Malaysian Journal of Mathematical Sciences 9(S) June: 21-35 (2015)
Special Issue: The 4th International Cryptology and Information Security Conference 2014 (Cryptology 2014)

MALAYSIAN JOURNAL OF MATHEMATICAL SCIENCES

Journal homepage: http://einspem.upm.edu.my/journal

Improved S-Box Construction from Binomial Power Functions

[1,2*]Herman Isa, [1]Norziana Jamil and [2]Muhammad Reza Z'aba

*[1]College of Information Technology,
Universiti Tenaga Nasional (UNITEN), Selangor, Malaysia*

*[2]Cryptography Lab, MIMOS Berhad,
Technology Park Malaysia, Kuala Lumpur, Malaysia*

E-mail: herman.isa@mimos.my

*Corresponding author

ABSTRACT

Substitution boxes with strong cryptographic properties are commonly used in block ciphers to provide the crucial property of nonlinearity. This is important to resist standard attacks such as linear and differential cryptanalysis. A cryptographically-strong S-box must have high nonlinearity, low differential uniformity and high algebraic degree. In this paper, we improve previous S-box construction based on binomial operation on two power functions over the finite field $\mathbb{F}_{2^8}$. By widening the scope of the power function and introducing new manipulation techniques, we managed to obtain cryptographically-strong S-boxes which are better than the previous construction.

Keyword: S-box construction, binomial power functions, nonlinearity, bijective, substitution boxes.

1. INTRODUCTION

In his seminal work in 1949, Shannon defined the property of confusion which should exist in an encryption system (Shannon, 1949). Basically confusion is required so that the ciphertext is related to both the plaintext and secret key, in a complex way. In modern block ciphers, this property can be provided by a component called a Substitution box (S-box). Since an S-box plays an important role in a block cipher, it must be cryptographically strong to resist various attacks such as differential (Biham et al., 1991) and linear cryptanalysis (Matsui, 1994). A cryptographically strong S-box should have high nonlinearity (NL), low differential uniformity (DU) and high algebraic degree (AD).

Generally, the construction of an S-box can be categorized into three generic methods which are random search, evolutionary or heuristic method and lastly mathematical function approaches. In Isa et al., 2013, the authors use the combination of mathematical function approach and heuristic method in their proposed S-boxes construction. In detail, they proposed the construction of an S-box using binomial operation between a non-permutation power function with another power function in the finite field $\mathbb{F}_{2^8}$. The resulting function's codomain is analysed to determine elements which are mapped by more than one input in its domain. These are referred to as *redundant* elements. If these elements exist, then the function is further manipulated using a heuristic method. The final S-box is produced if it exhibits strong cryptographic properties. They obtained an S-box which has a NL of 106, DU of 6 and AD of 7. We denote this as the tuple (106, 6, 7). Furthermore, the S-box is ranked sixth out of 20 where S-boxes are sorted according to their NL, then DU and AD. The best known S-box (e.g. AES (Daemen et al., 2002) has a property of (112, 4, 7).

Inspired by the uniqueness of cryptographic properties exhibits from the binomial power functions, we improve Isa et al., 2013 construction by widening the scope of the power functions over the finite field $\mathbb{F}_{2^8}$ to include both permutation and non-permutation. Furthermore, in analysing the redundant elements, we introduce two methods which are addition and multiplication. Using these approaches, we obtained three different S-boxes which have the cryptographic properties of (108, 4, 7), (108, 6, 4) and (106, 6, 7) respectively. Two of these S-boxes are better than the one proposed by Isa et al. (2013).

The rest of the paper is organized as follows. In the second section, the main cryptographic properties of an S-box are discussed. In the third section, we present and discuss our S-box construction and its findings. The paper is concluded in the last section.

2. S-BOX PROPERTIES

An S-box needs to have at least three strong cryptographic properties which are high nonlinearity (NL), low differential uniformity (DU) and high algebraic degree (AD). In this paper, our focus is bijective S-boxes over the finite field $\mathbb{F}_{2^8}$.

Let $\mathbb{F}_2$ and $\mathbb{F}_{2^n}$ be a finite field with 2 and 2^n elements, respectively. An $n \times n$ S-box is a Boolean map:

$$F: \mathbb{F}_{2^n} \to \mathbb{F}_{2^n} = \left(f_1(x_1, \dots, x_n), f_2(x_1, \dots, x_n), \dots, f_n(x_1, \dots, x_n)\right)$$

Nonlinearity. Let $c = (c_1, c_2, \dots, c_n)$ be a nonzero elements in $\mathbb{F}_{2^n}$. Let $c \cdot F = c_1 f_1 + c_2 f_2 + \cdots + c_n f_n$ be a linear combination of the coordinate Boolean functions f_1, f_2, …, f_n of F. The nonlinearity (NL) for an S-box is defined as:

$$\mathrm{NL}(F) = \min_{c \in \mathbb{F}_{2^n}, c \neq 0} \mathrm{NL}(c \cdot F)$$

The NL of F is the Hamming distance between the set of all non-constant linear combinations of component functions of F and the set of all affine functions over $\mathbb{F}_{2^n}$. The known highest NL value is 112 as obtained by AES's S-box (Daemen et al., 2002) and Li et al., 2012 proposed S-box. As suggested by Piret et al., 2012, the NL must be close to the best known nonlinearity (i.e. NL of AES's S-box) to thwart linear cryptanalysis (Matsui, 1994). Therefore in this study, we set and limit the value of NL > 100 for the S-box to be considered as cryptographically strong.

