The Nucleus ***56***, *No. 3 (2019) 86-95*

www.thenucleuspak.org.pk

The Nucleus
ISSN 0029-5698 (Print)
ISSN 2306-6539 (Online)

Problems and Progressive Cryptanalysis of Prominent Block Ciphers

I.A. Shoukat[1], U. Iqbal[1*], M.S.A. Malik[2] and F. Sahar[1]

[1]*Riphah College of Computing, Riphah International University (Faisalabad Campus), Faisalabad, Pakistan*

[2]*Department of Information Technology, Government College University, Faisalabad, Pakistan*

ARTICLE INFO

Article history:
Received: *05 November, 2018*
Accepted: *25 October, 2019*
Published: *20 January, 2020*

Keywords:
AES,
Cryptanalysis,
DES,
DES-Variants,
Security issues

ABSTRACT

Practical cracking of Data Encryption Standard (DES) and mathematical cracking of Advanced Encryption Standard (AES) is seriously questionable despite the fact that AES retains good length of the encryption key, but still all encryption rounds have been cracked mathematically. Therefore, there is a need to revisit the cracking excursion of these well-known cryptosystems to inquire into potential discrepancies associated with them and to evolve the design of future block ciphers. Thus, this study aims to enlighten the cryptanalysis journey of AES and DES, including all DES variants (TDES, DESX and DEX+) to discuss latent weaknesses, issues and problems associated with these block ciphers. To accomplish this review task, quality of related studies was collected from several well-known research repositories and each study was critically analyzed. Earlier review-efforts were found relatively marginal in scope, capacity and are not up-to-date with the latest issues, and cryptanalysis results thereby differ with this work. The resultant discussion shows that known parameters like static substitution, static permutation, fixed block size and repeated encryption rounds with a similar set of encryption operations support the crackers in executing effective cryptanalysis in symmetric block ciphers. Therefore, encrypting the secret data with too many repeated encryption rounds with identical encryption operations is not as effective in enhancing the security of symmetric block cipher as it is usually believed.

1. Introduction

Noteworthy problems and cryptanalysis of several well-known block ciphers have been reviewed in this research. Early cryptanalysis was started in 1981 with the first CRYPTO conference to observe the leakage of some secret properties of Data Encryption Standard (DES). Differential cryptanalysis [1], was considered in CRYPTO'90 and linear cryptanalysis [2] was revealed in 1993 and later presented in EUROCRYPT'93. From 1993 to 2018, there is a gap of in-depth and collective cryptanalysis highlights of these selected cryptosystems. Although, several review efforts related to cryptanalysis of symmetric encryption algorithms are part of literature but these are limited in reviewing scope, capacity and are not up-to-date with the latest cryptanalysis. The cryptanalysis-based review conducted by Kelsey et al. [3] is not up-to-date as it is just limited to the studies published up to 1996. The cryptanalysis performed by Dobbertin et al. [4] and Campbell et al. [5] is not up to date, as it is only limited to AES. Similarly, the cryptanalysis effort made by Alani [6] is limited to DES and TDES without having the latest cryptanalysis status of AES.

Moreover, in earlier studies [7-10], few cryptanalysis highlights of DES, TDES, and AES were reported as compared to this research work. The survey [11] and the cryptanalysis study [12] only describe the security pitfalls related to RSA algorithm. The other recent and related work is limited to penetration analysis of AES and DES [13]; thereby limited in scope and capacity of cryptanalysis survey. We have discussed the design-related weaknesses of AES, DES, and Triple-DES. Thus, this article is more significant in reviewing of noteworthy problems and comprehensive cryptanalysis insights of selected block ciphers than the existing work. This work is also beneficial for researchers aiming to evolve future block ciphers in order to resist modern cryptanalysis.

2. Cryptanalysis and Weaknesses of DES

Fixed and known parameters in cryptography provide easy startup of cryptanalysis. DES uses Feistel network with fixed-sized data blocks and static substitution policy for encrypting data under constant and repeated iterations. In DES, the iterative mapping $m = 2t$ bits plaintext message, having left and right *blocks* L_0 *and* R_0 with corresponding cipher-text (R_r, L_r) is achieved after *r-rounds* $r \geq 1$. Through several rounds $(1 \leq n \leq r)$, the round n maps $(Ln-1,\ Rn-1) \rightarrow (Ln, Rn)$ as in Eq. (1).

$$\begin{cases} L_n = R_{n-1} \\ R_n = L_{n-1} \oplus f(R_{n-1}, K_n) \end{cases} \tag{1}$$

$$L_{n-1} \oplus f(R_{n-1}, K_n) \oplus f(R_{n-1}, K_n) = L_{n-1} \tag{2}$$

In Eq. (1) sub-keys can be obtained from K_n. For DES $K = 56$, $r = 16$ and $n = 64$ the sub-key with 48 bits is converted into eight parts each having *6 bits*. Thus, all these parameters *(8 parts, 6 bits, 16 rounds, etc.)* are executed several times iteratively with static and publicly known operations followed by XOR operation with key and data blocks as shown in Eq. (2). These fixed properties convert the Feistel structure to behave as a static mechanism in encrypting any given data block with an encryption key. The other weak point of Feistel structure is that it deals with a fixed number of enciphering rounds with 4 bits fixed permutation table. Due to these

---

[*] Corresponding author: umeriqbal15@gmail.com

reasons, it is not well suited to accommodate variable-sized data blocks.

Moreover, Feistel structure is considerably simpler in hashing abilities to negate chosen-plaintext attacks as discussed by Heys [14]. Furthermore, due to the simple Feistel logic, its design properties can easily be detectable for launching related-key distinguisher attacks [15]. The generic attack related to the Feistel schemes up to 5 rounds has been discussed by Patarin [16]. This generic attack takes computations either $\boldsymbol{\Theta}(2^{7n/4})$ for random plain or cipher-text or $\boldsymbol{\Theta}(2^{3n/2})$ for chosen plain or cipher-text. Possibly the six Feistel rounds can be vulnerable with 2^{32} trials through utilizing 2^{32} chosen-plaintexts in future as discussed by Patarin [16]. Therefore, similar types of attacks can be produced up to any number of rounds. The Splice-and-cut attack can exploit the 32 rounds of Feistel cipher with $2^{7.75n}$ time and memory complexities [17]. By using Meet-in-the-Middle attack, the 32 Feistel rounds require 2^{15n} and $2^{0.5n}$ time and memory complexities respectively which can be further reduced to $2^{7.75n}$ time complexity with $2^{7.25n}$ memory lookup trials having $2^{0.25n}$ chosen-plaintexts under collision attack [18].

Another weakness of Feistel cipher is associated with key scheduler in case of having high probability of the used differential (difference of the derivative function). It makes Feistel cipher susceptible towards related-key attacks without any condition of number of rounds. The differential can be found in the key-scheduler for *m-bit* blocks having *K-bit* keys. There exists differential $(\exists\Delta = K_S(K \oplus \Delta) \oplus K_S(K) \rightarrow^{\mathcal{P}} (\Delta_1, \Delta_2, \Delta_1, \Delta_2 \ldots\Delta_1, \Delta_2)$ with computational transformation $\{\mathcal{P}.\ 2^{-[r/2](|(\Delta 1)_{n-1}|+|(\Delta 2)_{n-1}|)} > 2^{-K}$ and $2^{-[r/2](|(\Delta 1)_{n-1}|+|(\Delta 2)_{n-1}|)} > 2^{-m}\} \Leftrightarrow$ distinguisher $(\mathcal{P} > 2^{-K})$ with the weak key having $(\mathcal{P}.\ 2^{K})$ is satisfied by the cipher. Suppose, if the function $\digamma.K_S(K)$ is DES-Key-Scheduler, for the original key (K), $\digamma.K_S(K)$ recover keys with $K_j\ j = 1,\ldots.r$ rounds under transformation: $\digamma.K_S(K) = (K1 \ldots\ldots Kr)$. In case of 2-related keys (K1, K2) the difference becomes: $(K1 \oplus K2 = -1)$ of all original key bits which satisfies for all j $(K_j^1 \oplus K_j^2 = -1)$. Now suppose X^1, X^2 are related plaintexts then $(X^1 \oplus X^2 = -1)$, *i.e.* $(Y_0^1 \oplus Y_0^2 = -1)$ and $(r_0^1 \oplus r_0^2 = -1)$ then the transformation for each j can be achieved as: $(Y^1_{j+1} \oplus Y^2_{j+1}) = \digamma.K_S(Y_j^1, K_j^1) \oplus r_j^1 \oplus \digamma.K_S(Y_j^1, K_j^1) \oplus r_j^1| = |Z(Y_j^1 \oplus K_j^1) \oplus r_j^1 \oplus Z(Y_j^1 \oplus -1 \oplus |K_j^1 \oplus -1)| \oplus r_j^1| = r_j^1 \oplus r_j^2 = -1$ then $(r^1_{j+1} \oplus r^2_{j+1}) = (Y_j^1 \oplus Y_j^2 = -1)$ which satisfies the complete difference in cipher-text with calculating $(Y_r^1 \oplus Y_r^2 = -1)$ and $(r_j^1 \oplus r_j^2 = -1)$.

