Journal of Computer Science

Original Research Paper

Secure Symmetric Block Cipher Design for Encrypting the Bitcoin Wallets in Cryptocurrencies Applications

[1]**Omar A. Dawood,** [2]**Othman I. Hammadi and** [3]**Falath M. Mohammed**

[1]*Computer Science Department, University of Anbar, Anbar, Iraq*
[2.3]*College of Education for Humanities Sciences, University of Anbar, Anbar, Iraq*

Article history
Received: 27-02-2019
Revised: 04-05-2019
Accepted: 31-05-2019

Corresponding Author:
Omar A. Dawood
Computer Science Department,
University of Anbar, Anbar, Iraq
Email: support@thescipub.com

Abstract: This paper proposes a new symmetric secret-key cipher for construction of block cipher model. This new approach is considered as a smart step that can be applied to the long process research of modern designing methods used in developing earlier symmetric algorithms. The present cipher can encrypt block lengths of 128-bit by employing Substitution-Permutation Network (SPN) structure. The present cipher uses three options of strong ciphering-key along with variable lengths of 192-bit for 12 rounds, 128-bit for 10 rounds and long ciphering key of 256-bit for 14 rounds similar to standard ciphers. The proposed algorithm has been designed to trust applications that are based on Bitcoin and crypto-currencies. The current algorithm intended to encrypt addresses of Bitcoin wallet that work quite similar to the e-mail address. The bitcoin wallet includes sensitive information like private secret keys and derived password that are highly confidential. The Advance Encryption Standard (AES) is employed to encrypt most of the bitcoin wallet database. The proposed cipher can act as a good substitute for the standard cipher that allows trusting the Bitcoin wallet database with high security and with a much more complex scheme. The key goal of the submitted algorithm is to build a new enhanced modern cipher with a secure and efficient applicable algorithm that can be used for crypto currencies applications employing a wide trail design strategy.

Keywords: Block Cipher, Advance Encryption Standard, Cryptocurrency, BlockChain, Decentralized Currency, Bitcoin Wallets, Peer-to-Peer Network, Proof-of-Work

Introduction

A humongous volume of financial transactions is carried out over the network on a daily basis that involves processing and transmitting of millions of dollars via cryptocurrency systems. Such systems need to maintain a high level of security to protect against frauds (Karame and Androulaki, 2016). The proposed cipher has been developed to be in par with the information revolution as well as rapid growth of internet services that use bitcoin. Thus, the design of robust cipher structure has been proposed to deal with modern attacks as well as provide high protection level against malicious attacks. The present algorithm involves a series of developments via long process research has been used by authors for several years, as its design idea as well as the internal structure rely on various block cipher models that have been historically developed and recently published, such as Euphrates cipher, Tigris Cipher and FAROQ cipher designed by (Dawood *et al*., 2015a; 2015b; 2015c). These symmetric ciphers have been proposed by the same author and published recently. The mentioned ciphers paved the way in front of design the current cipher and their work quite similar to the AES standard cipher. The introduced cipher includes all improvements in terms of design structure based on successive models. The key aim of the submitted algorithm is to develop a new modern cipher that employs a secure and efficient applicable algorithm in crypto-currencies applications employing the wide trail design strategy that explained by (Daemen and Rijmen, 2001). Many block ciphers models are available and a majority of these ciphers as well as their structures have been developed by considering confusion with permutation, diffusion and substitution layers. Completely known encryption/decryption processes have been employed for all these ciphers, while just keeping the ciphering key as secret as per the Kerckhoff's design principles (FRANCO, 2015). The developed algorithm includes three trusted layers: Non-linear layer characterised by the complement of close box C-Box, Super-Mixing (P-Box) of Linear layer with Zigzag-Shifting process in addition to Key addition layer.

Literature Survey

In this part, a review about some introduced works which are classified according to the most relevant of current study is done. Thus, on the one hand of confidentiality will explain the following studies:

> In (Bitcoin Wiki-BIP 0032, 2012). The BIP 0032 was announced a new technique about generating multiple private keys and as a result several of various Bitcoin addresses will be generated depending on certain seed. This type of wallet is denoted by Hierarchical Deterministic (HD) wallets that accept a specific deterministic derivation rule for retrieving the private keys from the seed. This technique also gives the user possibility to make a backup for the seed instead of doing that for all the private keys.

A secure symmetric algorithm employed for encrypting the wallet.dat file that utilized in Bitcoin client as explained in (Mike Caldwell-BIP 0038, 2012). The encryption process involves a standard cipher of AES with Cipher Block Chaining (CBC) (AES-256-CBC) for encrypting the private keys that are generated in a wallet on client demand. AES-256-CBC encrypts the master key that undertakes the responsibility of encrypting the private keys which derivate from the passphrase. CBC refers to the Cipher Block Chaining (CBC) operation mode for block cipher algorithm. Where the encryption process comprises each cipher text unit is encrypted under secret of ciphering key and applied to the whole block. CBC represents an additional layer of complexity for the encrypted plaintext combined with Initialization Vector (IV) of a specific length.

