2018 1st Annual International Conference on Information and Sciences (AICIS)

Developing a New Secret Symmetric Algorithm for Securing Wireless Applications

Omar A. Dawood[1]
College of Arts
University Of Anbar
Anbar , Iraq
Omar-Abdulrahman@uoanbar.edu.iq

Othman I. Hammadi[2]
University Of Anbar
Anbar, Iraq
ed.osman.ibrahim@uoanbar.edu.iq

Thaar Kh. Asman[3]
University Of Anbar
Anbar, Iraq
thaerk20000@yahoo.com

***Abstract*— The security of wireless protocols has been evolved and become widespread for different sectors because it is very important in daily lives and it became ubiquitous. The introduced paper includes the developing of new variant fast block cipher design for trusted wireless security protocols with a high level of security. Currently, the security of wireless become one of the hottest topics in the cryptography fields. The recent active attacks on the internet and the networks' penetration in addition to several technical troubleshooting generated a substantial concern about data transmission. For these reasons, wireless security protocols can be considered the best solution for various environments and for different applications. The bandwidth limitations and the security of ciphering design consider the main challenges of wireless issues that took a great interest from researchers and pay attention to propose successful ways to solve these problems. The present cipher proposed to handle the security of transmitted data with secure communication. The proposed cipher works with Substitution-Permutation Network (SPN) structure and with three ciphering key of 128-bit, 192-bit and 256-bit similar to the Advance Encryption Standard (AES) cipher in term of the number of rounds and the design strategy. The proposed cipher designed to be suitable for encryption the packets of data across the wireless techniques to ensure a secure band through the synchronous broadcast from the transmission's station to the target destination. So the proposed cipher can trust the transmission media in a secure and effective way since it depends on a solid algebraic base and approvable mathematical foundation. The internal structure looks like a hybrid structure of several embedded stages from several modern ciphers.**

Keywords*— *AES Cipher, Block Cipher, Wireless Security, Wi-Fi Protected Access (WPA), Wireless Equivalent Privacy (WEP), Network Security.

I. INTRODUCTION

The wireless networks play a vital role in modern ubiquitous technologies via transferred data from source to target using the broadcasting radio wave. Recently the widespread utilization for the wireless techniques compared with the wired networks has taken a high interest to adopt the wireless techniques in most of the daily digital applications [1]. The wireless networks characterized by several good features like the effectiveness, flexibility and low cost. On other hand, the wireless networks transmitted the data in open space that exposing it to eavesdropping and vulnerable penetrations from intruders [2]. Data privacy is the main concern for the network security and communication systems, especially for wireless networks. There are several approaches of security methodologies for trusting the wireless infrastructure and network protocols. Since the network levels and the access control issues need compact ciphers with different visions and with different sizes [3][4]. This paper introduces a high margin of security for the security wireless protocols by implementing a new variant of the proposed symmetric cipher. The proposed cipher uses a new security strategy to trust the transmitted data and to encrypt the passwords at the access point and the router transmission devices in order to prevent the stealing of sensitive information and the secret data. Outline of the present paper: this paper is organized as follows: Section II Explains the main problem statement in this study: Section III Shows the global overview about the most common wireless security protocols: Section IV introduces the design strategy and the major stages construction of the proposed model: Section V Explains the internal structure and algebraic foundation for the round transformation: Section VI Involves the design criteria and the most cipher utilizations: The cipher analysis and the acquired results submitted in Section VII: Section VIII includes the conclusion of this study.

II. THE RESEARCH PROBLEM STATEMENT

The wireless networks have many restrictions compared with the wired networks represented by low data storage, low power consuming, additional cost of hardware and software in addition to several security challenges [5]. The main sensitive security issues in a wireless environment are the confidentiality, authentication, and integrity axes. The confidentiality matter comprises the encryption algorithms whether the block ciphers or stream ciphers that encrypt the transmitted packets over the network and should be secure. The most popular encryption algorithms are RC4 stream cipher and the Advance Encryption Standard (AES) block cipher [6]. From another perspective, the authentication matter involves the identification who generate a specific traffic from certain part to the intended node and verifying from its source identity to prevent an authorized access [7]. The integrity term comprises the data correction in communication networks in case of data mismatching, data corruption, noise interleaving and the most common kind of an occasional errors in data communication. The most popular integrity method is Cyclic Redundancy Check (CRC) which represents a code word of a fixed length