The question of DES security including its design logic has been intensively discussed in Federal Information Processing Standards (FIPS); because substitution boxes (S-boxes) in DES deal with *fixed positions* which means DES has *static substitution* policy [19]. Due to this issue, it is ideally susceptible to linear and differential cryptanalysis attacks [20]. Any symmetric algorithm like DES works with *m-bit* blocks, *K-bit* key having random permutation $(K \in 2^K)$ on *m-bit* blocks, can easily be attacked with linear cryptanalysis [21, 22]. Linear attack probability $(\mathcal{P})$ requires linear approximate $(\partial \rightarrow ß)$ of binary function $(\digamma)$ which can be filtered through given input (∂) and output $(ß)$ values with probability computation having $\mathcal{P} = \Pr_y\{\partial.y = ß|\digamma(y)|\}$ on given input (y). This can be further reduced through deviation of $\mathcal{P}$ from ½ in case of correlation (₲) of $\mathcal{P}$ with $\{₲ = (|2\mathcal{P}| - 1)\}$. This always satisfies $(0 \rightarrow 0)$ linearity having $(\partial \rightarrow 0)$ or $(\partial \neq 0)$. By considering $\digamma$ permutations the $₲ = (0 \rightarrow ß)$ gives 0 for all $(ß \neq 0)$.

The other significant security issue with Feistel structure of DES is that it cannot encrypt complete block bits in single round because it only encodes *32 bits* of a block in single iteration. Thus, DES deficiencies make it insecure against exhaustive key searching attack. Its 64 bit fixed block size is not reliable for bulky bandwidth applications, and it is also not efficient in terms of software implementation due to bit by bit operations [23]. Linear cryptanalysis attacks are highly applicable on DES as the DES contains linear computations which have been shown inadequate for its security [24]. For example, if the right DES register $(R32 = X)$, where $X = (1,2,3\ldots\ldots32)$ binary bits applies permutation-expansion after encryption $(A = E(X))$, it becomes 48 bits under *Modulo-2* operation followed by the construction of *8 bit* S-box which further applies permutations $(Y = P(C))$ and *Modulo-2* operation on left DES register $(L32)$ bits. This procedure continues until all number of rounds are going through this linear transformation attack as shown in Fig. 1.

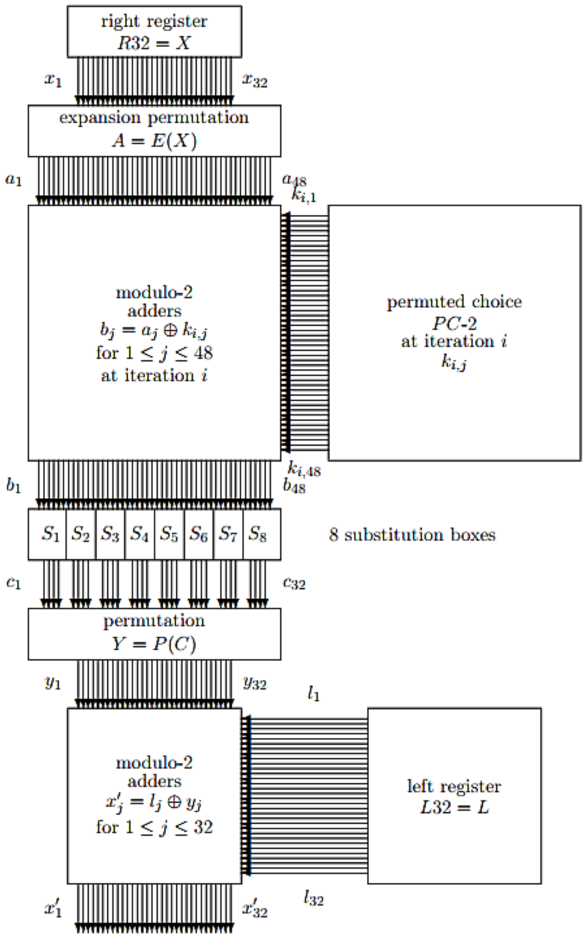

Fig. 1: Single round DES linear cryptanalysis.

This type of linear approximation can crack DES with a high success rate. Furthermore, smaller key bits of DES have made possible the implementation of several practical attacks. For example, in case of Feistel rounds *(r = 16)*, the key search $K = 2^{56}$ *bits* gives *(07.20581 × 10^{16} bits)* search trials that can be further reduced to 2^{55} bits which only gives *(03.60292 × 10^{16} bits)* average trails. The first exhaustive key searching attack was discussed by Hellman [25], which requires 10^6 DES chips to recover encryption key within 12 hours under the cost of US $ 20 million. A gate-level architecture was developed in 1993 as reported by Wiener [26] to crack DES with 57600 chips having 16 pipeline phases which can crack DES within 3.5 hours with a cost of US $ 1 million. Fig. 2, depicted the continued DES cracking efforts in different years to reduce the computational and financial cost [27].

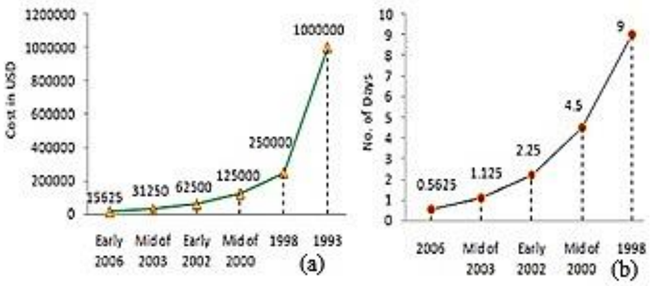

Fig. 2: (a) DES cracking cost in USD and (b) DES cracking time in days.

In 1998, the DES was cracked in *9 days* with a cost of US $ 250000 and later on, the number of days and cost were effectively reduced as shown in Fig. 2. The financial cost of DES cracking has been represented in Fig. 2 (A) and the reduction of cracking time has been depicted in Fig. 2 (B). In 1998, the Electronic Frontier Foundation (EFF) developed a cracker that cracked the DES in less than three days with the cost of US $ 250000 [28-30].

It has been discussed in several studies [1, 31-33], that the differential cryptanalysis with 2^{47} chosen plaintexts and 2^{50} known-plaintexts can efficiently crack DES as compared to the exhaustive key searching attack. The cryptanalysis review is summarized in Table 1, which shows that, the linear cryptanalysis takes 2^{43} known cipher and plaintext pairs to break the security of DES. The Spartan-3 FPGAs base COPACABANA machine can crack the security of DES within just nine days [34]. The cryptanalysis attacks such as Kunz-Jacques-Muller's and Matsui algorithm-2 can crack DES with time complexity (2^{43} and 2^{41}) respectively [35, 36]. Most significantly, the DES-56 has been cracked within 22 hours and 15 minutes as this attack was executed practically by Electronic Frontier Foundation [37]. However, the AES encryption key (128 bits) can be recovered within just 15 seconds through Semi-Synchronous Attack (SSA) [38] and the neuro-cryptanalysis attack can practically crack DES within just 51 minutes.