The client utilizes AES-256-CBC algorithm for encrypting Bitcoin wallet database. Most modern Bitcoin wallets give the client an option for encrypting user's private keys with the AES-256-CBC algorithm to introduce a trusted passphrase. The AES cipher encrypts the wallet database (Keys) and as a result the user must enter the passphrase to make the transaction and sending process. This step is to alleviate some practical attacks which are possible face the wallet.

The current studies of literature survey comprise the authentication and integrity aspects:

> Elliptic Curve Digital Signature Algorithm (ECDSA) has been proposed by (Gallagher and Romine, 2013). ECDSA acts one of the strongest security methods for Digital Signature Algorithm (DSA) that depends on (EC) and encounters the non-repudiation phenomena. The signature process depends mainly on the secret keys generated from the (EC) cryptographic method. The ECDSA is a standard cipher for generating random private keys of 256-bit (32-byte) and signing the transactions as well as verifying from the signature.

BitcoinWiki (2016) Base58Check announced a novel technique of Base58Check coding method. The Base58Check coding is a developed method of binary to text encoding schema that similar to base64 except it does not involve predefined symbols. It consists of two terms the first one is "Base58" that used base58 character for encoding process. The second term is "Check" which points to a checksum that used for data integrity and error detection. Base58Check works to encode the byte arrays in Bitcoin into string of 58 recognizable characters.

Crypto-Currency and Bitcoin Concept

A robust and effective algorithm is needed for the current advances accompanying to digital currency as well as rapid progress in the super computer industry. It should also have the capability to face recent as well as future challenges. The modern active attacks and the progress of the internet as well as network communications along with parallel computing have greatly helped to defeat and break popular encryption algorithms (Szmigielski, 2016; Sagheer *et al*., 2011). Since crypto currency is categorised as a virtual currency, it relies on cryptographic foundations and encryption rules with regards to verifying, signing and confirmation are applicable.

It can be defined as a decentralized digital currency involved in the electronic payment system employing the cryptographic Proof-of-Work (PoW) process and the distributed consensus protocol in place of Third Trusted Parity (TTP). Cryptocurrencies include favourable features such as privacy, anonymity, confidentiality as well as transparency that allow each person on the network to monitor the account balance pertaining to all parties (Matthew *et al*., 2015) There are many kinds of cryptocurrencies like ethereum, bitcoin, dogecoin, ripple, titcoin, litecoin, monero, gridcoin and dash. The bitcoin is the most famous as well as the most extensively used cryptocurrency. It was introduced by Nakamoto (2008). It can be considered as the currency employed in the network, software and protocol altogether. Figure 1 shows the key scenario involved with Bitcoin.

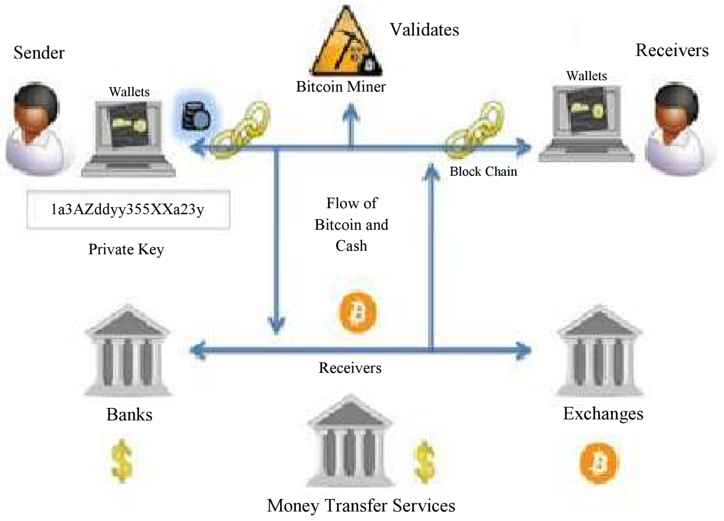

Fig. 1: Bitcoin scenario overview

Bitcoin as a digital currency ecosystem gained much popularity amongst individuals and governments due to its considerable use in trusted electronic payment, saving, purchasing and investments. Blockchain is the Bitcoin ledger signifying a back linked list. It can also be regarded as a public ledger with registries of all bitcoin transactions in the network. Transaction by using bitcoin on the user's public key involves a series of irreversible cryptographic hashing that allows moving the bitcoin from one address to another (Melanie, 2015). When sending in the transaction process, transaction fees are always involved to make a request by the bitcoin's user, which allows the miner for bundling them into a block. The term block involves a set of transactions that have been signed with cryptographic hashing of the previous block and timestamps. The main blockchain is included in the linked list of these validated blocks in the network, which starts via genesis block. The user can generate multiple public keys for various addresses to facilitate exchanging amongst participants (Andreas, 2015). Linking of the imposed addresses could be done with one or more trusted bitcoin wallets. Bitcoin wallets are basically software that stores all addresses and acts as a backup for keeping the secret of ciphering keys. Instead of the username, the bitcoin addresses include a string of letters and numbers. There no fixed size for the Bitcoin wallet database since each wallet may contain several millions of addresses and transactions that depend mainly on client activity and type of wallet (Aljosha, 2017).