978-1-5386-9188-5/18/$31.00 ©2018 IEEE
DOI 10.1109/AiCIS.2018.00038

CPS Conference Publishing Services

with a short binary sequence. CRC added as a check value to the text to determines the accidental change and disclose the tampering behavior in the receiving message. The core job for the CRC is to guaranty the integrity of data delivered by using a polynomial mathematical computation. The open communication in a wireless network and the transmitted data over aerospace create a big security challenge for imperative need to develop a high secure cipher [8]. So the fast encryption algorithm with a developed structure become a necessary demand to trust the transmitted data in unsecured network channels.

III. SPEED OVERVIEW ABOUT THE MOST COMMON WIRLESS PROTOCOLS

The wireless security protocols have gone through numerous stages of evolution for several decades. Thus, there are several versions of the wireless security protocols that have been upgraded throughout different stages and can be summarized as follows:

A. Wired Equivalent Privacy (WEP)

Wired Equivalent Privacy (WEP) is the most popular Wi-Fi security protocol that embedded in several router control panels. WEP was invented as the first version of Wi-Fi security protocol in 1999. The first version of the WEP protocol was suffered from the security vulnerability since the encryption at that time was subject to the industry restriction by using only 64-bit in encryption process [9]. After that time the encryption was increased to reach 128-bit and up to 256-bit. The 128-bit encryption technique was the most common widely used compared with the 256-bit. Although the WEP protocol was enhanced and increased the ciphering key size, but many of security flaws were present and still discover. Therefore; the awareness about the WEP protocol was increased since the WEP protocol cannot withstand in front of the speed of the modern computer and the recent advance technology [10].

B. Wi-Fi Protected Access (WPA)

Wi-Fi Protected Access (WPA) was appeared as a replacement for WEP due to the security flaws and the vulnerabilities of the WEP protocol. The WPA protocol works on IEEE 802.11i standard and it was adopted formally in 2003. The main additional prominent part in WPA protocol is the WPA-PSK (Pre-Shared Key) that deals with 256-bit encryption scheme [11]. Another significant change involves the message integrity checks that detects the packed altering or any data modification by the attacker. The WPA also includes the Temporal Key Integrity Protocol (TKIP) that used as a per-packet key system and have considered more trusted than the fixed key system of the previous WEP protocol. Later on, the TKIP encryption protocol replaced by Advanced Encryption Standard (AES) algorithm [12]. In spite of the significant improvements of WPA was over WEP and the ease of implementation across the embedded devices, but unfortunately, the developed protocol was suffered from the same problem of the previous version that involves the security vulnerability against the intrusion activities and it was facing some problems [13].

C. Wi-Fi Protected Access II (WPA2)

The wireless security protocol WPA2 has been adopted in 2006 as a replacement to WPA protocol. Since the previous protocol also encounters some penetration problems but in a very restricted size [14]. One of the most difference between WPA and WPA2 protocol is the use of (Counter Cipher Mode with Block Chaining Message Authentication Code Protocol) CCMP as an alteration for TKIP in the previous version. However, the security flaws in this protocol tend to be very limited but it is still a security concern [15].

