I. J. Computer Network and Information Security, **2017, 4, 29-36**
Published Online April 2017 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2017.04.04

New Symmetric Cipher Fast Algorithm of Revertible Operations' Queen (FAROQ) Cipher

Instructor Omar A. Dawood
English Department, College of Education for Humanities, Anbar University
E-mail: The_lionofclub@yahoo.com

Prof. Abdul Monem S. Rahma
Computer Science Department, University of Technology-Baghdad, Iraq
E-mail: Monem.rahma@yahoo.com

Assist. Prof Abdul Mohssen J. Abdul Hossen
Computer Science Department, University of Technology-Baghdad, Iraq
E-mail: Abdulmoohsen53@yahoo.com

Abstract—In this paper, we have proposed a new iterated symmetric cipher, which is designed with Substitution and Permutation Network (SPN) structure and depends on strong mathematical built. It uses a compact algorithm for encryption and decryption processes, which consists of four main stages that roughly similar in its work to the Advance Encryption Standard (AES) stages. Starting by the SubByte operation, ReversibleShiftrows operation, ReversibleMixcolumns operation, and Round key addition. The proposed operations in this cipher have implemented in a straightforward manner relatively in both Encryption/Decryption by an elegant way. These four stages designed to reduce the hardware requirements and to produces high efficiency, which keeps the encryption and decryption process at the same speed in the hardware devices and eliminates the difference of execution times as well as creates a balance in forward and backward operations. The proposed cipher interested with modern design by adopted new algebraic operations and clear mathematical notations to ensure a high level of security. The proposed cipher did not build suddenly or arbitrarily but it acts as a sequence of developments and represents as a long process of design for long time, since several proposed ciphers have been published recently by us that paved the way to its new design, so the designed cipher inherited a good properties from a proven famous algorithms' features to produce high resistance against all known attacks and to submit a high performance on many platforms and in a wide range of hardware and software applications.

Index Terms—Block Cipher, Symmetric Cipher, Advance Encryption Standard (AES), Substitution and Permutation Network (SPN), Feistel Structure (FS).

I. INTRODUCTION

The modern techniques for the design of symmetric cipher basically rely on the mathematical and practical aspects and encourage on flexible style and intractable manner with robust structure by selection effective factors of cryptographic primitives for the algorithm built [1]. The National Institute of Standards and Technology (NIST) invited the cryptographers, cryptanalysts academic researchers and data security specialists all over the world to apply their own algorithms in order to select one to be a good alternative for the Data Encryption Standard (DES) and triple-DES, because the DES cipher suffered from many problems, represented by short key that not withstand the advance technology through non-resistance against brute force attacks, and the Triple-DES suffered from slowness with three ciphering key [2]. Many ciphers were originally submitted by designers from several countries. Fifteen algorithms were selected as initial selection, then after deep study and hard analysis processes reduced to the best five algorithms as a finalist candidate in the second selection [3]. The five algorithms were MARS, RC6, RIJNDAEL, SERPENT and TWOFISH which are considered non-superior at all. On October 2nd 2000, NIST announced that the Rijndael algorithm is the best one that has got the higher voting scores. The Rijndael cipher appears to be a very good in both hardware and software implementation through a wide range of platforms [4]. Our proposed model called FAROQ cipher similar in its work to the Rijndael cipher from several aspects and can be pictured as a byte-oriented structure that iterated for a number of stable rounds. So the first stage is a Subbyte operation that designed by applying another irreducible equation and a new affine transformation that was chosen from the best selection of what we have gotten. They have been given acceptable results in randomness and non-linearity. The second stage is a ReversibleShiftRow that is based on the same rotate operations in forward and backward operations. The third stage is a ReversibleMixcolumn operation is also based on adoption new linear equation with Maximum Distance Separable (MDS) notation that has self-inverse, which uses a single 4*4 MDS matrix over GF(2^8)[5]. The ReversibleMixcolumns considers a

