An Improved AES S-box Based on Fibonacci Numbers and Prime Factor

Kamsiah Mohamed[1], Fakariah Hani Hj Mohd Ali[1], Suriyani Ariffin[1], Nur Hafiza Zakaria[2] and Mohd Nazran Mohammed Pauzi[3]

(Corresponding author: Kamsiah Mohamed)

Faculty of Computer and Mathematical Sciences, Universiti Teknologi MARA[1]

40450 Shah Alam,Selangor, Malaysia

Faculty of Science and Technology, University Sains Islam Malaysia[2]

71800 Nilai, Negeri Sembilan, Malaysia

Faculty of Engineering and Life Sciences, Universiti Selangor[3]

45600, Bestari Jaya, Selangor, Malaysia

(Email: kamsh@unisel.edu.my)

(Received Aug. 28, 2017; revised and accepted Dec. 18, 2017)

Abstract

This paper emphasises the study on ways of constructing the substitution boxes (S-boxes). To improve the strength of block cipher, a new proposed substitution box for symmetric key cryptography was designed based on Fibonacci numbers and prime factor. This new security approach was designed for better security of block ciphers. The level of security S-box was evaluated based on the cryptographic properties such as balance criteria, nonlinearity, correlation immunity, algebraic degree, transparency order, propagation, number of fixed points and opposite fixed points, algebraic immunity, robustness to differential cryptanalysis, signal to noise ratio (SNR) Differential Power Analysis (DPA) as well as confusion coefficient. The AES S-box and the new proposed S-box were analysed to verify the cryptographical security of the S-box. Result showed that the new proposed S-box using the Fibonacci numbers and prime factor possessed good cryptographic properties compared to the AES S-box.

Keywords: Block Cipher; Cryptography; Fibonacci; S-box

1 Introduction

Cryptography is an important part of information security that covers the investigation of algorithms and protocols for secure information. Within the advancement of technology, the design of cryptographic algorithm is often enhanced to ensure that information is secure. In terms of security, it is always a question of whether or not these algorithms are secure enough to protect information. Block ciphers are the most prominent and important elements to provide high level security. Generally, block cipher is a deterministic algorithm on fixed length group of bits known as blocks to transform a fixed length block of plaintext message blocks into cipher text blocks of the same length. Since 1970, block cipher design and analysis have been widely studied culminating in the selection of Rijndael [8] as the new Advanced Encryption Standard (AES) in 2001 [5]. Thus, a modern block cipher was designed based on the AES substitution box (called S-box) to substitute blocks of input bits to a set of output bits. S-box is a critical part of any block cipher that provides the primary source non-linear [12, 16].

This paper proposes a design of secure symmetric encryption S-box to improve the existing S-box. The design and characteristics of S-box in a block cipher are the central measures of resistance against all adequately high nonlinearities [9]. The confusion and diffusion properties are needed to build a strong encryption algorithm as suggested by [37]. However, there are some problems addressed in the process of the designing of a new S-box. The two sets of problems arise from the selection of an S-box before its cryptographic use can be considered secure. The first problem is related to the design (or search) of a good S-box while the second problem is in the verification of a given S-box as one cryptanalytic technique [2]. Hence, constructing secure S-boxes to use them in different cryptosystems for increasing their security is the current study problem [17]. S-box design is usually the most important task while designing a new cipher [7].

The design of the new S-box is an important concern in creating new and more secure cryptosystems [11]. The disadvantages of S-box design are the limitations that make it vulnerable and insecure [1, 18]. Currently, there are no algebraic procedures that can give the preferred and complete set of properties for an S-box [33]. Thus, there has been a lot of attention on redesigning, recreating or renewing the design and implementation of the original AES S-box.

Based on previous studies, there are various techniques used to construct the standard AES S-box such as linear-transform and non-linear function [39], fractional linear transformation [19], branch numbers [36], affine transformation [6, 41] and the network RFWKIDEA32-1 [26]. In another study, it was shown that Fibonacci number can make secure communication from cryptanalysis attacks [35]. This technique can fulfil the requirements for communication such as capacity, security and robustness to secure data transmission over an open channel. Recent studies proved that the performance of encryption and decryption algorithm using Fibonacci number is faster than symmetric algorithms [38] and RSA algorithms [14]. These studies demonstrated that the performance of encryption and decryption algorithm can be increased using Fibonacci numbers. However, no study has addressed Fibonacci technique and prime factor to construct the AES S-box. In this paper, Fibonacci numbers and prime factor were used to improve the original AES S-box.

