International Journal of Cryptology Research 6(1): (2016)

Hybrid Heuristic Methods in Constructing Cryptographically Strong S-boxes

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

[1]*College of Computer Science and Information Technology, Universiti Tenaga Nasional (UNITEN), Malaysia*
[2]*Network Security Lab, MIMOS Berhad, Kuala Lumpur, Malaysia*

E-mail: herman.isa@mimos.my
[*]*Corresponding author*

ABSTRACT

Isa et al. (2013, 2016) proposed two heuristic algorithms (redundancy removal and bee waggle dance) to construct cryptographically strong substitution boxes (S-boxes). The resulting S-boxes produced by these algorithms are suitable for cryptographic use. Inspired by their work, this paper explores a new method to optimise an S-box by integrating these two algorithms. Our experiments show that at least eight cryptographically strong S-boxes can be produced by the new method. The results also improves upon a previous construction by Mamadolimov et al. (2013) which utilises the redundancy removal algorithm.

Keywords: S-box, Nonlinearity, Heuristic, Redundancy Removal Algorithm, Bee Waggle Dance Algorithm

1 INTRODUCTION

A substitution box (S-box) is cores of nonlinear operation in symmetric cryptosystem especially block ciphers. An S-box typically used to obscure the

relationship between key and ciphertext, such that fulfils Shannon's property of confusion (Shannon, 1949).

In general, there are three generic methods in the construction of an S-box, which are random searching approach, heuristic or evolutionary (i.e. heuristic) approach and mathematical functions or algebraic (i.e. mathematical) approach. Each approach has its advantages and weaknesses. As an example, the advantage of each approach is random searching being the simplest method; heuristic approach has better implementation in both software and hardware; and lastly known best cryptography properties (National Institute of Standards and Technology, 2001) achieved by mathematical approach. Yet, the weakness of each approach is low cryptographic properties exhibited by random and heuristic approaches, and extremely hard to find a mathematical function that give a complete set of cryptographically strong S-boxes.

However, in recent years, the uses of heuristic approach in S-box construction are gaining the attention of researchers. This can be seen through the increasing number of S-box constructions proposed in literature such as using evolution of theorem of permutation polynomials (Yang et al., 2011), gradient descent (Kazymyrov et al., 2013), redundancy removal algorithm (Isa et al., 2013), chaotic map-based technique (Alkhaldi et al., 2015), reversed genetic algorithm (Ivanov et al., 2016) and latest is the S-box construction inspired by bee waggle dance (Isa et al., 2016).

In this paper, we optimise the construction of S-box by combining two algorithms proposed by Isa et al. (2013, 2016), which are redundancy removal algorithm (RRA) and bee waggle dance (BWD) algorithm. Our objective is to construct a permutation S-box from a non-permutation initial S-box that performs the RRA and then followed by the BWD algorithm.

The rest of the paper is organised as follows. In the second section, the main cryptographic properties of an S-box are discussed. Then, we share our S-box optimisation together with the involved algorithms in the third section. The paper is concluded in the last section.

2 S-BOX PROPERTIES

In this paper, our focused result is on bijective S-boxes over finite field $\mathbb{F}_{2^8}$. Therefore, a cryptographically strong S-box should at least exhibits the optimal values on the following three properties: (1) high nonlinearity (NL), (2) low differential uniformity (DU), and (3) high algebraic degree (AD).

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:

$$F : \mathbb{F}_{2^n} \rightarrow \mathbb{F}_{2^n} = (f_1(x_1, \ldots, x_n), \ldots, f_n(x_1, \ldots, x_n)) \tag{1}$$

2.1 Nonlinearity

Let $c \cdot F = c_1 f_1 + c_2 f_2 + \ldots + c_n f_n$ be a linear combination of the coordinate Boolean functions $(f_1, f_2, \ldots, f_n)$ of F where $c = (c_1, c_2, \ldots, c_n)$ be a nonzero elements in $\mathbb{F}_{2^n}$. The nonlinearity (NL) of an S-box F, is the Hamming distance between the set of all non-constant linear combination of component functions of F and the set of all affine functions over $\mathbb{F}_{2^n}$ as defined below:

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

Carlet (2011) suggested that the value of NL should be as close as to the best known NL (i.e. NL > 100) to thwart linear cryptanalysis (Matsui, 1994).