prominent change in polynomial matrices' nature and one of the two main diffusion resource in the algorithm. This means the same linear equation used in a forward and backward operation that has self-reversible inverse with involution characteristics. The fourth stage represents the Round key addition or what is known by the key addition operation that is based on some sophisticated operations and it uses an extra bit-wise shift and rotates operations. The purpose behind the idea of reversible operation is to design a fast algorithm of involution structure in most of its stages that can be implemented in restricted space environments and to be work with small amount of RAM and an accepted amount of ROM as well as support fast key setup. The proposed cipher designed with some flexibility in terms of block and key sizes which accommodates alterations in the number of rounds and balanced of round structure with instruction parallelism. Our submitted paper is organized as follows: Section II. Describes the main characteristics and the types of algorithms' structures for the modern block cipher. Section III. Explains the whitening and tweaking comprehensions. Section IV. Explicates the general structure diagram of the proposed algorithm and the main security layers. Section V. Attempts to show the rational design for the proposed cipher with basic criteria of construction steps. Section VI. Provides an overview of the important applications of the proposed algorithm. Section VII. Highlight the essential points of the analysis and the experimental results that have acquired, and we conclude in Section VIII.

II. Block Cipher Design

The design scheme for any symmetric cipher based mainly on the type of structure design that different from one algorithm to another, so there are several of compact structure which adopted in numerous famous ciphers. These structures determine the general form of the work of the algorithm and can be reviewing here rapidly.

A. Substitution-Permutation Network (SPN) Structure

Substitution-Permutation Network, represent a series of mathematical operations that use substitutions clue also called (S-Box) and permutations which are called (P-Boxes) and it represents a special type of an iterated ciphers that have a more uniform round transformation [6]. The combining of these two primitives represents a special form of product ciphers where S-boxes provide confusion of input bits and P-boxes provides diffusion across P-box inputs. SPN acts as an iterated structure designed for modern product cipher. The key scheduling in this structure expanded normally into round keys that will be XOR'ed at the beginning of each round. The Rijndael and Serpent ciphers represent a good example of the SPN structure [7].

B. Feistel Cipher Structure

The Feistel structure is the most popular constructions and the oldest structure that was used in the Lucifer cipher and designed by Horst Feistel of IBM Company and later it was used in DES cipher. Feistel structure uses F-Function that accept half a block and subkeys as an input then depends on the block size which process as a two halves of data [8]. The same algorithm of Feistel structure used for encryption and decryption, so it is a suitable structure for the implementation with low cost of hardware. The SubKey algorithm implemented with reversed order for decryption this mean K1 is the last round and Kn in the first round and Kn-1 in the second round and so on. A typical number of Feistel round is 16 rounds for each round uses the SubKey generation algorithm that makes the algorithm more resistance to cryptanalysis. DES, RC6, MARS, Twofish are good ciphers for the Feistel structure [9].

C. Unbalanced Feistel Network

This type of structure similar to the traditional Feistel networks but it consists of a series of rounds in which one part of the block operates on the rest of the block. The UFN has two parts which no need to be of equal size. The main difference between traditional or conventional Feistel and the Unbalanced Feistel cipher is the last uses modified structure where L_0 and R_0 are not of equal lengths. The Skipjack encryption algorithm is a good example of such structure [10].

D. Generalized Unbalanced Feistel Network

Schneier and Kelsey generalized the concept of UFN by dispense with the two blocks to be combined by XOR operation. For a Generalized Unbalanced Feistel Network (GUFN) it is enough that one part of the input block controls another part of the input block, in which all bits of the internal state of the round are used in the round transformation, therefore the cipher is called complete, from another perspective if the bits are left invariant by the round transformation, the cipher is called incomplete. The advantages of this structure is allow a parallel computations of n-bits for encryption and it can provide provable security against the traditional differential and linear cryptanalysis [11].

E. Involution Structure

An involution block cipher is a block cipher with operations of involutional properties which has the forward process is the same as the backward process that means the same algorithm used for encryption and decryption. The involution structure characterized by reduced cost of hardware and good software implementation, in addition, to providing the same level of security since it uses the same digital circuit in ciphering and deciphering.

The only difference between the encryption and decryption processes in these ciphers is the reverse key-scheduling that performed in reverse order. The Feistel and SPN structure sometimes in certain ciphers considered as an involution ciphers. Anubis, KHAZAD and BSPN ciphers designed with involution structure [12].

III. Whitening and Tweaking

Whitening it is the technique of bit-wise XORing between the cipher key and the text before the first round and after the last round. It is proven that whitening routine substantially increases the difficulty of key search and increases the difficulty of attacking the cipher, by obscuring from an attacker specific inputs to the first and last rounds. The same whitening key is used for each block makes the brute-force search for the key much more time-consuming [13]. In recent years a new comprehension has emerged about the block cipher design which is known by a Tweakable Block Cipher (TBC) that was first introduced by Liskov, Rivest, and Wagner [14]. The TBC concept on opposite to the traditional block cipher that consists of just two inputs of cleartext and cipher key. The CBT contains an additional input called the tweak that controls the main operations of the round transformation along the key. The tweak purpose is to apply variability which provides flexibility in applications but not security [15].