This paper is organized as follows: In Section 2, previous studies on Fibonacci numbers are reviewed. Section 3 briefly describes the AES S-box in cryptography, the Fibonacci numbers and prime factor. Comparison between the properties of Boolean functions of our new proposed S-box and the AES S-box is explained in Section 4. Finally, conclusion is presented in Section 5.

2 Review on Fibonacci Numbers

In the field of cryptography, numbers play an important role in different theoretical and practical applications. Cryptosystems rely on the assumption that a number of mathematical problems are computationally intractable since they cannot be solved in polynomial time [29]. The Fibonacci numbers are natural numbering system appropriate for the development of each living thing. Many studies have investigated on how Fibonacci sequence can be observed in the real world. These numbers occur everywhere in nature, ranging from the leaf arrangement in plants, the structure of DNA as well as various proportions in human face and structure of sea shells. One study has been conducted observing that the phyllotaxis of plants follows the Fibonacci sequence [28].

A study by [23] showed that the structure of DNA and its organization pattern is a fractal. Then, [31] discovered that the DNA gene-coding region sequences are strongly related to the Golden Ratio and Fibonacci/Lucas integer numbers. In another study, [3] examined the Fibonacci numbers can be seen in the structure of coronary arterial tree and that diseased atherosclerotic lesions in coronary arteries follow the Fibonacci distribution. Nevertheless, in computer science, the Fibonacci numbers act as a foundation for various algorithms that are widely applied. In a previous study, the Fibonacci numbers have been applied in the encryption and decryption algorithm to display encrypting message.

In another study [34], it was shown that the content of the original message were changed to the ciphertext by taking each character from the message and converting it based on the Fibonacci numbers. Based on these previous studies, understanding the role of the Fibonacci numbers may be a key to increase the performance of block cipher in cryptosystems.

3 AES S-box in Cryptography

Substitution is a nonlinear transformation that makes the confusion of bits. It is often considered as a look-up table, which uses several byte substitution transformations in the key expansion routine to perform a one-for-one substitution of a byte value. An $n \times m$ S-box is a mapping from n input bits to m output bits, $S : \{0,1\}^n \to \{0,1\}^m$. Basically, an S-box is a set of m single output Boolean functions combined in a fixed order. There are 2^n inputs and 2^m possible outputs for an $n \times m$ S-box. Generally, an $n \times m$ S-box, S, is represented as a matrix of size $2^{n \times m}$ for each m-bit entry. An $n \times m$ S-box is a bijective S-box where each input is mapped to a dissimilar output entry and all possible outputs are presented in the S-box.

In 2001, the National Institute of Standards and Technology (NIST) announced the AES as a new standard to replace the Data Encryption Standard (DES). This standard indicates that the Rijndael algorithm is generally utilized as a part of numerous cryptographic applications. It was designed to handle additional block sizes and key lengths 128, 192 and 256 bits. The 128 bits AES encrypted a 16 byte block using a 16 byte key of 10 encryption rounds. The value of each byte in the array is substituted according to a look-up table.

The Rijndael AES S-box is designed based on three transformations. The S-box is generated by determining multiplicative inverse for a given number in Galois Field GF(2^8) using the irreducible polynomial:

$$m(x) = x^8 + x^4 + x^3 + x^1.$$

The multiplicative inverse is then transformed as in Equation (1):

$$x_i' = x_i \oplus x_{(i+4)mod8} \oplus x_{(i+5)mod8} \oplus x_{(i+7)mod8} \oplus C_i. \quad (1)$$

Where x_i is the bit i of the byte and the column vector C_i is added with the value {63} or {01100011}. The affine transformation element of the Rijndael AES S-box can be expressed as shown in Figure 1.

This affine transformation is the sum of multiple rotations of the byte as a vector. Figure 2 shows the original AES S-box represented here with hexadecimal notation.

3.1 Construct AES S-box Using Fibonacci Numbers and Prime Factor

In this paper, the Fibonacci numbers and prime factor were applied to construct the AES S-box to propose a new S-box.

$$\begin{bmatrix} 1&0&0&0&1&1&1&1 \\ 1&1&0&0&0&1&1&1 \\ 1&1&1&0&0&0&1&1 \\ 1&1&1&1&0&0&0&1 \\ 1&1&1&1&1&0&0&0 \\ 0&1&1&1&1&1&0&0 \\ 0&0&1&1&1&1&1&0 \\ 0&0&0&1&1&1&1&1 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \\ x_8 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix}$$

