MULTI-OPERATION DATA ENCRYPTION MECHANISM USING DYNAMIC DATA BLOCKING AND RANDOMIZED SUBSTITUTION

IJAZ ALI SHOUKAT

UNIVERSITI TEKNOLOGI MALASIA

MULTI-OPERATION DATA ENCRYPTION MECHANISM USING DYNAMIC DATA BLOCKING AND RANDOMIZED SUBSTITUTION

IJAZ ALI SHOUKAT

A thesis submitted in fulfilment of the
requirements for the award of the degree of
Doctor of Philosophy (Computer Science)

Faculty of Computing
Universiti Teknologi Malaysia

MARCH 2016

Specially dedicated to Holy Prophet Hazrat Muhammad (P.B.U.H)

ACKNOWLEDGEMENT

On completion of my PhD Thesis, I significantly gratified and grateful to **"**Allah**"** Who endowed this passionate and flourishing occasion in my life. Furthermore, I appreciate the devoted and continuous support of my parents and family members in my entire academic pursuits.

Immensely, I would like to express my special and enthusiastic gratitude to my respected Supervisor *Professor Dr. Kamalrulnizam Abu Bakar* who prop up me in my thesis with technical directions, creative suggestions and supportive criticisms in order to polish my research abilities. I always found him encouraging, compassionate and sincere upon each request and query. I found myself repeatedly assisted with his professional and scientific exposure throughout the PhD program. I will forever be thankful to him for his fundamental and vital role in the completion of my degree.

Moreover, I greatly appreciate the support my co-supervisor *Associate Prof. Dr. Subariah Ibrahim* for her valuable guidelines and research directions related to the proposed idea. I am really thankful to her for the constant and technical collaboration in my PhD degree. I am also indebted to Faculty of Computing at Universiti Teknologi Malaysia (UTM) for facilitating luxury opportunities to international students to gain the knowledge of science and technology. I am also thankful to all of my teachers who taught me from class one to PhD level and trained me to compete with hurdles for achieving the complex goal of success.

ABSTRACT

Existing cryptosystems deal with static design features such as fixed sized data blocks, static substitution and apply identical set of known encryption operations in each encryption round. Fixed sized blocks associate several issues such as ineffective permutations, padding issues, deterministic brute force strength and known-length of bits which support the cracker in formulating of modern cryptanalysis. Existing static substitution policies are either not optimally fit for dynamic sized data blocks or contain known S-box transformation and fixed lookup tables. Moreover, static substitution does not directly correlate with secret key due to which it has not been shown safer especially for Advanced Encryption Standard (AES) and Data Encryption Standard (DES). Presently, entire cryptosystems encrypt each data block with identical set of known operations in each iteration, thereby lacked to offer dynamic selection of encryption operation. These discussed, static design features are fully known to the cracker, therefore caused the practical cracking of DES and undesirable security pitfalls against AES as witnessed in earlier studies. Various studies have reported the mathematical cryptanalysis of AES up to full of its 14 rounds. Thus, this situation completely demands the proposal of dynamic design features in symmetric cryptosystems. Firstly, as a substitute to fixed sized data blocks, the Dynamic Data Blocking Mechanism (DDBM) has been proposed to provide the facility of dynamic sized data blocks. Secondly, as an alternative of static substitution approach, a Randomized Substitution Mechanism (RSM) has been proposed which can randomly modify session-keys and plaintext blocks. Finally, Multi-operation Data Encryption Mechanism (MoDEM) has been proposed to tackle the issue of static and identical set of known encryption operations on each data block in each round. With MoDEM, the encryption operation can dynamically be selected against the desired data block from the list of multiple operations bundled with several sub-operations. The methods or operations such as exclusive-OR, 8-bit permutation, random substitution, cyclic-shift and logical operations are used. Results show that DDBM can provide dynamic sized data blocks comparatively to existing approaches. Both RSM and MoDEM fulfill dynamicity and randomness properties as tested and validated under recommended statistical analysis with standard tool. The proposed method not only contains randomness and avalanche properties but it also has passed recommended statistical tests within five encryption rounds (significant than existing). Moreover, mathematical testing shows that common security attacks are not applicable on MoDEM and brute force attack is significantly resistive.

ABSTRAK

Sistem kripto yang sedia ada berhubung kait dengan ciri-ciri reka bentuk statik seperti sekatan data bersaiz tetap, statik penggantian dan penggunaan set yang sama dalam operasi enkripsi bagi setiap pusingan enkripsi. Sekatan bersaiz tetap dikaitkan dengan beberapa isu seperti permutasi yang tidak berkesan, isu-isu *padding*, ketentuan kekuatan kuasa kasar dan panjang yang dikenali bagi bit yang dapat menyokong penceroboh di dalam menggubal analisis kripto moden. Dasar-dasar penggantian statik sedia ada adalah sama ada tidak bersesuaian secara optima untuk blok-blok data bersaiz dinamik atau kandungan yang dikenali sebagai transformasi kotak-S dan jadual carian tetap tanpa berhubung langsung dengan korelasi bersama kunci rahsia. Disebabkan oleh hal yang demikian, dasar-dasar ini menunjukkan tidak selamat terutamanya untuk Piawaian Penyulitan Lanjutan (AES) dan Piawaian Penyulitan Data (DES). Sehingga kini, keseluruhan sistem kripto menyulit setiap blok data dengan set yang serupa dalam operasi yang diketahui bagi setiap lelaran, sekali gus kurangnya penawaran pilihan operasi penyulitan yang dinamik. Melalui perbincangan ini, ciri-ciri reka bentuk statik adalah serba diketahui oleh penceroboh, sehingga menyebabkan pencerobohan praktikal oleh DES dan kesulitan keselamatan yang tidak diingini terhadap AES seperti yang dibuktikan dalam kajian sebelum ini. Pelbagai kajian telah melaporkan bahawa analisis kripto secara pendekatan matematik pada AES sehingga 14 pusingan keseluruhannya. Oleh itu berdasarkan situasi ini cadangan pendekatan reka bentuk dinamik pada sistem kripto simetri diperlukan. Pertamanya, Mekanisme Sekatan Data Secara Dinamik (DDBM) telah dicadangkan untuk menyediakan kemudahan blok bersaiz dinamik sebagai pengganti kepada sekatan data bersaiz tetap. Kedua, Mekanisme Penggantian Rawak (RSM) telah dicadangkan sebagai altenatif kepada pendekatan penggantian tetap untuk mengubah kunci-sesi dan blok teks biasa secara rawak. Akhirnya, Mekanisme Pelbagai Operasi Penyulitan Dinamik (MoDEM) telah dicadangkan untuk mengatasi perlaksanaan tetapan set bagi operasi penyulitan di setiap blok data dalam setiap pusingan. Melalui MoDEM, operasi penyulitan boleh memilih blok secara dinamik daripada senarai pelbagai operasi yang digandingkan dengan beberapa sub operasi. Kaedah atau operasi seperti eksklusif-OR, 8-bit pilih atur, penggantian rawak, syif kitaran dan operasi logik telah digunakan. Penilaian eksperimen menunjukkan bahawa DDBM boleh menyediakan blok data bersaiz dinamik jika dibandingkan dengan pendekatan yang sedia ada. Kedua-dua RSM dan MoDEM telah memenuhi sifat kedinamikan dan kerawakan seperti yang diuji dan disahkan mengikut piawaian analisis statistik yang disarankan. Kaedah yang dicadangkan bukan sahaja mempunyai sifat-sifat rawak dan runtuhan malah ia telah melepasi ujian statistik yang disarankan dalam tempoh hanya lima pusingan sahaja (ketara berbanding dengan sedia ada). Tambahan pula, ujian matematik menunjukkan bahawa serangan keselamatan biasa tidak berkaitan degan MoDEM dan serangan kuasa kasar adalah lebih ketara rintangannya.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

AES	–	Advanced Encryption Standard
AVG	–	Average
BFS	–	Brute Force Strength
DBAV	–	Data Block Average Value
DCA	–	Differential Cryptanalysis
DDBM	–	Dynamic Data Blocking Mechanism
DES	–	Data Encryption Standard
DMA	–	Data Modification Algorithm
FDBM	–	Fixed Data Blocking Mechanism
IETF	–	Internet Engineering Task Force
ISO	–	International Standard Organization
KBDV	–	Key Block Decimal Value
LBMA	–	Last Block Management Algorithm
LFSR	–	Linear Feedback Shift Register
MoDEM	–	Multi-operation Data Encryption Mechanism
NIST	–	National Institution of Standard and Technology
OP CODE	–	Operation Code
RSM	–	Randomized Substitution Mechanism
RXOR	–	Reverse Exclusive OR
SKGMA	–	Session Key Generation and Mixing Algorithm
SPN	–	Substitution-Permutation Network
STS	–	Statistical Testing Suite
TDES	–	Triple Data Encryption Standard
XOR	–	Exclusive OR

LIST OF SYMBOLS

DB	–	Data Blocks
B	–	Bits
μ	–	Number of bits of each block
β	–	Number of data blocks
$\mathcal{BL}_x$	–	block length
K	–	Initial Master Secret Key
ΔK	–	Session Key
D	–	Plaintext
$\acute{C}$	–	Cipher Text
μ	–	Number of block bits
$\mathcal{P}$	–	Probabilistic Randomness
$\exists DB$	–	Encrypted Data Block
DB^{av}	–	Data block Average Value
K_{β}^{DV}	–	Key Block Decimal Value
$\in$	–	Belongs to
$\neq$	–	Not equal to
$\Rightarrow$	–	Implies that
ΔD	–	Chosen Plain Text
$\Delta\acute{C}$	–	Chosen Cipher Text
$ßD$	–	Known Plain Text
$\oplus$	–	Exclusive XOR
$\ddot{\ominus}$	–	Reverse (RXOR)

LIST OF APPENDICES

CHAPTER 1

INTRODUCTION

1.1 Overview

Security is the major driving force for remote communication. Security against confidential transactions cannot be compromised over insecure communication channels. Variety of cryptosystems persist to offer encryption heuristics for such kind of transactions but the question of security strength of underlying algorithm matters against cryptanalysis attacks. Cryptanalysis is a way of breaking cryptographic algorithms using analytical reasoning, pattern locating, guessing and statistical analysis approaches as discussed in (Ayushi, 2010). Exhaustive key searching is commonly used, efficient and successful attack to defeat the security strength of any cryptographic algorithm discussed by Jarvinen (2008). Therefore, differential cryptanalysis, exhaustive key searching, shortcut attacks and side channel attacks are creating anxious and perilous scenario for remote communication. It is too critical to remain competitive in forgoing market with data privacy and security without the science of cryptography. Currently, symmetric cryptosystems are prime heuristics in designing of secure cryptosystems (Yadav, 2010) with several benefits such as short key length, computational efficiency and less memory consumption as compare to asymmetric cryptosystems (Rejani and Krishnan, 2015). Symmetric cryptosystems associate several noteworthy parameters such as fixed data blocking (FIPS Pub 46; Jain *et al.,* 2015), static substitution and fixed set of identical enciphering operations on each data block (Saini, 2014; Abdulgader *et al.,* 2015), which trigger actual security vulnerabilities (Biryukov *et al.,* 2014) for cryptosystems and play the vital role in the successfulness of modern

attacks as reflected through many studies against advanced encryption standard (Alex and Johann, 2012; Derbez *et al.,* 2013; Bogdanov *et al.*, 2014; Chang *et al.,* 2015; Gangadari *et al.,* 2015).