The bitcoin wall*et al*so allows receiving, sending, storing the bitcoin as well as register the transferred coins along with the owners' details. There are different kinds of hardware and software wallets which can be categorised into hot and cold storage wallets. The cold storage wallets and real wallets share many similarities and so people can use them daily. The offline wallet is completely secure, allowing storing of small amounts of bitcoins similar to the hardware wallet: dedicated device wallet, USB drive and paper wallet. The online hot cryptocurrency wallet is connected to the internet and can keep many bitcoins such as mobile, cloud and desktop wallets. The most extensively utilised bitcoin wallets are Trezer, Leger, Electrum, Mycelium, Exodus and Jaxx, etc. (Miraje, 2016).

AES-256-CBC is employed to encrypt most of the wallets where the stored sensitive database (password and private keys) are encrypted in the wallet. Two elementary reasons can be described to summarise the key motivations to the design of the proposed cipher: the recent concerns pertaining to the expiry date of AES cipher's life time and the security concerns with the advance techniques involved in cryptanalysis attacks. Furthermore; the world become in urgent need for an extended cipher algorithm with larger block and key size to satisfy the applications that require an extra processing speed. The Big Data field, Cloud computing, Cryptocurrencies applications and several of other modern applications that require a bulk of encrypted data have been emerged recently (David and Chuen, 2015; Dawood *et al*., 2018).

The Advantages of Bitcoin Currency

The are several advantages of Bitcoin use over the electronic traditional payment systems that can be listed as follows (Bunjaku, 2017):

1. Bitcoin currency is not subject to the limitations or permission from any part and transcends the borders

2. It is safe to seizure no one can take your Bitcoin since you possess it, it's not belongs to any national bank or organization
3. Bitcoin is control safe that depends on difficult computational notation called Proof-of-Work (PoW) which means nobody can prevent your exchanges
4. Decentralized Bitcoin feature means achieving the transactions over millions of nodes with the absence of trusted third party
5. Bitcoin is scalable because it is an open source where anyone can participate in developing the Bitcoin software
6. Bitcoin has a restricted supply that will just ever be 21 million bitcoins made and are created at an anticipated rate
7. It is peer-to-peer currency with less transaction cost than the traditional centralized networks payment such as master card and visa card and etc
8. Bitcoin currency cannot be refund when you transform amount of money to someone there is no chance to reverse the transaction and back it to your account
9. The Bitcoin can be used as a real currency in buying different things from the internet
10. Bitcoin is untraceable that can be defined as anonymous, since the use of Bitcoin need no identifying information
11. Bitcoin introduces freedom financial transactions around the world without any restrictions
12. It is Simple and easy to create a Bitcoin account compared with the procedure involved with banking account

The Disadvantages of Bitcoin Currency

After mention the above advantages the Bitcoin disadvantages can be stated below according to the author (Ivaschenko, 2016):

1. Strong financial market volatility-the rise and fall down Bitcoin value effected directly on the declared policies adopted by some countries represents a main problem in cryptocurrency sector
2. The large risks surrounding investment in cryptocurrency and the cyberspace attacks are considered the main threats

The Proposed Algorithm

The proposed cipher can be defined as an iterated cipher that has been developed based on the standard guidelines pertaining to the symmetric algorithms. Three layers are involved in the round transformation of the put developed model. Close-Box (C-Box) is the first one, where for each byte of the state array, substitution is done along with the complement clue. This stage is known as non-linear or substitution layer. In the second part, the transposition clue is employed to derive the diffusion layer stage, which also confers diffusion characteristics, followed by the Super-Mixing layer's P-Box stage that confers diffusion and confusion characteristics along with constant Maximum Distance Separable (MDS) of linear equations. MDS matrices act linear code which essential circulant matrices for constructing most symmetric blocks cipher algorithms that undertake the generating of diffusion functionality. MDS matric can be described as n×n matrix with a circulant feature that involves its rows are generated by previous cyclic shifts of its first row to reuse the multiplication circuit recursively and to reduce the implementation cost. In recent years, several studies look for generating and implementing MDS matrices in the context of hardware design with small logical integrated circuit.

In the final part, a key generation method is introduced via key expansion procedures that allow employing the AddRoundKey or key addition layer. The key addition stage functions along with the symmetry characteristic, pertaining to the round transformation across multiple rounds. Figure 2 shows the general structure of the proposed algorithm with the main operations in the round transformation.

Non-Linear Complement-Based C-Box

A nonlinear stage is signified by the complement box or Close-Box (C-Box), which facilitates data transformation in the introduced cipher and each block is modified via replacement of the C-Box table. The C-Box stage relies on a novel idea for building C-Box that chooses a unique new affine matrix that is multiplied by its inverse to provide the complement of identity matrix. Development of the C-Box is based on choosing a new irreducible polynomial of $x^8+x^5+x^3+x^2+1$ as well as a new affine transform that possesses a modern idea associates with the complement property. Three steps define the development of forward C-Box. In the first step, multiplicative inverse to the entire values in the tables is considered, after which the new complement-affine transform is applied while the value (75) is XORed as constant vector. The C-Box's resultant table includes 256 hexa-values that were segmented into two groups, represented by (black and dyed in yellow) of 128-values for every group. This was followed by the function of C-Box; intersection of the entry value was done based on the values in the C-Box table.

