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

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

{sy.jin, jm.baek, hysong}@yonsei.ac.kr
Coding and Information Theory Lab
Yonsei University, Seoul, KOREA

Sequences and Their Applications '06,
September 24–28, 2006, Beijing, China

Outline

Representation of Boolean Function

- Representation of **boolean function in n-variables**
  1. Truth table representation or Algebraic Normal Form (ANF): $f(\mathbf{x}) = f(x_{n-1}, \cdots, x_0), \mathbf{x} \in \mathbb{F}_2^n$
  2. (Trace represented) polynomial function: $f(x)$, $x \in \mathbb{F}_{2^n}$
- **Lagrange interpolation**: conversion from $f(\mathbf{x}), \mathbf{x} \in \mathbb{F}_2^n$ to $f(x), x \in \mathbb{F}_{2^n}$
  - $f(x) = \begin{cases} f(0, \cdots, 0) & x = 0, \\ \sum_{j=1}^{2^n-1} d_j x^j & x \in \mathbb{F}_{2^n}^* \end{cases}$ (x: indeterminant)
  - $d_j = \sum_{\lambda \in \mathbb{F}_{2^n}^*} g(x_{n-1}, \cdots, x_0) \lambda^{-j}$ 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 $\mathbb{F}_2$ ($\mathbb{F}_{2^n} = \langle \{\alpha_0, \cdots, \alpha_{n-1}\} \rangle$)
- **Evaluation**: inverse conversion from $f(x)$ to $f(\mathbf{x})$
  - $f(\mathbf{x}) = f(x_{n-1}, \cdots, x_0) = f\left(x_0 \alpha_0 + \cdots + x_{n-1} \alpha_{n-1}\right)$
  - $\mathbb{F}_{2^n} = \langle \{\alpha_0, \cdots, \alpha_{n-1}\} \rangle$

Some Definitions

- *Hadamard (Walsh) transform* of $f(\mathbf{x})$: $\widehat{f}(\mathbf{w}) = \sum_{\mathbf{x}\in\mathbb{F}_2^n}(-1)^{\mathbf{w}\cdot\mathbf{x}+f(\mathbf{x})}$, $\mathbf{w}\in\mathbb{F}_2^n$
- *Nonlinearity* N_f of $f(\mathbf{x})$:
  $N_f = \min_{\mathbf{w}\in\mathbb{F}_2^n,\ c\in\mathbb{F}_2} d\big(f(\mathbf{x}), \mathbf{w}\cdot\mathbf{x}+c\big) = 2^{n-1} - \frac{1}{2}\max_{\mathbf{w}\in\mathbb{F}_2^n}|\widehat{f}(\mathbf{w})|$
- *Additive correlation (Avalanche) transform* of $f(\mathbf{x})$:
  $(f * f)(\mathbf{w}) = F(\mathbf{w}) = \sum_{\mathbf{x}\in\mathbb{F}_{2^n}}(-1)^{f(\mathbf{x}+\mathbf{w})+f(\mathbf{x})}, \quad \mathbf{w}\in\mathbb{F}_{2^n}$
- Boolean function f satisfies **SAC** (Strict Avalanche Criterion) if $F(\mathbf{w}) = 0$, for all $\mathbf{w}$ with $\mathrm{wt}(\mathbf{w}) = 1$.
- Two boolean functions f and g are **equivalent** if there exist D, $\mathbf{a}$ and $\mathbf{b}$, and c such that $g(\mathbf{x}) = f\big(D\mathbf{x}^T \oplus \mathbf{a}^T\big) \oplus \mathbf{b}\cdot\mathbf{x}^T \oplus c$, for all $\mathbf{x}\in\mathbb{F}_2^n$.

