K}(r+1)$ is a non-linear, systematic $(2^{r+1}, 2^{2r+2}, 2^r - 2^{(r-1)/2})$ code having dual distance $d' = 6$.*

Applying Theorem 2.2, Stinson and Massey obtained resilient functions from these codes as follows.

Theorem 2.4 *[19] For any odd integer $r \geq 3$, there is a non-linear $(2^{r+1}, 2r+2, 2^r - 2^{(r-1)/2} - 1)-RF$ and a non-linear $(2^{r+1}, 2^{r+1} - 2r - 2, 5)-RF$.*

Example 1 *The code $\mathcal{P}(4)$ is the same as $\mathcal{K}(4)$, and it is also known as the Nordstrom-Robinson code. It is a $(16,256,6)$ code which yields a large set of $OA_8(5,16,2)$'s and a $(16,8,5)-RF$.*

Now, in order to disprove the conjecture made in [1], we need to consider the existence of linear RFs with the same parameters. Theorem 2.1 states that existence of these (hypothetical) RFs are equivalent to existence of linear codes as follows:

linear $(2^{r+1}, 2r+2, 2^r - 2^{(r-1)/2} - 1)-$RF	$\Leftrightarrow$	$[2^{r+1}, 2r+2, 2^r - 2^{(r-1)/2}]$ code
linear $(2^{r+1}, 2^{r+1} - 2r - 2, 5)-$RF	$\Leftrightarrow$	$[2^{r+1}, 2^{r+1} - 2r - 2, 6]$ code

It was proved in [8, Theorem 6.2] that there does not exist a $[2^{r+1}-1, 2^{r+1}-2r-2, 5]$ code for any odd integer $r \geq 3$. This immediately implies the nonexistence of a linear code with the parameters of a Preparata code, since puncturing a $[2^{r+1}, 2^{r+1}-2r-2, 6]$ code would produce a $[2^{r+1}-1, 2^{r+1}-2r-2, 5]$ code. Hence, there do not exist linear $(2^{r+1}, 2^{r+1}-2r-2, 5)-$RF's for these values of r (note that these resilient functions are the ones derived from the *Kerdock codes*).

As well, it is known that a $[64, 12, 28]$ code does not exist; hence, there is no linear $(64, 12, 27)-$RF. We summarize this discussion as follows.

Theorem 2.5 *[19]*

(1) *For any odd integer $r \geq 3$, a $(2^{r+1}, 2^{r+1} - 2r - 2, 5)-RF$ exists, but no linear resilient function with these parameters exists.*

(2) *A $(64, 12, 27)-RF$ exists, but no linear resilient function with these parameters exists.*

3 Symmetric resilient functions

A $(n, m, t)-$RF

$$f : \{0,1\}^n \longrightarrow \{0,1\}^m$$

is *symmetric* if, for every permutation $\pi : \{1, 2, \ldots, n\} \longrightarrow \{1, 2, \ldots, n\}$, we have

$$f(x_1, x_2, \ldots, x_n) = f(x_{\pi(1)}, x_{\pi(2)}, \ldots, x_{\pi(n)}).$$

In 1985, Chor *et al* [4] conjectured that the only symmetric $(n, 1, 1)-$RFs are

$$\sum_{i=1}^{n} x_i$$

and

$$1 + \sum_{i=1}^{n} x_i,$$

where the arithmetic is done in $\mathbf{Z}_2$. (Note that these two functions are in fact $(n, 1, n-1)-$RFs.)

This conjecture was disproved by Gopalakrishnan, Hoffman and Stinson in [9]. In fact, they found an infinite class of symmetric $(r^2 - 2, 1, 2)-$RFs (which are not of the form given above), as stated in the following theorem.

Theorem 3.1 *[9] For any even integer $r > 2$, there exists a symmetric $(r^2-2, 1, 2)-RF$ that is not the modulo−2 sum of the n inputs or its complement.*

Here is a brief description of how to construct these RFs. First, let

$$f : \{0,1\}^n \longrightarrow \{0,1\}$$

be a symmetric function. Then it is clear that there exists a function

$$g : \{0,1,\ldots,n\} \longrightarrow \{0,1\}$$

such that $f(x) = g(w(x))$ where $w(x)$ denotes the Hamming weight of the n-tuple x. This is because any two binary $n-$tuples with the same Hamming weight are permutations of each other, and thus they yield the same output.

The following can be proved easily.

Theorem 3.2 *There exists a symmetric $(n, 1, t)-RF$ if and only if there exists a function $g : \{0,1,\ldots,n\} \longrightarrow \{0,1\}$ such that*

$$\sum_{i=0}^{n-j} \binom{n-j}{i} g(i) = 2^{n-j-1}$$

for all j, $0 \leq j \leq t$.

By exhibiting a suitable function g, we can disprove the conjecture. First, define a function f as follows:

$$f(i) = \begin{cases} 0 & \text{if } i \text{ is even} \\ 1 & \text{if } i \text{ is odd.} \end{cases}$$

Now, let $n = r^2 - 2$ where $r > 2$ is even, and define $k = (n-r)/2$. Define g as follows:

$$f(i) = \begin{cases} 1 - g(i) & \text{if } i = k, k+1, n-k \text{ or } n-k+1 \\ g(i) & \text{otherwise.} \end{cases}$$

Then it is not difficult to prove that g gives rise to an $(n, 1, 2)-$RF; see [9] for details.

Example 2 *Suppose we take $r = 4$, then $k = 5$ and $n = 14$. We obtain the function g where*

$$(g(i) : 0 \leq i \leq 14) = (0,1,0,1,0,0,1,1,0,0,1,1,0,1,0).$$

This gives rise to a $(14, 1, 2)-RF$.

4 Bounds on resilient functions

Another conjecture made in [4] was that if an $(n, m, t)-$RF exists, then

$$t < \left\lfloor \frac{2^{m-1}n}{2^m - 1} \right\rfloor.$$

In [4], this conjecture was shown to be true for $m = 1, 2$ (and in these cases, the bound is tight). The conjecture was also proved true in [4] for arbitrary m in the special case of linear resilient functions. More recently, Friedman [7] proved the conjecture in general by studying colourings of the $n-$dimensional boolean cube.

In fact, Friedman's proof can be interpreted as a bound on orthogonal arrays. These orthogonal array bounds can be derived in a straightforward way from the well-known linear programming bounds of coding theory, which is work of Delsarte [5, 6]. We describe this approach now.

The *distance distribution* of an (n, M, d) code, $\mathcal{C}$, is defined to be the sequence $(B_0, B_1, \ldots, B_n)$, where

$$B_i = \frac{1}{M} |\{(u, v) : u, v \in \mathcal{C}, d(u, v) = i\}|.$$

Note that $B_0 = 1$ and $B_0 + B_1 + \ldots + B_n = M$.

For $0 \leq k \leq n$, define

$$B'_k = \frac{1}{M} \sum_{i=0}^{n} B_i P_k(i),$$

where

$$P_k(i) = \sum_{j=0}^{k} (-1)^j \binom{i}{j} \binom{n-i}{k-j}$$

is the value of the *Krawtchouk polynomial* $P_k(x)$ at integer i. The sequence

$$(B'_0, B'_1, \ldots, B'_n)$$

is called the *dual distance distribution* of $\mathcal{C}$.

If $B'_i = 0$ for $1 \leq i \leq d' - 1$ and $B'_{d'} \neq 0$, then d' is called the *dual distance* of the code $\mathcal{C}$.

If $\mathcal{C}$ is linear then $(B'_0, B'_1, \ldots, B'_n)$ is indeed the distance distribution of the dual code $\mathcal{C}^\perp$, and d' is the minimum distance of $\mathcal{C}^\perp$. However, it turns out that even when $\mathcal{C}$ is not a linear code, the dual distance d' has combinatorial significance. The following theorem describes the combinatorial significance of the dual distance d'; the proof, due to Delsarte, can be found in [6].