Figure 1: Affine transformation of Rijndael AES S-box

AES S-BOX

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

INVERSE AES S-BOX

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

Figure 2: The AES S-box

3.2 Fibonacci Numbers

In mathematics, the Fibonacci numbers or Fibonacci sequences are the numbers in the integer sequence of 0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, 233, 377, 610.... Based on the definition, the first two numbers in the Fibonacci sequence are 0 and 1, and each subsequent number is the sum of the previous two. In mathematical terms, the sequence F_n in Fibonacci numbers is defined by the recurrence relation

$$F_n = F_{n-1} + F_{n-2}. \tag{2}$$

With seed values

$$F_0 = 0, F_1 = 1. \tag{3}$$

The Fibonacci numbers were applied because they have a wide range of significant mathematical properties that make them very useful in computer science. Moreover, the Fibonacci numbers are efficiently computable. Based on this fact, the series can be generated efficiently. Any number can be written as the sum of unique Fibonacci numbers. The straightforwardness and beauty of Fibonacci numbers are persuaded to create matrix cryptosystems, which are helpful in securing information.

3.3 Prime Factor

The prime factor is the most remarkable and practical for cryptography. Many algorithms used in public-key cryptography contain various and critical security applications. Most of them are related to the fact that prime factorisation is unique. Prime factorisation is the finding of prime numbers that can be multiply together to make the original number. In a number of theories, prime factor is a positive integer where the prime numbers divide that integer exactly. For a prime factor p of n, the multiplicity of p is the largest exponent a for which pa divides n precisely. In this paper, the AES S-box was improved with the Fibonacci numbers and prime factor to make a strong and secure S-box against cryptanalysis attack.

The new proposed S-box was constructed by the following steps:

1) The multiplicative inverse in the finite field $GF(2^8)$ was taken and the element {00} was mapped to itself.

2) The affine transformation was applied (over $GF(2^8)$).

3) Each byte in the S-box was assumed to comprise 8 bits labelled $[x_7, x_6, x_5, x_4, x_3, x_2, x_1, x_0]$.

4) XOR with the value {63} or {01100011} which is a byte of C_i.

5) Then XOR with the Fibonacci number.

6) XOR with the prime factor.

NEW S-BOX

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

INVERSE S-BOX

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

Figure 3: Proposed S-box

The new equation of the Fibonacci numbers and prime factor is expressed as below.

$$x'_i = x_i \oplus x_{(i+4)mod8} \oplus x_{(i+5)mod8} \oplus x_{(i+7)mod8} \oplus C_i \oplus F_n \oplus P_i^{a_1}. \quad (4)$$

Based on the Equation (4), the proposed S-box generated is illustrated in Figure 3.

4 Analysis of S-boxes Properties

To ensure that the newly proposed S-box is secure, cryptographic tests were applied. In this paper, the AES S-box and the new proposed S-box were analysed using the S-box Evaluation Tool (SET). The SET is a tool utilised for analysing cryptographic properties of Boolean functions and S-boxes composing ANSI C code [32]. The quality of an S-box is determined based on cryptographic properties that must be considered in the designing and analysing of S-boxes.

The experiments were conducted on Ubuntu 16.04LTS operating system to test the cryptographic properties of S-boxes, which are balance criteria, nonlinearity, correlation immunity, algebraic degree, transparency order, propagation, number of fixed points and opposite fixed points, algebraic immunity, robustness to differential cryptanalysis, signal to noise ratio (SNR) Differential Power Analysis as well as confusion coefficient. Each property of S-boxes relates to a certain cryptographic attack.The results from the AES S-box and the new proposed S-box are depicted in Figure 4 and Figure 5.

Meanwhile, the explanation for the cryptographic properties of S-box is described as follows:

Balance: The most fundamental of all cryptographic properties desired to be presented by Boolean function is balance. For an $n \times m$, S-box is mapped from $GF(2^n)$ to $GF(2^m)$. If every value $\in GF(2^m)$ is mapped by an equal number of distinct input values, then the S-box is balanced. On the other hand, if an n-variable Boolean function whose Hamming weight is not equal to 2^{n-1}, it is called an unbalanced function [17].

Nonlinearity: One of the most important cryptographic properties of a Boolean function is nonlinearity. In fact, the nonlinearity of a n-variable Boolean function f represents a measure of the dissimilarity between f and the n-variable affine function a that f bears the closest bitwise similarity to be measured by the Hamming distance between f and a. $S : \{0,1\}^n \rightarrow \{0,1\}^m$ is defined as the least value of nonlinearity of all nonzero linear combination of n Boolean functions $f_i : \{0,1\} \rightarrow \{0,1\}, i = n-1, ?1, 0$ [17]. The nonlinearity of an S-box must be high to resist linear cryptanalysis. Without a nonlinear component, an attacker could express the input and output with a system of linear equations where the key bits are unknown.

