Improved Rijndael-Like S-Box and Its Transform Domain Analysis*

Seok-Yong Jin, Jong-Min Baek, and Hong-Yeop Song

Coding and Information Theory Lab,
School of Electrical and Electronic Engineering, Yonsei University,
134 Sinchon-dong, Seodaemun-gu, Seoul 120-749, Korea
{sy.jin, jm.back, hy.song}@coding.yonsei.ac.kr

Abstract. In this paper, we propose a simple scheme which produces a new S-box from a given S-box. We use the well-known conversion technique between the polynomial functions over $\mathbb{F}_{2^n}$ and the boolean functions from $\mathbb{F}_2^n$ to $\mathbb{F}_2$. We have applied the scheme to Rijndael S-box and obtained 29 new S-boxes, of which only one is a bijection with better algebraic expression than the original Rijndael S-box and has the same spectral properties as the original Rijndael S-box. All others turned out to be non-bijective, and have different spectral properties, and hence, they all are inequivalent to the original as boolean functions.

Keywords: Rijndael, AES, S-box, Hadamard transform, Avalanche transform.

1 Introduction

It is widely known that the properties of substitution box (S-box) are fundamental to the secrecy of symmetric encryption algorithms after Shannon [10]. Since S-boxes are usually implemented as look up tables, they are attractive for fast software encryption algorithms [3]. Most of popular block ciphers and some of stream ciphers have adopted various S-boxes and a lot of research has been given to designing "better" S-boxes.

There have been proposed [3] several methods to generate cryptographically useful S-boxes, such as the selection of nearly optimal (for differential [2] and linear [9] attacks) boolean functions as components of the S-boxes, random generation, using finite field operations and heuristic algorithms. Among these, finite field power operation based S-boxes achieve [3] several security criteria simultaneously, and have been used in many cipher proposals including Rijndael [14,15], major portfolio of NESSIE [19], ARIA [17] in Korea, and CRYPTREC [18] in Japan, mentioned only a few.

Rijndael was selected as the Advanced Encryption Standard (AES) by the US NIST in October 2000, and published as FIPS-197 [16] in November 2001.

* This work was supported by grant No.(R01-2003-000-10330-0) from the Basic Research Program of the Korea Science & Engineering Foundation.

G. Gong et al. (Eds.): SETA 2006, LNCS 4086, pp. 153–167, 2006.

Rijndael S-box is the finite field inversion together with a bitwise affine transformation. Until Rijndael was selected as AES, it was generally claimed that such S-box would prevent algebraic attacks. There have been some progress in the research of algebraic aspect of Rijndael S-box. It is known [13, 3, 7] that every component function of Rijndael S-box is a single term trace function on finite field GF(256), and has a property of algebraic linear redundancy that is inherent in finite field exponentiation. At the same time, researchers successively have proposed several improved S-boxes. In [7], the research effort has focused on the S-boxes with no simple algebraic expression while Fuller and Millan in [3] concentrates on the S-boxes with no linear redundancy.

This paper is organized as follows. In Section 2, we first introduce some background materials including one-to-one correspondence between the polynomial functions over a finite field and the boolean functions. Some definitions which are frequently used in the cryptanalysis of boolean functions will also be given. Section 3 describes the design scheme which produces a new S-box from a given S-box working on 4-bit inputs and outputs. We apply this scheme in Section 4 to Rijndael S-box and obtain 29 new S-boxes, of which only one is a bijection with better algebraic expression than the original Rijndael S-box and has the same spectral properties as the original Rijndael S-box. All others turned out to be non-bijective, and have different spectral properties, and hence, they all are inequivalent to the original as boolean functions. We give some concluding remarks and open problems in Section 5.

2 Preliminaries

2.1 Sequences, Trace-Represented Polynomial Functions and Boolean Functions

Let $\mathbb{F}_{2^n}$ be a finite field with 2^n elements and $\mathbf{a} = \{a_t\}_{t=0}^{N-1}$ be a sequence over $\mathbb{F}_2$ of period $N = 2^n - 1$. Let α be a primitive element in $\mathbb{F}_{2^n}$. The *discrete Fourier transform* (DFT) of $\mathbf{a}$ is defined as

$$A_k = \sum_{t=0}^{N-1} a_t \alpha^{-tk}, k = 0, 1, \cdots, N-1 \; .$$

Its inverse formula is given as follows:

$$a_t = \sum_{k=0}^{N-1} A_k \alpha^{kt}, t = 0, 1, \cdots, N-1 \; .$$

For a given sequence $\mathbf{a}$, there exists a polynomial function $f(x)$ from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$, associated with $\mathbf{a}$, such that $a_t = f(\alpha^t), t = 0, 1, \cdots, N-1$. We write $\mathbf{a} \leftrightarrow f$, and call $\mathbf{a}$ as an evaluation of the function f at α. By the inverse DFT or Lagrange interpolation, we have [5]:

$$\begin{aligned} a_t &= f(x)\Big|_{x=\alpha^t}, \quad t = 0, 1, \ldots N-1 , \\ &= \sum_{j \in \Gamma(N)} Tr_1^{n_j}\left(A_j x^j\right)\Big|_{x=\alpha^t}, \quad A_j \in \mathbb{F}_{2^n} , \end{aligned} \tag{1}$$

where $\Gamma(N)$ is the set of cyclotomic coset leaders modulo N with respect to 2, C_j is the coset which contains j, $n_j = |C_j|$, $Tr_1^{n_j}(x)$ is the trace [8] function from $\mathbb{F}_{2^{n_j}}$ to $\mathbb{F}_2$, and $A_j \in \mathbb{F}_{2^{n_j}}$ is the DFT coefficient of $\mathbf{a}$. Then the sum of trace functions of (1) is a desired polynomial function and called the *trace representation of sequence* $\mathbf{a}$.