2.2 Differential Uniformity

The largest value present in difference distribution table, after omitting the trivial entry case (i.e. $a = b = 0$), determine the value of differential uniformity (DU). The value of DU is defined as:

$$\mathrm{DU}(F) = \max_{a,b \in \mathbb{F}_{2^n}, a \neq 0} |\{x \in \mathbb{F}_{2^n} : F(x + a) + F(x) = b\}| \tag{3}$$

Smaller value of DU is more preferable (i.e. $2 \leq$ DU ≤ 6) (Carlet, 2011) to resist differential cryptanalysis (Biham and Shamir, 1991).

2.3 Algebraic Degree

The number of variables in the largest monomial for component function f of an S-box is denoted as $deg(f)$. Therefore, the algebraic degree (AD) of the S-box is determined by the maximum degree of all component functions:

$$\text{AD}(F) = \max\{deg(f_1), deg(f_2), \ldots, deg(f_n)\} \tag{4}$$

Carlet (2011) suggested that AD ≥ 4 in order to resist higher order differential cryptanalysis (Knudsen, 1995).

3 S-BOX OPTIMISATION

As mentioned above, in this study, we analyse the combination of two different algorithms proposed by Isa et al. (2013, 2016) in constructing a cryptographically strong S-box. The referred algorithms are *Redundancy Removal Algorithm* and *Bee Waggle Dance* algorithm. The following subsections will describe the said algorithms in brief.

3.1 Redundancy Removal Algorithm

Isa et al. (2013) proposed an S-box construction from non-permutation power functions. One of the algorithms included in their construction is called *Redundancy Removal Algorithm* (RRA). In principle, this RRA is an improvement of the algorithm proposed by (Mamadolimov et al., 2013). As the name suggest, the RRA was meant to remove or replace the redundant elements in an initial S-box with the non-existent elements such that a bijective S-box is generated.

Figure 1 illustrate the process flow in RRA. The algorithm start with a non-permutation initial S-box as an input. From the input, the information about redundant elements and non-existent elements were extracted. Then, a table called as Distance Matrix (DM) is generated. This table contains the Hamming distances which were calculated based on bit error rates between the redundant elements and the non-existent elements in the initial S-box. Then,

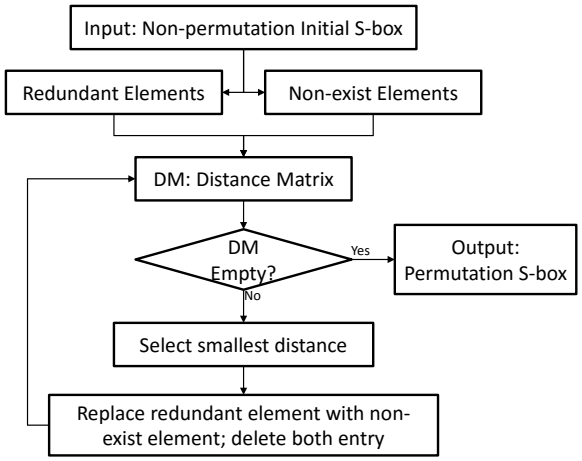

Figure 1: Redundancy Removal Algorithm (RRA)

the smallest Hamming distance is selected and its corresponding redundant element will be replaced by non-existent element in the initial S-box. This process is repeated until there is none DM generated. As a result, a permutation S-box is constructed.

3.2 Bee Waggle Dance Algorithm

Recently, Isa et al. (2016) introduced a new algorithm inspired by bees behaviour to construct an S-box. They name the algorithm as *Bee Waggle Dance* (BWD) adopt algorithm. As illustrated in Figure 2, BWD algorithm requires a starting point (y_1), eight different directions (r), 14 distinct distances (d) and at least a loop (l) to be completed. The BWD function is defined as the following:

$$\texttt{BWD}(r, d, l, y_1) = y_1 \rightarrow y_2 \rightarrow \ldots \rightarrow y_j \rightarrow y_1 \tag{5}$$

where the right hand side of equation 5 denotes the movement of bee from cell indexed by y_1 (i.e. starting point) to cell indexed by y_2. This movement will continue so on and so forth, until it returns to cell indexed by y_1. Thus, one complete loop (l) is counted.