The strength of S-box can be evaluated based on the nonlinearity criteria where the high nonlinearity is considered as cryptographically strong. Highly nonlinear functions were stimulated since algorithms close to linear are vulnerable to various approximation attacks [10]. The available limit of nonlinearity for 8×8 S-boxes is 100 [27].

An optimal value of nonlinearity is 120 [20]. Hence, the analysis of the nonlinearity must be high to resist linear cryptanalysis. Thus, the highest possible value of NL is $120 \leq NL \leq 100$.

Correlation Immunity: Correlation immunity is a property of Boolean functions that denotes the extent of independence between linear combinations of the input bits and the output. An n-variable Boolean function, $f(x)$, which is mth-order correlation immune, is denoted $CL(m)$ if it is statistically independent of the subset of m input variables where $1 \leq m \leq n$. An n-variable boolean function, $f(x)$, which is mth-order correlation immune, is denoted by $CL(m)$, if, for every ω such that $1 \leq HW(\omega) \leq m, \hat{F}(\omega) = 0$. Thus, the higher the order of correlation immunity m, the more positions in $\hat{F}(\omega)$ must have the values of zero [40].

Algebraic Degree: The S-boxes should be the algebraic functions of higher degree to resist higher order differential attacks [22]. The algebraic degree of an S-box (similarly, a Boolean function) is desired to be as high as possible to resist a cryptanalytic attack known as lower order approximation [42].

Algebraic Immunity: Boolean functions with high algebraic immunity (AI) are vital to reduce the possibility of utilising algebraic attacks in breaking an encryption system. The algebraic immunity of an S-box depends on the number and type of linearly independent multivariate equations it satisfies [30].

Transparency Order: Transparency order is proposed as a parameter for the robustness of S-boxes to Differential Power Analysis (DPA): lower transparency order denoting more resistance. However, most cryptographically strong Boolean functions have been found to have high transparency order [24]. Also to prevent DPA attacks, transparency order of the S-box should be as low as possible.

Propagation Characteristic: An n-variable Boolean function $f(\bar{x})$ satisfies the propagation characteristics of degree k if $f(\bar{x})$ changes with a probability of half when $i, (1 \leq i \leq k)$ bits of $f(\bar{x})$ are complemented. Propagation characteristic is a Boolean function property that enables a function to achieve good diffusion by ensuring output uniformity [15,17].

Fixed(Fp)and Opposite Fixed Points(OFp): For an $n \times m$ S-box, a fixed point is defined as $f(x) = x$ where if an input x is given, the output is also x. An opposite fixed point is defined as $f(x) = \bar{x}$, where $\bar{x}$ denotes the bitwise complement of x. The number of Fp and OFp should be kept as low as possible to avoid leakage in any statistical cryptanalysis [21].

Robustness to Differential Cryptanalysis: Let $F = (f_1, f_2, ..., f_n)$ be an $n \times m$ S-box where f_i is a component function of S-box mapping $f_i = \{0,1\}^n \rightarrow \{0,1\}^m$. F is said to be robust against differential cryptanalysis [25].

Signal to Noise Ratio (SNR) Differential Power Analysis: The SNR of the DPA signal increases with the resistance against linear or differential cryptanalysis. When the SNR is bounded, the lower bound is reached by the poorest cryptographic S-boxes namely affine S-boxes. High quality cryptographic S-boxes are evaluated based on high SNR, which is close to the maximum bound [15]. A higher SNR values mean that the signal strength is stronger in relation to the noise levels.

Confusion Coefficient: The confusion coefficient property was defined with the intention to characterise the resistance of an S-box. Recently, [13] introduced confusion coefficient as a new property that relates to the DPA resistance of S-boxes. A high confusion coefficient indicates that the S-box output is very distinctive. Table 1 shows the comparison between the proposed S-box and the standard AES S-box. Based on the balance properties, findings suggest that both S-boxes are balanced. There is no exploitable bias where an attacker is unable to trivially approximate the functions or the output. In particular, a large imbalance may enable the Boolean function to be easily approximated by a constant function.

The confusion in a cipher system is measured through the nonlinear properties. Thus, the results indicate that the nonlinearity value of the standard AES S-box and the proposed S-box is high, achieving the optimal value to resist linear cryptanalysis attack. For correlation immunity, the results show that the AES S-box and the proposed S-box are zero independence between linear combinations of the input bits and the output. Meanwhile, the result for the algebraic degree properties shows that the proposed S-box has achieved high algebraic degree compared to the AES S - box. The AES S-box showed an algebraic degree 7, whereas the proposed S-box displayed an algebraic degree 8. Therefore, the proposed S-box will be more difficult to be attacked by algebraic attacks or higher-order differential cryptanalysis.