IV. FAROQ Structural Features and Characteristics

The proposed cipher interests with the coherent internal structure which provides a new method to integrate the forward and backward operations into a full systematic crypto-cipher. This method assists the structure with reduced hardware resources and removes the vulnerability threat against the timing attack. The proposed architecture imposed to be suitable for critical applications, such as smartcard, personal digital assistant (PDA), and mobile phone, etc., among those difficult challenges the urgent need for lightweight block cipher become a demand and plays a vital role as a cornerstone for contemporary security applications. FAROQ cipher consists of three elementary layers: confusion layer, diffusion layer, and key addition layer. The confusion layer: A substitution of the bytes by means of a nonlinear transformation. The diffusion layer: Every byte is replaced by a linear combination of the bytes within the same column. The round key addition layer: The bytes are XORed with an n-bit round key.

FAROQ cipher supports the input plaintext block of 128-bit that represents as a state array of a square matrix 4*4 dimensions while it uses three variable secret keys of 128-bit, 192-bit, and 256-bit and with three limited rounds 10, 12, and 14 respectively. The main structure of the proposed cipher with ten rounds can be shown in Fig 1. One of the main points of the algorithm strength is the key length. Whenever the cipher key is big the resistance against the effective attacks will be difficult to exploit the byte-oriented structure and it will be extremely high, such as a square attack that deduces the key information with small size or with reduced number of rounds. So the proposed cipher followed the policy of utilizing the same key length of the AES cipher with three options according to the work sensitivity.

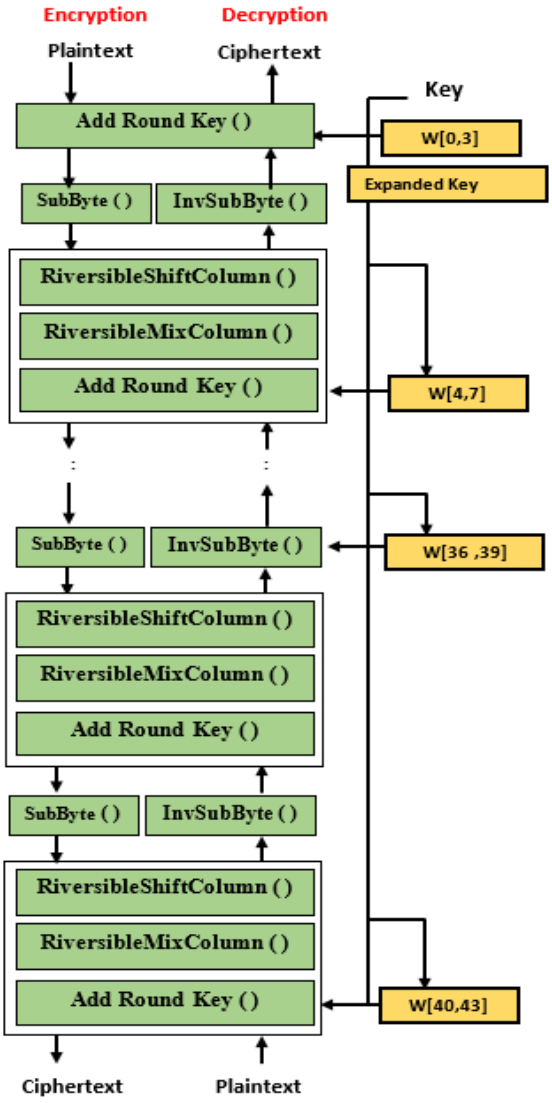

Fig.1. FAROQ Structure

V. The Design Framework

Our new design seeks to explain the positive aspects from the construction of a graceful algorithm that involves combining some operations in the main stages to provide a good structure. The new structure has to support a high speed and low cost hardware as well as applied a trusted cipher. The block size in any algorithm should be acceptable so as neither to be very big nor too small size. The designer should avoided the small block size because ciphertext will be subject to the dictionary attacks, since the large block has more resistant against the attacks. From other prospective with very big block size the algorithm will not work well and it will need to some padding operations. The suitable choice for the reasonable block size is multiple of a byte (8-bits) that can be implemented on most processors and devices easily. The proposed cipher expected to be capable of safeguarding against all known attacks, In the design of this cipher, we have taken into account the fact that the cipher must be feasible to implement perfectly in such a

way that it provides conservativeness design. This cipher designed according to several important criteria:

- High margin of security
- Design simplicity and ease of implementation
- Resistance against all known attacks
- Transparent and conservative structure
- Suitability for secure implementations
- Symmetry in the round transformation

A. *SubBytes Transformations*

SubBytes: This is the first stage in the algorithm for data substitution process in the FAROQ cipher where each small block is replaced by its substitution in S-Box table with other block of output. The S-box is a table-driven non-linear substitution operation that used in most block ciphers and can be created either randomly or mathematically, so it can be defined as a square matrix 16*16, which contains permutation of all possible 256 values. The proposed S-Box is a mapping of one to one relationship with 8-bit values that constructed by selected another irreducible polynomial $x^8 + x^5 + x^3 + x + 1$ and other affine equation as shown below matrix. The construction of the forward S-Box essentially depends on three steps, the first step is by taking the multiplicative inverse of all tables' values then applying the affine transform and the result XORred with the constant vector represented by the value (87) as it shown in the equation (1).

$$\begin{bmatrix} b'_0 \\ b'_1 \\ b'_2 \\ b'_3 \\ b'_4 \\ b'_5 \\ b'_6 \\ b'_7 \end{bmatrix} = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \\ b_6 \\ b_7 \end{bmatrix} \oplus \begin{bmatrix} 1 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \end{bmatrix} \quad (1)$$

Table 1. Forward S-Box

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

B. *InvSubyte Transformations*

The inverse of the proposed S-box is constructed by applying the inverse of the affine transformation followed by applying the multiplicative inverse in GF(2^8) and the result XORed with constant vector (3C). As shown in the equation (2).

$$\begin{bmatrix} b'_0 \\ b'_1 \\ b'_2 \\ b'_3 \\ b'_4 \\ b'_5 \\ b'_6 \\ b'_7 \end{bmatrix} = \begin{bmatrix} 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \\ b_6 \\ b_7 \end{bmatrix} \oplus \begin{bmatrix} 0 \\ 0 \\ 1 \\ 1 \\ 1 \\ 1 \\ 0 \\ 0 \end{bmatrix} \quad (2)$$

Table 2. Backward S-Box

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

C. *RevisibleShiftRows Transformations*

The main purpose of the step RevisibleShiftRows is to spread the bytes of each input column to different output columns. This phase is a linear diffusion process that works on a singular row and each row of the array is rotated by a certain number of byte positions. The first row (row 0) is not shifted, and the remaining rows proceed as follows 2nd, 3rd and 4th rows 2-bytecircular left shift is performed, see Fig 2. For decryption, the corresponding steps of shifting process repeated again, the same replacement rows is exactly implemented with the same direction without any change. This is a good method to obtain an optimal diffusion and high fast implementation in addition to gain resistance against truncated differential attacks and saturation attacks. This stage inspired from the Tigris cipher with the same shifting steps, see ref [16].

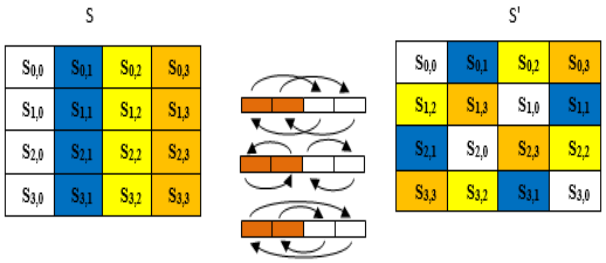

Fig.2. RevisibleShiftRows

D. *RevisibleMixColumns Transformations*

This stage includes shifting left and xoring of bits operation with themselves. These operations provide both confusion and diffusion particularity and mixing operations from various algebra. The mixcolumn transformation is based on multiplication of the state array with a certain matrix of Maximum Distance Separable (MDS). The MDS matrices are useful building blocks for ciphers because they guarantee a certain degree of diffusion and they are derived from the property that multiplication of a polynomial with a fixed polynomial over GF(2^8) results in a constant matrix multiplication. If one of the input elements is changed, all the output elements must change, as it defined in equation (3).