The third parameter of BWD algorithm (i.e. eight different directions (r)) is borrowed from the *points of the compass*. These points of the compass

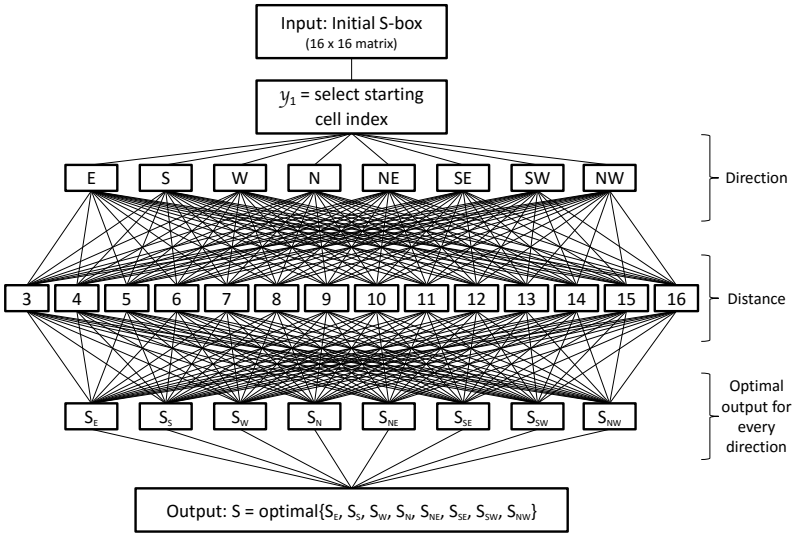

Figure 2: A loop of BWD Algorithm with static starting point

are composed of four cardinal directions (i.e. east (E), south (S), west (W) and north (N)) and four intercardinal directions (i.e. northeast (NE), southeast (SE), southwest (SW) and northwest (NW)).

The last parameter in BWD algorithm varies from the minimum distance (i.e. $d = 3$) to maximum distance (i.e. $d = 16$), thus make it 14 distinct distances as a whole. This distance is counted based on the height of the cell traversed on the dance floor. Basically, the dance floor is the initial S-box which was arranged in the form of a 16×16 matrix.

The final S-box in BWD algorithm is selected based on the most optimal cryptographic properties exhibited by the generated S-boxes.

3.3 Our Construction

Just like the construction proposed in Isa et al. (2013) and Isa et al. (2016), we also apply an initial S-box to be optimised by the RRA and BWD algorithms. However, in executing the optimisation, we have two options to perform the

construction which are either to execute RRA first (denoted as *Opt-1*) or to perform BWD first (denoted as *Opt-2*) on our initial S-box.

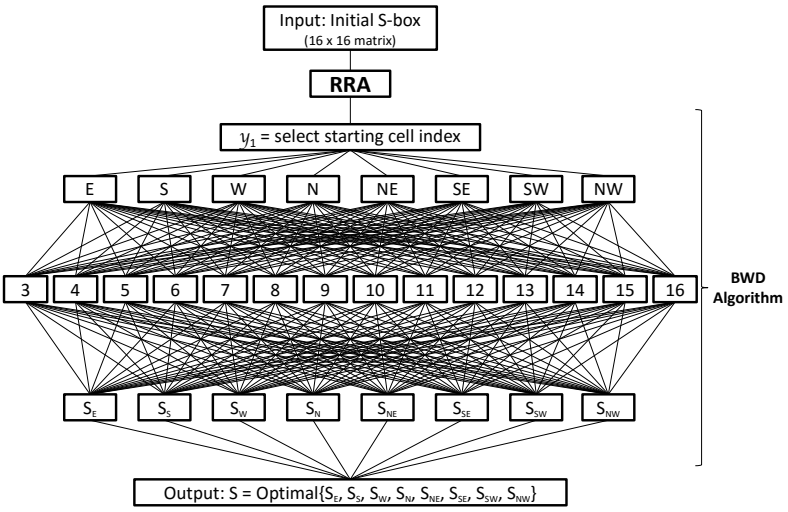

Figure 3: *Opt-1*: BWD(RRA(Initial S-box))

As illustrated in Figure 3, in *Opt-1* construction, the initial S-box which is non-permutation will first be executed in RRA to generate a permutation S-box. Then, this permutation S-box will perform the BWD algorithm until the most optimal S-box is identified.

Figure 4 depicted *Opt-2* construction. The initial S-box will perform the BWD algorithm first. Here, all the optimal outputs in every direction and every distance of BWD algorithm will be taken as candidates to perform RRA. This is because we cannot certain which candidate will exhibit the most optimal cryptographic properties after RRA is applied. Then from there, the most optimal result is taken to be the proposed S-box.