For algebraic immunity, the results demonstrated that the AES S-box and the proposed S-box is 4, which indicate that both S-boxes are secure from algebraic attack. For the transparency order properties, the proposed S-box was found to be smaller than the AES S-box, which means that the proposed S-box has better DPA resistance compared to the AES S-box. For propagation characteristic, the comparison of the PC(k) was satisfied by both S-boxes. While for the number of Fixed Points (Fp) and Opposite Fixed Points (OFp), the results showed that both S-boxes were satisfied. For robustness to differential cryptanalysis, the proposed S-box was seen to have higher resistance to DPA attacks than the AES S-box. The SNR (DPA) valued of the proposed S-box (9.8) was higher than the AES S-box (9.6). Thus, the proposed S-box has better resistance to DPA attacks in terms of SNR (DPA).

The last cryptographic property is confusion coefficient. From the results, the proposed S-box has a confusion coefficient variance of 0.1016 compared to the AES S-box, which is 0.1113. Hence, it was seen that the proposed S-box indicated a low confusion coefficient value to

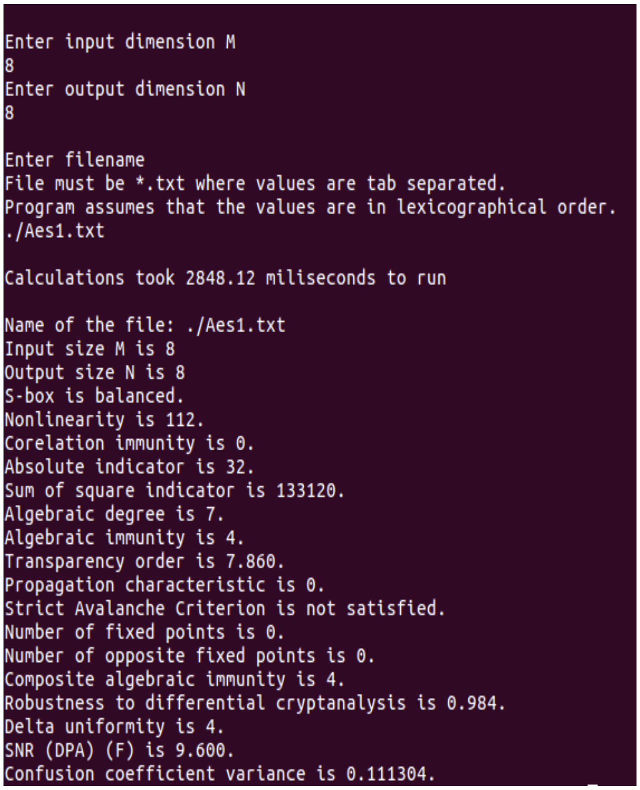

Figure 4: Result for AES S-box

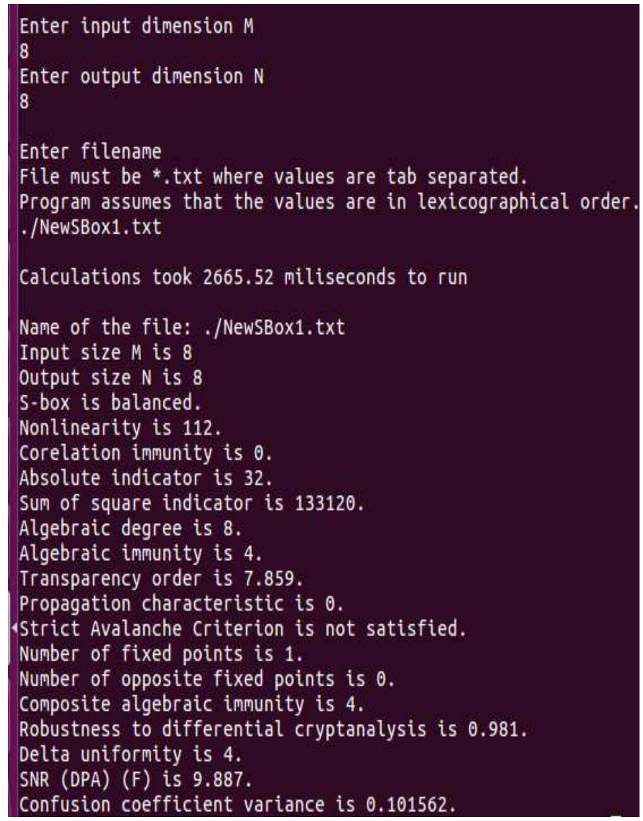

Figure 5: Result for the proposed S-box

make it harder for the side-channel attacks to attack the S-box.