Now, let $g(x_{n-1}, \cdots, x_0)$ be a boolean function in n-variables. By applying the Lagrange interpolation, its polynomial representation $f(x)$ of $g(x_{n-1}, \cdots, x_0)$ can be determined as: (x is just indeterminant)

$$f(x) = \begin{cases} g(0, \cdots, 0) & x = 0, \\ \sum_{j=1}^{2^n-1} d_j x^j & x \in \mathbb{F}_{2^n}^* , \end{cases} \tag{2}$$

with coefficient d_j, $1 \le j \le 2^n - 1$, being

$$d_j = \sum_{\lambda \in \mathbb{F}_{2^n}^*} g(x_{n-1}, \cdots, x_0)\lambda^{-j} , \tag{3}$$

where $\lambda = \sum_{i=0}^{n-1} x_i \alpha_i$, and $\{\alpha_0, \cdots, \alpha_{n-1}\}$ is a basis of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$, denoted by $\mathbb{F}_{2^n} = \langle\{\alpha_0, \cdots, \alpha_{n-1}\}\rangle$.

A conversion from a polynomial function to a boolean function is given by

$$g(x_{n-1}, \cdots, x_0) = f\big(x_0\alpha_0 + \cdots + x_{n-1}\alpha_{n-1}\big), \text{ where } \mathbb{F}_{2^n} = \langle\{\alpha_0, \cdots, \alpha_{n-1}\}\rangle . \tag{4}$$

In the rest of this paper, by a boolean function f in n variables, we mean two notations $f(\mathbf{x}) = f(x_{n-1}, \cdots, x_0)$, $\mathbf{x} \in \mathbb{F}_2^n$ and $f(x)$, $x \in \mathbb{F}_{2^n}$ interchangeably.

2.2 Transform Domain Analysis Tools

For transform domain analysis of cryptographic functions, see Gong and Golomb [4], for example. The following definitions are mainly from [5, Ch. 6 and 10] with the same notation as above. For $\mathbf{a} \leftrightarrow f(x)$, the *Hadamard transform* (HT) of $\mathbf{a}$ or $f(x)$ is defined by

$$\widehat{f}(\lambda) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{Tr(\lambda x) + f(x)}, \quad \lambda \in \mathbb{F}_{2^n} .$$

The *Walsh transform* of a boolean function $f(\mathbf{x})$ is defined by

$$\widehat{f}(\mathbf{w}) = \sum_{\mathbf{x} \in \mathbb{F}_2^n} (-1)^{\mathbf{w}\cdot\mathbf{x} + f(\mathbf{x})}, \ \mathbf{w} \in \mathbb{F}_2^n .$$

The Hadamard transform of $f(x)$ and the Walsh transform of $f(\mathbf{x})$ have the relation:

$$\widehat{f}(\mathbf{w}) = \widehat{f}(\lambda), \ \mathbf{w} \in \mathbb{F}_2^n, \ \lambda \in \mathbb{F}_{2^n}, \text{ where } \mathbf{w} \cdot \mathbf{x} = Tr(\lambda x) \ .$$

Nonlinearity N_f of a boolean function f in n variables is defined as

$$N_f = \min_{\mathbf{w} \in \mathbb{F}_2^n, \ c \in \mathbb{F}_2} d\big(f(\mathbf{x}), \mathbf{w} \cdot \mathbf{x} + c\big) \ ,$$

where $d(\mathbf{x}, \mathbf{y})$ denotes the Hamming distance between $\mathbf{x}$ and $\mathbf{y}$, and is calculated using Hadamard transform of f:

$$\begin{aligned} N_f &= 2^{n-1} - \frac{1}{2} \max_{\mathbf{w} \in \mathbb{F}_2^n} \big|\widehat{f}(\mathbf{w})\big| \\ &= 2^{n-1} - \frac{1}{2} \max_{\lambda \in \mathbb{F}_{2^n}} \big|\widehat{f}(\lambda)\big| \ . \end{aligned} \tag{5}$$

The *Avalanche transform* (AT) or *additive correlation (convolution)* of $f(x)$ is defined by

$$(f * f)(w) = F(w) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{f(x+w)+f(x)}, \quad w \in \mathbb{F}_{2^n} \ . \tag{6}$$

Avalanche transform analysis of cryptographic functions was first introduced by Webster and Tavares [12]. We say that a boolean function f satisfies *Strict Avalanche Criterion* (SAC) if its Avalanche transform $F(\mathbf{w}) = 0$ for all $\mathbf{w}$ with binary hamming weight $\mathrm{wt}(\mathbf{w}) = 1$.

2.3 Equivalence Classes of Boolean Functions

Let f and g be two boolean functions in n-variables. If there exist a non-singular binary matrix D of order n, two n-tuple binary vectors $\mathbf{a}$ and $\mathbf{b}$, and a binary constant c such that for all $\mathbf{x} \in \mathbb{F}_2^n$

$$g(\mathbf{x}) = f\big(D\mathbf{x}^T \oplus \mathbf{a}^T\big) \oplus \mathbf{b} \cdot \mathbf{x}^T \oplus c \ ,$$

where $\mathbf{b} \cdot \mathbf{x}^T = b_1x_1 \oplus b_2x_2 \oplus \cdots \oplus b_nx_n$ denotes a linear function selected by $\mathbf{b}$, then f and g are said to be *(affine) equivalent* [3].

The absolute values of the Hadamard transform and the correlation transform are both re-arranged by affine transform and thus nonlinearity of a boolean function is unchanged under affine transform [3].

2.4 Description of Rijndael S-Box

An n-bit processing substitution box is a *a vector valued boolean function* $\mathbf{s}(\mathbf{x})$ from $\mathbb{F}_2^n$ to $\mathbb{F}_2^n$. If we let $\mathbf{s}(\mathbf{x}) = \big(s_{n-1}(\mathbf{x}), \cdots, s_1(\mathbf{x}), s_0(\mathbf{x})\big)$, then each $s_i(\mathbf{x})$,

$i = 0, \cdots, n-1$, is an ordinary boolean function in n variables and called a *component function* or *coordinate function* of the given S-box. By (4), $s_i(\mathbf{x})$, $\mathbf{x} \in \mathbb{F}_2^n$ can be identified as $s_i(x)$, $x = \sum_{i=0}^{n-1} x_i b_i \in \mathbb{F}_{2^n}$ where $\{b_0, b_1, \ldots, b_{n-1}\}$ is a basis of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$.

