International Journal of Applied Engineering Research ISSN 0973-4562 Volume 13, Number 23 (2018) pp. 16252-16278

A Review on Combined Attacks on Security Systems

B. Srinivasa Rao[1] and P. Premchand[2]

[1] Department of Computer Science and Engineering
Gokaraju Rangaraju Institute of Engineering and Technology, Hyderabad-500090
Jawaharlal Nehru Technological University Hyderabad, Hyderabad 500038 Telangana, India.

[2] Department of Computer Science Engineering, University College of Engineering,
Osmania University, Hyderabad-500007 India.

Abstract

Cryptology is a combination of both cryptography and cryptanalysis and is extensively used to design security systems related to data, communication and networking domains. The science of secret codes or ciphers and the devices used to create and decipher them is known as Cryptology. On the other hand the science of breaking secret codes to find the plain information is Cryptanalysis. Due to significance of applications of these techniques in wide range of scientific, engineering, technology, social networks and other domains an extensive research is being carried out throughout the world. As the subject is as old as the human evolution the research work in this field is extensive and wide range. The rapid growth in technology over few decades has significantly increased the dimensions of the field. Due to accumulation of the bulk information reviews and surveys help to comprehend the subjects in the relevant areas of the field. In the present review paper a concise review is presented on aspects of various security attacks related to the field of cryptology. The objective of the review is to assimilate the various ideas and techniques that are being used for cryptanalysis for evaluation of security of systems involved in the transmission of data and information. The review will be very much useful in identifying various existing security measures and techniques and their implementation.

Keywords: cryptology, cryptography, cryptanalysis, attacks, differential, linear, related-key, and combined attacks

I. INTRODUCTION

Cryptanalysis is a discipline of Cryptology and is converse to another well known discipline Cryptography. Cryptanalysis is a science of breaking the security of various computing systems provided by cryptography, mostly through mathematical understanding of the cipher structure. In general, the main objective of cryptography is to ensure security for information by designing strong cryptosystems. The aim of the cryptanalyst is to identify weaknesses of cryptosystems and defeat the security of the cryptosystem. In the present information age the cryptology is plays a significant role in various fields like commerce, military, governments etc. in providing security. At the same time, due to remarkable advances in cryptanalytic techniques, now-a-days it is also becoming essential to consider including a systematic, qualitative and quantitative analysis of security against newly designed techniques [1-3]. Although, availability of cryptology literature is not abundant as compared to other fields of sciences, but most of the literature in existence is well-written and presented [4-21]. At the same time the available literature surveys and reviews concerned with cryptanalysis are very less in comparison with cryptography due to complexity of the subject and its availability to the public. The main aim of the present survey is to review the state -of -the art ideas and techniques related to cryptography and cryptanalysis including the latest concepts of combined attack techniques. In section-II, the concepts, ideas and techniques of cryptography are briefly discussed. Section-III deals with various attacking models and classification of cryptanalytic attacks. The cryptanalysis and the attacks that are being used for cryptanalysis for defeating the security of various systems have been discussed in detail in section-IV. The concept of combined attacks and their implementation for various crypto systems is discussed in section-V. Finally some cryptanalytic tools have been presented in section-VI. The conclusion part is in section-VII

II. CRYPTOGRAPHY

A conventional model for network security is as shown in fig.1. It shows four basic tasks for design of a network security model. 1. An algorithm for encoding. 2. Generation of secret key. 3. Distribution System for sharing key. 4. A protocol to achieve a particular security service. In the encryption-decryption mechanism Sender and Receiver are two communicating ends. Both share common secret information through a Secure Distribution System. At Senders end a Plain Text is encrypted by an Encryption algorithm using the secret information to generate a Cipher Text. The Cipher Text is communicated to the Receiver over a communication channel. The cipher text received by receiver is decrypted by a decryption algorithm using the Receiver's secret key to reproduce the Plain Text. Thus Cryptography plays a significant role in providing security to information. A general model for cryptosystems is shown in fig2. It depicts the design of security mechanisms using some algorithms or procedures that provide security services for information. The primary objective of using cryptography is to provide the following four fundamental information security services. The information security services are:

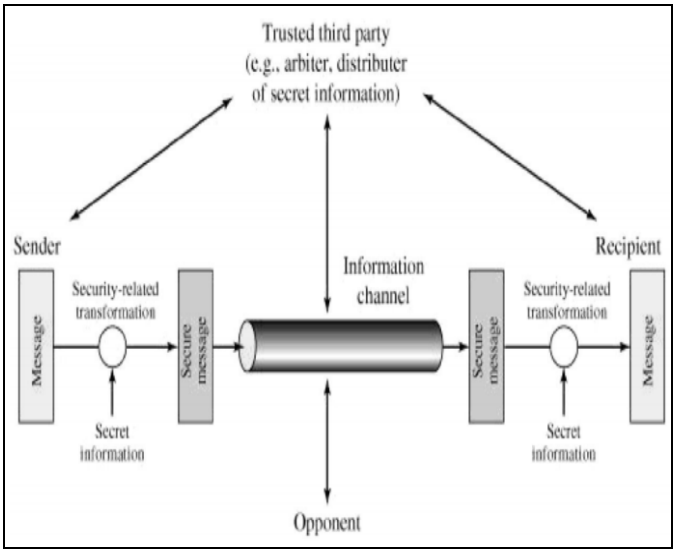


Fig. 1. Model for Network Security

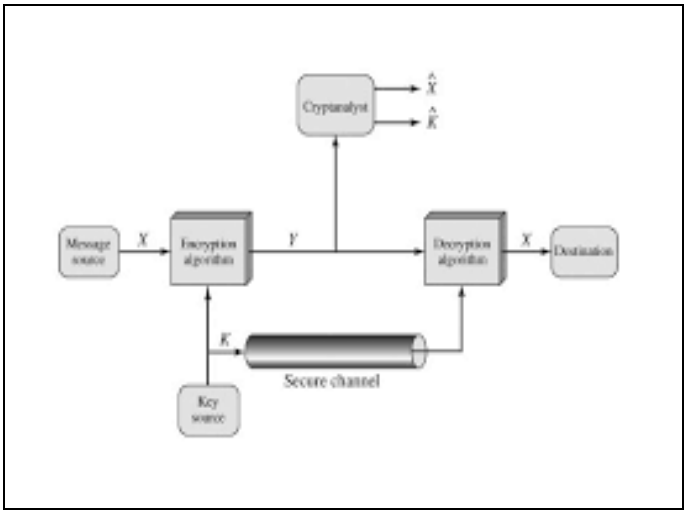


Fig. 2 A general model for cryptosystem

(i) Confidentiality: The aim of this security service is to secure information from an unauthorized user by implementing appropriate security measures.

(ii) Data Integrity: This security service detects the unauthorized modification of information and provides preventive measures.

(iii) Authentication: This service verifies the originator of information, receipt of information by receiver along with time and date of creation/transmission.

(iv) Non-repudiation: This security service ensures that an entity cannot refuse the ownership of a previous commitment or an action.

Cryptosystems- Types

A system that provides security services is known as cryptosystem. Based upon the way encryption-decryption mechanism the cryptosystems are considered to be two types. (i) Classical Encryption (also known as symmetric key encryption) (ii) Public Key Encryption (also known as Asymmetric Key Encryption).

(i) Classical Encryption:

In classical encryption a single secret key is used for both encryption and decryption and is known as Symmetric Key Encryption or secret key encryption. The mechanism of encryption and decryption is as shown fig.2. Digital Encryption Standard (DES), Triple-DES (3DES), IDEA, and BLOWFISH etc are examples for symmetric key encryption. Two challenging issues are associated with symmetric key encryption. (1) Establishment of key. The sender and receiver should come to an agreement to have s common secret key for encryption and decryption process. (2) Trust Issue: The sender and receiver should 'trust' each other.

(ii) Public Key Encryption:

In this method two different but mutually mathematically related keys are used. One key is used for encryption and the second key is used for decryption. As two different keys are being used the mechanism is also known as asymmetric encryption. The Asymmetric Key Encryption as shown in fig.3.

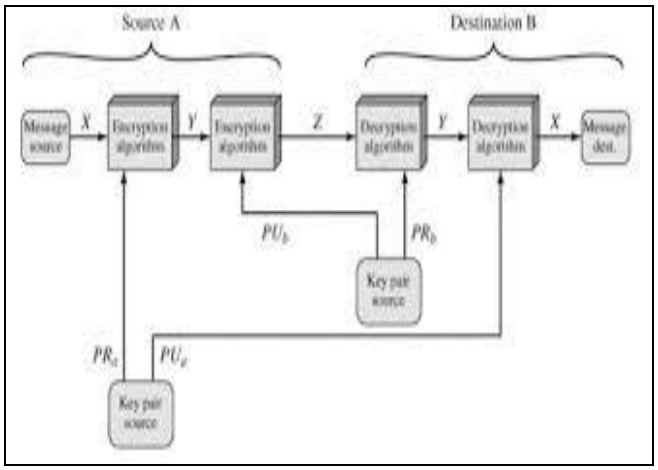


Fig.3 Asymmetric Cryptosystem

Though the encryption key and the decryption key are related, it is impossible to deduce the one key from another because of the strong and tricky mathematical relation established between them. Sometimes this is also referred as modern key cryptography. Ex: RSA algorithm etc.

Challenge of Public Key Cryptosystem

The system has some challenges: A trusted third party is required to provide secure public key infrastructure as keys may be spoofed by trusted third party. The trusted third party provides a digital signature for trusted keys [22-25].

