Enhancing Hierocrypt-3 Performance by Modifying Its S-Box and Modes of Operations

Wageda I. El Sobky[1], Ahmed R. Mahmoud[1], Ashraf S. Mohra[1], and T. El-Garf [2]
[1] Benha Faculty of Engineering, Benha University, Egypt
[2] Higher Technological Institute 10th Ramadan, Egypt
Email: wageda.alsobky@bhit.bu.edu.eg; ahmed.mokhtar@bhit.bu.edu.eg;

Abstract—Human relationships rely on trust, which is the reason that the authentication and related digital signatures are the most complex and confusing areas of cryptography. The Massage Authentication Codes (MACs) could be built from cryptographic hash functions or block cipher modes of operations. Substitution-Box (S-Box) is the unique nonlinear operation in block ciphers, and it determines the cipher performance. The stronger S-Box, the stronger and more secure the algorithm. This paper focuses on the security considerations for MACs using block cipher modes of operations with the Hierocrypt-3 block cipher. the Hierocrypt-3 could be considered as a week cipher. It could be enhanced by changing its S-Box with a new one that has better performance against algebraic attack with using different modes of operations. The mathematical model for the new S-Boxes with its properties is provided. The result of this change appeared in the mirror of Average Strict Avalanche Criterion (SAC) and some other properties. SAC could be improved from 0.80469 to 0.16406. The Hierocrypt-3 could be enhanced for more security.

Index Terms—Hierocrypt, S-Box, Security, block cipher, Cryptography, MACs, COVID-19

I. INTRODUCTION

Nowadays, with the wide spread of the corona virus (COVID-19) and the extremely large growth of online shopping processes, digital data communication and online bank transactions over computer networks, information content security becomes a prime concern in the whole world. Internet itself has many security threats that could be easily used to corrupt the data transferring over the network. Cryptography plays an important role for providing security for digital data transmission over such this insecure network. Cryptographic algorithms scramble data into unreadable text which can be only read or decrypted by those possesses the associated security key. Message authentication codes (MACs) are commonly used in network transactions to maintain information integrity [1]. They confirm that a message is authentic; that it really does come, in other words, from the stated sender, and hasn't undergone any changes during the transaction using digital signatures [2]. A verifier who also possesses the key can use it to identify changes to the content of the message in transaction.

Manuscript received May 25, 2020; revised November 12, 2020.
Corresponding author email: ahmed.mokhtar@bhit.bu.edu.eg.
doi:10.12720/jcm.15.12.905-912

The Substitution box (S-Box) is the unique nonlinear operation in block cipher, and it determines the cipher performance [3]. The stronger S-Box, the stronger and more secure algorithm. By selecting a strong S-Box, the nonlinearity and complexity of these algorithms increases and the overall performance is modified [4]. This change will be seen here on the Hierocrypt-3 [5] as an example of block ciphers.

The S-Box construction is a major issue from initial days in cryptology [6]-[8]. Use of Irreducible Polynomials to construct S-Boxes had already been adopted by crypto community [9].

The Hierocrypt-L1 and Hierocrypt-3 are algorithms of symmetric block ciphers that were submitted to the NESSIE project [10], [11], but were not selected. Both algorithms were among the cryptographic strategies prescribed by CRYPTREC for the Japanese government utilize in 2003 [12], however, both algorithms have been dropped to "candidate" by CRYPTREC revision in 2013. The Hierocrypt algorithms were candidate block ciphers for the NESSIE project, where Toshiba corporation started developing it from 2000 to 2002. In September 2001, Toshiba Corporation announced for the Hierocrypt-L1 specifications which was an algorithm that uses 64-bit block iterated cipher using a 128-bit cipher key [11]. In September 2001, Toshiba Corporation also announced for the Hierocrypt-3 specifications which was an iterated 128-bit block cipher algorithm that uses 6.5, 7.5, or 8.5 rounds of encryption, according to the key size 128, 192 or 256, respectively [5]. In October 2001, Toshiba Corporation announced for the Hierocrypt-3 Self Evaluation which mentioned that the Hierocrypt-3 is secured [13]. In January 2004, Rogawski published an article that mentioned that the Hierocrypt-3 is a very flexible algorithm and could be optimized for any purpose like speed, area and memory [14]. In 2016, KUROKAWA et al published an article which mentioned that related key attacks and meet-in-the-middle attacks (including biclique attacks) were evaluated on Hierocrypt-3. In their evaluations [15], no flaws that could be realistic threats were found [16].

In this article, The S-Box principle is deeply analyzed and a new S-Box is provided with its principle. the Hierocrypt-3 structure is simply illustrated and a comparative analysis of Hierocrypt-3 performance using the original and the new modified S-Boxes is provided.

The Hierocrypt-3 performance is evaluated using different modes of operations.

The rest of paper is organized as follows. Principle and deep Analysis of S-Boxes is provided in section II-1. The Hierocrypt-3 is studied and illustrated in section II-2. The modes of operations are given in section II-3. Experimental setup and procedures steps are shown in section III. Section IV provides the results and discussion. Then, the paper is concluded.