Table 1: Cryptanalysis status of DES.

DES atacks	Source	Memory trial	Time complexity
Chosen-plaintext differential attack	[1, 31, 32]	–	2^{47} trials
Known-Plaintext-Cipher Pairs Linear cryptanalysis Attack	[2, 24]	–	2^{43} rials
Neuro-cryptanalysis	[6]	–	51 minutes
16-round Linear cryptanalysis of DES		–	$03.60292 \times 10^{16\ \text{bits}}$
Brute force search attack with 10^6 chips	[22]	–	12 hours
Gate-circuit based DES cracker with 57600 chips and16 pipelines	[26]	–	3.5 hours
EFF DES Cracker	[28-30]	–	3 days
Known-plaintext improved Davies' attack	[32, 33]	–	2^{50} trials
Spartan-3 FPGAs based COPACABANA DES cracker	[34]	–	9 days
Matsui algorithm-2 attack	[35]	2^{33}	2^{41}
Kunz Jacques-Muller's attack	[36]	2^{53}	2^{43}
EFF DES cracker-2008	[37]	–	22.25 hours

Nowadays DES is considered as insecure due to several practical attacks such as exhaustive key search attack. This attack can recover secret key in such a way, if key bits *($b_1, b_2, b_3 \ldots. b_{2^k}$) $\in K$* having binary values *h* with parameter $1 \leq j \leq 2^h$ then the attacker (A_{tk}) can compute n-bit computations with *$\{(n-1) \rightarrow M_n; F(M_n) \rightarrow C_n\}$*. Similarly for whole key $_2{}^k$ bits this calculation requires $\{\forall\ a \in (1, \ldots j): E(T_a, M_n) = C_n\}$ *gives T_a then $E(A_{tk}) = 1$* because $T \in \{ b_1, b_2, b_3 \ldots b_2{}^k \}$and *K is constant* with *$(M_1, C_1) \ldots\ldots.. (M_j, C_j)$and* in case of small *j*, the *$\forall\ (J) > K/h$* can recover *K*. In 2005, for practical implementation of exhaustive key search, specialized hardware referred as SHARK, was developed to factor 1024 bit key by Kumar et al. [34]. US $ 200 million were consumed in this factorization. For the same factorization, the time and financial cost was further decreased to just US $ 2 million through matrix calculations.

3. Cryptanalysis of DES Variants

The smaller key (*56 bits*) of DES was the main reason for its security crackdown. Therefore, variety of DES variants such as Triple DES, Extend Data Encryption Standard (DESX) and DESX+ were introduced. Double DES uses two 56 bits key(s), and DESX uses 120-bit lengthy encryption key.

Both DESX and DESX+ also remained unable to resists cryptanalysis attacks in past years, as summarized in Tables 2 and 3, respectively.

According to the cryptanalysis summary (Tables 2 and 3), the computational complexity, to crack DESX was 2^{120} in 1992 under two related key pairs which was further reduced to 2^{113} with the use of 2^{32} related key pairs in 1996-2001. Similarly, with 2^{32} and $2^{32.5}$ related key pairs, the cryptanalysis complexities were limited to 2^{88} and $2^{87.5}$ encryption trails in 1992 and 2000, respectively. In 1997 and later on in 2008, the overall DESX complexity was reduced to 2^{56} encryption trials. In case of cryptanalysis of DESX+, the cracking complexities were initially limited to 2^{120} encryption trials in 2004 under two-pairs related key attack which was further reduced to 2^{56} encryption trails in 2008. Thus, DESX is more resistive than DESX+ in related key attacks.

Table 2: Cryptanalysis status of DESX.

Attacks on DESX	Source	Memory trails	Encryption trails
Related key pairs (2 pairs) attack	[39]	–	2^{120}
Chosen-Plaintext (2^{32}) related key Attack	[39]	–	2^{88}
Related key pairs (2^{32} pairs) attack	[40, 41]	–	2^{113}
Related key pairs ($2^{32.5}$ pairs) attacks	[42]	$2^{32.5}$	$2^{87.5}$
2^7 related key pairs attack		–	2^{56}
$2^{3.5}$ faulty key pairs attack	[43]	–	2^{56}

Table 3: Cryptanalysis status of DESX+.

Attacks on DESX+	Source	Memory trails	Encryption trails
2^7 related key pairs attack	[43]	–	2^{56}
Faulty key pairs (2 pairs) attacks	[43]	-	2^{56}
Related key pairs (2 pairs) attacks	[44]	2^{56}	2^{56}
Related key pairs (2 pairs) attacks	[44]	–	2^{120}

4. Cryptanalysis and Weaknesses of TDES

Triple-DES (TDES) proposal was the enhancement of DES to maximize its security using multiple encryption key(s). TDES uses 64 fixed block size [45, 46] and three encryption keys *(K1 = 56, K2 = 56, K3 = 56)* where the *K1* and *K3* are the same which reduces its effective key length up to just 112 bits rather to 168 bits. The double encryption in Triple-DES is not optimal to maximize TDES security over the security of the first version of DES with single key encryption. Moreover, TDES can be attacked through known-plaintext attack. This attack only requires 2^{56} memory spaces with time complexity (2^{112}) to search out its encryption key. The cryptanalysis status of TDES has been summarized in Table 4.

By using parallel hardware machines, another attack was introduced by Van-Oorschot and Wiener [47]; which requires time complexity (2^{32}) to break the security of Triple DES. This attack is four times faster than the exhaustive key searching attack. By choosing three or four different chucks of cipher-texts under chosen-ciphertext-attack, the mathematical cracking of the TDES algorithm requires only 2^{56} memory lookup trails within time complexity having 2^{58} encryption trials [48]. Similarly, many efforts have also been reported previously to break the security of TDES using Known-IV attack under time complexity of 2^{56} trails without considering memory trails [49, 50]. This type of Known-IV attack, takes plaintext chunks denoted with *(A, A, B)* for attacking the two modes *ECB|ECB* of TDES having cipher-texts $(\acute{C}_0^{tx}, \acute{C}_1^{tx}, \acute{C}_2^{tx})$. The middle values $\{(A`, A`, B`), (A``, A``, B``)\}$ after applying the first and 2nd ECB modes as shown in Fig. 3. This can be further transformed as $\{Z^{-1}_{K3}(IV_3 \oplus \acute{C}_0^{tx}) = IV_3 \oplus \acute{C}_0^{tx} \oplus \acute{C}_1^{tx}\}$ which can recover K in 2^{56} *bits* exhaustive search trails rather to 2^{64} bits trails.

Table 4: Cryptanalysis status of TDES.

TDES attacks	Source	Memory space	Time complexity
Practical Neuro-Cryptoanalysis with 2^{12} plaintext-cipher-text pairs	[6]	–	72 minutes
Known Plaintext Attack	[45]	2^{56}	2^{112}
Parallel Hardware Machine with Known plaintext and cipher-text pairs	[47]	–	2^{32}
Chosen Plaintext of Cipher Text (3 or 4)	[48]	2^{56}	2^{58}
Known-IV attack	[49]	–	2^{56}

The small block size is another issue with TDES just like DES, therefore, it is more feasible to apply quantum attacks. The use of TDES is on peak but, it is three times slower than DES and its limited key size is not resistive against quantum computers which might be applicable on TDES any time in future [51].