We take $b_i = \alpha^i$ for $0 \leq i < 8$ where α is a root of $z^8 + z^4 + z^3 + z^1 + 1$, which is the defining irreducible (but not primitive) polynomial of $\mathcal{F} = \mathbb{F}_{2^8}$ for the Rijndael cipher. This transforms eight boolean functions into eight polynomial functions from $\mathcal{F}$ to $\mathbb{F}_2$, which are

$$\begin{aligned}
s_0(x) &= Tr(\beta^{166}x^{-1}) + 1 = Tr(\beta^{83}x^{127}) + 1 \\
s_1(x) &= Tr(\beta^{53}x^{-1}) + 1 \;\; = Tr(\beta^{154}x^{127}) + 1 \\
s_2(x) &= Tr(\beta^{36}x^{-1}) \qquad\;\; = Tr(\beta^{18}x^{127}) \\
s_3(x) &= Tr(\beta^{11}x^{-1}) \qquad\;\; = Tr(\beta^{133}x^{127}) \\
s_4(x) &= Tr(\beta^{72}x^{-1}) \qquad\;\; = Tr(\beta^{36}x^{127}) \\
s_5(x) &= Tr(\beta^{76}x^{-1}) + 1 \;\; = Tr(\beta^{38}x^{127}) + 1 \\
s_6(x) &= Tr(\beta^{51}x^{-1}) + 1 \;\; = Tr(\beta^{153}x^{127}) + 1 \\
s_7(x) &= Tr(\beta^{26}x^{-1}) \qquad\;\; = Tr(\beta^{13}x^{127}),
\end{aligned} \tag{7}$$

where $\beta = \alpha + 1$ is a primitive element of $\mathcal{F}$, and $x = \sum_{i=0}^{7} x_i b_i \in \mathcal{F}$. The above algebraic expressions of component functions $s_i(x)$ have been determined by Inverse DFT or Lagrange interpolation (2), dual basis approach [13], or q-polynomial method [7].

3 Proposed Scheme of Designing a New S-Box from a Given S-Box

We will describe a proposed scheme of designing a new S-box from a given one. For convenience, we explain using a smaller size example, e.g., over $\mathbb{F}_{2^4}$.

Consider the following S-box denoted as SB-0 (the left-most one in Table 1), defined by $s(x) = x^{-1}$ over the field $\mathcal{F} = \mathbb{F}_{2^4}$ using the irreducible polynomial $g_0(z) = z^4 + z^3 + z^2 + z + 1$. Then, the following algorithm produces SB-1 and SB-2 in the middle and right-most in Table 1, respectively.

Table 1. Three S-boxes (in hexadecimal)

	00	01	10	11
00	0	1	f	a
01	8	6	5	9
10	4	7	3	e
11	d	c	b	2

SB-0

	00	01	10	11
00	0	1	a	f
01	6	8	5	9
10	2	b	d	c
11	3	e	7	4

SB-1

	00	01	10	11
00	0	c	7	0
01	6	7	4	7
10	e	2	e	6
11	8	a	5	a

SB-2

Polynomial functions for each of the 4 coordinate boolean functions of SB-0 over $\mathcal{F}$ can be found using Lagrange interpolation explained in Section 2:

$$\begin{aligned}\mathbf{s}(\mathbf{x}) &= \big(s_3(\mathbf{x}),\ s_2(\mathbf{x}),\ s_1(\mathbf{x}),\ s_0(\mathbf{x})\big), \quad \text{or} \\ s(x) &= \big(s_3(x),\ s_2(x),\ s_1(x),\ s_0(x)\big) \\ &= \big(Tr_1^4(\beta^{14}x^7), Tr_1^4(\beta^7x^7), Tr_1^4(\beta^{10}x^7), Tr_1^4(\beta^8x^7)\big), \end{aligned} \tag{8}$$

where $\mathbf{x} = (x_3, x_2, x_1, x_0)$ is the input to SB-0, $x = \sum_{i=0}^{3} x_i b_i \in \mathcal{F} \cong \langle\{b_i \mid b_i = \alpha^i, 0 \le i < 4\}\rangle$, α is a root of $g_0(z)$ which is the defining polynomial of $\mathcal{F}$, and $\beta = 1 + \alpha$ is a primitive element of $\mathcal{F}$.

Now, we let $\mathcal{K}$ be the field defined by $g_1(z) = z^4 + z^3 + 1$. Then the polynomial functions of SB-0 over $\mathcal{K}$ are determined as

$$\begin{aligned} r(x) &= \big(r_3(x),\ r_2(x),\ r_1(x),\ r_0(x)\big) \\ &= \begin{pmatrix} Tr_1^4(\gamma^{10}x + \gamma^{12}x^3 + \gamma^{14}x^7) + Tr_1^2(\gamma^{10}x^5) \\ Tr_1^4(\gamma^3x + \gamma^4x^3 + \gamma^5x^7) + Tr_1^2(x^5) \\ Tr_1^4(\gamma^9x + \gamma^{10}x^3 + \gamma^{13}x^7) + Tr_1^2(\gamma^5x^5) \\ Tr_1^4(\gamma^2x + \gamma^{13}x^3 + \gamma^6x^7) + Tr_1^2(\gamma^5x^5) \end{pmatrix}^T \end{aligned} \tag{9}$$

where $x = \sum_{i=0}^{3} x_i c_i \in \mathcal{K} \cong \langle\{c_i \mid c_i = \gamma^i, 0 \le i < 4\}\rangle$ and γ is a root of $g_1(z)$.

To obtain polynomial functions for the new S-box, which we call SB-1, we simply replace the coefficients (some powers of γ in (9)) with the corresponding powers of β. This gives new polynomial functions from (9), which are

$$\begin{aligned} h_3(x) &= Tr_1^4(\beta^{10}x + \beta^{12}x^3 + \beta^{14}x^7) + Tr_1^2(\beta^{10}x^5), \\ h_2(x) &= Tr_1^4(\beta^3x + \beta^4x^3 + \beta^5x^7) + Tr_1^2(x^5), \\ h_1(x) &= Tr_1^4(\beta^9x + \beta^{10}x^3 + \beta^{13}x^7) + Tr_1^2(\beta^5x^5), \\ h_0(x) &= Tr_1^4(\beta^2x + \beta^{13}x^3 + \beta^6x^7) + Tr_1^2(\beta^5x^5). \end{aligned}$$

Finally, to construct SB-1 shown in the middle of Table 1, we evaluate the above polynomial functions over $\mathcal{F} = \mathbb{F}_{2^4}$ with multiplication mod $g_0(z)$.

