A Recursive Construction Method of S-boxes Satisfying Strict Avalanche Criterion

Kwangjo Kim
Tsutomu Matsumoto
Hideki Imai

Division of Electrical and Computer Engineering
Yokohama National University
156 Tokiwadai, Hodogaya, Yokohama 240 Japan

Abstract

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. We present some interesting properties of S-boxes and propose an efficient and systematic means of generating arbitrary input size *bijective* S-boxes satisfying the SAC by applying simple rules recursively given 3-bit input *bijective* S-box(es) satisfying the SAC.

1 Introduction

For the good S-box design of DES [NBS]-like cryptosystems (FEAL [MSS],LOKI [BPS],etc) in the open cryptologic society, Kam and Davida [KD] proposed the *completeness* condition that each output bit depends on all input bits of the substitution. Webster and Tavares [WT] introduced the *strict avalanche criterion*("SAC") in order to combine the notions of the *completeness* and the *avalanche effect* [Fe]. Moreover, Forré [Fo] discussed the Walsh spectral properties of S-boxes satisfying the 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 [Ll] re-stated the Forré's extended SAC and suggested the counting functions satisfying a higher order SAC.

A.J. Menezes and S.A. Vanstone (Eds.): Advances in Cryptology - CRYPTO '90, LNCS 537, pp. 564-574, 1991.

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 $f : Z_2^n \rightarrow Z_2^m$ satisfies the SAC, or f is a strong S-box, if for all i $(1 \leq i \leq n)$ there hold the following equations :*

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

If a function satisfies the 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 % [Ba] of the cases, strong S-boxes play significant roles in cryptography.

Notation For a function $f : Z_2^n \rightarrow Z_2^m$, denote by f_j $(1 \leq j \leq m)$ the function $Z_2^n \rightarrow Z_2$ such that $f(\mathbf{x}) = (f_m(\mathbf{x}), f_{m-1}(\mathbf{x}), \ldots, f_2(\mathbf{x}), f_1(\mathbf{x}))$. We identify an element $\mathbf{z} = (z_k, z_{k-1}, \ldots, z_2, z_1)$ of Z_2^k with an integer $\sum_{i=1}^{k} z_i 2^{i-1}$. To represent a function $f : Z_2^n \rightarrow Z_2^m$, we often use the integer tuple $< f >= [f(0), f(1), f(2), \ldots, f(2^n - 1)]$ and call it the integer representation of f. This representation can be obtained by combining $< f_m >, < f_{m-1} >, \ldots, < f_2 >, < f_1 >$ as $< f >= \sum_{j=1}^{m} < f_j > \cdot 2^{j-1}$.

3 Properties of Strong S-box

Let us discuss the cryptographic properties of strong S-boxes *or* functions satisfying the SAC.

3.1 Some Functions Never Satisfy the 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 $\mathbf{A}_f$ over Z_2 and an m-dimensional vector $\mathbf{b}_f$ over Z_2 such that*

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

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

It is well known[HM] 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 SAC ? The answer is of course "no".

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

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 SAC.*

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 $n \geq 5$ it becomes rather difficult to efficiently generate single output strong S-boxes in the same computational environment.

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

$$< p >= [1, 0, 1, 1, 1, 0, 0, 0],$$

$$< q >= [1, 1, 1, 0, 0, 0, 1, 0],$$

$$< r >= [1, 1, 0, 1, 0, 1, 0, 0]$$

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

$$< p' >= [0, 1, 0, 0, 0, 1, 1, 1],$$

$$< q' >= [0, 0, 0, 1, 1, 1, 0, 1],$$

$$< r' >= [0, 0, 1, 0, 1, 0, 1, 1].$$

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

By the definition of the SAC and by the above observation, we can readily show the following.

Theorem 3 *Let e (g, resp.) denote an affine function from Z_2^n (Z_2^m, resp.) into itself with a permutation matrix and an arbitrary binary vector. Then, a function $f : Z_2^n \to Z_2^m$ satisfies the SAC if and only if the composite function $g \circ f \circ e : Z_2^n \to Z_2^m$ satisfies the SAC.*

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 $f(\mathbf{x}) = (r(\mathbf{x}), p(\mathbf{x}), q'(\mathbf{x}))$ is strong, *i.e.*, satisfies the SAC. Since

$$< r >= [1,1,0,1,0,1,0,0],$$

$$< p >= [1,0,1,1,1,0,0,0],$$

$$< q' >= [0,0,0,1,1,1,0,1],$$

then, the integer representation of f is

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

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 recursive construction of 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 $k \in \{1,2,\ldots,n\}$ and a constant $b \in Z_2$, define a function $\mathbf{D}_b^k[f] : Z_2^{n+1} \to Z_2$ by $\mathbf{D}_b^k[f](0,\mathbf{x}) = f(\mathbf{x})$ and $\mathbf{D}_b^k[f](1,\mathbf{x}) = f(\mathbf{x} \oplus \mathbf{c}_k^{(n)}) \oplus b$ for all $\mathbf{x} \in Z_2^n$.*

