East Asian Math. J.
Vol. 37 (2021), No. 1, pp. 001–007
http://dx.doi.org/10.7858/eamj.2021.001

ON THE MODIFICATION OF FINITE FIELD BASED S-BOX

Jun Kyo Kim

Abstract. In modern block ciphers, S-box plays a very important role in the secrets of symmetric encryption algorithms. Many popular block ciphers have adopted various S-Boxes to design better S-Boxes. Among the researches, Jin et al. proposed a simple scheme to create a new S-box from Rijndael S-box. Only one of the new S-boxes for 29 is a bijection with a better algebraic representation than the original. Therefore, they asked a few questions. In this paper, we answer the following question : When the resulting S-box is bijection?

1. Introduction

S-box is a basic component of a symmetric encryption algorithm. Since S-box plays an important role in modern ciphers, many popular block ciphers adopt various S-boxes and research is underway to design more powerful S-boxes. Low differential and high nonlinearity are very much taken into account to design a strong encrypted S-box. Several methods are used to create powerful S-boxes such as heuristic algorithms, random generation, finite field operations, etc (see [6], [7], [8]).

Among the researches, Jin et al. proposed a simple scheme to create a new S-box from Rijndael S-box (see [5]). Only one of the new S-boxes for 29 is a bijection with a better algebraic representation than the original. Hence they have made some questions.

In this paper, we answer the question : When the resulting S-box is bijection? Section 2 introduces the preliminary mathematics for Cryptography, Section 3 introduce Jin at el. scheme and answer the question. We also hope this paper will be helpful to readers studying abstract algebra.

Received October 30, 2020; Accepted November 4, 2020.
2010 *Mathematics Subject Classification.* 11J70, 05A17.
Key words and phrases. Rijndael, AES, S-box.
This work was supported by the BK21 plus program through the National Research Foundation (NRF) funded by the Ministry of Education of Korea.

(pISSN 1226-6973, eISSN 2287-2833)

2. Preliminary Mathematics

2.1. Galois Field in Cryptography

A finite field is a field that contains a finite number of elements. If the characteristic of a finite field is prime p and the field is a vector space of some finite dimension n over $\mathbb{Z}/p\mathbb{Z}$, then the field has p^n elements. Finite field has two notation, $\mathbb{F}_{p^n}$ and $\mathrm{GF}(p^n)$, where the letters GF stand for "Galois field". Two finite fields of the same size are isomorphic.

The quotient ring

$$\mathbb{F}_{2^n} \cong \mathbb{F}_2[X]/\langle g(X)\rangle$$

of the polynomial ring $\mathbb{F}_2$ by the ideal generated by an irreducible polynomial $g(X)$ is a field of order 2^n. A generator for the multiplicative group of $\mathbb{F}_{p^n}^\times$ is called a primitive element, i.e there exists an element ξ in $\mathbb{F}_{p^n}$ such that

$$\mathbb{F}_{p^n}^\times = \{1, \xi, \xi^2, ..., \xi^{p^n-2}\} = \langle \xi \rangle.$$

For example, to construct a field of size 8, we could start with the irreducible polynomial x^3+x+1 over $\mathbb{F}_2 = \{0,1\}$. For example, The polynomial x^3+x+1 is irreducible in $\mathbb{F}_2[x]$, so $\mathbb{F}_2[x]/(x^3+x+1) = \mathbb{Z}[x]/(2, x^3+x+1)$ is a field of order $2^3 = 8$. Its element has the form ax^2+bx+c, where a, b, and c lie in $\mathbb{F}_2$, and the multiplication is defined by rearranging this equation $x^3 = x+1$.

2.2. Vectorial Boolean Function

Let n and m be two positive integers greater than 1. It is well known [2] that a simple Boolean function f is defined as

$$f : \mathbb{F}_2^n \to \mathbb{F}_2.$$

The functions from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$ are called (n,m)-functions. Such function F being given, the Boolean functions $f_1(x), \ldots, f_m(x)$ defined, at every $x \in \mathbb{F}_2^n$, by $F(x) = (f_1(x), \ldots, f_m(x))$, are called the coordinate functions of F. When the numbers m and n are not specified, (n,m)-functions are called multi-output Boolean functions, vectorial Boolean functions or S-boxes.