There is another irreducible polynomial of degree 4 over $\mathbb{F}_2$, which is $g_2(z) = z^4 + z + 1$. We denote $\mathcal{E}$ by the field defined by $g_2(z)$. Then, similarly, over $\mathcal{E}$, the polynomial functions of SB-0 are determined as

$$\begin{aligned} t(x) &= \big(t_3(x),\ t_2(x),\ t_1(x)\ , t_0(x)\big) \\ &= \begin{pmatrix} Tr_1^4(\delta^2x + \gamma^9x^3 + \delta^{10}x^7) + Tr_1^2(\delta^5x^5) \\ Tr_1^4(\delta^4x + \delta^{12}x^3 + \delta^{12}x^7) + Tr_1^2(x^5) \\ Tr_1^4(\delta^6x + \delta^2x^3 + \delta^{14}x^7) + Tr_1^2(x^5) \\ Tr_1^4(\delta^{11}x + \delta^{11}x^3 + \delta^2x^7) + Tr_1^2(\delta^{10}x^5) \end{pmatrix}^T \end{aligned} \tag{10}$$

where $x = \sum_{i=0}^{3} x_i d_i \in \mathcal{E} \cong \langle\{d_i \mid d_i = \delta^i, 0 \le i < 4\}\rangle$ and δ is a root of $g_2(z)$.

By replacing δ in (10) with β, we obtain another set of polynomial functions from (10):

$$
\begin{aligned}
u_3(x) &= Tr_1^4(\beta^2 x + \beta^9 x^3 + \beta^{10} x^7) + Tr_1^2(\beta^5 x^5),\\
u_2(x) &= Tr_1^4(\beta^4 x + \beta^{12} x^3 + \beta^{12} x^7) + Tr_1^2(x^5),\\
u_1(x) &= Tr_1^4(\beta^6 x + \beta^2 x^3 + \beta^{14} x^7) + Tr_1^2(x^5),\\
u_0(x) &= Tr_1^4(\beta^{11} x + \beta^{11} x^3 + \beta^2 x^7) + Tr_1^2(\beta^{10} x^5).
\end{aligned}
$$

This, in turn, gives a third S-box, SB-2, shown in the right-most of Table 1, when we evaluate the above polynomial functions over $\mathcal{F} = \mathbb{F}_{2^4}$ with multiplication mod $g_0(z)$.

Remark 1. Observe that SB-1 is a bijection but SB-2 is not. The reason why they are so different would be a topic of further research.

Remark 2. A simple calculation shows that all three S-boxes in Table 1 have the same spectral properties. That is, they have the same profiles of Hadamard transform and Avalanche transform, where the transform is applied to each of the coordinate boolean functions. It turned out that the spectral properties do not have to be all the same when this scheme is applied to larger S-boxes, which we will discuss in the next section.

4 Application of Proposed Scheme to Rijndael S-Box

4.1 Using $z^8 + z^4 + z^3 + z^2 + 1$

We apply the proposed design scheme explained in Section 3 to the original Rijndael S-box, which we denote by BOX-0. From now on, we use the parallel notations in Section 3, but $g_0(z)$ and $g_1(z)$ are changed to:

$$g_0(z) = z^8 + z^4 + z^3 + z^1 + 1, \quad \text{and} \quad g_1(z) = z^8 + z^4 + z^3 + z^2 + 1,$$

where $g_0(z)$ is the defining polynomial of $\mathbb{F}_{2^8}$ for the Rijndael cipher and $g_1(z)$ is a primitive polynomial of degree 8 over $\mathbb{F}_2$.

Recall that the polynomial functions $s_i(x)$, $0 \le i < 8$, for the coordinate boolean functions of BOX-0 were determined as in (7) over $\mathcal{F} = \mathbb{F}_{2^8}$ defined by $g_0(z)$, where $\beta = 1 + \alpha$ is a primitive element of $\mathcal{F}$, where α is a root of $g_0(z)$, and $x = \sum_{i=0}^{7} x_i b_i \in \mathcal{F} \cong \langle \{b_i | b_i = \alpha^i, 0 \le i < 8\} \rangle$.

Now, over $\mathcal{K} = \mathbb{F}_{2^8}$ defined by $g_1(z)$, the same boolean functions give some other polynomial functions $r_i(x)$, $0 \le i < 8$, where, for example,

$$
\begin{aligned}
r_7(x) = {} & Tr_1^2(\gamma^{85} x^{85}) + Tr_1^4(\gamma^{238} x^{17} + \gamma^{34} x^{51} + \gamma^{136} x^{119})\\
& + Tr_1^8(\gamma^4 x^1 + \gamma^{43} x^3 + \gamma^{60} x^5 + \gamma^3 x^7 + \gamma^{54} x^9 + \gamma^{155} x^{11})\\
& + Tr_1^8(\gamma^{86} x^{13} + \gamma^{157} x^{15} + \gamma^{157} x^{19} + \gamma^{48} x^{21} + \gamma^{163} x^{23} + \gamma^{98} x^{25})\\
& + Tr_1^8(\gamma^{50} x^{27} + \gamma^{92} x^{29} + \gamma^{67} x^{31} + \gamma^{69} x^{37} + \gamma^{181} x^{39} + \gamma^1 x^{43})\\
& + Tr_1^8(\gamma^2 x^{45} + \gamma^{194} x^{47} + \gamma^{110} x^{53} + \gamma^{145} x^{55} + \gamma^{105} x^{59} \gamma^{246} x^{61})\\
& + Tr_1^8(\gamma^{192} x^{63} + \gamma^{45} x^{87} + \gamma^{20} x^{91} + \gamma^{160} x^{95} + \gamma^{144} x^{111} + \gamma^{13} x^{127})\ ,
\end{aligned}
\tag{11}
$$