As a conclusion, the proposed S-box has good cryptographic properties for algebraic degree, transparency order, robustness to differential cryptanalysis, SNR(DPA) and confusion coefficient than the AES S-box. Besides, the result of balance = 0, nonlinearity = 112, correlation immunity = 0, and algebraic immunity = 4 is similar to AES S-box.

According to [40], if an S-box satisfies these cryptographic properties, the S-box can be considered cryptographically secure. Therefore, it is important for every S-box to be evaluated based on cryptographic properties to resist linear attack, differential attack, algebraic attack and side channel attack.

5 Conclusions

In this paper, a new way to enhance the AES S-box has been explored using the Fibonacci numbers and prime factor approach to increase the security of S-box in a block cipher. The results showed that the values of several cryptography properties of the proposed S-box are similar with that of the existing S-box such as balance, nonlinearity, correlation immunity, algebraic immunity and propagation characteristic. Hence, the proposed S-box inherits all good cryptographic characteristics of the standard AES S-box. From the result, it was observed that the proposed S-box has a high algebraic degree, low transparency order, low robustness to differential cryptanalysis, high signal to noise ratio (SNR) differential power analysis and high confusion coefficient compared to the standard AES S-box. The experiments have shown that the new proposed S-box fulfilled the confusion and diffusion properties as described by [37].

The experimental results indicate that the proposed S-box has a high quality of cryptography properties. Therefore, the Fibonacci numbers and prime factor have made the proposed S-box to have more resistant to linear cryptanalysis attacks and differential cryptanalysis. As a result, this approach had increased the security level of S-box to achieve high quality cryptography properties. Future studies can be done by demonstrating of cache-timing attacks against the proposed S ?box as introduced by [4].

Timing attack is a type of side-channel attacks that allows an attacker to extract information based on the time taken to execute cryptographic algorithms. Since cryptographic systems generally work on the keys, hence, side-channel attacks have been developed to break a system. The size of the proposed S - box was analysed to see whether or not it leaks timing information during cache hits to determine its immunity against cache-timing attacks.

Table 1: Comparison of cryptographic properties between the AES S-box and the proposed S-box

Cryptographic Properties	**AES S-Box**	**Proposed S-Box**	**Range of Value (Parameter n)**	**Good Cryptographic Properties**
Balance	0	0	$n = 0$	No Exploitable Bias
Nonlinearity	112	112	$120 \geq n \geq 100$	High
Correlation Immunity	0	0	$n \leq 0$	Low
Algebraic Degree	7	8	$n \geq 10$	High
Algebraic Immunity	4	4	$n \leq 4$	Low
Transparency Order	7.860	7.859	$n < 7.8$	Low
Propagation Characteristic	0	0	$n \leq 0$	Low
Fixed (Fp) and Opposite Fixed points (OFp)	0,0	1,0	$n \leq 4$	Low
Robustness to Differential Cryptanalysis	0.984	0.981	$n < 0.98$	Low
Signal to Noise Ratio (SNR) Differential Power Analysis	9.600	9.887	$n > 0.98$	High
Confusion Coefficient	0.111	0.101	$n \leq 0$	Low

Acknowledgments

This research was supported by the Institute of Research Management and Innovation, Universiti Teknologi MARA (UiTM), Malaysia and registered under the research grant 600-IRMI/FRGS 5/3 (017/2017) by the Ministry of Education Malaysia. The authors gratefully acknowledge the anonymous reviewers for their valuable comments.

References

[1] C. Adams and S. Tavares, "The structured design of cryptographically good S-boxes," *Journal of Cryptology*, vol. 3, no. 1, pp. 27–41, 1990.

[2] N. Ahmed, "Testing an S-box for cryptographic use," *International Journal of Computer and Electrical Engineering*, pp. 1–5.

[3] H. Ashrafian and T. Athanasiou, "Fibonacci series and coronary anatomy," *Heart, Lung and Circulation*, vol. 20, no. 7, pp. 483–484, 2011.

[4] D. J. Bernstein, "Cache-timing attacks on AES", 2005.

[5] C. Cid and R. Weinmann, *Block Ciphers: Algebraic Cryptanalysis and Gröbner Bases. In Gröbner Bases, Coding, and Cryptography*, 2009.

[6] J. Cui, L. Huang, H. Zhong, C. Chang and W. Yang, "An Improved AES S-box and Its Performance Analysis," *International Journal of Innovative Computing, Information and Control*, vol. 7, no. 5, pp. 2291–2302, 2011.

[7] A. G. Czurylo, "Cryptographic Properties of Modified AES-like S-boxes," *Annales Universitatis Mariae Curie-Sklodowska Informatica*, vol. 11, no. 2, pp. 37–48, 2011.

[8] J. Daemen and V. Rijmen, *The design of Rijndael:* AES-*the advanced encryption standard*, 2013.

