PAPER ⟨Special Issue on Cryptography and Information Security⟩

On Generating Cryptographically Desirable Substitutions

Kwangjo KIM†, Tsutomu MATSUMOTO† and Hideki IMAI†, Members

SUMMARY S(ubstitution)-boxes are quite important components of modern symmetric cryptosystems. S-boxes bring nonlinearity to cryptosystems and strengthen their cryptographic security. An S-box satisfies the strict avalanche criterion (SAC), if and only if for any single input bit of the S-box, the inversion of it changes each output bit with probability one half. This paper presents some interesting properties of S-boxes and proposes an efficient and systematic means of generating arbitrary input size bijective S-boxes satisfying SAC.

1. Introduction

In 1949, Shannon[1] proposed the outstanding notion of "mixing transformations" which randomly distribute the meaningful messages uniformly over the set of all possible ciphertext messages. Mixing transformations could be created by alternatively applying permutations* and substitutions. In practice, a substitution (afterward, we call "S-box") is implemented as a logic circuit or a table lookup memory and a permutation is implemented as a one-to-one wiring. S-boxes bring nonlinearity to cryptosystems and strengthen their cryptographic security.

It could be considered that published symmetric cryptosystems like DES[2], FEAL[3] etc. are the good design practices of the mixing transformation. In DES, the substitution is implemented as eight 6-bit input 4-bit output lookup tables. In FEAL, the arithmetic operations like cyclic rotation, addition modulo 2, etc. are used for the substitution.

In order to design the good S-box, Kam and Davida[4] proposed the completeness condition that each output bit depends on all input bits of the substitution. Webster and Tavares[5] introduced the strict avalanche criterion ("SAC") in order to combine the notions of the completeness and the avalanche effect[6] as explained in Sect. 2. Moreover, Forré[7] discussed the Walsh spectral properties of S-boxes satisfying SAC and extended the concept of SAC to the subfunctions obtained from the original function by keeping one or more input bits constant, in order to prevent partial approximation cryptanalysis. Lloyd[8] re-stated the Forrés extended SAC and counted the number of S-boxes satisfying the criterion.

Some results[9],[10] were published to design S-boxes by randomly selecting from all possible reversible transformation. However in the open literature there are sparse publications concerning the systematic design techniques for the generation of S-boxes satisfying SAC.

Thus the main purpose of this paper is to suggest the properties of S-boxes satisfying SAC and to propose the practical generation methods of S-boxes satisfying SAC.

The organization of this paper is as follows: In Sect. 2, we formally define and summarize the basic definition of the cryptographically desirable S-box. In Sect. 3, we discuss the simple generation method of S-boxes satisfying SAC. In Sect. 4, we prove some interesting theorems for S-box satisfying SAC and propose the systematic and efficient enlargement of bijective S-boxes into any input size.

2. Basic Definitions

We summarize here the formal definition of the related criteria. Let Z denote the set of integers. Also, let Z_2^n denote the n-dimensional vector space over the finite field $Z_2=GF(2)$, and $\oplus$ denote the addition over Z_2^n, or, the bit-wise exclusive-or.

[Definition 1] For a positive integer n, define $\boldsymbol{c}_1^{(n)}, \boldsymbol{c}_2^{(n)}, \cdots \boldsymbol{c}_n^{(n)} \in Z_2^n$ by

$$\boldsymbol{c}_1^{(n)}=[0, 0, \cdots, 0, 0, 1]$$
$$\boldsymbol{c}_2^{(n)}=[0, 0, \cdots, 0, 1, 0]$$
$$\vdots$$
$$\boldsymbol{c}_n^{(n)}=[1, 0, \cdots, 0, 0, 0].$$

[Definition 2 (Completeness)] A function $f: Z_2^n \to Z_2^m$ is complete if and only if

$$\sum_{\boldsymbol{x} \in Z_2^n} f(\boldsymbol{x}) \oplus f(\boldsymbol{x} \oplus \boldsymbol{c}_i^{(n)}) > (0, \cdots, 0)$$

for all i $(1 \leqq i \leqq n)$, where both the summation and the greater-than are component-wise over Z^m.