Table 2. Polynomial functions r_i's of BOX-0 over $\mathcal{K}$ (h_i's of BOX-1 over $\mathcal{F}$)

k	n_k	r_7	r_6	r_5	r_4	r_3	r_2	r_1	r_0
const.		–	**1**	**1**	–	–	–	**1**	**1**
85	2	85	0	170	0	170	170	0	85
17	4	238	0	102	136	136	68	17	119
51	4	34	102	238	17	85	17	17	85
119	4	136	0	187	85	0	∞	187	51
1	8	4	129	65	213	52	83	14	127
3	8	43	251	43	12	233	23	174	30
5	8	60	163	162	197	79	57	166	24
7	8	3	19	50	233	134	193	246	119
9	8	54	221	120	97	33	139	159	33
11	8	155	31	242	163	92	∞	2	226
13	8	86	80	199	91	17	151	208	153
15	8	157	143	74	56	242	41	86	214
19	8	157	∞	231	16	99	148	65	251
21	8	48	28	69	3	190	33	106	136
23	8	163	48	100	173	16	198	248	120
25	8	98	78	37	9	197	242	225	72
27	8	50	29	25	115	16	157	189	167
29	8	92	74	21	220	162	25	71	174
31	8	67	49	69	157	233	130	107	35
37	8	69	253	52	155	32	6	219	230
39	8	181	145	68	145	114	121	12	91
43	8	1	125	168	228	244	242	217	58
45	8	2	253	127	200	25	64	133	164
47	8	194	246	233	173	43	102	108	119
53	8	110	23	129	77	16	133	245	136
55	8	145	173	74	35	6	143	159	64
59	8	105	65	121	186	228	90	182	108
61	8	246	176	111	176	17	161	213	100
63	8	192	252	141	80	142	81	213	178
87	8	45	7	157	61	230	6	98	78
91	8	20	239	73	76	251	20	123	94
95	8	160	236	186	66	236	222	156	248
111	8	144	41	149	35	167	32	154	210
127	8	13	141	14	91	90	220	166	71
LS		254	247	255	254	254	242	255	255

where γ is a root of $g_1(z)$ in this section, and is a primitive element of $\mathcal{K}$. For the other $r_i(x)$, see Table 2.

The first and second column of Table 2 represents cyclotomic coset leaders and sizes, respectively. The values in the third column are the exponents of the coefficients of x^k in the trace representation of $r_7(x)$, with the convention of $\gamma^\infty = 0$, where γ is a primitive element in $\mathcal{K}$. The bottom row of Table 2 shows the number of nonzero terms in each $r_i(x)$. Note that these values are very large (255 is the maximum) compared to that of the expression in (7).

By replacing the coefficients (which are the powers of γ in (11)) with the corresponding powers of β, as described in Section 3, we obtain a set of 8 new polynomial functions $h_i(x)$, $0 \le i < 8$, one of which is

$$\begin{aligned} h_7(x) &= Tr_1^2(\beta^{85}x^{85}) + Tr_1^4(\beta^{238}x^{17} + \beta^{34}x^{51} + \beta^{136}x^{119}) \\ &+ Tr_1^8(\beta^{4}x^{1} + \beta^{43}x^{3} + \beta^{60}x^{5} + \beta^{3}x^{7} + \beta^{54}x^{9} + \beta^{155}x^{11}) \\ &+ Tr_1^8(\beta^{86}x^{13} + \beta^{157}x^{15} + \beta^{157}x^{19} + \beta^{48}x^{21} + \beta^{163}x^{23} + \beta^{98}x^{25}) \\ &+ Tr_1^8(\beta^{50}x^{27} + \beta^{92}x^{29} + \beta^{67}x^{31} + \beta^{69}x^{37} + \beta^{181}x^{39} + \beta^{1}x^{43}) \\ &+ Tr_1^8(\beta^{2}x^{45} + \beta^{194}x^{47} + \beta^{110}x^{53} + \beta^{145}x^{55} + \beta^{105}x^{59} + \beta^{246}x^{61}) \\ &+ Tr_1^8(\beta^{192}x^{63} + \beta^{45}x^{87} + \beta^{20}x^{91} + \beta^{160}x^{95} + \beta^{144}x^{111} + \beta^{13}x^{127}), \end{aligned} \tag{12}$$

where $\beta = 1 + \alpha$ is the primitive element of $\mathcal{F}$, where α is a root of $g_0(z)$. Now, evaluating these polynomials over $\mathcal{F} = \mathbb{F}_{2^8}$ with multiplication mod $g_0(z)$ gives a new S-box, BOX-1, shown in Table 3.

Table 3. BOX-1 (in hexadecimal)

	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	63	7c	7b	77	6b	f2	6f	c5	76	ab	fe	d7	67	2b	01	30
1	82	ca	c9	7d	fa	59	f0	47	72	c0	a4	9c	af	a2	ad	d4
2	c3	23	04	c7	05	9a	96	18	eb	27	75	b2	12	07	80	e2
3	93	26	fd	b7	cc	f7	36	3f	d8	71	31	15	34	a5	f1	e5
4	fc	20	b1	5b	53	d1	ed	00	be	39	cb	6a	cf	58	4a	4c
5	1b	6e	a0	5a	83	09	2c	1a	b3	d6	52	3b	2f	84	e3	29
6	33	85	4d	43	fb	aa	d0	ef	f9	45	02	7f	50	3c	a8	9f
7	f5	38	92	9d	40	8f	a3	51	bc	b6	21	da	ff	10	f3	d2
8	16	bb	b0	54	2d	0f	99	41	8c	a1	0d	89	e6	bf	42	68
9	28	df	55	ce	e9	87	9b	1e	f8	e1	98	11	69	d9	94	8e
a	4b	bd	8a	8b	dd	e8	74	1f	2e	25	ba	78	b4	c6	a6	1c
b	c1	86	1d	9e	61	35	b9	57	b5	66	3e	70	0e	f6	48	03
c	ac	62	d3	c2	79	e4	91	95	06	49	24	5c	e0	32	0a	3a
d	ea	f4	6c	56	ae	08	7a	65	8d	d5	a9	4e	c8	e7	37	6d
e	ee	46	b8	14	de	5e	db	0b	90	88	2a	22	dc	4f	60	81
f	c4	a7	3d	7e	5d	64	19	73	17	44	5f	97	13	ec	0c	cd

We now list some cryptographic properties of BOX-1 in parallel with those of BOX-0. We will use $h_i(x)$ in Table 2 for BOX-1 and $s_i(x)$ in (7) for BOX-0.