Differential Uniformity. The Differential Uniformity (DU) of an S-box is the largest value present in its difference distribution table by omitting the trivial entry case, $a = b = 0$. The DU is defined as:

$$\mathrm{DU}(F) = \max_{a,b \in \mathbb{F}_{2^n}, a \neq 0} \left|\{x \in \mathbb{F}_{2^n}: F(x + a) + F(x) = b\}\right|$$

Better S-box has smaller value (i.e. $2 \leq \mathrm{DU} \leq 6$) as preferred in Piret et al., (2012) to resist against differential cryptanalysis (Biham et al., 1991).

Algebraic Degree. The Algebraic Degree (AD) of an S-box can be determined by the maximum degree between all component functions:

$$\mathrm{AD}(F) = \max\{\deg(f_1), \deg(f_2), \dots, \deg(f_n)\}$$

where $\deg(f)$ is the number of variables in the largest monomial of an S-box. Preferable measurement of $\mathrm{AD} \geq 4$ is suggested in Piret et al., 2012 in order to resist higher order differential cryptanalysis (Knudsen, 1995).

3. S-BOX CONSTRUCTION AND FINDINGS

In the works of Isa et al., 2013 and Mamadolimov et al., 2013, the authors proposed a construction of an S-box using binomial power function approach. However, they only focus on non-permutation power functions that carry high cryptographic properties as one of the two seed functions. In this study, we do thorough analysis on all power functions (permutation and non-permutation) over the finite field $\mathbb{F}_{2^8}$. We study the cryptographic properties exhibited from the binomial operation on the two power functions. If the resulting function is shown to be non-bijective, then additional operations are performed which are:

(i) *Addition* with another power function, and
(ii) *Multiplication* with coefficients.

Let x^d denotes a power function in $\mathbb{F}_{2^8}$ with the irreducible polynomial $x^8 + x^4 + x^3 + x^2 + 1$, where $d = \{1, 2, \dots, 2^8 - 2\}$ and $x \in \mathbb{F}_{2^8}$. All these functions can be classified into linearly non-equivalent functions using the squaring method (Aslan et al., 2008) as shown in Table 1.

The first column of Table 1 represents the powers d that are non-equivalent to each other. The second column lists all the equivalent power functions for each of power d. For instance, the power x^{127} is equivalent to x^{223}. Other columns give the values of nonlinearity (NL), differential uniformity (DU) and algebraic degree (AD) of the S-box produced using the underlying power function.

Our construction is illustrated in Figure 1 and described as follows. The construction starts by generating a binomial power function over the finite field $\mathbb{F}_{2^8}$ as a seed function. To achieve this, we add two different power functions F_1 and F_2 to produce F:

$$F = F_1 + F_2. \tag{1}$$

There are a total of $C_2^{254} = 32131$ possible combinations of binomial power functions. To select which of these to become the seed function, two types of analyses are performed. The first analysis evaluates the cryptographic properties exhibited by the resulting S-box generated by the binomial function as in Eq. (1). The second analysis examines the occurrences of the elements in the resulting function's codomain.

In the first analysis, two cryptographic properties of the S-box are measured which are nonlinearity (NL) and differential uniformity (DU). The results of the analysis on all binomial power functions are then stored in the *Cryptographic Properties Table* which is given in Table 2. The table shows the number of S-boxes (FREQ) categorized into 195 groups (#) where each group has the same value for NL and DU. For instance, there are 192 S-boxes that have NL = 112 and DU = 2.

TABLE 1: Classification of power function, x^d based on maximum nonlinearity in $\mathbb{F}_{2^8}$.