Theorem 4.1 *If we write the vectors in $\mathcal{C}$ as rows of an $M \times n$ array, then any set of $r \leq d' - 1$ columns contains each r-tuple exactly $M/2^r$ times, and d' is the largest number with this property. In other words, $\mathcal{C}$ is an orthogonal array $OA_\lambda(d' - 1, n, 2)$ where $\lambda = M/2^{d'-1}$.*

It is clear that for any code $\mathcal{C}$, we have $B_i \geq 0$ for $i = 0, 1, \ldots n$. On the other hand, it is a non-trivial theorem (see for example [6]) the $B_i' \geq 0$ for $i = 0, 1, \ldots n$.

Suppose an $OA_\lambda(t, n, 2)$ exists. Let $M = \lambda 2^t$ be the number of rows in this orthogonal array. If we view the rows of this orthogonal array as codewords of a code $\mathcal{C}$, then a lower bound on M can be obtained by solving a suitable linear programming problem (see [5] for similar approaches to a different problem).

We can formulate the following linear programming problem which we will refer to as **LP1**:

Minimize $B_1 + B_2 + \cdots + B_n$
subject to

$$\sum_{i=1}^{n} B_i P_k(i) = -\binom{n}{k} \text{ for } 1 \leq k \leq t$$

$$\sum_{i=1}^{n} B_i P_k(i) \geq -\binom{n}{k} \text{ for } t+1 \leq k \leq n$$

$B_i \geq 0$ for $1 \leq i \leq n$

Let $B = B(n, t)$ be the optimal solution to the above linear programming problem. Then we have

$$M = \sum_{i=0}^{n} B_i \geq 1 + B \tag{1}$$

Now let us return to our original problem of establishing stronger upper bounds for the optimal value of t. Recall that an (n, m, t) resilient function exists if only if $LOA_{2^{n-m-t}}(t, n, 2)$ exists. Clearly $LOA_{2^{n-m-t}}(t, n, 2)$ exists only if an $OA_{2^{n-m-t}}(t, n, 2)$ exists. The number of rows in this orthogonal array is given by

$$M = 2^{n-m-t} 2^t = 2^{n-m}.$$

In view of the bound of inequality (1), this immediately implies that

$$m \leq n - \log_2(1 + B).$$

In order to obtain explicit bounds on OA's and resilient functions, it is more convenient to work with the dual LP (which we name **LP2**), defined as follows:

Maximize $\sum_{i=1}^{n} x_i \binom{n}{i}$

subject to

$$\sum_{i=1}^{n} x_i P_i(k) \geq -1 \text{ for } k = 1 \text{ to } n$$

$x_1, x_2, \ldots x_t$ unrestricted
$x_{t+1}, x_{t+2}, \ldots x_n \leq 0$

It is a standard theorem in the theory of linear programming that in a pair of primal-dual linear programs the optimal value of the minimization problem will always be greater than or equal to the value attained by the objective function of the maximization problem at any feasible solution vector. So any feasible solution to the dual linear program **LP2** yields a lower bound on the size of the orthogonal array of strength t and length n and consequently an upper bound on m of t-resilient functions on n-tuples.

Consider the solution vector

$$x_i = 1 - \frac{i}{t+1}.$$

It can be shown that this is a feasible solution for **LP2**. If we compute the objective function, then it follows that

$$M \geq 1 + B \geq 2^n - \frac{n2^{n-1}}{t+1}.$$

As a consequence, we get the following Theorem, which was first proved by Friedman [7] using very different methods.

Theorem 4.2 *If an (n, m, t)-resilient function exists, then*

$$t \leq \left\lfloor \frac{2^{m-1}n}{2^m - 1} \right\rfloor - 1.$$

The power of this linear programming approach is that other bounds can be obtained by finding other feasible solutions to **LP2**. For example, another feasible solution is given by

$$x_i = 1 - \frac{\lceil \frac{i}{2} \rceil}{\lceil \frac{t+1}{2} \rceil}.$$

This gives rise to the following:

$$M \geq 1 + B \geq 2^n - \frac{2^{n-2}(n+1)}{\lceil \frac{t+1}{2} \rceil}.$$

As a consequence, we get the following new bound on RF's.

Theorem 4.3 (Gopalakrishnan and Stinson) *If an (n, m, t)-resilient function exists, then*

$$t \leq 2 \left\lfloor \frac{2^{m-2}(n+1)}{2^m - 1} \right\rfloor - 1.$$

As an illustration, let's look at the optimal resiliency of resilient functions with $m = 3$. The bound of Theorem 4.2 gives $t \leq \lfloor 4n/7 \rfloor - 1$ and the bound of Theorem 4.3 gives $t \leq 2\lfloor (2n+2)/7 \rfloor - 1$. We tabulate the two bounds as follows:

n	$\lfloor 4n/7 \rfloor - 1$	$2\lfloor (2n+2)/7 \rfloor - 1$
$7h$	$4h-1$	$4h-1$
$7h+1$	$4h-1$	$4h-1$
$7h+2$	$4h$	$4h-1$
$7h+3$	$4h$	$4h+1$
$7h+4$	$4h+1$	$4h+1$
$7h+5$	$4h+1$	$4h+1$
$7h+6$	$4h+2$	$4h+3$

We see that Theorem 4.2 gives the strongest bound for $n \equiv 3, 6 \bmod 7$, Theorem 4.3 gives the strongest bound for $n \equiv 2 \bmod 7$, and the two bounds are equal for $n \equiv 0, 1, 4, 5 \bmod 7$.

Of course these are only upper bounds on t. But if we use known results on linear codes to obtain lower bounds on t, then the following theorem results.

Theorem 4.4 (Gopalakrishnan and Stinson) *The maximum value of t such that an $(n, 3, t)-RF$ exists is*

$$\begin{array}{ll} \lfloor \frac{4n}{7} \rfloor - 1 & \text{if } n \not\equiv 2 \bmod 7 \\ \lfloor \frac{4n}{7} \rfloor - 2 & \text{if } n \equiv 2 \bmod 7 \end{array}.$$

By applying similar techniques for $m = 4$, we have been able to determine the optimal resiliency for 13 of the 15 congruence classes modulo 15.

References

[1] C. H. Bennett, G. Brassard and J.-M. Robert. Privacy amplification by public discussion. *SIAM J. Comput.* **17** (1988), 210–229.

[2] C. H. Bennett, G. Brassard and A. K. Ekert. Quantum cryptography. *Scientific American*, vol. 267, no. 5 (1992), 50–57.

[3] P. Camion, C. Carlet, P. Charpin and N. Sendrier. On correlation-immune functions. *Lecture Notes in Computer Science* **576** (1992), 86–100.

[4] B. Chor, O. Goldreich, J. Hastad, J. Friedman, S. Rudich and R. Smolensky. The bit extraction problem or $t-$resilient functions. *Proc. 26th IEEE Symp. on Foundations of Computer Science* (1985), 396–407.

[5] P. Delsarte. Bounds for unrestricted codes, by linear programming. *Philips Research Reports* **27** (1972), 272–289.

[6] P. Delsarte. Four fundamental parameters of a code and their combinatorial significance. *Information and Control* **23** (1973), 407–438.

[7] J. FRIEDMAN. On the bit extraction problem. *Proc. 33rd IEEE Symp. on Foundations of Computer Science* (1992), 314–319.

[8] J.-M. GOETHALS AND S. L. SNOVER. Nearly perfect binary codes. *Discrete Math.* **3** (1972), 65–88.

[9] K. GOPALAKRISHNAN, D. G. HOFFMAN AND D. R. STINSON. A note on a conjecture concerning symmetric resilient functions. *Information Processing Letters* **47** (1993), 139–143.

[10] K. GOPALAKRISHNAN AND D. R. STINSON. Characterizations of non-binary correlation-immune and resilient functions. Submitted to *Designs, Codes and Cryptography.*

[11] X. GUO-ZHEN AND J. L. MASSEY. A spectral characterization of correlation-immune functions. *IEEE Trans. Inform. Theory* **34** (1988), 569–571.

[12] A. M. KERDOCK. A class of low rate non-linear codes. *Inform. and Control* **20** (1972), 182–187.

[13] F. J. MACWILLIAMS AND N. J. A. SLOANE. *The Theory of Error-correcting Codes*, North-Holland, 1977.

[14] U. M. MAURER AND J. L. MASSEY. Local randomness in pseudorandom sequences. *Journal of Cryptology* **4** (1991), 135–149.