IV. THE DESIGN STRATEGY OF THE PROPOSED CIPHER

The proposed cipher uses 128-bit message block of (16 bytes) and 128-bit, 192-bit and 256-bit of ciphering key lengths the same ciphering secret key lengths that supported by AES cipher. The message block and the ciphering key can be realized as a 4*4 state matrix. Each state matrix represents 16 (4*4) bytes which are equal to 128-bits. The proposed cipher uses basically 4 main stages. These operations are XORed add operation between the message block and the round key (AddRoundKey), S-Box tables (SubByte operation), row shifting (RevisibleShiftRows) and mixing each column in the matrix (Mixing-layer). The proposed algorithm performs efficiently in applications with low covered area resources and the applications that need high-speed cryptosystems to speed up high-bandwidth data transfers and to protect the privacy quickly. Proposed cipher designed to applies high volume of protection with high resistant against the recent of malicious attacks and it provides an elegant key schedule (key setup) that expands in two directions in rows/columns states. The key expansion algorithm designed to increase the complexity of key generation and to increase the guessing probability of the key estimation. The proposed technique works to eliminate the weak and semi-weak keys in generation process. The design process took a long period of design experience and series of practical developments by depending on several previous of published models for the same contribution like Euphrates cipher, Tigris cipher and FAROQ cipher see [16] [17] [18] respectively. The main motivation behind the design of the proposed cipher is to design a convenient cipher for the wireless applications and protocols. Accordingly, the proposed cipher focused on increasing the performance and the speed of submitted cipher in addition to the security aspects with design simplicity. This matter leads to figure out the algorithm details and the entire aspects of rational design in addition to the implementation sides and the whole description for the encryption and decryption process. This cipher imposed to provide a good and reasonable resistance against theoretical and practical cryptanalyses attacks. Since it has inherited most of its good characteristics from the standard cipher and other well-known proved algorithms. The proposed algorithm uses a complex round transformation of multiple layers with two constant vectors in its key generation process. Many effective attacks have been taken into account through the design process. The proposed algorithm is designed to be implemented efficiently in both software and hardware and to defeat the effective threats. This cipher also designed to accommodate the Wi-Fi security requirements taken into

considerations many elements such as gate counts, memory requirements, code size, power consumption, latency and software performance on multiple executive environments.

V. THE INTERNAL STRUCTURE OF THE PROPOSED CIPHER

The internal structure for the proposed cipher can be explained by the round transformation that consists of the elementary stages which repeated regularly according to the number of rounds. These stages act the main internal operations of the proposed cipher as it is stated in Fig 1.

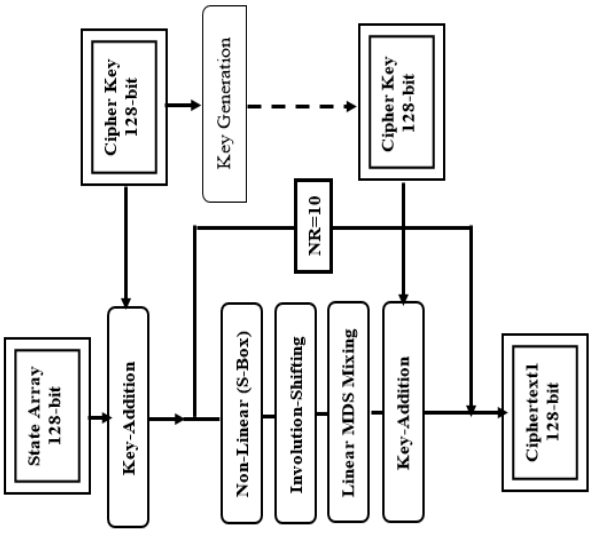

Fig 1. The General Structure of Proposed Cipher

A. Non-Linear (Subbyte layer)

One of the most significant operations in any cipher construction is the S-Box. The proposed S-Box is a non-linear stage with a matrix of 16*16 dimension. The construction of the proposed S-Box is very similar to the AES S-Box which build in two steps: The first step takes the 8-bit quantity of entry byte and calculates the multiplicative inverse according to the irreducible polynomial of $x^8 + x^5 + x^3 + x^2 + 1$. If the entry byte is non-zero the S-Box intersection ith row and jth column will give a new value otherwise will map to 00 as it is shown in TABLE I. at the appendix.

$$f(x) = \begin{cases} x^{-1}, & x \neq 0 \\ 0, & x = 0 \end{cases} \qquad (1)$$

The second step deals with the implication over GF(2^8) and the values as an independent byte. The sliding multiplication is implemented by affine multiplication for each byte and the resultant table can be shown at the appendix with TABLE II. The resultant table is XORed with the constant vector of (63) to produce the final of forward S-Box that can be illustrated in TABLE III.