This means that each output bit depends on all of the input bits. Thus, if it were possible to find the simplest Boolean expression for each output bit in terms

Manuscript received February 14, 1990.
Manuscript revised April 11, 1990.
† The authors are with the Faculty of Engineering, Yokohama National University, Yokohama-shi, 240 Japan.

* The term permutation have been used here our preference to the term transposition.

of the input bits, each of those expressions would have to contain all of the input bits if the function is complete.

[Definition 3 (Avalanche effect)] A function f: $Z_2^n \to Z_2^m$ exhibits the avalanche effect if and only if

$$\sum_{x \in Z_2^n} wt(f(\boldsymbol{x}) \oplus f(\boldsymbol{x} \oplus \boldsymbol{c}_i^{(n)})) = m2^{n-1}$$

for all $i(1 \leq i \leq n)$. Here $wt(\ )$ denotes the Hamming weight function.

This means that an average of one half of the output bits change whenever a single input bit is complemented.

[Definition 4 (SAC, Strong S-box)] We say that a function $f: Z_2^n \to Z_2^m$ satisfies the strict avalanche criterion (SAC), or f is a strong S-box, if for all $i(1 \leq i \leq n)$ there hold the following equations:

$$\sum_{x \in Z_2^n} f(\boldsymbol{x}) \oplus f(\boldsymbol{x} \oplus \boldsymbol{c}_i^{(n)}) = (2^{n-1}, 2^{n-1}, \cdots, 2^{n-1}, 2^{n-1}). \tag{1}$$

If a function satisfies SAC, each of its output bits should change with a probability of one half whenever a single input bit is complemented. Clearly, a strong S-box is complete and exhibits the avalanche effect.

If some output bits depend on only a few input bits, then, by observing a significant number of input-output pairs such as chosen plaintext attack, a cryptanalyst might be able to detect these relations and use this information to aid the search for the key. And because any lower-dimensional space approximation of a mapping yields a wrong result in 25 % of the cases, strong S-boxes play significant roles in cryptography.

Notation : For a function $f: Z_2^n \to Z_2^m$, denoted by $f_j(1 \leq j \leq m)$ the function $Z_2^n \to Z_2$ such that

$$f(\boldsymbol{x}) = (f_m(\boldsymbol{x}), f_{m-1}(\boldsymbol{x}), \cdots, f_2(\boldsymbol{x}), f_1(\boldsymbol{x})).$$

We identify an element

$$\boldsymbol{z} = (z_k, z_{k-1}, \cdots, z_2, z_1)$$

of Z_2^k with an integer $\sum_{i=1}^{k} z_i 2^{i-1}$. To represent a function f: $Z_2^n \to Z_2^m$, we often use the integer tuple

$$\langle f \rangle = [f(0), f(1), f(2), \cdots, f(2^n - 1)]$$

and call it the integer representation of f. This representation can be obtained by combining $\langle f_m \rangle$, $\langle f_{m-1} \rangle$, $\cdots$, $\langle f_2 \rangle$, $\langle f_1 \rangle$ as

$$\langle f \rangle = \sum_{j=1}^{m} \langle f_j \rangle \cdot 2^{j-1}.$$

3. Properties of Strong S-box

Let us discuss the cryptographic properties of strong S-boxes or functions satisfying the strict avalanche criterion.

3.1 Some Functions Never Satisfy SAC

[Definition 5 (Linearity, Affinity)] A function f from Z_2^n into Z_2^m is affine if there exist an $n \times m$ matrix $\boldsymbol{A}_f$ over Z_2 and an m-dimensional vector $\boldsymbol{b}_f$ over Z_2 such that

$$f(\boldsymbol{x}) = \boldsymbol{x}\boldsymbol{A}_f + \boldsymbol{b}_f$$

where $\boldsymbol{x}$ denotes the indeterminate n-dimensional vector. A function f is linear if it is affine with $\boldsymbol{b}_f = \boldsymbol{0}$.

It is well known[11] that any cryptosystem which implements linear or affine functions can be easily broken. This fact brings us the question : Are there linear or affine functions satisfying the strict avalanche criterion ?

The answer is of course "no".

[Theorem 1] A strong S-box is neither linear nor affine.