III. ATTACK MODELS FOR DEFEATING SECURITY OF SYSTEMS

In general it is assumed that Encryption algorithm and Decryption algorithms are available to cryptanalyst and secret information (also known as Key (K)) is completely unknown. Also Plain Text and Cipher Text copies may be obtained with some skilful efforts. This scenario will make the cryptosystem vulnerable to attacks. The main objective of the attackers is to reveal the secret information (key) to break the cipher for reproducing original Plain Text. In cryptology, an attack is any attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of data or resources. An attack of a cryptographic system may break the security of system either completely or partially and provides various kinds of information of the system. It has been proposed various levels of attacker's success during cryptanalysis [26]. (i) Total break: deducing and obtaining a secret key. (ii) Global deduction: Discovering an algorithm, that may allow decrypting many messages without knowing the actual secret key. (iii) Local deduction: Discovering an original plaintext of the specific given ciphertext. (iv)Information Deduction: obtaining some information about the secret key or original message. However, the best ciphers should protect against all the cipher's failures levels mentioned above and should not be able to reveal any information related to the secret key and plaintext messages [26]. In spite of all security measure due to flaws in the system, the crypto systems are pruned to various types of attacks. In general the attacks are classified as active and passive attacks. An active attack is a network attack characterized by the attacker attempting to break into the system. During an active attack, the intruder will introduce data into the system as well as potentially change data within the system. A passive attack is a network attack in which the purpose is solely to gain information about the target and no data is changed on the target [22-26]. Thus the process of attempting to discover plain text or key or both is cryptanalysis. The strategy used by the cryptanalysis depends on the nature of the encryption scheme and the information available to the cryptanalyst.

From the Table-1 it can observe various types of cryptanalytic attacks based on the amount of information known to the cryptanalyst.

Table 1: Attack Models for Defeating Security of Systems

Element/ Type	**Only**	**Chosen**	**Known**	**Adaptive chosen**
Plain Text(PT)	No attack	Obtaining the CTs by choosing some PTs and using EA: Key is obtained from PT and CT pair.	Some known PTs are collected from Sender for available CTs.	n-PTs are chosen to obtain n-CTs using Encryption algorithm (EA)
Cipher Text(CT)	Only cipher text is available: key is to obtained	Obtaining the PTs by choosing some CTs and using DA: Key is obtained from CT and PT pair.	Some known CTs are collected from Receiver for available PTs.	n-CTs are chosen to obtain n-PTs using Decryption Algorithm (DA)
Key(K)	Total Break	A portion of key may be obtained which can be iteratively used to obtain the original key or at least a new key that can break the system.	Total Break	No attack

1. Cipher text only: A copy of cipher text alone is known to the cryptanalyst. 2. Chosen plaintext: The cryptanalysts gains temporary access to the encryption machine. They cannot open it to find the key, however; they can encrypt a large number of suitably chosen plaintexts and try to use the resulting cipher texts to deduce the key. 3. Chosen cipher text: The cryptanalyst obtains temporary access to the decryption machine, uses it to decrypt several string of symbols, and tries to use the results to deduce the key. 4. Chosen Key attack. 5. Known plaintext: The cryptanalyst has a copy of the cipher text and the corresponding plaintext. 6. Known ciphertext: The cryptanalyst has a copy of the plain text and the corresponding ciphertext. 7. Adaptive chosen plaintext: n-PTs are chosen to obtain n-CTs using EA. 8.Adaptive Chosen ciphertext: n-CTs are chosen to obtain n-PTs using DA [22-26]. 1. Ciphertext only: During ciphertext-only attacks, the attacker may have access only to a number of encrypted messages but not to the plaintext data or the secret key. In this technique the goal is to recover as much plaintext messages as possible or to guess the secret key. The discovery of the encryption key enables one to break all the other messages which have been encrypted by this key. Encryption algorithms designed securely against ciphertext-only attacks are not very vulnerable to these kinds of attacks. However, one may still find examples of protocols that have been broken by various attacks based on ciphertext-only approach. There are a few techniques which proved to be very effective even when targeting modern ciphers and which are based only on the

knowledge of the ciphertext messages. The most important methods are: Attack on Two-Time Pad and Frequency Analysis [26]. 2. Chosen-plaintext attack: During the chosen-plaintext attack, an arbitrary plaintext is chosen to be encrypted and its cipher text is obtained. From this attempts are made to acquire the secret encryption key or alternatively to create an algorithm which would allow decrypting any ciphertext messages encrypted using this key. Hence one can obtain more information about the secret key and about the whole attacked system. This enables us to analyse the system behaviour and output ciphertext, based on any kind of input data. During breaking deterministic ciphers with the public key, the intruder can easily create a database with popular ciphertexts and interpret encrypted messages by comparing the collected databases [26]. 3. Chosen-ciphertext attack: In this technique some chosen cipher texts along with corresponding plain texts are analysed to obtain the secret key. Chosen-ciphertext attacks are usually used for breaking systems with public key encryption. For example, early versions of the RSA cipher were vulnerable to such attacks. They are used less often for attacking systems protected by symmetric ciphers. Some self-synchronizing stream ciphers have been also attacked successfully in that way [26]. 4. Chosen-key attack: These techniques are used to break the large system which relies on a cipher rather than the individual ciphers by obtaining the relationship between various keys that can be used in the cipher to break the original key or getting a new key that can break the larger system even in the absence of the original key. For instance the attacker may find a key that can compromise a hash function that based on a block cipher [26]. 5. Known-plaintext attack: The known-plaintext attack (KPA) is an attack model for cryptanalysis where the attacker has access to both the plaintext and its encrypted version (cipher text). In cryptography, the known plaintext attack, or KPA, is an attack based on having samples of both the plaintext and corresponding encrypted or cipher text for that information available. Understanding Known Plain Text Attack Alice sends a message to Bob encrypted with his public key. Eve overhears an encrypted communication from Bob to Alice, and later observes them meeting at Baker Street. Eve can now guess that the communication contained the word "baker street" somewhere, a form of known plaintext attack [22-26]. 6. Known ciphertext: The cryptanalyst has a copy of the plain text and the corresponding ciphertext. 7. Adaptive chosen plaintext: n-PTs are chosen to obtain n-CTs using EA. 8. The adaptive-chosen-ciphertext attack: The adaptive-chosen-ciphertext attack is kinds of chose n-ciphertext attacks, during which an attacker can make the attacked system decrypt many different ciphertexts. It is not a realistic model [26]. From the above attacking models the following groups of attacks may be observed in the literature. A general classification attacks is shown in fig.4. A more precise classification of cryptanalytic attacks is shown in fig.5.

1. Chosen Plaintext and Cipher text attacks.

1.1 Differential Cryptanalysis

1.2 Truncated cryptanalysis

1.3 Higher order Cryptanalysis

1.4. Impossible differential Cryptanalysis

1.5 Integral cryptanalysis.

1.6. Multiset attack

1.7. Amplified Boomerang cryptanalysis.

1.8. Rectangle attack

2. Adaptive Plaintext /Cipher text attack

2.1 Boomerang attack

3. Chosen Key attack

3.1 Related Key attack

3.2 The Slide attack

3.3 Statistical related key attack

4. Known plaintext/ciphertext attack

4.1 Liner cryptanalysis

4.2 Zero correlation attack

4.3 Bi-linear cryptanalysis

5. Statistical cryptanalysis

6. Brute force attack

7. DoS

8. Attack on Two-Time Pad

9. Frequency analysis

10. Man-in-the-middle attack

11. Meet-in-the-middle attack

12. Replay attack

13. Homograph attack

14. Birthday attack

15. Rainbow attack

16. Combined attacks

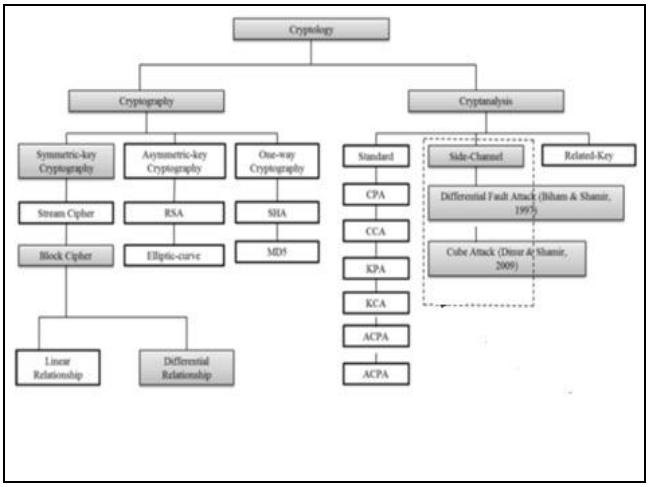


Fig.4 General Classification of attacks

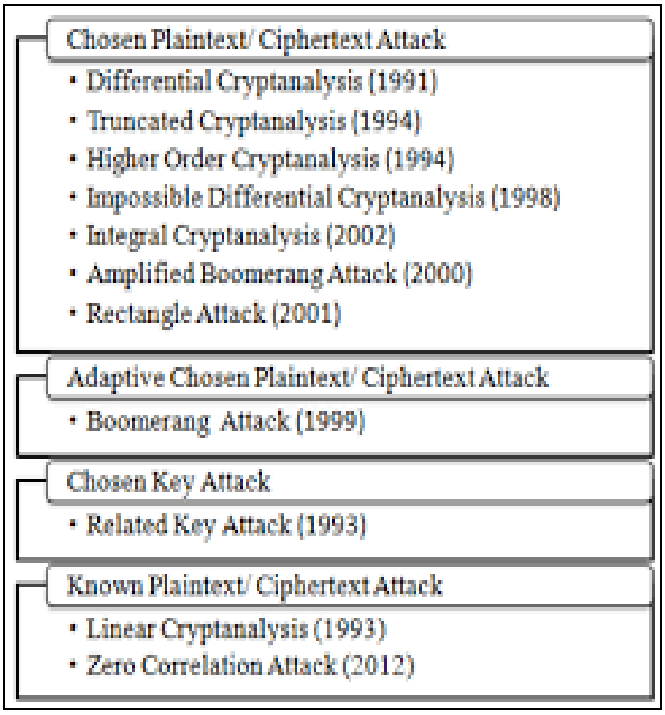


Fig.5 Classification of cryptanalytic attacks

In addition, several other attacks are also available in literature. The main theme of the cryptanalysis is to obtain the secret key from the available information to the cryptanalyst. The general procedure for cryptanalysis is depicted in fig.6.