d	**{d x 2} mod 2^8-1**	**NL**	**DU**	**AD**
127	254, 253, 251, 247, 239, 223, 191	112	4	7
111	222, 246, 189, 123, 237, 219, 183	112	4	6
21	42, 84, 168, 162, 138, 81, 69	112	4	3
39	78, 156, 114, 228, 57, 201, 147	112	2	4
3	6, 12, 24, 48, 96, 192, 129	112	2	2
9	18, 36, 72, 144, 66, 132, 33	112	2	2
31	62, 124, 248, 241, 227, 199, 143	112	16	5
91	182, 218, 214, 109, 181, 107, 173	112	16	5
63	126, 252, 249, 243, 231, 207, 159	104	6	6
47	94, 188, 242, 121, 229, 203, 151	104	16	5
19	38, 76, 152, 98, 196, 49, 137	104	16	3
95	190, 250, 125, 245, 235, 215, 175	96	4	6
5	10, 20, 40, 80, 160, 130, 65	96	4	2
7	14, 28, 56, 112, 224, 193, 131	96	6	3
37	74, 148, 82, 164, 146, 41, 73	96	6	3
25	50, 100, 200, 70, 140, 145, 35	96	6	3
29	58, 116, 232, 142, 209, 163, 71	96	10	4
11	22, 44, 88, 176, 194, 97, 133	96	10	3
59	118, 236, 206, 217, 179, 103, 157	96	12	5
55	110, 220, 230, 185, 115, 204, 155	96	12	5
13	26, 52, 104, 208, 134, 161, 67	96	12	3
61	122, 244, 158, 233, 211, 167, 79	96	16	5
23	46, 92, 184, 226, 113, 197, 139	96	16	4
53	106, 212, 166, 154, 169, 83, 77	96	16	4
27	54, 108, 216, 198, 177, 99, 141	80	26	4
87	174, 186, 234, 93, 117, 213, 171	80	30	5
43	86, 172, 178, 202, 89, 101, 149	80	30	4

TABLE 1 (continued): Classification of power function, x^d based on maximum nonlinearity in $\mathbb{F}_{2^8}$.

d	{d x 2} mod 2^8-1	NL	DU	AD
15	30, 60, 120, 240, 225, 195, 135	76	2	4
45	90, 180, 210, 150, 105, 165, 75	76	2	4
17	34, 68, 136	0	16	2
119	238, 221, 187	0	22	6
51	102, 204, 153	0	24	4
85	170	0	60	4
1	2, 4, 8, 16, 32, 64, 128	0	256	1

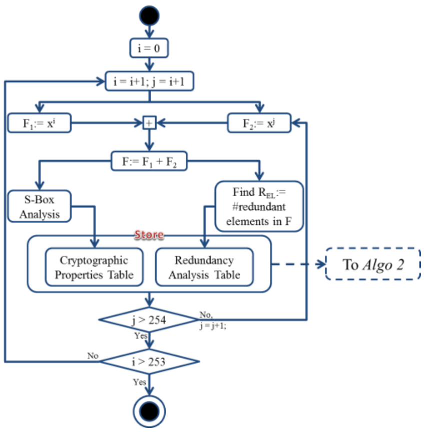

Figure 1: Binomial Power Function Construction

TABLE 2: Cryptographic Properties Table on Binomial Power Functions

#	NL	DU	FREQ	#	NL	DU	FREQ	#	NL	DU	FREQ	#	NL	DU	FREQ	#	NL	DU	FREQ
1	112	2	192	41	96	14	992	81	88	18	232	121	80	32	8	161	60	12	16
2	112	4	245	42	96	16	1048	82	88	20	368	122	78	34	16	162	60	16	16
3	112	8	16	43	96	18	336	83	88	22	176	123	76	6	40	163	40	34	24
4	112	16	128	44	96	20	208	84	88	24	24	124	76	8	104	164	40	36	8
5	106	6	8	45	96	22	136	85	88	26	8	125	76	10	16	165	40	62	24
6	106	8	32	46	96	24	56	86	88	28	8	126	76	14	128	166	40	116	8
7	104	6	96	47	96	26	8	87	88	30	8	127	76	16	32	167	16	8	32
8	104	8	464	48	96	28	8	88	88	32	16	128	76	18	32	168	16	16	32
9	104	10	200	49	96	34	8	89	88	34	8	129	76	20	24	169	0	4	80
10	104	12	48	50	94	4	8	90	86	6	16	130	74	32	8	170	0	6	16
11	104	14	24	51	94	8	16	91	86	8	112	131	74	34	8	171	0	8	104
12	104	16	160	52	94	10	168	92	86	10	112	132	72	6	24	172	0	10	8
13	104	18	8	53	94	12	96	93	86	12	24	133	72	8	216	173	0	12	80
14	104	20	32	54	94	14	48	94	86	14	40	134	72	10	208	174	0	16	56
15	104	22	8	55	94	16	8	95	86	18	104	135	72	12	16	175	0	18	32
16	102	6	56	56	94	18	112	96	86	20	24	136	72	14	24	176	0	20	116
17	102	8	224	57	94	20	32	97	86	22	32	137	72	16	56	177	0	22	76
18	102	10	64	58	94	22	56	98	86	30	16	138	72	18	32	178	0	24	88
19	102	16	16	59	94	24	8	99	84	8	112	139	72	20	16	179	0	26	40
20	100	6	48	60	94	26	24	100	84	10	64	140	72	24	56	180	0	28	84
21	100	8	472	61	94	30	24	101	84	12	48	141	72	26	56	181	0	30	32
22	100	10	360	62	92	8	72	102	84	14	8	142	72	28	32	182	0	32	36