[15] F. P. PREPARATA. A class of optimum non-linear double-error-correcting codes. *Inform. and Control* **13** (1968), 378–400.

[16] R. RUEPPEL. *Analysis and Design of Stream Ciphers*, Springer Verlag, Berlin, 1986.

[17] R. T. SIEGENTHALER. Correlation immunity of nonlinear combining functions for cryptographic applications. *IEEE Trans. Inform. Theory* **30** (1984), 776–780.

[18] D. R. STINSON. Resilient functions and large sets of orthogonal arrays. *Congressus Numer.* **92** (1993), 105–110.

[19] D. R. STINSON AND J. L. MASSEY. An infinite class of counterexamples to a conjecture concerning non-linear resilient functions. To appear in *Journal of Cryptology.*

Information Leakage of Boolean Functions as a Measure of Cryptographic Strength

M. Zhang[†], S. E. Tavares[†] and L. L. Campbell[††]

[†]Department of Electrical and Computer Engineering
[††]Department of Mathematics and Statistics
Queen's University, Kingston, Ontario, Canada, K7L 3N6
Phone: (613) 545–2925
Fax: (613) 545–6615
email: tavares@ee.queensu.ca

Abstract

This paper presents some results on the cryptographic strength of Boolean functions from the information theoretic point of view. It is argued that a Boolean function is resistant to statistical analysis if there is no significant static and dynamic information leakage between its inputs and its output. We note that some conventional cryptographic criteria require zero static or dynamic information leakage in only one domain. Such a requirement can result in a large information leakage in another domain. To avoid this weakness, it is better to jointly constrain all kinds of information leakage in the function. This approach can lead to the discovery of cryptographically strong Boolean functions. In fact, we claim that information leakage can be used as a fundamental measure of the strength of a cryptographic algorithm.

1 Introduction

The recent development of statistical attacks such as correlation attacks [1], differential cryptanalysis [2], and linear cryptanalysis [3], has enhanced the success of cryptanalysis of private-key cryptosystems. As a result, there has been considerable interest in the development of cryptosystems that resist statistical cryptanalysis. Information theory can be an important tool in this objective. Forré [4] suggested that it is desirable that a cryptographic transformation minimize the mutual information between the inputs and outputs. This idea was further developed by Dawson and Tavares [5] who proposed the *information leakage measure* for the design of S-boxes. Recently the measure was further applied to the construction of substitution-permutation networks [6].

In this paper, we present some results on the cryptographic strength of Boolean functions from the information theoretic perspective. Boolean functions are the basic components from which many private-key cryptographic transformations can be analyzed and constructed. The cryptographic power of those transformations depends to a large extent on the strength of the component Boolean functions. Conventionally, the strength of a Boolean function is evaluated by cryptographic criteria such as 0–1 balance, completeness [7], Strict Avalanche Criterion (SAC) [8], correlation immunity [9], nonlinearity [10], higher order SAC by Adams & Tavares [11, 12] (also called propagation criterion [13]) and higher order SAC by Forré [14]. This paper relates these criteria within the framework of information leakage.

Statistical analysis of a Boolean function aims at determining the statistical relationship between the output and the inputs either statically or dynamically. A function is resistant

to statistical analysis if no significant information leakage exists by both static and dynamic measurement. In the information theoretic point of view, the nature of some conventional criteria is to require zero mutual information between the output and a certain number of inputs, or zero information leakage between the change of output and prescribed change patterns of the inputs. These exact requirements often constrain the Boolean functions and may result in cryptographic weakness. So we suggest that a cryptographically good function does not necessarily satisfy those criteria exactly. In fact, information leakage can be used as a fundamental measure of the cryptographic strength of a Boolean function or cryptographic transformation and enables the discovery of strong functions.

2 Definition of information leakage

Let $Y = f(\mathbf{X})$ be a Boolean function of n variables, where $\mathbf{X} = (X_1, X_2, ..., X_n)$. $X_1, X_2, ..., X_n$ are independent binary random variables equally likely to be zeros and ones. The changes of input variables, denoted by $\Delta X_1, \Delta X_2, ..., \Delta X_n$, are also assumed to be independent and equiprobable random variables. The output change is defined by $\Delta Y = f(\mathbf{X} \oplus \Delta\mathbf{X}) \oplus f(\mathbf{X})$, where $\Delta\mathbf{X} = (\Delta X_1, \Delta X_2, ..., \Delta X_n)$. The XOR operation can be applied to a group of k ($0 < k \leq n$) distinct input variables $\mathbf{X_k} = (X_{i_1}, ..., X_{i_k})$, and the result $\sum_k \mathbf{X} = X_{i_1} \oplus X_{i_2} \oplus ... \oplus X_{i_k}$ is called the ***sum*** of the k variables. Let $\Delta\mathbf{X_k}$ denotes the change of $\mathbf{X_k}$. Finally, $\mathbf{x_k}$ and $\Delta\mathbf{x_k}$ represent the value of $\mathbf{X_k}$ and $\Delta\mathbf{X_k}$ respectively.

A cryptographic function is resistant to statistical analysis if the predictability of the output and output change is poor without complete information about the inputs. Using information theory, the unpredictability can be measured by the conditional entropy of the output variable(s) or the change(s) of output variable(s). Conversely, information leakage may be used as a measure of the predictability of the variables. We define two general types of statistical analysis—static analysis and dynamic (or differential) analysis. By static analysis, we include all methods of determining the statistical relationship between the inputs and outputs of a transformation. By dynamic or differential analysis, we include all means of determining the statistical relationship between the difference in the inputs and the difference in the outputs. For example, the correlation attacks and linear cryptanalysis use the static analysis, and the differential cryptanalysis uses the dynamic analysis. We classify information leakage into static and dynamic information leakage (abbreviation: *SL, DL*) in order to demonstrate their different roles in measuring the vulnerability to two types of statistical analysis.

When the value of $\mathbf{X_k}$ is given by $\mathbf{x_k}$, we may write the entropy of Y as $H(Y|\mathbf{X_k} = \mathbf{x_k})$. Then the entropy $H(Y|\mathbf{X_k})$ is the probability average of $H(Y|\mathbf{X_k} = \mathbf{x_k})$ over all $\mathbf{x_k} \in Z_2^k$. Similarly, $H(\Delta Y|\Delta\mathbf{X_k})$ is the probability average of $H(\Delta Y|\Delta\mathbf{X_k} = \Delta\mathbf{x_k})$ over all $\Delta\mathbf{x_k} \in Z_2^k$. Using the notation defined above, we introduce the following measurements of information leakage.

Definition 1 *Let Y be the output of a Boolean function, then the static information leakage of Y, given input vector $\mathbf{x_k}$, is defined by*

$$SL(Y; \mathbf{X_k}|\mathbf{x_k}) = 1 - H(Y|\mathbf{X_k} = \mathbf{x_k}) . \tag{1}$$

Similarly, the dynamic information leakage of Y, given input change vector $\Delta\mathbf{x_k}$, is defined by

$$DL(\Delta Y; \Delta\mathbf{X_k}|\Delta\mathbf{x_k}) = 1 - H(\Delta Y|\Delta\mathbf{X_k} = \Delta\mathbf{x_k}) . \tag{2}$$

Definition 2 *The static/dynamic information leakage between* $Y = f(\mathbf{X})$ *and* $\mathbf{X_k}$ *is defined by*

$$SL(Y;\mathbf{X_k}) = 1 - H(Y|\mathbf{X_k}) \tag{3}$$

$$or \quad DL(\Delta Y;\Delta\mathbf{X_k}) = 1 - H(\Delta Y|\Delta\mathbf{X_k}). \tag{4}$$

The self static/dynamic information leakage of Y, *defined by* $SL(Y) = 1 - H(Y)$ *or* $DL(\Delta Y) = 1 - H(\Delta Y)$, *can be considered as the static/dynamic information leakage in the case of* $k = 0$.

Remarks: When $k = n$, $SL(Y;\mathbf{X_k}|\mathrm{x_k})$ becomes $SL(Y;\mathbf{X}|\mathrm{x})$, which is always equal to 1. As well, $SL(Y;\mathbf{X}) = 1$. In this case, the inputs are completely known, yielding no uncertainty in the output.