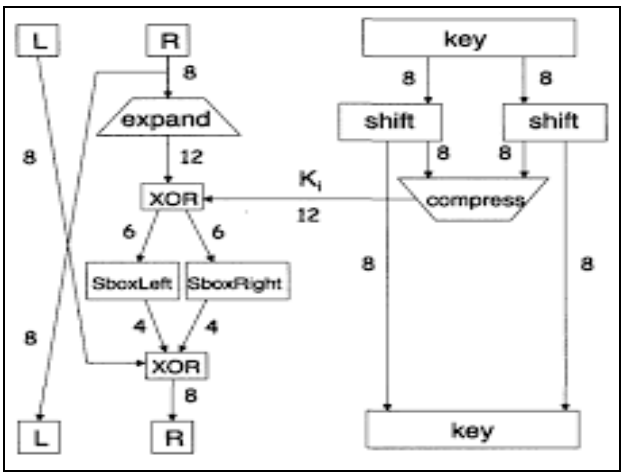


Fig.6 Cryptanalysis: Breaking of Cipher for key

IV. CRYPTANALYSIS AND ATTACKS

In the present paper some important attacking models have been reviewed.

4.1. Chosen Plaintext and Cipher text attacks.

4.1.1 Differential Cryptanalysis:

It is a Chosen Plaintext and Cipher text attack applied on block ciphers introduced by Biham and Shamir in 1990[27] to exploit the high probability of certain occurrences of plaintext differences and cipher text differences into the last round of the cipher. Its initial design was extensively applied for block ciphers in particular for DES and its advancements. The basic and conceptual ideas of the algorithm with respect to DES are shown fig.7 to9.

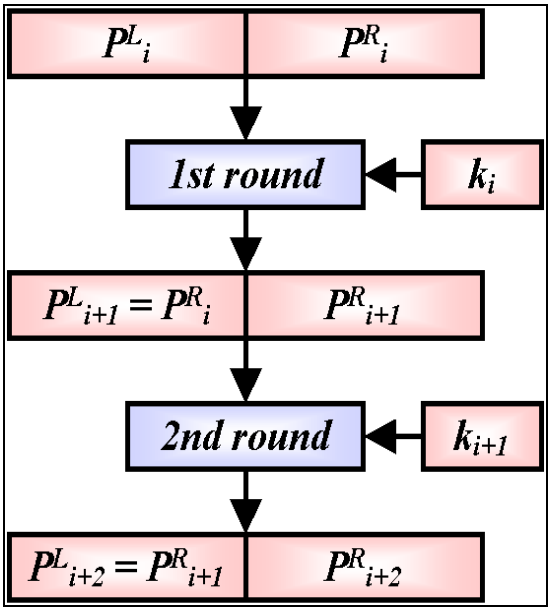


Fig.7. DES Rounds

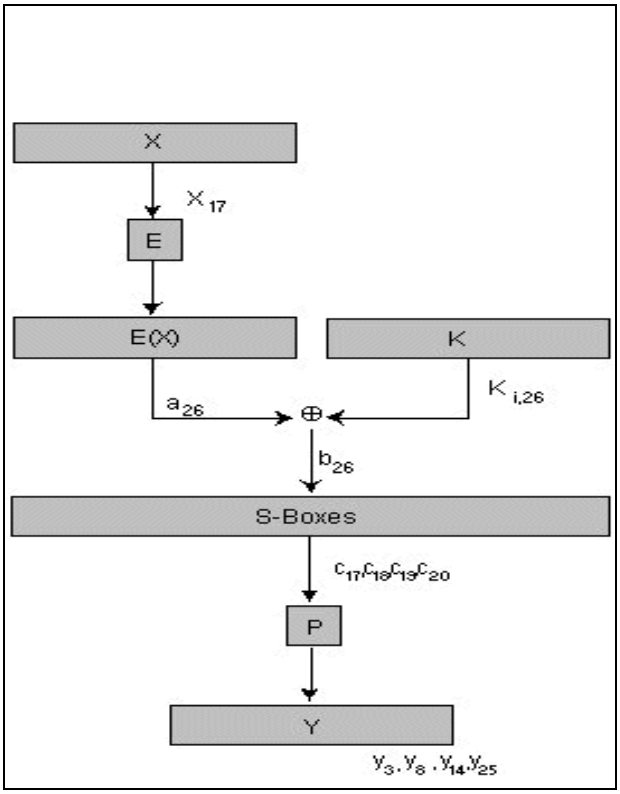


Fig.8 Differential cryptanalysis round function

In this technique the attacker has the choice to choose inputs and test the outputs to obtain the key. Let P and P' are two

plain-texts and C and C' are corresponding ciphertexts of given block cipher. Let $\Delta P = P \oplus P'$ and $\Delta C = C \oplus C'$ be some fixed plaintext difference, and certain ciphertext differences respectively that may occur with high probability. This high probability is used to find the secret key using differential cryptanalysis. In differential cryptanalysis high probability differential are calculated for S-BOX of the block cipher. For this the concept of Substitution Permutation Net-work (SPN) is considered. Further to compute plaintext difference $\Delta P = P \oplus P'$ to the ciphertext difference $\Delta C = C \oplus C'$ products of high probabilities of differential of S-boxes used [27, 28]. The probability of a particular pair (ΔP ΔC) (known as differential) is $1/2^n$ where n is the number of bits of P. In such a system let $X = [X_1 X_2 ... Xn]$ be the input and $Y = [Y_1 Y_2 ... Y_n]$ be the output .Let Y′ and Y″ be the outputs for any two inputs X′ and X″ respectively. The input and output differences $\Delta X = [\Delta X_1 \Delta X_2 .....\Delta X_n]$ and $\Delta Y = [\Delta Y_1 \Delta Y_2 ..... \Delta Y_n]$ are computed by using bit-wise exclusive-OR for the pairs(X′ and X″) and Y′ and Y″ respectively. As discussed earlier to compute the differential characteristics, for each S-Box and for each input difference ΔX and output difference ΔY Difference distribution tables are computed.

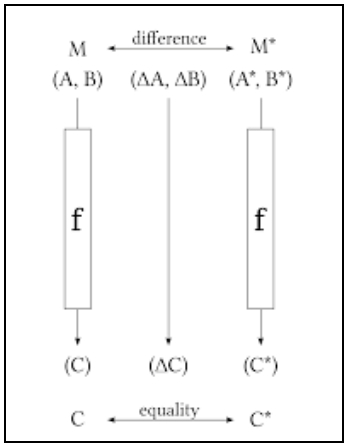


Fig.9. Computation of differential for both plaintext and ciphertext pair

The high probabilities of (ΔX; ΔY) can be identified due to the weakness of the S-Box. By considering each S-Box is independent, all pairs of (ΔX; ΔY) of each S-Box the high probabilities are traversed and combined from first round to second last round. Hence, It is possible to find some bits of last round sub key by obtaining the second last round with sufficient high probability p_D. Hence we obtain Target Partial Subkeys (TPS).The mechanism of the Differential cryptanalysis is implemented in two steps as follows [27-30].

(i)Computation of Distinguisher (ii) Key Recovery.

(i) Computation of Distinguisher:

1. Construct Difference distribution table for each S-Box for pairs of (ΔX; ΔY).
2. Compute probability of the each for pairs of (ΔX, ΔY).
3. Traverse the S-Boxes from first round till second last round of the cipher to obtain the differential probability p_D [27, 28].
4. Now, the differential probability p_D is the distinguisher.

(ii)Key Recovery:

1. Using ΔP obtain plaintext/ciphertext pairs (N).
2. For each TPS the following steps are followed:
   i. Set COUNT =0
   ii. Perform the partial decryption for each Ciphertext (CT) (for i =1to N).
      (a) CT (i) $\oplus$ TPS*
      (b) Traverse through S-boxes backward to get bits into the last Round
      (c) Verify the equality of value of the computed partial decryption and the differential characteristic
      (d) In case of equality COUNT is incremented. Also the partial sub key value with largest COUNT is considered for each TPS.
3. Construct a table for partial sub key values and corresponding probability P = (COUNT / N).
4. If $P = p_D$, Exact TPS is obtained.

The differential characteristics are shown in Fig.10 and 11.

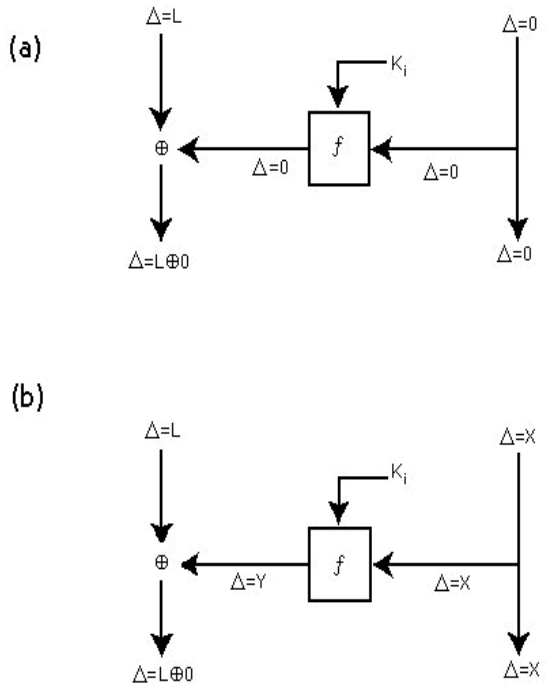


Fig.10. DES Characteristics

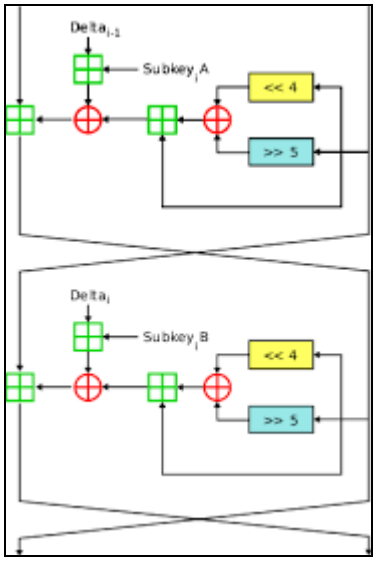


Fig. 11 Two round DES characteristic

4.1.2 Truncated Differential Cryptanalysis

Knudsen [31] developed the truncated differential cryptanalysis attack against block ciphers in the background of the differential cryptanalysis. In this technique only partial differences are determined for some small blocks of the cipher but not for the entire block cipher. Also, only the probabilities of subset of plaintext differences and subset of predicted Ciphertext differences are considered [32]. The probability of recovering key is high as predicted probability of truncated differential increases the number of plaintext and Ciphertext pairs [33]. The Truncation mechanism is based upon the mathematical formulation show in the diagram of fig.12.

$$x_0 \in_R P$$
$$x_1 = x_0 \oplus \Delta_i$$
$$\Delta_o = f(x_0) \oplus f(x_1) = f(x_0) \oplus f(x_0 \oplus \Delta_i)$$
$$\Delta_i \rightarrow \Delta_o$$

Fig.12 Truncation mechanism

The truncation function working for above truncation mechanism has been described in fig. 13.