TABLE 2 (continued): Cryptographic Properties Table on Binomial Power Functions

#	NL	DU	FREQ	#	NL	DU	FREQ	#	NL	DU	FREQ	#	NL	DU	FREQ	#	NL	DU	FREQ
23	100	12	112	63	92	10	432	103	84	18	64	143	72	32	8	183	0	34	16
24	100	14	64	64	92	12	208	104	84	20	24	144	72	42	16	184	0	36	12
25	100	16	48	65	92	14	136	105	84	22	32	145	70	8	32	185	0	40	12
26	100	18	136	66	92	16	72	106	84	30	16	146	70	10	8	186	0	42	8
27	100	20	96	67	92	18	104	107	80	4	32	147	70	12	24	187	0	44	8
28	100	22	40	68	90	6	8	108	80	6	88	148	70	14	32	188	0	48	16
29	100	30	24	69	90	8	112	109	80	8	480	149	70	18	32	189	0	50	36
30	100	38	8	70	90	10	184	110	80	10	1464	150	64	4	32	190	0	60	32
31	98	6	32	71	90	12	88	111	80	12	928	151	64	8	216	191	0	64	6
32	98	8	40	72	90	14	48	112	80	14	584	152	64	10	152	192	0	76	2
33	98	10	48	73	90	18	8	113	80	16	336	153	64	12	24	193	0	84	18
34	98	12	24	74	90	20	8	114	80	18	352	154	64	14	16	194	0	120	1
35	98	18	8	75	88	6	8	115	80	20	192	155	64	16	56	195	0	256	28
36	96	4	216	76	88	8	560	116	80	22	120	156	64	18	16				
37	96	6	520	77	88	10	1400	117	80	24	88	157	64	20	64				
38	96	8	2296	78	88	12	1064	118	80	26	136	158	64	22	72				
39	96	10	4608	79	88	14	424	119	80	28	24	159	64	24	48				
40	96	12	2512	80	88	16	208	120	80	30	128	160	64	26	8				

In the second analysis, a table called the *Redundancy Analysis Table* which is shown by Table 3 is created. This table stores the number of elements in the resulting function's codomain which are mapped by more than one input in its domain. We denote this number as R_{EL} and refer these elements as *redundant* elements. The table also stores the number of elements that do not exist in the codomain of the resulting binomial function. We denote this number as N_{EL} and refer to these elements as *non-existent* elements.

From the analysis, we can categorize the binomial functions into 130 groups. All functions in a group have the same values for the (N_{EL}, R_{EL}) pair. The FREQ column denotes the number of binomial function in that particular group. As an example, there are 1024 binomial functions that have 15 non-existent elements and one redundant element (i.e. one element of the function's codomain is mapped by more than one input in its domain). Based on Table 3, it can be clearly seen that all binomial power functions generated by Eq. (1) are non-bijective (when coefficient is set to 1 for both power functions).

From these two tables, we select the seed functions from two groups. The first group contains functions which exhibit high cryptographic properties (NL$\geq$112 and DU$\leq$8). There are 453 functions that met these criteria, which are the first three functions listed in Table 2. The second group contains functions for which the values of R_{EL} are less or equal to 30, i.e. $1 \leq R_{EL} \leq 30$. A total of 3,171 functions satisfy this condition where the functions are the first 25 listed in Table 3. This brings the total number of seed functions to 3,624.

All the seed functions are then sent to *Algo 2* for further analysis. *Algo 2* consists of two methods to manipulate the output so that a nearly bijective function is obtained. The methods are i) *Addition* with another power function, and ii) *Multiplication*, where both power functions from the seed function are multiplied with coefficients. This is illustrated in Figure 2.

Note that before we perform the *Addition* or *Multiplication* methods in *Algo 2*, we first perform equivalence check on the involved functions. This equivalence check is intended to ensure that not all involved power functions in each method is from linearly equivalent power function. If this happens, then the output of the generated functions will likely to have the same cryptographic properties as in Table 1.