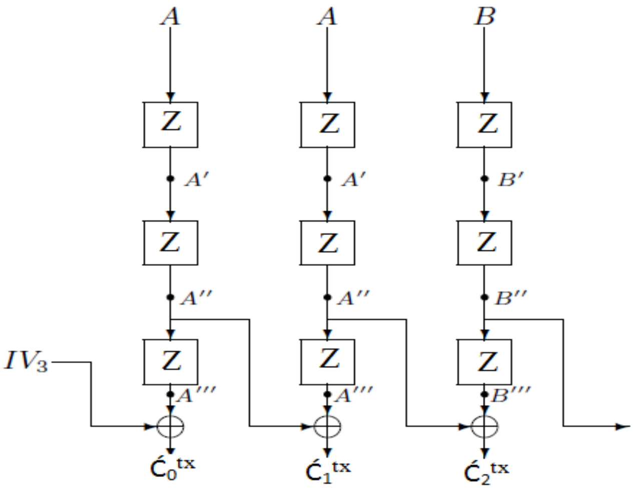

Fig. 3: TDES Known-IV attack [49].

Both DES and TDES utilize Feistel logic and static S-boxes without having any direct correlation with encryption key [52, 53]. These S-boxes retain static and publicly known values which are not dependent on the secret key. As the substitution process creates diffusion in any encryption algorithm by changing or substituting the plaintext, but in case of DES and TDES, this substitution function is based on static and known values due to which it is not a good approach to get optimal security [54]. A recent neural network based known-plaintext-attack can practically crack Triple-DES in just 72 minutes with computational complexity of 2^{12} plaintext-cipher-text pairs. This attack was executed without the use of encryption key. The total 1093 trails were considered to execute this attack in which 993 failed, but 100 trials worked successfully to crack TDES. In case of DES 833 trails were trained with complexity 2^{11} plaintext-cipher-text pairs in which 733 failed and 100 were successful. In case of DES the training complexity (2^{11} plaintext-cipher-text pairs) are many times lesser to differential and linear approximation complexity (2^{47}, 2^{43}) of DES. Triple DES is a variant of DES and also based on Feistel cipher; therefore, it associates all Feistel design limitations such as fixed-sized data blocks, static substitution, repeated encryption rounds with similar operations, weak block size and non-applicability of Feistel cipher for dynamic data blocks.

5. Cryptanalysis and Weaknesses of AES

Advanced Encryption Standard (AES) with variable key lengths (128, 192, 256 bits) was declared as Federal Information Processing Standard by National Institute of Standards and Technology (NIST) in 2001 FIPS [55]. AES picks message chunks with *fixed block lengths (128 bits)* and applies static substitution along with constant and repeated encryption process. Random permutations are not effective in fixed-sized data blocks. Existing S-box design of AES is unchangeable with corresponding secret key due to which it is more likely to be vulnerable against differential attacks [56]. The S-box algebra denotes input *(α)* and output *(β)* as a fixed relation of $\alpha \rightarrow \beta$ which becomes $6 \rightarrow 4$ in case of DES and $8 \rightarrow 8$ S-box in case of *AES*. Due to ineffective permutations, the differential probability becomes negligible against the larger probability of differential attacks [57]. This fixed relationship is the significant discrepancy of AES to assault its S-box design with linear and differential attacks. Therefore, fixed-sized data blocks, static substitution, and constantly repeated encryption rounds with identical encryption operations have been considered as major weaknesses of AES. Fixed parameters are significantly beneficial in triggering of linear and differential attacks. Linear and differential attacks ideally require known parameters to be established as explained by Xiao and Heys [58].

The Substitution-Permutation Network (SPN) is more secure than the Feistel Network; however, several discrepancies in SPN have been pointed out in recent years [59]. The surreptitious architecture of any SPN based block cipher can be recovered under practical assumptions because SPN is feeble in linear cryptanalysis. This clearly invokes the inadequacy of SPN to resist side-channel attacks. The differential cryptanalysis of SPN based cipher (AES) has been conducted; where by selecting the eight thousand ciphers and plaintexts SPN was shown breakable. Therefore, SPN is vulnerable to modern cryptographic attacks. Cryptanalysis of AES has actively been performed in past years. Initially, a chosen-plaintext attack was introduced by Biryukov et al. [60]; that can crack five rounds of AES with 2^{46} and 6 rounds of AES with 2^{78} encryption trails. This attack is also known as Boomerang attack. The time complexity of the same attack was reduced to 2^{32}, and 2^{72} encryption tries against the fifth and sixth round of AES as discussed by Daemen et al. [61]. Initially, this attack was limited up to the fifth or sixth number of rounds, but later on, the AES with 192-bit key and the AES with 256-bit key was considered to crack up to 7 rounds by executing 2^{32} chosen plaintext attack with 2^{140} encryption efforts as reported by Gilbert and Minier [62].

A practical cache timing attack was applied on AES in open secure socket layer (open SSL) based local server connected with several computers. For executing this attack, 200 million chosen plaintexts were selected, and as a result, AES key was successfully recovered in 1 day as reported. In defense, AES defenders claimed that it was due to the incorrect implementation of AES and to get actual AES security it should be implemented on well-designed hardware by Bernstein [63]. In recent and past years, AES has been affected by a bundle of cryptanalysis attacks with a different number of rounds with different complexities, as summarized in Table 5.

The AES proposal was to resist attacks but through recent cryptanalysis, the 8 AES rounds can be cracked with computational complexities (2^{172} and 2^{196}) [64]. In case of AES-192 and AES-256, the 6 rounds of AES-128 can be cracked even with lesser computational complexities [65, 66]. This type of AES cracking might be possible practically in the future for those attack models which accept chosen input data block as chosen key to perform cryptanalysis [67]. The time complexity of the 7 AES rounds was further reduced in 2009, which was significantly lesser than the complexity of previous attacks [68].

Cryptanalysis approaches were carried out in 2011, 2014 and 2015. Lu, introduced a new cryptanalysis attack ("Impossible boomerang attack – an extension of boomerang attack") that can crack AES. He executed impossible boomerang attack to break all versions of AES with nine rounds and find reasonable security limitations in AES. However, recent literature contains significant cryptanalysis of AES with surprising outcomes [69, 70]. Moreover, AES with the 256-bit key was academically cracked up to 10 numbers of round with 2^{39} encryption and 2^{45} encryption trials as discussed by Biryukov et al. [71]. The working criteria of these attacks were to take XOR of cipher-text by selecting 2-related keys in different manners. The ten rounds of AES have also been shown insecure against two relate-sub-keys based chosen cipher-text attack with the complexity of 2^{45} lookup trials and 11 rounds with 2^{70} lookup trials through implementing the *quasi-practical attack*. The full 14 rounds of AES-256 are now considered as insecure with 2^{120} data and time complexity trials under the implementation of *chosen key distinguisher attack*. According to the cryptanalysis efforts claimed in [71], AES is not optimally secure because AES-192 is vulnerable under differential cryptanalysis with 2^{176} encryption trails and AES-256 can be cracked with the computational complexity of 2^{119}. The most recent full round attack complexities have been reduced to $2^{253.87}$ in case of AES-256, $2^{189.51}$ for AES-192 and $2^{125.56}$ for AES-128. The biclique attack only requires $2^{126.3}$ up to $2^{127.4}$ computational complexities for defeating the security of AES-128.

Table 5: Cryptanalysis status of AES.