Existing well-known encryption algorithms such as Advanced Encryption Standard (AES) and Data Encryption Standard (DES) are reliant on a reality of fixed data blocking (FIPS Pub 46; Chavan and Annadate, 2015) which means the block size (bit length) is not dynamic, fully known and total number of blocks against a plain text are also known before initiating encryption phase. AES deals with 8 bit static substitution and 128 bit fixed data blocking (Senthilkumar and Rajamani, 2014; Abdulgader et al., 2015). Similarly, DES contains 64 bit fixed block size (Jain et al., 2015). In existing algorithms (e.g. AES), each time fixed set of known and identical encryption operation are applied to encrypt data (Srinivas et al., 2014; Kaur and Madaan, 2014; Dara and Manochehri, 2014; Saini, 2014) which means there is no multi-operation based dynamic enciphering. Existing dynamic substitutions approaches have been designed to work with fixed-sized data blocking approaches (See Chapter 2, Section 2.7) due to which it cannot fit with dynamic natured ciphers which contains dynamic features such as dynamic data blocking, randomized substitution, dynamic selection of encryption opertions. The knowledge of block sets and fixed sizes are increasingly beneficial for any cryptanalyst to possibly crack any symmetric encryption algorithm (Biryukov *et al.,* 2014; Gangadari *et al.,* 2015). Static substitution causes less random permutation and is the primary weakness of existing block ciphers (Ritter, 1998; Mehla and Kaur, 2014) which means just to increase processing computational ability that can easily be defeated in current era's based high computing processors. In this situation, the practical cracking of DES (Biryukov *et al.,* 2010) and academic (theoretical) cracking of all AES versions are noteworthy (Biryukov *et al.,* 2009; Biryukov and Großschäd, 2012; Chang *et al.,* 2015).

Moreover, the AES security strength is not as stronger as it is believed or conveyed (Biryukov *et al.,* 2010). The 4 rounds of AES-128 requires 2^{17} time with 2^{16} data complexities and 5 rounds takes 2^{38} time and 2^{40} data complexities which become 2^{90} time with 2^{64} data complexities against 6 round of AES-128 (Tiessen *et*

al., 2015). On 8 rounds of AES-192 and AES-256, the key recovery attack takes 2^{172} and 2^{196} time complexities respectively which give overall 2^{107} chose plaintext complexity with 2^{96} memory lookup trails as well as 9-rounds based key recovery attack requires 2^{120} chosen plaintext complexity with 2^{203} memory lookup trails on AES-256 (Derbez *et al.* 2013). The 10, 11 and full 14 rounds of AES-256 are also vulnerable against modern attacks (Biryukov *et al.*, 2009a; Biryukov *et al.*, 2010; Lu, 2010; Bogdanov *et al.*, 2011; Bogdanov *et al.*, 2014; Chang *et al.*, 2015). *Lu* (2010) claimed, AES has lowest impossible-boomerang-attack computational complexity (2^{56}) and according to *Biryukov* the quasi-practical attack takes only 2^{70} time traces to recover 11 rounds of AES-256 with 2^{45} time complexity having 2^{33} memory lookups and 2^{44} data complexity trials. This gives almost practical cracking complexity of ($q.2^{67}$) queries against full rounds of AES-256. Furthermore in year 2014 and 2015 the cryptanalysis of full rounds of AES remained carry on with further improvements. For full rounds of all AES versions (AES-128, AES-192 and AES-256), the latest and outperformed attack complexities ($2^{125.56}$, $2^{189.51}$ and $2^{253.87}$) have been found respectively (Bogdanov *et al.*, 2014). The large scale machine (hardware) based attacks are also feasible on AES-128 and AES-256 which can be applied with time complexity of 2^{100} search trails (Biryukov and Großschäd, 2012). The hashing based biclique-cryptanalysis of AES-128 was conducted by change *et al.*, (2015) and he observed that attack complexities lie between $2^{126.3}$ up to $2^{127.4}$ search trails. Thus, the critical literature findings show that full rounds of all AES versions are vulnerable to modern cryptanalysis attacks and overall discussion made in this section triggers the need of significant design parameters such as dynamic data blocking rather to fixed data blocking, randomized substituion rather to static substitution and dynamic selection of encryption operations as compare to static and identical selection of encryption operations in symmetric cryptosystems to encrypt data.

1.2 Problem Background

This section discusses the problem background which has been divided to three sub-sections. Each sub section highlights and discusses the related issues.

1.2.1 Fixed Data Blocking

Existing well-know symmetric cryptosystems (AES, DES, TDES) use fixed sized data blocks (FIPS Pub 46; Mehla and Kaur, 2014; Jain *et al.,* 2015) with Substitution-Permutation Network (SPN) or Feistel cipher structure (Tu *et al.,* 2015) which means they did not create dynamic sized blocks. Due to the lack of dynamicity in data blocking, the fixed sized block parameters help the cracker in cryptanalysis inspection as discussed by Biryukov *et al.,* (2014), in case of Feistel based block ciphers (SIMON and SPECK), he considered four differential (d_1, d_2,….d_4) to recover key of SIMON32 through constructing of one set of 2^{23} fixed plaintexts blocks (each with 9 bits) and he was succeed to locate several plaintext pairs 2^{25} for each differential (d_i). In case of 4 key guess approach upon 2 ciphered rounds, to locate $2^{30.5}$ plaintext pairs, the achieved complexity was $\{2^{33.5} * 4* (2/29)\} \approx 2^{32}$ which gives ultimate 2^{34} computational complexity to apply full key recovery attack. Moreover as compare to the random permutation on fixed or same sized (length) blocks, the differential attacks always provide larger differential probability for cryptanalysis (Lu, 2008; Lu, 2010) which has reflected the full cracking of all AES versions (128, 192, 256) with computational complexities trails $2^{125.56}$, $2^{189.51}$ and $2^{253.87}$ respectively (Bogdanov *et al.,* 2014) because AES also uses fixed sized data blocking. Several other studies about the cryptanalysis of AES are the part of literature (Une and Kanda , 2007; Biryukov *et al.,* 2009; Alex and Johann, 2012; Derbez *et al.,* 2013; Chang *et al.,* 2015).

Other significant issue is that, the secret sub-keys of fixed sized block based SPN structure can be recovered (Guo *et al.,* 2014) and SPN also associates the discrepancy in linear cryptanalysis and its secret design can be re-produced by matching of cipher and plaintext values each with 16 bits as discussed in (Brown *et al.,* 2009; Rivain and Roche, 2013). Thus, it truly reflects the literature that the fixed length blocks support the cracker in matching of supposed decrypted string (block) with the targeted chosen plaintext string to get accurate final results. Another noteworthy problem with fixed (known) length block is the brute force attacking because any chosen fixed sized block means that same sized key is implemented due

to which the brute force attack is more likely and effectively to be applicable as explained in Table 1.1.

Table 1.1: Randomness Comparison between Dynamic and Static Data Blocking

Factors	**With Prior Fixed Data Blocking Mechanism of (DES, AES-128)**	**With Proposed Dynamic Data Blocking Mechanism**
Probabilistic Randomness Calculation	Suppose, Plaintext (D) = 2048 bits. Blocking with AES-128= 2048/128= **16** blocks, So Number of Data Blocks (β) = 16 Number of bits of each block(μ) : 128 bits Probabilistic Randomness Calculation Formula: $\beta * 2^{\mu \text{ bits}}$ where For each single block= $1* 2^{\mu \text{ bits}}$ β is fixed = 16 in supposed case **μ** is fixed = 128 in supposed case So, $16 * 2^{128 \text{ bits}}$ The condition (P≠NP) is not satisfied. because each parameter is known and fixed	Suppose Plaintext (D) = 2048 bits Number of Data Blocks are based on Random (dynamic) parameter (say) = ₱(β) Number of bits of each block are based on Random (dynamic) parameter (say) = ₱(μ) bits Probabilistic Randomness Calculation Formula: $₱(\beta)* 2^{₱(\mu) \text{ bits}}$ Where ₱(β) is random ₱(μ) is random As these are unknown to the cracker. So it is quite hard for the cracker to guess it. So (P≠NP) is effectively satisfied because both parameters (β,μ) are un-known and random.
Result of guessing of block partitioning	Weak and guessable	hard to guess

Research Gap: Furthermore, in existing literature there is gap of dynamic block ciphers because AES, DES are fixed-natured ciphers having fixed data blocking (Jain *et al.,* 2015), fixed substitution (Dara and Manochehri, 2014) and fixed selection of encryption operation for each encryption round (Shyamala-Bai, *et al.,* 2011; Srinivas *et al.,* 2014). Rather to dynamic-natured ciphers, either fixed-natured or few variable-natured block ciphers exist which did not deal with dynamic data blocking approach, neither with effective randomized substitution nor with dynamic selection of encryption operations for each round such as RC5 (Rivest, 1995) which utilizes three fixed and known variable block sizes (32, 64, 128 bits)

and similarly the Rijndael (Daemen and Rijmen, 2002) has also three fixed and known block sizes (128,192,256 bits). User can select any of block size from the 3 available options. These block sizes are publically known, variable in nature but not dynamic in nature. The Modified Symmetric Encryption Algorithm (MSEA) (Kumar *et al.,* 2014) provides large block size selection list (128, 192, 216, 256…728, 936, 1024, 1384, 1712, 2048 bits) these are also fixed and publically known. Therefore, MSEA also provides fixed and known variable block sizes which are not dynamic in nature. In case of MSEA the many block size options (728, 936, 1024, 1384, 1712, 2048 bits) are inadequate because the block size range that has been used in recent well-known algorithms (DES, AES) lies among (64, 128, 256 bits) which means the block size larger to 256 bit is not a recommended approach. Many other ideas of dynamic encryptions are either based on dynamic Steganography approach with fixed block size (Sawant *et al.,* 2015) or variable blocking using dynamic key (Shyamala-Bai *et al.,* 2011) or pair of keys (static and dynamic) with fixed block size (Harmouch and Kouch, 2015) which means their data blocking approach is not dynamic.