Thus, the projection would be represented either in yellow colour or with black values. With regards to black values, these are direct and the desired value can be found with the intersection of the table's ith row and jth column to provide the output value. On the other hand, the group with highlighted yellow colour values will require an extra step that allows addressing the complement process regarding to the yellow value to be compatible with its inverse for the backward operation.

E.x: If a row/column index of (08) is taken in forward C-Box, the intersection result is a highlighted value with yellow colour of (42); when a value (42) or (01000010) in binary notation for the complement process is taken, then the result of (BD) or (10111101) is chieved.

Inverse Complement-Based C-Box

The construction of the inverse for the C-box is done by adopting the inverse of the affine matrix after which computation is carried out for the multiplicative inverse to each value in Galois Field GF(2^8) as well as the resultant XORed to the constant vector characterized by the value (FB).

E.x: In the case of backward C-Box, the row/column index of (BD) from an earlier example is taken. It would provide the highlighted yellow value of (08) and when in forward C-Box, the row/column index pertaining to the highlighted yellow value of (08) is taken, a value of (42) is obtained. In this paper, we have explained how this occurs as well as the key idea beyond the complement C-Box.

The secret behind the C-Box is signified by multiplying the forward affine matrix by the backward affine matrix, which yields the identity matrix's complement.

The complement identity matrix signifies that the values to the key diagonal of the matrix are zeroes, while the others yield one value. This also suggests that when the forward is multiplied by backward affine equations, no identity matrix is yielded and alternatively a complement matrix is yielded. This kind of matrix yields the complement identity matrix, which is a key point in the building of the C-Box, which has been seen to be stern and complex against the most effective attacks. To reverse the steps, there is no fixed easy point and has been considered to be insurmountable against the analysis. The forward and backward C_Box tables can be shown in Table 1 and 2.

Transposition Diffusion Layer

The functioning of the transposition diffusion layer is similar to rearrange the byte positions, where it essentially acts as a transposition cipher wherein only the positions of the elements are rearranged without altering their identities in the encryption process. This stage is a transposition method that responsible for generating the diffusion property. It is a new mechanism for rearranging the elements of state array in a zigzag way as shown in Fig. 3. These values are permutated in simple steps to distribute each entry input byte to various output byte. Thus, the cryptographic cipher with high diffusion scheme considers a more secure cipher. This method is optimum to achieve an optimal diffusion on hardware cost-effectively and allow rapid implementation along with protection against saturation and truncated differential attacks.

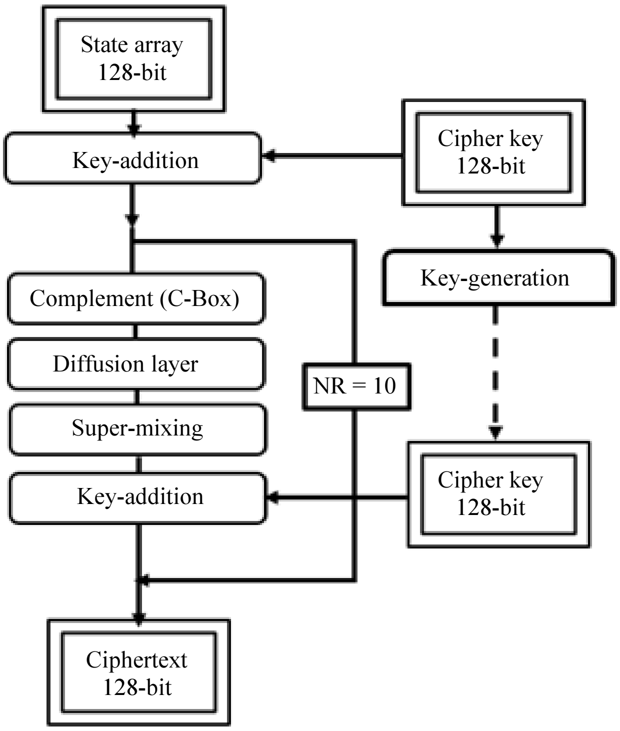

Fig. 2: General structure of the proposed cipher

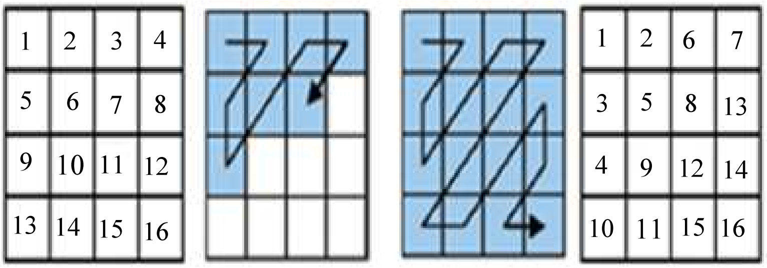

Fig. 3: The proposed zigzag diffusion stage

Table 1: Forward encryption C-Box

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

Table 2: Backward decryption C-Box

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

Linear of Mixing Layer

The third stage involves linear diffusion layers of Mixing notation that are denoted as a matrix multiplication of $Y = MX$, which can be described by super-mixing transformation. Although the put forward MDS matrix has no role in decreasing the correlation of a linear characteristic, it allows increasing the diffusion property. Implementing large MDS matrices could be a costly affair for hardware and would need additional overhead processing. The super-mixing transformation can be defined as the state array multiplied by certain MDS matrix of order four. Addressing of the MDS matrices could be done by multiplying a polynomial over GF(2^8). Altering any one entry incoming byte would result in impacting all the outcome bytes, as demonstrated in the following equations:

$$Forward\ \ a(x) = \{03\}x3 + \{05\}x2 + \{01\}x + \{06\} \qquad (1)$$

$$Backward\, b(x) = \{0B\}x3 + \{09\}x2 + \{09\}x + \{0A\} \qquad (2)$$

A linear equation called the super-mixing operation offers added diffusion and confusion, which makes analysis of the ciphertext more challenging. The selection of super-mixing matrices is based on the obtained best linear equations. This allows decreasing the gap in terms of difference in the encryption/decryption processes as well as maintaining a balance in the internal operations.

The generator matrix pertaining to a linear code (m*m) over GF(q) can be defined as a series of expanded algebraic forms that give: *G* = [*C*0, *C*1, *C*2,…, *C*p-1].

The linear diffusion arrays can be defined as the matrix multiplication arranged in a 4*4 square array of bytes, which have been moved via cyclic shifting to the left for the successive row as per the equation order. The implementation of entry values multiplied by the linear equation is similar to the constant circular matrix multiplied by the vector of entry values Y= MDS*V.

The identity matrix is obtained through the forward MDS matrix multiplied by the backward MDS matrix. As stated below, a modulo of reducible polynomial (x^4+1) is employed to transform the multiplication of the 4-byte column over GF(2^8):

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

$$d(x) = a(x) * c(x)\ mod\ \left(x^4 + 1\right) \qquad (3)$$

$$\begin{bmatrix} 06 & 03 & 05 & 01 \\ 01 & 06 & 03 & 05 \\ 05 & 01 & 06 & 03 \\ 03 & 05 & 01 & 06 \end{bmatrix} \times \begin{bmatrix} 0A & 0B & 09 & 09 \\ 09 & 0A & 0B & 09 \\ 09 & 09 & 0A & 0B \\ \mathrm{0B} & 09 & 09 & 0A \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

To implement the inverse super-mixing stage, the state array is multiplied by the backward MDS matrix as the matrix has been deemed invertible. When compared with the encryption implementation, the decryption.

Key Generation Layer

For each round, the key addition process is regarded as the main lock since adding the ciphering key results in termination of all the round transformations. The attacker needs to analyze the XORed operation to perform cryptanalyses with any cipher algorithm, as a majority of the algorithms function is based on the whitening concept of Kerckhoff's principle where XORed is the cipher key at both the end and the start of the algorithm.

The key addition process signifies simplification of the bitwise XORed operation between the cipher key array and the state array, column by column and bit by bit. Both decryption and encryption processes employ the same key addition process as the XORed operation is deemed self-inverse operation.

Proposed Key Generation Process

In both decryption and encryption operations, the ciphering key forms the core algorithm to generate sub-keys that need to be kept secret. The ciphering key is a one-way algorithm that allows expanding the initial ciphering key to numerous sub-ciphering keys in a bid to encompass all the rounds. Two complex functions (F and g) were employed to establish the generated cipher key and these functions almost similarly with few minor differences as presented in Fig. 4.

State array of 4*4 byte was received by Function (F), which implemented certain operations on the last word (4-byte). Three simple operations are involved with function (F): subbyte based on the C-Box table, then consider the word's 1st complement and lastly XORed with constant vector1 (b7e15163) as the base natural logarithm. For the Function (g): subbyte based on the C-Box table, rotate towards the right along with cyclic shifting pertaining to the word, XORed with constant vector2 (b7e15163) as a golden ratio.

The two constant vectors were employed, while concatenation of the golden ratio and base natural logarithm vectors were done with forward & backward operations. The key expansion algorithm totally relies on the complex functions to remove weak and semi-weak keys and completing the symmetric loop pertaining to the key generation process.

The complex functions are aimed at avoiding the steps in the reverse internal algebraic operations and establish an intractable procedure that would allow analyzing the internally correlated ciphertext. Identical state array of 4*4 byte is received by Function (g) but includes a vertical orientation as well as implementation of certain simple operations on the first word (4-byte). State array of 4*4 for the generated sub-keys of function (F) are twisted and exchange the columns in different order for the state array of Function (g). The exchanging of column order for the state array increase the randomness and the diffusion property for the whole ciphering keys along all rounds.