Notice that since all input variables and their changes are independent and equally likely to be zeros and ones, the above two definitions are related by

$$SL(Y;\mathbf{X_k}) = 2^{-k}\sum_{\mathrm{x_k}} SL(Y;\mathbf{X_k}|\mathrm{x_k})\,, \tag{5}$$

$$DL(\Delta Y;\Delta\mathbf{X_k}) = 2^{-k}\sum_{\Delta\mathrm{x_k}} SL(\Delta Y;\Delta\mathbf{X_k}|\Delta\mathrm{x_k})\,, \tag{6}$$

where the summation is over all values of $\mathrm{x_k}$ or $\Delta\mathrm{x_k}$. Using mutual information $I(Y;\mathbf{X_k})$ and $I(\Delta Y;\Delta\mathbf{X_k})$, it follows from $H(Y|\mathbf{X_k}) = H(Y) - I(Y;\mathbf{X_k})$ or $H(\Delta Y|\Delta\mathbf{X_k}) = H(\Delta Y) - I(\Delta Y;\Delta\mathbf{X_k})$ that

$$SL(Y;\mathbf{X_k}) = 1 - H(Y) + I(Y;\mathbf{X_k})\,, \tag{7}$$

$$DL(\Delta Y;\Delta\mathbf{X_k}) = 1 - H(\Delta Y) + I(\Delta Y;\Delta\mathbf{X_k})\,. \tag{8}$$

Hence the above defined information leakage is equivalent to mutual information if and only if the Boolean functions are balanced. Otherwise, it equals the mutual information plus self information leakage.

Proposition 1 *Information leakage increases when more input variables are given. Precisely,* $SL(Y;\mathbf{X_k}) \geq SL(Y;\mathbf{X_{k-1}})$ and $DL(\Delta Y;\Delta\mathbf{X_k}) \geq DL(\Delta Y;\Delta\mathbf{X_{k-1}})$.

Proof: By the chain rule [15, Th.2.5.2], we have

$$I(Y;\mathbf{X_k}) = I(Y;\mathbf{X_{k-1}}) + I(Y;X_{i_k}|\mathbf{X_{k-1}}) \geq I(Y;\mathbf{X_{k-1}})\,. \tag{9}$$

Following (7), it is obvious that adding $1 - H(Y)$ to both sides of above inequality yields $SL(Y;\mathbf{X_k}) \geq SL(Y;\mathbf{X_{k-1}})$. By similar derivation, we can get $DL(\Delta Y;\Delta\mathbf{X_k}) \geq DL(\Delta Y;\Delta\mathbf{X_{k-1}})$. □

Definition 3 *The static information leakage of* Y, *given the sum of input variables* $\sum_k\mathbf{X} = \beta$, $(\beta \in Z_2)$, *is defined by*

$$SL\left(Y;\textstyle\sum_k\mathbf{X}|\beta\right) = 1 - H\left(Y|\sum_k\mathbf{X} = \beta\right)\,. \tag{10}$$

Remarks: If for fixed k and all choices of $\mathbf{X_k}$, $SL(Y;\mathbf{X_k}) = 0$, then the function $Y = f(\mathbf{X})$ satisfies ***zero static information leakage of order k.*** Such a function has maximum entropy $H(Y|\mathbf{X_k}) = 1$, and hence satisfies $H\left(Y|\sum_k\mathbf{X} = \beta\right) = 1$ for all $\beta \in Z_2$. In other words,

$SL\left(Y;\sum_k \mathbf{X}|\beta\right) = 0$ $(\beta = 0, 1)$ follows from $SL(Y;\mathbf{X_k}) = 0$. By Proposition 1, it is obvious that zero static information leakage of order k includes zero static information leakage of order less than k. Therefore, the function has no static information leakage when k or less input variables are known.

3 Static information leakage and its relation to cryptographic criteria

Static information leakage measures the vulnerability of a function to static analysis. If there is no significant static information leakage between the output and the partially given inputs, the function is resistant to static analysis. Cryptographic properties that resist static analysis should act in some way to reduce static information leakage. To show this, we characterize the causes of static information leakage.

Theorem 1 *Let $f(\mathbf{X_{n-k}}|\mathbf{x_k})$ be the sub-function obtained from $f(\mathbf{X})$ by fixing $\mathbf{X_k}$ at value $\mathbf{x_k}$, where $\mathbf{X_{n-k}}$ denotes the set of variables obtained from $\mathbf{X}$ with components $X_{i_1}X_{i_2}...X_{i_k}$ removed. Let N_0 and N_1 denote the number of 0's and 1's respectively in the output sequence of the sub-function. Define coefficient $r(\mathbf{x_k}) = |N_0 - N_1|/(N_0 + N_1)$ as the balance coefficient of sub-function $f(\mathbf{X_{n-k}}|\mathbf{x_k})$. Then*

$$SL(Y;\mathbf{X_k}|\mathbf{x_k}) = 1 - h\left(\frac{1}{2} - \frac{r(\mathbf{x_k})}{2}\right), \tag{11}$$

where $h(\cdot)$ is the binary entropy function, $h(t) = -t\log_2 t - (1-t)\log_2(1-t)$.

Proof: The probabilities that a sub-function $Y' = f(\mathbf{X_{n-k}}|\mathbf{x_k})$ is 0 or 1 are computed by:

$$p(Y'=0) = \frac{N_0}{N_0+N_1} = \frac{1}{2} + \frac{N_0 - N_1}{2(N_0+N_1)}, \tag{12}$$

$$p(Y'=1) = \frac{1}{2} - \frac{N_0 - N_1}{2(N_0+N_1)}. \tag{13}$$

Consequently, $H(Y|\mathbf{X_k} = \mathbf{x_k}) = h(p(Y'=1)) = h(1/2 - r(\mathbf{x_k})/2)$. Applying above results to (1) yields the theorem. □

It may be seen that $SL(Y;\mathbf{X_k}|\mathbf{x_k}) = 0$ if and only if the balance coefficient $r(\mathbf{x_k})$ is zero, and the value of $SL(Y;\mathbf{X_k}|\mathbf{x_k})$ increases if the coefficient increases. In general, $SL(Y;\mathbf{X_k}) = 0$ if and only if all the sub-functions obtained from $f(\mathbf{X})$ by fixing $\mathbf{X_k}$ are balanced. From this, we conclude that the static information leakage between the output and given inputs is caused by the imbalance of its sub-functions.

The relationship between information leakage and the 0–1 balance criterion is clear. A function $Y = f(\mathbf{X})$ is called 0–1 balanced if it has an equal number of 0's and 1's in the output sequence. 0–1 balance is achieved if and only if $SL(Y) = 0$. Consider $\Delta Y = f(\mathbf{X} \oplus \Delta\mathbf{X}) \oplus f(\mathbf{X})$ being a function with two sets of inputs $\mathbf{X}$ and $\Delta\mathbf{X}$. Since $f(\mathbf{X})$ is balanced, the function $f(\mathbf{X} \oplus \Delta\mathbf{X}) \oplus f(\mathbf{X})$ must also be balanced. As a result, $H(\Delta Y) = 1$ (or $DL(\Delta Y) = 0$). Thus the 0–1 balance criterion is equivalent to zero self information leakage.

The self information leakage is of interest since it measures the vulnerability to statistical analysis when no information about the inputs is available. If partial information about the inputs is available up to n–1 bits, static information leakage between the output and arbitrary n–1 input variables would be one of our main concerns because it reflects the vulnerability to

static analysis in one of the the worst cases. It is proved in Proposition 1 that more information about inputs yields more information leakage.