Table 3: Redundancy Analysis Table

#	N_{EL}	R_{EL}	FREQ	#	N_{EL}	R_{EL}	FREQ	#	N_{EL}	R_{EL}	FREQ	#	N_{EL}	R_{EL}	FREQ
1	15	1	1024	34	214	42	64	67	88	64	384	100	84	76	256
2	17	1	128	35	85	43	512	68	96	64	256	101	108	76	256
3	51	1	256	36	213	43	256	69	192	64	128	102	179	77	1024
4	85	1	128	37	50	46	128	70	89	65	640	103	178	78	64
5	16	2	128	38	82	46	256	71	191	65	128	104	177	79	128
6	254	2	1	39	90	46	512	72	94	66	256	105	96	80	256
7	253	3	2	40	210	46	64	73	85	67	256	106	100	80	256
8	252	4	4	41	209	47	64	74	93	67	256	107	85	81	896
9	251	5	4	42	75	49	128	75	97	67	256	108	125	81	256
10	40	6	128	43	99	49	256	76	189	67	64	109	175	81	512
11	250	6	4	44	207	49	256	77	84	68	384	110	104	82	256
12	248	8	12	45	206	50	128	78	92	68	768	111	105	83	256
13	247	9	8	46	85	51	256	79	77	69	128	112	97	85	256
14	246	10	8	47	125	51	128	80	85	69	384	113	105	85	128
15	245	11	32	48	205	51	224	81	97	69	128	114	171	85	256
16	244	12	8	49	72	52	256	82	187	69	192	115	90	86	128
17	243	13	32	50	84	52	640	83	78	70	128	116	102	86	128
18	80	16	128	51	204	52	64	84	92	70	768	117	120	86	128
19	240	16	96	52	77	53	256	85	94	70	128	118	170	86	64
20	239	17	112	53	85	55	256	86	96	70	128	119	96	88	256
21	68	18	128	54	80	56	256	87	93	71	256	120	104	88	256
22	238	18	16	55	90	58	512	88	185	71	64	121	102	90	256
23	64	22	256	56	89	59	1024	89	84	72	128	122	160	96	64
24	51	25	512	57	88	60	256	90	92	72	256	123	99	97	128
25	230	26	16	58	92	60	384	91	75	73	640	124	100	98	128
26	69	31	512	59	75	61	256	92	93	73	256	125	108	100	128
27	85	35	256	60	99	61	768	93	97	73	256	126	144	112	64
28	221	35	64	61	195	61	64	94	99	73	640	127	113	113	128
29	75	37	256	62	84	62	128	95	123	73	256	128	120	120	128
30	217	39	64	63	85	63	256	96	183	73	320	129	136	120	192
31	45	41	128	64	89	63	768	97	92	74	256	130	128	128	576
32	81	41	512	65	193	63	64	98	93	75	128				
33	85	41	256	66	84	64	128	99	181	75	320				

In the *Addition* method, the coefficients of all involved power functions is set to 1 while for the *Multiplication* method, the coefficients are multiplied on both power functions of the seed function. The purpose of this technique is to study the degree of generated output likelihood towards bijective function in addition to measuring the strength of the exhibited cryptographic properties.

Both methods (i.e. *Addition* and *Multiplication*) will perform equivalence check on the given binomial function, $F = x^i + x^j$. An additional equivalence check will be performed in *Addition* method which is between F and a new power function, $x^k, k \neq \{i, j\}$. If all equivalence checks give linearly equivalent function, then the process is discarded. Otherwise, the process continues with either addition with another power function, (i.e. $F = x^i + x^j + x^k, i \neq j \neq k$) or multiplication with coefficients, (i.e. $F = \alpha x^i + \beta x^j, \alpha, \beta \in \{1,2, \ldots, 2^8 - 1\}$). If no redundant elements found in F (i.e. R_{EL} = 0), the S-box properties will be measured on that output. Then, the output will be stored as a new S-box if the desired value is achieved. In *Addition* method (i.e. *Algo 2(i)*), the operation continues until the power function x^k reaches the end (i.e x^{2^8-2}), while the iteration in *Multiplication* method (i.e. *Algo 2(ii)*) will stop when both coefficients α and β reaches $2^8 - 1$.

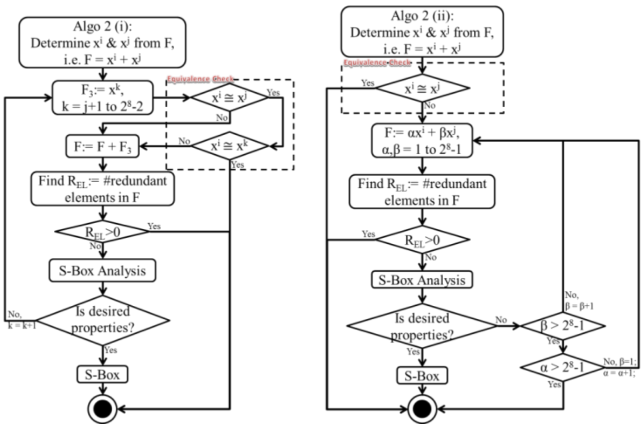

Figure 2: *Algo 2(i): Addition with another power function;*
Algo 2(ii): Multiplication with coefficients.

Using this method, we obtained three cryptographically strong S-boxes. These S-boxes come from the seed functions which have R_{EL} = 1. The rest of the seed functions did not produce S-boxes that have strong cryptographic properties. One may ask why the functions from the first group of seed functions (which already have high cryptographic properties) did not make the cut. This is probably because the application of the addition and multiplication operations makes the functions linearly equivalent to existing power functions. This means that the S-boxes resulted from the functions exhibit the same cryptographic properties with existing S-boxes. This is not the aim of this paper since we are seeking for new and cryptographically strong S-boxes.

Other possible reasons that the operations did not produce strong S-boxes from the functions which have $R_{EL} > 1$ is because the number of redundant and non-existent elements is high. The addition and multiplication operations therefore are unable to reduce these numbers to make the functions bijective.