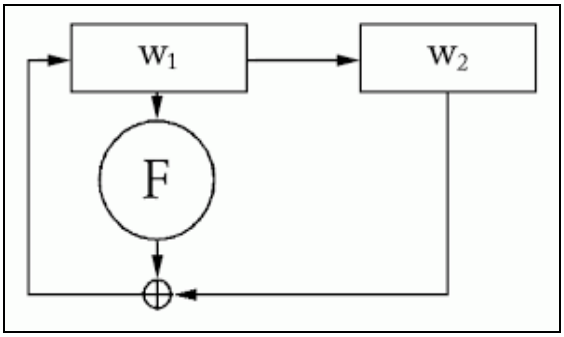


Fig.13 Truncating Function

The procedure of Truncated Differential cryptanalysis has been shown in fig.14.

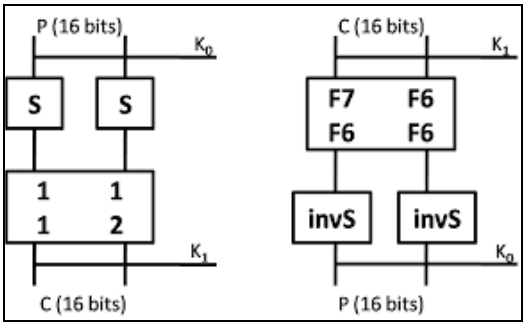


Fig.14 Truncated Differential Cryptanalysis

The attack is as follows:

a) Computation of the Distinguisher

1. Let the non trivial difference subset is ΔQ_β for enciphering function gf(2^m) -→gf(2^m up to l rounds. Thus the truncated differentials $\Delta Q_\beta \rightarrow \Delta O_\delta$
2. Consider H, a table of size 2^m where all entries initially zero.
3. For all possible input y; y ∈ gf(2^m), obtain H by placing 1 at position f(y) ⊕f(y⊕ΔQ_β).

b) Key Recovery

The last round key k_l can be obtained from H.

1. Compute N pair plain text (Q, Q') and ciphertext (O, O') respectively.
2. Do the following for all last round key k_l:

   Decipher one round reverse (O, O') with k_l, and obtain the interim ciphers S, S'
3. Do the below steps for all the second last round key, k_{l-1}.
   i. Compute $z_1 = f(S+k_l-1)$; $z_2 = f(S'+k_l - 1)$
   ii. If $H[z_1 + z_2 + S + S'] > 0$, then $k_r - 1$ and k_r will be appropriate one.
4. Repeat the attack for N times to obtain one unique pair of keys $k_l - 1$ and k_l to provide a right key that can be stored as output.

This attack has been implemented on ciphers like SAFER, IDEA, Skipjack etc. [34-41]. As an example the truncated differentials for Markov Truncated Differential Cryptanalysis for Skipjack has been shown in fig.15.

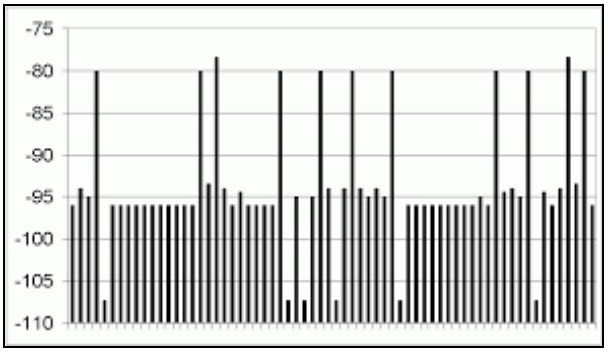


Fig.15 Markov Truncated Differential Cryptanalysis for Skipjack

4.1.3 Higher order Cryptanalysis

In this technique two inputs are used simultaneously to compute the secret key. The basic idea of the technique is in case a derivative for an interim round has high probability the last round key is easily derivable [42-44] may be with negligible limitations. The higher order differential cryptanalysis is proposed by Knudsen based on the concept introduced by Lai [45] and Duan et al [46]. Consider the derivative of function f: GenF(2^p) → GenF(2^q) at the point a is $\Delta_a f(y) = f(y + a) - f(y)$ where a ∈ GenF(2^p). For i th derivative of f at the point (a_1, a_2,... a_i) ∈ GenF(2^p) is defined as $\Delta\, a_1^{(i)}$, ...$a_i f(y) = \Delta_{ai}\,(\Delta_{a1}{}^{(i-1)}$,....$a_{i-1})f(y)$, where $(\Delta_{a1}{}^{(i-1)}$,....$a_{i-1})f(y)$ is the $(i-1)^{th}$ derivative of f at (a_1, a_2,.. a_{i-1}), the 0^{th} derivative of f is defined to be f(y) itself, also degree($\Delta_a f(y)$) ≤ degree(f(y))-1. Also for any y ∈GenF(2^p), let LR[a_1,.....a_i] be the list of all 2^i possible combinations of a_1,.....a_i [47]. Standaert et al [48] provided the further details.

i) Computation of the Distinguisher

1. Select a plaintext Q ∈ GenF(2^p) at random.
2. Encipher plaintexts Q⊕ u, ∀ u ∈ LR[a_1,.....a_i] to X_u.
3. Obtain $\bigoplus_{u \in LR[a1,...ai]} f(y \oplus u)$
4. If $\bigoplus_{u \in LR[a1,...ai]} f(y \oplus u) = K$, a constant, ∀ y ∈ GenF(2^p), for (t-1) round with any round keys k_1, k_2,.k_{t-1}.

ii) Key Recovery

1. Create M random plaintexts. Implement the following steps for each plaintext Q.
2. For each TPS corresponding to 2^l possibilities of k_t implement the following steps.
   i. Decipher all X_u for one round back using TPS.
   ii. Store all TPS values satisfying step 4 of distinguisher generation in a table H excluding other TPS values.
4. For all M plaintexts and the keys of table H, iterate the step-2 to obtain the highest probability key k_t.

This technique can be implemented to maximum 5 Feistel rounds of cipher. Figures 16-18 shows implementation of Higher order cryptanalysis on the cipher MISTY1 [49].

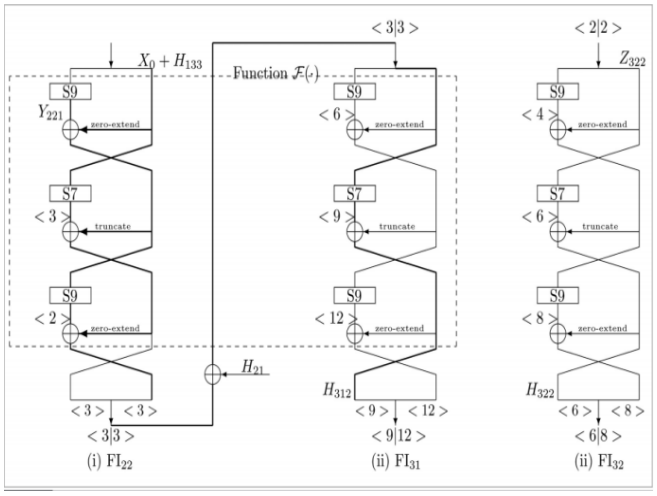


Fig.16 Formal estimation of the increase in order for r-round Feistel (MISTY1)

$\hat{h}_0$	$x_0x_1x_2x_3x_4x_5x_6 + (y_0+y_3+y_5+y_6+y_8)x_0x_1x_2x_3x_4x_5 + \cdots + 1$
$\hat{h}_1$	$(y_0+y_2+y_4+y_7)x_0x_1x_2x_3x_4x_5 + \cdots + y_5y_7 + y_5y_8 + y_6y_8 + y_6$
$\hat{h}_2$	$x_0x_1x_2x_3x_4x_5x_6 + (y_0+y_2+y_4+y_5+y_7+y_8+1)x_0x_1x_2x_3x_4x_5 + \cdots + 1$
$\hat{h}_3$	$x_0x_1x_2x_3x_4x_5x_6 + (y_0+y_3+y_4+y_6+y_8)x_0x_1x_2x_3x_4x_5 + \cdots + 1$
$\hat{h}_4$	$(y_0+y_2+y_3+y_6+y_7)x_0x_1x_2x_3x_4x_5 + \cdots + y_6y_7y_8 + y_7 + y_8 + 1$
$\hat{h}_5$	$x_0x_1x_2x_3x_4x_5x_6 + (y_1+y_6+y_8+1)x_0x_1x_2x_3x_4x_5 + \cdots + y_8$
$\hat{h}_6$	$x_0x_1x_2x_3x_4x_5x_6 + (y_0+y_2+y_5+y_7+1)x_0x_1x_2x_3x_4x_5 + \cdots + y_6 + y_7$