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

TABLE III. Non-Linear S-Box

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

B. Inverse Non-Linear (Inv-Subbyte layer)

The inverse process of the proposed subbyte operation (Inv-S-box) is built by computing the inverse affine transformation accompanied by computing the multiplicative inverse whereby the new irreducible polynomial over GF(2^8). The reconstruction of InvS-Box is implemented in two steps. The first step is computing the inverse of affine transform XORed with constant vector (05) where the result will be in TABLE IV.at the appendix. Then taking the XORing vector with the mentioned table and the outcome will be a final backward table that can be shown in TABLE V. The main clue beyond the use of constant vector is to increase the computational complexity level and to prevent the appearance of any tractable formula through which the reverse computational steps can be exploited.

$$\begin{bmatrix} b'_0 \\ b'_1 \\ b'_2 \\ b'_3 \\ b'_4 \\ b'_5 \\ b'_6 \\ b'_7 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \\ b_6 \\ b7 \end{bmatrix} + \begin{bmatrix} 1 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} \qquad (3)$$

TABLE V. Backward Non-Linear S-Box

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

C. *Reversible Shifting Stage & Inv-Reversible Shifting Stages*

The basic notation behind this stage is to distribute the values of the input column to spread output positions. The shifting phase is a diffusion layer that works on rows addresses and the array is rotated by a number of byte. The first row remains without shifting and 2nd, 3rd and 4th rows are shifted by 2-byte to the left as it is shown in Fig 2. The decryption process in shifting stage is implemented by the same strategy since the shifting stage acts a self-reversible steps by implementing the same shifting steps.

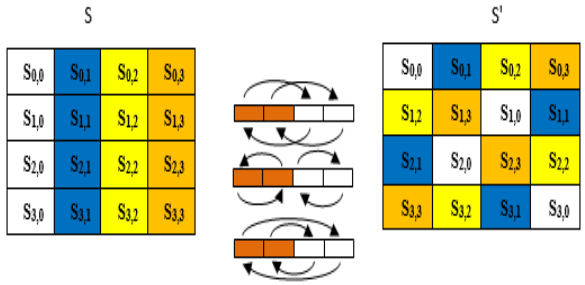

Fig 2. RevisibleShiftRows Stage

D. *Linear Code of Mixing-Layer & Inv-Mixing Layer*

This stage basically depends upon a new linear equation of order four that works as a Maximum Distance Seperable (MDS) of the linear code. The Mixing layer provides both confusion and diffusion properties to the whole structure of the proposed cipher. The last round transformation in the proposed algorithm does not involve the mixing layer similar to the AES structure. Mixing layer takes a 4×4 state matrix which multiplies each column vector by the constant matrix. The multiplication process includes the shifting and multiplication operations. The proposed MDS equations selected from several best equations that we have gotten through computer computation search. The forward/backward equations can be illustrated in equation (4) and (5) respectively.

$$a(x)= \{06\}x3 + \{01\}x2 + \{05\}x + \{03\} \quad (4)$$

$$b(x)= \{09\}x3 + \{0b\}x2 + \{0a\}x + \{09\} \quad (5)$$

$$a(x) * b(x) = I \quad (6) \quad \text{Where I identity matrix}$$

The proposed linear equation reformed as a circular matrix multiplication where each subsequent row is constituted by a circular shifting from the previous one, by one placement to the left. This polynomial is coprime to the reducible polynomial of $(x^4 + 1)$. Thus, the proposed MDS matrix is invertible linear code of circular matrix.

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

$$\begin{bmatrix} S'_{0,c} \\ S'_{1,c} \\ S'_{2,c} \\ S'_{3,c} \end{bmatrix} \otimes \begin{bmatrix} 03 & 06 & 01 & 05 \\ 05 & 03 & 06 & 01 \\ 01 & 05 & 03 & 06 \\ 06 & 01 & 05 & 03 \end{bmatrix} = \begin{bmatrix} S_{0,c} \\ S_{1,c} \\ S_{2,c} \\ S_{3,c} \end{bmatrix} \otimes \begin{bmatrix} 09 & 09 & 0b & 0a \\ 0a & 09 & 09 & 0b \\ 0b & 0a & 09 & 09 \\ 09 & 0b & 0a & 09 \end{bmatrix} = \begin{bmatrix} S'_{0,c} \\ S'_{1,c} \\ S'_{2,c} \\ S'_{3,c} \end{bmatrix}$$

