COUNTING FUNCTIONS SATISFYING A HIGHER ORDER STRICT AVALANCHE CRITERION

Sheelagh Lloyd

Hewlett-Packard Laboratories
Filton Road, Stoke Gifford
Bristol, ENGLAND
BS12 6QZ

I . INTRODUCTION

The strict avalanche criterion was introduced by Webster and Tavares [3] in order to combine the ideas of completeness and the avalanche effect. A cryptographic transformation is complete if each output bit depends on all the input bits, and it exhibits the avalanche effect if an average of one half of the output bits change whenever a single input bit is complemented. To fulfil the strict avalanche criterion, each output bit should change with probability one half whenever a single input bit is complemented. This means, in particular, that there is no good lower order (fewer bits) approximation to the function. This is clearly a desirable cryptographic property since such an approximation would enable a corresponding reduction in the amount of work needed for an exhaustive search.

The notion of strict avalanche criterion was recently extended by Forré to consider subfunctions obtained from the original function by keeping one or more input bits constant. This is also important cryptographically because, in a chosen plaintext attack, the cryptanalyst could arrange for certain input bits to be kept constant. Forré defined the strict avalanche criterion of order m, with order 0 being the original strict avalanche criterion, and made a conjecture, supported by experimental evidence, concerning the number of functions satisfying a higher order strict avalanche criterion.

J.J. Quisquater and J. Vandewalle (Eds.): Advances in Cryptology - EUROCRYPT '89, LNCS 434, pp. 63-74, 1990.

In this paper, we shall first present unified definitions of the three concepts of completeness, the avalanche effect and the strict avalanche criterion. We shall then show how Forré's definition of the higher order strict avalanche criterion may be simplified, and then use this simplified form to prove her conjecture.

II . DEFINITIONS

In this section we shall discuss more fully the ideas of completeness, the avalanche effect and the strict avalanche criterion. We shall present these three criteria in a unified framework, in order to highlight the connections between them.

Let $f : \mathbf{Z}_2^n \rightarrow \mathbf{Z}_2^m$ $(n \geq m)$ be a cryptographic transformation. Then f is said to be complete [2] if and only if for each pair (i, j), $1 \leq i \leq n$, $1 \leq j \leq m$, there exists a pair of n-bit vectors $\underline{x}$ and $\underline{x}'$ such that $\underline{x}$ and $\underline{x}'$ differ only in bit i, and $f(\underline{x})$ and $f(\underline{x}')$ differ in at least bit j. This property ensures that each output bit depends on all the input bits. If some output bits depended on only a few input bits, then, by observing a significant number of input-output pairs, a cryptanalyst might be able to detect these relations and use this information to aid the search for the key.

Webster and Tavares [3] pointed out that this condition can be restated as follows. Let us fix i, $1 \leq i \leq n$, and write $\underline{c}_i$ for the n-bit vector with a 1 in the ith position and 0 elsewhere. Now consider the set of m-bit vectors $f(\underline{x}) \oplus f(\underline{x} \oplus \underline{c}_i)$ as $\underline{x}$ ranges over $\mathbf{Z}_2^n$. (These are called "avalanche vectors" in [3]). For each j, $1 \leq j \leq m$, at least one of these vectors has a 1 in the jth position. So, if we add these vectors together (as elements of $\mathbf{Z}^m$ rather than elements of $\mathbf{Z}_2^m$), all components should be greater than 0. Thus we have the following definition.

Definition 2.1 Let $f : \mathbf{Z}_2^n \rightarrow \mathbf{Z}_2^m$ be a cryptographic transformation. Then f is complete if and only if

$$\sum_{\underline{x} \in \mathbf{Z}_2^n} f(\underline{x}) \oplus f(\underline{x} \oplus \underline{c}_i) > (0, .., 0) \qquad \text{for all } i,\ 1 \leq i \leq n$$

where both the summation and the greater-than are component-wise over $\mathbf{Z}^n$.