Out of the three S-boxes, two of them are generated from the *Addition* method while the other one from the *Multiplication* method. These S-boxes are given in Tables 4, 5 and 6. The first column in Tables 4, 5 and 6 denotes the first four bits of the input while the first row in each table denotes the remaining four bits of the 8-bit input to the S-box. For example, in Table 4, the input 63 gives the output F5. i.e. F(63) = F5 where the input and output are in hexadecimal.

Table 4 gives us the first S-box, S-Box1, generated from *Addition* method, with function $F_{S-Box1} = x^{35} + x^{137} + x^{239}$. This function exhibits (108, 4, 7) for its (NL, DU, AD).

TABLE 4: S-Box1 from *Addition* Method

	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**A**	**B**	**C**	**D**	**E**	**F**
0	00	01	14	67	0D	AC	BF	31	58	25	98	0A	F9	21	52	0F
1	51	37	08	46	2F	68	2D	1B	D9	40	1A	9A	7C	D1	CC	E8
2	FF	76	8B	A4	24	04	26	4C	53	F0	73	F8	2C	02	EF	A5
3	A1	F7	3D	6A	D5	B7	1F	11	7E	88	85	3B	4B	B2	F3	9B
4	90	65	FE	D8	4E	44	C0	61	EA	8E	50	F2	C2	F4	0B	DC
5	F6	75	C3	7F	D4	55	BB	28	4A	59	09	32	CD	82	72	87
6	60	9D	30	F5	64	10	5B	03	A2	66	33	E0	FD	38	49	81
7	56	77	5E	C9	E2	B0	7B	CE	6F	D2	AB	57	1C	48	13	5A
8	8F	17	97	3A	A0	06	2B	E7	B3	D0	39	E5	47	EE	27	54
9	89	91	4F	92	41	6D	96	CA	93	45	0C	FB	A7	DA	16	AF
A	84	9F	7D	2A	C4	B1	42	9C	1D	A9	70	CF	05	95	B4	3E
B	E1	8A	80	9E	AE	7A	1E	5D	5F	B9	FA	CB	A6	69	EB	71
C	D3	C1	6B	62	3F	34	07	6E	83	E3	15	ED	A8	0E	3C	79
D	A3	B5	B6	86	DB	F1	D7	D6	B8	DE	FC	BD	DD	99	C6	DF
E	22	C5	74	BA	EC	C7	E9	23	29	E6	35	BE	12	8C	78	2E
F	18	94	C8	5C	4D	8D	BC	36	AD	63	19	43	AA	6C	E4	20

Table 5 also is an S-box generated from *Addition* method but with different function, $F_{S-Box2} = x^{29} + x^{89} + x^{164}$. We denote it as S-Box2. Its S-box properties are (108, 6, 4) for its (NL, DU, AD) respectively.

Another proposed S-box denoted as S-Box3 is shown in Table 6. This was generated using the *Multiplication* method with function $F_{S-Box3} = 101x^{69} + 47x^{239}$. Its S-box properties of (NL, DU, AD) are (106, 6, 7).

Empirically, all three proposed S-box functions (i.e. F_{S-Box1}, F_{S-Box2} and F_{S-Box3}) were identified based on smallest combination of (N_{EL}, R_{EL}) from Table 3. As an example, the binomial operation of any two elements in F_{S-Box1} will give us the combination of (51, 1), (i.e. $(x^{35} + x^{137})$ or $(x^{35} + x^{239})$ or $(x^{137} + x^{239})$ will generated a function with (51, 1) for its (N_{EL}, R_{EL}) combination). The F_{S-Box2} is identified from (15, 1) combination while F_{S-Box3} is generated from the combination of (85, 1) of its (N_{EL}, R_{EL}) pair.

TABLE 5: S-Box2 from *Addition* Method

	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**A**	**B**	**C**	**D**	**E**	**F**
0	00	01	8F	FF	46	E2	3E	53	E5	D3	DD	98	D2	38	FB	06
1	D9	AE	E0	A5	3D	D5	D4	79	76	AA	C2	B6	33	82	97	25
2	94	7E	EE	C9	2E	13	B4	81	AD	04	70	16	BE	80	5A	B2
3	A4	09	BF	56	36	10	72	1A	02	66	5C	E6	A1	85	5F	73
4	BB	C6	27	90	92	4E	39	4A	65	1B	A9	C3	17	6C	45	93
5	C7	29	60	86	F2	14	BC	F8	6E	DA	C0	3A	23	B0	EB	40
6	6A	12	D8	AB	20	18	F4	DF	41	77	8C	6F	C4	2F	F9	03
7	FE	9F	55	37	1E	F0	95	AF	1D	7D	48	6D	59	A0	9C	2B
8	71	7A	34	52	EF	CD	88	BA	DB	26	69	63	58	A8	9A	3C
9	ED	87	44	4F	DE	2D	D1	F1	0B	DC	64	D0	E9	08	54	B8
A	C1	7C	E1	47	E3	5B	AC	0F	5D	74	42	EA	96	A7	8B	E7
B	1F	32	4D	BD	49	B7	68	84	19	FD	9D	A6	22	83	9E	F3
C	B3	0D	78	9B	2A	F7	2C	0C	0E	61	24	50	CA	3F	30	A2
D	CB	35	15	3B	B9	07	D7	D6	89	28	E4	4B	99	0A	7F	51
E	8D	E8	CF	FC	4C	F5	C8	FA	21	CE	75	8A	05	F6	B5	57
F	5E	31	62	1C	91	67	8E	7B	B1	CC	11	A3	EC	43	6B	C5