AES rounds	Attack type	Data trails	Memory trails	Time complexity
6-round partial sum attack to recover 128 bit AES Key [9]	Partial sum with different Δ-set (2 and 3) using 156 sub-processes.	–	–	25.8 hours
Full 10 rounds of AES-128 [22]	Key recovery without Sieve-in-the-middle (SIM)	2^{128}	2^{8}	$2^{125.56}$
Full 12 rounds of AES-192 [22]	Key recovery without SIM	2^{128}	2^{8}	$2^{189.51}$
Full 14 rounds of AES-256 [22]	Key recovery without SIM	2^{128}	2^{8}	$2^{253.87}$
9 Rounds of AES-256 [46]	Related key impossible Boomerang attack	2^{123}	–	$2^{239.9}$
Full 14 rounds of AES-256 [63]	chosen key distinguisher attack	2^{120}	–	2^{120}
8 Rounds of AES-128	Biclique cryptanalysis key recovery attack	2^{88}	2^{8}	$2^{125.34}$
Full 10 rounds of AES-128	Biclique cryptanalysis key recovery attack	2^{88}	2^{8}	$2^{126.18}$
9 Rounds of AES-192	Biclique cryptanalysis key recovery attack	2^{80}	2^{8}	$2^{188.8}$
Full 12 rounds of AES-192	Biclique cryptanalysis key recovery attack	2^{80}	2^{8}	$2^{189.74}$
Nine rounds of AES-256	Biclique cryptanalysis key recovery attack	2^{120}	2^{8}	$2^{251.92}$
Full 14 rounds of AES-256	Biclique cryptanalysis key recovery attack	2^{40}	2^{8}	$2^{254.42}$
7 rounds of AES-128 [64]	Meet-in-the-Middle (MITM) attack	2^{97}	2^{98}	2^{99}
8 rounds of AES-192 [64]	MITM attack	2^{107}	2^{96}	2^{172}
9 rounds of AES-256 [64]	MITM attack	2^{120}	2^{203}	2^{203}
6 rounds of AES-128 [65]	Integral cryptanalysis	2^{64}	–	2^{90}
Full 10 rounds of AES-128 [66]	Biclique cryptanalysis (IV)	–	–	$2^{126.3} – 2^{127.4}$

The cracking – of AES up to all of its rounds is very shocking and minimizing its security satisfaction. The AES design simplicity is a major cause of understanding its design by crackers [72, 73]. The AES proposal was to resist attacks but recent cryptanalysis is more critical to be applicable practically any time in future for those modes of operations which accept chosen input block in the form of key. Because large scale machine attack requires only time complexity (2^{100}) against AES-128 and AES-256 [74]. Thus, AES is fixed-sized block cipher, having fixed substitution strategy and these both static features are more helpful for the crackers to build a cryptanalysis attack [75]. For recovering 16 bytes (16 × 8 = 128 bits) key, the 6-round partial sum attack was applied in 2015. There were four machines used with four cores Intel Pentium processors (G640 @ 2.80GHz) each having 8GB RAM. Total 25 processes were initiated in which very first process was for the main attack. Similarly, other 24 sub-processes were also initiated as a supportive process for the main attack. After that, two different numbers of Δ-set (2 and 3) were selected to recover 128-bit AES key under 6-round partial attack. Finally, the 128-bit secret key of 6th AES-round was recovered in 25.8 hours as discussed in Table 5.

6. Analysis and Discussion

In cryptography, the open challenge is to discover a truly hard problem in the form of a cryptographic algorithm. In terms of cryptanalysis, the truly hard problem means that cryptanalysis cannot be discovered or initiated against the cryptographic algorithm. Almost, all the existing well-known and complex cryptographic puzzles (AES, TDES, DES) have been solved either mathematically or practically as witnessed in this article (Table 6). In order to stay secure, future cryptanalysis and security threats would significantly be preventive against cryptosystems. Secure and reliable data transmission is essentially exigent in insecure communication channels. Secure communication can either be fulfilled through the use of symmetric or asymmetric cryptosystems. Symmetric cryptosystems, generally known as block ciphers, are effective in speedy encryption but unreliable in key exchange [76].

However, asymmetric cryptosystems are inefficient in data encryption, require large memory, consume more electric power and are not able to encrypt large data, but asymmetric cryptosystems retain the advantage of reliable key exchange [77]. In this situation, the use of hybrid cryptosystems can provide the advantages of both schemes, but this does not mean that question of secure communication or secure encryption algorithm has been solved because the security of any cryptosystem is based on randomness and dynamic properties. How a hybrid system can be amalgamated, it has been elaborated previously by Shoukat et al. [77]. Several new metrics have been suggested in order to evaluate the security of newly designed cryptographic algorithms [78]. These new security evaluation metrics include block dynamicity-dynamic sized data blocks, dynamic substitution with random masking of key-bits, and operational randomness. Although existing encryption algorithms have good randomness properties but the recent mathematical cracking of AES and practical cracking of (DES and TDES) is seriously questionable. The current security status of DES, TDES and AES are summarized in Table 6.

Table 6: Current security status of prominent block ciphers.

Parameters	DES	TDES	AES
Mathematically cracked	✓	✓	✓
Practically cracked	✓	✓	✗
Significantly resistive to Brute force search attack	✗	✓	✓
Applicability of differential and linear attacks	✓	✓	✓
Works with Feistel network Note: Attacks exist for Feistel network	✓	✓	✗
Works with SPN Note: Attacks exist for SPN	✗	✗	✓

In the presence of modern cryptanalysis, the current design of DES and AES are not effective in dynamic properties, e.g., dynamic sized data blocks and dynamic substitution. AES takes fixed data block chunks (128 bits) for encryption which should be changed to dynamic block chunks. The dynamic data blocking idea for symmetric cryptosystems was introduced in early 2014 by Shoukat et al. [79].

Rather taking of fixed chunks data blocks for encryption, the dynamic block selection involves little more processing effort, which is negligible for today's high-speed processors. Even the small devices like iPads, tabs, and smartphones retain very speedy processors. Speedy encryption and security both are important factors, but security is more essential than encryption speed. The existence of asymmetric encryption algorithms justifies this statement because asymmetric encryption algorithms are almost 100 times slower than symmetric encryption algorithms [80]. Both speed and security always contradict each other because a number of encryption rounds in existing block ciphers increase processing time but do not enhance encryption security. In terms of speed and security, the existence of Triple-DES is also notable because it is much slower than DES [81]. Therefore, security cannot be compromised upon speed. Thus, it is needful to use dynamic sized data blocks in symmetric cryptosystems to resist modern cryptanalysis. Modern attacks are more likely or effectively applicable to fixed-sized data blocks due to known bit-length of data blocks. Fixed block length means the same sized secret key is implemented on it. Therefore, known block length provides calculative exhaustive key searching, which can be more dangerous in case of known-plaintext attack.

Fixed block size is always publically known, meaning that it is also known to a cracker. Known parameters in cryptographic algorithms always provide ideal trapdoor to build effective cryptanalysis [82]. The recent cryptanalysis status of TDES and AES (Tables 4 and 5) justifies the consequences of fixed-sized blocks and static natured substitution. Both encryption algorithms DES and AES deal with fixed-sized data blocks and static natured substitution policy. Static Substitution and fixed-sized blocks are not good to resist modern attacks, as discussed earlier. Permutations are least effective in case of static substitution, because permutations in case of static substitution become just a matter of computational efforts. With static substitution, after fourth AES-round, the difference based active S-boxes in AES is around 25 in any differential path. The idea of approximating of active S-box in AES is helpful in reducing the higher probability limit (upper limit) of a differential path. Moreover, recent advancements in Universal Symmetry Detection algorithm might be more helpful to reveal symmetries in fixed S-box of existing block ciphers [83]. At present AES deals with single-key security model rather than related-key security module through which attacker can easily insert the differences in plaintext, cipher-text as well as in secret key. It is more censorious towards the security of AES that its statics-box has no direct correlation secret key. Therefore, static substitution policy should be replaced with dynamic or randomized substitution approach and fixed-sized data blocks in symmetric cryptosystems should be replaced with dynamic sized data blocks.