$$a(x) = \{05\}\, x^3 + \{06\}\, x^2 + \{05\}\, x + \{07\} \qquad (3)$$

This equation written as a matrix multiplication where the matrix is a circular matrix with the first row equal to a0; a3; a2; a1, each subsequent row is obtained by a circular shift of the previous one by 1 position to the left. This polynomial is coprime to ($x^4 + 1$). Therefore, the transformation is invertible. This formula can be addressed under the shape of a matrix multiplication that is for all the 4 columns in the state matrix. The results of this multiplication are 4 bytes in the column, the matrix multiplication of s'(x) as follows.

$$\begin{bmatrix} S'_{0,c} \\ S'_{1,c} \\ S'_{2,c} \\ S'_{3,c} \end{bmatrix} \otimes \begin{bmatrix} 07 & 05 & 06 & 05 \\ 05 & 07 & 05 & 06 \\ 06 & 05 & 07 & 05 \\ 05 & 06 & 05 & 07 \end{bmatrix} = \begin{bmatrix} S_{0,c} \\ S_{1,c} \\ S_{2,c} \\ S_{3,c} \end{bmatrix} \otimes \begin{bmatrix} 07 & 05 & 06 & 05 \\ 05 & 07 & 05 & 06 \\ 06 & 05 & 07 & 05 \\ 05 & 06 & 05 & 07 \end{bmatrix} = \begin{bmatrix} S'_{0,c} \\ S'_{1,c} \\ S'_{2,c} \\ S'_{3,c} \end{bmatrix}$$

for $0 \le c < Nb$ where $Nb = 4$ no of bytes

As a result of this multiplication, the four bytes in a column are multiplied by the same matrix, in forward and backward, since the multiplying this matrix by itself give the identity matrix, this proved with a reducible polynomial of ($x^4 + 1$) over GF(2^8), as stated below.

$$a(x) = b(x) \bmod (x^4 + 1)$$

$$\begin{bmatrix} 07 & 05 & 06 & 05 \\ 05 & 07 & 05 & 06 \\ 06 & 05 & 07 & 05 \\ 05 & 06 & 05 & 07 \end{bmatrix} \times \begin{bmatrix} 07 & 05 & 06 & 05 \\ 05 & 07 & 05 & 06 \\ 06 & 05 & 07 & 05 \\ 05 & 06 & 05 & 07 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

E. *FAROQ Add Round Key Transformation*

The key addition is denoted by AddRoundKey. In this transformation the 128-bits of state matrix are bitwise XORed with 128-bit of the round key. The process is saw as a column by column between the 4 bytes of a state column and 4-bytes of round key column. The AddRoundKey transformation being as simple as possible and affects every bit of the state. There is no need to explain the inverse of AddRoundKey transformation because the forward of ciphering key transformation is identical to the inverse operation since the XOR operation has its own inverse.

F. *FAROQ Key Expansion*

Ciphering key represents the heart of encryption and decryption operations that must be kept secret which effects to the whole algorithm. The Rijndael cipher receive the initial cipher key K and executes a key expansion routine to generate a key schedule. The key expansion process determines in which method the expanded key is generated from the cipher key because the cipher model requires one round key for the initial key (primary key) to be XORed with the state array and one for each round which is known by subkeys and the operation called the key scheduling. The key expansion technique has been modified to be possible to execute the key schedule using a small amount of working memory and with high key agility feature. The expansion technique is the same that one adopted in Euphrates cipher, as shown in Fig 3. See ref [17] that achieved with two constants vectors represented by base natural logarithm and golden ratio, in order to eliminate any symmetries, prevent any weak keys through the progressive generation process of subkeys and to give an efficient diffusion for cipher key layer through the expansion process. The first use of these two constant vectors in the RC6 cipher's key expansion [18] and then adopted in the proposing of developed new variant AES paper [19] that published by us.