(Proof) Kam and Davida[4] showed that there are no complete affine functions, and as mentioned before a function which satisfies the strict avalanche criterion must be complete. Thus the conclusion is obvious. However, it is an easy task to give a direct proof :

Let f be an affine function :

$$f(\boldsymbol{x}) = x\boldsymbol{A}_f \oplus \boldsymbol{b}_f.$$

Then, for each $i(1 \leq i \leq n)$ it holds that

$$\begin{aligned}
&\sum_{x \in Z_2^n} f(\boldsymbol{x}) \oplus f(\boldsymbol{x} \oplus \boldsymbol{c}_i^{(n)}) \\
&= \sum_{x \in Z_2^n} \boldsymbol{x}\boldsymbol{A}_f \oplus \boldsymbol{b}_f \oplus \boldsymbol{x}\boldsymbol{A}_f \oplus \boldsymbol{c}_i^{(n)}\boldsymbol{A}_f \oplus \boldsymbol{b}_f \\
&= \sum_{x \in Z_2^n} \boldsymbol{c}_i^{(n)}\boldsymbol{A}_f.
\end{aligned}$$

Because each component of the above summation has either 0 or 2^n, thus f could not satisfy the definition of the strict avalanche criterion. □

And also it is easy to see that

[Theorem 2] For $n=1$, or 2, any bijective function f from Z_2^n into Z_2^n never satisfy the strict avalanche criterion.

(Proof) By virtue of Theorem 1 it is sufficient to show that f is affine. Since if $n=1$ any function from Z_2 into Z_2 is apparently affine, we consider the case $n=2$ in the following. When $n=2$, f can be uniquely represented by

$$f(x_2, x_1) = \boldsymbol{a}_0 \oplus \boldsymbol{a}_1 x_1 \oplus \boldsymbol{a}_2 x_2 \oplus \boldsymbol{a}_3 x_1 x_2$$

where $\boldsymbol{a}_i \in Z_2^2 (i=0, 1, 2, 3)$. Thus,

$$\left.\begin{aligned}
f(0) \oplus f(1) &= \boldsymbol{a}_1 \\
f(0) \oplus f(2) &= \boldsymbol{a}_2 \\
f(1) \oplus f(2) &= \boldsymbol{a}_1 \oplus \boldsymbol{a}_2
\end{aligned}\right\} \tag{2}$$

$$\left.\begin{aligned}
f(2) \oplus f(3) &= \boldsymbol{a}_1 \oplus \boldsymbol{a}_3 \\
f(1) \oplus f(3) &= \boldsymbol{a}_2 \oplus \boldsymbol{a}_3 \\
f(0) \oplus f(3) &= \boldsymbol{a}_1 \oplus \boldsymbol{a}_2 \oplus \boldsymbol{a}_3
\end{aligned}\right\} \tag{3}$$

Since f is bijective, none of the above six vectors are zero. From Eq. (2), we observe that $\boldsymbol{a}_1 \neq 0$, $\boldsymbol{a}_2 \neq 0$, $\boldsymbol{a}_1 \oplus \boldsymbol{a}_2 \neq 0$ which means that

$$\{\boldsymbol{a}_1, \boldsymbol{a}_2, \boldsymbol{a}_1 \oplus \boldsymbol{a}_2\} = \{1, 2, 3\}$$

The facts $\boldsymbol{a}_1 \neq \boldsymbol{a}_3$, $\boldsymbol{a}_2 \neq \boldsymbol{a}_3$, $\boldsymbol{a}_1 \oplus \boldsymbol{a}_2 \neq \boldsymbol{a}_3$ from Eq. (3) indicate that $\boldsymbol{a}_3 = 0$. Thus f must be affine. □

Thus in order to obtain bijective strong S-boxes, we must treat at least quadratic function of at least three variables.

3.2 Use of Single Output Strong S-box

When $m=1$, and $n=3$ or 4, the experiments tell us that we can easily generate many strong S-boxes f: $Z_2^n \to Z_2$ by random search on an engineering workstation (SONY NWS810) in a few microseconds. But for the case of $n \geqq 5$ it becomes rather difficult to efficiently generate single output strong S-boxes in the same computational environments.