TABLE 6: S-Box3 from *Multiplication* Method

	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**A**	**B**	**C**	**D**	**E**	**F**
0	00	4A	3D	86	13	E8	84	95	FA	CF	58	40	7C	7E	3B	81
1	96	F1	9D	3C	DB	1E	23	87	0A	C3	2A	B7	D1	F6	46	C9
2	45	97	EF	D2	80	48	14	5A	2B	EB	CD	85	EA	10	DD	51
3	5B	92	04	B1	78	AB	6D	9A	4F	0F	52	D5	E1	F9	47	21
4	C8	05	B9	1D	AE	FD	4E	75	07	C6	BF	B0	7D	56	59	D0
5	19	F5	B3	BE	28	DC	88	CA	F2	83	64	0D	E9	D7	A8	2C
6	C2	02	32	6E	F7	E6	6F	BC	93	E7	3E	09	2F	E4	76	27
7	65	26	F8	77	6B	B2	B6	61	5F	12	55	B5	57	7A	4B	FF
8	B8	8B	03	ED	22	94	0B	25	66	9E	A0	5E	24	A2	DE	63
9	16	70	42	62	E0	1A	9B	C1	30	F3	20	7F	D8	EE	A4	2D
A	17	8C	98	A1	79	43	6A	8F	18	7B	C5	38	35	D6	3A	8A
B	8E	1C	C4	34	CB	2E	F0	99	AC	AF	4D	1B	37	60	06	6C
C	08	D3	82	AA	E5	BD	90	15	FC	A5	D9	E2	AD	11	9F	31
D	71	B4	EC	A6	72	0C	73	5C	67	C0	8D	74	BA	FE	89	CC
E	1F	49	5D	9C	A3	DF	FB	4C	33	53	29	50	DA	A7	68	E3
F	01	69	0E	54	41	3F	BB	44	F4	A9	91	C7	39	D4	CE	36

Table 7 summarize and compares our obtained S-boxes with the existing 8×8 cryptographically strong S-boxes in literature. As we mention in the earlier section, to be considered as cryptographically strong S-boxes, the following cryptographic properties condition must be satisfied: i) $\mathrm{NL} > 100$, ii) $2 \leq \mathrm{DU} \leq 6$ and iii) $\mathrm{AD} \geq 4$.

As a result, there are a total of 21 proposed S-boxes with several different techniques that include multiplicative inverse in $\mathbb{F}_{2^8}$, conversion function from $\mathbb{F}_{2^9}$ to $\mathbb{F}_{2^8}$, gray S-box, linear fractional transformation, theorem of polynomial permutation, 4-step tweaking on inverse function and manipulation of power functions in $\mathbb{F}_{2^8}$ as a based function. All the S-boxes are then ranked based on the cryptographic properties exhibited by each S-box.

TABLE 7: Comparison of Cryptographically Strong S-Boxes

Rank	**S-box**	**NL**	**DU**	**AD**	***Techniques***
1	AES (Daemen et al., 2002)	112	4	7	Multiplicative Inverse, x^{-1} in $\mathbb{F}_{2^8}$
	Camellia (Aoki et al., 2001)				
	ARIA (Kwon et al., 2004)				
	HyRAL (Hirata, 2010)				
	Hierocrypt-HL (Ohkuma et al., 2001)				
	CLEFIA-S_1 (Shirai et al., 2007)				
	Tran et al., 2008				Gray S-Box
	Hussain et al., (2013)				Linear Fractional Transformation
2	Li et al., 2012	112	4	5	Conversion $\mathbb{F}_{2^9} \rightarrow \mathbb{F}_{2^8}$
3	Yang et al., 2011	112	6	7	Theorem of Permutation Polynomials
4		110	4	7	
5		110	6	7	
6	**S-Box1**	**108**	**4**	**7**	**Trinomial Power Functions (*Addition*)**
7	**S-Box2**	**108**	**6**	**4**	
8	**S-Box3**	106	6	7	**Binomial Power Function (*Multiplication*)**
	Hierocrypt-LL (Ohkuma et al., 2001)				Unknown
	Fuller et al., 2003				4-Step tweaking on AES s-box
	Isa et al., 2013				Binomial Power Function

TABLE 7 (continued): Comparison of Cryptographically Strong S-Boxes

Rank	S-box	NL	DU	AD	*Techniques*
9	Isa et al., 2013	104	6	7	Binomial Power Function + Heuristic Techniques
10	Mamadolimov et al., 2013	102	8	7	Binomial Power Functions

The most used technique in the early construction of an S-box is using multiplicative inverse in $\mathbb{F}_{2^8}$ (Daemen et al., 2002, Aoki et al., 2001, Kwon et al., 2004, Hirata, 2010, Ohkuma et al., 2001 and Shirai et al., 2007). This technique gives the best known cryptographic properties for an S-box and ranked first in Table 7. There are also proposed S-boxes's by Tran et al., 2008 and Hussain et al., 2013 which were using different techniques but gave the same S-box properties as the best known S-box.

