ELSEVIER

Information Processing Letters 60 (1996) 271–275

Information Processing Letters

Comment on "Bounds on the number of functions satisfying the Strict Avalanche Criterion"

A.M. Youssef, S.E. Tavares *

Department Of Electrical and Computer Engineering, Queen's University, Kingston, Ontario, Canada K7L 3N6

Received 1 May 1996
Communicated by S.G. Akl

Abstract

The Strict Avalanche Criterion (SAC) was introduced by Webster and Tavares (1995) in a study of design criteria for certain cryptographic functions. O'Connor (1994) gave an upper bound for the number of functions satisfying the SAC. Cusick (1996) gave a lower bound for the number of functions satisfying the SAC. He also gave a conjecture that provided an improvement of the lower bound. We give a constructive proof for this conjecture. Moreover, we provide an improved lower bound.

Keywords: Cryptography; Strict Avalanche Criterion; Boolean functions; Enumeration; Combinatorial problems

Notation. Throughout this paper, let

$f_n : \mathbb{Z}_2^n \to \mathbb{Z}_2$ describe a boolean function with n input variables.

$V = \{\boldsymbol{v}_i \mid 0 \leqslant i \leqslant 2^n - 1\}$ denotes the set of vectors in $\mathbb{Z}_2^n$ in lexicographical order. A boolean function $f_n(\boldsymbol{x})$ is specified by $f_n(\boldsymbol{x}) = [b_0, b_1, \ldots, b_{2^n-1}]$, where $b_i = f_n(\boldsymbol{v}_i)$.

$\boldsymbol{e}$ denotes any element of $\mathbb{Z}_2^n$ with Hamming weight 1. Let $\grave{e}$, $\grave{\boldsymbol{v}}_i \in \mathbb{Z}_2^{n-1}$ denote the $n-1$ least significant bits of $\boldsymbol{e}$ and $\boldsymbol{v}_i$ respectively.

$\boldsymbol{a}$ denotes any element of $\mathbb{Z}_2^{n-1}$ with odd Hamming weight.

$g_{n-1} : \mathbb{Z}_2^{n-1} \to \mathbb{Z}_2$ denotes the boolean function $\mathbf{1} \cdot \boldsymbol{x} \oplus b$, $b \in \mathbb{Z}_2$ where $\mathbf{1}$ denotes the all ones vector in $\mathbb{Z}_2^{n-1}$, $\cdot$ denotes the dot product operation over $\mathbb{Z}_2$ and $\oplus$ denotes the XOR operation. It is easy to see that g_{n-1} satisfies

$$g_{n-1}(\boldsymbol{x}) = g_{n-1}(\boldsymbol{x} \oplus \boldsymbol{a}) \oplus \mathbf{1}. \quad (1)$$

$MSB(\cdot)$ denotes the most significant bit of the enclosed argument.

$\mathcal{SAC}^n$ denotes the number of functions with n input bits that satisfy the SAC.

* Corresponding author. Email: tavares@ee.queensu.ca.

0020-0190/96/$12.00
PII S0020-0190(96)00166-4

Definition 1 [8]. A boolean function $f_n : \mathbb{Z}_2^n \to \mathbb{Z}_2$ is said to satisfy the SAC if complementing a single input bit results in changing the output bit with probability exactly one half, i.e.,

$$\sum_{i=0}^{2^n-1} f_n(\boldsymbol{v}_i) \oplus f_n(\boldsymbol{v}_i \oplus \boldsymbol{e}) = 2^{n-1}, \tag{2}$$

for all $\boldsymbol{e}$.

Definition 2 [4,5]. A linear structure of a boolean function $f_n : \mathbb{Z}_2^n \to \mathbb{Z}_2$ is identified as a vector $\boldsymbol{c} \neq \boldsymbol{0} \in \mathbb{Z}_2^n$ such that $f_n(\boldsymbol{v}_i \oplus \boldsymbol{c}) \oplus f_n(\boldsymbol{v}_i)$ takes the same value (0 or 1) for all i, $0 \leqslant i \leqslant 2^n - 1$.

The following conjecture is given in [2] without proof. This conjecture implies that there are at least $2^{2^{n-1}}$ boolean functions of n variables which satisfy the SAC.

Conjecture [2]. Given any choice of the values $f_n(\boldsymbol{v}_i)$, $0 \leqslant i \leqslant 2^{n-1} - 1$, there exists a choice of $f_n(\boldsymbol{v}_i)$, $2^{n-1} \leqslant i \leqslant 2^n - 1$, such that the resulting function $f_n(\boldsymbol{x})$ satisfies the SAC.