The variable block partitioning policy of Message Based Random Variable Length Key Encryption Algorithm (MRVLK) (Mirvaziri *et al.,* 2009; Davahli *et al.,* 2014) is based on a secret number ranged from (R_{nd}: 7 to 61) in which initial (very first) block size is decided in between 7 to 61 and other block sizes become arbitrary longer in such a way: ($R_{nd,}$ $2R_{nd,}$ $4R_{nd,}$ $6R_{nd}$ ……). But, MRVLK has several discrepancies such as, it's very first *small-sized* block (Mirvaziri *et al.,* 2009) for which DES like weak block attacks are permissible (Minematsu, 2008; Paar and Pelzl, 2010) or arbitrary longer blocks even greater to 720 bits (un-recommended), fixed padding, and its non multiple of 8 bit block size is not feasible for disk encryption (Zhang, 2012) as well as its non-secure enciphering and randomness limitations (Davahli *et. al.,* 2014). Thus, the critical literature analysis shows that, the variable data blocking solution of MRVLK has been found deficient in block length, disk encryption, enciphering strength, padding, cryptanalysis *etc.* and all other prior variable solutions contain fixed block sizes which is also known to the cracker.

Concussively, fixed sized blocking (AES, DES) and fixed padding are more helpful (Biryukov *et al.,* 2014) for cracker in succeeding of exhaustive key searching attack (brute-force attack) (Du and Atallah, 2001), reaction attack (Bellare *et al.,* 2004), biclique attack (Chang *et al.,* 2015) as well as other cryptanalysis attacks on AES (Bogdanov *et al.,* 2014; Guo *et al.,* 2014). Random padding is fine but not always especially in case if block size is fixed or known (e.g. 128 bit in AES) because if the random padding (e.g. 16 bits) has been used with 128 bits fixed block size which simply meaning that (128-16 = 112 bits) resulting many bits (112 bits) as a "waste bits" in cipher-text (*C*) due to which attacker can recover secret key bits through matching all possible keys ($K \in K'$) until block cipher ($E^{-1}_{K'}(C)$) starts with 112 zeros (Black and Rogaway, 2002), thus random-padding also provides trapdoor to render the algorithms vulnerable through back-door of an encryption key (Russell *et al.,* 2015). Variable-input-length (VIL) based cipher designs associate several issues such as infeasibility of encrypting disk sectors, weak security strength with smaller sized message, fixed padding, known-bit and weak block attacks (Bellare and Rogaway, 1999; Patel *et al.,* 2005; Zhang, 2012; Nandi, 2014) that demand the improvement in data blocking approach with dynamic features such as block size should be dynamic rather to fixed or variable, must be multiple of 8 without fixed padding, not greater than 256 bits, and must not be known to the cracker.

1.2.2 Static Substitution

The existing S-box design of AES is static (fixed) and un-changeable (Dara and Manochehri, 2014). Therefore, the static substitution policy of AES is its weak point (Mehla and Kaur, 2014; Abdulgader *et al.,* 2015) because of happening of static connection with input and output bits due to which AES has no direct association with secret key that is the only changeable parameter (Senthilkumar and Rajamani, 2014). The modern attacks (linear and differential) ideally require known transformation of lookup tables (i.e. S-box) as agreed by Kazlauskas *et al.,* (2015). Moreover, Senthilkumar and Rajamani discussed that differential attacks are more applicable on static s-boxes because these attacks are based on the information of *XOR* tables produced against S-Boxes. The *XOR* table contains columns and rows starting with indexes $(0, 1, 2 \ldots\ldots 2^{m-1})$ against the related $(m \times m)$S-box which can

further mapped with *XOR* table entries $q,f \in (0, 1, 2 \ldots\ldots 2^{m-1})$ deal with position q , f having $\{value|(Z \in \{0, 1\}^m : S(Z) \oplus S(Z \oplus q) = f)|\}$. Thus, modern cryptanalysis attacks ideally demand fixed (static) relationship of input and output bits with S-boxes that prompt the need of key dependent randomized substitution policy (Senthilkumar and Rajamani, 2014). Furthermore, the substitution policy of AES is based on static numerical search tables which lead the AES to vulnerable against modern security attacks and have not been shown safe in terms of designing various cryptanalysis methods (Moreno-Diaz and Pichler, 2011; Gangadari *et al.,* 2015).

The linearity in static substitution is significant weakness of AES (Shyamala-Bai *et al.,* 2011; Sikdar, 2014) due which permutation produces only bit re-distribution which does not satisfies the sufficient diffusion properties (Ritter, 1998) because strength of algorithm and hindrance of cryptanalysis significantly relies on S-Box parameters (Jithendra and Shahana, 2015). The internal Substitution components of DES and AES (Sub-Bytes, Shift Column, ShiftRow) are insecure because they do not contain any correlation with secret key (Ramly *et al.,* 2001; Sreedharan, 2014) by itself and key is the only changing parameter (Senthilkumar and Rajamani, 2014). Moreover, the prior symmetric block ciphers implement substitution through look-up tables and look-up substitution tables (fixed S-Boxes) help the cracker (Saini, 2014; Kazlauskas *et al.,* 2015) and are more vulnerable upon timing attacks (Smith, 2007; Sahmoud *et al.,* 2013) therefore as a result, static substitution boxes should be eliminated from prior algorithms. Kocher *et al.* (2011) have claimed that the secret parts in symmetric cryptographic algorithms can be changed or masked under fresh randomness and if key state is updated on some random bases dynamically then it can be resulted as reasonably hard for adversary (attacker) to get useful secret information. Also, the dynamic substitution is significant area of improvement (Flamm, 2014) better to static s-box (ReddyK and Vishnuvardhan, 2014) and can enhance confusion (strength) properties (Kazlauskas *et al.,* 2015) of encryption algorithms which make them more difficult in cryptanalysis (Mirvaziri *et al.*, 2009; Hosseinkhani and Javadi, 2012; Saini, 2014; Velayutham *et al.,* 2015). Furthermore, the related (existing) substitution methods are deficient in many aspects (e.g. design, known parameters, feasibility *etc.*) as it has been discussed in Chapter 2. Thus, substitution should not be fixed and it should

be done against the probabilistic random values achieved from key. All these evidences negate the utilization of static (fixed) substitution in future cryptosystems.

1.2.3 Static and Identical Enciphering Operations

Each AES version has fixed number of multiple encryption rounds with repetition of identical (similar) operations having known strategies (Saini, 2014; Srinivas *et al.*, 2014; Kaur and Madaan, 2014) and last-round-attack can be applied on the final round of AES because this round does not apply mix-column operation (Tange and Andersen, 2014). AES encryption operations are publically well-known which is more serious aspect towards AES because the linear and differential attack always require known S-box transformation (Kazlauskas *et al.,* 2015) but on the other hand, the dynamic transformation which is not known to the cracker makes the algorithm more resistive against modern attacks (Al-Wattar *et al.,* 2015; Velayutham *et al.,* 2015). Moreover, each round in AES is identical and computationally feeble (Mirvaziri *et al.,* 2009) which are unclear to predict whether large number of rounds with fixed operations are really feasible to create strong enciphering as agreed by Ritter, (1998) in US Patient No. 5727062. Furthermore, existing enciphering designs (Feistel, SPN) are not reliably secure or suspected against various cryptanalysis attacks (Brown *et al.,* 2009; Isobe and Shibutani, 2013; Biryukov and Nikolic, 2014; Guo *et al.,* 2014). The other more surprising fact that reflecting the weakness of current enciphering mechanism is the cracking of DES (Franke *et al.,* 2005; Batina *et al.,* 2005; Zaidan *et al.,* 2010) and the cryptanalysis of AES (Biryukov *et al.,* 2009; Biryukov *et al.,* 2010; Biryukov and Großschäd, 2012; Derbez *et al.,* 2013; Chang *et al.,* 2015) which has been discussed in Chapter 2.

Security of any cryptographic algorithm is essentially reliant on randomness that can be achieved through probabilistic process (dynamicity) (Duta et *al.,* 2014). The term operational dynamicity means to select encryption operation run time on dynamic bases so that, it should not be aware to the cracker, which encryption operation has applied on which data block. This sort of operational dynamicity creates sufficient operational randomness because unpredictable information directly co-relates with pseudo-randomness (Sanjeev and Barak, 2008; Alimomeni, 2014).

Enhancing the randomness means enhancing the security of encryption algorithm (Al-Shakarchi, 2014). Poor, predictable and repeated randomness can be resulted as full security breakdown of cryptosystems (Ristenpart and Yilek, 2010; Alimomeni, 2014). Thus, for designing secure algorithms, randomness and dynamicity are the needy constraints because randomness enhances confusion to resist modern and common attacks (Cook, 2006; Mishra and Mankar, 2012). All these evidences prompt that the cryptographic algorithm is always as secure as it contains randomness and operational dynamicity. The solution to cope the issue of constant and static selection of encryption operations in prior algorithms (DES, AES) requires the need of dynamic selection of encryption operations by developing multi set of operations having sub-operations inside. This type of multiple operation development approach is known as design diversity approach and it can be achieved through joint committee of different sub-operations under a master encryption operation (Schneier, 1994). Currently, multi-encryption is the most focused area of development for symmetric cryptosystems (Harmouch and Kouch, 2015). Currently, there is a significant gap of this type of particular feature (i.e. dynamic selection of encryption operation for each data block) in existing literature.