2.3. Lagrange Interpolation and Trace Function

Let $\mathbb{F}_2[\alpha]$ be a finite field with 2^n elements and β be a primitive element in $\mathbb{F}_{2^n}$. Now, let $h(x) = (s_{n-1}(x), \cdots, s_0(x))$ be a boolean function of n-variables. By applying the Lagrange interpolation, its polynomial representation $\mathfrak{f}_\beta(x)$ of $h(x)$ can be determined as

$$\begin{aligned} \mathfrak{f}_\beta : \mathbb{F}_{2^n}^\times &\to \mathbb{F}_{2^n}^\times \\ x &\mapsto \begin{cases} h(O), & \text{if } x = O; \\ h(x)x\prod_{\substack{y\in\langle\beta\rangle \\ y\neq x}}(x-y), & \text{if } x \neq O. \end{cases} \end{aligned}$$

Note that for a positive integer k, we have

$$\mathfrak{f}_\beta(\beta^k) = h(\beta^k)\beta^k \prod_{\substack{j=1 \\ j\neq k}}^{2^n-1} (\beta^k - \beta^j) = h(\beta^k) \prod_{j=1}^{2^n-1} \beta^j = h(\beta^k).$$

Since $\mathbb{F}_2[\alpha]/\mathbb{F}_2$ is a Galois extension, if γ is in $\mathbb{F}_2[\alpha]$, then the trace of γ is the sum of all the Galois conjugates of γ, i.e.

$$\mathrm{Tr}_{\mathbb{F}_2[\gamma]/\mathbb{F}_2}(\gamma) = \gamma + \gamma^2 + \cdots + \gamma^{2^{n-1}}.$$

In this setting, we have the additional property

$$\mathrm{Tr}_{\mathbb{F}_2[\alpha]/\mathbb{F}_2}(\gamma) = \mathrm{Tr}_{\mathbb{F}_2[\alpha]/\mathbb{F}_2}(\gamma^2) \in \mathbb{F}_2.$$

For convenience's sake throughout the paper we denote by Tr_1^n as $\mathrm{Tr}_{\mathbb{F}_2[\alpha]/\mathbb{F}_2}$, i.e. if γ is in $\mathbb{F}_{2^m}$ then $\mathrm{Tr}_1^m(\gamma) = \sum_{i=1}^m \gamma^{2^{i-1}}$.

3. Jin et al.'s Scheme of Designing a New S-Box from a Given S-Box

3.1. Rijndael S-box

Rijndael is selected as the AES and established as FIPS-197 in 2001 (see [3], [4]). It is a finite field operation based S-Box and key iterated block cipher and is generated by determining the multiplicative inverse for a given number in $\mathrm{GF}(2^8) = GF(2)[x]/\langle x^8 + x^4 + x^3 + x + 1\rangle$, Rijndael's finite field (see [1]). The multiplicative inverse is then transformed using the following affine transformation:

$$\begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \\ b_6 \\ b_7 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \\ a_4 \\ a_5 \\ a_6 \\ a_7 \end{bmatrix} + \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix}$$

where $[b_0, \ldots, b_7] = b_0 + b_1 x + b_2 x^2 + ... + b_7 x^7$ is the inverse of $[a_0, \ldots, a_7] = a_0 + a_1 x + a_2 x^2 + \ldots + a_7 x^7$.

3.2. Coordinate function of the Rijndael S-box

An n-bit processing substitution box is a a vector valued boolean function $s(\mathbf{x})$ from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^n}$. Let $\mathfrak{s}(\mathbf{x}) = (\mathbf{s}_{n-1}(\mathbf{x}), \cdots, \mathbf{s}_1(\mathbf{x}), \mathbf{s}_0(\mathbf{x}))$, $(x_{n-1}, \cdots, x_0) \in \mathbb{F}_2^n$, then each $\mathbf{s}_i(\mathbf{x})$, $i = 0, \ldots, n-1$, is an ordinary boolean function in n variables and is called a *component function* or *coordinate function* of the given S-box. $\mathbf{x} \in \mathbb{F}_{2^n}$ can be identified as $\mathbf{s}_i(x)$, $x = \sum_{i=0}^{n-1} x_i b_i$ where $(b_0, b_1, \ldots, b_{n-1})$ is a basis of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$.