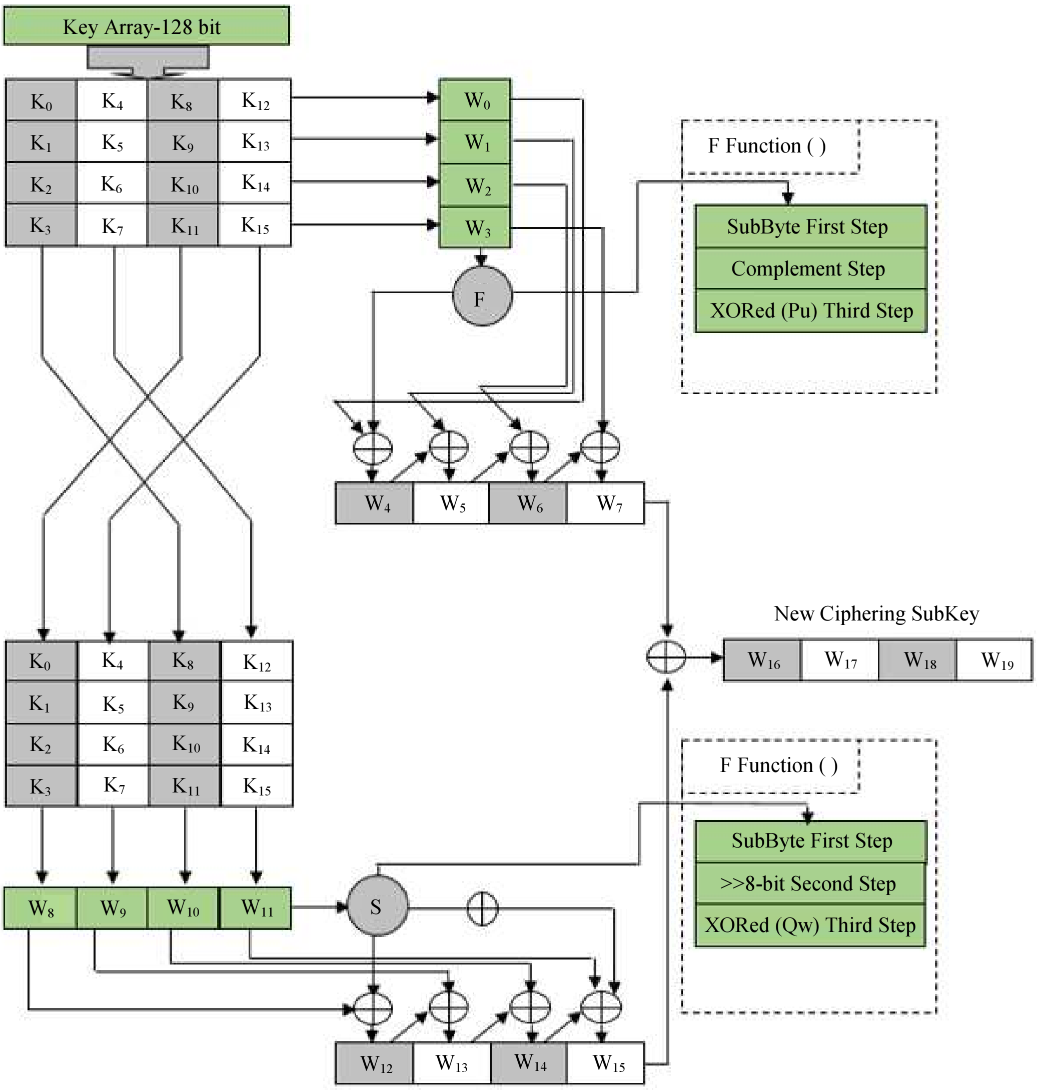

Fig. 4: Key generation algorithm with two complex functions (F1 and F2)

Analysis and Security Investigation

The key concept behind the put forward design is to establish high confidentiality level as well as effective implementation even when there are constrained resources of hardware that work on different platforms and meet both the present and future needs. To deal with malicious attacks, the put forward cipher employs a coherent internal structure that includes a solid algebraic expression. For each stage, the round transformation is constructed precisely to provide robust encryption layers.

In the first stage, C-Box is built by accounting for high algebraic complexity as well as non-linearity to safeguard against linear and differential attacks. The non-linear stage or the subbyte layer define the strength of any cipher design and is regarded crucial for any algorithm. The design of C-Box is based on the maximum output and input correlation as well as ensuring that the maximum difference propagation probability is kept as small as possible. The put forward C-Box stage employs the polynomial of GF(2^8) that is regarded as polynomials possessing a degree that is smaller than eight of coefficients GF(2).

The construction of C-Box is done as a series of compact affine transformations that have a complicated algebraic notation. In backward and forward affine transformations, the two constant vectors and value 00 do not map onto their own value. This suggests that mounting of interpolation attacks is not possible since these do not impact the non-linearity characteristics.

The algorithm that has been recommended constitutes of a strong, robust and satisfactorily long ciphering key, which can withstand most of the commonly known practical attacks. The propagation trail of the algorithm generally cannot be exploited due to the presence of the internal complex (F) functions, as is the case with algorithms with less number of rounds that get impacted by attacks like the square attack. With due consideration of the practical and theoretical attacks, the proposed C-Box is adopted to be a solid wall since it impacts the entire structure of the algorithm.

Table 3, 4 and Fig. 5 show consequences of the implementation time for the AES and the proposed cipher according to several metrics. The proposed algorithm tested with Windows-10 Pro 64-bit, Intel (R) Core-i7 Tm, with HD graphics 5500-CPU, 2.40 GHz, NVIDIA GEFORCE 820m and with the Visual Studio 2013, C# programming language.