II. Theoretical Approach

A. Hierocrypt -3 Block Cipher

Hierocrypt-3 cipher is an iterated 128-bit symmetric block cipher that uses 6.5, 7.5, or 8.5 rounds of encryption, according to the key size 128, 192 or 256. The last round consists of an output transformation slightly different from the other rounds. The Hierocrypt-3 uses the nested SPN structure in the data randomizing part, and the Feistel structure in the key scheduling part to insure sufficient security against major attacks and high performance.

1) System structure

Toshiba corporation provided the algorithm construction [5] and it will be just previewed clearly. The Hierocrypt-3 encryption algorithm diagram is shown in Fig. 1. The decryption is the same blocks using the inverse functions and arrangement. The Hierocrypt-3 encryption uses 6, 7 and 8 rounds according to key sizes 128, 192 and 256 bits and one X_s block round then an Add Final key block round.

To summarize the encryption scenario, The Hierocrypt-3 encryption of T rounds consists of (T−1) iterations of round function ρ followed by the final round function Xs and the final key addition.

$$\mathrm{Enc} = \mathrm{AK}(\mathrm{K}^{(\mathrm{T}+1)\alpha}) \circ X_s(\mathrm{K}^{(\mathrm{T})}) \circ \rho(\mathrm{K}^{(\mathrm{T}+1)}) \circ \cdots \circ \rho(\mathrm{K}^{(2)}) \circ \rho(\mathrm{K}^{(1)})$$

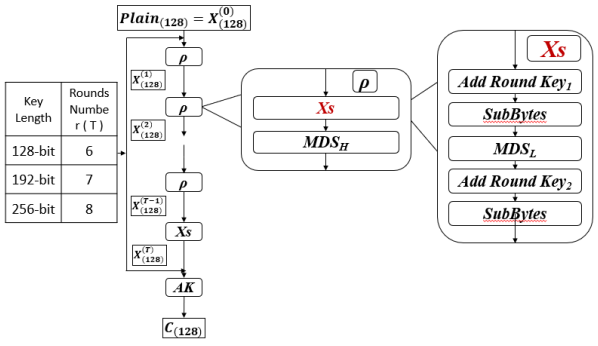

Fig. 1. Graphical representation of Hierocrypt-3 structure.

2) Key scheduling

The key scheduling part consists of an initial key expansion – Padding – KX and iterative key generations KH. As shown in Fig. 2, [17] and Table I. The KH consists of σ_0 which is the Prewhitening function that takes the original key and produce the initial intermediate key that will be used in the intermediate key generations using the σ function which consists of (T_{turn-1}) rounds and then σ^{-1} function which consists of (T_{turn}) rounds where T is the number of rounds and T_{turn} equals 4, 4, and 5 for 128, 192, and 256 key lengths, respectively as shown in Fig. 3. The round key is generated from each intermediate key [17].

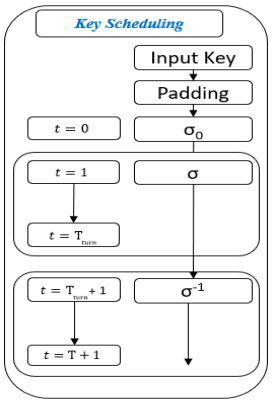

Fig. 2. Hierocrypt key scheduling.

TABLE I: Key Schedule Rounds

Key schedule for X-bit key			X=		
			128	192	256
T =			6	7	8
Round key	t	Operation	$G_{(64)}^{(t)}$		
--	−1 (PAD)	--	$H_3 \| \| H_2$		
--	0 (PW)	σ_0	$G_0(5)$	$G_0(5)$	$G_0(5)$
$K_{(256)}^{(1)}$	1	σ	$G_0(0)$	$G_0(1)$	$G_0(4)$
$K_{(256)}^{(2)}$	2	σ	$G_0(1)$	$G_0(0)$	$G_0(0)$
$K_{(256)}^{(3)}$	3	σ	$G_0(2)$	$G_0(3)$	$G_0(2)$
$K_{(256)}^{(4)}$	4	σ	$G_0(3)$	$G_0(2)$	$G_0(1)$
$K_{(256)}^{(5)}$	5	128-192: σ^{-1} / 256: σ	$G_0(3)$	$G_0(2)$	$G_0(3)$
$K_{(256)}^{(6)}$	6	σ^{-1}	$G_0(2)$	$G_0(3)$	$G_0(3)$
$K_{(256)}^{(7)}$	7	σ^{-1}	$G_0(1)$	$G_0(0)$	$G_0(1)$
$K_{(256)}^{(8)}$	8	σ^{-1}		$G_0(1)$	$G_0(2)$
$K_{(256)}^{(9)}$	9	σ^{-1}			$G_0(0)$

B. Principle and Deep Analysis of S-Boxes

In this article, The Hierocrypt-3 symmetric block cipher algorithm was studied and evaluated using different S-Boxes. The S-Box is a unique nonlinear operation in block cipher, that plays an important role in the cipher overall performance [18] as will be shown. A new S-Box with very good polynomial is provided and analyzed. The term Hierocrypt could be used in the rest of paper instead for Hierocrypt-3.