Theorem 2 *With random inputs* $\mathbf{X}$, *suppose the output* Y *changes with probability* p_{i_n} *when* X_{i_n} *is complemented, then* $SL(Y;\mathbf{X_{n-1}}) = 1 - p_{i_n}$, *where* $\mathbf{X_{n-1}}$ *denotes the set of variables obtained from* $\mathbf{X}$ *with component* X_{i_n} *removed.*

Proof: Following Theorem 1, sub-function $f(X_{i_n}|\mathbf{x_{n-1}})$ is obtained from $f(\mathbf{X})$ by fixing $\mathbf{X_{n-1}}$ at the value $\mathbf{x_{n-1}}$, and there are two bits in the output sequence. If Y changes when X_{i_n} is complemented, the balance coefficient $r(\mathbf{x_{n-1}})$ is 0. Otherwise, the coefficient is 1. Also the binary entropy function $h(\cdot)$ satisfies $h(1/2) = 1$ and $h(0) = 0$. As a result,

$$h\left(\frac{1}{2} - \frac{r(\mathbf{x_{n-1}})}{2}\right) = \begin{cases} 1, & Y \text{ changes when } X_{i_n} \text{ is complemented} \\ 0, & Y \text{ doesn't change when } X_{i_n} \text{ is complemented} \end{cases}. \tag{14}$$

Applying all possible input value $\mathbf{x_{n-1}}$ and letting s be the total number of times that Y changes when X_{i_n} is complemented, yields

$$2^{-(n-1)} \sum_{\mathbf{x_{n-1}}} h\left(\frac{1}{2} - \frac{r(\mathbf{x_{n-1}})}{2}\right) = \frac{s}{2^{n-1}} = p_{i_n}. \tag{15}$$

Replacing k with n–1 in equation (5) and then combining it with equation (11) and (15), we get Theorem 2. □

All functions, with some known exceptions, are most vulnerable to static analysis when arbitrary n–1 input bits can be exposed, ignoring the trivial case where all inputs are given. Limiting the static information leakage between the output and every choice of n–1 input variables is important to the security of a function. It follows from Theorem 2 that $p_{i_n} = 0$ yields $SL(Y;\mathbf{X_{n-1}}) = 1$. In other words, if Y is independent of X_{i_n}, the knowledge of the other n–1 input variables completely gives away the output. Then the function degenerates into an (n–1)-input function. To avoid this situation, the completeness criterion must be satisfied. The completeness criterion requires that Y depend on every input variable. It guarantees $p_{i_n} > 0$ for all i_n, $1 \le i_n \le n$. Obviously, an equivalent description of the completeness criterion is that the static information leakage between the output and every n–1 input variables is less than 1 bit.

The strict avalanche criterion requires the output Y changes with a probability 1/2 whenever a single input variable is complemented. Its relationship with static information leakage is described in the following corollary.

Corollary 2.1 *A function satisfies the strict avalanche criterion if and only if* $SL(Y;\mathbf{X_{n-1}}) = 1/2$ *for all choices of n–1 input variables* $\mathbf{X_{n-1}}$.

Further than the completeness criterion, the strict avalanche criterion constrains the static information leakage between the output and every n–1 input variables to 1/2 bit, so the function can not be approximated by an (n–1)-input sub-function.

Theorem 3 *The static information leakage* $SL(Y;\mathbf{X_k})$ *is equal to the self static information leakage* $1 - H(Y)$ *if and only if the mutual information* $I(Y;\mathbf{X_k})$ *is zero.*

Proof: The theorem follows from (7). □

Reducing the mutual information between the output and the inputs could result in a reduction of static information leakage between the output and given inputs. In the extreme case where mutual information is zero, a function satisfies the correlation immune criterion. By definition, function $Y = f(\mathbf{X})$ is k-th order correlation immune if every k-tuple obtained by choosing k components from $\mathbf{X}$ is statistically independent of Y. Using the notation of mutual information, we may refer to the k-th order correlation immunity as $I(Y;\mathbf{X_k}) = 0$ for all every choice of k distinct variables. In equation (7), it is clear that the k-th order correlation immunity reduces static information leakage $SL(Y;\mathbf{X_k})$ to self static information leakage of Y.

Corollary 3.1 *For an arbitrary choice of* $\mathbf{X_k}$, *the static information leakage* $SL(Y;\mathbf{X_k})$ *is equal to the self static information leakage* $1 - H(Y)$ *if and only if function* $Y = f(\mathbf{X})$ *is k-th order correlation immune.*

A k-th order correlation immune function can still have large static information leakage if the function is unbalanced. Balancing the correlation immune function would give us a *k-resilient function*, which is defined by Chor *et al.* [16] as follows: a function $f(\mathbf{X})$ is k-resilient if every possible output is equally likely to occur when the values of k arbitrary input bits are fixed by an opponent, and the remaining n–k bits are chosen independently at random.

Corollary 3.2 *A function has zero static information leakage of order k if and only if it is a k-resilient function.*

Corollary 3.2 makes it clear that a function with zero static information leakage of order n–1 is an (n–1)-resilient function. Such a function is (n–1)-th order correlation immune. According to Siegenthaler [9], the (n–1)-th order correlation immune functions are non-degenerate affine functions. Therefore, only non-degenerate affine functions have no static information leakage up to order (n–1).

However, functions with a high order of zero static information leakage are not necessarily stronger against statistical analysis than functions with a low order. This is because a high order of zero static information leakage may cause a large static information leakage between the output and the given sum of input variables. For example, a nondegenerate affine function has no static information leakage up to order (n–1). Then trouble arises at $k = n$, where $SL(Y;\sum_k \mathbf{X}|\beta) = 1$ for $\beta = 0, 1$. In fact, there exists a trade-off between the obtainable order of zero static information leakage and the obtainable lowest bound on the static information leakage of output by given sums of input variables. This is discussed in [17].

Introduce the notation $N_{\alpha\beta} = \#\left\{\mathbf{x} : f(\mathbf{x}) = \alpha, \sum_k \mathbf{x} = \beta\right\}$, where $\#\{\cdot\}$ denotes the cardinality of the enclosed set and $\alpha, \beta \in Z_2$. Since the linear function $b(\mathbf{X_k}) = \sum_k \mathbf{X}$ is balanced, $N_{0\beta} + N_{1\beta} = 2^{n-1}$ follows. We can write

$$H\left(Y|\textstyle\sum_k \mathbf{X} = \beta\right) = h\left(\frac{N_{0\beta}}{N_{0\beta} + N_{1\beta}}\right) = h\left(\frac{1}{2} - \frac{|N_{0\beta} - N_{1\beta}|}{2^n}\right), \tag{16}$$

and hence

$$SL\left(Y;\textstyle\sum_k \mathbf{X}|\beta\right) = 1 - h\left(\frac{1}{2} - \frac{|N_{0\beta} - N_{1\beta}|}{2^n}\right). \tag{17}$$

Theorem 4 *Let l_0 and l_1 be two arbitrary integers in the range $0 \le l_0, l_1 \le 2^{n-1}$. If the information leakage $SL(Y; \sum_k \mathbf{X}|\beta)$, $(\beta = 0, 1)$, is limited by*

$$SL\left(Y; \sum_k \mathbf{X}|0\right) \le 1 - h\left(\frac{1}{2} - \frac{l_0}{2^n}\right) \tag{18}$$

and

$$SL\left(Y; \sum_k \mathbf{X}|1\right) \le 1 - h\left(\frac{1}{2} - \frac{l_1}{2^n}\right) \tag{19}$$

then

$$\min\left\{d(f(\mathbf{X}), b(\mathbf{X_k}))\,,\ d\left(f(\mathbf{X}), \overline{b}(\mathbf{X_k})\right)\right\} \ge 2^{n-1} - \frac{l_0 + l_1}{2}\,, \tag{20}$$

where $d(\cdot,\cdot)$ denotes the Hamming distance, and $\overline{b}(\mathbf{X_k})$ denotes the complement of $b(\mathbf{X_k})$.