Forré considers only the case $m = 1$, and, in this case, we see that $f : \mathbf{Z}_2^n \rightarrow \mathbf{Z}_2$ is complete if and only if

$$\sum_{\underline{x} \in \mathbf{Z}_2^n} f(\underline{x}) \oplus f(\underline{x} \oplus \underline{c}_i) > 0 \qquad \text{for all } i,\ 1 \leq i \leq n.$$

We consider now the avalanche effect. A function exhibits the avalanche effect if and only if an average of one half of the output bits change whenever a single input bit is changed. This may be formalised [3] by considering again the "avalanche vectors" $f(\underline{x}) \oplus f(\underline{x} \oplus \underline{c}_i)$ as $\underline{x}$ varies over $\mathbf{Z}_2^n$. The bits of these vectors are referred to as "avalanche variables". Then f is said to exhibit the avalanche effect if and only if, for each i, $1 \leq i \leq n$, one half of the avalanche variables are equal to 1.

We shall write this condition as follows. For each i, there are 2^n avalanche vectors, and hence $m2^n$ avalanche variables. If exactly half of them are 1, then their sum must be $m2^{n-1}$. Thus we have the definition below.

Definition 2.2 Let $f : \mathbf{Z}_2^n \rightarrow \mathbf{Z}_2^m$ be a cryptographic transformation. Let w denote the Hamming weight function. Then f exhibits the avalanche effect if and only if

$$\sum_{\underline{x} \in \mathbf{Z}_2^n} w(f(\underline{x}) \ominus f(\underline{x} \oplus \underline{c}_i)) = m2^{n-1} \qquad \text{for all } i,\ 1 \leq i \leq n.$$

In the case $m = 1$, w is essentially the identity, so we see that $f : \mathbf{Z}_2^n \rightarrow \mathbf{Z}_2$ exhibits the avalanche effect if and only if

$$\sum_{\underline{x} \in \mathbf{Z}_2^n} f(\underline{x}) \ominus f(\underline{x} \oplus \underline{c}_i) = 2^{n-1} \qquad \text{for all } i,\ 1 \leq i \leq n.$$

Note that, in this case, if f exhibits the avalanche effect, then f must automatically be complete.

Finally, we consider the strict avalanche criterion. For a function to satisfy this, each output bit should change with probability one half whenever a single input bit changes. This can be written as below (see, e.g. [3]).

Definition 2.3 Let $f : \mathbf{Z}_2^n \rightarrow \mathbf{Z}_2^m$ be a cryptographic transformation. Then f satisfies the strict avalanche criterion if and only if

$$\sum_{\underline{x} \in \mathbf{Z}_2^n} f(\underline{x}) \ominus f(\underline{x} \oplus \underline{c}_i) = (2^{n-1}, .., 2^{n-1}) \qquad \text{for all } i,\ 1 \leq i \leq n.$$

In the case $m = 1$, we see that the strict avalanche criterion is exactly the same as the avalanche criterion.

It is clear that a necessary and sufficient condition for a function $f : \mathbf{Z}_2^n \rightarrow \mathbf{Z}_2^m$ to satisfy the strict avalanche criterion is that the m functions which specify the behaviour of each bit should all satisfy the strict avalanche criterion. We are, therefore, justified in considering only the case $m = 1$ in what follows.

III . PRELIMINARIES

Let f be a function from $\mathbf{Z}_2^n$ to $\mathbf{Z}_2$. It turns out to be convenient to consider instead the function $\hat{f}$ defined by $\hat{f}(\underline{x}) = (-1)^{f(\underline{x})}$ which has the same domain as f, but takes values in $\{1, -1\}$ rather than in $\mathbf{Z}_2$. We shall use the following characterisation of functions satisfying the strict avalanche criterion (SAC) due to Forré.

Theorem 3.1 [1] A function $f : Z_2^n \rightarrow Z_2$ satisfies the SAC if and only if

$$\sum_{\underline{x} \in Z_2^n} \hat{f}(\underline{x}) \hat{f}(\underline{x} \oplus \underline{c}) = 0$$

for all $\underline{c} \in Z_2^n$ with Hamming weight 1, where $\hat{f}(\underline{x}) = (-1)^{f(\underline{x})}$.

The definition of the higher order SAC is as follows:

Definition 3.2 [1] A function $f : Z_2^n \rightarrow Z_2$ satisfies the SAC of order m, where $1 \leq m \leq (n-2)$ if and only if

(a) any function obtained from f by keeping m of its input bits constant satisfies the SAC (for any choice of the positions and of the values of the constant bits)

and

(b) f satisfies the SAC of order $m-1$.