Note

Pw = base natural logarithm (b7e15163),
Qw = golden ratio (9e377969)
>>8 bit =right rotate over the vector

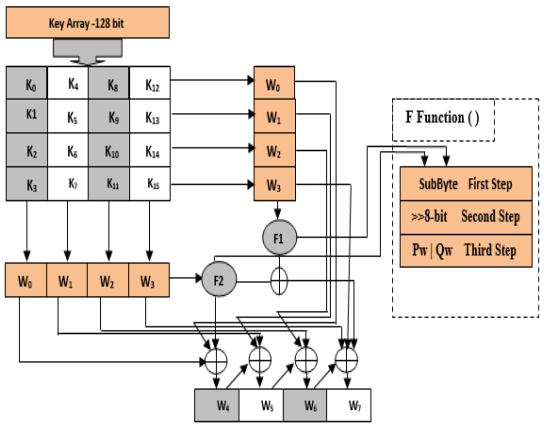

Fig.3. FAROQ Key Expansion

G. FAROQ (F) Function

The function (F) forms the backbone for the SubKey generator. It is a complex function that is responsible for the key expansion, the terms F1 and F2 are work with the same manner and with the same three steps but the main difference between them, the (F1) manipulate the state matrix row by row and uses the base natural logarithm as a constant vector whether (F2) manipulate the state matrix column by column and uses the golden ratio as a constant vector. So the third step is performed as XORed vector with the previous vector. So, we will define the function (F) in more detail, it consists of three sub-functions through which each byte is run with its own key-dependent S-box. Each S-box is an 8-bit permutation: it takes eight bits of input and produces eight bits of output. The second sub function applied 8-bit right rotate over the vector and the third sub-function includes two constant vectors (base natural logarithm and golden ratio) that XORed with the previous result of the second sub-function. The key generator of our cipher can work efficiently in environments that need fast key change and can be built in a few gates of hardware that supported complex round function. The usage of two constant vectors are to derive the key information and through which eliminate weak keys and add a substantial resistance against related-key attacks as well as increase the computational complexity.

VI. Applications of The Proposed Model

The proposed cipher can be utilized in several areas, so the entire algorithm can be implemented completely using byte operation routine and the submitted cipher can be applied efficiently for the following applications:

- FAROQ cipher considers a good choice for the securing in E-commerce.
- It can be used in smart phone applications and handheld devices.
- It is sufficient cipher to apply in secured E-mails system Pretty Good Privacy (PGP).
- It provides secure financial transactions among banks Automata Teller Machine (ATM).
- The proposed model is inexpensive in software/hardware implementation so, it may be built with a few amount of resources.
- The proposed algorithm can be implemented to online ciphering of high speed-networking protocols like Fiber Distributed Data Interface (FDDI).
- Flexible design: e.g., accept additional key lengths; can be implemented on a wide variety of platforms and applications, it is suitable for a stream cipher, hash function, and MAC.
- Can be used to protect the E-Voting and online examinations from malicious activities.
- The elegant structure for the algorithm make it a multi-use model for several of light and heavy applications.
- FAROQ cipher acts a good solution for the sensor network applications.
- It's a convenient choice for the trusted of network access control.
- FAROQ algorithm is applicable on Wi-Fi and WiMAX techniques.

VII. Analysis and Experimental Results

FAROQ cipher is a new cipher design which supports key expansion unit with simple design and high complexity that performed efficiently in applications with low covered area resources that has the ability to change keys quickly and with a minimum of resources (high key agility). This cipher uses an innovative paradigm, in the form of key-dependent S-boxes that creates an unusual dependency between the security of the algorithm and the structure of the key schedule that makes the known attacks very hard. We have proposed a more efficient combination of ReversibleShiftrows and ReversibleMixColumn operations that uses in the same manner in forward and backward, in order to use less resource than separated block implementations. This cipher ensures high performance with applications that require frequent change of the key relatively with high parallelism of computations to ensure fast encryption speed. The proposed cipher is tested using several statistical tests; the results of these tests do not indicate any deviation from random behavior. These tests are so important and necessary but not adequate for security needs. Simple comparison in encryption speed in Ms between the proposed cipher and the standard AES cipher can be shown in Table 1.

Table 1. Comparison Speed between FAROQ Cipher and the Original AES

Algorithms	No. of Rounds	Block Size	Number of Byte	Time of Encryption
Rijndael Cipher	10-Rounds	128-bit	1000	0.68
			10000	0.76
			100000	1.19
FAROQ Cipher	10-Rounds	128-bit	100	0.49
			10000	0.69
			100000	1.10

We have tested the algorithm's implementation several times and select the best results with taken in to consideration the uncontrollable parameters and the deviation of statistical analysis with 16 bytes per block, see Table 2. The algorithm measured under Windows 10 Pro 32-bit, Intel (R) Core i7 Tm, with HD graphics 5500 NVIDIA GEFORCE 820m.