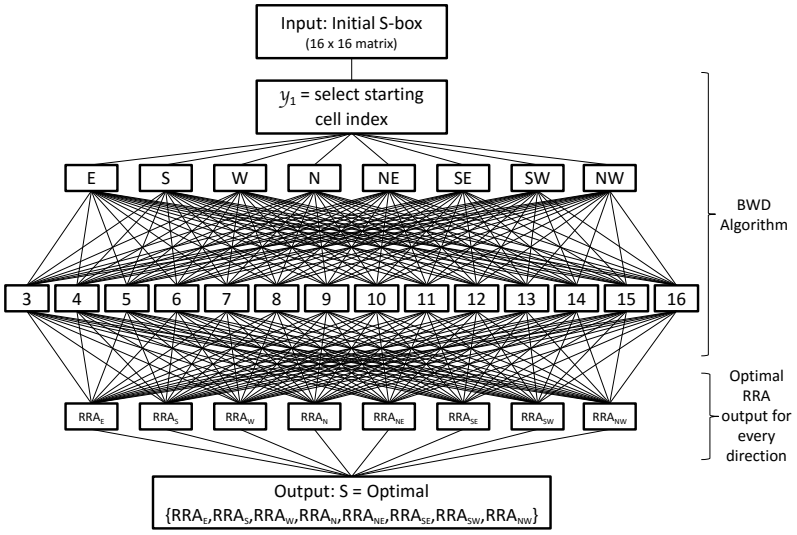

Figure 4: *Opt-2*: RRA(BWD(Initial S-box))

3.3.1 Initial S-box Generation

In our construction, the initial S-box must be from a non-permutation function. Therefore, our first candidates to fulfil this requirement are the set of non-permutation power functions as used by Isa et al. (2013). However, preliminary investigation shows that almost no candidates from this set can retain its cryptographic properties once performing the RRA. It might because of the large number of non-existent elements in the function. Therefore, this set of candidates was discarded.

As a solution, we adopt the S-box proposed by Isa et al. (2014, 2015) called as S-Box2. This S-Box2 is generated using trinomial power functions over finite field $\mathbb{F}_{2^8}$ with the following function:

$$F_{S-Box2} = x^{29} + x^{89} + x^{164} \tag{6}$$

which exhibits (108, 6, 4) for its (NL, DU, AD), respectively. This S-Box2 is selected because its exhibits a non-optimal value for AD (i.e. AD $= 4$).

One way to fulfil the requirement specified for the initial S-box, at least

three elements must be replaced with the same element from S-Box2 (i.e. redundant entries), such that a non-permutation initial S-box is obtained. In this example, we replaced the elements located at position 85, 115 and 165 in S-Box2 with entry "0". Now, the current cryptographic properties of the initial S-box are changed to (105[1], 8, 4) for its (NL, DU, AD), respectively.

3.3.2 Result

Table 1 and Table 2 shows the optimal results obtained from the initial S-box for *Opt-1* and *Opt-2* construction, respectively. The entries in both tables represent the cryptographic properties of nonlinearity, differential uniformity and algebraic degree of each result and the starting point, y_1 used in the BWD algorithm. We denote these entries as (NL, DU, AD, y_1). Note that, as discussed in Section 2, an S-box is considered as cryptographically strong if it satisfies the following requirements: i) NL $>$ 100, ii) $2 \leq$ DU ≤ 6 and iii) AD ≥ 4. There are a total of eight S-boxes (3 from Table 1 + 5 from Table 2) that meet these requirements which are highlighted in the tables.