[Example 1] For $n=3$ and $m=1$,

$$\langle p \rangle = [1, 0, 1, 1, 1, 0, 0, 0],$$

$$\langle q \rangle = [1, 1, 1, 0, 0, 0, 1, 0],$$

$$\langle r \rangle = [1, 1, 0, 1, 0, 1, 0, 0]$$

are integer representations of strong S-boxes p, q and r respectively. By complementing the output bit of the single output strong S-box p, q and r, we have

$$\langle p' \rangle = [0, 1, 0, 0, 0, 1, 1, 1],$$

$$\langle q' \rangle = [0, 0, 0, 1, 1, 1, 0, 1],$$

$$\langle r' \rangle = [0, 0, 1, 0, 1, 0, 1, 1].$$

It is easy to check that all of these functions are strong S-boxes.

By the definition of the strict avalanche criterion and by the above observation, we can readily show the following.

[Theorem 3] Let g denote an affine function from Z_2^m into itself with a permutation matrix $\boldsymbol{A}_g$ and an arbitrary binary vector $\boldsymbol{b}_g$. Then, a function $f: Z_2^n \to Z_2^m$ satisfies the strict avalanche criterion if and only if the composite function $g \circ f: Z_2^n \to Z_2^m$ satisfies the strict avalanche criterion.

(Proof) Since every component of the tuple in the right-hand side of Eq. (1) is the same, a permutation of the output bits of f does not affect whether f satisfies the strict avalanche criterion. Also, when we complement any output bit(s) of f, the number of output bits from 1 to 0 and from 0 to 1 keeps constant. This completes the proof. □

Given some single output strong S-boxes, we can generate multiple output strong S-boxes using the idea summarized in the above theorem. (However, note that a strong S-box of $m=n$ generated by this method is not guaranteed to be bijective.)

[Example 2] The 3-input 3-output S-box f defined by

$$f(\boldsymbol{x}) = (r(\boldsymbol{x}), p(\boldsymbol{x}), q'(\boldsymbol{x}))$$

is strong, i. e., satisfies the strict avalanche criterion. Since

$$\langle r \rangle = [1, 1, 0, 1, 0, 1, 0, 0],$$

$$\langle p \rangle = [1, 0, 1, 1, 1, 0, 0, 0],$$

$$\langle q' \rangle = [0, 0, 0, 1, 1, 1, 0, 1],$$

then, the integer representation of f is

$$\langle r \rangle \cdot 4 + \langle p \rangle \cdot 2 + \langle q' \rangle = [6, 4, 2, 7, 3, 5, 0, 1].$$

Thus we can conclude this section by describing that there are no difficulties to efficiently generate many strong S-boxes up to the 4-bit input case.

4. Enlargement of Strong S-box

4.1 Construction

Next we discuss the expandable properties of strong S-boxes and present the constructive methods of generating strong S-boxes of arbitrary n and m.

Let us construct $(n+1)$-bit input S-boxes using n-bit input S-boxes.

[Definition 6] For a function $f: Z_2^n \to Z_2$, an integer $k \in \{1, 2, \cdots, n\}$ and a constant $a \in Z_2$, define a function $\boldsymbol{D}_a^k[f]: Z_2^{n+1} \to Z_2$ by

$$\boldsymbol{D}_a^k[f](0, \boldsymbol{x}) = f(\boldsymbol{x})$$

$$\boldsymbol{D}_a^k[f](1, \boldsymbol{x}) = f(\boldsymbol{x} \oplus \boldsymbol{c}_k^{(n)}) \oplus a$$

for all $\boldsymbol{x} \in Z_2^n$.

[Definition 7] For a function $f: Z_2^n \to Z_2^n$ such that

$$f(\boldsymbol{x}) = (f_n(\boldsymbol{x}), f_{n-1}(\boldsymbol{x}), \cdots, f_1(\boldsymbol{x})),$$

and a function $g: Z_2^n \to Z_2$ and an integer $k \in \{1, 2, \cdots, n\}$, define the function $\boldsymbol{E}^k[g, f]: Z_2^{n+1} \to Z_2^{n+1}$ by

$$\boldsymbol{E}^k[g, f](\boldsymbol{y}) = (\boldsymbol{D}_1^k[g](\boldsymbol{y}), \boldsymbol{D}_0^k[f_n](\boldsymbol{y}), \boldsymbol{D}_0^k[f_{n-1}](\boldsymbol{y}), \cdots, \boldsymbol{D}_0^k[f_1](\boldsymbol{y}))$$

for all $\boldsymbol{y} \in Z_2^{n+1}$.