Proof: Inequalities (18) and (19) are true if and only if $|N_{10} - N_{00}| \le l_0$ and $|N_{01} - N_{11}| \le l_1$, which yields $-(l_0 + l_1) \le N_{01} + N_{10} - (N_{00} + N_{11}) \le l_0 + l_1$. Since $N_{01} + N_{10} + N_{00} + N_{11} = 2^n$, we have $N_{01} + N_{10} \ge 2^{n-1} - (l_0 + l_1)/2$ and $N_{00} + N_{11} \ge 2^{n-1} - (l_0 + l_1)/2$. The $N_{01} + N_{10}$ equals the Hamming distance from $f(\mathbf{X})$ to $b(\mathbf{X_k})$ and the $N_{00} + N_{11}$ equals the distance from $f(\mathbf{X})$ to $\overline{b}(\mathbf{X_k})$. □

Thus, for any function $Y = f(\mathbf{X})$, it is impossible to limit the static information leakage $SL(Y; \sum_k \mathbf{X}|\beta)$, $(\beta = 0, 1)$, unless there are adequate distances from $f(\mathbf{X})$ to the linear function $b(\mathbf{X_k})$ and $\overline{b}(\mathbf{X_k})$. Considering the resistance to static analysis, static information leakage between the output and the sum of input variables is equally undesirable no matter which and how many input variables are added up. To constrain this static information leakage in all cases, it is necessary that a function has adequate distance to all affine functions. The nonlinearity of $f(\mathbf{X})$ is defined as the minimum Hamming distance between $f(\mathbf{X})$ and all affine functions. Obviously high nonlinearity is a necessary (not sufficient) condition for a function to avoid large static information leakage between the output and the sum of input variables.

4 Dynamic information leakage and it relation to cryptographic criteria

Dynamic information leakage measures the vulnerability of a function to differential analysis. We discuss the cause of dynamic information leakage by means of *autocorrelation function.*

Definition 4 *The autocorrelation function of $(-1)^{f(\mathbf{X})}$ is a mapping $\pi(\cdot)$: $Z_2^n \to [-1, 1]$ defined by:*

$$\pi(\Delta\mathbf{X}) = 2^{-n} \sum_{\mathbf{x}} (-1)^{f(\mathbf{x} \oplus \Delta\mathbf{X}) \oplus f(\mathbf{x})}. \tag{21}$$

*For brevity, we call $\pi(\Delta\mathbf{X})$ **the autocorrelation function of** $f(\mathbf{X})$ and $\pi(\Delta\mathbf{x})$ **the autocorrelation coefficient of** $f(\mathbf{X})$, where $\Delta\mathbf{x}$ denotes the value of $\Delta\mathbf{X}$. If $\Delta\mathbf{x} \ne \underline{0}$, $\Delta\mathbf{x}$ is also called the input change pattern. Note that, $\pi(\underline{0}) = 1$.*

Let $\pi(\Delta\mathbf{X_{n-k}}|\Delta\mathbf{x_k})$ be the sub-function of $\pi(\Delta\mathbf{X})$ obtained by fixing $\Delta\mathbf{X_k}$ at $\Delta\mathbf{x_k}$, where $\Delta\mathbf{X_{n-k}}$ denotes the set of variables obtained from $\Delta\mathbf{X}$ with components $\Delta X_{i_1} \Delta X_{i_2} \ldots \Delta X_{i_k}$ removed. Applying all possible value of $\Delta\mathbf{X_{n-k}}$ to the sub-function, we get 2^{n-k} autocorrelation coefficients of $f(\mathbf{X})$. Let $\widehat{r}(\Delta\mathbf{x_k})$ be the absolute value of the average autocorrelation over these 2^{n-k} coefficients, we may write

$$\widehat{r}(\Delta\mathbf{x_k}) = 2^{k-n} \left| \sum_{\Delta\mathbf{x_{n-k}}} \pi(\Delta\mathbf{x_{n-k}}|\Delta\mathbf{x_k}) \right|. \tag{22}$$

Note if $k = n$, $\widehat{r}(\Delta \mathbf{x_k}) = \widehat{r}(\Delta \mathbf{x}) = |\pi(\Delta \mathbf{x})|$.

Theorem 5 With partial average autocorrelation coefficient $\widehat{r}(\Delta \mathbf{x_k})$ given by equation (22), the dynamic information leakage of Y, given input change vector $\Delta \mathbf{x_k}$, satisfies

$$DL(\Delta Y; \Delta \mathbf{X_k} | \Delta \mathbf{x_k}) = 1 - h\left(\frac{1}{2} - \frac{\widehat{r}(\Delta \mathbf{x_k})}{2}\right). \tag{23}$$

In particular if $k = n$,

$$DL(\Delta Y; \Delta \mathbf{X} | \Delta \mathbf{x}) = 1 - h\left(\frac{1}{2} - \frac{|\pi(\Delta \mathbf{x})|}{2}\right). \tag{24}$$

Proof: Suppose $\Delta \mathbf{x_k}$ is given, we define

$$\widehat{N}_0 = \#\{\mathbf{x} \Leftrightarrow \Delta \mathbf{x_{n-k}} \text{ pairs}: \ \Delta Y = f(\mathbf{x} \oplus (\Delta \mathbf{x_k}, \Delta \mathbf{x_{n-k}})) \oplus f(\mathbf{x}) = 0\}, \tag{25}$$

$$\widehat{N}_1 = \#\{\mathbf{x} \Leftrightarrow \Delta \mathbf{x_{n-k}} \text{ pairs}: \ \Delta Y = f(\mathbf{x} \oplus (\Delta \mathbf{x_k}, \Delta \mathbf{x_{n-k}})) \oplus f(\mathbf{x}) = 1\}. \tag{26}$$

For given $\Delta \mathbf{x_k}$, the probability of $\Delta Y = 0$ is $\widehat{N}_0 / \left(\widehat{N}_0 + \widehat{N}_1\right)$. Then we have

$$H(\Delta Y | \Delta \mathbf{X_k} = \Delta \mathbf{x_k}) = h\left(\frac{\widehat{N}_0}{\widehat{N}_0 + \widehat{N}_1}\right) = h\left(\frac{1}{2} - \frac{1}{2}\frac{\left|\widehat{N}_0 - \widehat{N}_1\right|}{\widehat{N}_0 + \widehat{N}_1}\right). \tag{27}$$

Subtracting and adding $\widehat{N}_0$ and $\widehat{N}_1$ yields

$$\widehat{N}_0 - \widehat{N}_1 = \sum_{\Delta \mathbf{x_{n-k}}} \sum_{\mathbf{x}} (-1)^{f(\mathbf{x} \oplus (\Delta \mathbf{x_k}, \Delta \mathbf{x_{n-k}})) \oplus f(\mathbf{x})} = 2^n \sum_{\Delta \mathbf{x_{n-k}}} \pi(\Delta \mathbf{x_{n-k}} | \Delta \mathbf{x_k}) \tag{28}$$

and

$$\widehat{N}_0 + \widehat{N}_1 = 2^{2n-k}. \tag{29}$$

Applying equation (28) and (29) to (27) and then using (22), we get

$$H(\Delta Y | \Delta \mathbf{X_k} = \Delta \mathbf{x_k}) = h\left(\frac{1}{2} - \frac{\widehat{r}(\Delta \mathbf{x_k})}{2}\right). \tag{30}$$

Replacing the right-hand side of equation (30) into (2), we get equation (23). Since $\widehat{r}(\Delta \mathbf{x_n}) = |\pi(\Delta \mathbf{x})|$, equation (24) is deduced from (23) by setting $k = n$. □

It follows from Theorem 5 that $DL(\Delta Y; \Delta \mathbf{X_k} | \Delta \mathbf{x_k}) = 0$ if and only if $\widehat{r}(\Delta \mathbf{x_k}) = 0$, and the increase of $\widehat{r}(\Delta \mathbf{x_k})$ results in the increase of $DL(\Delta Y; \Delta \mathbf{X_k} | \Delta \mathbf{x_k})$. In particular, $DL(\Delta Y; \Delta \mathbf{X} | \Delta \mathbf{x}) = 0$ if and only if $\pi(\Delta \mathbf{x}) = 0$. In other words, the dynamic information leakage between the output and any k ($k < n$) inputs is zero if and only if the autocorrelations of $f(\mathbf{X})$ cancel out over all coefficients $\pi(\Delta \mathbf{x})$ with those k bits of $\Delta \mathbf{x}$ fixed by an arbitrary value. The dynamic information leakage between Y and $\mathbf{X}$ is zero if and only if $Y = f(\mathbf{X})$ is not autocorrelated in any cases. Thus we claim that the dynamic information leakage between Y and any k ($1 \leq k < n$) input variables is caused by the nonvanishing partial average autocorrelations of function $f(\mathbf{X})$. The dynamic information leakage between Y and $\mathbf{X}$ is caused by autocorrelations of $f(\mathbf{X})$.