Toy Example

SB-0

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

Read SB-0 as

Input	Output
0011	a: 0000
0111	9: 1001
1011	e: 1110
1111	2: 0010

SB-1

	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-2

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

Toy Example: Finite Field with 2^4 elements

- Three irreducible polynomials of degree 4 over $\mathbb{F}_2$

	$\mathscr{F}$	$\mathscr{K}$	$\mathscr{E}$
Irreducible polynomial	$z^4+z^3+z^2+z+1$ $(=g_0(z))$	z^4+z^3+1 $(=g_1(z))$	z^4+z+1 $(=g_2(z))$
Primitive element	$\beta=\alpha+1$	γ	δ
Basis	$\{1,\alpha^1,\alpha^2,\alpha^3\}$	$\{1,\gamma^1,\gamma^2,\gamma^3\}$	$\{1,\delta^1,\delta^2,\delta^3\}$

- Example
  - $\mathbf{x}=(x_3,x_2,x_1,x_0)\in\mathbb{F}_2^4 \longleftrightarrow x=x_3\alpha^3+x_2\alpha^2+x_1\alpha^1+x_0\alpha^0\in\mathscr{F}$
  - Multiplication in $\mathscr{F}$ performed modulo $g_0(z)$, in $\mathscr{K}$ modulo $g_1(z)$, and in $\mathscr{E}$ modulo $g_2(z)$, respectively

Toy Example: SB-0 in finite field terminology

SB-0

Input				Output			
0	0	0	0	0	0	0	0
0	0	0	1	0	0	0	1
0	0	1	0	1	1	1	1
0	0	1	1	1	0	1	0
0	1	0	0	1	0	0	0
0	1	0	1	0	1	1	0
0	1	1	0	0	1	0	1
0	1	1	1	1	0	0	1
1	0	0	0	0	1	0	0
1	0	0	1	0	1	1	1
1	0	1	0	0	0	1	1
1	0	1	1	1	1	1	0
1	1	0	0	1	1	0	1
1	1	0	1	1	1	0	0
1	1	1	0	1	0	1	1
1	1	1	1	0	0	1	0
$x_3 x_2 x_1 x_0$							

1. SB-0: interpretation over $\mathscr{F}$
   - output: $\left(s_3(\mathbf{x}), s_2(\mathbf{x}), s_1(\mathbf{x}), s_0(\mathbf{x})\right) \in \mathbb{F}_2^4$
   - $\mathbf{x} = (x_3, x_2, x_1, x_0) \in \mathbb{F}_2^4 \longleftrightarrow$
     $x = x_3\alpha^3 + x_2\alpha^2 + x_1\alpha^1 + x_0\alpha^0 \in \mathscr{F}$
   - output: $\left(s_3(\mathbf{x}), s_2(\mathbf{x}), s_1(\mathbf{x}), s_0(\mathbf{x})\right) =$
     $\left(tr_1^4(\beta^{14}x^7), tr_1^4(\beta^7 x^7), tr_1^4(\beta^{10}x^7), tr_1^4(\beta^8 x^7)\right)$

2. SB-0: interpretation over $\mathscr{K}$
   - output: $\left(r_3(\mathbf{x}), r_2(\mathbf{x}), r_1(\mathbf{x}), r_0(\mathbf{x})\right) \in \mathbb{F}_2^4$
   - with $\mathbf{x} = (x_3, x_2, x_1, x_0) \in \mathbb{F}_2^4 \longleftrightarrow$
     $x = x_3\gamma^3 + x_2\gamma^2 + x_1\gamma^1 + x_0\gamma^0 \in \mathscr{K}$
   - output:
     $r_3(x) = tr_1^4(\gamma^{10}x + \gamma^{12}x^3 + \gamma^{14}x^7) + tr_1^2(\gamma^{10}x^5)$
     $r_2(x) = tr_1^4(\gamma^3 x + \gamma^4 x^3 + \gamma^5 x^7) + tr_1^2(x^5)$
     $r_1(x) = tr_1^4(\gamma^9 x + \gamma^{10}x^3 + \gamma^{13}x^7) + tr_1^2(\gamma^5 x^5)$
     $r_0(x) = tr_1^4(\gamma^2 x + \gamma^{13}x^3 + \gamma^6 x^7) + tr_1^2(\gamma^5 x^5)$

Toy Example: step by step algorithm from SB-0 to SB-1

SB-0

Input	Output
0000	0000
0001	0001
0010	1111
0011	1010
0100	1000
0101	0110
0110	0101
0111	1001
1000	0100
1001	0111
1010	0011
1011	1110
1100	1101
1101	1100
1110	1011
1111	0010