Definition 7 *For a function $f : Z_2^n \to Z_2^n$ such that $f(\mathbf{x}) = (f_n(\mathbf{x}), f_{n-1}(\mathbf{x}), \ldots, f_1(\mathbf{x}))$, and a function $g : Z_2^n \to Z_2$ and an integer $k \in \{1,2,\ldots,n\}$, define the function $\mathbf{E}^k[g,f] : Z_2^{n+1} \to Z_2^{n+1}$ by*

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

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

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 SAC, then for any $k \in \{1,2,\ldots,n\}$ and any $b \in Z_2$, $\mathbf{D}_b^k[f]$ also satisfies the SAC.*

Proof: Since f satisfies the SAC, it holds that

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

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

$$\begin{aligned} & \sum_{\mathbf{x} \in Z_2^n} f(\mathbf{x}) \oplus f(\mathbf{x} \oplus \mathbf{c}_i^{(n)}) \oplus 1 \\ = \; & 2^n - \sum_{\mathbf{x} \in Z_2^n} f(\mathbf{x}) \oplus f(\mathbf{x} \oplus \mathbf{c}_i^{(n)}) \\ = \; & 2^n - 2^{n-1} \\ = \; & 2^{n-1} \end{aligned}$$

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

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

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

$$\begin{aligned} & \sum_{\mathbf{y} \in Z_2^{n+1}} g(\mathbf{y}) \oplus g(\mathbf{y} \oplus \mathbf{c}_i^{(n+1)}) \\ = \; & \sum_{\mathbf{x} \in Z_2^n} g(0, \mathbf{x}) \oplus g(0, \mathbf{x} \oplus \mathbf{c}_i^{(n)}) + \sum_{\mathbf{x} \in Z_2^n} g(1, \mathbf{x}) \oplus g(1, \mathbf{x} \oplus \mathbf{c}_i^{(n)}) \\ = \; & \sum_{\mathbf{x} \in Z_2^n} f(\mathbf{x}) \oplus f(\mathbf{x} \oplus \mathbf{c}_i^{(n)}) + \sum_{\mathbf{x} \in Z_2^n} (f(\mathbf{x} \oplus \mathbf{c}_k^{(n)}) \oplus b) \oplus (f((\mathbf{x} \oplus \mathbf{c}_i^{(n)}) \oplus \mathbf{c}_k^{(n)}) \oplus b) \\ = \; & \sum_{\mathbf{x} \in Z_2^n} f(\mathbf{x}) \oplus f(\mathbf{x} \oplus \mathbf{c}_i^{(n)}) + \sum_{\mathbf{x} \in Z_2^n} f(\mathbf{x} \oplus \mathbf{c}_k^{(n)}) \oplus f((\mathbf{x} \oplus \mathbf{c}_k^{(n)}) \oplus \mathbf{c}_i^{(n)}) \\ = \; & 2 \cdot \sum_{\mathbf{x} \in Z_2^n} f(\mathbf{x}) \oplus f(\mathbf{x} \oplus \mathbf{c}_i^{(n)}) \\ = \; & 2 \cdot 2^{n-1} \\ = \; & 2^n \end{aligned}$$

(Case 2) $i = n + 1$

$$\begin{aligned} & \sum_{\mathbf{y} \in Z_2^{n+1}} g(\mathbf{y}) \oplus g(\mathbf{y} \oplus \mathbf{c}_{n+1}^{(n+1)}) \\ = \; & \sum_{\mathbf{x} \in Z_2^n} g(0, \mathbf{x}) \oplus g(1, \mathbf{x}) + \sum_{\mathbf{x} \in Z_2^n} g(1, \mathbf{x}) \oplus g(0, \mathbf{x}) \\ = \; & 2 \cdot \sum_{\mathbf{x} \in Z_2^n} g(0, \mathbf{x}) \oplus g(1, \mathbf{x}) \\ = \; & 2 \cdot \sum_{\mathbf{x} \in Z_2^n} f(\mathbf{x}) \oplus f(\mathbf{x} \oplus \mathbf{c}_k^{(n)}) \oplus b \\ = \; & 2 \cdot 2^{n-1} \\ = \; & 2^n \end{aligned}$$

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 $k \in \{1, 2, \ldots, n\}$, the function $\mathbf{E}^k[g, f] : Z_2^{n+1} \to Z_2^{n+1}$ is bijective.*