1.3 Problem Statement

Fixed data blocking approach is inadequate to create effective dynamicity and larger computational probability due to which it helps the cracker in succeeding of modern attacks as witnessed in the literature. Static substitution approaches do not create sufficient diffusion (distribution of output bits) which depends on the input bits, but only within the scope of substituted number of bits and in this way the permutation is just bit re-distribution. Moreover, existing substitution approaches are either infeasible for dynamic sized data blocks or deal with known S-box formulations or lacked of direct association with encryption key or behaves as a trapdoor for building and succeeding of cryptanalysis attacks due the fixed relation of input and output bits. Similarly, the known selection of identical operations on each data block is not an optimal way of creating effective operational randomness under least number of encryption rounds. Thus, fixed data blocking, static

substitution and constant implementation of fixed set of known enciphering operations are the critical factors limiting the dynamicity and randomness in cryptosystems as reflected through mathematical cracking of AES-256 up to full of its14 rounds.

1.4 Research Questions

Prominent literature problems prompt the need to answer these several research questions.

i. How to improve fixed data blocking approach in symmetric cryptosystems with dynamic data blocking:-

   (a) How to achieve effective and dynamic sized data blocks?

   (b) How to avoid fixed padding and weak sized dynamic block even by fulfilling the condition of multiple of 8 bits?

ii. How effectively to enhance static substitution policy in symmetric cryptosystems with randomized substitution approach:-

   (a) How to achieve key-dependent randomized substitution?

   (b) How to enhance pseudo-randomness and dynamicity with randomized modifications in key and data?

iii. How to achieve effective and secure encryption in symmetric cryptosystems:-

   (a) How to use multi-encryption operations dynamically for each data block?

   (b) How to achieve effective data encryption (security) with least number of encryption rounds?

1.5 Research Aim

The aim of this research is to develop dynamic multi-encryption method by ‘improving’ fixed data blocking with dynamic data blocking, static substitution with randomized substitution and known operation based identical encryption approach with dynamic multi-encryption method to improve data encryption effectively.

1.6 Research Objectives

To answer the projected research questions, this study includes several objectives which potentially required to be accomplished as an optimal solution for the said problem.

i. To develop dynamic data blocking mechanism for converting the data to dynamic sized blocks in order to achieve effective dynamicity and larger computational probability.

ii. To develop a randomized substitution mechanism for mixing (key and Data) through dynamic modifications in order to achieve effective dynamicity and probabilistic randomness.

iii. To develop a multi-operation data encryption mechanism to select enciphering operation dynamically in order to achieve effective data encryption (security) with less number of encryption rounds.

1.7 Significance of the Study

Data security and privacy against confidential information are increasingly important in remote transactions over insecure communication channels. The encryption practices are actively employed in banking sectors, exchange of confidential data in academic organizations, medical sectors, storage of data in forensic and scientific laborites and securing of network communications. This study

is enriched with great significance of data encryption with optimal security. It provides an encryption method with dynamic design features such as dynamic data blocking, randomized substitution and multi-operation based dynamic enciphering mechanism. These features are an optimal way to enhance the security of data encryption method. Earlier encryption algorithms (DES, AES) possesses static design features in various stages such as data blocking, substitution and selection of enciphering operations which are seriously effecting the overall security of already deployed design ciphers (Feistel, SPN) as discussed in problem background section. These static features are not effectively sufficient to create dynamicity, larger probability and optimal randomness due to which the past cryptanalysis of DES and present academic cracking of AES are being more critical day by day. Thus, the proposed study is timely significant to improve the static design features with dynamic design features through development of dynamic data blocking, randomized substitution and multi-operation data encryption mechanism. The proposed idea is essentially important to boost the security of symmetric cryptosystems. Furthermore, the proposed idea is effectively innovative for the researchers to design future cryptosystems and highly beneficial for the academic researchers to evolve the cryptography research.

1.8 Research Scope

This study focuses on symmetric data encryption method for providing both data privacy and security upon confidential data. The proposed idea mainly covers the design and development of proposed encryption method which includes dynamic data blocking, randomized substitution and multi-operation data encryption mechanism. Furthermore the scope of this study covers:-

i. The different natured plaintext (alphabets, numerical data, special characters or their combination) have been used to make user input samples for testing the system.

ii. Development has been done by using Visual Studio.Net tool.

iii. Evaluation is done using standard tool - Statistical Testing Suite(STS) recommended by National Institute of Standard and Technology (NIST).

iv. In statistical evaluation, some tests require large sized input sample (10^6 bit longer sequence) which is recommended by NIST. Therefore, large sequence size has been used for some tests (Serial test, Lempel-Ziv, overlapping and non-overlapping tests).

v. The longer sequence size (1268784 bits) is used for evaluating the Randomized Substitution Mechanism (RSM) during the statistical randomness testing, because the longer parameter length in STS, must be greater than or equal to 10^6.

vi. The larger sequence (1153440 bits) is used to test the Multi-operation Data Encryption Mechanism (MoDEM) because it is recommended parameter length ($\geq 10^6$) for STS tool.

1.9 Thesis Structure

The rest of this thesis is structured as:-

In Chapter 1, overview, problem background related to fixed data blocking, static substation including static and constant enciphering operations have been discussed to generate problem statement. Furthermore, the study aim, research questions, objectives, significance and research scope have been highlighted.

Chapter 2, provides the extensive literature review of most related research topics (Issues in symmetric cryptosystems, Feistel structure limitations, SPN design deficiencies, other potential security issues, need of proposed design and discussion of latest attacks on AES and DES).

Chapter 3, outlines the research methodology and flow used in this research. It discusses the research plan, design and procedures followed against the development of proposed method. Furthermore, it elaborates the research scope and

evaluation metrics through which the proposed method can be evaluated. Detail about the recommend statistical tests and tool with experimental setup has also been discussed in this chapter.

Chapter 4, contributes the design, development and evaluation of proposed Dynamic Data Blocking Mechanism (DDBM) which is the first objective of this study. The DDBM has been developed in Visual Studio.Net and its evaluation has been done through practical experimentations.

Chapter 5, provides the design, development and evaluation of proposed Randomized Substitution Mechanism (RSM) by discussing all interrelated steps. The RSM is the second objective of this study which firstly developed through utilizing the Visual Studio. Net tool and after that it has been evaluated and validated by executing several statistical randomness tests (discussed in Chapter 3) by using Statistical Testing Suite (STS) tool recommended by National Institute of Standard and Technolgoy (NIST).

Chapter 6, discusses the design, development and evaluation of Multi-Operation Data Encryption Mechanism (MoDEM) which is the third objective of this study. The proposed MDEM has been developed in Visual Studio. Net and subsequently, it has been evaluated and validated through experimental testing of NIST's recommend statistical tests conducted through STS Tool. Mathematical testing of common attacks against proposed method including brute force strength attack have also been provided in Chapter 6.

Chapter 7, comprehensively summarizes the achievements and contributions against each study objective in addition with the concluding remarks. Moreover, this chapter directs the researchers how to continue this research work toward more revolutionary enhancements about cryptosystems in near future.

REFERENCES

Abdulgader, A., Ismail, M., Zainal, N., and Idbeaa, T. (2015). Enhancement of AES Algorithm Based On Chaotic Maps and Shift Operation For Image Encryption. *Journal of Theoretical and Applied Information Technology*, 71(1), 1-12.

Abomhara, M., Zakaria, O., Khalifa, O. O., Zaidan, A. A., and Zaidan, B. B. (2010). Enhancing selective encryption for H. 264/AVC using advanced encryption standard. *International Journal of Computer and Electrical Engineering*, *2*(2), 223-229.

Acharya, B. (2015). *Towards an automated and customizable linear cryptanalysis of a substitution-permutation network cipher,* Master thesis, Washington and Lee University, West Washington.

Agrawal, H., and Sharma, M. (2010). Implementation and analysis of various symmetric cryptosystems. *Indian Journal of Science and Technology*, *3*(12), 1173-1176.

Ahmad, M., Khan, P. M. and Ansari, M. Z. (2014). A simple and efficient key-dependent S-box design using fisher-yates shuffle technique. In *Recent Trends in Computer Networks and Distributed Systems Security* CCIS,420, 540-550, Springer.

Alabaichi, A., Mahmod, R., and Ahmad, F. (2013). Randomness Analysis of 128 bits Blowfish Block Cipher on ECB and CBC Modes. *International Journal of Digital Content Technology and its Applications, 7*(15), 77-89.

Alani, M. M. (2012). Neuro-Cryptanalysis of DES and Triple-DES. In *Neural Information Processing* – Lecture Notes in Computer Science, 7667,637-646.Springer Berlin Heidelberg.

Alanazi, H., Zaidan, B. B., Zaidan, A. A., Jalab, H. A., Shabbir, M., and Al-Nabhani, Y. (2010). New comparative study between DES, 3DES and AES within nine factors. *Journal of Computing*. 2(3), 152-157.

Alimomeni M. (2014). *New Notions of Secrecy and User Generated Randomness in Cryptography*, Doctoral Thesis, Department Of Computer Science, University Of Calgary, Alberta.

Al-Shakarchi, N. D. (2014). Encryption and Decryption Digital Image Using Confusion System. European Academic Research. 1(11), 3947-3968.

Al-Wattar, A. H., Mahmod, R., Zukarnain, Z. A. *et al.* (2015). A New DNA based Approach of Generating Key Dependent Shift Rows Transformation, International Journal of Network Security & Its Applications, 7(1), 79-89

Amin, S., F., and Hunnergi, N., S. (2013). Hill Cipher algorithm with Self Repetitive Matrix for Secured Data Communication. In *International Journal of Engineering Research and Technology*, 2(9), 2960-2971

Anderson, R., Biham, E., and Knudsen, L. (2000). Serpent and smartcards. In *Smart Card Research and Applications* (pp. 246-253). Springer Berlin Heidelberg

Arora M., (2012), How secure is AES against brute force attacks, EE-Times. Cited at URL: http://www.eetimes.com/document.asp?doc_id=1279619, Visited on September 2015.

Ayushi, (2010), A Symmetric Key Cryptographic Algorithm. *International Journal of Computer Applications*. 1(15), 01-04.