Cryptanalysis often uses chosen plaintexts. By differentiating the plaintexts, the input changes of a transformation are completely known. So it is supposed that the changes of all input variables are obtainable in differential analysis. We judge the vulnerability of a function to differential analysis by $DL(\Delta Y; \Delta \mathbf{X} | \Delta \mathbf{x})_{\max}$ for $\Delta \mathbf{x} \neq \underline{0}$. A function is secure from the analysis only if the $DL(\Delta Y; \Delta \mathbf{X} | \Delta \mathbf{x})_{\max}$ does not exceed a certain threshold. Notice that small

$DL(\Delta Y;\Delta\mathbf{X}|\Delta\mathbf{x})$ means small $|\pi(\Delta\mathbf{x})|$ (see equation (24)). Being resistant to differential analysis requires that a function have no significant autocorrelation with every input change pattern.

Proposition 2 *A function is affine if and only if its autocorrelation function satisfies* $|\pi(\Delta\mathbf{X})| = 1$.

Proof: Consider $f(\mathbf{X})$ in algebraic normal form. Let $a(\mathbf{X})$ and $g(\mathbf{X})$ be the affine part and the nonlinear part of $f(\mathbf{X})$ respectively, then we have $f(\mathbf{X}) = g(\mathbf{X}) \oplus a(\mathbf{X})$ and $f(\mathbf{X} \oplus \Delta\mathbf{X}) \oplus f(\mathbf{X}) = g(\mathbf{X} \oplus \Delta\mathbf{X}) \oplus g(\mathbf{X}) \oplus \mathbf{c} \cdot \Delta\mathbf{X}$, where $\mathbf{c} \in Z_2^n$ and $\mathbf{c} \cdot \Delta\mathbf{X}$ denotes the dot product of vector $\mathbf{c}$ and $\Delta\mathbf{X}$.

If $f(\mathbf{X})$ is affine, then $f(\mathbf{X} \oplus \Delta\mathbf{X}) \oplus f(\mathbf{X}) = \mathbf{c} \cdot \Delta\mathbf{X}$. This guarantees $|\pi(\Delta\mathbf{X})| = 1$.

Conversely, suppose $|\pi(\Delta\mathbf{X})| = 1$ and $f(\mathbf{X})$ is nonlinear, then the lowest nonlinear order, denoted by m, in $g(\mathbf{X})$ is greater than 1. We have $g(\mathbf{x}) = 0$ for all $\mathbf{x}$ with Hamming weight less than m. There exists an $\Delta\mathbf{x}$ of Hamming weight m such that $g(\Delta\mathbf{x}) = 1$. It is easy to find an $\hat{\mathbf{x}}$ with $wt(\hat{\mathbf{x}}) < m$ and satisfying $wt(\hat{\mathbf{x}} \oplus \Delta\mathbf{x}) < m$. So we obtain

$$g(\mathbf{x} \oplus \Delta\mathbf{x}) \oplus g(\mathbf{x}) = \begin{cases} 1, & \mathbf{x} = \underline{0} \\ 0, & \mathbf{x} = \hat{\mathbf{x}} \oplus \Delta\mathbf{x} \end{cases}. \tag{31}$$

It follows that $f(\mathbf{x} \oplus \Delta\mathbf{x}) \oplus f(\mathbf{x})|_{\mathbf{x}=\underline{0}} \neq f(\mathbf{x} \oplus \Delta\mathbf{x}) \oplus f(\mathbf{x})|_{\mathbf{x}=\hat{\mathbf{x}}\oplus\Delta\mathbf{x}}$. Then we find

$$\pi(\Delta\mathbf{x}) = 2^{-n} \sum_{\mathbf{x}} (-1)^{f(\mathbf{x}\oplus\Delta\mathbf{x})\oplus f(\mathbf{x})} \neq \pm 1 . \tag{32}$$

This contradicts our previous assumption that $|\pi(\Delta\mathbf{X})| = 1$ and $f(\mathbf{X})$ is nonlinear. So $f(\mathbf{X})$ must be affine. □

Proposition 2 points out that affine functions and only affine functions have maximum autocorrelation with every input change pattern. Such functions have dynamic information leakage $DL(\Delta Y;\Delta\mathbf{X}|\Delta\mathbf{x}) = 1$ for all $\Delta\mathbf{x} \in Z_2^n$. As a result, affine functions are most vulnerable to differential analysis. On the other hand, a function has no autocorrelation with every input change pattern (i.e., $\pi(\Delta\mathbf{x}) = 0$ for all $\Delta\mathbf{x} \neq \underline{0}$) if and only if it is bent [10]. Such a function has no dynamic information leakage by whatever given input change pattern (i.e., $DL(\Delta Y;\Delta\mathbf{X}|\Delta\mathbf{x}) = 0$ for all $\Delta\mathbf{x} \neq \underline{0}$). So bent functions are least vulnerable to differential analysis.

The propagation criterion is closely related to the dynamic information leakage of Y by some given input change patterns. Function $f(\mathbf{X})$ satisfies Propagation Criterion of degree k (PC-k) if the output changes with a probability of 1/2 whenever m ($0 < m \leq k$) bits of input are complemented. Using the notation of autocorrelation function, we may represent the PC-k by $\pi(\Delta\mathbf{x}) = 0$ for all $\Delta\mathbf{x}$, $0 < wt(\Delta\mathbf{x}) \leq k$, where $wt(\cdot)$ is an abbreviation of Hamming weight. By equation (24), PC-k is further equivalent to $DL(\Delta Y;\Delta\mathbf{X}|\Delta\mathbf{x}) = 0$ for all $\Delta\mathbf{x}$, $0 < wt(\Delta\mathbf{x}) \leq k$.

In the differential analysis of functions, we assume that computing the probability of the output change by complementing one bit of input is as useful as computing the same probability by complementing k ($1 < k \leq n$) bits of input. Hence the dynamic information leakage of Y by every given input change pattern is equally undesirable. In the information theoretic point of view, the nature of propagation criterion (including SAC) is to require zero dynamic information leakage of Y by certain $\mathbf{X}$ change patterns (such as $0 < wt(\Delta\mathbf{x}) \leq k$) regardless of the dynamic information leakage of Y by other $\mathbf{X}$ change patterns. Consequently, functions may be overly

restricted and turn out to be vulnerable to differential analysis. For example, when the input dimension n is odd, the highest PC degree is n–1, and all PC-(n–1) fulfilling functions have autocorrelation coefficient $r(\underline{1}) = \pm 1$, where $\underline{1}$ denotes the vector of which all the components taking the value 1. These functions are vulnerable to differential analysis because knowledge of input pattern $\underline{1}$ completely gives away the output change (i.e., $DL(\Delta Y; \Delta \mathbf{X}|\underline{1}) = 1$). This input change pattern $\underline{1}$ happens to be a linear structure defined by Evertse [18] and Meier & Staffelbach [10].

A function resistant to differential analysis is allowed to have a small amount of information leakage between the output change and the 1–bit input change patterns, thus it may not satisfy any degree of propagation criterion. In fact it is the maximum dynamic information leakage $DL(\Delta Y; \Delta \mathbf{X}|\Delta \mathbf{x})_{\max}$ (for $\Delta \mathbf{x} \neq \underline{0}$) that determines the vulnerability to differential analysis. The propagation criterion in general does not care the maximum dynamic information leakage, and therefore does not reflect the resistance to differential analysis. So a cryptographically strong function does not necessarily satisfy the propagation criterion.

In many cryptographic applications balanced functions are required. Modified bent functions are popular in these cases. Considering the resistance to differential analysis, we suggest the modification be done based on the idea of no significant information leakage between the change of output and every input change pattern. Otherwise, suppose that a bent function is modified for the purposes of 0–1 balance and PC fulfilling such that the highest PC degree is k, there might exist a large value of $DL(\Delta Y; \Delta \mathbf{X}|\Delta \mathbf{x})$ for certain $\Delta \mathbf{x}$, $wt(\Delta \mathbf{x}) > k$. This large dynamic information leakage can make the function vulnerable to differential analysis.