1) Algebraic system of polynomial

In this section, we will show how to represent the system of polynomial equations over finite field of characteristic two GF (2). We consider the algebraic descriptions of two S-Boxes in details. The first S-Box is the Hierocrypt original S-Box and the second is a new improved S-Box which enhanced the characteristics of Hierocrypt algorithm.

Theorem 1. [19] Let $u, v \in N, X_0, \ldots, X_u$ be variables representing the S-Box input, $S_0, \ldots, S_v$, the S-Box output. Then every S-Box can be written as a system of polynomial equations over F_2 or F_2^n for some $n \in N$ with variables X_i, S_i.

The only non-linear part of symmetric block ciphers are the S-Boxes. Let $G: GF(2)^s \rightarrow GF(2)^s$ be such an S-Box $G: x = (x_1 \ldots x_s) \rightarrow y = (y_1 \ldots y_s)$. In Rijndael AES algorithm – One of the encryption standards – and Hierocrypt-3, like for all other good block ciphers, the S-Boxes are built with good Boolean functions. There are many criteria on Boolean functions that are more or less applied in cryptography. One of them is that each y_i should have a high algebraic degree when expressed as a multivariate polynomial in the x_i. However, all this does not assure that there are no implicit multivariate equations of the form $P(x_1, \ldots, x_s, y_1, \ldots, y_s)$ that are of low algebraic degree.

2) Principle and property of hierocrypt original S-Box

The Hierocrypt uses 2 types of constant 8-bit S-Boxes: S-Box S(x) for encryption and inverse-S-Box $S^{-1}(x)$ for decryption. Also, it is used within the Hierocrypt key scheduling process.

C. Principle of Hierocrypt-3 S-Box

The substitution table (or S-Box) is invertible and is constructed by the composition of three transformations:

1. Taking multiplicative inverse $(m)^{-1}$ in GF (2^8). $(m)^{-1}$ is defined by:

$$Inv(m) = (m)^{-1} = \begin{cases} (m)^{254} & m \neq 0 \\ 0 & m = 0 \end{cases} \quad (1)$$

2. Applying an affine (over GF (2)) transformation defined by:

$$z(m) = La * Inv(m) + 07 = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} m_7 \\ m_6 \\ m_5 \\ m_4 \\ m_3 \\ m_2 \\ m_1 \\ m_0 \end{bmatrix} + \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 1 \end{bmatrix} \quad (2)$$

3. Therefore, the S-Box function - S(m) - could be calculated as:

$$S(m) = z(m) \circ Inv(m) = Z(Inv(m)) \quad (3)$$

a) Properties of Hierocrypt original S-Box

For the definitions, assume $F(x) = (f_1(x), \ldots, f_n(x))$ *from* $GF(2)^n$ *to* $GF(2)^n$ *is a multiple-output Boolean function.*

Definition 1. *The differential uniformity is denoted by* $\delta(F)$ *and is defined to be*

$$\delta(f) = \max_{\substack{\alpha \in GF(2)^n \\ \alpha \neq 1}} \max_{\beta \in GF(2)^n} |\{x | F(x) + F(x+\alpha) = \beta\}| \quad (4)$$

Using the mathematical model functions, we can obtain that Hierocrypt S-Box has $\delta(F) = 4$.

The resistance against differential cryptanalysis is measured by $\delta(F)$. It is known that the minimum of $\delta(F)$ is 1. Similarly, the Hierocrypt S-Box has $\delta(F) = 4$, so the Hierocrypt S-Box is able to resist against differential attack.

Definition 2.

Assume $\forall \alpha = (\alpha_n, \alpha_{n-1}, \ldots, \alpha_1) \in GF(2)^n, w(\alpha) = 1, if\ w(f_i(x+\alpha) + f_i(x)) = 2^{n-1}, (1 \leq i \leq n)$*, then* $F(x)$ *satisfies Strict Avalanche Criterion (SAC).*

Definition 3. *The distance to SAC is denoted by* $DSAC(F)$ *and is designed to be*

$$DSAC(F) = \left(\sum_{i=1}^{n} \sum_{\substack{\alpha \in GF(2)^n \\ w(\alpha)=1}} |w(f_i(x+\alpha) + f_i(x)) - 2^{n-1}|\right) \quad (5)$$

Obviously, $F(x)$ satisfies SAC when $DSAC(F) = 0$. The Hierocrypt S-Box does not satisfy SAC.

Using the mathematical model equations $F(x) = (f1(x), \ldots, f8(x))$, the SAC of Hierocrypt-3 S-Box can be calculated and then, we can obtain *DSAC* (Hierocrypt *S-Box*) = 464 from Definition 3.

D. Principle and Property of Hierocrypt-3 new S-Box

Performance analysis demonstrates that the improved new S-Box has following cryptographic properties: the affine transformation period is increased from 4 to the most 16, the iterative period is increased from less than 88 to the most 256, and the DSAC is reduced from 464 to 424 using Eq. 5.