We can show that the constructed S-boxes have nice properties.

[Theorem 4] If a function $f: Z_2^n \to Z_2$ satisfies the strict avalanche criterion, then for any $k \in \{1, 2, \cdots, n\}$ and any $a \in Z_2$, $\boldsymbol{D}_a^k[f]$ also satisfies the strict avalanche criterion.

(Proof) Since f satisfies the strict avalanche criterion, it holds that

$$\sum_{x \in Z_2^n} f(\boldsymbol{x}) \oplus f(\boldsymbol{x} \oplus \boldsymbol{c}_i^{(n)}) = 2^{n-1}$$

for any $i \in \{1, 2, \cdots, n\}$. Thus it also holds that

$$\sum_{x \in Z_2^n} f(x) \oplus f(\boldsymbol{x} \oplus \boldsymbol{c}_i^{(n)}) \oplus 1$$

$$=2^n-\sum_{x\in Z_2^n} f(\boldsymbol{x})\oplus f(\boldsymbol{x}\oplus \boldsymbol{c}_i^{(n)})$$
$$=2^n-2^{n-1}$$
$$=2^{n-1}$$

To prove the theorem, we denote $\boldsymbol{D}_a^k[f]$ by g and show that for any $i\in\{1, 2, \cdots, n+1\}$.

$$\sum_{y\in Z_2^{n+1}} g(\boldsymbol{y})\oplus g(\boldsymbol{y}\oplus \boldsymbol{c}_i^{(n+1)})=2^n$$

(Case 1) $i\in\{1, 2, \cdots, n\}$.

$$\sum_{y\in Z_2^{n+1}} g(\boldsymbol{y})\oplus g(\boldsymbol{y}\oplus \boldsymbol{c}_i^{(n+1)})$$
$$=\sum_{x\in Z_2^n} g(0, \boldsymbol{x})\oplus g(0, \boldsymbol{x}\oplus \boldsymbol{c}_i^{(n)})$$
$$+\sum_{x\in Z_2^n} g(1, x)\oplus g(1, \boldsymbol{x}\oplus \boldsymbol{c}_i^{(n)})$$
$$=\sum_{x\in Z_2^n} f(\boldsymbol{x})\oplus f(\boldsymbol{x}\oplus \boldsymbol{c}_i^{(n)})$$
$$+\sum_{x\in Z_2^n} (f(\boldsymbol{x}\oplus \boldsymbol{c}_k^{(n)})\oplus a)\oplus(f((\boldsymbol{x}\oplus \boldsymbol{c}_i^{(n)})\oplus \boldsymbol{c}_k^{(n)})\oplus a)$$
$$=\sum_{x\in Z_2^n} f(\boldsymbol{x})\oplus f(\boldsymbol{x}\oplus \boldsymbol{c}_i^{(n)})$$
$$+\sum_{x\in Z_2^n} f(\boldsymbol{x}\oplus \boldsymbol{c}_k^{(n)})\oplus f((\boldsymbol{x}\oplus \boldsymbol{c}_i^{(n)})\oplus \boldsymbol{c}_k^{(n)})$$
$$=2\cdot \sum_{x\in Z_2^n} f(\boldsymbol{x})\oplus f(\boldsymbol{x}\oplus \boldsymbol{c}_i^{(n)})$$
$$=2\cdot 2^{n-1}$$
$$=2^n$$

(Case 2) $i=n+1$

$$\sum_{y\in Z_2^{n+1}} g(\boldsymbol{y})\oplus g(\boldsymbol{y}\oplus \boldsymbol{c}_{n+1}^{(n+1)})$$
$$=\sum_{x\in Z_2^n} g(0, \boldsymbol{x})\oplus g(1, \boldsymbol{x})+\sum_{x\in Z_2^n} g(1, \boldsymbol{x})\oplus g(0, \boldsymbol{x})$$
$$=2\cdot \sum_{x\in Z_2^n} g(0, \boldsymbol{x})\oplus g(1, \boldsymbol{x})$$
$$=2\cdot \sum_{x\in Z_2^n} f(\boldsymbol{x})\oplus f(\boldsymbol{x}\oplus \boldsymbol{c}_k^{(n)})\oplus a$$
$$=2\cdot 2^{n-1}$$
$$=2^n$$