Note that it would be impossible for a function to satisfy the SAC of order $(n-1)$, since this would be equivalent to finding a function $g : Z_2 \rightarrow Z_2$ satisfying the SAC. Using Theorem 3.1, this would mean that $\hat{g}(0)\hat{g}(1) = 0$ which is impossible, since both $\hat{g}(0)$ and $\hat{g}(1)$ have values in $\{1, -1\}$.

IV . SIMPLIFICATION

In this section we shall show that condition (b) of Definition 3.2 is not necessary. For ease of notation, we introduce the following terminology.

Definition 4.1 A function $f : Z_2^n \rightarrow Z_2$ satisfies the partial strict avalanche criterion (PSAC) of order m, where $0 \leq m \leq (n-2)$ if and only if any function obtained from f by keeping m of its input bits constant satisfies the SAC (for any choice of the positions and of the values of the constant bits).

Note that the PSAC of order 0 is exactly the same as the SAC (of order 0) and that a function satisfies the SAC of order m if and only if it satisfies both the PSAC of order m and the SAC of order $(m-1)$.

We shall show that the PSAC of order m alone is sufficient to ensure the SAC of order m. We shall first prove a result concerning the PSAC.

Lemma 4.2 Let f be a function from Z_2^n to Z_2 satisfying the PSAC of order m $(1 \leq m \leq (n-2))$. Then f satisfies the PSAC of order $(m-1)$.

Proof

Let g be a function obtained from f by keeping $(m-1)$ input bits fixed. We must show that g satisfies the SAC. By Theorem 3.1, we need to show that

$$S = \sum_{\underline{x} \in Z_2^{n-m+1}} \hat{g}(\underline{x})\hat{g}(\underline{x} \oplus \underline{c}) = 0$$

for all $\underline{c} \in Z_2^{n-k}$ with Hamming weight 1. Without loss of generality, we may assume that $\underline{c} = (0, .., 0, 1)$. Now, since $(n-m+1) > 1$, we know that $\underline{x}$ and $\underline{x} \oplus \underline{c}$ agree on the first bit, so we may split the sum up into those terms where the first bit of $\underline{x}$ is 0, and those where it is 1.

$$S = \sum_{\underline{y} \in Z_2^{n-m}} \hat{g}_0(\underline{y})\hat{g}_0(\underline{y} \oplus \underline{c}') + \sum_{\underline{y} \in Z_2^{n-m}} \hat{g}_1(\underline{y})\hat{g}_1(\underline{y} \oplus \underline{c}')$$

where g_0, g_1 denote the functions obtained from g by setting the first input bit to 0, 1 respectively, and $\underline{c}'$ denotes the vector of length $(n-m)$ obtained from $\underline{c}$ by deleting the first bit. Now both g_0 and g_1 are obtained from g by fixing one bit, and hence from f by fixing m bits, so by our assumption, they satisfy the SAC. Hence by Theorem 3.1, both the sums above are zero, and so $S = 0$ as required. We have therefore proved the result.

We are now able to prove the following theorem.

Theorem 4.3 A function $f : Z_2^n \rightarrow Z_2$ satisfies the Strict Avalanche Criterion (SAC) of order m if and only if any function obtained from f by keeping m of its input bits constant satisfies the SAC (for any choice of the positions and of the values of the constant bits)

Proof

In other words, we must prove that f satisfies the SAC of order m if and only if it satisfies the PSAC of order m. Clearly, by the definitions of the SAC and PSAC, we know that if f satisfies the SAC of order m, then it satisfies the PSAC of order m. Hence we need only prove that if f satisfies the PSAC of order m, then it satisfies the SAC of order m.

The proof is by induction. The base step is trivial, since, as we have already remarked, the PSAC of order 0 is identical to the SAC (of

order 0). So let us assume the result for $m = k$, and try to prove it for $m = k+1$. Suppose that f satisfies the PSAC of order $(k+1)$. We must show that f satisfies the SAC of order $(k+1)$. By Lemma 4.2, f satisfies the PSAC of order k. By the inductive hypothesis, therefore, f satisfies the SAC of order k. Hence, by the definition of the SAC, f satisfies the SAC of order $(k+1)$.

V . COUNTING FUNCTIONS

In this section, we shall prove a result conjectured by Forré [1] in the light of experimental results.

Theorem 5.1 Let $n \in \mathbf{Z}$ be such that $n \geq 2$. Then the number of functions $f : \mathbf{Z}_2^n \rightarrow \mathbf{Z}_2$ satisfying the SAC of order $(n-2)$ is 2^{n+1}.