This section introduces our new methodology to create a robust 16 x 16 S-box.

1) Principle of hierocrypt-3 New S-Box

The Hierocrypt-3 new (S-Box) is invertible and is constructed by the composition of three transformations:

1. Applying the affine transformation $L_{5B,5D}$, $L_{5B,5D}$ is denoted as follows:

$$X' = L_{5B,5D}(x) = 5B * x + 5D = \begin{bmatrix} 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 \end{bmatrix} \begin{bmatrix} x_7 \\ x_6 \\ x_5 \\ x_4 \\ x_3 \\ x_2 \\ x_1 \\ x_0 \end{bmatrix} + \begin{bmatrix} 0 \\ 1 \\ 0 \\ 1 \\ 1 \\ 1 \\ 0 \\ 1 \end{bmatrix} \quad (6)$$

2. Taking multiplicative inverse $(X')^{-1}$ in GF (2^8). $(m)^{-1}$ is defined by:

$$X'' = (X')^{-1} = \begin{cases} (X')^{254} & X' \neq 0 \\ 0 & X' = 0 \end{cases} \quad (7)$$

3. Applying the affine transformation again denoted as follows:

$$S(m) = \mathrm{L}_{5B,5D}(X'') = 0x5B\ X'' + 0x5D \quad (8)$$

The new S-Box is shown in Table II.

TABLE II: THE HIEROCRYPT-3 NEW S-BOX [18].

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

And the Hierocrypt-3 new inverse S-Box is shown in Table III.

TABLE III: THE HIEROCRYPT-3 NEW INVERSE S-BOX

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

2) Performance analysis of the hierocrypt-3 new S-Box

- *The differential uniformity δ(F)* = 4.
- *The distance to SAC DSAC*(*F*) = *372.*

The S-Box not only affect the encryption, decryption performance in Hierocrypt-3, but also, it affects the strength and performance of the key scheduling part as it is involved within its algorithm which ensures the whole performance of the system to be increased very much.

E. Modes of Operation

As previously mentioned, in block cipher, a block of plaintext is treated as a single unit and is encrypted as a whole to obtain a block of ciphertext with the same size, thus to enable encryption of plaintext with size which is different from the defined size of one block, we use the modes of operation [20]. For achieving this goal, NIST have defined five modes of operation of the block ciphers which were standardized as follows:

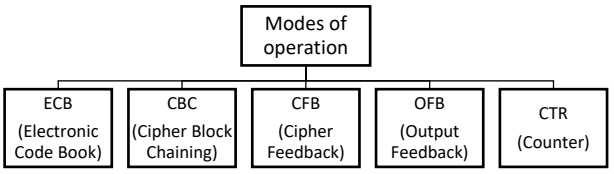

Fig. 3. Modes of operation.

Some of these modes are used in MACs directly or as a heading block with additional blocks. Some of these modes of operation may convert the block cipher into a stream cipher in order to strengthen the effect of the encryption algorithm such as CFB, OFB and CTR modes. Some of these modes have a feedback such as CBC, CFB and OFB modes and the other modes do not have a feedback such as ECB and CTR modes. In this section we will present each mode of operation in more details.

1) Electronic Code Book (ECB)

A mode of operation in which each block is encrypted separately. This is the most intuitive mode of operation and enables encryption parallelization, decryption parallelization, and random read access. It, however, is not useful for encrypting information, since while intra-block data is completely jumbled, large-scale patterns are very obvious in the ciphertext, sometimes even noticeable by the naked eye. The encryption and decryption can be calculated using the formulas in Equations 9,10 (see Fig. 4).

$$\mathrm{C}_i = \mathrm{E}_\mathrm{K}(\mathrm{P}_\mathrm{i}) \quad (9)$$

$$\mathrm{P}_i = \mathrm{D}_\mathrm{K}(\mathrm{C}_\mathrm{i}) \quad (10)$$

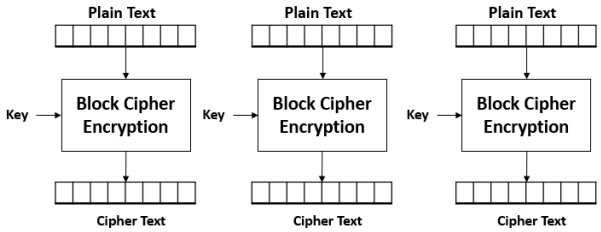

Fig. 4. Electronic Code Book Operation (ECB).