We prove this conjecture below. After completing our proof, we learned that Cusick and Stănică [3] independently proved the conjecture. Also, Biss [1] has proved a much stronger result by a much more complicated argument. If we let $L_n = \log_2 \mathscr{SAC}^n/2^n$, $L = \lim_{n\to\infty} L_n$, then Biss proved that $L = 1$. The conjecture, of course, only says that $L_n \geqslant 1/2$.

For $n = 1$, it is trivial to show that if $f_1(1) = f_1(0) \oplus 1$ then the resulting function satisfies the SAC. In the following lemma we prove that, for $n \geqslant 2$, there exist at least two choices for $f_n(\boldsymbol{v}_i)$, $2^{n-1} \leqslant i \leqslant 2^n - 1$, such that the resulting function satisfies the SAC.

Lemma 3. *Let $f_n = [h_{n-1}[h_{n-1} \oplus g_{n-1}]]$, where h_{n-1} is an arbitrary boolean function with $n-1$ input variables, $n \geqslant 2$, and g_{n-1} is constructed as above to satisfy Eq.* (1). *Then f_n satisfies the SAC.*

Proof. *Case* 1: $MSB(\boldsymbol{e}) = 0$.

$$\begin{aligned}
&\sum_{i=0}^{2^n-1} f_n(\boldsymbol{v}_i) \oplus f_n(\boldsymbol{v}_i \oplus \boldsymbol{e}) \\
&= \sum_{i=0}^{2^{n-1}-1} f_n(\boldsymbol{v}_i) \oplus f_n(\boldsymbol{v}_i \oplus \boldsymbol{e}) + \sum_{i=2^{n-1}}^{2^n-1} f_n(\boldsymbol{v}_i) \oplus f_n(\boldsymbol{v}_i \oplus \boldsymbol{e}) \\
&= \sum_{i=0}^{2^{n-1}-1} h_{n-1}(\grave{\boldsymbol{v}}_i) \oplus h_{n-1}(\grave{\boldsymbol{v}}_i \oplus \grave{e}) \\
&= \sum_{i=0}^{2^{n-1}-1} h_{n-1}(\grave{\boldsymbol{v}}_i) \oplus h_{n-1}(\grave{\boldsymbol{v}}_i \oplus \grave{e}) \oplus g_{n-1}(\grave{\boldsymbol{v}}_i) \oplus g_{n-1}(\grave{\boldsymbol{v}}_i \oplus \grave{e}) \\
&= \sum_{i=0}^{2^{n-1}-1} h_{n-1}(\grave{\boldsymbol{v}}_i) \oplus h_{n-1}(\grave{\boldsymbol{v}}_i \oplus \grave{e}) + \sum_{i=0}^{2^{n-1}-1} \overline{(h_{n-1}(\grave{\boldsymbol{v}}_i) \oplus h_{n-1}(\grave{\boldsymbol{v}}_i \oplus \grave{e}))} = 2^{n-1}.
\end{aligned}$$

Case 2: $MSB(e)=1$.

$$\sum_{i=1}^{2^n-1} f_n(v_i)\oplus f_n(v_i\oplus e) = 2\sum_{i=0}^{2^{n-1}-1} f_n(v_i)\oplus f_n(v_i\oplus e)$$

$$= 2\sum_{i=0}^{2^{n-1}-1} h_{n-1}(\grave{v}_i)\oplus h_{n-1}(\grave{v}_i)\oplus g_{n-1}(\grave{v}_i)$$

$$= 2\sum_{i=0}^{2^{n-1}-1} g_{n-1}(\grave{v}_i) = 2^{n-1},$$

which proves the lemma. □

From Lemma 1, and by noting that we have two choices for g_n, we conclude that, for $n \geqslant 2$, the number of function satisfying the SAC is lower bounded by $2^{2^{n-1}+1}$. Using the following lemma, one can provide some improvement to the above bound.