The multiplication of the entry vector (column) is implemented as four bytes (32-bits) multiplied by the constant MDS matrix(4x4) in forward and backward. The multiplication of this matrix by its inverse matrix gives the identity matrix as it is shown below:

$$\begin{bmatrix} 03 & 06 & 01 & 05 \\ 05 & 03 & 06 & 01 \\ 01 & 05 & 03 & 06 \\ 06 & 01 & 05 & 03 \end{bmatrix} \times \begin{bmatrix} 09 & 09 & 0b & 0a \\ 0a & 09 & 09 & 0b \\ 0b & 0a & 09 & 09 \\ 09 & 0b & 0a & 09 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

E. *Key Addition Layer & Key Scheduling Algorithm*

The key addition layer includes the byte-addition that XORed byte by byte between the ciphering key and the state array over G(2). The same operation is achieved for both encryption and decryption processes since the XOR operation has its own inverse. The Key scheduling algorithm is the main part that responsible for the generating sub-ciphering keys to all rounds. The derivated sub-ciphering key is generated by the complex functions that regenerate a new sub-ciphering key from the previous one for each round. Key generation algorithm represents the core segment for the key expansion that accept a 128-bit input key and generate a new 128-bit of ciphering secret key. The proposed key expansion consists of two internal complex functions Function(g) and Function(F). where the Function(g) involves three steps: Subbyte, Complement word and XORed constant vector of (Qw = 9e3779b9). The Function (F) also consists of three main subfunctions: Subbyte, Right rotate(word) and XORed with another constant vector of (Pw = b7e1516). The general structure for the key expansion algorithm can be stated in Fig 3.

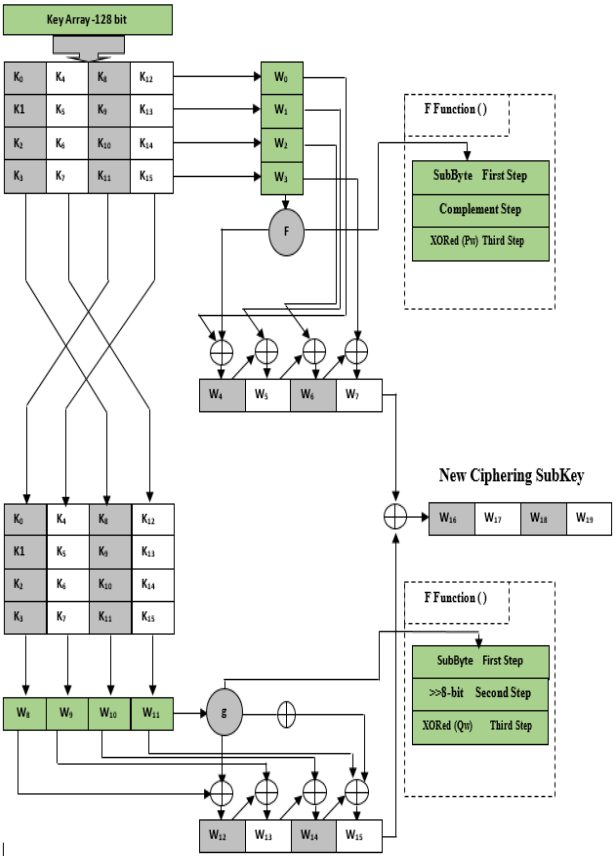

Fig 3. Key Generation with Two Complex Functions

The key expansion steps has been enhanced to be able to implement the key generation procedure using a small size of memory amount as possible as to give more flexibility in key agility and structure scalability. The basic secret beyond the two internal of the complex functions is to remove any symmetries in the repeated words and to prevent the appearance of weak keys and semi-weak key and to provide high confusion and diffusion properties.

VI. THE DESIGN CRETERIA AND THE APPLICATIONS OF THE PROPOSED CIPHER

There are several significant criteria in designing the proposed algorithm regarding the characteristics of the proposed cipher structure and the internal mathematical foundations in addition to the complexity of the algorithm. The proposed cipher constructed according to the following criteria:

1. Design with a high level of security.
2. Algorithm Simplicity with scalability structure.
3. Conservativeness design.
4. An efficient implementation cipher in SW&HW.
5. A suitable cipher for constrained and embedded devices.
6. The design simplicity and balance structure.