We shall prove this by giving an explicit form for the functions satisfying the SAC of order $(n-2)$.

Lemma 5.2 Suppose that $n \in \mathbf{Z}$, $n \geq 2$ and $f : \mathbf{Z}_2^n \rightarrow \mathbf{Z}_2$. Then f satisfies the SAC of order $(n-2)$ if and only if for all $S \subseteq \{1, 2, .., n\}$,

$$\hat{f}(\underline{e}_S) = (-1)^{\frac{|S|(|S|-1)}{2}} (\hat{f}(\underline{0}))^{(|S|+1)} \prod_{r \in S} \hat{f}(\underline{e}_{\{r\}})$$

where $\underline{e}_S$ denotes the element of $\mathbf{Z}_2^n$ which satisfies $e_i = 1 \iff i \in S$ and as before, $\hat{f}(\underline{x}) = (-1)^{f(\underline{x})}$.

Proof

By Theorem 4.3 and Theorem 3.1, f satisfies the SAC of order $(n-2)$ if and only if

$$\sum_{\underline{x} \in \mathbf{Z}_2^2} \hat{g}(\underline{x}) \hat{g}(\underline{x} \oplus \underline{c}) = 0$$

for all $\underline{c} \in \mathbf{Z}_2^2$ with Hamming weight 1, and all functions g obtained from f by fixing $(n-2)$ bits. There are two choices for $\underline{c}$, namely $\underline{c} = (1, 0)$ or $\underline{c} = (0, 1)$.

In fact, these two give rise to the same equation as follows.

$$\sum_{\underline{x} \in \mathbf{Z}_2^2} \hat{g}(\underline{x})\hat{g}(\underline{x} \oplus (1,0)) = 2(\hat{g}(0,0)\hat{g}(1,0) + \hat{g}(0,1)\hat{g}(1,1)) = 0$$

and

$$\sum_{\underline{x} \in \mathbf{Z}_2^2} \hat{g}(\underline{x})\hat{g}(\underline{x} \oplus (0,1)) = 2(\hat{g}(0,0)\hat{g}(0,1) + \hat{g}(1,0)\hat{g}(1,1)) = 0.$$

But all $\hat{g}(\underline{x})$ have the value ± 1, so we may multiply the second equation through by $\hat{g}(0,1)\hat{g}(1,0)$ to obtain the first equation. Hence we have essentially one equation for each function g. This equation may be written as

$$\hat{g}(1,1) = -\hat{g}(0,0)\hat{g}(0,1)\hat{g}(1,0).$$

For example, if g were obtained from f by setting the last $(n-2)$ bits to 0, then this equation becomes, in terms of values of f

$$\hat{f}(1,1,0,..,0) = -\hat{f}(0,..,0)\hat{f}(0,1,0,..,0)\hat{f}(1,0,..,0).$$

In general, the equation defines the value of $\hat{f}$ at a point $\underline{x}$ of Hamming weight $(w+2)$ in terms of the values of $\hat{f}$ at points with Hamming weight $(w+1)$ and w. This means that we can express the value of f at all points of Hamming weight greater than or equal to 1 in terms of the values of f at points with Hamming weight 0 or 1. Of course, in general, there will be more than one equation defining the value of $f(\underline{x})$, so we will need to check that these equations are consistent. Each equation corresponds to a set $S \subseteq \{1,2,..,n\}$ with $|S| \geq 2$ together with a pair $i,j \in S$, $i \neq j$. This corresponds to the function obtained from f by setting all but the ith and jth bits to agree with $\underline{e}_S$. Then the equation obtained is (writing T for $S \setminus \{i,j\}$)

$$\hat{f}(\underline{e}_S) = -\hat{f}(\underline{e}_T)\hat{f}(\underline{e}_{T \cup \{i\}})\hat{f}(\underline{e}_{T \cup \{j\}})$$

We shall prove the result by induction on the size of the set S. The base step consists of the cases in which $|S| \leq 1$. We may subdivide these cases

into $S = \emptyset$ and $S = \{r\}$ for some $r \in \{1, .., n\}$. In the first case, we want to show that

$$\hat{f}(\underline{0}) = (-1)^0(\hat{f}(\underline{0}))^1$$

which is clearly true, and in the second case that

$$\hat{f}(\underline{e}_{\{r\}}) = (-1)^0(\hat{f}(\underline{0}))^2\hat{f}(\underline{e}_{\{r\}})$$

which is also clearly true.