(1a) SB-0 interpreted over $\mathscr{F}$:

$$\begin{aligned} s_3 &: \quad tr_1^4(\beta^{14}x^7) \\ s_2 &: \quad tr_1^4(\beta^{7}x^7) \\ s_1 &: \quad tr_1^4(\beta^{10}x^7) \\ s_0 &: \quad tr_1^4(\beta^{8}x^7) \end{aligned}$$

(1b) SB-0: interpreted over $\mathscr{K}$:

$$\begin{aligned} r_3(x) &: \quad tr_1^4(\gamma^{10}x+\gamma^{12}x^3+\gamma^{14}x^7)+tr_1^2(\gamma^{10}x^5) \\ r_2(x) &: \quad tr_1^4(\gamma^{3}x+\gamma^{4}x^3+\gamma^{5}x^7)+tr_1^2(x^5) \\ r_1(x) &: \quad tr_1^4(\gamma^{9}x+\gamma^{10}x^3+\gamma^{13}x^7)+tr_1^2(\gamma^{5}x^5) \\ r_0(x) &: \quad tr_1^4(\gamma^{2}x+\gamma^{13}x^3+\gamma^{6}x^7)+tr_1^2(\gamma^{5}x^5) \end{aligned}$$

(2) Modified: (coeff. & func. image over $\mathscr{F}$):

$$\begin{aligned} h_3(x) &: \quad tr_1^4(\beta^{10}x+\beta^{12}x^3+\beta^{14}x^7)+tr_1^2(\beta^{10}x^5) \\ h_2(x) &: \quad tr_1^4(\beta^{3}x+\beta^{4}x^3+\beta^{5}x^7)+tr_1^2(x^5) \\ h_1(x) &: \quad tr_1^4(\beta^{9}x+\beta^{10}x^3+\beta^{13}x^7)+tr_1^2(\beta^{5}x^5) \\ h_0(x) &: \quad tr_1^4(\beta^{2}x+\beta^{13}x^3+\beta^{6}x^7)+tr_1^2(\beta^{5}x^5) \end{aligned}$$

(3) Evaluation over $\mathscr{F} \longrightarrow$ SB-1

SB-1

Input	Output
0000	0000
0001	0001
0010	1010
0011	1111
0100	0110
0101	1000
0110	0101
0111	1001
1000	0010
1001	1011
1010	1101
1011	1100
1100	0011
1101	1110
1110	0111
1111	0100

Toy Example: SB-0 $\longrightarrow$ SB-2 (same way)

SB-0

Input	Output
0000	0000
0001	0001
0010	1111
0011	1010
0100	1000
0101	0110
0110	0101
0111	1001
1000	0100
1001	0111
1010	0011
1011	1110
1100	1101
1101	1100
1110	1011
1111	0010

(1a) SB-0 interpreted over $\mathscr{F}$:

$$
\begin{aligned}
s_3 &: \quad tr_1^4(\beta^{14}x^7)\\
s_2 &: \quad tr_1^4(\beta^{7}x^7)\\
s_1 &: \quad tr_1^4(\beta^{10}x^7)\\
s_0 &: \quad tr_1^4(\beta^{8}x^7)
\end{aligned}
$$

(1b) SB-0: interpreted over $\mathscr{E}$:

$$
\begin{aligned}
t_3(x) &: \quad tr_1^4(\delta^2 x+\delta^9 x^3+\delta^{10}x^7)+tr_1^2(\delta^5 x^5)\\
t_2(x) &: \quad tr_1^4(\delta^4 x+\delta^{12} x^3+\delta^{12}x^7)+tr_1^2(x^5)\\
t_1(x) &: \quad tr_1^4(\delta^6 x+\delta^2 x^3+\delta^{14}x^7)+tr_1^2(x^5)\\
t_0(x) &: \quad tr_1^4(\delta^{11} x+\delta^{11} x^3+\delta^2 x^7)+tr_1^2(\delta^{10}x^5)
\end{aligned}
$$