The proposed algorithm can be used in several applications in addition to the wireless protocols

1. The proposed cipher considers a good choice for the Internet of Things (IoT) applications.
2. It can be implemented effectively in sensor network applications.
3. Its a suitable choice to trust network access control.
4. The proposed cipher can be applied in cloud computing applications.
5. A secure cipher for E-commerce and the the digital cash payment like the ATM devices.

VII. ANALYSIS AND EXPERIMENTAL TEST

The proposed cipher is a modern secret cipher which is designed to be a multi-purposes cipher and specifically for the wireless applications. The proposed cipher supports key expansion algorithm with high complexity and simple construction which can be implemented efficiently in a low covered area and constrained environment. The proposed cipher adopts strong key-dependent S-box that generates unusual dependency between the structure of the algorithm and the ciphering sub-keys. Some main stages in the round transformation have been combined to reduce the hardware built in board likewise the shifting stage.

The structure design for the proposed cipher was engineered to be suitable for the wireless environment requirements. The goal of an enhanced structure is to ensure high performance for the constrained environment that requires fast change for the ciphering key relative to the necessity requirments. The proposed cipher is tested regarding to the most popular statistical tests. The test results did not show any deviation in term of random mapping. These statistical tests are necessary but not enough to determine the algorithm security level. Since it does not determine the strength points for the algorithm aspects just it determines the randomness tendency for the ciphertext. Significant comparison of encryption implementation in Ms between the proposed algorithm and the standard AES cipher can be shown in TABLE VI. and TABLE VII. respectively.

TABLE VI. IMPLEMENTATION METRICS BETWEEN THE AES CIPHER AND THE PROPOSED MODEL

Algorithms	Block Size	Key Size	Number of Bytes	Time of Encryption
Original AES	128-bit	128-bit	1000	0.0468
			10000	0.46
			100000	4.12
Proposed Model	128-bit	128-bit	1000	0.0468
			10000	0.44
			100000	4.07

TABLE VII. PERFORMANCE COMPARISON BETWEEN THE PROPOSED CIPHER AND THE AES

Key Length	Language	Processor	Code Size	Clock Cycle of Key Scheduling	Clock Cycle of Encryption
AES 128-Bit	Assembly	Intel-Core i7	9150	11050	12930
Proposed Model 128-Bit	Assembly	Intel-Core i7	9074	11032	12650

The proposed cipher has been tested several times and the current results are chosen from the best results taken in to account the uncontrollable factors and the statistical deviation of randomness behavior. The proposed model measured by Windows 10 Pro 32-bit, Intel (R) Core-i7 Tm. The main stages in the round transformation are enhanced to reduce the power consumption and to increase the throughout of encrypted data, as well as increasing the implementation speed as much as possible. The S-Box is well-constructed layer to thwart linear cryptanalysis attack and the interpolation attack using low-bit correlation property. The proposed structure characterized by balancing internal operations that make the power analysis and timing attacks are very hard. The selected MDS code in the linear layer was to apply full diffusion property with an effected coefficients to the whole rounds operations. There is no R-con table in the key expansion stages, in order to close the road infront of the attacker from exploiting the constant word by mounting their attacks. The involutional shifting stage is to reduce the Gate Equivalent (GE) and to produce an accepted diffusion property. The addition process of two constant vectors to the key generation complex function was to prevent the round symmtries form repeated difference propagation of plaintext/ciphertext in each round.

VIII. CONCLUSIONS

The proposed design provides an efficient symmetric cipher with an iterative structure that optimized its internal round transformation with top security margin. The algebraic base for the proposed cipher gives a robust structure that able to encounter the various algebraic attacks. Thus, the implementation results show an accepted implementation in a restricted environment with low power consumption. The enhanced cipher architecture characterized by high processing throughput with design simplicity using byte-oriented manipulation. The security strategy completely depends upon increasing the complexity of mathematical operations for the entire stages. The proposed algorithm can be employed for trusting the wireless security protocols and most the wireless applications.

REFERENCES

[1] O. Aliu, A. Imran, M. Imran, and B. Evans, "A survey of self organisation in future cellular networks," IEEE Communications Surveys & Tutorials, vol. 15, no. 1, pp. 336-361, February 2013.

[2] Chih-Wei Yi, "A Unified Analytic Framework Based on Minimum Scan Statistics for Wireless Ad Hoc and Sensor Networks", IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 20, NO. 9, SEPTEMBER 2009.