Lemma 4. *Let* $f_n=[h_{n-1}[l_{n-1}\oplus g_{n-1}]]$, *where* h_{n-1} *is an arbitrary boolean function with* $n-1$ *input variables,* $l_{n-1}(x)=h_{n-1}(x\oplus a)$, $n\geqslant 2$, *and* g_{n-1} *is constructed as above to satisfy Eq.* (1). *Then* f_n *satisfies the SAC.*

Proof. *Case* 1: $MSB(e)=0$.

$$\sum_{i=0}^{2^n-1} f_n(v_i)\oplus f_n(v_i\oplus e)$$

$$= \sum_{i=0}^{2^{n-1}-1} f_n(v_i)\oplus f_n(v_i\oplus e) + \sum_{i=2^{n-1}}^{2^n-1} f_n(v_i)\oplus f_n(v_i\oplus e)$$

$$= \sum_{i=0}^{2^{n-1}-1} h_{n-1}(\grave{v}_i)\oplus h_{n-1}(\grave{v}_i\oplus\grave{e})$$

$$+ \sum_{i=0}^{2^{n-1}-1} h_{n-1}(\grave{v}_i\oplus a)\oplus h_{n-1}(\grave{v}_i\oplus a\oplus\grave{e})\oplus g_{n-1}(\grave{v}_i)\oplus g_{n-1}(\grave{v}_i\oplus\grave{e})$$

$$= \sum_{i=0}^{2^{n-1}-1} h_{n-1}(\grave{v}_i)\oplus h_{n-1}(\grave{v}_i\oplus\grave{e}) + \sum_{i=0}^{2^{n-1}-1}\overline{\left(h_{n-1}(\grave{v}_i)\oplus h_{n-1}(\grave{v}_i\oplus\grave{e})\right)} = 2^{n-1}.$$

Case 2: $MSB(e)=1$.

$$\sum_{i=0}^{2^n-1} f_n(v_i)\oplus f_n(v_i\oplus e)$$

$$= 2\sum_{i=0}^{2^{n-1}-1} h_{n-1}(\grave{v}_i)\oplus h_{n-1}(\grave{v}_i\oplus a)\oplus g_{n-1}(\grave{v}_i)$$

Table 1
Exact number of functions satisfying SAC versus the derived lower bounds

n	2	3	4	5
$\mathscr{LS}^{n-1}$	4	8	128	4992
Old bound [2]	2	4	16	256
New bound (exp. (3))	8	64	1536	1099776
New bound (exp. (4))	8	64	1920	1157568
Exact number	8	64	4128	27522560

$$= \sum_{i=0}^{2^{n-1}-1} h_{n-1}(\hat{v}_i) \oplus h_{n-1}(\hat{v}_i \oplus a) \oplus g_{n-1}(\hat{v}_i) + \sum_{i=0}^{2^{n-1}-1} h_{n-1}(\hat{v}_i \oplus a) \oplus h_{n-1}(\hat{v}_i) \oplus g_{n-1}(\hat{v}_i \oplus a)$$

$$= \sum_{i=0}^{2^{n-1}-1} h_{n-1}(\hat{v}_i) \oplus h_{n-1}(\hat{v}_i \oplus a) \oplus g_{n-1}(\hat{v}_i)$$

$$+ \sum_{i=0}^{2^{n-1}-1} \overline{h_{n-1}(\hat{v}_i \oplus a) \oplus h_{n-1}(\hat{v}_i) \oplus g_{n-1}(\hat{v}_i)} = 2^{n-1},$$

which proves the lemma. □

Note that if the function f_{n-1} does not have any linear structures, then all the functions generated by $l_{n-1} \oplus g_{n-1}$ will be unique for all the 2^{n-2} choices of $\boldsymbol{a}$. From Lemmas 3 and 4 we have $2^{n-1}+2$ distinct choices for $f_{n-1}(v_i)$, $2^{n-1} \leqslant i \leqslant 2^n - 1$. Thus we have the following corollary:

Corollary 5. *The number of functions satisfying the SAC is lower bounded by*

$$(2^{2^{n-1}} - \mathscr{LS}^{n-1})(2^{n-1}+2) + 2\mathscr{LS}^{n-1} \tag{3}$$

where $\mathscr{LS}^{n-1}$ is the number of functions with $n-1$ input bits having any linear structure. A complicated formula for $\mathscr{LS}^{n}$ is given in [7]. *It can also be shown* [7] *that $\mathscr{LS}^{n}$ is asymptotic to $(2^n - 1)2^{2^{n-1}+1}$.*

One should note that while this bound provides some improvement over the proved bound in [2], exhaustive search (see Table 1) shows that the quality of this bound degrades as n increases. One can improve this bound slightly by identifying special classes of functions $f_n(v_i)$, $0 \leqslant i \leqslant 2^{n-1}-1$ for which there is a large number of choices for $f_n(v_i)$, $2^{n-1} \leqslant i \leqslant 2^n - 1$ such that the resulting function, f_n, satisfies the SAC. For example, if the function h_{n-1} satisfies the SAC, then the function $f_n = [h_{n-1}[h_{n-1} \oplus c \cdot x \oplus b]]$, $b \in \mathbb{Z}_2$ also satisfies the SAC. Thus our bound is slightly improved to

$$(2^{2^{n-1}} - \mathscr{LS}^{n-1} - \mathscr{SAC}^{n-1})(2^{n-1}+2) + 2^n\mathscr{SAC}^{n-1} + 2\mathscr{LS}^{n-1}. \tag{4}$$

We now give a lower bound on the number of balanced functions that satisfy the SAC.