2) Cipher Block Chaining (CBC)

In order to solve the previous disadvantage of ECB mode and make each time encrypting the same plaintext block should result to a different ciphertext block, we use an initialization vector (IV) in CBC mode. The initialization vector (IV) has the same size as the block that is encrypted. Therefore, when identical plaintext blocks are encrypted, different results are obtained by using a different initialization vector (IV) for each new encryption and thus CBC mode unlike ECB mode is nondeterministic mode. The first result of ciphertext block (C_1) is used as an input instead of initialization vector (IV) to encrypt the second plaintext block (P_2) to produce (C_2) and so on. The encryption and decryption can be calculated using the formulas in Equations 11,12. (see Fig. 5).

$$C_i = E_K(P_i \oplus C_{i-1}), C_0 = IV \quad (11)$$

$$P_i = D_K(C \oplus C_{i-1}), C_0 = IV \quad (12)$$

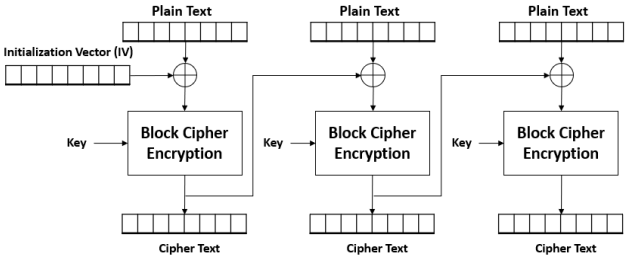

Fig. 5. Cipher Block Chaining Operation (CBC).

3) Cipher Feedback (CFB)

The CFB (Cipher Feedback) mode of operation enables the block cipher to be used as a stream cipher as mentioned previously. As well as CBC mode, CFB mode also use initialization vector (IV) to prevent identical plaintext blocks to produce identical ciphertext blocks. The difference between CFB mode and CBC mode that in CBC mode, the XOR operation is done first, then the encryption with the key is done but in CFB mode in the contrary, the encryption with the key is done first then the XOR operation is done. The encryption and decryption operations in CFB mode are the same operations, thus we can use the encryption block in both the encryption and the decryption operations of CFB mode.

The encryption and decryption can be calculated using the formulas in Equations 13, 14. (see Fig. 6).

$$C_i = E_K(C_{i-1}) \oplus P_i, C_0 = IV \quad (13)$$

$$P_i = E_K(C_{i-1}) \oplus C_i, C_0 = IV \quad (14)$$

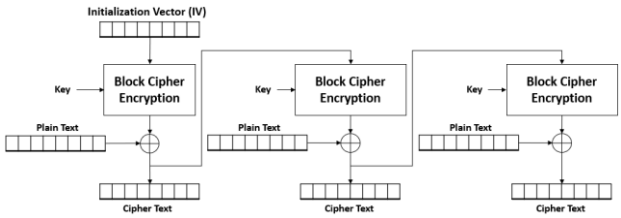

Fig. 6. Cipher Feedback Operation (CFB).

4) Output Feedback (OFB)

The OFB mode is similar in structure to that of CFB mode except that in OFB mode, the output of the encryption block is fed back to become the input for encrypting the next plaintext block, while in CFB mode, the output of the XOR operation which is the ciphertext block is fed back to become the input for encrypting the next plaintext block. Encryption and decryption are the same operations as well as CFB mode, thus we can use the encryption block in both the encryption and the decryption operations of OFB mode.

The encryption and decryption can be calculated using the formulas in Equations 15-18. (see Fig. 7).

$$C_i = P_i \oplus O_i \quad (15)$$

$$P_i = C_i \oplus O_i \quad (16)$$

$$O_i = E_k(O_{i-1}) \quad (17)$$

$$O_0 = IV \quad (18)$$

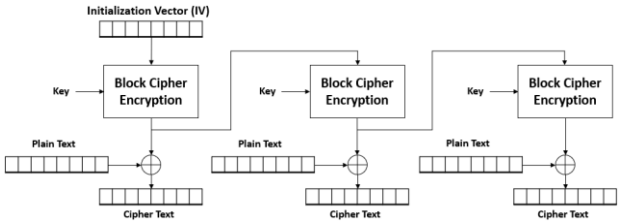

Fig. 7. Output Feedback Operation (OFB).

5) Counter (CTR)

Encryption and decryption are the same operations as CFB and OFB modes, thus we can use the encryption block in both the encryption and decryption operations of CTR mode. At CTR mode, instead of using initialization vector (IV) as the case in CBC, CFB and OFB mode, a counter is used to achieve the same purpose of using IV which is to prevent identical plaintext blocks to produce identical ciphertext blocks and thus cannot be easily detected. The counter has the same size as the encrypted block as the initialization vector (IV). The values of the counter are incremented by 1 for each block. There is no feedback in CTR mode as ECB mode. The encryption and decryption can be calculated using the formulas in Equations 19,20. (see Fig. 8).

$$C_i = E_K(C_{i-1}) \oplus P_i, C_0 = 0 \quad (19)$$

$$P_i = E_K(C_{i-1}) \oplus C_i, C_0 = 0 \quad (20)$$

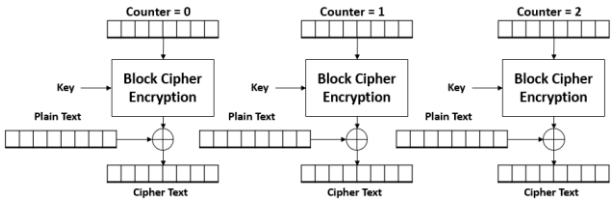

Fig. 8. Counter Operation (CTR).