Balakrishnan, B. (2010). Three Tier Encryption Algorithm for Secure File Transfer. In *Second International Conference on Computer Engineering and Applications*, 2, IEEE, 259-263

Batina L., Mentens N., Oswald E., Pelzl J., Priplata C., *et al.* (2005), DVAM3 Hardware Crackers, ECRYPT-European Network of Excellence in Cryptology, IST-2002-507932

Bellare, M., and Rogaway, P. (1999). On the construction of variable-input-length ciphers. In *Fast Software Encryption*. 231-244. Springer Berlin Heidelberg.

Bellare, M., Kohno, T. and Namprempre, C. (2004). Breaking and provably repairing the SSH authenticated encryption scheme: A case study of the Encode-then-Encrypt-and-MAC paradigm. *ACM Transactions on Information and System Security (TISSEC)*, *7*(2), 206-241.

Bellini, E., Morgari, G., and Coppola, M. (2015). An Extension of Cook's Elastic Cipher. CSIT, *arXiv preprint arXiv:1310.4050V2*: (01-18)

Biham, E., and Shamir, A. (1991). Differential cryptanalysis of DES-like cryptosystems. *Journal of CRYPTOLOGY*, *4*(1), 3-72.

Biham, E., and Shamir, A. (1993). *Differential cryptanalysis of the data encryption standard (1st Edition)*, ISBN 978-1-4613-9314-6, Pages: 188, Springer-Verlag New York.

Biham, E., and Biryukov, A. (1995). An improvement of Davies' attack on DES. In *Advances in Cryptology—EUROCRYPT'94* (pp. 461-467). Springer Berlin Heidelberg.

Biham, E., and Biryukov, A. (1997). An improvement of Davies' attack on DES. *Journal of Cryptology*, *10*(3), 195-205.

Biham, E. (1999). Cryptanalysis of Triple Modes of Operation. Journal of Cryptology, 12(3), 161-184.

Bernstein, D. J. (2005). Cache-timing attacks on AES. Technical Report, 2005, The University of Illinois at Chicago, Chicago, IL 60607-7045.

Biryukov, A. and Kushilevitz, E. (1998). Improved cryptanalysis of RC5. In Advances in Cryptology - EUROCRYPT '98, Finland, May 31 - June 4, 1998, Proceeding of Lecture Notes in Computer Science, 1403, 85–99. Springer

Biryukov, A., De Canniere, C., Lano, J., Ors, S. B., *et al.* (2004). Security and performance analysis of ARIA. *Final report, KU Leuven ESAT/SCD-COSIC, 3(2004)*, 4-58.

Biryukov, A. (2005). The boomerang attack on 5 and 6-round reduced AES. In *Advanced Encryption Standard–AES*. 3373, 11-15. Springer Berlin Heidelberg.

Biryukov, A., and Khovratovich, D. (2009a). Related-key cryptanalysis of the full AES-192 and AES-256. In *Advances in Cryptology–ASIACRYPT 2009. Lecture Notes in Computer Science*. 5912,1-18. Springer Berlin Heidelberg.

Biryukov, A., Khovratovich, D., and Nikolić, I. (2009). Distinguisher and related-key attack on the full AES-256. In *Advances in Cryptology-CRYPTO 2009*. 5677, 231-249. Springer Berlin Heidelberg.

Biryukov, A., Dunkelman, O., Keller, N., Khovratovich, D., and Shamir, A. (2010). Key recovery attacks of practical complexity on AES-256 variants with up to 10 rounds. In *Advances in Cryptology–EUROCRYPT 2010.Lecture Notes in Computer Science*. 6110, 299-319. Springer Berlin Heidelberg.

Biryukov A., Gong G. (2010), *Selected Areas in Cryptography*, Douglas R. Stinson (Eds.), ISBN: 978-3-642-19573-0, LNCS, Springer, New York.

Biryukov, A., and Großschädl, J. (2012). Cryptanalysis of the full AES using GPU-like special-purpose hardware. *Fundamenta Informaticae, 114*(3), 221-237.

Biryukov, A., and Nikolic, I. (2014). Complementing Feistel ciphers. Fast Software Encryption- Lecture Notes in Computer Science, 8424: 3-18, Springer

Biryukov, A., Roy, A., and Velichkov, V. (2014). Differential analysis of block ciphers SIMON and SPECK. In International Workshop on Fast Software Encryption *(FSE'14)* London, UK, March (3-5), 2014: 546-570

Biryukov, A., and Velichkov, V. (2015). Improved Data Complexity of Attacks on RC5. *Early Symetric Crypto ESC-2015, 12-16 January*, Luxembourg, 96-103.

Black, J., and Rogaway, P. (2002). Ciphers with arbitrary finite domains. In *Topics in Cryptology—CT-RSA* . 114-130. Springer Berlin Heidelberg.

Bogdanov, A., Khovratovich, D., Rechberger, C.(2011). Biclique Cryptanalysis of the Full AES. (2011). In Lee, D.H., Wang, X., (Eds).: ASIACRYPT, Lecture Notes in Computer Science, 7073, 344-371, Springer

Bogdanov, A., and Wang, M. (2012). Zero correlation linear cryptanalysis with reduced data complexity. In *Fast Software Encryption* (pp. 29-48). Springer Berlin Heidelberg.

Bogdanov, A., Chang, D., Ghosh, M., and Sanadhya, S. K. (2014). Bicliques with Minimal Data and Time Complexity for AES (Extended Version). in 16th International Conference on Information Security and Cryptology. 29-30 May, Tokyo, Japan, 1-19

Brown, J. A., Houghten, S., and Ombuki-Berman, B. (2009). Genetic algorithm cryptanalysis of a substitution permutation network. In *IEEE Symposium on Computational Intelligence in Cyber Security, 2009. CICS'09.* March 30- April 2, Nashville, 115-121. IEEE.

Canteaut, A. and Roué, J. (2015). Differential Attacks Against SPN: A Thorough Analysis. In *Codes, Cryptology, and Information Security,* LNCS , 9084, 45-62, Springer

Chakraborty, R., Agarwal, S., Misra, S., Khemka, V., *et al*. (2011). Triple SV: A bit level symmetric block cipher having high avalanche effect. *IJACSA) International Journal of Advanced Computer Science and Applications*, *2*(7): 61-68

Chang, D., Ghosh, M. and Sanadhya, S. K. (2015). Biclique cryptanalysis of full round AES-128 based hashing modes. Technical Report IIITD-TR-2015-006, Indraprstha Institute of Information Technology Delhi.

Chavan, N. R., and Annadate, S. A. (2015). VHDL implementation of AES-128 on FPGA. International Journal of Innovative Research In Electrical, Electronics, Instrumentation And Control Engineering, 03(01), 43-45.

Chouinard, JY. (2002). Design of Secure Computer System Notes on Data Encryption Standard. CSI4138/CEG4394, PP. 1-31

Cook, D. L. (2006). *Elastic block ciphers*. Doctoral dissertation, Columbia University, Columbia.

Cook, D. L., Yung, M., and Keromytis, A. D. (2008). Methods for linear and differential cryptanalysis of elastic block ciphers. In Information Security and Privacy (2008), Springer, 187–202.

Cook, D. L., Yung, M., and Keromytis, A. D. (2009). Elastic block ciphers in practice: constructions and modes of encryption. In Proceedings of the 3rd European Conference on Computer Network Defense (2009), Springer, 69–91.

Daemen, J., Knudsen, L., and Rijmen, V. (1997). The block cipher Square. In *Fast Software Encryption.*LNCS, vol. 1267, 149-165. Springer Berlin Heidelberg

Daemen, J., and Rijmen, V. (2000). The block cipher Rijndael. In *Smart Card Research and Applications* (pp. 277-284). Springer Berlin Heidelberg.

Daemen, J. and Rijmen, V. (2002). *Design of Rijndael. AES—The Advanced Encryption Standard.* ISBN 3-540-42580-2, Springer Berlin Heidelberg.

Daemen, J., and Rijmen, V. (2010). The first 10 years of advanced encryption. *IEEE Security & Privacy*, *8*(6), 0072-74.

Daemen, J. and Rijmen, V. (2013). *The design of Rijndael: AES-the advanced encryption standard*. Springer Science and Business Media, ISBN: 978-3-642-076466, Springer Berlin Heidelberg.

Damico, T. M. (2009). A Brief History of Cryptography. *Student Pulse*, *1*(11): 1-1.

Dara, M., and Manochehri, K. (2014). Using RC4 and AES Key Schedule to Generate Dynamic S-Box in AES. *Information Security Journal: A Global Perspective*, *23*(1-2), 1-9. Taylor & Francis

Das, S., Uz-Zaman, J.K.M.S. and Ghosh R. (2013). Generation of AES S-Boxes with various modulus and additive constant polynomials and testing their randomization, CIMTA-2013, Procedia Technology 10(2013):957–962, Science Direct

Das, S. (2014). Generation of AES-like 8-bit random S-Box and comparative study on randomness of corresponding cipher-texts with other 8-bit AES S-Boxes. In

Intelligent Computing, Networking, and Informatics, Advances in Intelligent System and Computing 243 (pp. 303-318), Springer

Davahli, A., Mirvaziri, H., and Aminian, M. (2014), Structural Cryptanalysis of the Message Based Random Variable Length Key Encryption Algorithm (MRVLK), Journal of mathematics and computer science 12 (2014), 201-210

David C. W., and Jan Zizka, (2012). Advances *in Computer Science, Engineering and Applications* (Dhinaharan Nagamalai Eds.), in Proceedings of the Second International Conference on Computer Science, Engineering and Applications (ICCSEA 2012), May 25-27, Vol. 2, 2012 Springer.

Demirci, H., and Selçuk, A. A. (2008). A meet-in-the-middle attack on 8-round AES. In *Fast Software Encryption* . LNCS, 5086, 116-126. Springer Berlin Heidelberg.

Demirci, H., Taşkın, İ., Çoban, M., and Baysal, A. (2009). Improved meet-in-the-middle attacks on AES. In *Progress in Cryptology-INDOCRYPT 2009*. LNCS 5922, 144-156. Springer Berlin Heidelberg.

Derbez, P., Fouque, P. A. and Jean, J. (2013). Improved Key Recovery Attacks on Reduced-Round AES in the Single-Key Setting. In *EUROCRYPT* - Advances in Cryptology – 2013, 7881, 371-387, Springer

Dey, H., Das, S., and Ghosh, R. (2014). An Approach to find out the Optimal Randomness of Modified RC4, International Journal of Innovations & Advancement in Computer Science, 3(8),01-10.