[3] Jiannan Wei, "Accountable and Privacy-Enhanced Access Control in Wireless Sensor Networks", IEEE Transactions on Wireless Communications, 15(4), 3097–3099. doi:10.1109/twc.2015.2507124.

[4] Omar A. Dawood, A. M. Sagheer, and S. S. Al-Rawi, "Design Large Symmetric Algorithm for Securing Big Data", 1th International Conference on the Developments in eSystems Engineering, 2nd –5th September 2018 Cambridge, England, UK, 978-1-5386-6712-5/18/$31.00 ©2018 IEEE.

[5] Thaier Hayajneh and et al, "An Enhanced WLAN Security System With FPGA Implementation for Multimedia Applications", IEEE Systems Journal, 11(4), 2536–2545. doi:10.1109/jsyst.2015.2424702.

[6] A. M. Sagheer, S. S. Al-Rawi, and O. 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.

[7] Khaneja and et al, " Wireless Sensor Network Specific Voltage Scaling Based Energy Efficient Circuit Design for Cyclic Redundancy Check", 2015 International Conference on Computational Intelligence and Communication Networks (CICN). doi:10.1109/cicn.2015.48.

[8] Yuejun Wei and et al, "A CRC-Aided Hybrid Decoding Algorithm for Turbo Codes", IEEE WIRELESS COMMUNICATIONS LETTERS, VOL. 2, NO. 5, OCTOBER 2013, 2162-2337/13$31.00 c 2013 IEEE.

[9] Vipin Poddar and Hitesh Choudhary, "A COMPARITIVE ANALYSIS OF WIRELESS SECURITY PROTOCOLS (WEP and WPA2)", International Journal on AdHoc Networking Systems (IJANS) Vol. 4, No. 3, July 2014.

[10] Kashish Monga , Vishal Arora and Ashish Kumar, "Analyzing the behavior of WP A with modification ", 2015 IEEE International Conference on Communication Networks (ICCN) 978-1-5090-0051-7 115/$31.00©20 15 IEEE DOI 10.1109/ICCN.2015.11.

[11] Ravi Kishore Kodali, Satya Kesav Gundabathula and Lakshmi Boppana, "Implementation of Toeplitz Hash based RC-4 in WSN", 978-1-4799-1823-2/15/$31.00 ©2015 IEEE.

[12] I. P. Mavridis, and et al, "Real-life paradigms of wireless network security attacks", 2011 Panhellenic Conference on Informatics, 978-0-7695-4389-5/11 $26.00 © 2011 IEEE DOI 10.1109/PCI.2011.25.

[13] A. H. Lashkari, F. Towhidi and R. S. Hoseini, "Wired Equivalent Privacy(WEP)", ICFCC Kuala Lumpur Conference, 2009.

[14] T. A. T. Aziz, Mohd Raziff Abd Razak and Noormazatul Elena Abdul Ghani, "The Performance of Different IEEE802.11 Security Protocol Standard on 2.4GHz and 5GHz WLAN Networks", 2017 International Conference on Engineering Technology and Technopreneurship (ICE2T), 978-1-53861807-3/17/$31.00 ©2017 IEEE

[15] Iman Saberi and et al, "Improving confidentiality of AES-CCMP in IEEE 802.11i", 2012 Ninth International Conference on Computer Science and Software Engineering (JCSSE). doi:10.1109/jcsse.2012.6261930.

[16] Omar A. Dawood, Abdul Monem S. Rahma, Abdul Mohssen 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.

[17] Omar A. Dawood, Abdul Monem S. Rahma, Abdul Mohssen J. Abdul Hossen, "The New Block Cipher Design (Tigris Cipher)", International Journal of Computer Network and Information Security (IJCNIS), Vol.7, No.12, pp. 10-18, 2015.DOI: 10.5815/ijcnis.2015.12.02.

[18] 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.

Appendix

TABLE I. The Multiplicative Inverse according to Irreducible Polynomial $x^8 + x^6 + x^3 + x^2 + 1$

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

TABLE II. The Result of the Forward Affine Transform

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

TABLE V. The Result of the Backward Affine Transform just XORed Vector without Taken Multiplicative Inverse

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