To make the coordinate functions of the Rijndael S-box (see [9]), take $b_i = \alpha^i$ for $0 \le i \le 7$. α is a root of $x^8 + x^4 + x^3 + x + 1$, which is irreducible polynomial of $\mathbb{F}_{2^8}$ in Rijndael finite field. Note α is not primitive element. Let $\beta = \alpha + 1$ be a primitive element of $\mathbb{F}_{2^8}$ then the coordinate functions of the Rijndael S-box is given by

$$\begin{aligned}
\mathbf{s}_0(x) &= Tr(\beta^{166}x^{-1}) + 1 &&= Tr(\beta^{83}x^{127}) + 1\\
\mathbf{s}_1(x) &= Tr(\beta^{53}x^{-1}) + 1 &&= Tr(\beta^{154}x^{127}) + 1\\
\mathbf{s}_2(x) &= Tr(\beta^{36}x^{-1}) &&= Tr(\beta^{18}x^{127})\\
\mathbf{s}_3(x) &= Tr(\beta^{11}x^{-1}) &&= Tr(\beta^{133}x^{127})\\
\mathbf{s}_4(x) &= Tr(\beta^{72}x^{-1}) &&= Tr(\beta^{36}x^{127})\\
\mathbf{s}_5(x) &= Tr(\beta^{76}x^{-1}) + 1 &&= Tr(\beta^{38}x^{127}) + 1\\
\mathbf{s}_6(x) &= Tr(\beta^{51}x^{-1}) + 1 &&= Tr(\beta^{153}x^{127}) + 1\\
\mathbf{s}_7(x) &= Tr(\beta^{26}x^{-1}) &&= Tr(\beta^{13}x^{127}).
\end{aligned}$$

So $\mathfrak{s}(x)$ can be identified as

$$\begin{aligned}
\mathfrak{s}(x) &= s_7(x)\alpha^7 + s_6(x)\alpha^6 + \cdots + s_0(x)\\
&= \beta^{195} + \beta^{232}x^{127} + \beta^{96}x^{191} + x^{223} + \beta^{197}x^{239} + \beta^{185}x^{247}\\
&\quad + \beta^{99}x^{251} + \beta^{199}x^{253} + \beta^2x^{254}\\
&= (\alpha+1)^{195} + (\alpha+1)^{232}x^{127} + (\alpha+1)^{96}x^{191} + x^{223}\\
&\quad + (\alpha+1)^{197}x^{239} + (\alpha+1)^{185}x^{247}\\
&\quad + (\alpha+1)^{99}x^{251} + (\alpha+1)^{199}x^{253} + (\alpha+1)^2x^{254}.
\end{aligned}$$

3.3. Jin at el. Scheme to Design New S-box from Given S-box

There are 30 irreducible polynomials of degree 8 over $\mathbb{F}_2$:

$g_0(z) = z^8 + z^4 + z^3 + z^1 + 1$, (used in Rijndael S-Box)
$g_1(z) = z^8 + z^4 + z^3 + z^2 + 1$,
$g_2(z) = z^8 + z^5 + z^3 + z^1 + 1$,
$\vdots$
$g_{29}(z) = x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + 1$.

Jin et al. proposed a simple scheme which produces a new S-box from the given S-box, which are based on operations over $\mathbb{F}_{2^8}$. Let $g_k(z)$ be a irreducible polynomial of kth S-box where α_k is a root of $g_k(z)$, $k = 0, 1, \ldots, 29$. We define β_k as a primitive element of $\mathbb{F}_{2^8}$ and $\beta_0 = \alpha_0 + 1$.

Let $\mathbf{r}(\mathbf{x}) = (r_7(x), r_6(x), r_5(x), r_4(x), r_3(x), r_2(x), r_1(x), r_0(x))$ be an another boolean function defined on $g_2(z)$ where α_2 is a root of $g_2(z)$. The essential steps of the construction are:

(1) 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.

(2) replace the coefficients in the trace represented polynomial functions with the corresponding powers of the original primitive element.
(3) evaluate new polynomials in $\mathbb{F}_{2^n}$ with the multiplication now performed modulo the original irreducible polynomial.