Fig.17 Computation of higher order terms

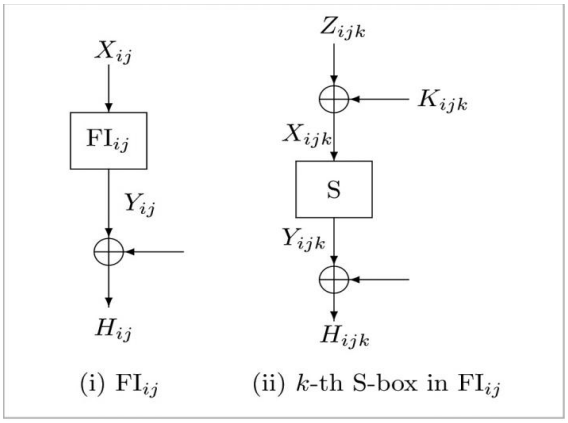


Fig.18 Last round of a five-round modified MISTY1

4.1.4. Impossible differential Cryptanalysis

This technique is developed by Biham etal [50] in 1998.In Impossible differential Cryptanalysis the differential predicts difference with zero or less probability. This technique finds the correct key by eliminating all other key with zero or less probability and is very much useful to defeat the ciphers of

different structures by combining with linear cryptanalysis [50-52]. The basic impossible differential cryptanalysis concept has been presented in fig.19 and 20 [45]. This technique was explicitly described in [53-55].

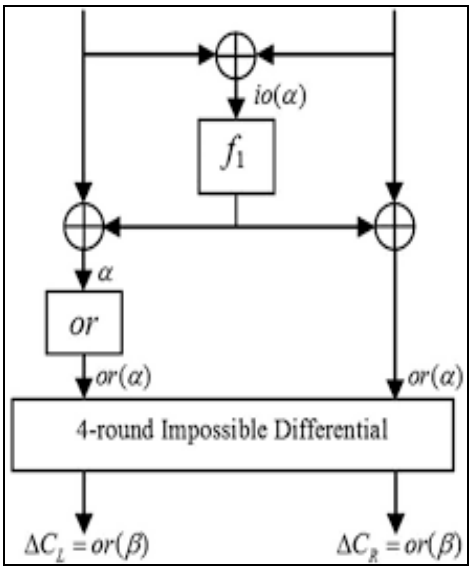


Fig.19. Impossible differential attack on 5-round FOX64

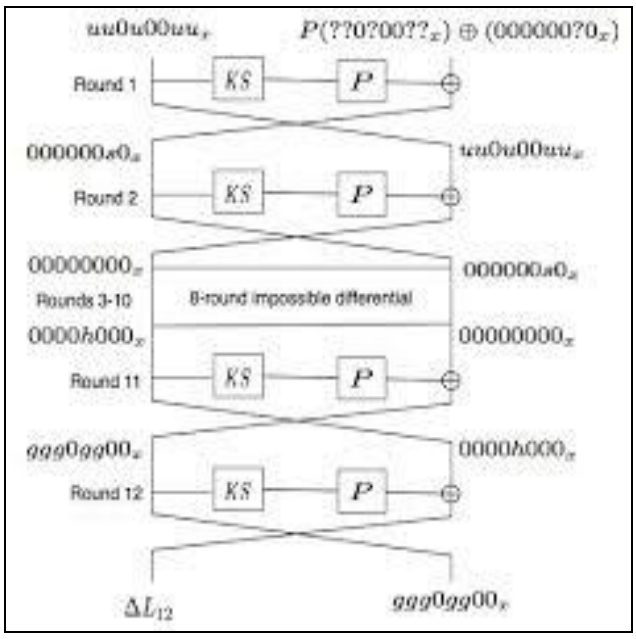


Fig.20 Impossible differential attack on 8-round cipher

Let P and P' be the two plaintexts with difference ΔP. Let ΔC be the difference of two cipher texts C and C'. Let α δ be the differences ΔP and ΔC after x and y rounds of encryption of the P and P' and C and C'. Similarly, the difference α after $l_1 + l_2$ rounds produces the output difference δ. According to the principle of impossible differential after l_1 rounds of partial encryption α becomes β and for partial decryption of l_2 rounds δ becomes γ as shown in fig.3. If $\beta \neq \gamma$ the difference α — δ after $l_1 + l_2$ rounds of encryption is impossible as α — δ ≠ γ← δ and (α, δ) is called impossible differential pair. The keys and subkeys that meet the condition $\beta \neq \gamma$ are excluded.

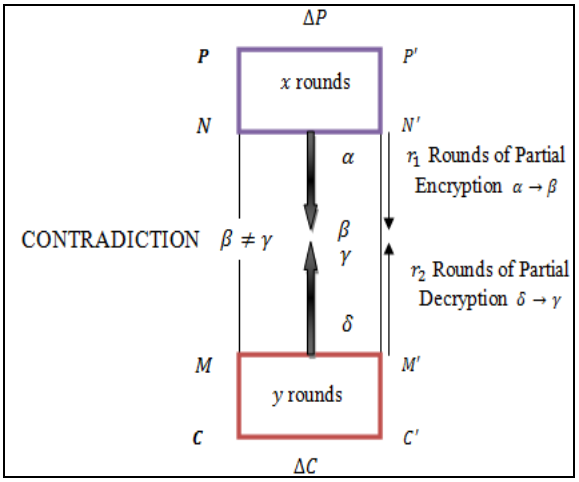


Fig.21 Miss in Middle: Impossible Cryptanalysis

i) Compute Distinguisher

To obtain impossible differentials (α — δ)

1. Compute $\alpha = X \oplus X'$, encipher X, X' by l_1 rounds to obtain β such that Pr (α — β) = 1
2. for $\delta = Y \oplus Y'$, decrypt Y, Y' by l_2 rounds to obtain γ such that Pr (δ → γ) = 1
3. (α — β) is impossible if $\beta \neq \gamma$ is true.
4. Iterate above steps for different (α, δ) to obtain ID = $(\alpha_1, \delta_1); (\alpha_2, \delta_2) \ldots (\alpha_n, \delta_n)$.

ii) Key Filtering Process: Compute subkeys for each k at rounds x and y.

Implement below steps to exclude the keys that are invalid.

1. Compute $\alpha = X \oplus X'$ and $\delta = Y \oplus Y'$ such that (α, δ) ∈ ID for all (X, Y) and (X' Y').
2. Compute differential by enciphering X and X' by round l_1
3. Compute differential by enciphering Y and Y' by round l_2
4. Verify $\beta \neq \gamma$ for invalidity of subkeys.
5. Exclude the invalid keys.

The mechanism is shown in fig.21.

4.1.5 Integral cryptanalysis

Integral cryptanalysis is a unified and extended single consistent framework where sums are propagated and integrals are computed as shown in fig.22. The general Integral cryptanalysis mechanism is shown in fig.23. The bijective ciphers can be used to find simultaneous relationship between many encryptions and resembles dual differential

cryptanalysis [56] and can be applicable ciphers that are not vulnerable to differential cryptanalysis [57]. The improved versions were reported by Knudsen and Wagner [58].

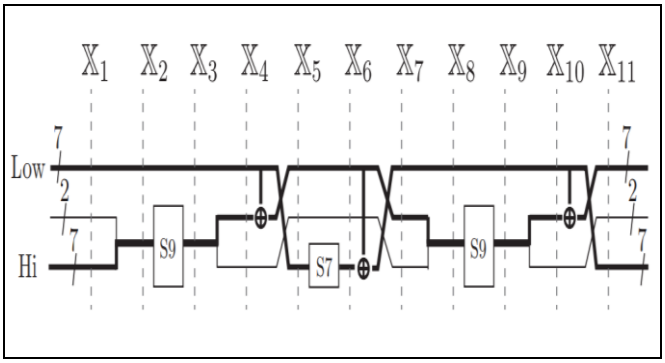


Fig.22 Propagation of sums

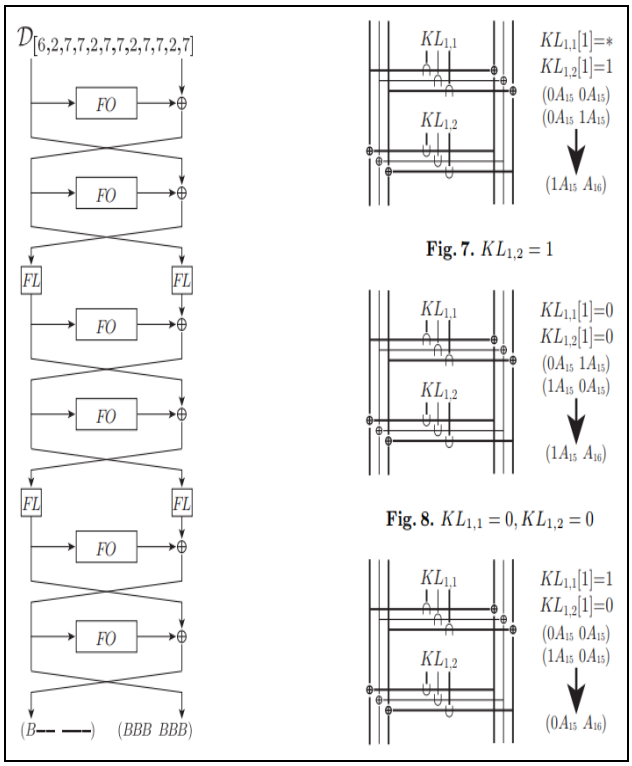


Fig.23 Integral cryptanalysis propagation rounds

According to Knudsen and Wagner, the bijective components of the Block ciphers are vulnerable to integral cryptanalysis. For any set of state vectors $S=s_1,s_2,...s_p$ and multiset of state vectors M, $\int M = \sum_{s \in M}$ defines the integral, where each $s_i \in$ GenF (2^p) . The integral distinguisher is constructed using the following properties. (a) For all $S \in M$, $s_i = z$ (constant), where $z \in$ GenF (2^p). (b) All i^{th} words are different s_i: $S \in M$ = GenF (2^p), denoted by symbol 'A'.(c) For all s_i , the sums to some values predicted in advance $\bigoplus_{s \in M} si = z$', denoted by symbol 'B', for which z' $\in$ GenF(2^p), are constants.(d) The unpredictable terms are denoted by '?' .