The second phase is dependent on the symmetry of the Zigzag-shifting steps that decrease the cost of the Gate Equivalent (GE). It also improves the diffusion property in order to overcome the saturation attacks. The third phase constitutes of the P-Box or Super-Mixing operation that is an MDS form based linear equation, which renders additional confusion and diffusion to the ciphertext, making it even more incomprehensible.

The selection of the suggested MDS matrices is made from the best linear equations of order four. The main objective for selecting MDS was to develop a balance in the internal operations of the linear and non-linear layers and minimize the disparities in the encryption and decryption processes. The last phase involves the inclusion of the secret key to the ciphertext for every round that balances the key expansion or the key scheduling function. To counter the slide attack and to hold sufficient working memory, the key generation algorithm obtains the cipher key using the symmetry round transform. The constant vector and certain simple operations support the key expansion that is necessary to eradicate the probability of the occurrence of weak and semi-weak keys.

The inadequacies of the suggested cipher are that there is involved a certain amount of delay in time implementation in the decryption process. Additionally, in the encryption and decryption processes using the same algorithm, there is no existence of any involutional symmetric structure. The symmetry operation comprises the involutional phases in backward and forward operations that use the same code and implementation. A number of arbitrary statistical tests are executed for the suggested cipher and a realistic result is obtained without any deviation during the course of the testing procedure. An accurate and thorough analysis is required for the suggested cipher structure parts, along with critical scrutiny from designers and analysts to assess the hidden vulnerabilities and disseminate the practical attack. I would be grateful for accepting the advantages and disadvantages resulting from evaluation of the proposed cipher and I would be pleased to accept any scientific criticism which helps improve the work.

Table 3: Comparison between the proposed cipher and AES algebraic properties

Algebraic properties	Proposed Cipher	AES Cipher
Non-Linear Stage		
Correlation Immunity	Zero	Zero
Algebraic Degree	Seven	Seven
Algebraic Complexity	253/255	9/255
Bijection	Yes	Yes
Strict Avalanche Criteria (SAC)	1/2	1/2
Non-Linearity	114	112
Differential Uniformity	4	4
Power Mapping	Complement-Affine	Direct-Affine
Zigzag-Shifting Stage		
Diffusion	Optimal	Optimal
Invertibility	Zigzag-Shifting	Cyclic-Shifting
Offset Positions	x = (x + n) % n	
y = (y + n) % n	(i,j)= (J + C_i) mod Nb	
Super-Mixing Stage		
Dimension-Degree	4-Bytes	4-Bytes
Linearity	Modulo (X^4 +1)	Modulo (X^4 +1)
8-Bit Process	Sum of Power (02) with	Sum of Power (02) with
32-Bit Process	recursive multiplication	X-time Function
Key-Addition Stage		
Constant Vector	Pw/Qw Two Const. Vectors	Fixed-Rcon-Table
Symmetric Elimination	Non-weak key	Non-weak key
S-Box Dependency	Yes	Yes
Key Scheduling	Duplicated-Key	Single-Key

Table 4: Different evaluation metrics between the AES and the proposed cipher

Block Cipher Algorithm	Code Size	GE-Gate Equivalent Estimation	Enc/Dec (Cycles)	Key Setup (Cycles)	Minimum of Memory Requirements
Proposed 128-bit	3795	3625 GE	75592	33975	512
AES 128-bit	3780	3400 GE	73856	32764	512

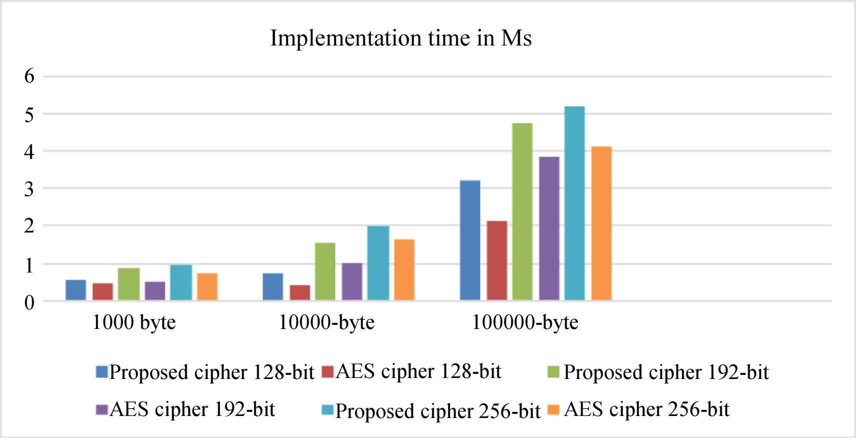

Fig. 5: Time implementation comparison between the proposed cipher and the AES

Conclusion

A new symmetric algorithm with a robust mathematical composition and an elegant structure has been introduced in this paper. The suggested symmetric cipher model is made up of a new block cipher design where the data block of 128-bit is encrypted with three variable robust ciphering keys. An efficient implementation of the recommended cipher design constitutes of a high-margin of security and is in line with the conventional design.