For example, The trace-represented polynomial function $r_7(x)$ is

$$\begin{aligned} r_7(x) &= \mathrm{Tr}_1^2(\beta_2^{85}\mathrm{x}^{85}) + \mathrm{Tr}_1^4(\beta_2^{221}\mathrm{x}^{119} + \beta_2^{102}\mathrm{x}^{51} + \beta_2^{68}\mathrm{x}^{17}) \\ &+ \mathrm{Tr}_1^8(\beta_2^{121}\mathrm{x} + \beta_2^{133}\mathrm{x}^3 + \beta_2^{154}\mathrm{x}^5 + \beta_2^{156}\mathrm{x}^7 + \beta_2^{7}\mathrm{x}^9 + \beta_2^{134}\mathrm{x}^{11} \\ &+ \beta_2^{78}x^{13} + \beta_2^{225}x^{15} + \beta_2^{13}x^{19} + \beta_2^{75}x^{21} + \beta_2^{248}x^{23} + \beta_2^{201}x^{25} \\ &+ \beta_2^{246}x^{27} + \beta_2^{104}x^{29} + \beta_2^{224}x^{31} + \beta_2^{133}x^{37} + \beta_2^{9}x^{39} + \beta_2^{19}x^{43} \\ &+ \beta_2^{41}x^{45} + \beta_2^{231}x^{47} + \beta_2^{189}x^{53} + \beta_2^{22}x^{55} + \beta_2^{88}x^{59} + \beta_2^{92}x^{61} \\ &+ \beta_2^{120}x^{63} + \beta_2^{197}x^{87} + \beta_2^{62}x^{91} + \beta_2^{178}x^{95} + \beta_2^{202}x^{111} + \beta_2^{142}x^{127}) \end{aligned}$$

where $\beta_2 = \alpha_2^{59} = 1 + \alpha_2 + \alpha_2^2 + \alpha_2^3 + \alpha_2^4$ is a primitive element of $\mathbb{F}_2[\alpha_2]$. By replacing β_2 into β_0, we obtain another set of 8 polynomial functions $\mathbf{h}(\mathbf{x})$. For example,

$$\begin{aligned} h_7(x) &= \mathrm{Tr}_1^2(\beta_0^{85}\mathrm{x}^{85}) + \mathrm{Tr}_1^4(\beta_0^{221}\mathrm{x}^{119} + \beta_0^{102}\mathrm{x}^{51} + \beta_0^{68}\mathrm{x}^{17}) \\ &+ \mathrm{Tr}_1^8(\beta_0^{121}\mathrm{x} + \beta_0^{133}\mathrm{x}^3 + \beta_0^{154}\mathrm{x}^5 + \beta_0^{156}\mathrm{x}^7 + \beta_0^{7}\mathrm{x}^9 + \beta_0^{134}\mathrm{x}^{11} \\ &+ \beta_0^{78}x^{13} + \beta_0^{225}x^{15} + \beta_0^{13}x^{19} + \beta_0^{75}x^{21} + \beta_0^{248}x^{23} + \beta_0^{201}x^{25} \\ &+ \beta_0^{246}x^{27} + \beta_0^{104}x^{29} + \beta_0^{224}x^{31} + \beta_0^{133}x^{37} + \beta_0^{9}x^{39} + \beta_0^{19}x^{43} \\ &+ \beta_0^{41}x^{45} + \beta_0^{231}x^{47} + \beta_0^{189}x^{53} + \beta_0^{22}x^{55} + \beta_0^{88}x^{59} + \beta_0^{92}x^{61} \\ &+ \beta_0^{120}x^{63} + \beta_0^{197}x^{87} + \beta_0^{62}x^{91} + \beta_0^{178}x^{95} + \beta_0^{202}x^{111} + \beta_0^{142}x^{127}). \end{aligned}$$

Evaluating the new polynomials $h_i(z)$,$0 \le i \le 8$ is in $\mathbb{F}_{2^n}$, with the multiplication performing modulo the original irreducible polynomial $g_0(z)$ gives a new S-Box.

They have applied the steps to Rijndael S-Box and constructed 29 different S-boxes. But only one is to be a bijective to given S-box and all others turned out to be non-bijective. Hence they made some questions. One of them is the following:

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

3.4. Scheme to Design a Bijective S-box

In this section, let k be a fixed nonnegative integer less than 30. If the function η_k from $\mathbb{F}_2(\alpha_0)$ to $\mathbb{F}_2(\alpha_k)$ is an isomorphism, then the S-Box$_k$ is the composition of the following steps :

(1) Let $t = (a_0, ..., a_7) \in \mathbb{F}_2^7$.
(2) $H_0(t) := a_0 + a_1\alpha_0 + ... + a_7\alpha^7$.
(3) $\beta_0^{d_t} = a_0 + a_1\alpha_0 + ... + a_7\alpha_0^7$ for some nonnegative integer $d_t < 255$.
(4) If $b_0 + b_1\beta_k^1 + ... + b_7\beta_k^7 = c_0 + c_1\alpha_k^1 + ... + c_7\alpha_k^7$, then $\mathbf{h} \circ \mathbf{r}(\beta_0^{d_t}) := c_0 + c_1\alpha_0 + ... + c_7\alpha_0^7$.