Thus, we complete the proof. □

[Theorem 5] For a bijection $f:Z_2^n\to Z_2^n$, a function $g: Z_2^n\to Z_2$, and an integer $k\in\{1, 2, \cdots, n\}$ the function $\boldsymbol{E}^k[g, f]: Z_2^{n+1}\to Z_2^{n+1}$ is bijective.

(Proof) By the definition of $\boldsymbol{E}^k[g, f]$ we have for any $\boldsymbol{x}\in Z_2^n$,

$$\boldsymbol{E}^k[g, f](0, \boldsymbol{x})=(g(\boldsymbol{x}), f(\boldsymbol{x})),$$
$$\boldsymbol{E}^k[g, f](1, \boldsymbol{x}\oplus \boldsymbol{c}_k^{(n)})=(g(\boldsymbol{x})\oplus 1, f(\boldsymbol{x})).$$

For any $\boldsymbol{u}\in Z_2^n$ and $\boldsymbol{v}\in Z_2^n$, let

$$A(\boldsymbol{u}, \boldsymbol{v})=\boldsymbol{E}^k[g, f](0, \boldsymbol{u})\oplus \boldsymbol{E}^k[g, f](0, \boldsymbol{v}),$$
$$B(\boldsymbol{u}, \boldsymbol{v})=\boldsymbol{E}^k[g, f](1, \boldsymbol{u}\oplus \boldsymbol{c}_k^{(n)})\oplus \boldsymbol{E}^k[g, f](1, \boldsymbol{v}\oplus \boldsymbol{c}_k^{(n)}),$$
$$C(\boldsymbol{u}, \boldsymbol{v})=\boldsymbol{E}^k[g, f](0, \boldsymbol{u})\oplus \boldsymbol{E}^k[g, f](1, \boldsymbol{v}\oplus \boldsymbol{c}_k^{(n)}).$$

We have

$$A(\boldsymbol{u}, \boldsymbol{v})=B(\boldsymbol{u}, \boldsymbol{v})$$
$$=(g(\boldsymbol{u})\oplus g(\boldsymbol{v}), f(\boldsymbol{u})\oplus f(\boldsymbol{v})),$$
$$C(\boldsymbol{u}, \boldsymbol{v})=(g(\boldsymbol{u})\oplus g(\boldsymbol{v})\oplus 1, f(\boldsymbol{u})\oplus f(\boldsymbol{v})).$$

Since f is bijective, $f(\boldsymbol{u})\oplus f(\boldsymbol{v})=0$ if and only if $\boldsymbol{u}=\boldsymbol{v}$. Therefore, if $\boldsymbol{u}\neq\boldsymbol{v}$, we have $A(\boldsymbol{u},\boldsymbol{v})=B(\boldsymbol{u},\boldsymbol{v})\neq(0,0)$ and $C(\boldsymbol{u},\boldsymbol{v})\neq(0,0)$. And if $\boldsymbol{u}=\boldsymbol{v}$, we have $A(\boldsymbol{u}, \boldsymbol{v})=B(\boldsymbol{u}, \boldsymbol{v})=(0, 0)$ and $C(\boldsymbol{u}, \boldsymbol{v})=(1, 0)\neq(0, 0)$. Thus, $A(\boldsymbol{u}, \boldsymbol{v})$ and $B(\boldsymbol{u}, \boldsymbol{v})$ equals to zero if and only if $\boldsymbol{u}=\boldsymbol{v}$, and $C(\boldsymbol{u}, \boldsymbol{v})$ never equals to zero for any $\boldsymbol{u}$ and $\boldsymbol{v}$. These facts show that for any $\boldsymbol{s}\in Z_2^{n+1}$ and $\boldsymbol{t}\in Z_2^{n+1}$, $\boldsymbol{E}^k[g, f](\boldsymbol{s})=\boldsymbol{E}^k[g, f](\boldsymbol{t})$ if and only if $\boldsymbol{s}=\boldsymbol{t}$, in other words, that $\boldsymbol{E}^k[g, f]$ is bijective.