(2) Modified: (coeff. & func. image over $\mathscr{F}$):

$$
\begin{aligned}
u_3(x) &: \quad tr_1^4(\beta^2 x+\beta^9 x^3+\beta^{10} x^7)+tr_1^2(\beta^5 x^5)\\
u_2(x) &: \quad tr_1^4(\beta^4 x+\beta^{12} x^3+\beta^{12}x^7)+tr_1^2(x^5)\\
u_1(x) &: \quad tr_1^4(\beta^6 x+\beta^2 x^3+\beta^{14}x^7)+tr_1^2(x^5)\\
u_0(x) &: \quad Tr_1^4(\beta^{11} x+\beta^{11} x^3+\beta^2 x^7)+tr_1^2(\beta^{10}x^5)
\end{aligned}
$$

(3) Evaluation over $\mathscr{F} \longrightarrow$ SB-2

SB-2

Input	Output
0000	0000
0001	1100
0010	0111
0011	0000
0100	0110
0101	0111
0110	0100
0111	0111
1000	1110
1001	0010
1010	1110
1011	0110
1100	1000
1101	1010
1110	0101
1111	1010

Toy Example (Cont'd)

	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

Figure: Three S-boxes

Application to Rijndael S-Box: $\mathbb{F}_{2^8}$

- 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)
  - $g_1(z) = z^8 + z^4 + z^3 + z^2 + 1$,
  - $g_2(z) = z^8 + z^5 + z^3 + z^1 + 1$,
  - ....., $g_{29}(z)$
- Parallel notation

	$\mathscr{F}$	$\mathscr{K}$	$\mathscr{E}$
Irreducible polynomial	$g_0(z)$	$g_1(z)$	$g_2(z)$
Primitive element	$\beta = \alpha + 1$	γ	δ
Basis	$\{\alpha^0, \cdots, \alpha^7\}$	$\{\gamma^0, \cdots, \gamma^7\}$	$\{\delta^0, \cdots, \delta^7\}$

  - $\mathbf{s}(x) = \left(s_7(x), s_6(x), \cdots, s_0(x)\right)$
  - $x = x_7\alpha^7 + \cdots + x_0\alpha^0 \in \mathscr{F}$

Application to Rijndael S-Box: Original S-box

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

BOX-0: S-BOX in Rijndael
- adopted as AES
- field inversion & bitwise affine transform
- input: $\mathbf{x} = (x_7, \cdots, x_0) \in \mathbb{F}_2^8$
- output: $\big(s_7(\mathbf{x}), \cdots, s_0(\mathbf{x})\big) \in \mathbb{F}_2^8$

- Polynomial representation of BOX-0
  - Lagrange interpolation (DFT technique), Dual basis approah (Youssef & Tavares, 2005), q-polynomial method (Jing-mei, et. al, 2005), etc.
  - $s_0(x) = Tr(\beta^{166} x^{-1}) + 1$
  - $s_1(x) = Tr(\beta^{53} x^{-1}) + 1$
  - $s_2(x) = Tr(\beta^{36} x^{-1})$
  - $s_3(x) = Tr(\beta^{11} x^{-1})$
  - $s_4(x) = Tr(\beta^{72} x^{-1})$
  - $s_5(x) = Tr(\beta^{76} x^{-1}) + 1$
  - $s_6(x) = Tr(\beta^{51} x^{-1}) + 1$
  - $s_7(x) = Tr(\beta^{26} x^{-1})$

Application to Rijndael S-Box: from BOX-0 to BOX-1

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

BOX-0 $\longrightarrow$ BOX-1: the same way

1. B0X-0: given Rijndael S-box defined on $\mathscr{F}$
2. $r_i(x)$: poly. expression of BOX-0 over $\mathscr{K}$

$$r_7(x) = tr_1^2(\gamma^{85}x^{85}) + tr_1^4(\gamma^{238}x^{17} + \gamma^{34}x^{51} + \gamma^{136}x^{119}) + tr_1^8(\gamma^4 x^1 + \gamma^{43}x^3 + \cdots + \gamma^{144}x^{111} + \gamma^{13}x^{127})$$

3. $h_i(x)$: modified polynomial function for BOX-1
   - β instead of γ (coefficients replacement)

$$h_7(x) = tr_1^2(\beta^{85}x^{85}) + tr_1^4(\beta^{238}x^{17} + \beta^{34}x^{51} + \beta^{136}x^{119}) + tr_1^8(\beta^4 x^1 + \beta^{43}x^3 + \cdots + \beta^{144}x^{111} + \beta^{13}x^{127})$$