Diffie, W., and Hellman, M. E. (1977). Special feature exhaustive cryptanalysis of the NBS data encryption standard. *Computer*, *10*(6), 74-84.

Dinur, I., Dunkelman, O., Keller, N. and Shamir, A. (2015). New Attacks on Feistel Structures with Improved Memory Complexities. In: Advances in Cryptology – CRYPTO 2015, Lecture Notes in Computer Science, 1, 433-454, Springer

Doganaksoy, A., Ege, B., Koçak, O. and Sulak, F. (2010). Statistical Analysis of Reduced Round Compression Functions of SHA-3 Second Round Candidates.Technical Report, Institute of Applied Mathematics, Middle East Technical University, Turkey, *IACR Cryptology ePrint Archive, 2010*, 611.

Du, W. and Atallah, M. J. (2001, December). Privacy-preserving cooperative statistical analysis. In *Computer Security Applications Conference, 2001. ACSAC 2001. Proceedings 17th Annual* (pp. 102-110). IEEE.

Duta, C., Mocanu, B., Vladescu, F. and Gheorghe L. (2014). Randomness Evaluation Framework of Cryptographic Algorithms, International Journal on Cryptography and Information Security, 4(01), 31-49

Ebrahim, M., Khan, S., and Khalid, U. B. (2013). Symmetric Algorithm Survey: A Comparative Analysis. *International Journal of Computer Applications*, 61(20), 12-19.

Faragallah, O. S., El-Rabaie, E. S. M., El-Samie, F. E. A., *et al.* (2014). *Multilevel Security for Relational Databases*. CRC Press.

Feistel, H. (1973). Cryptography and Computer Privacy. *Scientific American, 228(5),* 15-23. USA.

FIPS PUB 197, (2001). Announcing the Advanced Encryption Standard, Federal Information Processing Standards Publication 197, National Institute of Standard and Technology (NIST), 2001

FIPS PUB 46, (1977). *Appendix A, Federal Information Processing Standards Publication 46.* National Institute of Standard and Technology (NIST), 1977

FIPS PUB 46-3, (1999). *Appendix A, Federal Information Processing Standards Publication 46.* National Institute of Standard and Technology (NIST), 1999

Flamm B. M. (2014). *Extending Differential Fault Analysis to Dynamic S-Box Advanced Encryption Standard Implementations*, Master Thesis. Department of Electrical and Computer Engineering, Graduate School of Engineering and Management, Air University, USA.

Fontaine, C., andGaland, F. (2007). A survey of homomorphic encryption for nonspecialists. *EURASIP Journal on Information Security*, *2007*, Article ID: 13801, pp.10 .Hindawi Publishing Corporation.

Franke, J., Kleinjung, T., Paar, C., Pelzl, J., Priplata, C., and Stahlke, C. (2005). SHARK: a realizable special hardware sieving device for factoring 1024-bit integers. In *Cryptographic Hardware and Embedded Systems–CHES.* 119-130. Springer Berlin Heidelberg.

Gangadari, B. R., Ahamed, S. R., Mahapatra, R. and Sinha, R. K. (2015). Design of Cryptographically Secure AES S-Box Using Cellular Automata, IEEE international conference on EESCO. 978-1-4799-7678, IEEE

Geiselmann, W., Shamir, A., Steinwandt, R., and Tromer, E. (2005). Scalable hardware for sparse systems of linear equations, with applications to integer

factorization. In *Cryptographic Hardware and Embedded Systems–CHES 2005*, 131-146, Springer Berlin Heidelberg.

Gilbert, H., and Minier, M. (2000). A collisions attack on the 7-rounds Rijndael.Third AES Candidate Conference.

Gondal, M. A., Raheem, A., and Hussain, I. (2014). A Scheme for Obtaining Secure S-Boxes Based on Chaotic Baker's Map. *3D Research*, *5*(3), 1-8.

Goots, N., Izotov, B., Moldovyan, A., and Moldovyan, N. (2003). *Modern Cryptography Protect your data with fast block CIPHERS*, Wayne, A-LIST Publishing 2003.

Grundgeiger, D. (2002). *Programming Visual Basic. NET*. (1st Edition), ISBN: 0-596-00093-6, 464 pages O'Reilly Publisher.

Gülmezoglu, B., Inci, M. S., Irazoqui, G., Eisenbarth, T., and Sunar, B. (2015). A Faster and More Realistic Flush+ Reload Attack on AES. In COSADE-2015, 13-14 April, Berlin, 1-16

Gunasundari, T., and Elangovan, K. (2014). A Comparative Survey on Symmetric Key Encryption Algorithms. *International Journal of Computer Science and Mobile Applications*, 2(2), 78-83.

Guo, J., Jean, J., Nikolić, I., amd Sasaki, Y. (2014). Meet-in-the-Middle Attacks on Generic Feistel Constructions. In *Advances in Cryptology–ASIACRYPT 2014* (pp. 458-477). Springer Berlin Heidelberg.

Harmouch, Y. and El Kouch, R. (2015). A New Algorithm for Dynamic Encryption. International Journal of Innovation and Applied Studies, 10(1), 305-312.

Hellman, M. E. (1980). A cryptanalytic time-memory trade-off. *Information Theory, IEEE Transactions on*, *26*(4), 401-406.

Heys, H. M., and Tavares, S. E. (1996). Cryptanalysis of substitution-permutation networks using key-dependent degeneracy. *Cryptologia*, *20*(3), 258-274.

Heys, H. M. (2001). Information leakage of Feistel ciphers. *IEEE Transactions on Information Theory*, *47*(1), 23-35.

Hong, D., Sung, J., Hong, S., Lee, W., Lee, S., Lim, J., and Yi, O. (2001). Known-IV attacks on triple modes of operation of block ciphers. In *Advances in Cryptology—ASIACRYPT*. 208-221. Springer Berlin Heidelberg.

Hosseinkhani, R., and Javadi, H. H. S. (2012). Using cipher key to generate dynamic S-box in AES cipher system. *International Journal of Computer Science and Security (IJCSS)*, *6*(1), 19-28.

Isobe, T., and Shibutani, K. (2013). Generic Key Recovery Attack on Feistel Scheme. In *Advances in Cryptology-ASIACRYPT 2013* Lecture Notes in Computer Science, vol. (8269): 464–485. Springer.

Jacob, G., Murugan, A., and Viola, I. (2015).Towards The Generation of A Dynamic Key-Dependent S-Box to Enhance Security, IACR Cryptology ePrint Archive 92,1-5

Jain B., Rao V., chowdhary B. *et al.* (2015). Secure Mobile Internet Messaging, International Journal of Computer Application, 5(2): 201:205

Jarvinen. K. (2008). Studies on Efficient Implementation of Cryptographic Algorithms, Doctoral Thesis. Department of Signal Processing and Acoustics, Helsinki University of Technology, P.O. BOX 1000, FI-02015 TKK, Finland.

Jithendra, K. B., and Shahana, T. K. (2015). Hardware Efficient Parallel Substitution Box for Block Ciphers with Static and Dynamic Properties. *Procedia Computer Science*, *46*, 540-547, Science Direct

Junod. P. (2004). Statistical Cryptanalysis of Block Ciphers. Doctoral Thesis. Presentee La Faculte Informatique & Communications, Institute de systems de communication.

Kaliski J., R., B. S., and Yin, Y. L. (1995). On differential and linear cryptanalysis of the RC5 encryption algorithm. In *Advances in Cryptology—CRYPT0'95* USA, August 27-31, 1995, Proceedings, Lecture Notes in Computer Science, 963,171–184, Springer

Kaur, G., and Madaan, N. (2014). A Comparative Study of AES Encryption Decryption. *International Journal*. of Science and Research, 3(4), 279-283

Kazlauskas, K., Vaicekauskas, G., and Smaliukas, R. (2015). An Algorithm for Key-Dependent S-Box Generation in Block Cipher System. *INFORMATICA*, *26*(1), 51-65

Kelsey, J. (2002). Compression and information leakage of plaintext. In *Fast Software Encryption* (pp. 263-276). Springer Berlin Heidelberg.

Kessler. G. C. (1998).An Overview of Cryptography. Edition 1999. Published in Handbook on Local Area Networks: Auerbach Publishers.

Khan, M., and Shah, T. (2014). A novel image encryption technique based on Hénon chaotic map and S8 symmetric group. *Neural Computing and Applications*, *25*(7-8), 1717-1722. Springer

Khatri, N., Dhanda, R., and Singh, J. (2012). Comparison of Power Consumption and Strict Avalanche Criteria at Encryption/Decryption Side of Different AES Standards, *International Journal of Computational Engineering Research, 2(4), 1092-1096*

Knudsen, L. R. and Meier, W. (1996). Improved differential attacks on RC5. In Advances in Cryptology - CRYPTO '96, USA, August 18-22, 1996, Proceedings of Lecture Notes in Computer Science, 1109, 216–228. Springer

Knudsen, J. D. L., and Rijmen, V. (1997). The block cipher SQUARE. In *Fast Software Encryption: 4th International Workshop, FSE'97, Haifa, Israel, January 1997. Proceedings* (p. 149-165). Springer Berlin/Heidelberg.

Kocher, P., Jaffe, J., Jun, B., and Rohatgi, P. (2011). Introduction to differential power analysis. *Journal of Cryptographic Engineering*, *1*(1), 5-27.

Kumar V, Syed I. (2004). A Project Report On Password Encryption Using DES Algorithm. California State University Hayward

Kumar, S., Paar, C., Pelzl, J., Pfeiffer, G., and Schimmler, M. (2006). Breaking ciphers with COPACOBANA–a cost-optimized parallel code breaker. In *Cryptographic Hardware and Embedded Systems-CHES.*vol. 4249,101-118. Springer Berlin Heidelberg.

Kumar, R., Mishra, K. K., Tripathi, A., Tomar, A., and Singh, S. (2014). MSEA: Modified Symmetric Encryption Algorithm. *IACR Cryptology*, 280, 1-14

Lambić, D. (2013). A novel method of S-box design based on chaotic map and composition method. *Chaos, Solitons & Fractals*, *58*,16-21, Springer

Lee, R. B., Rivest, R. L., Robshaw, M. J. B., Shi, Z. J., and Yin, Y. L. (2004). Permutation Operations in Block Ciphers. *Embedded Cryptographic Hardware: Design and Security*. In

Nadia Nedjah and Luiza de Macedo Mourelle, editors, Embedded Cryptographic Hardware: Design and Security, Chapter 13. Nova Science Publishers, Hauppauge, NY, USA, 2004

Li, Y., and Cusick, T. W. (2007). Strict avalanche criterion over finite fields. *Journal of Mathematical Cryptology*, 1(1), 65.