Now let us assume that the result is true for all T with $|T| \leq k$ $(k \geq 1)$ and let $|S| = k + 1$. Then we obtain a set of equations

$$\hat{f}(\underline{e}_S) = -\hat{f}(\underline{e}_T)\hat{f}(\underline{e}_{T\cup\{i\}})\hat{f}(\underline{e}_{T\cup\{j\}})$$

for each distinct pair $i, j \in S$, where $T = S \setminus \{i, j\}$. Now since $|T| = k-1$ and $|T \cup \{i\}| = |T \cup \{j\}| = k$, we may apply the induction hypothesis and obtain

$$\hat{f}(\underline{e}_T) = (-1)^{\frac{(k-1)(k-2)}{2}}(\hat{f}(\underline{0}))^k \prod_{r\in T} \hat{f}(\underline{e}_{\{r\}})$$

$$\hat{f}(\underline{e}_{T\cup\{i\}}) = (-1)^{\frac{k(k-1)}{2}}(\hat{f}(\underline{0}))^{(k+1)} \prod_{r\in T\cup\{i\}} \hat{f}(\underline{e}_{\{r\}})$$

$$\hat{f}(\underline{e}_{T\cup\{j\}}) = (-1)^{\frac{k(k-1)}{2}}(\hat{f}(\underline{0}))^{(k+1)} \prod_{r\in T\cup\{j\}} \hat{f}(\underline{e}_{\{r\}})$$

Now for each $r \in T$, the term $\hat{f}(\underline{e}_{\{r\}})$ will occur once in each of those expressions, and so exactly three times in the expression for $\hat{f}(\underline{e}_S)$, while the terms $\hat{f}(\underline{e}_{\{i\}})$ and $\hat{f}(\underline{e}_{\{j\}})$ occur exactly once each in the expression for $\hat{f}(\underline{e}_S)$. Furthermore, the terms $(-1)^{\frac{k(k-1)}{2}}$ and $(\hat{f}(\underline{0}))^{k+1}$ both occur twice in the expression and so cancel out, leaving

$$\hat{f}(\underline{e}_S) = (-1)^{1+\frac{(k-1)(k-2)}{2}}(\hat{f}(\underline{0}))^k \prod_{r\in S} \hat{f}(\underline{e}_{\{r\}})$$

Now

$$1 + \frac{(k-1)(k-2)}{2} = \frac{k^2 - 3k + 4}{2} \equiv \frac{k(k+1)}{2} (\mathrm{mod} 2)$$

and $k \equiv (k+2)(\mathrm{mod}2)$, so

$$\hat{f}(\underline{e}_S) = (-1)^{\frac{k(k+1)}{2}} (\hat{f}(\underline{0}))^{(k+2)} \prod_{r \in S} \hat{f}(\underline{e}_{\{r\}})$$

as required.

Example

Let us consider the simple case of $n = 3$. We want to discover which functions f satisfy the SAC of order $(n-2) = 1$. Then as at the beginning of the proof of the lemma, we must have

$$\hat{g}(1,1) = -\hat{g}(0,0)\hat{g}(0,1)\hat{g}(1,0)$$

for all g obtained from f by fixing one bit. Now there are six such functions g, giving us the following equations.

$$\begin{aligned}
\hat{f}(0,1,1) &= -\hat{f}(0,0,0)\hat{f}(0,0,1)\hat{f}(0,1,0) \\
\hat{f}(1,1,1) &= -\hat{f}(1,0,0)\hat{f}(1,0,1)\hat{f}(1,1,0) \\
\hat{f}(1,0,1) &= -\hat{f}(0,0,0)\hat{f}(0,0,1)\hat{f}(1,0,0) \\
\hat{f}(1,1,1) &= -\hat{f}(0,1,0)\hat{f}(0,1,1)\hat{f}(1,1,0) \\
\hat{f}(1,1,0) &= -\hat{f}(0,0,0)\hat{f}(0,1,0)\hat{f}(1,0,0) \\
\hat{f}(1,1,1) &= -\hat{f}(0,0,1)\hat{f}(0,1,1)\hat{f}(1,0,1)
\end{aligned}$$