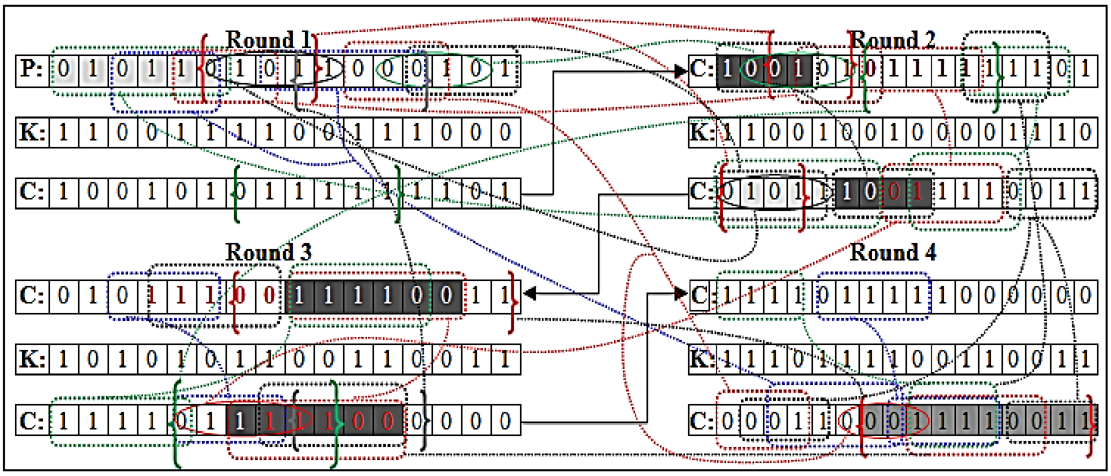

Fig. 4: Repeated bit patterns with repeated rounds under static operation(s).

Moreover, repeating too many encryption rounds with a static or similar set of encryption operations is not a wise decision. It has been elucidated that the idea of repeated encryption rounds with the same number of encryption operations does not offer optimal difficulties for the crackers because of changing binary digits 0 to 1 and 1 to 0 again and again. Therefore, the conversion from 0 to 1 and 1 to 0 within the repeated loop is not as effective for enhancing the security of symmetric ciphers as it has been assumed. Thus, it is a significant misunderstanding that repeated encryption rounds greatly enhances the security of a cipher. For example, in Fig. 4, we have applied a static encryption operation up to 4 rounds under randomly selected encryption key. The plaintext (P) was ciphered using static encryption operation *(Exclusive-OR)* to generate cipher-text *(C)* in each round by using random encryption key *(K)* as $C = P \oplus K$. Each time the C of the first round was considered as Plaintext *(C = P)* for subsequent encryption rounds as depicted in Fig. 4.

The overall encryption process was conducted to show that the use of static or fixed encryption operation even under random encryption key gives several repeated binary patterns in cipher-text. Too many repeated binary patterns were found among the round-based encryption, as highlighted in Fig. 4. Regardless of the number of rounds whether it's 4 or 14, it is very difficult to reduce repeating binary patterns in block ciphers while using static encryption operation due to the limit of binary digits up to only digits, i.e., (0 or 1). Upon applying the static or fixed encryption operation repeatedly causes only the replacement of either 1→0 or 0→1 in each iteration using random encryption key as shown in Fig. 4. This type of repeated behavior of binary bits may cause the worst situation in case of similar key on each round.

Only a few efforts have been made to evolve the design of static block ciphers with dynamic features such as randomized substitution [84], dynamic data blocking [85] and dynamic selection of encryption operations in each encryption round [86]. In the last ten years, efforts have been made to convert the static S-box design to dynamic S-box [87, 88]. Therefore, there is a need to revise the design of existing symmetric block ciphers with randomized properties.

It is seriously noticeable towards existing encryption methods that utilize static encryption operations. Fixed parameters or repeated patterns in cryptographic algorithms ideally provide trapdoors to crackers during cryptanalysis. Currently, all well-known block ciphers deal with fixed features. These fixed features include fixed sized data blocks, fixed substitution and a fixed set of known encryption operations in each encryption round. These fixed features should be replaced with dynamic features in order to enhance the security of block ciphers. As much dynamicity and randomness will be increased in cryptographic algorithms, the chances of cryptanalysis will effectively be decreased. In earlier paragraphs, it has been discussed why dynamic features are needed and why security cannot be compromised upon speed.

7. Conclusions

From the present study we can conclude that it is too risky to use existing block ciphers (TDES and AES) to achieve optimal data encryption with their current designs. The attack models are being evolved day by day with novel cracking tricks. DES security badly failed in earlier decades due to its practical cracking. Now, TDES has also been cracked practically under neuro-cryptanalysis, and AES has been cracked mathematically, as shown in Tables 5 and 6. One thing which can be calculated mathematically can undoubtedly be executed practically. The broken history of AES is alarming. The danger of practical attacks which can be possible at any time in near future. Thus, there is an emergent need to revise the design of symmetric cryptosystems in order to introduce more dynamic features. The use of dynamic features is a good and timely decision to accelerate the dynamicity and randomness in symmetric block ciphers. In this way, the attacking trapdoors will be diminished and cryptographic algorithms will significantly be resistive to modern cryptanalysis. Future crypto-designs should deal with dynamic sized data blocks rather then fixed-sized data blocks. Moreover, static substitution should not be linked to the lookup table(s); it should be dynamic or randomized in linkage with a secret encryption key.

References

[1] E. Biham and A. Shamir "Differential cryptanalysis of the data encryption standard (1st edition)", ISBN 978-1-4613-9314-6, vol. 1, pp. 188, 1993.

[2] M. Matsui, "Linear cryptanalysis method for DES cipher", Adv. Cryptol. - Eurocrypt'93, vol. 765, no. 5, pp. 386-397, 1993.

[3] J. Kelsey, B. Schneier and D. Wagner, "Related-key cryptanalysis of 3-way, biham-des, cast, des-x, newdes, rc2, and tea", Inf. Commun. Secur., vol. 1334, pp. 233-246, 1997.

[4] H. Dobbertin, L. Knudsen and M. Robshaw, "The cryptanalysis of the AES– A brief survey", Adv. Encryption Standard-AES, LNCS, vol. 3373, pp. 1–10, 2005.

[5] S. Campbell, M. Grinchenko and W. Smith, "Linear cryptanalysis of simplified AES under change of S-box", Cryptol., vol. 37, no. 2, pp. 120-138, 2013.

[6] M.M. Alani, "Neuro-Cryptanalysis of DES and Triple-DES", Neural Inf. Process., Lect. Notes Comput. Sci., vol. 7667, no. 1, pp. 637-646, 2012.

[7] H. Alanazi, B.B. Zaidan, A.A. Zaidan, H.A. Jalab, M. Shabbir and Y. Al-Nabhani, "New comparative study between DES, 3DES and AES within nine factors", J. Comput., vol. 2, no. 3, pp. 152-157, 2010.

[8] L.R. Knudsen and M.J. Robshaw, "A short survey and six prominent ciphers", The Block Cipher Companion, vol. 1, pp. 193-219, 2011.

[9] M. Ågren, C. Löndahl, M. Hell and T. Johansson, "A survey on fast correlation attacks", Cryptogr. Commun., vol. 4, no. 3, pp. 173-202, 2012.

[10] P. Mahajan and A. Sachdeva, "A study of encryption algorithms AES, DES and RSA for security", Global J. Comput. Sci. Tech. (GJCST), vol. 13, no. 15, 2013.

[11] K. Gagneja and K.J. Singh, "A survey and analysis of security issues on RSA algorithm", Res. J. Appl. Sci., Eng. Tech., vol. 11, no. 8, pp. 847-853, 2015.

[12] D. Genkin, A. Shamir and E. Tromer, "Acoustic cryptanalysis", J. Cryptol., doi: 10.1007/s00145-015-9224-2, vol. 30, no. 02, pp. 392-443, 2017.

[13] S. Ahuja, R. Johari and C. Khokhar, "CRiPT: cryptography in penetration testing", Proc. Second Int. Conf. Comput. Commun. Techn., vol. 3, pp. 95-106, 2016.

[14] H.M. Heys, “Information leakage of Feistel ciphers”, IEEE Trans. on Inf. Theory, vol. 47, no. 1, pp. 23-35, 2001.