(5) $H_0^{-1}(c_0 + c_1\alpha_0 + ... + c_7\alpha_0^7) = (c_0, c_1, ..., c_k) \in \mathbb{F}_2^7$.

So if the function η_k is an isomorphism, then S-Box$_k$ is a bijective function. You can check by programming that if η_k is not an isomorphism, then S-box$_k$ is not a bijective function.

So S-box $_k$ is a bijective function only if η_k is a bijective function. The primitive root of each η_k is :

	primitive root		primitive root		primitive root
g_1(z)	α_1	g_2(z)	α_2^{59}	g_3(z)	α_3^{91}
g_4(z)	$(\alpha_4+1)^{91}$	g_5(z)	$(\alpha_5+1)^{59}$	g_6(z)	α_6^{13}
g_7(z)	α_7^7	g_8(z)	α_8^{61}	g_9(z)	α_9^{47}
g_{10}(z)	α_{10}^{37}	g_{11}(z)	α_{11}^{127}	g_{12}(z)	$(\alpha_{12}+1)^{127}$
g_{13}(z)	$\left(\alpha_{13}^3+1\right)^{53}$	g_{14}(z)	α_{14}^{53}	g_{15}(z)	$\left(\alpha_{15}^2+\alpha_{15}\right)^{91}$
g_{16}(z)	α_{16}^{11}	g_{17}(z)	$(\alpha_{17}+1)^{29}$	g_{18}(z)	$(\alpha_{18}+1)^{23}$
g_{19}(z)	α_{19}^{19}	g_{20}(z)	$\left(\alpha_{20}^2+\alpha_{20}\right)^{13}$	g_{21}(z)	$\left(\alpha_{21}^2+\alpha_{21}+1\right)^{127}$
g_{22}(z)	α_{22}^{43}	g_{23}(z)	α_{23}^{23}	g_{24}(z)	$\left(\alpha_{24}^2+\alpha_{24}+1\right)^{127}$
g_{25}(z)	$\left(\alpha_{25}^2+\alpha_{25}\right)^{13}$	g_{26}(z)	α_{26}^{29}	g_{27}(z)	$\left(\alpha_{27}^2+\alpha_{27}\right)^{91}$
g_{28}(z)	α_{28}^{31}	g_{29}(z)	$(\alpha_{29}+1)^{53}$		

4. Conclusion

Jin at el. have propose a simple scheme producing a new S-box from the given S-box and made some questions. We answer the question : When the resulting S-box is bijection? There are three steps in the existing step, but with Galois theory you can skip replacing the coefficients with a trace representation polynomial function. This scheme can easily form a new S-box using the bijective coordinate function. Unfortunately, what's vulnerable to encryption is an algebraically unstable feature. This type of encryption is not preferred. We also hope this paper will help you apply Galois Theorem.

References

[1] C. Carlet, *Vectorial Boolean Functions for Cryptography,* Cambridge University Press, 2006.

[2] Joan Daemen, Vincent Rijmen, *The Design of Rijndael: AESThe Advanced Encryption Standard,* Springer-Verlag, 2002.

[3] Joan Daemen, Vincent Rijmen, *AES Proposal: Rijndael,* National Institute of Standards and Technology, 2003.

[4] N. Ferguson, R. Schroeppel, D. Whiting, *A simiple algebraic representation of Rijndael,* In S. Vaudenay and A. Youssef, editors, Proceedings of Selected Areas in Cryptography, LNCS, Springer-Verlag, (2001), 103–111.

[5] S-Y. Jin, J-M. Baek, H-Y. Song, *Improved Rijndael-like S-Box and its transform domain analysis,* Sequences and Their Applications SETA 2006, LNCS, vol. 4086, (2006), 153–167.

[6] N. Kokash, *An introduction to heuristic algorithms,* Department of Informatics and Telecommunications, 2005.

[7] D. Lambi, *S-box design method based on improved one-dimensional discrete chaotic map,* Journal of Information and Telecommunication, vol. 2- Issue 2, (2018), 181–191.

[8] J. Liu, W. Li and G. Bai, *An improved S-Box of lightweight block cipher roadrunner for hardware optimization,* China Semiconductor Technology International Conference (CSTIC), Shanghai, (2018), 1–4.

[9] A.M. Youssef, S.E. Tavares, *Affine equivalence in the AES round function,* affine equivalence in the AES round function, (2005), 161–170.

Jun Kyo Kim
Department of Mathematics, Pusan National University, Busan 609-735,
Republic of Korea
E-mail address: junkyo@pusan.ac.kr