Table 2. FAROQ Performance of Different Key Implementations

Key Length	Language	Processor	Code Size	Clocks to Key	Clock to Encrypts
128-Bit	Assembly	Intel-Core i7	8950	10800	12850
192-Bit	Assembly	Intel-Core i7	8950	12250	14730
256-Bit	Assembly	Intel-Core i7	8950	13500	15690

FAROQ cipher provides both cipher execution and key setup/key change very fast with flexible design, timing and power analysis attacks have been taken into account. Our cipher mainly designed to be convenient with non-sacrifice of hardware resources and to be work with sufficient throughput. The S-Box is designed with restricting linear correlations between the plaintext and ciphertext bits so as to thwart linear cryptanalysis; this design is reasonable and provides an acceptable degree of confusion. FAROQ cipher interest with the high degree of balancing that makes the power analysis attack impossible for exploiting the difference in internal implementation of instructions.

VIII. Conclusions

We are introduced a new cipher design that can be implemented efficiently on smartcard processors and applications that require a small amount of RAM and ROM and gate count, especially in embedded systems. Number of modern design considerations have been done through designing of this cipher. This cipher focuses on the most important issues that have adopted in the design of most standard ciphers which include computational complexity and the hardware implementation in addition to the performance that effects on the cost and power consumption. FAROQ cipher can be considered as a lightweight cipher with a high margin security and highly processing rate to fully utilizing the affordable network bandwidth. The developed model designed to defeat the real security threats and to satisfy the current and the perspective of future requirements.

Acknowledgment

The authors would like to apply special thanks and grateful to those kind people in Computer Science Department-University of Technology for their support and help. The authors also would like to extend special thanks to Dr. Rafi Hussen for his great contribution in editing and proof reading this paper from a linguistic point of view.

References

[1] Christof Paar Jan Pelzl, "Understanding Cryptography" A Textbook for Students and Practitioners© Springer-Verlag Berlin Heidelberg 2010.

[2] Sourabh Chandra and Siddhartha et al, "A Study and Analysis on Symmetric Cryptography", International Conference on Science, Engineering and Management Research (ICSEMR 2014), 978-1-4799-7613-3/14/$31.00 ©2014 IEEE.

[3] Olivier Baudron et al, "Report on the AES Candidates", Second AES Candidate Conference (AES2), Rome, Italy, March 22, 1999.

[4] Cetin Kaya Koc, "Cryptographic Engineering", Library of Congress Control Number: 2008935379, © Springer Science + Business Media, LLC 2009.

[5] Svenja Huntemann, "The upper bound of general Maximum Distance Separable codes", University of New Brunswick Saint John, Faculty of Science, Applied Science, and Engineering, Math 4200: Honours Project, May 28, 2012.

[6] Bac Do Thi, Minh Nguyen Hieu and Duy Ho Ngoc, "An Effective and Secure Cipher Based on SDDO", DOI: 10.5815/ijcnis.2012.11.01, I. J. Computer Network and Information Security, 2012, 11, 1-10.

[7] Nicolas Sklavos and Xinmiao Zhang," Wireless Security and Cryptography Specifications and Implementations", © 2007 by Taylor & Francis Group, LLC.

[8] Thomas W. Cusick and Pantelimon Stanica, "Cryptographic Boolean Functions and Applications", Copyright © 2009 Elsevier Inc. All rights reserved.

[9] Boris Ryabko and Andrey Fionov, "BASICS OF C O N T E M P O R A R Y CRYPTOGRAPHY FOR IT PRACTITIONERS", Series on Coding Theory and Cryptology - Vol. 1, Copyright Q 2005 by World Scientific Publishing Co. Re. Ltd.

[10] Andrey Bogdanov, "On unbalanced Feistel networks with contracting MDS diffusion", DOI 10.1007/s10623-010-9462-0, Des. Codes Cryptogr. (2011) 59:35–58.

[11] Jiali Choy Guanhan Chew Khoongming Khoo and Huihui Yap, "Cryptographic properties and application of a Generalized Unbalanced Feistel Network structure", DOI 10.1007/s12095-011-0042-6, Cryptogr. Commun. (2011) 3:141–164.