1. BOX-1 is a bijective map. So is BOX-0.
2. The component boolean functions of BOX-1 are balanced. So is BOX-0.
3. It is not difficult to show that the highest degree in its algebraic normal form (ANF) of a boolean function f is the maximum binary Hamming weight $\mathrm{wt}(k)$ as k runs through all the exponents in the trace representation of f [5]. For $k = 127$, $\mathrm{wt}(k) = 7$ and every coordinate function $h_i(x)$, $i = 0, \cdots, 7$,

has the term θx^{127} in its trace representation for some nonzero $\theta \in \mathbb{F}_{2^n}^*$. The ANF of any boolean function can be found by exhaustive "truth table summation" [11]. In fact, the number of linear and highest degree terms in the ANF of $h_i(x)$ and $s_i(x)$ turns out to be given as follows:

	h_0	h_1	h_2	h_3	h_4	h_5	h_6	h_7	s_0	s_1	s_2	s_3	s_4	s_5	s_6	s_7
Number of linear terms	4	3	4	4	6	3	3	3	6	4	6	4	6	2	4	4
Number of degree 7 terms	4	4	5	1	5	4	3	3	5	4	2	4	2	3	4	4

4. Since the linear span of a function or a sequence is just the number of nonzero terms in its polynomial function [5], we have:

	h_0	h_1	h_2	h_3	h_4	h_5	h_6	h_7	s_0	s_1	s_2	s_3	s_4	s_5	s_6	s_7
Linear span	255	255	242	254	254	255	247	254	9	9	8	8	8	9	9	8

5. Hadamard transform of a boolean function has a connection (5) with nonlinearity and with the first-order correlation immunity [11]. Hadamard transform profile of component functions of BOX-1 and BOX-0 are determined as:

Absolute HT value	0	4	8	12	16	20	24	28	32	Total
h_i for all $0 \leq i < 8$	17	48	36	40	34	24	36	16	5	256
s_i for all $0 \leq i < 8$	17	48	36	40	34	24	36	16	5	256

6. From the above calculation, it is easy to see that nonlinearity of every coordinate function of BOX-1 is 112, which is the same as that of BOX-0, the original Rijndael S-box.
7. The frequency distribution of Avalanche (additive correlation) transform of each component function of BOX-1 and BOX-0 is determined as:

Absolute AT value	0	8	16	24	32	Total
h_i for all $0 \leq i < 8$	32	84	74	52	13	255
s_i for all $0 \leq i < 8$	32	84	74	52	13	255

8. It is interesting to observe that for all $i = 0, 1, \cdots, 7$, h_i and s_i have the same Hadamard and Avalanche transform spectrum (as a profile), which is not an accident due to the following theorem.

Theorem 1. *Let $\Gamma = \{s_0, s_1, \cdots, s_7, h_0, h_1, \cdots, h_7\}$ be the set consisting of all the component functions of* BOX-0 *and* BOX-1*. Then any two boolean functions in Γ are pairwise equivalent.*

Proof. Since $s_i(x) = Tr(\theta_i x^{-1}) + e_i$ for some $\theta_i \in \mathbb{F}_{2^8}$, $i = 0, \cdots, 7$, and e_i is either 1 or 0 as shown in (7), it is easily shown [3, Theorem 3] that s_i and s_j are equivalent for any $0 \leq i, j \leq 7$.

Now it is enough to establish the affine equivalence between s_0 and h_i for all $i = 0, 1, \cdots, 7$. Some calculation shows that $h_0(\mathbf{x}) = s_0(\mathcal{D}_0 \mathbf{x}^T)$, where binary 8×8 square matrix $\mathcal{D}_0$ is given as

$$\mathcal{D}_0 = [\ 11_d\ \ 148_d\ \ 182_d\ \ 82_d\ \ 224_d\ \ 8_d\ \ 105_d\ \ 31_d\ ],$$

where the first column 11_d is the decimal form of $[00001011]^T$. Similarly, for $i = 1, 2, \cdots, 7$, we have $h_i(\mathbf{x}) = s_0(\mathcal{D}_i\mathbf{x}^T) + c_i$, where

$$\begin{array}{lcl}
\mathcal{D}_1 & = & [\ 51_d\ \ 150_d\ \ 235_d\ \ 156_d\ \ 223_d\ \ 77_d\ \ 28_d\ \ 1_d\ ] \\
\mathcal{D}_2 & = & [\ 47_d\ \ 78_d\ \ 142_d\ \ 86_d\ \ 149_d\ \ 164_d\ \ 62_d\ \ 240_d\ ] \\
\mathcal{D}_3 & = & [\ 35_d\ \ 112_d\ \ 68_d\ \ 4_d\ \ 213_d\ \ 186_d\ \ 121_d\ \ 129_d\ ] \\
\mathcal{D}_4 & = & [\ 26_d\ \ 94_d\ \ 156_d\ \ 1_d\ \ 172_d\ \ 55_d\ \ 85_d\ \ 124_d\ ]\ , \\
\mathcal{D}_5 & = & [\ 42_d\ \ 101_d\ \ 4_d\ \ 220_d\ \ 237_d\ \ 35_d\ \ 247_d\ \ 191_d\ ] \\
\mathcal{D}_6 & = & [\ 47_d\ \ 90_d\ \ 18_d\ \ 241_d\ \ 151_d\ \ 137_d\ \ 143_d\ \ 122_d\ ] \\
\mathcal{D}_7 & = & [\ 67_d\ \ 146_d\ \ 81_d\ \ 29_d\ \ 161_d\ \ 199_d\ \ 246_d\ \ 61_d\ ]
\end{array}$$

and constant c_i is given by $c_2 = c_3 = c_4 = c_7 = 1$ and $c_1 = c_5 = c_6 = 0$. □

9. Finally, we check SAC for BOX-1 and BOX-0.

	00000001	00000010	00000100	00001000	00010000	00100000	01000000	10000000
h_7	0	-16	-8	-24	-32	-8	16	8
h_6	24	-16	8	-8	8	-24	16	-32
h_5	8	16	24	24	24	-8	-16	-8
h_4	24	-8	-16	-8	32	0	24	16
h_3	-32	16	24	-16	8	-8	16	-16
h_2	24	-16	32	24	-16	0	0	-8
h_1	-8	0	24	-16	8	-8	8	-24
h_0	-8	16	24	-8	-8	0	16	0
s_7	-8	16	-8	-16	24	24	-16	-8
s_6	-8	8	-8	-16	0	-8	-16	-32
s_5	24	-32	0	16	24	-8	16	-8
s_4	-32	0	16	24	-8	16	-8	-16
s_3	24	8	-32	0	0	16	16	8
s_2	8	24	0	-16	0	-24	-16	-16
s_1	24	0	-16	0	-24	-16	-16	8
s_0	0	-16	0	-24	-16	-16	8	-8