   - $h_i(x)$: over $\mathscr{F}$ NOT over $\mathscr{K}$ (multiplication modulo $g_0(z)$ NOT by $g_1(z)$)
4. BOX-1: by evaluating $h_i(x)$ $(i = 0, \cdots, 7)$ over $\mathscr{F}$

Application to Rijndael S-Box: modified S-box, BOX-1

	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

Figure: BOX-1: modified S-box (in hexadecimal)

Properties of BOX-1

1. BOX-1: bijection; All coordinate functions: balanced
2. In ANF

	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
# of linear terms	4	3	4	4	6	3	3	3	6	4	6	4	6	2	4	4
# of degree 7 terms	4	4	5	1	5	4	3	3	5	4	2	4	2	3	4	4

3. Linear span

	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
LS	255	255	242	254	254	255	247	254	9	9	8	8	8	9	9	8

4. Spectral properties: Hadamard transform profile

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

Nonlinearity: $N_f = 112$

Properties of BOX-1 (Cont'd)

Spectral properties: Avalanche transform

1. Avalanche transform profile

|AT value|	0	8	16	24	32	Total
h_i, $0 \le i < 8$	32	84	74	52	13	255
s_i, $0 \le i < 8$	32	84	74	52	13	255

2. Strict Avalanche Criterion: similar performance with Rijndael S-box

	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

Properties of BOX-1 (Cont'd)

Theorem

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.

1. Equivalence between s_i and s_j, $(0 \le i, j < 8)$: obvious
2. Equivalence between s_0 and h_k, $k = 0, 1, \cdots, 8$: see p. 163

□

BOX-2

	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

Figure: BOX-2: modified S-box using $g_2(z) = z^8 + z^5 + z^3 + z^1 + 1$

Properties of BOX-2 (and All Others)

1. BOX-2: non-bijective; Its coordinate functions: not balanced
2. Hadamard transform spectrum: degraded, but pairwise distinct (⇒inequivalent) component functions

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

3. Coordinate functions: no simple algebraic expression over $\mathbb{F}_{2^n}$ with the multiplication modulo any irreducible polynomial
4. Worse Avalanche spectrum: check for SAC

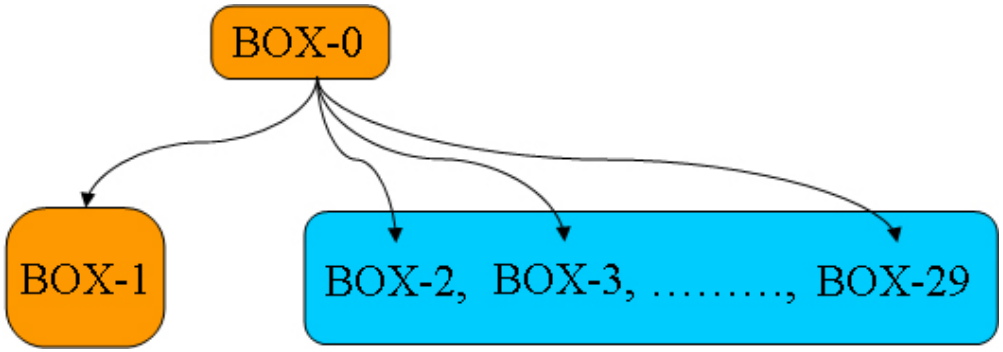
	10000000	01000000	00100000	00010000	00001000	00000100	00000010	00000001
u_7	-8	8	-8	-24	0	-8	8	-24
u_6	16	24	-24	-24	0	-24	0	8
u_5	40	24	8	-8	-8	0	-8	-24
u_4	24	-32	16	0	8	0	56	8
u_3	24	16	-24	8	-8	8	24	-32
u_2	-8	8	-8	-8	-24	-8	24	0
u_1	0	8	8	32	16	-8	16	16
u_0	40	16	24	-16	0	16	-8	0

Summary of Proposed Scheme

Essential steps of the construction

1. 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
2. To replace the coefficients in the trace-represented polynomial functions with the corresponding powers of the original primitive element
3. To evaluate new polynomials in $\mathbb{F}_{2^n}$ with the multiplication now performed modulo the original irreducible polynomial.

Open Questions



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? (Why interesting? Note 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 $\mathbb{F}_2$?