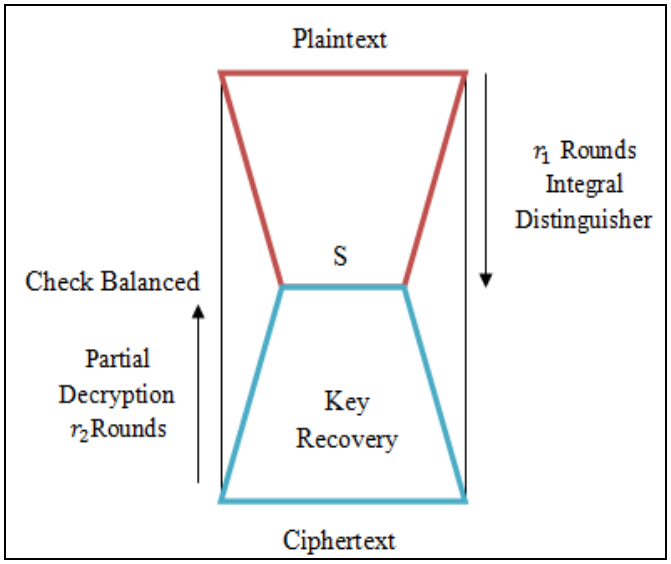


Fig. 24 Integral attack

i) Computation of Distinguisher

a. Select M with 2^p chosen plaintexts such that some specific terms being with A and the rest with C. Let. P = (CCCC, CCCC), P' = (ACCC, CCCC).

b. Encipher M to have states B with probability 0 and 1 during the round r_1 to distinguish random permutations.

ii) Key Recovery

a. Compute all TPS.

b. Compute partial decryptions to extent of the Integral distinguisher output.

c. Find balanced sub keys with exclusive-or sum of the states is zero.

d. Do the step 1-3 repeatedly for all M, to obtain right sub keys.

The concept of distinguisher is shown in fig.24

4.1.6. Multi set attack

Multiset attack is a chosen plain text attack. Biryukov and Shamir [59] proposed Multiset attack which is a combinations integral crypt analysis, S-boxes, and linear transformations. The secret S-boxes are associated with SP network. The multiset has two element pairs: value and multiplicity. Value is the value of the element and multiplicity is the frequency of occurrence of element. Then the propagation of the multiset through the cipher is observed. In this attack the following operations are performed. (a) Distinguish multiset values equal or unequal.(b) The frequency of occurrence multiset values is even or odd. (c) Sum of XORs is zero or not [57]. Multiset attacks are among the best attacks on AES-128 due to its bitwise structure and will be a promising direction for future research.

4.1.7 Amplified Boomerang Attack

It is a chosen plain text attack and is developed on the principles of the original Boomerang attack. Short differential characteristics are the main features of the Amplified boomerang attack. These characteristics have high probability and make the attack reliable and strong. This attack has been applied to hash functions like SHA family. The structure of the Amplified Boomerang attack is as shown in fig. 25. This attack resembles with the neutral bit tool based boomerang attack reported by Biham and Chen [60]. Joux and Peyrin [61] designed the amplified boomerang attack and computed basic differential path on an iterated hash function like SHA-1 successfully.

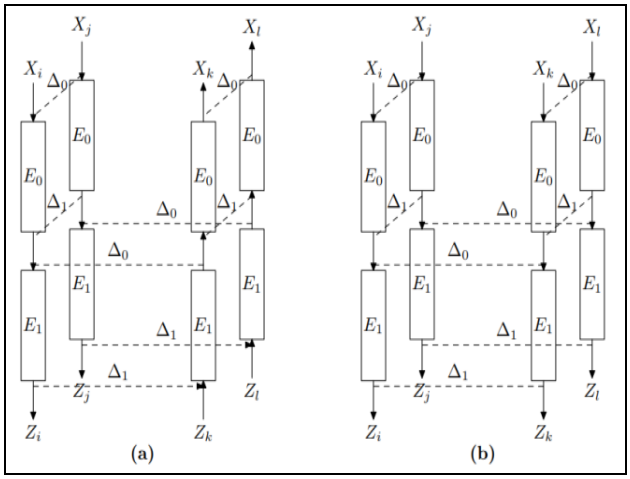
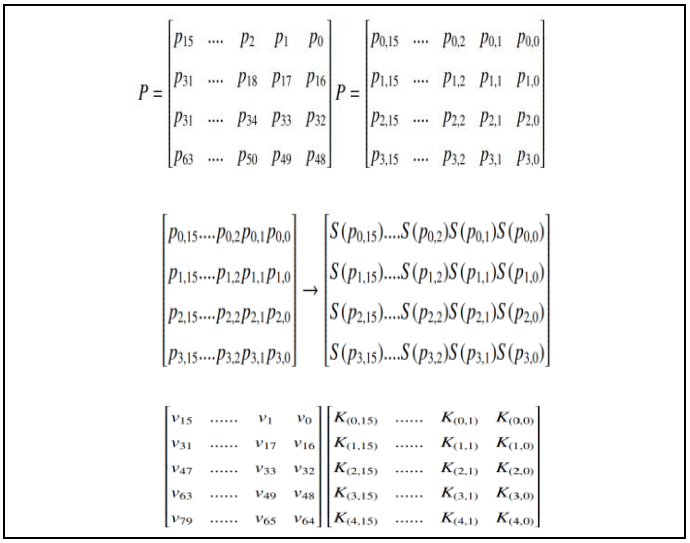


Fig.25 Amplified Boomerang attack structure

4.1.8 Rectangle attack

The rectangle attack is chosen plaintext attack. It is an enhancement to Amplified boomerang attack in which chosen plaintext variations are included. It was successfully applied to a block cipher namely Serpent [62-64].



RC[0] = 0X01	RC[5] = 0X05	RC[10] = 0X13	RC[15] = 0X1C	RC[20] = 0X0D
RC[1] = 0X02	RC[6] = 0X0B	RC[11] = 0X07	RC[16] = 0X18	RC[21] = 0X1B
RC[2] = 0X04	RC[7] = 0X16	RC[12] = 0X0F	RC[17] = 0X11	RC[22] = 0X17
RC[3] = 0X09	RC[8] = 0X0C	RC[13] = 0X1F	RC[18] = 0X03	RC[23] = 0X0E
RC[4] = 0X12	RC[9] = 0X19	RC[14] = 0X1E	RC[19] = 0X06	RC[24] = 0X1D

When the key is provided by user as 128 bits, the key is stored in a 128 bits key register and arranged as 4 × 32 array of bits as shown in below.

$$\begin{bmatrix} K_{(0,31)} & \ldots\ldots & K_{(0,2)} & K_{(0,1)} & K_{(0,0)} \\ K_{(1,31)} & \ldots\ldots & K_{(1,2)} & K_{(1,1)} & K_{(1,0)} \\ K_{(2,31)} & \ldots\ldots & K_{(2,2)} & K_{(2,1)} & K_{(2,0)} \\ K_{(3,31)} & \ldots\ldots & K_{(3,2)} & K_{(3,1)} & K_{(3,0)} \end{bmatrix}$$

Fig. 26 Rectangle attack on a block cipher

The attack may be implemented in two steps [65].

(1) Computation of Distinguisher

(2) Finding the secret key

(1)Computation of Distinguisher

1. Let (X, X') and (Y.Y') be the two randomly chosen plaintext pairs. Let α be difference of these pairs. Compute α using α =X'⊕ X and α = Y'⊕ Y.
2. Encipher the plaintext pairs (X, X') and (Y.Y') for obtaining intermediate ciphertexts denoted by U = E_0(X) and U' = E_0(X') and V = E_0(Y) and V'' = E_0(Y'). Find β and γ. where U ⊕U' = β, V ⊕V' = β and U ⊕V = γ, that implies to U'⊕V' = (U⊕ β) ⊕ (V ⊕ β) = γ.
3. Compute the right quartets that satisfy the following relations. G = E_1(U);G' = E_1(U') and H =E_1(V);H' = E_1(V'), G ⊕ H = δ and G'⊕ H' = δ after E_1.
4. Construct a Table of right quartets by iteration the above steps to obtain the distinguisher.

(2)Finding secret key

1. Compute TPS: From the table of distinguishers, for each set of distinguisher obtain all possible non-zero differences for last round i.e. TPS
2. Implement the following steps for all TPS.
   i. For each right quartet, i Set COUNT=0
   ii Implement one round partial decryption.
   iii. Verify the difference between partial decryption and corresponding input difference is zero.
   iv. In case of zero, increment COUNT of that TPS.
3. TPS with maximum COUNT denotes the right quartet.

For example a Rectangle attack on a block cipher is shown in fig.26.

4.2. Adaptive plaintext/ cipher text attack:

4.2.1The boomerang attack

The Boomerang attack comes in to the category of Adaptive plaintext/ cipher text attack. The attack was initially proposed by Wagner [66] for defeating the block ciphers. The general structure of the Boomerang attack is as shown in fig.27. Two separate Differential Characteristics (DC) are combined together to form a single attack. Let (P, P') and (O, O') two pairs of independent plaintexts. The original block cipher encryption is treated as combination two sub-encryptions E_0 and E_1. From fig.27 it can be observed that $E_0(P)=M$; $E_0(P')=M'$; $E_0(O)=N$; $E_0(O')=N'$; $E_1(M)=C$; $E_1(M')=C'$; $E_1(N)=D$; $E_1(N')=D'$; ($\alpha \rightarrow \beta$) is the DC of E_0 having probability p and ($\delta \rightarrow \gamma$) is the Dc of and E_1^{-1} with probability q. Here the distinguisher decided by the difference with certain probability that is common to all plain texts [27].