[9] A. Datta, D. Bhowmik and S. Sinha, "A Novel Technique for Analysing Confusion in S-boxes," *International Journal of Innovative Research in Computer and Communication Engineering*, vol. 4, no. 6, pp. 11608–11615, 2016.

[10] O. Dunkelman and N. Keller, "A New Criterion for Nonlinearity of Block Ciphers," in *Cryptographers Track at the RSA Conference*, pp. 295–312, 2006.

[11] M. H. Dawson and S. E Tavares, "An Expanded Set of S-box Design Criteria Based on Information Theory and Its Relation to Differential-like Attacks," in *Workshop on the Theory and Application of of Cryptographic Techniques*, pp. 352–367, 1991.

[12] C. Easttom, *Creating Cryptographic S-Boxes: A Guideline for Designing Cryptographic S-boxes*, Feb. 25, 2018. (`https://pdfs.semanticscholar.org/7ae7/bcad617a7106afabc0ee7f29b16b6cadcb22.pdf`)

[13] Y. Fei, A. A. Ding, J. Lao, and L. Zhang, "A Statistics-based Fundamental Model for Side-channel Attack Analysis," *IACR Cryptology ePrint Archive*, vol. 2014, pp. 152, 2014.

[14] N. G. Gonsalves, N. G. Bhat and K. K Tangod, "Performance Analysis of Secured Communication With Cryptography Using Fibonacci Series," *International Journal of Innovations In Engineering Research And Technology (IJIERT'17)*, vol. 4, no. 6, 2017.

[15] S. Guilley, P.E. Hoogvorst and R. Pacalet, "Differential power analysis model and some results," *Smart Card Research and Advanced Applications VI*, pp. 127–142, 2004.

[16] T. Gulom, "The encryption algorithms GOST28147-89-IDEA8-4 and GOST28147-89-RFWKIDEA8-4,"

International Journal of Electronics and Information Engineering, vol. 6, no. 2, pp. 59-71, 2017.

[17] I. Hussain and T. Shah, *Literature Survey on Nonlinear Components and Chaotic Nonlinear Components of Block Ciphers*, Dordrecht: Springer Science & Business Media, 2013.

[18] I. Hussain, T. Shah, M. Afzal and H. Mahmood, "Comparative analysis of S-boxes based on graphical SAC," *International Journal of Computer Applications*, vol. 2, no. 5, 2010.

[19] I. Hussain, T. Shah, M. A. Gondal and W. A. Khan, "Construction of Cryptographically Strong 8× 8 S-boxes," *World Applied Sciences Journal*, vol. 13, no. 11, pp. 2389–2395, 2011.

[20] I. Hussain, T. Shah, H. Mahmood and M. A. Gondal, "A projective general linear group based algorithm for the construction of substitution box for block ciphers," *Neural Computing and Applications*, vol. 22, no. 6, pp. 1085–1093, 2013.

[21] H. Isa, N. Jamil and M. R. Z'aba, "S-box construction from non-permutation power functions," in *Proceedings of the 6th International Conference on Security of Information and Networks*, pp. 46–53, 2013.

[22] L. R. Knudsen, "Truncated and Higher Order Differentials," in *International Workshop on Fast Software Encryption*, pp. 196–211, 1994.

[23] B. B. Mandelbrot, "The Fractal Geometry of Nature," *WH Freeman and Company New York, USA*, 1982.

[24] B. Mazumdar, D. Mukhopadhyay, and I. Sengupta, "Constrained Search for a Class of Good S-boxes with Improved DPA Resistivity," *IACR Cryptology ePrint Archive*.

[25] B. Mazumdar, D. Mukhopadhyay and I. Sengupta, "Design for security of block cipher S-boxes to resist differential power attacks," in *25th International Conference on VLSI Design (VLSID'12)*, pp. 113–118, 2012.

[26] A. Mersaid and T. Gulom, "The Encryption Algorithm AES-RFWKIDEA32-1 Based on Network RFWKIDEA32-1," *International Journal of Electronics and Information Engineering*, vol. 4, no. 1, pp. 1–11, 2016.

[27] W. Millan, "How to improve the nonlinearity of bijective S-boxes," in *Australasian Conference on Information Security and Privacy*, pp. 181–192, 1998.

[28] G. J. Mitchison, "Phyllotaxis and the Fibonacci Series," *Science*, vol. 196, no. 4287, pp. 270–275, 1977.

[29] M. H. Mohamed, Y. B. Mahdy and W. A. E. Shaban, "Confidential Algorithm for Golden Cryptography Using Haar Wavelet," in *International Journal of Computer Science and Information Security (IJCSIS'15)*, 2015.