Since an affine transformation rearranges additive correlation values, the Avalanche transform of h_i is possibly non-identical to that of s_i. However, for $\mathbf{w} \in \mathbb{F}_2^8$ with binary Hamming weight one, the maximum absolute correlation value of $(h_i * h_i)(\mathbf{w})$ is equal to that of $(s_j * s_j)(\mathbf{w})$ for $0 \leq i, j \leq 7$, and the frequency of occurrences of each possible values of both BOX-1 and BOX-0 are very similar. Therefore, BOX-1 and BOX-0 have almost the same level of performance in correlation aspect.

4.2 Using All Other Irreducible Polynomials of Degree 8

Analysis result of BOX-1, especially the items from 4 to 7 in the above list, and Theorem 1, shows that BOX-1 is equivalent to the original S-box of Rijndael in many aspects.

The effect of replacing the irreducible polynomial in Rijndael has been enough studied previously. Any replacement of irreducible polynomial in Rijndael cipher with different one can create a new cipher, but it is equivalent to the original in all aspects. Barkan and Biham [1] concluded that the arbitrary choice for the irreducible polynomial to be replaced works the same always, and hence, there is no advantage to changing the original irreducible polynomial with any other. Careless conclusion from the above information would lead to a guess that the remaining S-boxes, BOX-2, ... , BOX-29, using each of the remaining irreducible polynomials of degree 8, respectively, would have the similar properties. That is, every BOX-i for $2 \leq i \leq 29$ might be a balanced bijection with the same spectral properties (the same Hadamard and correlation transform profile) and whose coordinate functions would be all affine equivalent to that of Rijndael S-box. To our surprise, it turned out that this is not the case. Careful examination of the proposed scheme described in Section 3 will reveal that our scheme is completely different from simply changing the irreducible polynomial in Rijndael cipher. Instead, it is a method of constructing only a new S-box from the given one, and the whole cipher runs over the field defined by the same irreducible polynomial.

For example, we examine BOX-2, which is constructed using the irreducible polynomial $g_2(z) = z^8 + z^5 + z^3 + z^1 + 1$ in the conversion process. Again we use the parallel notations with Section 3, but in this case, we use the field $\mathcal{E}$ defined by $g_2(z)$. BOX-2 is shown in Table 4. The polynomial functions for BOX-2 are denoted by $u_i(x)$, their Hadamard transform profiles and SAC table are given in Table 5 and Table 6, respectively.

In summary, BOX-2 is completely different from BOX-1 or BOX-0:

1. BOX-2 is not bijective and no coordinate function is balanced. Therefore, it is worse against the linear attack than BOX-0.

Table 4. BOX-2 (in hexadecimal)

	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	63	12	31	1d	f9	50	e6	22	4f	2f	2e	e8	18	f1	03	08
1	4a	eb	84	c2	b9	90	34	d4	02	b6	61	6c	ea	29	46	2b
2	cd	d3	c7	f2	2f	34	9e	d4	c3	14	b3	56	7b	9d	d0	58
3	ff	d4	7e	82	85	55	90	88	21	ba	af	23	b2	aa	ba	49
4	1e	ac	27	2f	94	cb	0c	eb	7f	c3	9f	b1	53	2b	19	d2
5	78	2e	dd	ca	c3	18	a3	51	12	31	22	6e	2d	59	87	da
6	4a	ec	f2	a7	a8	1e	1b	33	5e	60	94	f5	07	f4	6d	ac
7	9b	01	64	55	93	d9	80	1c	2b	de	98	78	42	eb	65	c5
8	3f	56	f3	dc	e1	18	f0	db	59	e7	ab	cc	fa	3d	89	18
9	a8	3c	62	8b	70	55	7c	7a	0d	aa	c7	4c	9e	d4	bf	00
a	e7	48	50	7c	48	9b	89	72	cb	c4	a5	40	05	b1	00	fc
b	4a	b4	ac	85	bb	62	98	22	6d	b4	e4	b7	ac	30	d0	70
c	ce	09	bb	e8	ef	11	e6	f8	3a	14	ac	7c	75	29	c1	79
d	1b	ff	9c	31	49	7b	5a	57	cb	b6	d0	3e	b9	48	47	c8
e	1d	02	eb	7d	d7	df	31	3f	72	9c	a3	91	b5	75	c9	08
f	38	06	a4	b9	2d	f6	20	99	3a	9b	5e	6e	7e	36	58	14

Table 5. Hadamard transform profile (frequency distribution) of BOX-2

Absolute HT value	0	4	8	12	16	20	24	28	32	36	40	44	48	52	Total
u_7	27	59	45	28	21	30	25	7	5	4	2	0	3	0	256
u_6	26	45	46	42	31	22	17	13	6	4	1	2	1	0	256
u_5	22	55	42	38	32	23	18	8	10	3	4	1	0	0	256
u_4	25	45	38	33	42	31	15	17	5	2	3	0	0	0	256
u_3	23	46	44	46	34	25	16	7	5	3	4	1	2	0	256
u_2	33	53	38	32	33	22	15	15	5	6	3	0	1	0	256
u_1	22	55	40	39	35	21	21	10	6	1	3	1	1	1	256
u_0	30	44	47	41	29	20	15	16	4	6	2	1	1	0	256

Table 6. Check for SAC of BOX-2

	10000000	01000000	00100000	00010000	00001000	00000100	00000010	00000001
u_7	-8	8	-8	-24	0	-8	8	-24
u_6	16	24	-24	-24	0	-24	0	8
u_5	40	24	8	-8	-8	0	-8	-24
u_4	24	-32	16	0	8	0	56	8
u_3	24	16	-24	8	-8	8	24	-32
u_2	-8	8	-8	-8	-24	-8	24	0
u_1	0	8	8	32	16	-8	16	16
u_0	40	16	24	-16	0	16	-8	0

2. BOX-2 has worse spectrum in transform domain than BOX-0.
3. The Hadamard transform profiles of the eight component functions of BOX-2 are all distinct.
4. All coordinate functions of BOX-2 are *pairwise inequivalent* as boolean functions, which is one of the desirable characteristics of an S-box.
5. *None* of the component functions of BOX-2 has a simple algebraic expression over $\mathbb{F}_{2^n}$ with the multiplication performed modulo *any* irreducible polynomial, while *all* coordinates of BOX-0 do have the simplest equations such as (7) with the current Rijndael irreducible polynomial. Therefore, BOX-2 is better against the interpolation attack [6] than the original S-box, BOX-0.