[Theorem 6] If both a bijection $f:Z_2^n\to Z_2^n$ and a function $g:Z_2^n\to Z_2$ satisfy the strict avalanche criterion, then for any integer $k\in\{1, 2, \cdots, n\}$, the function $\boldsymbol{E}^k[g, f]: Z_2^{n+1}\to Z_2^{n+1}$ is a bijection satisfying the strict avalanche criterion.

(Proof) This theorem follows directly from Theorems 4 and 5. □

[Remark] Define $f_i: Z_2^n\to Z_2 (i=1, 2, \cdots, n)$ by

$$f(\boldsymbol{x})=(f_n(\boldsymbol{x}), f_{n-1}(\boldsymbol{x}), \cdots, f_1(\boldsymbol{x}))$$

from the bijection $f:Z_2^n\to Z_2^n$ satisfying the strict avalanche criterion. Noting that f_i satisfies the strict avalanche criterion, Theorem 6 tells us that given a bijection $f:Z_2^n\to Z_2^n$ satisfies the strict avalanche criterion we can construct a bijection $\boldsymbol{E}^k[f_i, f]: Z_2^{n+1}\to Z_2^{n+1}$ satisfying the strict avalanche criterion using only f. □

By using these construction methods, we can generate strong S-boxes in an efficient and systematic way. Next section we give some examples.

4.2 Examples

Here we give detailed examples to generate strong S-boxes.

[Example 3] A function $f:Z_2^3\to Z_2$ which satisfies the strict avalanche criterion is given as below:

$$\langle f\rangle=[1, 1, 0, 0, 0, 1, 0, 1].$$

Then,

$$\langle \boldsymbol{D}_1^0[f]\rangle=[1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 0, 1, 0],$$
$$\langle \boldsymbol{D}_1^1[f]\rangle=[1, 1, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1].$$

By Theorem 4, these expanded functions also satisfy the strict avalanche criterion.

[Example 4] When a strong S-box $g:Z_2^3\to Z_2$ is [1, 0, 0, 0, 1, 1, 0, 1] and a bijective strong S-box $f:Z_2^3\to Z_2^3$ is [3, 1, 4, 0, 2, 5, 6, 7],

$$\langle \boldsymbol{D}_1^1[g]\rangle=[1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1]$$

and

$$\langle \boldsymbol{D}_0^1[f]\rangle=[3, 1, 4, 0, 2, 5, 6, 7, 1, 3, 0, 4, 5, 2, 7, 6].$$

By Theorem 6, we can get a strong bijective S-box.

$$\langle \boldsymbol{E}^1[g, f]\rangle=[11, 1, 4, 0, 10, 13, 6, 15, 9, 3, 8, 12, 5, 2, 7, 14].$$

By the same way, we can get 6-bit input bijective strong S-boxes,

[4, 53, 16, 57, 43, 45, 2, 6, 12, 55, 63, 33, 8, 26, 30, 51, 37, 20, 41, 0, 61, 59, 22, 18, 39, 28, 49, 47, 10, 24, 35, 14, 21, 36, 25, 48, 13, 11, 38, 34, 23, 44, 1, 31, 58, 40, 19, 62, 52, 5, 32, 9, 27, 29, 50, 54, 60, 7, 15, 17, 56, 42, 46, 3]

and

[36, 21, 48, 57, 43, 45, 2, 38, 12, 23, 63, 1, 8, 58, 30, 19, 37, 20, 9, 0, 29, 27, 22, 50, 39, 60, 49, 15, 10, 56, 35, 46, 53, 4, 25, 16, 13, 11, 6, 34, 55, 44, 33, 31, 26, 40, 51, 62, 52, 5, 32, 41, 59, 61, 18, 54, 28, 7, 47, 17, 24, 42, 14, 3].

Therefore, we can generate arbitrary input size bijective strong S-boxes if we find 3-bit input bijective strong S-boxes.