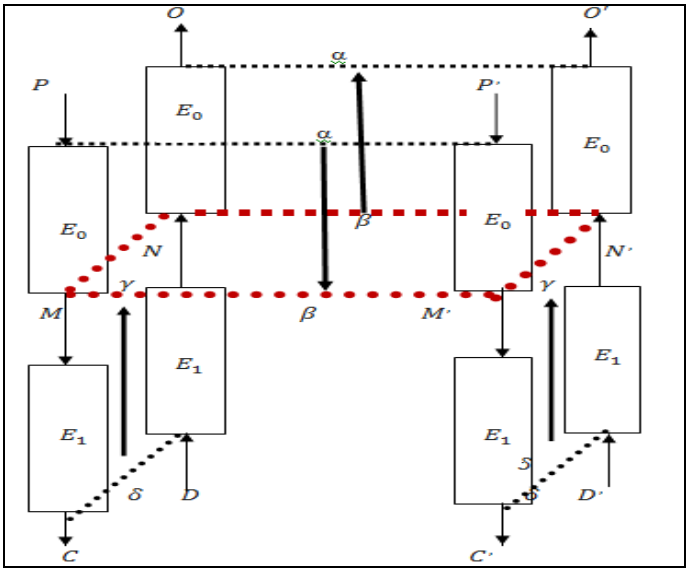


Fig. 27 Structure of Boomerang Attack

The above Boomerang attack may be implanted on some cipher with following notation.

(a).Obtain Distinguisher:

1. Find $\alpha = X' \oplus X$ for any two plaintexts X, X'.
2. Compute the middle ciphertexts, $U = E_0(X)$ and $U' = E_0(X')$; $A = E_1(U)$, $A' = E_1(U')$.
3. Compute $B = A \oplus \delta$ and $B' = A' \oplus \delta$ such that $E_1^{-1}(A) \oplus E_1^{-1}(B) = E_1^{-1}(A') \oplus E_1^{-1}(B') = \gamma$
4. Decipher partially B and B' for E_1^{-1} to obtain V, V' and decipher it for E_0^{-1} to obtain. $Y = E_0^{-1}(V)$ and $Y' = E_0^{-1}(V')$.
5. If $Y \oplus Y' = \alpha$, for all Y and Y' then (X, X', Y, Y') form right quartets. .
6. Iterate above steps and construct Boomerang Distinguisher Table for other X, X', Y and Y' sets.

(b) Finding secret key

1. Compute right quartets (X, X', Y, Y')
2. Compute TPS.
3. Do the following all TPS (k_r)
   - i Set COUNT=0
   - ii Encipher (X, X',Y,Y') to ciphertext quartet (A, A',B, B').
   - iii Compute the following steps for one round partial decryption d_k under key k_r.
     - a) $A = d\ k_r(A)$, $A'' = d\ k_r(A')$ and $B = d\ k_r(B)$, $B'' = d\ k_r(B')$
     - b) If ($A \oplus A'' = B \oplus B''$) increment COUNT.
4. Obtain the TPS with maximum count for right quartet.

Fig. 28 depicts the Boomerang attack implementation on AES-256.

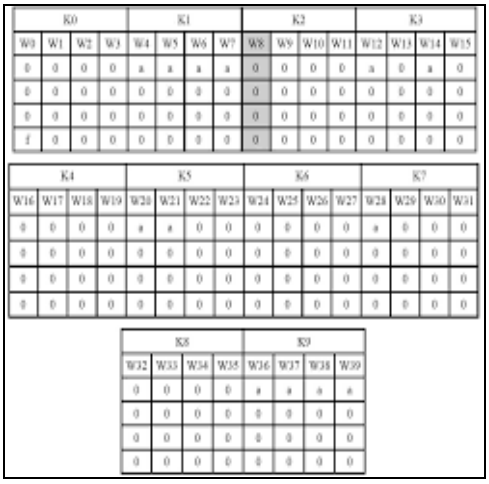


Fig. 28 Boomerang Attack on AES-256

4.3. The Chosen Key Attacks (CKA)

The Chosen Key attack is classified as 1. Chosen Key Known Plaintext (CKKP) Attack and 2. Chosen Key Chosen Plaintext (CKCP) Attack

The relation between the keys is significant in CKKP. In CKCP the relation between the keys and plain text is significant. The key recovery for the two attacks is same and as follows.

i.. Discovery of secret key.

1. Choose a plain text pair X and X* such that $X_R = X_L^*$.
2. Do encryptions $E_K(X)$ and $E_{K^*}(X^*)$ for all values of X and X* for all possible rounds to obtain cipher texts Y and Y* that satisfy $Y_L = Y_R^*$, for key K.
3. If the condition is satisfied then with X, X*, Y, Y* the key K can be derived.

Based up this algorithm mainly three techniques have been designed. 1. Related Key attacks 2 The Slide Attack 3 Statistical Related-Key Attacks

4.3.1 Related Key attack

Biham [56, 67-69] proposed the related key attack by using some known relationships among the keys to obtain the original secret keys. During encryption if pairs of keys maintain a consistent relation in different rounds, then with the relations between a set of new sub keys that have been obtained from the sub keys that were shifted one round backward can be used to attack on ciphers to break the original secret keys [30]. A basic related key model is shown in fig.29. The Related-Key Model leads to two new attacks designated as First Related-Key Attack and Second Related-Key Attack. This model may not be strong enough when the block cipher uses compression function [70].

1. First Related-Key Attack

This attack is designed upon a two bit shift relation between two keys K and K'. If a key generation algorithm maintains a relation $K_i = K'_{i+1}$ then the first n number of rounds of K and K' are similar [71].

2. Second Related-Key Attack

This attack is based on the complementary properties of keys. If a Key K has m other keys that induce a related-encryption process then by analysing the m keys original key K may be obtained doing trial encryption with all the m keys [70]. Implementation of the Related-Key Attack on a Slightly Modified DES is shown fig.30.

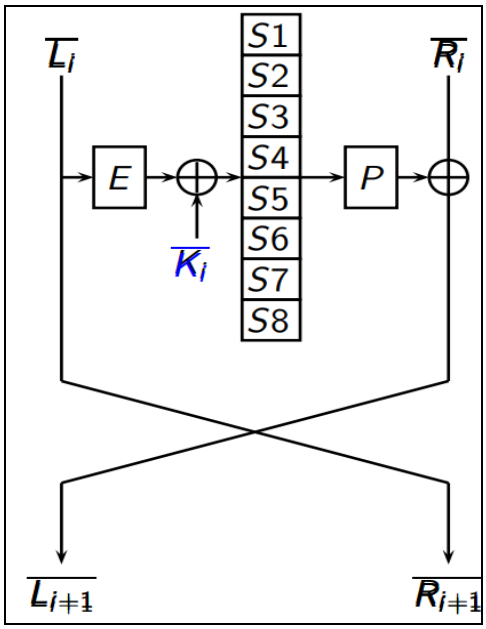


Fig. 29 The Related key Model

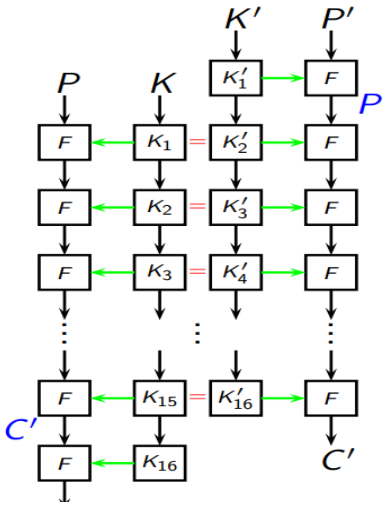


Fig.30 Related-Key Attack on a Slightly Modified DES

4.3.2 The Slide Attack

This attack may be a known or chosen plaintext attack developed by Biryukov and Wagner [72]. Using this attack the ciphers may broken in independent of number of rounds with same keyed permutation. It has been practically implemented on ciphers like DES, Variants of DES, Treyfer, and Blowfish.

Procedure for Slide Attack [70]:

1. Let X_i and Y_i two cipher pairs and K_1 and K_2 are corresponding key pair..
2. For each pair of X_i and Y_i solve such that $F_{K1,K2}(X_i) = X_j$; $F_{K1,K2}(Y_i) = Y_j$.
3. For each candidate key pairs(suggested keys) K_i and K_j repeat step 2.
4. Analyse keys computed from step2: if the suggested keys satisfy the relations $F_{K1,K2}(X_i) = X_j$; $F_{K1,K2}(Y_i) = Y_j$ then store the candidate keys as slide pair.

The above procedure is depicted in the diagrams of fig.31 and fig.32.