Lim, C. H. (1998). CRYPTON: A new 128-bit block cipher. In the First AES Candidate Conference, *National Institute of Standard and Technology.*

Liu, T., Gui, Y., Sun, Y., Liu, Y., Sun, Y., and Xiao, F. (2014, March). SEDE: state estimation-based dynamic encryption scheme for smart grid communication. In

Proceedings of the 29th Annual ACM Symposium on Applied Computing, ACM, 539-544

Lu J.(2008). Cryptanalysis of block ciphers. PhD Thesis. The University of London, UK (2008). A copy is available online as Technical Report RHUL-MA-2008-19, Department of Mathematics, Royal Holloway, University of London, UK.

Lu, J., Dunkelman, O., Keller, N., and Kim, J. (2008). New impossible differential attacks on AES. In *Progress in Cryptology-INDOCRYPT 2008* .LNCS, vol. 5365, 279-293. Springer Berlin Heidelberg.

Lu, J. (2010). The (related-key) impossible boomerang attack and its application to the AES block cipher. *Designs, Codes and Cryptography*, *60*(2), 123-143.

Machicao, J., Baetens, J. M., Marco, A. G., *et al.* (2015). A dynamical systems approach to the discrimination of the modes of operation of cryptographic systems. Communications in Nonlinear Science and Numerical Simulation. 29(3), 102-115

Maheswari, T., S., Kanagaraj, S. and Vasudevan, S., K. (2014). Enhancement of Cloud Security Using AES 512 Bits, Research Journal of Applied Sciences, Engineering and Technology 8(20), 2116-2120

Mahmoud, E. M., Abd, A., Hafez, E., and Elgarf, T. A. (2013). Dynamic AES-128 with key-dependent S-Box. International Journal of Engineering Research and Applications, 03(01),1662-1670

Mandal, A. K., Parakash, C. and Tiwari, A. (2012). Performance evaluation of cryptographic algorithms: DES and AES. In *IEEE Students' Conference on Electrical, Electronics and Computer Science (SCEECS), 2012*, IEEE, 1-5

Mankotia, S., and Sood, M. (2015). A Critical Analysis of Some Symmetric Key Block Cipher Algorithms. International Journal of Computer Science and Information Technologies, 6 (1) : 495-499

Marinakis, G. (2013). Minimum key length for cryptographic security. *Journal of Applied Mathematics and Bioinformatics*, *3*(1), 181-191.

Matsui, M. (1993). Linear cryptanalysis method for DES cipher. In *Advances in Cryptology—EUROCRYPT'93*. Vol. 765, 386-397. Springer Berlin Heidelberg.

Matsui, M. (1994). The first experimental cryptanalysis of the Data Encryption Standard. In *Advances in Cryptology—Crypto'94.*vol.839, 1-11. Springer Berlin Heidelberg.

Mehla, R., and Kaur, H. (2014). Different Reviews and Variants of Advance Encryption Standard, International Journal of Science and Research (3(05), 1895-1896

Menezes, V., O. (1997). Handbook of Applied Cryptography, 1997. *CRC Press*, *200*, 6-10.

Merkle, R. C., and Hellman, M. E. (1981). On the security of multiple encryption. *Communications of the ACM*, *24*(7), 465-467.

McMillan, S., and Patterson, C. (2001). JBits™ Implementations of the Advanced Encryption Standard (Rijndael). In *Field-Programmable Logic and Applications*. 162-171. Springer Berlin Heidelberg.

Millan, W., Dawson, E. P., and O'Connor, L. J. (1994). Cryptanalysis of tree-structured ciphers. *Electronics Letters*, *30*(12), 941-942.

Min, L., and Chen, G. (2013). A novel stream encryption scheme with avalanche effect. *Eur. Phys. J. B*, *86*, 459.

Minematsu, K. (2008). *A study of block cipher modes for encryption and authentication*, Doctoral Thesis,Graduate School of Science and Engineering, Waseda University

Mishra, M., and Mankar, V. H. (2012). A Chaotic encryption algorithm: Robustness against Brute-force attack. In *Advances in Computer Science, Engineering & Applications* (pp. 169-179). Springer Berlin Heidelberg.

Moreno-Diaz R., Pichler F. (2011). Computer Aided Systems Theory, Alexis Quesada Arenicbia Part -1 (Eds.) in 13th Int. Conf. of System Theory-EUROCAST, Spain, 2011.

Mohamed, F. K. (2014). A parallel block-based encryption schema for digital images using reversible cellular automata. *Engineering Science and Technology, an International Journal*, *17*(2), 85-94.

Mohan, H. S., and Reddy, A. R. (2011). Performance analysis of AES and MARS encryption algorithms. *IJCSI International Journal of Computer Science Issues*,*8*(4),1694-0814.

Mona, M. C., Chitra, S. B., and Gayathri, V. (2014). A Survey on Various Encryption and Decryption Algorithms. International Journal of Security, 6(6), 289-300

Mouha, N. and Luykx, A. (2015). *Multi-Key Security: The Even-Mansour Construction Revisited*. In Proceeding of CRYPTO 2015, Cryptology ePrint Archive, Report 2015/101. Springer

Mousa, A. (2005). Data encryption performance based on Blowfish. In *ELMAR, 2005. 47th International Symposium*, (8-10) jun 2005, Zadar, 131-134. IEEE.

Mui-Edwin, NC. (2007).Practical implementation of Rijndael S-box using Combinational logic. *Custom R&D Engineer Texco Enterprise Pvt. Ltd*. 1-16.

Mirvaziri, H., Ismail, K. J., and Hanapi, Z. M. (2009). Message based random variable length key encryption algorithm. *Journal of Computer Science*, *5*(8), 573-578.

Nandi, M. (2014). XLS is Not a Strong Pseudorandom Permutation. In *Advances in Cryptology–ASIACRYPT 2014* (pp. 478-490). Springer Berlin Heidelberg.

Nechvatal, J., Barker, E., Dodson, D., Dworkin, M., Foti, J., and Roback, E. (1999). Status report on the first round of the development of the Advanced Encryption Standard. *Journal of Research-National Institute of Standards and Technology*, *104*(5), 435-460.

Nechvatal, J., Barker, E., Bassham, L., Burr, W., and Dworkin, M. (2000). *Report on the development of the Advanced Encryption Standard (AES)*. Computer Security Division, National Inst Of Standards and Technology, Gaithersburg.

Nie, T., and Zhang, T. (2009). A study of DES and Blowfish encryption algorithm. In *TENCON 2009-2009 IEEE Region 10 Conference*, (23-26) Jan, 2009, Singapore, 1-4, IEEE.

Paar, I. C., and Pelzl, I. J. (2010). The Advanced Encryption Standard (AES). In *Understanding Cryptography* (pp. 87-121). Springer Berlin Heidelberg.

Paar C., Pelzl J. (2009). Understanding Cryptography: A Textbook for Students and Practitioners. Springer Science & Business Media - Computers - 372 pages

Park, J. J. J. H., Barolli, L., Xhafa, F., and Jeong, H. Y. (Eds.). (2013). *Information Technology Convergence: Security, Robotics, Automations and Communication, Lecture Notes in Electrical Engineering,* 253. ISBN: 978-94-007-6995-3,Springer

Parmar, N. D., and Kadam, P. (2015). Pipelined Implementation of Dynamic Rijndael S-Box. *International Journal of Computer Applications*, *111*(10), 36-38.

Pathan, P. K. and Verma, B.(2011). Hyper Secure Cryptographic Algorithm to Improve Avalanche Effect for Data Security. International Journal of Computer Technology and Electronics Engineering, 1(2), 140-145.

Patarin, J. (2001). Generic attacks on Feistel schemes. In *Advances in Cryptology—ASIACRYPT 2001*. 222-238. Springer Berlin Heidelberg.

Patel, S., Ramzan, Z., and Sundaram, G. S. (2005). Efficient constructions of variable-input-length block ciphers. In *Selected Areas in Cryptography*. 326-340. Springer Berlin Heidelberg.

Patidar, G., Agrawal, N., and Tarmakar, S. (2013). A block based Encryption Model to improve Avalanche Effect for data Security. *International Journal of Scientific and Research Publications*, 309. 3(1):1-4

Pazynyuk, T., Li, J. Z., and Oreku, G. S. (2008). Improved Feistel-based ciphers for wireless sensor network security. *Journal of Zhejiang University SCIENCE A*, *9*(8), 1111-1117.

Pradeep, L. N. and Bhattacharjya, A. (2013). Random Key and Key Dependent S-box Generation for AES Cipher to Overcome Known Attacks. In *Security in Computing and Communications*, CCIS 377, 63-69, Springer.

Raghav, V., Chhatarpal , Sharma, B. (2015). study and design of pipelined 128 bit advanced encryption algorithm using verilog, International Journal For Technological Research In Engineering, 2(12), 3012-3016.

Ramly, S. H., El-Garf, T., and Soliman, A. H. (2001). Dynamic generation of S-boxes in block cipher systems. In *Radio Science Conference, 2001. NRSC 2001. Proceedings of the Eighteenth National* .Vol. 2, 389-397. IEEE.

Ramanujam, S., & Karuppiah, M. (2011). Designing an algorithm with high Avalanche Effect. *IJCSNS International Journal of Computer Science and Network Security*, 11(1), 106-111.

Rejani, R. , Krishnan, D. V. (2015). Study of Symmetric key Cryptography Algorithms. International Journal of Computer Techniques, 2(2), 46-50

ReddyK, N. A. and Vishnuvardhan, B. (2014). Secure Linear Transformation Based Cryptosystem using Dynamic Byte Substitution, International Journal of Security (IJS), 8(3), 24-32.