The proposed cipher is developed securely in order to meet the encryption requirements for the Bitcoin wallets database and the cryptocurrencies applications. This cipher is a byte-oriented cipher that is constructed for general-purpose algorithms and is also suitable for large-scale applications. To counter most modern practical attacks, the design of the cipher is improved using an iterated complex round transformation that supports strong ciphering key and solid algebraic construction.

Acknowledgement

The authors would like to apply special thanks to Mr. Khaled Qais for his great contribution in editing and proof reading this paper from a linguistic point of view.

Author’s Contributions

All authors have submitted equally contribution in this research.

Ethics

This article is unpublished and contains original works that have not been published elsewhere, nor are currently under consideration in any other refereed journal. The corresponding author confirms that the coauthor has read and approved the manuscript and there are no ethical issues involved.

References

Aljosha, J., 2017. Blocks and Chains, Introduction to Bitcoin, Cryptocurrencies and Their Consensus Mechanisms. 1st Edn., Morgan and Claypool.

Andreas, M.A., 2015. Mastering Bitcoin, Unlocking Digital Cryptocurrencies. 1st Edn., O’Reilly Media, Inc.

Bitcoin Wiki-BIP 0032, 2012. BIP 0032-bitcoin wiki. BitcoinWiki. https://en.bitcoin.it/wiki/BIP_0032

BitcoinWiki, 2016. Base58Check encoding-Bitcoin Wiki. https://en.bitcoin.it/wiki/Base58Check_encoding

Bunjaku, 2017. Cryptocurrencies-advantages and disadvantages. J. Economics.

Daemen, J. and V. Rijmen, 2001. The Wide Trail Design Strategy. In: Cryptography and Coding, Honary, B. (Ed.), Springer, Heidelberg, pp: 222-238.

David, L. and K. Chuen, 2015. Handbook of Digital Currency Bitcoin, Innovation, Financial Instruments and Big Data. 1st Edn., Elsevier Inc.

Dawood, O.A., A.S. Rahma and A.J.A. Hossen, 2015a. The new block cipher design (Tigris cipher). Int. J. Comput. Netw. Informat. Security, 7: 10-18. DOI: 10.5815/ijcnis.2015.12.02

Dawood, O.A., A.S. Rahma and A.J.A. Hossen, 2015b. The euphrates cipher. Int. J. Comput. Sci. Issues, 12: 1694-1694.

Dawood, O.A. A.S. Rahma and A.J.A. Hossen, 2015c. New symmetric cipher Fast Algorithm of Revertible Operations' Queen (FAROQ) Cipher. Int. J. Comput. Netw. Informat. Security, 9: 29-36. DOI: 10.5815/ijcnis.2017.04.04

Dawood, O.A., A.M. Sagheer and S.S. Al-Rawi, 2018. Design Large Symmetric Algorithm for Securing Big Data. Proceedings of the 1st International Conference on the Developments in eSystems Engineering, (DEE' 18), Cambridge, England, UK, DOI: 978-1-5386-6712-5/18/$31.00

FRANCO, P., 2015. Understanding Bitcoin Cryptography, Engineering and Economics. 1st Edn., John Wiley and Sons Ltd, Pedro Franco.

Gallagher, P.D. and C. Romine, 2013. FIPS PUB 186-4 Digital Signature Standard (DSS).

Ivaschenko, A.I., 2016. Using Cryptocurrency in the activities of Ukrainian small and medium enterprises in order to improve their investment attractiveness. Problems Economy, 3: pp: 267-273.

Karame, G. and E. Androulaki, 2016. Bitcoin and Blockchain Security. 1st Edn., Artech House.

Matthew, D.S., A.P. Lauf and R. Yampolskiy, 2015. Bitcoin message: Data insertion on a proof-of-work cryptocurrency system. Proceedings of the International Conference on Cyberworlds, Oct. 7-9, IEEE Xplore Press, Visby, Sweden, DOI: 10.1109/CW.2015.56

Melanie, S., 2015. Blockchain Blueprint for a New Economy. 1st Edn., Published by O'Reilly Media, Inc.

Mike Caldwell-BIP 0038, 2012. BitcoinWiki. BIP 0038-BitcoinWiki. https://en.bitcoin.it/wiki/BIP_0032

Miraje, G., 2016. TrustZone-backed Bitcoin Wallet. Master Thesis, to obtain the Master of Science Degree in Electrical and Computer Engineering.

Nakamoto, S., 2008. Bitcoin: A peer-to-peer electronic cash system. http:// bitcoin.org/ bitcoin.pdf

Sagheer, A.M. S.S. Al-Rawi and O.A. Dawood, 2011. Proposing of developed Advanced in Encryption Standard AES. Proceedings of the 4th International Conference in Developments in E System Engineering (ESE' 11), Dubai. pp: 197-197. DOI: 10.1109/DESE

Szmigielski, A., 2016. Bitcoin Essentials Gain insights into Bitcoin, a Cryptocurrency and a Powerful Technology, to Optimize your Bitcoin Mining Techniques. 1st Edn., Birmingham-Mumbai.