Our proposed S-box is ranked sixth, seventh and eighth after the proposed S-box's by Li et al., 2012 and three different S-boxes by Yang et al., 2011. Two of our proposed S-boxes are better than the S-boxes proposed by Isa et al., 2013 which were ranked eighth and ninth. At rank number 8, there are several others proposed S-boxes which are by Fuller et al., 2003 and by Ohkuma et al., 2001 denoted as Hierocrypt-LL. Last ranked S-box in this study is an S-box proposed by Mamadolimov et al.'s, 2013 at rank number 10.

4. CONCLUSION

In this paper, we manage to improve the S-box construction based on binomial operation on power functions proposed by Isa et al., 2013. By widening the scope of the power function and introducing new manipulation techniques, we managed to obtain a stronger S-box than the previous construction. All the S-boxes are the results of manipulating binomial power functions which have one redundant element. Two of these S-boxes are produced using the addition method and the other one using the multiplication method.

ACKNOWLEDGMENT

The authors would like to thank you Ministry of Higher Education (MOHE), Malaysia for supporting and financing this research project under the Exploratory Scheme Research Grant 2012/13.

REFERENCES

Aoki, K., Ichikawa, T., Kanda, M., Matsui, M., Moriai, S., Nakajima, J., and Tokita, T. (2001). Camellia: A 128-Bit Block Cipher Suitable for Multiple Platforms - Design and Analysis. *Selected Areas in Cryptography*: 39-56.

Aslan, B., Sakalli, M. T. and Bulus, E. (2008). Classifying 8-bit to 8-bit S-Boxes based on Power Mappings from the Point of DDT and LAT Distributions. *Arithmetic of Finite Fields*: 123-133.

Biham, E. and Shamir, A. (1991). Differential Cryptanalysis of DES-Like Cryptosystems. *Advances in Cryptology (CRYPTO '90)*: 2-21.

Isa, H., Jamil, N. and Z'aba, M. R. (2013). S-Box Construction from Non-Permutation Power Functions, *Proceeding of the 6th International Conference on Security of Information and Networks (SIN '13)*: 46-53.

Knudsen, L. R. (1995). Truncated and Higher Order Differentials. *Fast Software Encryption*: 196-211.

Kwon, D., Kim, J., Park, S., Sung, S., Sohn, Y., Song, J., Yeom, Y., Yoon, E.-J., Lee, S., Lee, J., Chee, S., Han, D., and Hong, J. (2004). New Block Cipher: ARIA. *Information Security and Cryptology*: 432 - 445.

Li, Y. and Wang, M. (2012). Constructing Differentially 4-uniform Permutations over $GF(2^{2m})$ from Quadratic APN Permutations over $GF(2^{2m+1})$. *Designs, Codes and Cryptography*: 1-16.

Mamadolimov, A., Isa, H. and Mohamad, M. S. (2013). Practical Bijective S-Box Design. Accessed 21st Jan 2013. Sourced from http://arxiv.org/abs/1301.4723

Matsui, M. (1994). Linear Cryptanalysis Method for DES Cipher. *Advances in Cryptology (EUROCRYPT '93)*: 386-397.

Ohkuma, K., Muratani, H., Sano, F., and Kawamura, S. (2001). The Block Cipher Hierocrypt. *Selected Areas in Cryptography*: 72-88.

Piret, G., Roche, T. and Carlet, C. (2012). PICARO - A Block Cipher Allowing Efficient Higher-Order Side-Channel Resistance. *Applied Cryptography and Network Security*: 311-328.

Shannon, C. E. (1949). Communication Theory of Secrecy Systems. *Bell System Technical Journal*. **28**(7): 656-715.

Shirai, T., Shibutani, K., Akishita, T., Moriai, S., and Iwata, T. (2007). The 128-bit Blockcipher CLEFIA. *Fast Software Encryption*: 181-195.

Tran, M. T., Bui, D. K. and Duong, A. D. (2008). Gray S-Box for Advanced Encryption Standard. *Computational Intelligence and Security, CIS* '08, 253-258.

Yang, M., Wang, Z., Meng, Q. and Han, L. (2011). Evolutionary Design of S-box with Cryptographic Properties. *Parallel and Distributed Processing with Applications Workshops (ISPAW)*, 12-15.