[15] A. Biryukov and I. Nikolic, “Complementing Feistel ciphers”, Fast Softw. Encryption- Lect. Notes Comput. Sci., vol. 8424, pp. 3-18, 2014.

[16] J. Patarin, “Generic attacks on Feistel schemes”, Adv. Cryptol. - ASIACRYPT 2001, vol. 2248, pp. 222-238, 2001.

[17] T. Isobe and K. Shibutani, “Generic key recovery attack on Feistel scheme”, Adv. Cryptol. - ASIACRYPT 2013 Lect. Notes Comput. Sci., vol. 8269, pp. 464–485, 2013.

[18] I. Dinur, O. Dunkelman, N. Keller and A. Shamir, “New attacks on Feistel structures with improved memory complexities”, Adv. Cryptol. – CRYPTO 2015, Lect. Notes Comput. Sci., vol. 1, pp. 433-454, 2015.

[19] B. Saini, “Implementation of AES using S-box rotation”, Int. J. Adv. Res. Comput. Sci. Softw. Engrg., vol. 4, no. 5, pp. 1322-1326, 2014.

[20] S. Sahmoud, W. Elmasry and S. Abudalfa, “Enhancement the security of AES against modern attacks by using variable key block cipher”, Int. Arab J. e-Technol., vol. 3, no. 1, pp. 17-26, 2013.

[21] M. Matsui, “The first experimental cryptanalysis of the Data Encryption Standard”, Adv. Cryptol. - Crypto’99, vol. 839, pp. 1-11, 1994.

[22] A. Bogdanov and M. Wang, “Zero correlation linear cryptanalysis with reduced data complexity”, Fast Softw. Encryption, vol. 7549, pp. 29-48, 2012.

[23] S. McMillan and C. Patterson, “JBits™ implementations of the advanced encryption standard (Rijndael)”, Field-Programmable Log. Appl., vol. 2147, pp. 162-171, 2001.

[24] M. Ebrahim, S. Khan and U.B. Khalid, “Symmetric algorithm survey: A comparative analysis”, Int. J. Comput. App., vol. 61, no. 20, pp. 12-19, 2013.

[25] M.E. Hellman, “A cryptanalytic time-memory trade-off”, Inf. Theory, IEEE Trans. on, vol. 26, no. 4, pp. 401-406, 1980.

[26] M.J. Wiener, “Efficient DES key search”, Sch. Comput. Sci., Carleton Univ., vol. 1, 1993.

[27] S.G. Kelly, “Security implications of using the data encryption standard (DES). RFC 4772: Informational DES security implications”, IETF Trust, 2006.

[28] L. Batina, N. Mentens, E. Oswald, J. Pelzl and C. Priplata, “DVAM3 hardware crackers”, ECRYPT-European Netw. Excellence Cryptol., IST-2002-507932, vol. 1, no. 7, pp. 2-3, 2005.

[29] A.A. Zaidan, B.B. Zaidan, O.H. Alanazi, A. Gani, O. Zakaria and G.M. Alam, “Novel approach for high (secure and rate) data hidden within triplex space for executable file”, Sci. Res. Essays, vol. 5, no. 15, pp. 1965-1977, 2010.

[30] M. Abomhara, O. Zakaria, O.O. Khalifa, A.A. Zaidan and B.B. Zaidan, “Enhancing selective encryption for H. 264/AVC using advanced encryption standard”, Int. J. Comput. Electrical. Engg., vol. 2, no. 2, pp. 223-229, 2010.

[31] E. Biham and A. Shamir, “Differential cryptanalysis of DES-like cryptosystems”, J. Cryptol., vol. 4, no. 1, pp. 3-72, 1991.

[32] E. Biham and A. Biryukov, “An improvement of Davies' attack on DES”, Adv. Cryptol - EUROCRYPT'94, vol. 950, pp. 461-467, 1995.

[33] E. Biham and A. Biryukov, “An improvement of Davies’ attack on DES”, J. Cryptol., vol. 10, no. 3, pp. 195-205, 1997.

[34] S. Kumar, C. Paar, J. Pelzl, G. Pfeiffer and M. Schimmler, “Breaking ciphers with COPACOBANA – A cost-optimized parallel code breaker”, Crypt. Hardw. Embedded Syst-CHES. vol. 4249, pp. 101-118, 2006.

[35] Y. Lu and Y. Desmedt, “Improved Davies-Murphy’s Attack on DES Revisited”, Found. Pract. Secur., vol. 8352, pp. 264-271, 2014.

[36] S. Kunz-Jacques and F. Muller, “New improvements of Davies-Murphy cryptanalysis”, In ASIACRYPT, LNCS, vol. 3788, pp. 425-442, 2005.

[37] T. Pazynyuk, J.Z. Li and G.S. Oreku, “Improved Feistel-based ciphers for wireless sensor network security”, J. Zhejiang Univ. SCI. A, vol. 9, no. 8, pp. 1111-1117, 2008.

[38] B. Gülmezoglu, M.S. Inci, G. Irazoqui, T. Eisenbarth and B. Sunar, “A faster and more realistic flush+reload attack on AES”, In COSADE-2015, 13-14 April, Berlin, vol. 9064, pp. 1-16, 2015.

[39] J. Daemen, “Limitations of the Even-Mansour construction”, Adv. Cryptol. - ASIACRYPT'91, vol. 739, pp. 495-498, 1992.

[40] J. Kilian and P. Rogaway, “How to protect DES against exhaustive key search”, Adv. Cryptol. - CRYPTO’96, vol. 1109, no. 8, pp. 252-267, 1996.

[41] J. Kilian and P. Rogaway, “How to protect DES against exhaustive key search (an analysis of DESX)”, J. Cryptol., vol. 14, no. 1, pp. 17-35, 2001.

[42] A. Biryukov and D. Wagner, “Advanced slide attacks”, Adv. in Cryptol. – EUROCRYPT 2000, vol. 1807, no. 5, pp. 589-606, 2000.

[43] R.C.W. Phan and A. Shamir, “Improved related-key attacks on DESX and DESX+”, Cryptol., vol. 32, no. 1, pp. 13-22, 2008.

[44] R.C.W. Phan, “Related-key attacks on triple-DES and DESX variants”, Top. Cryptol. - CT-RSA 2004, vol. 2964, pp. 15-24, 2004.

[45] R.C. Merkle and M.E. Hellman, “On the security of multiple encryption”, Commun. ACM, vol. 24, no. 7, pp. 465-467, 1981.

[46] J. Lu, “The (related-key) impossible boomerang attack and its application to the AES block cipher”, Des., Code. Crypto., vol. 60, no. 2, pp. 123-143, 2010.

[47] P.C. Van-Oorschot and M.J. Wiener, “A known-plaintext attack on two-key triple encryption”, Adv. Cryptol. - Eurocrypt’90, vol. 473, pp. 318-325, 1991.

[48] E. Biham and A. Shamir, “Differential cryptanalysis of the data encryption standard”, Springer Sci. Bus. Media, Springer Verlag, pp. 1-188, 2012.

[49] D. Hong, J. Sung, S. Hong, W. Lee, S. Lee, J. Lim and O. Yi, “Known-IV attacks on triple modes of operation of block ciphers”, Adv. Cryptol-ASIACRYPT, vol. 2248, pp. 208-221, 2001.

[50] E. Biham, “Cryptanalysis of Triple Modes of Operation”, J. Cryptol., vol. 12, no. 3, pp. 161-184, 1999.

[51] M. Une and M. Kanda, “Year 2010 issues on cryptographic algorithms”, Monetary Econ. Stud., vol. 25, no. 1, pp. 129-164, 2007.

[52] A. Sreedharan, “Dynamic S-box based AES algorithm for image encryption”, Comp. Inf. Eng., vol. 01, no. 11, 2014.

[53] C. Tu, N. Gao, Z. Liu and L. Wang, “A practical chosen message power analysis method on the Feistel-SP ciphers with applications to Clefia and Camellia”, IACR Cryptol. ePrint Archive: Rep. 2015, vol. 174, pp. 1-19, 2015.