Direction / Distance	EAST	SOUTH	WEST	NORTH	NORTHEAST	SOUTHEAST	SOUTHWEST	NORTHWEST
3	(102, 6, 7, 235)	(102, 8, 7, 194)	(104, 8, 7, 180)	(102, 8, 7, 207)	(104, 8, 7, 8)	(102, 8, 7, 3)	(102, 6, 7, 179)	(104, 8, 7, 181)
4	(102, 8, 7, 172)	(102, 8, 7, 184)	(102, 8, 7, 61)	(102, 8, 7, 175)	(102, 8, 7, 10)	(102, 8, 7, 1)	(102, 8, 7, 242)	(102, 6, 7, 94)
5	(102, 8, 7, 69)	(100, 8, 7, 162)	(100, 8, 7, 108)	(100, 8, 7, 172)	(102, 8, 7, 14)	(102, 8, 7, 5)	(102, 8, 7, 185)	(102, 8, 7, 254)
6	(100, 8, 7, 25)	(98, 8, 7, 155)	(100, 8, 7, 234)	(100, 8, 7, 103)	(102, 8, 7, 22)	(102, 8, 7, 65)	(102, 8, 7, 248)	(100, 8, 7, 253)
7	(98, 8, 7, 106)	(98, 8, 7, 134)	(100, 8, 7, 185)	(100, 8, 7, 154)	(100, 8, 7, 7)	(100, 8, 7, 23)	(100, 8, 7, 217)	(100, 8, 7, 216)
8	(100, 8, 7, 73)	(100, 8, 7, 98)	(98, 8, 7, 202)	(98, 8, 7, 137)	(98, 8, 7, 27)	(100, 8, 7, 132)	(100, 8, 7, 163)	(98, 8, 7, 250)
9	(94, 8, 7, 104)	(98, 8, 7, 118)	(94, 8, 6, 185)	(98, 8, 7, 126)	(98, 8, 7, 29)	(98, 8, 7, 39)	(98, 8, 7, 216)	(96, 8, 7, 169)
10	(98, 8, 7, 72)	(98, 10, 7, 114)	(98, 10, 7, 201)	(98, 8, 7, 126)	(96, 8, 7, 110)	(96, 8, 7, 1)	(100, 10, 7, 145)	(98, 8, 7, 237)
11	(98, 8, 7, 56)	(98, 10, 7, 114)	(98, 10, 7, 233)	(98, 10, 7, 123)	(98, 8, 7, 15)	(94, 8, 7, 34)	(96, 8, 7, 246)	(98, 8, 7, 238)
12	(98, 8, 7, 56)	(96, 10, 7, 114)	(98, 10, 7, 201)	(98, 10, 7, 123)	(98, 10, 7, 13)	(98, 8, 7, 35)	(92, 8, 7, 226)	(94, 8, 7, 206)
13	(98, 10, 7, 56)	(98, 10, 7, 115)	(98, 10, 7, 201)	(98, 10, 7, 124)	(98, 10, 7, 13)	(96, 10, 7, 1)	(98, 10, 7, 210)	(96, 10, 7, 221)
14	(96, 10, 7, 24)	(94, 10, 7, 116)	(96, 10, 7, 233)	(96, 10, 7, 125)	(96, 10, 7, 16)	(98, 10, 7, 3)	(96, 10, 7, 243)	(96, 10, 7, 239)
15	(96, 10, 7, 40)	(94, 12, 7, 115)	(96, 12, 7, 233)	(98, 10, 7, 126)	(96, 10, 7, 31)	(94, 10, 7, 2)	(96, 10, 7, 241)	(92, 10, 7, 239)
16	(94, 10, 7, 24)	(90, 12, 7, 114)	(94, 12, 7, 233)	(92, 10, 7, 127)	(94, 10, 7, 16)	(98, 10, 7, 1)	(94, 10, 7, 241)	(94, 12, 7, 256)

Table 1: Experiment Results of *Opt-1* on Initial S-box

The S-box obtained at direction northwest and distance 4 in Table 1 is represented in hexadecimal in Table 3. As stated in Table 1, this S-box exhibits cryptographic properties of (102, 6, 7) for its (NL, DU, AD), respectively.

Table 4 represents the hexadecimal of optimal S-box generated using *Opt-2* construction. This S-box is obtained from distance 3 and at direction southwest

[1]Some of non-permutation S-boxes gives an odd value of NL. (Mamadolimov et al., 2013)