III. Experimental Setup and Procedures

Fig. 9. Sample input data image.

For experimental work, a program was created that uses Hierocrypt-3 to encrypt/decrypt a message or a file of any type to measure the performance parameters of the

Hierocrypt algorithm [21], [22]. An image sample and text file sample were encrypted/decrypted using the electronic code book (ECB) mode of operation for the two algorithms as seen in Fig. 9, Fig. 10 for the image and Table III for the text.

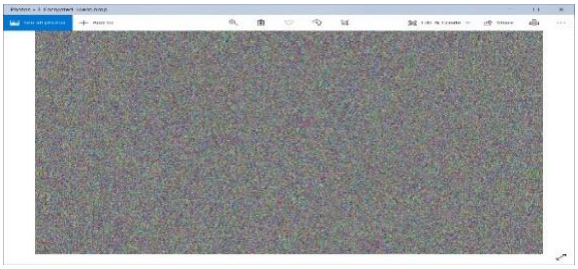

Fig. 10. Encrypted image in ECB mode using Hierocrypt-3

TABLE IV: ENCRYPTED TEXT IN ECB MODE USING HIEROCRYPT-3

Input text	This is a text massage to be encrypted by the Hierocrypt.
Ciphered text using the Hierocrypt	2A3A8796639D7B9E1814E821754527F3A93BC 6D448F17F3FE813CC3199FACF3930BA674A2 967C795FE42F166DACA9210

As seen from Fig. 10 and Table IV, the Hierocrypt scrambles data with high security level to ensure no one can understand anything from the encrypted data meaning it could be used normally as one of the encryption standards.

To identify the effect of using modes of operations, an example was made on another image Fig. 11 and encrypted using all modes of operations (see Fig. 12-16).

Fig. 11. Sample image.

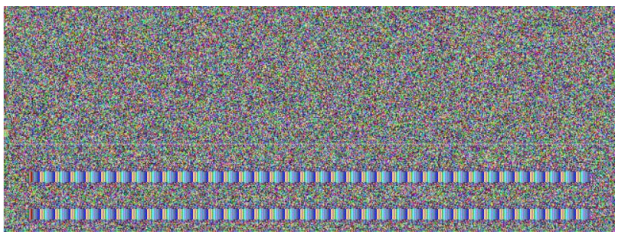

Fig. 12. Encrypted image with ECB mode

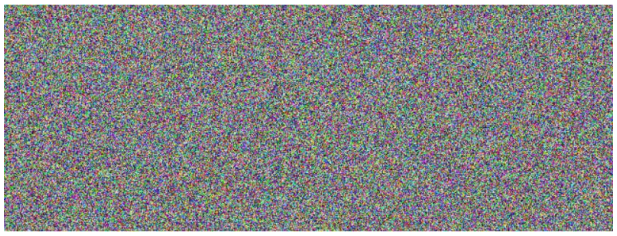

Fig. 13. Encrypted image with CBC mode.

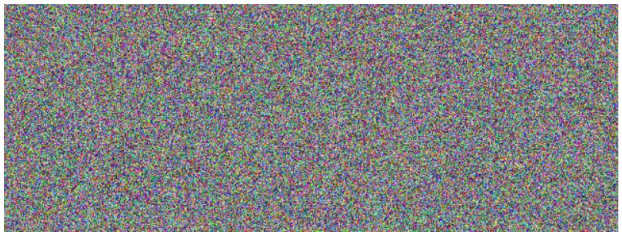

Fig. 14. Encrypted image with CFB mode.

Fig. 15. Encrypted image with OFB mode.

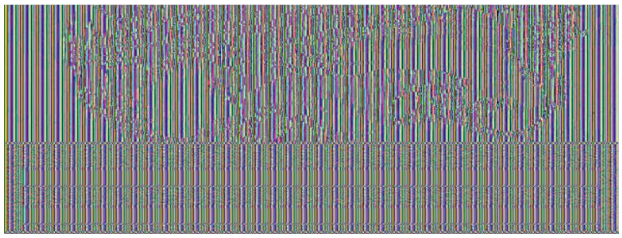

Fig. 16. Encrypted image with CTR mode.

The second process is generally to encrypt a message of any type (image, text, sound) and decrypt it by applying all modes of operation to compare the speed and performance of the Hierocrypt-3 for all modes of operations on the same machine with same parameters.

IV. RESULTS

The tests showed that the S-Box plays an important part in the performance of the block cipher and it can modify its performance to a noticeable degree. The experiments with Hierocrypt-3 original S-Box resulted in average SAC = 63.19531, giving DSAC = 0.80469, and that with the improved S-Box resulted in average SAC = 63.83594, giving DSAC = 0.16406, which is better and ensures that the Hierocrypt-3 can be enhanced by changing some of its blocks.

The performed testing indicated also the modes of operation also play an important part when the input data has similarities as noticed from the sample image in Fig. 11. The encrypted image in Fig. 12 shows that the ECB mode is so bad when the input image has similar objects and also in Fig. 16 with CTR mode. While the figures also show that the CBC, CFB, and OFB modes are very good for most situations.