[54] B. Senthilkumar and V. Rajamani, “VLSI implementation of key dependent substitution box using error control algorithm for substitution-permutation supported cryptography”, J. Theor. App. Inf. Technol., vol. 64, no. 01, pp. 74-83, 2014.

[55] FIPS PUB 197, “Announcing the advanced encryption standard, federal information processing standards publication 197”, National Inst. Stand. Technol. (NIST), 2001.

[56] K. Kazlauskas, G. Vaicekauskas and R. Smaliukas, “An algorithm for key-dependent S-box generation in block Cipher system”, Informatica, vol. 26, no. 1, pp. 51-65, 2015.

[57] J. Lu, “Cryptanalysis of block ciphers”, PhD Thesis. The Univ. of London, UK, A copy is available online as Technical Report RHUL-MA-2008-19, Department of Mathematics, Royal Holloway, University of London, UK, 2008.

[58] L. Xiao and H.M. Heys, “Software performance characterization of block cipher structures using S-boxes and linear mappings”, Commun., IEEE Proc.-, vol. 152, no. 5, pp. 567-579, 2005.

[59] M.H. Howard and E.T. Stafford, “The design of substitution-permutation networks resistant to differential and linear cryptanalysis”, J. Cryptol. vol. 9, no. 1, pp. 148-155, 1994.

[60] A. Biryukov, C. De Canniere, J. Lano and S.B. Ors, “Security and performance analysis of ARIA”, Final Rep., KU Leuven ESAT/SCD-COSIC, vol. 3, pp. 4-58, 2004.

[61] J. Daemen, L. Knudsen and V. Rijmen, “The block cipher Square”, Fast Softw. Encryp. LNCS, vol. 1267, pp. 149-165, 1997.

[62] H. Gilbert and M. Minier, “A collisions attack on the 7-rounds Rijndael”, Third AES Candidate Conf., vol. 230, pp. 241-252, 2000.

[63] D.J. Bernstein, “Cache-timing attacks on AES. Technical Report, 2005”, The Univ. of Illinois at Chicago, Chicago, 2005.

[64] A. Biryukov, A. Roy and V. Velichkov, “Differential analysis of block ciphers SIMON and SPECK”, Int. Workshop Fast Softw. Encryption (FSE’14) London, UK, March (3-5), vol. 8540, pp. 546-570, 2014.

[65] P. Derbez, P.A. Fouque and J. Jean, “Improved key recovery attacks on reduced-round AES in the single-key setting”, EUROCRYPT - Adv. Cryptol. - 2013, vol. 7881, pp. 371-387, 2013.

[66] T. Tiessen, L.R. Knudsen, S. Kölbl and M.M. Lauridsen, “Security of the AES with a Secret S-box”, IACR Cryptol. ePrint Archive 2015, vol. 9054, pp. 144, 2015.

[67] D. Chang, M. Ghosh and S.K. Sanadhya, “Biclique cryptanalysis of full round AES-128 based hashing modes”, Tech. Report IIITD-TR-2015-006, Indraprstha Inst. of Inf. Tech. Delhi, vol. 9589, pp. 3-21, 2015.

[68] H. Demirci, I. Taşkın, M. Çoban and A. Baysal, “Improved meet-in-the-middle attacks on AES”, Prog. Cryptol. - INDOCRYPT 2009, LNCS, vol. 5922, pp. 144-156, 2009.

[69] A. Biryukov, “The boomerang attack on 5 and 6-round reduced AES”, Adv. Encryption Standard, vol. 3373, pp. 11-15, 2005.

[70] H. Demirci and A.A. Selçuk, “A meet-in-the-middle attack on 8-round AES”, Fast Softw. Encryption, LNCS, vol. 5086, pp. 116-126, 2008.

[71] A. Biryukov, O. Dunkelman, N. Keller, D. Khovratovich and A. Shamir, “Key recovery attacks of practical complexity on AES-256 variants with up to 10 rounds”, Adv. Cryptol. - EUROCRYPT 2010. Lect. Notes Comput. Sci., vol. 6110, pp. 299-319, 2010.

[72] J. Nechvatal, E. Barker, D. Dodson, M. Dworkin, J. Foti and E. Roback, “Status report on the first round of the development of the Advanced Encryption Standard”, J. Res.-National Inst. Stand. Technol., vol. 104, no. 5, pp. 435-460, 1999.

[73] J. Daemen and V. Rijmen, “The first 10 years of advanced encryption”, IEEE Secur. & Privacy, vol. 8, no. 6, pp. 0072-74, 2010.

[74] A. Biryukov and J. Großschädl, “Cryptanalysis of the full AES using GPU-like special-purpose hardware”, Fundam. Informaticae, vol. 114, no. 3, pp. 221-237, 2012.

[75] A. Abdulgader, M. Ismail, N. Zainal and T. Idbeaa, “Enhancement of AES algorithm based on chaotic maps and shift operation for image encryption”, J. Theor. App. Inf. Technol., vol. 71, no. 1, pp. 1-12, 2015.

[76] I.A. Shoukat, A. AL-Dhelaan and M. Al-Rodhaan, “Reliability and performance assessment of multifarious hybrid cryptosystems”, WSEAS Trans. Inf. Sci. App., vol. 13, no. 7, pp. 60-71, 2016.

[77] I.A. Shoukat, K.A. Bakar and S. Ibrahim, “A generic hybrid encryption system (HES)”, Res. J. App. Sci., Engineer. Tech., vol. 5, no. 09, pp. 2692-2700, 2013.

[78] I.A. Shoukat and K.A. Bakar, “Effective evaluation metrics for the assessment of cryptographic algorithms and key exchange tactics”, Int. Inf. Inst. (Tokyo), Inf., vol.16, no. 5, pp. 2801-2814, 2013.

[79] I.A. Shoukat, K.A. Bakar and S. Ibrahim, “A Novel Dynamic Data Blocking Mechanism for Symmetric Cryptosystems”, Res. J. App. Sci., Eng. Tech., vol. 7, no. 21, pp. 4476-4489, 2014.

[80] B. Schneier, “Applied Cryptography: protocols, algorithms, and source code in C”, 2007, ISBN: 0471128457, John Wiley & Sons, Ed. 2nd, 2007.

[81] A. Ramesh and A. Suruliandi, “Performance analysis of encryption algorithms for Information Security”, Int. Conf. in Circuits, Power and Comput. Tech, vol. 3, pp. 840-844, 2013.

[82] M. Szaban and F. Seredynski, “Dynamic cellular automata-based S-boxes”, Comput. Aided Syst. Theory- EUROCAST 2011, Part I, LNCS, vol. 6927, pp. 184-191, 2012.

[83] P.M. Maurer, “A universal symmetry detection Algorithm”, SpringerPlus, vol. 4, no. 1, pp. 1-30, 2015.

[84] Z. Guosheng and W. Jian, “Security analysis and enhanced design of a dynamic block cipher”, China Commun., vol. 13, no. 1, pp 150-60, 2016.

[85] P. Agarwal, A. Singh, A., and A. Kilicman, “Development of key-dependent dynamic S-boxes with dynamic irreducible polynomial and affine constant”, Adv. in Mech. Engineer., vol. 10, no. 7, pp. 1-18, 2018.

[86] J. Wang, Q. Ding, “Dynamic rounds chaotic block cipher based on keyword abstract extraction”, Entropy. vol. 20, no. 9, pp. 693-707, 2018.

[87] A.H. Zahid, M.J. Arshad, “An Innovative Design of Substitution-Boxes Using Cubic Polynomial Mapping”, Symmetry, vol. 11 no. 3 pp. 437-446, 2019.

[88] A.H. Zahid, M.J. Arshad, M. Ahmad, “A novel construction of efficient substitution-boxes using cubic fractional transformation”, Entropy. vol. 21, no. 3, pp. 245-256, 2019.