Lemma 6. *Let $f_n = [h_{n-1}[l_{n-1} \oplus g_{n-1}]]$, where h_{n-1} is an arbitrary boolean function with $n-1$ input variables that satisfies $\sum_{\mathrm{wt}(v_i)\mathrm{odd}} h_{n-1}(v_i) = 2^{n-3}$, $l_{n-1}(x) = h(x \oplus a)$, $n \geqslant 2$, and g_{n-1} is constructed as above to satisfy Eq.* (1). *Then f_n is a balanced function that satisfies the SAC.*

Proof. From Lemma 6, it follows that f_n satisfies the SAC. Here we will prove that f_n is a balanced function.

$$\sum_{i=1}^{2^n-1} f_n(v_i) = \sum_{i=0}^{2^{n-1}-1} h_{n-1}(\hat{v}_i) + \sum_{i=0}^{2^{n-1}-1} h_{n-1}(\hat{v}_i \oplus a) \oplus g_{n-1}(\hat{v}_i)$$

$$= \sum_{i=0}^{2^{n-1}-1} h_{n-1}(\hat{v}_i) + \sum_{i=0}^{2^{n-1}-1} h_{n-1}(\hat{v}_i) \oplus g_{n-1}(\hat{v}_i \oplus a)$$

$$= \sum_{i=0}^{2^{n-1}-1} h_{n-1}(\grave{v}_i) + \sum_{i=0}^{2^{n-1}-1} \overline{h_{n-1}(\grave{v}_i) \oplus 1 \cdot \grave{v}_i}$$

$$= \sum_{\mathrm{wt}(\grave{v}_i)\ \mathrm{even}}^{2^{n-1}-1} \left(h_{n-1}(\grave{v}_i) + \overline{h_{n-1}(\grave{v}_i)}\right) + 2 \sum_{\mathrm{wt}(\grave{v}_i)\ \mathrm{odd}}^{2^{n-1}-1} h_{n-1}(\grave{v}_i) = 2^{n-2} + 2 \cdot 2^{n-3} = 2^{n-1},$$

which proves the lemma. □

Similarly, one can also show that the function $f_n = [h_{n-1}[h_{n-1} \oplus g_{n-1}]]$ where h_{n-1} is an arbitrary boolean function that satisfies $\sum_{\mathrm{wt}(v_i)\ \mathrm{even}} h_{n-1}(v_i) = 2^{n-3}$ is a balanced function that satisfies the SAC. From the lemma above, it follows that the number of balanced SAC functions is lower bounded by

$$\binom{2^{n-2}}{2^{n-3}} 2^{2^{n-2}+1}. \tag{5}$$

References

[1] D.K. Biss, A lower bound on the number of functions satisfying the Strict Avalanche Criterion, Submitted.
[2] T.W. Cusick, Bounds on the number of functions satisfying the Strict Avalanche Criterion, *Inform. Process. Lett.* **57** (1996) 261–263.
[3] T.W. Cusick and P. Stănică, Bounds on the number of functions satisfying the Strict Avalanche Criterion, *Inform. Process. Lett.* **60** (1996) 215–219.
[4] J.H. Evertse, Linear structures in block ciphers, in: *Advances in Cryptology: Proc. of EUROCRYPT'87* (Springer, Berlin, 1988) 249–266.
[5] W. Meier and O. Staffelbach, Nonlinearity criteria for cryptographic functions, in: *Advances in Cryptology: Proc. of EUROCRYPT'89* (Springer, Berlin, 1990) 549–562.
[6] L.J. O'Connor, An upper bound on the number of functions satisfying the Strict Avalanche Criterion, *Inform. Process. Lett.* **52** (1994) 325–327.
[7] L.J. O'Connor and A. Klapper, Algebraic nonlinearity and its application to cryptography, *J. Cryptology* **7** (1994) 213–227.
[8] A.F. Webster and S.E. Tavares, On the design of S-boxes, in: *Advances in Cryptology: Proc. of CRYPTO'85* (Springer, Berlin, 1986) 523–534.