The speed of encrypting/decrypting input file of different sizes are made and the results are shown in Table V which shows that the encryption is slightly slower than decryption and the time varies when using different modes of operation.

TABLE V: PERFORMANCE COMPARISON BETWEEN HIEROCRYPT SPEED PERFORMANCE USING DIFFERENT MODES OF OPERATIONS

Size	Process	ECB	CBC	CFB	OFB	CTR
100 KB	Encryption	964 ms	946 ms	933 ms	927 ms	918 ms
	Decryption	963 ms	908 ms	914 ms	913 ms	863 ms
200 KB	Encryption	1839 ms	1850 ms	1888 ms	1817 ms	1736 ms
	Decryption	1815 ms	1862 ms	1878 ms	1816 ms	1702 ms
400 KB	Encryption	3635 ms	3601 ms	3657 ms	3611 ms	3379 ms
	Decryption	3592 ms	3566 ms	3618 ms	3644 ms	3400 ms
800 KB	Encryption	7128 ms	7203 ms	7196 ms	7432 ms	6804 ms
	Decryption	7105 ms	7340 ms	7240 ms	7213 ms	6752 ms
1 MB	Encryption	9231 ms	9263 ms	9191 ms	9273 ms	8609 ms
	Decryption	9102 ms	9215 ms	9215 ms	9200 ms	8622 ms
2 MB	Encryption	18 Sec	18 Sec	18 Sec	18 Sec	17 Sec
	Decryption	18 Sec	18 Sec	18 Sec	18 Sec	16 Sec
4 MB	Encryption	36 Sec	36 Sec	36 Sec	36 Sec	34 Sec
	Decryption	36 Sec	36 Sec	36 Sec	36 Sec	34 Sec
8 MB	Encryption	73 Sec	72 Sec	72 Sec	72 Sec	68 Sec
	Decryption	72 Sec	72 Sec	72 Sec	72 Sec	68 Sec
16 MB	Encryption	149 Sec	144 Sec	145 Sec	146 Sec	144 Sec
	Decryption	143 Sec	143 Sec	154 Sec	146 Sec	149 Sec
32 MB	Encryption	310 Sec	297 Sec	303 Sec	299 Sec	282 Sec
	Decryption	295 Sec	299 Sec	310 Sec	300 Sec	286 Sec
64 MB	Encryption	614 Sec	623 Sec	585 Sec	583 Sec	546 Sec
	Decryption	622 Sec	620 Sec	584 Sec	585 Sec	547 Sec

V. CONCLUSIONS

The Hierocrypt-3 is a good block cipher. The S-Box plays an important role in the block cipher overall performance. By replacing the Hierocrypt-3 S-Box with a proposed new one, the SAC is improved and the security is increased. The modes of operation play an important part when using block ciphers to overcome the problem of resulting the same output for the same input every time which could make it so easy to attack the algorithm using look up table. The results show that the Hierocrypt-3 became more secure for specific modes of operations in MACs. Future research should be devoted to study the effect of the provided modification to the algorithm performance and security from NIST point of view.

ACKNOWLEDGMENT

We would like to express our very great appreciation to Prof. Abdelhalim Zekry for his valuable and constructive suggestions during the reviewing of the manuscript. His willingness to give his time so generously has been very much appreciated.

CONFLICT OF INTEREST

The authors declare no conflict of interest.

AUTHOR CONTRIBUTIONS

Under the supervision of Prof. Talaat El-Garf and Prof Ashraf S. Mohra and Dr Wageda I. El Sobky, Ahmed R. Mahmoud has conducted and wrote the paper; all authors had approved the final version.

REFERENCES

[1] J. Kurmi, R. S. Verma, and S. Soni, "An approach for data aggregation strategy in wireless sensor network using MAC authentication," *Advances in Computational Sciences and Technology*, vol. 10, no. 5, pp. 1037–1047, 2017.

[2] I. Afrianto, *et al.*, "E-Document autentification with digital signature for Smart City : Reference E-Document autentification with digital signature for Smart City : Reference model," no. 7, 2019.

[3] M. Mansour, W. Elsobky, A. Hasan, and W. Anis, "Appraisal of multiple AES modes behavior using traditional and enhanced substitution boxes," no. 5, pp. 530–539, 2020.

[4] Z. H. Abdelwahab, T. A. Elgarf, and A. Zekry, "Approved algorithmic security enhancement of stream cipher for advanced mobile communications," *Inf. Secur. J. A Glob. Perspect*, pp. 1–25, 2020.

[5] T. Corporation, *Specification on a Block Cipher : Hierocrypt-3*, no. 5, pp. 1–26, 2002.

[6] R. A. Alez, *Algebraic Construction of Powerful Substitution Box*, no. 6, pp. 405–409, 2020.

[7] Performance and Security Evaluation of S-Box Using Current-Pass.pdf

[8] M. S. Saeed, "An algorithm for the construction of substitution box for block ciphers based on projective general linear group," *AIP Advances*, vol. 035116, no. 2, 2017.