[30] Y. Nawaz, K. C. Gupta, and G. Gong, "Algebraic immunity of S-boxes based on power mappings: analysis and construction," *IEEE Transactions on Information Theory*, vol. 55, no. 9, pp. 4263–4273, 2009.

[31] J. C. Perez, "Chaos, DNA and Neuro-computers: A golden link: The hidden language of genes, global language and order in the human genome," *Speculations in Science and Technology*, vol. 14, no. 4, pp. 339–346, 1991.

[32] S. Picek, L. Batina, D. Jakobović, B. Ege and M. Golub, "S-box, SET, Match: A Toolbox for S-box Analysis," in *Workshop on Information Security Theory and Practice (WISTP)*, pp. 140–149, 2014.

[33] S. Picek, B. Ege, L. Batina, D.J. Jakobovic, L. Chmielewski and M. Golub, "On Using Genetic Algorithms for Intrinsic Side-channel Resistance: The Case of AES S-box," in *Proceedings of the First Workshop on Cryptography and Security in Computing Systems*, pp. 13–18, 2014.

[34] A. Q. Quazi, P. G. Maddikar and K. K Tangod, "A Survey on Secure E-mailing System with Cryptography Using Fibonacci Series," *International Journal of Innovative Research in Computer and Communication Engineering*, vol. 5, no. 5, pp. 9911–9915, 2017.

[35] A. J. Raphael and V. Sundaram, "Secured Communication through Fibonacci Numbers and Unicode Symbols," *International Journal of Scientific & Engineering Research*, vol. 3, no. 4, pp. 2229–5518, 2012.

[36] P. C. Ruisanchez, "A New Algorithm to Construct S-boxes with High Diffusion," *International Journal of Soft Computing, Mathematics and Control (IJSCMC)*, vol. 4, no. 3, 2015.

[37] C. E. Shannon, "Communication Theory of Secrecy Systems," *Bell Labs Technical Journal*, vol. 28, no. 4, pp. 656–715, 1949.

[38] B. S. Tarle and G. L. Prajapati, "On The Information Security Using Fibonacci Series," in *Proceedings of the International Conference and & Workshop on Emerging Trends in Technology (ICWET'11)*, pp. 791–797, 2011.

[39] B. N. Tran, T. D. Nguyen and T. D. Tran, "A New S-box Structure to Increase Complexity of Algebraic Expression for Block Cipher Cryptosystems," in *International Conference on Computer Technology and Development(ICCTD'09)*, vol. 2, pp. 212–216, 2009.

[40] G. Z. Xiao and J. L. Massey, "A Spectral Characterization of Correlation-immune Combining Functions," *IEEE Transactions on information Theory*, vol. 34, no. 3, pp. 569–571, 1988.

[41] N. H. Zakaria, R. Mahmod, N. I. Udzir and Z. A. Zukarnain, "Enhancing Advanced Encryption Standard (AES) S-box Generation Using Affine Transformation," *Journal of Theoretical & Applied Information Technology*, vol. 72, no. 1, 2015.

[42] Y. Zheng and X. M. Zhang, "Improved upper bound on the nonlinearity of high order correlation immune functions," in *Selected Areas in Cryptography (SAC'00)*, vol. 2012, pp. 262–274, 2000.

Biography

Kamsiah Mohamed received her Master degree in Software Engineering from Universiti Putra Malaysia (UPM). She is currently a Ph.D. candidate in Computer Science at Universiti Teknologi MARA (UiTM), Malaysia. Her research interest is Cryptography.

Fakariah Hani Hj Mohd Ali is a senior lecturer in the Faculty of Computer and Mathematical Sciences, Universiti Teknologi MARA (UiTM), Malaysia. She received her PhD degree in Network Security from the University Putra Malaysia (UPM). Her research interest includes Cryptography, Network Security and Big Data.

Suriyani Ariffin is a senior lecturer in the Faculty of Computer and Mathematical Sciences (UiTM), Malaysia. She received her PhD degree in Network Security from Universiti Putra Malaysia (UPM). Her research interest includes Cryptography and Network Security.

Nur Hafiza Zakaria is a lecturer in the Faculty of Science and Technology, Universiti Sains Islam Malaysia (USIM). She received her PhD degree in Security in Computing from the Universiti Putra Malaysia (UPM). Her research interest includes Cryptography and Computer Security.

Mohd Nazran Mohammed Pauzi is a lecturer in the Faculty of Engineering and Life Sciences, Universiti Selangor (UNISEL), Malaysia. He is currently a Ph.D. candidate in Mathematics at Universiti Kebangsaan Malaysia (UKM). His research interest is Cryptography and Complex Analysis.