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

$$\begin{aligned} \mathbf{E}^k[g,f](0,\mathbf{x}) &= (g(\mathbf{x}), f(\mathbf{x})), \\ \mathbf{E}^k[g,f](1,\mathbf{x} \oplus \mathbf{c}_k^{(n)}) &= (g(\mathbf{x}) \oplus 1, f(\mathbf{x})). \end{aligned}$$

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

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

We have

$$\begin{aligned} A(\mathbf{u},\mathbf{v}) &= B(\mathbf{u},\mathbf{v}) \\ &= (g(\mathbf{u}) \oplus g(\mathbf{v}), f(\mathbf{u}) \oplus f(\mathbf{v})) \\ C(\mathbf{u},\mathbf{v}) &= (g(\mathbf{u}) \oplus g(\mathbf{v}) \oplus 1, f(\mathbf{u}) \oplus f(\mathbf{v})) \end{aligned}$$

Since f is *bijective*, $f(\mathbf{u}) \oplus f(\mathbf{v}) = 0$ if and only if $\mathbf{u} = \mathbf{v}$. Therefore, if $\mathbf{u} \neq \mathbf{v}$, we have $A(\mathbf{u},\mathbf{v}) = B(\mathbf{u},\mathbf{v}) \neq (0,0)$ and $C(\mathbf{u},\mathbf{v}) \neq (0,0)$. And if $\mathbf{u} = \mathbf{v}$, we have $A(\mathbf{u},\mathbf{v}) = B(\mathbf{u},\mathbf{v}) = (0,0)$ and $C(\mathbf{u},\mathbf{v}) = (1,0) \neq (0,0)$. Thus, $A(\mathbf{u},\mathbf{v})$ and $B(\mathbf{u},\mathbf{v})$ equals to zero if and only if $\mathbf{u} = \mathbf{v}$, and $C(\mathbf{u},\mathbf{v})$ never equals to zero for any $\mathbf{u}$ and $\mathbf{v}$. These facts show that for any $\mathbf{s} \in Z_2^{n+1}$ and $\mathbf{t} \in Z_2^{n+1}$, $\mathbf{E}^k[g,f](\mathbf{s}) = \mathbf{E}^k[g,f](\mathbf{t})$ if and only if $\mathbf{s} = \mathbf{t}$, in other words, that $\mathbf{E}^k[g,f]$ 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 SAC, then for any integer $k \in \{1, 2, \ldots, n\}$, the function $\mathbf{E}^k[g,f] : Z_2^{n+1} \to Z_2^{n+1}$ is a bijection satisfying the SAC.*

Proof: This theorem follows directly from **Theorems 4** and **5**. □

For the explanatory purpose, we illustrate this method like Fig.1 in the **Appendix**.

Remark: Define $f_i : Z_2^n \to Z_2$ $(i = 1, 2, \ldots, n)$ by $f(\mathbf{x}) = (f_n(\mathbf{x}), f_{n-1}(\mathbf{x}), \ldots, f_1(\mathbf{x}))$ from the *bijection* $f : Z_2^n \to Z_2^n$ satisfying the SAC. Noting that f_i satisfies the SAC, **Theorem 6** tells us that given a *bijection* $f : Z_2^n \to Z_2^n$ satisfies the SAC we can construct a *bijection* $\mathbf{E}^k[f_i, f] : Z_2^{n+1} \to Z_2^{n+1}$ satisfying the SAC using only f (See Fig.2 in the **Appendix**). □

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

4.2 Examples

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

Example 3 A function $f : Z_2^3 \rightarrow Z_2$ which satisfies the SAC is given as $< f >= [1,1,0,0,0,1,0,1]$. Then,

$$< \mathbf{D}_0^1[f] >= [1,1,0,0,0,1,0,1,1,1,0,0,1,0,1,0],$$

and

$$< \mathbf{D}_1^1[f] >= [1,1,0,0,0,1,0,1,0,0,1,1,0,1,0,1].$$

By **Theorem 4**, these expanded functions also satisfy the SAC.

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

$$< \mathbf{D}_1^1[g] >= [1,0,0,0,1,1,0,1,1,0,1,1,0,0,0,1],$$

and

$$< \mathbf{D}_0^1[f] >= [3,1,4,0,2,5,6,7,1,3,0,4,5,2,7,6].$$

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

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

Also by applying **Thereom 6** two times, 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

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

As stated earlier, the experiments on the random search show that we can easily find 3-bit input *bijective* strong S-boxes, but when the number of input is increased, it becomes more and more difficult to find even a 5-bit input *bijective* strong S-box.

By applying **Theorem 6** recursively, however, we can generate arbitrary input size *bijective* strong S-boxes given 3-bit input *bijective* strong S-boxes. This method is very useful in designing a *bijective* strong S-box with a larger input size.