[12] Xueying Zhang, H. M. Heys and Cheng Li, "FPGA Implementation and Energy Cost Analysis of Two Light-Weight Involutional Block Ciphers Targeted to Wireless Sensor Networks, DOI 10.1007/s11036-012-0353-7, © Springer Science+Business Media, LLC 2012

[13] Debra L. Cook Moti Yung Angelos D. Keromytis, "Elastic block ciphers: method, security and instantiations", Int. J. Inf. Secur. (2009) 8:211–231 DOI 10.1007/s10207-008-0075-9, © Springer-Verlag 2008.

[14] M. Liskov, R. L. Rivest, and D.Wagner, "Tweakable block ciphers," in Proc. CRYPTO (Lecture Notes in Computer Science), M. Yung, Ed. Berlin, Germany: Springer-Verlag, 2002, vol. 2442, pp. 31–46.

[15] Palash Sarkar, "Tweakable enciphering schemes using only the encryption function of a block cipher", Information Processing Letters 111 (2011) 945–955, © 2011 Elsevier B.V.

[16] Omar A. Dawood, Abdul Monem S. Rahma and Abdul Mohsen J. Abdul Hossen, "The New Block Cipher Design (Tigris Cipher)", I.J.Computer Network and Information Security (IJCNIS), Published Online November 2015 in MECS (http://www.mecs-press.org/) DOI: 10.5815/ijcnis.2015.12.02.

[17] Omar A. Dawood, Abdul Monem S. Rahma and Abdul Mohsen J. Abdul Hossen, "The Euphrates Cipher", IJCSI International Journal of Computer Science Issues, Volume 12, Issue 2, March 2015, ISSN (Print): 1694-0814 | ISSN (Online): 1694-0784.

[18] Ronald L. Rivest1, M.J.B. Robshaw and Yiqun Lisa Yin, "The Security of the RC6TM Block Cipher", RSA Laboratories Version 1.0, August 20, 1998.

[19] Ali M. Sagheer, Salah S. Al-Rawi, and Omar A. Dawood, "Proposing of Developed Advanced in Encryption Standard AES", IEEE Computer Society DOI 10.1109/DESE, Page No. 197, 2011, The Fourth International Conference in Developments in E System Engineering DESE, Dubai, 2011.

Authors' Profiles

Omar Abdulrahman Dawood was born in Habanyah, Anbar, Iraq (1986), now he lives in Ramadi, Anbar. He obtained B.Sc. (2008), M.Sc. (2011) in Computer Science from the College of Computer, Anbar University, Iraq. He got the first ranking in two above studies. He got his Ph.D. from Technology University-Baghdad, Computer Science Department. He is a teaching staff member in English Department in College of Education for humanities sciences. His research interests Data and Network Security, Coding, Number Theory and Cryptography.

Prof. Abdul Monem S. Rahma Ph.D Awarded his M.Sc. from Brunel University and his Ph.D. from Loughborough University of technology United Kingdom in 1982, 1984 respectively. He taught at Baghdad university department of computer science and the Military College of Engineering, computer engineering department from 1986 till 2003. He fills the position of Dean Asst. of the scientific affairs and works as a professor at the University of Technology computer Science Department. He published 88 Papers, 4 Books in the field of computer science, supervised 28 Ph.D. and 57 M.Sc. students. His research interests include Computer graphics image processing, Biometrics and Computer Security. And he attended and submitted in many scientific global conferences in Iraq and many other countries. From 2013 to Jan. 2015 he fills the position of Dean of the computer Science Department at the University of Technology.

Abdul Mohssen J. Abdul Hossen is an Associate Professor of applied mathematics, Computer Science Department, University of Technology, where he teaches undergraduate and graduate courses in mathematics. Abdul Hossen received the B. Sc. degree in mathematics from Mustansiriyah University, Iraq in1977, the M. Sc. degree in applied mathematics from Bagdad University, Iraq. in1980, the Ph.D degree in applied mathematics from the University of Technology, Iraq, 2005. He is a member of the IEEE system and Member of the editorial Journal.

How to cite this paper: Omar A. Dawood, Abdul Monem S. Rahma, Abdul Mohssen J. Abdul Hossen,"New Symmetric Cipher Fast Algorithm of Revertible Operations' Queen (FAROQ) Cipher", International Journal of Computer Network and Information Security(IJCNIS), Vol.9, No.4, pp. 29-36, 2017.DOI: 10.5815/ijcnis.2017.04.04