5. Concluding Remarks

We have summarized the cryptographic desired criteria for S-boxes of symmetric cryptosystems and proved several interesting theorems of strong S-boxes. Moreover, we proposed the systematic and efficient enlargement of bijective S-boxes into an arbitrary input size.

Next problem is when we combine the generated strong S-boxes with a permutation, to design the cryptographically desirable permutation.

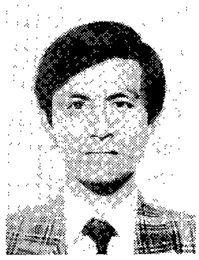
Acknowledgement

The first author is supported in part by Electronics and Telecommunications Research Institute.

References

(1) C. E. Shannon: "Communication theory of secrecy systems", BSTJ, **28**, pp. 656-715 (Oct. 1949).
(2) "Data encryption standard", National Bureau of Standards, Federal Information Processing Standard, **46**, U. S. A. (Jan. 1977).
(3) S. Miyaguchi, A. Shiraishi and A. Shimizu: "Fast data encryption algorithm FEAL-8", Electr. Comm. Lab. Tech. J., NTT, **37**, 4/5, pp. 321-327 (1988).
(4) J. B. Kam and G. I. Davida: "Structured design of substitution-permutation encryption network", IEEE Trans. Comput., **C-28**, 10, pp. 747-753 (Oct. 1979).
(5) A. F. Webster and S. E. Tavares: "On the design of S-boxes", Proc. of CRYPTO'85, Springer (1985).
(6) H. Feistel: "Cryptography and computer privacy", Scientific American, **228**, 5, pp. 15-23 (1973).
(7) R. Forré: "The strict avalanche criterion: spectral properties of Boolean functions and an extended definition", Proc. of CRYPTO'88 (1988).
(8) S. Lloyd: "Counting functions satisfying a higher order strict avalanche criterion", Proc. of EUROCYRPT'89 (1989).
(9) J. A. Gordon and H. Retkin: "Are big S-boxes best?", IEEE workshop on computer security, pp. 257-262 (1981).
(10) F. Ayoub: "Probabilistic completeness of substitution-permutation encryption networks", IEE, **129**, E, 5, pp. 195-199 (Sept. 1982).
(11) M. Hellman, R. Merkle, R. Schroeppel, L. Washington, W. Diffie, S. Pohlig and P. Schweitzer: "Results of an initial attempt to analyze the NBS data encryption standard", Information Systems Laboratory Report, Stanford University (1976).

Kwangjo Kim was born in Kwangwon, Korea on April 10, 1956. He received the B. Eng. and M. Eng. degrees in electronic engineering from Yonsei University, Seoul,Korea in 1980 and 1983 respectively. Since 1980, he has been with Electronics and Telecommunications Research Institute, Daejeon, Korea. By ETRI's program, he is currently a candidate for the Ph. D under the supervision of Professor Hideki Imai. His research interests include cryptography, communication security and their applications. He is a member of IEE of Japan and KITE of Korea.



Tsutomu Matsumoto was born in Maebashi, Japan, on October 20, 1958. He received the B. Eng. and M. Eng. degrees in computer eng. both from Yokohama National University, Yokohama, Japan, in 1981 and 1983, respectively, and Ph. D. degree in electronic eng. from The University of Tokyo, Tokyo, Japan, in 1986. From 1986 to 1989, he was a Lecturer for Electrical and Computer Engineering at Yokohama National University. Since 1989, he has been an Associate Professor and is currently working in cryptography, complexity theory, computational mathematics, and their applications to information security. Dr. Matsumoto is a member of ACM, IACR, IEEE, IPSJ, ITA and Akarui Angou Kenkyu-kai.

Hideki Imai was born in Shimane, Japan on May 31, 1943. He received the B. E., M. E. and Ph. D. degrees in electrical engineering from University of Tokyo, Tokyo, in 1966, 1968 and 1971, respectively. He is currently a Professor in the Division of Electrical and Computer Engineering, Yokohama National University, Yokohama. His current research interests include information theory, coding theory, cryptography and their applications. He is the author of three books and coauthor of several books. Dr. Imai is a member of IEEE, IEE of Japan, IPS of Japan, SITA of Japan, and ITE of Japan.