5 Concluding Remarks

We have summarized the cryptographically significant criteria for S-boxes of symmetric cryptosystems and proved several interesting theorems of strong S-boxes. Moreover, we proposed two recursive construction methods from 3-bit input *bijective* strong S-box(es) to an arbitrary input size *bijective* strong S-box.

The generated strong S-boxes can be useful for a basic building block of symmetric cryptosystems or pseudorandom generators, etc.

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

References

[NBS] NBS, "Data Encryption Standard(DES)", FIPS PUB 46, US National Bureau of Standards, Washinston DC, Jan., 1977.

[MSS] S.Miyaguchi, A.Shiraishi and A.Shimizu, "Fast data encryption algorithm FEAL–8 (in Japanese)", Electr. Comm. Lab. Tech. J., NTT, Vol.37, No.4/5, pp.321–327, 1988.

[BPS] L. Brown, J.Pieprzyk and J. Seberry, "LOKI – a cryptographic primitive for authentication and secrecy", Proc. of AUSCRYPT90, 1990.

[KD] J.B. Kam and G.I. Davida, "Structured design of substitution–permutation encryption network", IEEE Trans. on Comput., Vol.C-28, No.10, pp.747–753, Oct., 1979.

[WT] A.F. Webster and S.E. Tavares, "On the design of S-boxes", Proc. of CRYPTO85, Springer-Verlag, 1985.

[Fe] H. Feistel, "Cryptography and computer privacy", Scientific American, Vol.228, No.5, pp 15–23, 1973.

[Fo] R.Forré, "The strict avalanche criterion : spectral properties of Boolean functions and an extended definition", Proc.of CRYPTO88, Springer-Verlag, 1988.

[Ll] S.Lloyd, "Counting functions satisfying a higher order strict avalanche criterion", Proc. of EUROCYRPT89, Springer-Verlag, 1989.

[GR] J.A.Gordon and H. Retkin, "Are big S-boxes best ? ", IEEE workshop on computer security, pp.257–262, 1981.

[Ay] F.Ayoub, "Probabilistic completeness of substitution–permutation encryption networks", IEE, Vol.129, E, 5, pp195–199, Sep., 1982.

[Pi] J.P.Pieprzyk, "Non-linearity of exponent permutations", Proc. of EUROCRYPTO89, Springer-Verlag, 1989.

[Ba] S.Babbage, "On the relevance of the strict avalanche criterion", Electronics Letters, Vol.26, No.7, pp.461-462, 29th Mar., 1990.

[HM] 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.

Appendix

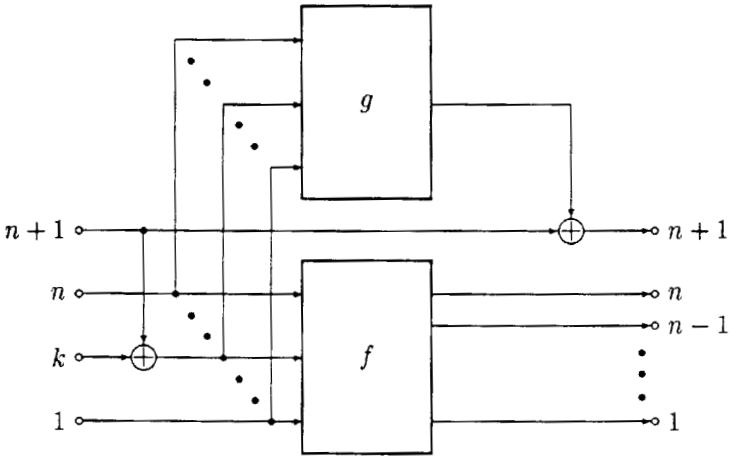

Figure 1: Construction method using f and g ($1 \leq k \leq n$).

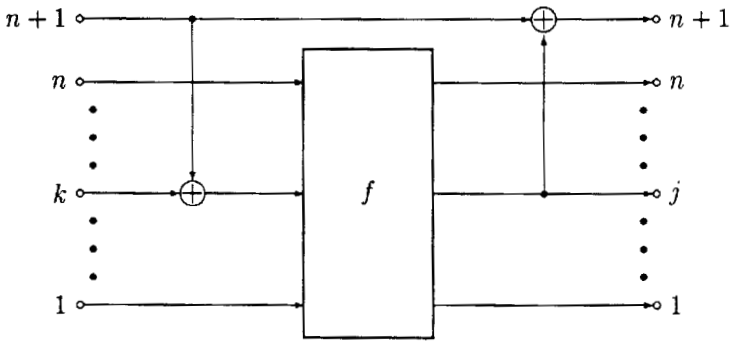

Figure 2: Construction method using only f ($1 \leq k, j \leq n$).