Higher order strict avalanche criterion by Forré is related to information leakage of the sub-functions of $f(\mathbf{X})$. According to Lloyd[19], $f(\mathbf{X})$ satisfies SAC of order k if and only if every sub-function obtained by keeping k input variables constant fulfills SAC. A sub-function of $f(\mathbf{X})$ obtained by keeping k input variables constant can be represented by $Y' = f(\mathbf{X}_{\mathbf{n-k}}|\mathbf{x}_{\mathbf{k}})$. Using the notation of entropy, we can easily prove the sub-function fulfills SAC if and only $H(\Delta Y'|\Delta \mathbf{X}_{\mathbf{n-k}} = \Delta \mathbf{x}_{\mathbf{n-k}}) = 1$ for all $\Delta \mathbf{x}_{\mathbf{n-k}}$, $wt(\Delta \mathbf{x}_{\mathbf{n-k}}) = 1$. By Definition 1, above expression is equivalent to $DL(\Delta Y'; \Delta \mathbf{X}_{\mathbf{n-k}}|\Delta \mathbf{x}_{\mathbf{n-k}}) = 0$ for all $\Delta \mathbf{x}_{\mathbf{n-k}}$, $wt(\Delta \mathbf{x}_{\mathbf{n-k}}) = 1$. Clearly, if $f(\mathbf{X})$ satisfies SAC of order k, all the sub-functions obtained by keeping k input variables constant have no information leakage between the changes of their outputs and every 1-bit input change pattern, and vice versa.

The higher order SAC requires all sub-functions satisfies SAC (or PC-1) in order to guarantee that a function can not be roughly approximated by its sub-functions and no sub-function can be roughly approximated by its further sub-functions. By doing this, however, higher order SAC may overly restricted functions and make them weak to differential analysis. For example, it is proved in [13, Th.10] that all functions satisfying SAC of order (n–2) or (n–3) must be quadratic. Notice that all autocorrelation coefficients of quadratic functions take the value 0 or ± 1 [20, Th.5]. If the input dimension n is odd, the quadratic functions can not be bent. Consequently there is a large information leakage $DL(\Delta Y; \Delta \mathbf{X}|\Delta \mathbf{x})$ for certain input change pattern. These functions are vulnerable to differential analysis. As a matter of fact, a little information leakage between the output change and the 1–bit input change patterns of a sub-function will not result in a good and simpler approximation of the sub-function. Allowing a small information leakage between the output change and 1–bit input change patterns could loosen the restriction on the original function without reducing its cryptographic strength. Thus a cryptographically good function may not strictly satisfy higher order SAC.

5 Conclusion

Information leakage of a function measures, in terms of entropy, the predictability of a function. The measurement is carried out both in static and dynamic ways. The static and dynamic information leakage reflect the vulnerability of a cryptographic transformation to statistical analysis. Each type of information leakage measures one aspect of the vulnerability. Generally, a cryptographically strong function should have no significant information leakage by both static and dynamic measurement. However, when minimizing all types of information leakage, conflicts arise. At this time it is not clear, when optimizing, what the approriate cost function should be. In most cases, a desirable function results from a trade-off between the abilities to withstand static and dynamic analyses.

References

[1] W. Meier and O. Staffelbach. Fast Correlation Attacks on Certain Stream Ciphers. *Journal of Cryptology*, Vol.1, No.3:159–176, 1989.

[2] E. Biham and A. Shamir. Differential Cryptanalysis of DES-like Cryptosystems. *Advances in Cryptology, Proceedings of Crypt'90, Springer-Verlag, Berlin*, pages 1–21, 1991.

[3] M. Matsui. Linear Cryptanalysis Method for DES Cipher. *Advances in Cryptology, Proceedings of Eurocrypt'93, Springer-Verlag, Berlin.*

[4] Réjane Forré. Methods and Instruments for Designing S-Boxes. *Journal of Cryptology*, Vol.2, No.3:115–130, 1990.

[5] M.H. Dawson and S.E. Tavares. An Expanded Set of S-box Design Criteria Based on Information Theory and its Relation to Differential Attacks. *Advances in Cryptology, Proceedings of Eurocrypt'91, Springer-Verlag, Berlin*, pages 352–365, 1992.

[6] M. Sivabalan, S.E. Tavares, and L.E. Peppard. On the Design of SP Networks from an Information Theoretic Point of View. *Advances in Cryptology, Proceedings of Crypt'92, Springer-Verlag, Berlin*, pages 260–279, 1993.

[7] J.B. Kam and G.I. Davida. Structured Design of Substitution-Permutation Encryption Networks. *IEEE Transaction on Computers*, C-28:747–753, 1979.

[8] A.F. Webster and S.E. Tavares. On the Design of S-boxes . *Advances in Cryptology, Proceedings of Crypt'85, Springer-Verlag, Berlin*, pages 523–534, 1986.

[9] T. Siegenthaler. Correlation-Immunity of Nonlinear Combining Functions for Cryptographic Applications. *IEEE Trans. on Info. Theory*, Vol.IT-30, No.5:776–780, Sept. 1984.

[10]W. Meier and O. Staffelbach. Nonlinearity Criteria for Cryptographic Functions. *Advances in Cryptology, Proceedings of Eurocrypt'89, Springer-Verlag, Berlin*, pages 549–562, 1990.

[11]C. M. Adams and S.E. Tavares. The Use of Bent Sequences to Achieve Higher-Order Strict Avalanche Criterion in S-Box Design. *Techn. Rept. TR 90-013, Dept. of Electrical Engineering, Queen's University, Kingston, Ontario*, 1990.

[12]C. M. Adams. On Immunity Against Biham and Shamir's Differential Cryptanalysis. *Information Processing Letters*, Vol.41, No.2:77–80, 1992.

[13]B. Preneel, W. V. Leekwijk, L. V. Linden, R. Govaerts, and J. Vandewalle. Propagation Characteristics of Boolean Functions. *Advances in Cryptology, Proceedings of Eurocrypt'90, Springer-Verlag, Berlin*, pages 161–173, 1991.

[14]Réjane Forré. The Strict Avalanche Criterion: Spectral Properties of Boolean Functions and an Extended Definition. *Advances in Cryptology, Proceedings of Crypt'88, Springer-Verlag, Berlin*, pages 450–468, 1989.

[15]T.M. Cover and J.A. Thomas. *Elements of Information Theory*. John Wiley & Sons, Inc., 1991.

[16]B. Chor, O. Goldreich, J. Hastad, J. Friedman, and R. Smolensky S. Rudich. The Bit Extraction Problem or t-resilient Functions. *Proc. 26th IEEE Symposium on Foundations of Computer Science*, pages 396–407, 1985.

[17]M. Zhang, S. E. Tavares, and L. L. Campbell. Information Leakage of Boolean Functions and its Relationship to Other Cryptographic Criteria . *Techn. Rept. Dept. of Electrical and Computer Engineering, Queen's University, Kingston, Ontario*, 1994.

[18]J.-H. Evertse. Linear Structures in the Block Ciphers. *Advances in Cryptology, Proceedings of Eurocrypt'87, Springer-Verlag, Berlin*, pages 249–266, 1988.

[19]Sheelagh Lloyd. Counting Functions Satisfying a Higher Order Strict Avalanche Criterion. *Advances in Cryptology, Proceedings of Eurocrypt'89, Springer-Verlag, Berlin*, pages 63–74, 1990.

[20]B. Preneel, R. Govaerts, and J. Vandewalle. Boolean Functions Satisfying Higher Order Propagation Criteria. *Advances in Cryptology, Proceedings of Eurocrypt'91, Springer-Verlag, Berlin*, pages 141–152, 1992.

How to Better the SAC

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

January 25, 1994

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 is due to Webster and Tavares, and appeared first in 1985 [Web85, WT86]:

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 $t \geq s$ 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 $f_1, \ldots, f_m$ 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 $\gamma_1, \ldots, \gamma_{k-1}$ 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 $\gamma_1, \ldots, \gamma_k$ 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, $\psi_1(x) = f_1(xA), \ldots, \psi_m(x) = f_m(xA)$ 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 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 Commnications Security*, pages 172 – 182. The Association for Computing Machinery, New York, 1993.

[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 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.