Direction / Distance	EAST	SOUTH	WEST	NORTH	NORTHEAST	SOUTHEAST	SOUTHWEST	NORTHWEST
3	(102, 6, 7, 235)	(104, 8, 7, 45)	(102, 6, 7, 206)	(102, 6, 7, 117)	(104, 8, 7, 8)	(104, 8, 7, 5)	(104, 6, 7, 179)	(104, 8, 7, 59)
4	(102, 8, 7, 23)	(102, 8, 7, 58)	(102, 8, 7, 55)	(102, 8, 7, 51)	(104, 8, 7, 133)	(104, 8, 7, 25)	(102, 8, 7, 50)	(102, 6, 7, 132)
5	(100, 8, 7, 21)	(102, 8, 7, 150)	(100, 8, 7, 54)	(100, 8, 7, 68)	(102, 8, 7, 27)	(102, 8, 7, 10)	(102, 8, 7, 73)	(102, 8, 7, 74)
6	(100, 8, 7, 25)	(98, 8, 7, 82)	(100, 8, 7, 119)	(100, 8, 7, 87)	(100, 8, 7, 10)	(102, 8, 7, 139)	(100, 8, 7, 84)	(100, 8, 7, 94)
7	(100, 8, 7, 102)	(98, 8, 7, 117)	(100, 8, 7, 231)	(100, 8, 7, 124)	(100, 8, 7, 7)	(100, 8, 7, 22)	(100, 8, 7, 118)	(100, 8, 7, 107)
8	(100, 8, 7, 121)	(100, 8, 7, 98)	(98, 8, 7, 106)	(98, 8, 7, 103)	(100, 8, 7, 121)	(100, 8, 7, 132)	(98, 8, 7, 119)	(98, 8, 7, 154)
9	(94, 8, 7, 104)	(98, 8, 7, 118)	(96, 8, 6, 185)	(98, 8, 7, 124)	(98, 8, 7, 57)	(98, 8, 7, 39)	(98, 8, 7, 134)	(96, 8, 7, 138)
10	(98, 8, 7, 72)	(96, 8, 7, 116)	(98, 10, 7, 137)	(98, 8, 7, 124)	(96, 8, 7, 32)	(96, 8, 7, 7)	(100, 10, 7, 145)	(98, 8, 7, 170)
11	(98, 8, 7, 56)	(98, 10, 7, 114)	(96, 8, 7, 169)	(98, 10, 7, 123)	(98, 8, 7, 15)	(96, 8, 7, 34)	(98, 10, 7, 161)	(98, 8, 7, 238)
12	(98, 10, 7, 40)	(96, 10, 7, 114)	(98, 10, 7, 201)	(98, 10, 7, 123)	(98, 10, 7, 12)	(98, 8, 7, 35)	(94, 8, 7, 226)	(98, 10, 7, 222)
13	(98, 10, 7, 56)	(98, 10, 7, 114)	(98, 10, 7, 185)	(96, 10, 7, 124)	(98, 10, 7, 13)	(98, 10, 7, 52)	(98, 10, 7, 196)	(96, 8, 7, 221)
14	(98, 10, 7, 24)	(94, 10, 7, 116)	(94, 10, 7, 201)	(96, 10, 7, 125)	(96, 10, 7, 16)	(98, 10, 7, 3)	(96, 10, 7, 210)	(96, 10, 7, 224)
15	(96, 10, 7, 40)	(94, 12, 7, 114)	(96, 12, 7, 217)	(98, 10, 7, 126)	(96, 10, 7, 31)	(94, 10, 7, 2)	(96, 10, 7, 241)	(92, 10, 7, 239)
16	(94, 10, 7, 24)	(90, 12, 7, 114)	(92, 12, 7, 233)	(94, 10, 7, 127)	(94, 10, 7, 16)	(98, 10, 7, 1)	(96, 10, 7, 241)	(92, 12, 7, 256)

Table 2: Experiment Results of *Opt-2* on Initial S-box

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

Table 3: Optimal S-box using *Opt-1* Construction

(refer Table 2). In term of its cryptographic properties, this S-box exhibits a better value of NL (i.e. NL $= 104$) than the S-box in Table 3, while the value for DU and AD are same for both result (i.e. DU $= 6$ and AD $= 7$).

The first column in Tables 3 and 4 denote the first four bits of the input while the first row denote the remaining four bits of the 8-bit input to the S-box. For instance, the input `4A` gives the output of `74` in Table 3 (i.e. F(`4A`) = `74`), and `3B` in Table 4 (i.e. F(`4A`) = `3B`). There are a total of 14 highlighted elements in Table 3, and nine highlighted elements in Table 4 which represents the changed elements of these two optimal S-boxes from the initial S-box, S-Box2. While the bold elements at the same positions in Tables 3 and 4 are to differentiate these two optimal S-boxes.

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

Table 4: Optimal S-box using *Opt-2* Construction

In general, the S-box construction using *Opt-2* technique produced more cryptographically strong S-boxes than the construction using *Opt-1* technique. This can be verified by the number of optimal generated S-boxes in Table 2 is higher than the number of optimal generated S-boxes in Table 1. However, independently, there are a total of 24 results from Table 1 compared to only 22 results from Table 2 which exhibits NL > 100. For DU, Table 2 produced five results that fulfil pre-condition requirements of $2 \leq \text{DU} \leq 6$ compared to three results from Table 1. The number of AD that reaches optimal value (i.e. AD $= 7$) are same in both construction options.