Rearranging these, we obtain

$$\begin{aligned}
\hat{f}(0,1,1) &= -\hat{f}(0,0,0)\hat{f}(0,0,1)\hat{f}(0,1,0) \\
\hat{f}(1,0,1) &= -\hat{f}(0,0,0)\hat{f}(0,0,1)\hat{f}(1,0,0) \\
\hat{f}(1,1,0) &= -\hat{f}(0,0,0)\hat{f}(0,1,0)\hat{f}(1,0,0) \\
\hat{f}(1,1,1) &= -\hat{f}(0,0,1)\hat{f}(0,1,0)\hat{f}(1,0,0).
\end{aligned}$$

So we see that the 16 functions $f_1, ..f_{16} : \mathbf{Z}_2^3 \rightarrow \mathbf{Z}_2$ satisfying the SAC of order 1 are the following.

$\underline{x}$	000	001	010	100	011	101	110	111
$f_1(\underline{x})$	0	0	0	0	1	1	1	1
$f_2(\underline{x})$	0	0	0	1	1	0	0	0
$f_3(\underline{x})$	0	0	1	0	0	1	0	0
$f_4(\underline{x})$	0	0	1	1	0	0	1	1
$f_5(\underline{x})$	0	1	0	0	0	0	1	0
$f_6(\underline{x})$	0	1	0	1	0	1	0	1
$f_7(\underline{x})$	0	1	1	0	1	0	0	1
$f_8(\underline{x})$	0	1	1	1	1	1	1	0
$f_9(\underline{x})$	1	0	0	0	0	0	0	1
$f_{10}(\underline{x})$	1	0	0	1	0	1	1	0
$f_{11}(\underline{x})$	1	0	1	0	1	0	1	0
$f_{12}(\underline{x})$	1	0	1	1	1	1	0	1
$f_{13}(\underline{x})$	1	1	0	0	1	1	0	0
$f_{14}(\underline{x})$	1	1	0	1	1	0	1	1
$f_{15}(\underline{x})$	1	1	1	0	0	1	1	1
$f_{16}(\underline{x})$	1	1	1	1	0	0	0	0

Proof of Theorem 5.1

By Lemma 5.2, the set of functions $f : \mathbf{Z}_2^n \rightarrow \mathbf{Z}_2$ satisfying the SAC of order $(n-2)$ is the same as the set of functions $f : \mathbf{Z}_2^n \rightarrow \mathbf{Z}_2$ satisfying the set of equations

$$\hat{f}(\underline{e}_S) = (-1)^{\frac{|S|(|S|-1)}{2}} (\hat{f}(\underline{0}))^{(|S|+1)} \prod_{r \in S} \hat{f}(\underline{e}_{\{r\}})$$

where the notation is as in the statement of Lemma 5.2. Now, since any element in $\mathbf{Z}_2^n$ can be written as $\underline{e}_S$ for exactly one set $S \subseteq \{1, 2, ..., n\}$,

this determines the value of $g(\underline{x})$ for all values of $\underline{x}$ with Hamming weight greater than 1 in terms of the values of $g(\underline{x})$ for values of $\underline{x}$ with Hamming weight less than or equal to 1. In other words, if we choose values for $g(\underline{0})$ and for $g(\underline{e}_{\{r\}})$ for all $r \in \{1, .., n\}$, then g is completely determined on the whole of $\mathbf{Z}_2^n$. Thus there are 2^{n+1} ways to choose such a function, and so the size of the set of these functions is 2^{n+1}.

We have the following immediate corollary.

Corollary 5.3 The proportion of functions $f : \mathbf{Z}_2^n \to \mathbf{Z}_2$ satisfying the SAC of order $(n-2)$ is $2^{n+1}/2^{(2^n)}$.

VI . CONCLUSIONS

We have presented a simplified definition of the higher order strict avalanche criterion and showed its equivalence with the original. We have then used this to calculate the number of n-bit binary functions which satisfy the strict avalanche criterion of order $(n-2)$.

REFERENCES

[1] R. Forré, *The Strict Avalanche Criterion : Spectral Properties of Boolean Functions and an Extended Definition*, Abstracts CRYPTO88.

[2] J.B. Kam and G.I. Davida, *A structured design of substitution-permutation encryption networks*, IEEE Trans. on Computers, Vol. 28, No. 10 (1979).

[3] A.F. Webster and S.E. Tavares, *On the design of S-boxes*, Advances in Cryptology, Proceedings CRYPTO85, Springer Verlag, Heidelberg, 1986