Ristenpart, T., and Yilek, S. (2010). When Good Randomness Goes Bad: Virtual Machine Reset Vulnerabilities and Hedging Deployed Cryptography. In Proc. ISOC Network and Distributed Security Symposium (2010)

Ritter, T. F. (1998). Variable Size Block Ciphers. *U.S. Patent No. 5,727,062*. Washington, DC: U.S. Patent and Trademark Office.

Rivain, M. (2009). *On the physical security of cryptographic implementations*. Doctoral dissertation, Université Catholique de Louvain.

Rivain, M., and Roche, T. (2013). SCARE of secret ciphers with SPN structures. In *Advances in Cryptology-ASIACRYPT 2013*.LNCS 8269, 526-544. Springer Berlin Heidelberg.

Rivest, R. L. (1995). The RC5 encryption algorithm. In *Fast Software Encryption* . 86-96. Springer Berlin Heidelberg.

Rogaway, P., Wooding, M., and Zhang, H.(2012). The security of ciphertext stealing. In Fast Software Encryption (2012), Springer, 180– 195.

Röllgen, C. K. B. (2010). Block cipher. *U.S. Patent Application No. 12/925,347*, filed October 21, 2010. United States.

Rukhin, A., Soto, J., Nechvatal, J., Smid, M., Barker, E., Leigh, S., *et al.* (2010). NIST special publication 800-22. *A statistical test suite for random and pseudorandom number generators for cryptographic applications*. Booz-Allen and Hamilton Inc Mclean Va.

Russell, A., Tang, Q., Yung, M. and Zhou, H. S. (2015). *Cliptography: Clipping the power of kleptographic attacks*. Cryptology ePrint Archive, Report 2015/695, 2015.

Sahmoud, S., Elmasry, W., and Abudalfa, S. (2013). Enhancement the Security of AES against Modern Attacks by Using Variable Key Block Cipher. *Int. Arab J. e-Technol., 3*(1), 17-26.

Saini, B. (2014). Implementation of AES Using S-Box Rotation. International Journal of Advanced Research in Computer Science and Software Engineering, 4(5), 1322-1326

Sarmah, H. K., and Paul, R. (2010). Period doubling route to chaos in a two parameter invertible map with constant Jacobian. *Int J Res Rev Appl Sci*, *3*(1), 72-82.

Sawant, G., Jadeja, K., Bahat, K., and Dalal, J. (2015). The New Cryptography Algorithm with Dynamic Steganography, International Research Journal of Computer Science. 2(2),10-17

Saxena, P., and Shibu, S. (2014). A Novel Approach to Design Time Efficient and Secure encryption Algorithm (T-SEA), *IOSR Journal of Computer Engineering, 16(01), 29-34.*

Sbiaa, F., Zeghid, M., Baganne, A., Daradkeh, Y. I., & Tourki, R. (2014). An efficient Encryption scheme based on Block Cipher Algorithms. Recent Advances In Telecommunications, Informatics And Educational Technologies. ISBN: 978-1-61804-262-0. WSEAS, 134-138.

Senthilkumar, B. and Rajamani, V. (2014). VLSI implementation of key dependent substitution box using error control algorithm for substitution-permutation supported cryptography, Journal of Theoretical and Applied Information Technology, 64(01), 74-83

Schneier, B. (1994). Description of a new variable-length key, 64-bit block cipher (Blowfish). In *Fast Software Encryption*. 191-204. Springer Berlin Heidelberg.

Schneier, B., Kelsey, J., Whiting, D., Wagner, D., Hall, C., and Ferguson, N. (1998). Twofish: A 128-bit block cipher. *NIST AES Proposal*, *15*: 1-68

Shannon, C. E. (1949). Communication Theory of Secrecy Systems. *Bell system technical journal*, *28*(4), 656-715.

Shyamala-Bai, K., Satyanarayana, M. V., and Vijaya, P. A. (2011). Variable Size Block Encryption using Dynamic-key Mechanism (VBEDM). *International Journal of Computer Applications*, *27*(7).

Sikdar, D. (2014). S-box Optimization Technique with a Primitive Irreducible Polynomial, *International Journal of Emerging Trends & Technology in Computer Science, 3(3), 97-99*

Singh, A., and Bansal, M. (2010). FPGA Implementation of Optimized DES Encryption Algorithm on Spartan 3E. *Published in International Journal of Scientific & Engineering Research*, *1*(1):1-6

Singh, S., Maakar, S. K., and Kumar, D. S. (2013). A Performance Analysis of DES and RSA Cryptography. *International Journal of Emerging Trends & Technology in Computer Science (IJETTCS), 2(3), 418-423.*

Singh, P. S. and Agarwal, A. K. (2014). Architecture and Implementation of a Security Algorithm CPBFC for WSN. International Journal of Innovative Research in Computer and Communication Engineering, *2*(8), 5409-5414.

Smith, W. D. (2007). 1. AES seems weak. 2. Linear time secure cryptography. *IACR Cryptology ePrint Archive*, *2007*, 248.

Song, J., Lee, K., and Lee, H. (2014). Biclique Cryptanalysis on the Full Crypton-256 and mCrypton-128. *Journal of Applied Mathematics*, *2014*, 1-10

Soto, J. (1999). Statistical testing of random number generators. In *Proceedings of the 22nd National Information Systems Security Conference*, Gaithersburg 10(99),1-12.

Sreedharan, A. (2014). Dynamic S-BOX Based AES Algorithm for Image Encryption, Computer and Information Engineering, 01(11), 2014

Srinivas, L., Patel, Z. M., and Naik, B. C. S. (2014). VLSI Implementation of Enhanced AES Cryptography. *International Journal of Computational Engineering Research, 4(07), 51-58*

Stalling W. (2013), *Cryptography and Network Security: Principles and Practice*.(6th Edition). ISBN-13: 978-0133354690

Suzaki, T., and Minematsu, K. (2010). Improving the generalized Feistel. In *Fast Software Encryption*, LNC, 6147: 19-39 Springer Berlin Heidelberg.

Sýs, M., and Říha, Z. (2014). Faster Randomness Testing with the NIST Statistical Test Suite. In *Security, Privacy, and Applied Cryptography Engineering* (pp. 272-284). Springer International Publishing.

Szaban, M., and Seredynski, F. (2010). CA-based Generator of S-boxes for Cryptography Use. In *Parallel & Distributed Processing, Workshops and Phd Forum (IPDPSW), IEEE International Symposium on*. 1-8. IEEE.

Tange, H., and Andersen, B. (2014). Dynamic AES–Extending the Lifetime. *Journal of Cyber Security, 2(2-3)*, 243–264.

Thulasimani, L., and Madheswaran, M. (2010). A single chip design and implementation of aes-128/192/256 encryption algorithms. *International Journal of Engineering Science and Technology*, *2*(5), 1052-1059.

Tiessen, T., Knudsen, L. R., Kölbl, S. and Lauridsen, M. M. (2015). *Security of the AES with a Secret S-box*. IACR Cryptology ePrint Archive 2015, 144

Traore, I. and Liu, M., Y. (2003). Evaluation of Whitenoise Cryptosystem Part 1: Encryption Algorithm, Technical Report No ECE03-3, University of Victoria.

Tu, C., Gao, N.,Liu, Z., Wang, L. et al. (2015). A Practical Chosen Message Power Analysis Method on the Feistel-SP ciphers with Applications to CLEFIA and Camellia. IACR Cryptology ePrint Archive: Report 2015/174: (1-19)

Une, M., and Kanda, M. (2007). Year 2010 Issues on Cryptographic Algorithms. *Monetary and Economic Studies*, *25*(1), 129-164.

Van-Oorschot, P. C., and Wiener, M. J. (1991). A known-plaintext attack on two-key triple encryption. In *Advances in Cryptology—Eurocrypt'90*. 318-325. Springer Berlin Heidelberg.

Velayutham, R., Ganesh, E. S., and Manimegalai, D. (2015). Enhancing the Security of AES Algorithm in Wireless Network. In *Power Electronics and Renewable Energy Systems,* Lecture Notes in Electrical Engineering 326, 1289-1295. Springer .

Vergili, I. and Yücel, M. D. (2001). Avalanche and Bit Independence Properties for the Ensembles of Randomly Chosen× S-Boxes. *Turk J Elec Engin*, *9*(2), 137-145.

Wadhwa, N., Hussain, s. Z., and Rizvi, s. (2013). Review of the journey from des to AES. *International Journal of Computer Science*. 3(2), 351-366.

WangX, and WangQ. (2013). A novel image encryption algorithm based on dynamic S-boxes constructed by chaos. *Nonlinear Dynamics*, *75*(3), 567-576.

Wang, Q., Liu, Z., Toz, D., Varici, K., and Gu, D. (2015). Related-key rectangle cryptanalysis of Rijndael-160 and Rijndael-192. *IET Information Security*. 9(5): 266 – 276

Webster, A. F., and Tavares, S. E. (1986). On the design of S-boxes. In *Advances in Cryptology—CRYPTO'85 Proceedings*. 523-534. Springer Berlin Heidelberg

Wei, Y., Li, C., and Sun, B. (2011). Related-key impossible differential cryptanalysis on crypton and crypton v1. 0. In *World Congress on Internet Security (WorldCIS), 2011,* IEEE. 227-232

Wiener, M. J. (1993). *Efficient DES key search*. School of Computer Science, Carleton University.

Wiener, M. (2011). Exhaustive Key Search. In *Encyclopedia of Cryptography and Security*, 431-433, Springer US.

Xiao, L., and Heys, H. M. (2005). Software performance characterisation of block cipher structures using S-boxes and linear mappings. In *Communications, IEE Proceedings-* . 152(5), 567-579. IET.

Yadav, S. K. (2010). *Some problems in symmetric and asymmetric cryptography*, Doctoral dissertation, Department of Mathematics, DR. BR AMBEDKAR UNIVERSITY, AGRA.

Young-Oh, J. Y., Yang, D. I. and Chon, K. H. (2010). A selective encryption algorithm based on AES for medical information. *Healthcare informatics research*, *16*(1), 22-29

Zaidan, A. A., Zaidan, B. B., Alanazi, O. H., Gani, A., Zakaria, O., and Alam, G. M. (2010). Novel approach for high (secure and rate) data hidden within triplex space for executable file. *Scientific Research and Essays*, *5*(15), 1965-1977.

Zhang, H. (2012). Length-doubling ciphers and tweakable ciphers. In *Applied Cryptography and Network Security*. 100-116. Springer Berlin Heidelberg.