3.4 Discussion

By adopting and combining the *Redundancy Removal Algorithm* (Isa et al., 2013) and *Bee Waggle Dance* algorithm (Isa et al., 2016), we manage to obtain cryptographically strong S-boxes that compare well with the original proposed constructions. Table 5 summarised the main cryptographic properties (i.e. NL, DU, and AD) exhibited by each proposed S-box construction involved in this study which are Mamadolimov et al. (2013), Isa et al. (2013), Isa et al. (2016) and our result.

In summary, the S-box generated using BWD algorithm (Isa et al., 2016) is ranked first since it exhibits NL = 108, DU = 6 and AD = 7. As described

Construction	NL	DU	AD	Technique
Isa et al. (2016)	108	6	7	Bee Waggle Dance Algorithm
Isa et al. (2013)	**104**	**6**	**7**	Redundancy Removal Algorithm*
This paper				***Opt-2*: RRA (BWD (Initial S-box))**
	102	**6**	**7**	***Opt-1*: BWD (RRA (Initial S-box))**
Mamadolimov et al. (2013)	102	8	7	Redundancy Removal Algorithm

*This technique is not utilised in the said paper. See discussion below.

Table 5: Comparison Result

in Section 3.2 above, the final S-box was generated after performing eight different dance directions, 14 distinct dance distances and at least a loop on the initial S-box that was generated from trinomial power function.

Our *Opt-2* S-box construction and Isa et al. (2013)'s proposed construction are ranked second. At this rank, the proposed S-box exhibits (104, 6, 7) for its (NL, DU, AD), respectively. In brief, Isa et al. (2013) took a non-permutation power function with highest NL (i.e. NL = 112) and lowest DU (i.e. DU = 2) as a base-function and add it with another power function over $\mathbb{F}_{2^8}$ to generate an initial S-box. If the initial S-box is found not bijective, then RRA is applied. Otherwise, at least any two elements in initial S-box were swapped to generate the final S-box. For our *Opt-2* construction, we adopt the S-box generated in Isa et al. (2014, 2015) with slight modification which lastly exhibits (105, 8, 4) for its (NL, DU, AD) as an initial S-box. Then this initial S-box performs the BWD algorithm on its distance and direction parameters, then followed by the RRA on the generated S-box to obtain the final cryptographically strong S-box.

Our *Opt-1* S-box construction is ranked third. Using the same initial S-box generated in *Opt-2* construction, we first perform the S-box optimisation through the RRA and followed by BWD algorithm to obtain the final bijective S-box with cryptographic properties of (102, 6, 7) for its (NL, DU, AD), respectively.

The proposed S-box by Mamadolimov et al. (2013) is ranked last. This proposal was the first introducing the RRA in the construction of an S-box. However, since the value of their DU = 8, thus make the S-box fail to fulfil one of the pre-condition required to be considered as cryptographically strong (i.e. $2 \leq \text{DU} \leq 6$).

Our best result produced so far, however, fail to outperform the original proposal of Isa et al. (2016). We only manage to obtain the same result as the proposed construction by Isa et al. (2013) using *Opt-2* construction. The key factor of our result might due to the selection of initial S-box with lower NL (instead of NL = 112 as used in Isa et al. (2016)). Besides that, we notice that the exemplary construction in Isa et al. (2013) was not invoking the RRA. This is because, after an intermediate processing stage, their initial S-box is already bijective. Thus, their final S-box was generated from swapping the elements in the initial S-box. Nevertheless, as an alternative, our proposed method manage to produce several cryptographically strong S-boxes that fulfils our pre-condition requirements as discussed in Section 2.

Note that although our S-box with an NL value of 102 and 104 is lower than the best known value of 112, it does not necessarily mean that it is weak. Other prominent block ciphers such as Skipjack (National Institute of Standards and Technology, 1998) and CLEFIA (Shirai et al., 2007) use S-boxes with NL = 100. These ciphers were designed by a team of cryptographers from the United States National Security Agency (NSA) and Sony Corporation, respectively.

4 CONCLUSION

In this paper, we manage to combine two different algorithms proposed by Isa et al. (2013) and Isa et al. (2016) named as *Redundancy Removal Algorithm* and *Bee Waggle Dance* algorithm, respectively to construct an S-box. We conducted two options of construction. First option, we performed RRA first and followed by BWD algorithm on the initial S-box. While for the second option, we first utilised BWD algorithm on the initial S-box, then finalised the optimisation using RRA. With the right selection of initial S-box, this combination managed to produce several cryptographically strong S-boxes that fulfils our pre-condition requirements of i) NL > 100, ii) $2 \leq$ DU ≤ 6 and iii) AD ≥ 4. Our experiments show that the second option, *Opt-2* produced more cryptographically strong S-boxes.