We have experimentally checked all the remaining 27 S-boxes which are constructed from Rijndael S-box using the remaining 27 irreducible polynomials of degree 8, respectively. We have verified that all these share almost the same properties listed above with BOX-2.

5 Concluding Remarks

We proposed a simple scheme which produces a new S-box from the given S-box, which are based on operations over $\mathbb{F}_{2^n}$. The essential steps of the construction are (i) to determine the trace-represented polynomial functions of the given S-box over $\mathbb{F}_{2^n}$ with the multiplication performed modulo some other irreducible polynomial than the one originally used, (ii) to replace the coefficients in the trace-represented polynomial functions with the corresponding powers of the original primitive element, and finally, (iii) to evaluate new polynomials in $\mathbb{F}_{2^n}$ with the multiplication now performed modulo the original irreducible polynomial.

We have applied the scheme to Rijndael S-box, BOX-0, and constructed 29 different S-boxes, denoted by BOX-1, BOX-2, ... , BOX-29. All 29 S-boxes have much improved algebraic expressions over $\mathbb{F}_{2^n}$ with the multiplication performed modulo the original irreducible polynomial $g_0(z)$ (compare with (7)). Only BOX-1 has almost the same cryptographic properties as BOX-0. It is because only BOX-1 is equivalent to BOX-0 as boolean functions. Only BOX-0 and BOX-1 have the property that the algebraic expressions over $\mathbb{F}_{2^n}$ with the multiplication performed modulo some appropriate irreducible polynomial turned out to consist of a single trace function. No other S-boxes have such a simple algebraic expression.

Some theoretical developments that would be interesting are the following:

Q1 When and why the resulting S-box is a bijection or not a bijection?

Q2 When and why the resulting S-box has the same or different spectral properties as the original S-box?

Q3 Restricting to the case of Rijndael S-box, why is only BOX-1 similar to the original S-box? This is very surprising considering that $g_1(z)$ is an arbitrary choice among 29 irreducible polynomials of degree 8 over $\mathbb{F}_2$.

Q4 What are the distinctive properties of $g_1(z) = z^8 + z^4 + z^3 + z^2 + 1$ relative to $g_0(z) = z^8 + z^4 + z^3 + z^1 + 1$ compared with all other 28 irreducible polynomials of degree 8 over $\mathbb{F}_2$?

References

1. E. Barkan and E. Biham, "In how many ways can you write Rijndael?," In: Y. Zheng (Ed.), *ASIACRYPT 2002*, LNCS vol. 2501, Springer-Verlag, 2002, pp. 160–175.
2. E. Biham and A. Shamir, "Differential cryptanalysis of DES-like cryptosystems," *Journal of Cryptology*, vol. 4, pp. 3–72, 1991.
3. J. Fuller and W. Millan, "Linear redundancy in S-boxes," In: T. Johansson (Ed.), *Fast Software Encryption 2003*, LNCS vol. 2887, Springer-Verlag, 2003, pp. 74–86.
4. G. Gong and S.W. Golomb, "Transform domain analysis of DES," *IEEE Transactions on Information Theory*, vol. 45, no. 6, pp. 2065–2073, Sep., 1999.
5. S.W. Golomb and G. Gong, *Signal Design for Good Correlation: for wireless communication, cryptography, and radar.* Cambridge University Press, 2005.
6. T. Jakobsen and L.R. Knudsen, "The interpolation attack on block ciphers," In: E. Biham (Ed.), *Fast Software Encryption '97*, LNCS vol. 1267, Springer-Verlag, 1997, pp. 28–40.
7. L. Jing-mei, W. Bao-dian, C. Xiang-guo, and W. Xin-mei, "Cryptanalysis of Rijndael S-box and improvement," *Applied Mathematics and Computation*, vol. 170, pp. 958–975, 2005.
8. R. Lidl and H. Niederreiter, *Introduction to Finite Fields and Their Applications.* Cambridge University Press, 1986.

9. M. Matsui, “Linear cryptanalysis method for DES cipher,” In: T. Helleseth (Ed.), *Advances in Cryptology: Eurocrypt ’93*, LNCS vol. 765, Springer-Verlag, 1993, pp. 386–397.
10. C.E. Shannon, “Communication theory of secrecy systems,” *Bell Systems Technical Journal*, vol. 28, pp. 656–715, 1949.
11. T. Siegenthaler, “Correlation-immunity of nonlinear combining functions for cryptographic applications,” *IEEE Transactions on Information Theory*, vol. 30, no. 5, pp. 776–780, Sep., 1984.
12. A.F. Webster and S.E. Tavares, “On the design of S-box,” In: H.C. Williams (Ed.), *Advances in Cryptology: Crypto ’85*, LNCS vol. 218, Springer-Verlag, 1986, pp. 523–534.
13. A.M. Youssef and S.E. Tavares, “Affine equivalence in the AES round function,” *Discrete Applied Mathematics*, vol. 148, pp. 161–170, 2005.
14. J. Daemen and V. Rijmen, *AES proposal: Rijndael*
15. J. Daemen and V. Rijmen, *The Design of Rijndael: AES—The Advanced Encryption Standard*, Springer-Verlag, 2002.
16. FIPS-197: Advanced Encryption Standard (AES), Nov. 2001, `http://csrc.nist.gov/publications/fips`
17. Block Cipher ARIA, `http://www.nsri.re.kr/ARIA/doc/ARIA-specification.pdf`
18. CRYPTEC, `http://www.ipa.go.jp/` (in Japanese).
19. NESSIE (The New European Schemes for Signatures, Integrity and Encryption), `http://www.cryptonessie.org`