[9] H. M. El-Sheikh, O. A. Mohsen, T. Elgarf, and A. Zekry, *A New Approach for Designing Key-Dependent S-Box Defined over GF (2 4) in AES*, 2012.

[10] L. Granboulan, G. Martinet, M. Dichtl, P. Serf, and M. Schafheutle, NESSIE Phase I-- Selection of primitives (2001).pdf, 2001.

[11] Toshiba, "Specification on a block cipher: Hierocrypt-L1," *First Open NESSIE Work.*, no. 9, pp. 1–26, 2000.

[12] CRYPTREC | About CRYPTREC. [Online]. Available: https://www.cryptrec.go.jp/en/about.html

[13] Toshiba Corporation, *Self Evaluation : Hierocrypt – 3*, pp. 1–16, 2000.

[14] M. Rogawski, "Analysis of hardware implementation of HIEROCRYPT-3 algorithm (and its comparison with CAMELLIA algorithm) using ALTERA devices," *Biul. Wojsk. Akad. Tech.*, vol. 53, no. June, pp. 87–112, 2004.

[15] T. Kurokawa, S. Kanamori, R. Nojima, M. Ohkubo, and S. Moriai, "7-3 CRYPTREC activities and a revision of the e-government recommended ciphers list," *J. Natl. Inst. Inf. Commun. Technol.*, vol. 63, no. 2, pp. 203–214, 2016.

[16] A. Abdelkhalek, R. AlTawy, M. Tolba, and A. M. Youssef, "Meet-in-the-middle attacks on reduced-round hierocrypt-3," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2015, vol. 9230, pp. 187–203.

[17] K. Ohkuma, H. Muratani, F. Sano, and S. Kawamura, "The block cipher Hierocrypt," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 2012, pp. 72–88, 2001.

[18] J. Cui, L. Huang, H. Zhong, C. Chang, and W. Yang, "An improved AES S-box and its performance analysis," *Int. J. Innov. Comput. Inf. Control*, vol. 7, no. 5 A, pp. 2291–2302, 2011.

[19] R. Weinmann, "Evaluating algebraic attacks on the AES," *Diplom thesis, Tech.…*, 2003, [Online]. Available: http://wwwold.cdc.informatik.tudarmstadt.de/reports/reports/Ralf-Philipp_Weinmann.diplom.pdf.

[20] V. H. Krishna, A. Rama, and N. Deepa, "A secure file storage in cloud computing using hybrid cryptography," *Test Eng. Manag.*, vol. 82, no. April, pp. 10469–10474, 2020.

[21] M. Annaqeeba, H. M. El-Sheikhb, T. A. Elgarf, and A. Zekry, Software Implementation of Advanced Encryption Standard Algorithm on Android and Windows Phone Platforms Software Implementation of Advanced Encryption Standard Algorithm on Android and Windows Phone Platforms, no. 7, 2014.

[22] H. M. El-Sheikh, O. A. Mohsen, T. Elgarf, and A. Zekry, *Efficient Hard ware Implementation Technique for Key-Dependent s-box Defined over GF (2^4) in AES*, 2011.

Ahmed Ragab Mokhtar was born in Egypt in 1993. He received the B.Sc. degree in communications and computers from benha faculty of engineering in 2016. He is currently a demonstrator at Benha Faculty of Engineering, Benha University, Egypt.

Wageda Ibrahim El Sobky was born in Egypt in 1981. She received the B.Sc. degree in communications and computers from benha faculty of engineering in 2003. She received the B.Sc. degree in science from benha faculty of science in 2008. She received the M.Sc. in applied mathematics from Benha University, Cairo, Egypt, in 2012 and the Ph.D. degree in cryptography from Ain Shams University, Cairo, Egypt, in 2017. She is currently a doctor in basic engineering sciences, at Benha Faculty of Engineering, Benha University, Egypt. Her current research interests include data security, and cryptography.

Ashraf Shouki Seliem Mohra was born in Egypt in 1963. He received the B.Sc. degree in Electronics and communications from Shoubra faculty of engineering in 1986. He received the M.Sc. and Ph.D. degree in Electronics and communications from Ain Shams University, Cairo, Egypt, in 1994 and 2000, respectively. He is currently professor of Electrical Engineering, at Benha Faculty of Engineering, Benha University, Egypt. His current research interests include microstrip antennas, filters, couplers, Hybrid junctions, computer aided design of planar and uniplanar of MIC's and MMIC's, Non-destructive techniques, Metamaterials and defected ground struct.

Talaat Abd El Latif El Garf was born in Egypt in 1953. He received the B.Sc. degree in Electrical Engineering (Communications), from the Military Technical College, Cairo, Egypt, 1976. He received the M.Sc. and Ph.D. degree in Communications and from Ain Shams University, Cairo, Egypt, in 1990 and 1993, respectively. He is currently professor of Communications Engineering, at HTI (Higher Technological Institute) Since 2005, Egypt. His current research interests include data security, communications filters.