ACKNOWLEDGMENTS

The authors would like to express their deepest gratitude to Ministry of Higher Education (MOHE), Malaysia for the financial support in this research project under the Exploratory Scheme Research Grant 2012/13.

REFERENCES

Alkhaldi, A. H., Hussain, I., and Gondal, M. A. (2015). A Novel Design for the Construction of Safe S-boxes based On TDERC Sequence. *Alexandria Engineering Journal*, 54(1):65–69.

Biham, E. and Shamir, A. (1991). Differential Cryptanalysis of DES-like Cryptosystems. *Journal of Cryptology*, 4(1):3–72.

Carlet, C. (2011). On Known and New Differentially Uniform Functions. In Parampalli, U. and Hawkes, P., editors, *Information Security and Privacy: 16^{th} Australasian Conference, ACISP 2011, Melbourne, Australia, July 11-13, 2011. Proceedings*, volume 6812 of *Lecture Notes in Computer Science*, pages 1–15. Springer Berlin Heidelberg, Berlin, Heidelberg.

Isa, H., Jamil, N., and Z'aba, M. R. (2013). S-box Construction from Non-Permutation Power Functions. In *Proceedings of the 6^{th} International Conference on Security of Information and Networks*, SIN '13, pages 46–53, New York, NY, USA. ACM.

Isa, H., Jamil, N., and Z'aba, M. R. (2014). Improved S-box Construction from Binomial Power Functions. In *Proceedings of the 4^{th} International Cryptology and Information Security Conference 2014 (CRYPTOLOGY2014)*, CRYPTOLOGY2014, pages 131–139, UPM Serdang, Selangor, Malaysia. Institute for Mathematical Research (INSPEM).

Isa, H., Jamil, N., and Z'aba, M. R. (2015). Improved S-box Construction from Binomial Power Functions. *Malaysian Journal of Mathematical Sciences*, 9(S)(1):21–35.

Isa, H., Jamil, N., and Z'aba, M. R. (2016). Construction of Cryptographically Strong S-Boxes Inspired by Bee Waggle Dance. *New Generation Computing*, 34(3):221–238.

Ivanov, G., Nikolov, N., and Nikova, S. (2016). Reversed Genetic Algorithms for Generation of Bijective S-boxes with Good Cryptographic Properties. *Cryptography and Communications*, 8(2):247–276.

Kazymyrov, O., Kazymyrova, V., and Oliynykov, R. (2013). A Method for Generation of High-Nonlinear S-Boxes based on Gradient Descent. Cryptology ePrint Archive, Report 2013/578.

Knudsen, L. R. (1995). Truncated and Higher Order Differentials. In Preneel, B., editor, *Fast Software Encryption: Second International Workshop Leuven, Belgium, December 14–16, 1994 Proceedings*, volume 1008 of *Lecture Notes in Computer Science*, pages 196–211. Springer Berlin Heidelberg, Berlin, Heidelberg.

Mamadolimov, A., Isa, H., and Mohamad, M. S. (2013). Practical Bijective S-box Design. *CoRR*, abs/1301.4723.

Matsui, M. (1994). *Linear Cryptanalysis Method for DES Cipher*, volume 765 of *Lecture Notes in Computer Science*, pages 386–397. Springer Berlin Heidelberg, Berlin, Heidelberg.

National Institute of Standards and Technology (1998). SKIPJACK and KEA Algorithm Specifications.

National Institute of Standards and Technology (2001). Advanced Encryption Standard. Federal Information Processing Standard (FIPS) 197.

Shannon, C. E. (1949). Communication Theory of Secrecy Systems. *Bell System Technical Journal*, 28(4):656–715.

Shirai, T., Shibutani, K., Akishita, T., Moriai, S., and Iwata, T. (2007). *The 128-Bit Blockcipher CLEFIA (Extended Abstract)*, pages 181–195. Springer Berlin Heidelberg, Berlin, Heidelberg.

Yang, M., Wang, Z., Meng, Q., and Han, L. (2011). Evolutionary Design of S-box with Cryptographic Properties. In *Ninth IEEE International Symposium on Parallel and Distributed Processing with Applications Workshops (ISPAW), 2011*, ISPAW '11, pages 12–15. IEEE Computer Society.