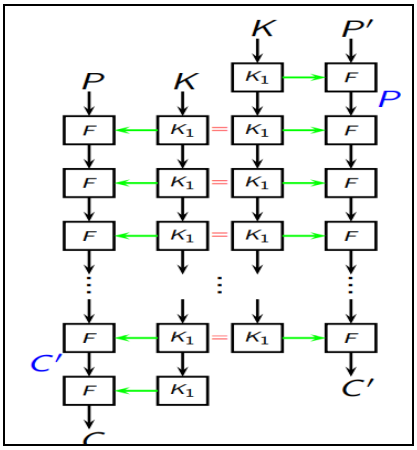


Fig. 31 A Slide Attack on 2K-DES

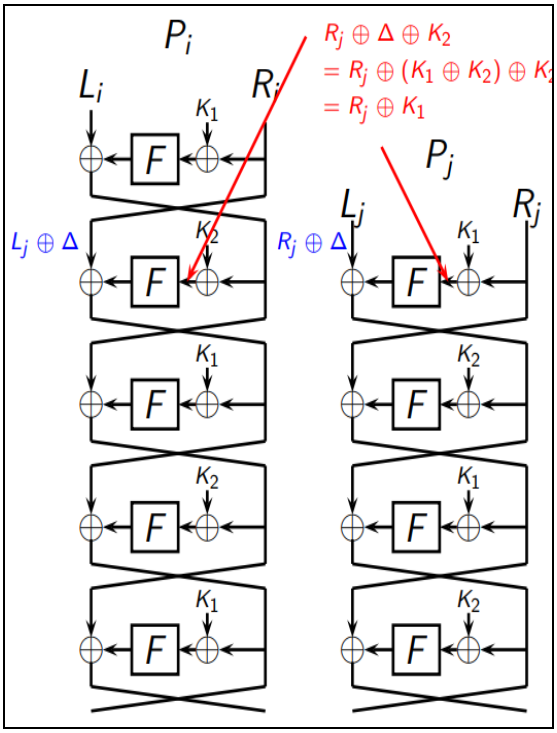


Fig. 32 Complementation Slide Attack

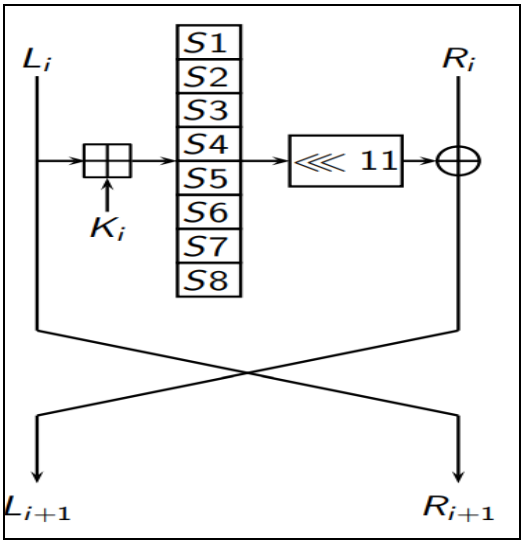


Fig. 33 The Block Cipher GOST

4.3.3 Statistical Related-Key Attacks

The Statistical key-recovery attacks are generally designed to obtain the keys trough statistical estimation based upon analysis of the relationship between the keys by testing them for a large number of ciphertexts. These attacks successfully estimate the keys, when the keys are generated by random number generator and when attacker controls the relationships between the keys [73]. Two important models have been reported in the literature. 1. Related-Key Differential Attacks 2. Certification Attacks

1. Related-Key Differential Attacks [73]

The Related-key differential attack was proposed by Kelsey et al [73] using the complementation property of DES algorithm for keys. The complementation property allows computing the probability of regular differentials. The differences in keys propagate as differences in sub keys and during the input round function these differences may cancelled. Based on this one can find a trivial relation key for the relations K′ = K∧C and K’ = K∨C, for any constant C. If n is the block size, then 2^{n-1} distinct pairs are possible for any given input. In case of two keys, 2^n distinct pairs are possible. In a typical Related-key attack, for an s-bit round function 2^{s-1} output differences are possible for an input difference of a key. The implementations of Related-Key Differential Attacks on GOST cipher are shown in fig.33 and fig 34.

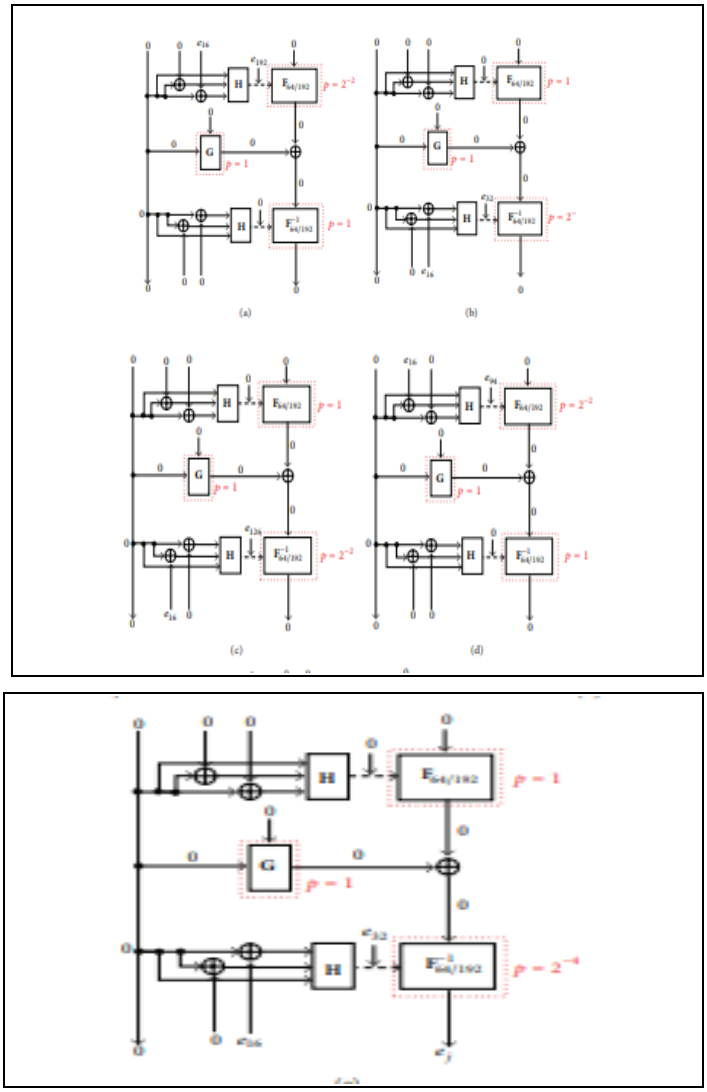


Fig. 34 Related-Key Differential Attacks on a cipher

2. Certification Attacks on AES

Several certification attacks have been designed [68, 70] using Advanced Encryption Standard versions the full AES-192 and AES-256. Several attacks on AES-256 in Davies-Meyer (a transformation into a compression function) were reported. A 2^{99} data/time attack on AES-256 in the related-sub key model (using 4 related keys) and a 2^{176} data/time attack on AES-192 in the related-sub key model were also proposed[68-70]. These models are intuitive procedures as the relation between the keys and sub keys is very simple and not practical. Despite the fact that this model may seem too strong, it is not. There are cases where the required relations can be satisfied: Hash functions built on top of AES-256, Protocols which allow such related-sub key tampering, and when the key schedule algorithm is not too strong, an adversary may use more keys in the related-key model. In any case, in the theoretical settings, a block cipher should not show this type of weakness (ideal cipher model) [70].

4. LINEAR CRYPTANALYSIS

Linear cryptanalysis is known plaintext attack which is implemented successfully on various block ciphers like DES, FEAL, Serpent etc [71, 74-77]. This attack obtains highly probable linear expressions that relate plaintext, ciphertext and sub key bits. The details of the linear crypt analysis are available in the literature [71, 74-77]. Let u be bits of input and v be bits of output with high and low probabilities and form a linear expression. If P_L is probability to hold the expression, then bias probability is defined as $\varepsilon = |p_L - 1/2|$. If $P_L > 1/2$, then the expression $X_{i1} \oplus X_{i2} \oplus X_{i3} \ldots \oplus X_{iu} \oplus Yi_1 \oplus Y_{i2} \oplus Y_{i3} \ldots \oplus Y_v = 0$ is said to be linear approximation otherwise it is known as affine approximation. When ε is large, the system will be weak and may be vulnerable to attack. To attack the cipher a linear approximation table (T) is constructed.

The general principle for linear crypt analysis is shown in fig.35.

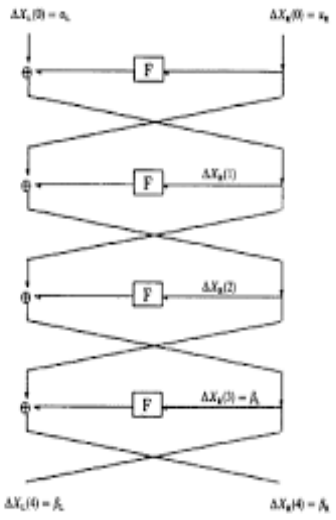


Fig.35 Linear cryptanalysis principle

1. Compute T for each S-Box of size nxm.
   (i) Consider the linear relations $a.x = a_1x_1 \oplus a_2x_2 \oplus \ldots\ldots \oplus a_nx_n$ and $b.y = b_1y_1 \oplus b_2y_2 \oplus \ldots\ldots \oplus b_my_m$ for input and output. Here a, b represents n and m bit numbers respectively for $0 \leq a \leq 2^{n-1}$ and $0 \leq b \leq 2^{m-1}$.
   (ii) Obtain p_L from the Table T by dividing the elements of linear approximation table by 2^n.
   (iii) Compute p_L of each S-Box for each round with the expression $\varepsilon = |p_L - 1/2|$.
2. Store the linear trail for the elements with highest bias probability ε in each round till second last round.
3. Compute the expected bias probability p_D on calculating ε_i for each round and at last probability of $p_D(x_1 \oplus x_2 \oplus \ldots\ldots \oplus x_n = 0) = 1/2 + 2^{k-1} \pi_{i=1tok} \varepsilon_i$ where $\varepsilon_{1.2\ldots.k} = 2^{k-1} \pi_{i=1tok} \varepsilon$.

ii) Obtaining the secret key

1. Produce M pairs of plaintext (PT) and ciphertext (CT)
2. For each TPS from 2^n possibilities n-bit TPS, do the following:
   i Set COUNT=0
   ii For each CT(i) for i = 1 to M do the partial decryption
      a. CT (i) ⊕ TPS
      b. Run S-boxes backward to get bits into the last round
      c. XOR the bits of PT (i) with XOR of the last round bits of S-boxes obtained in step (b)
      d. If the result of step (c) is 0, then increments COUNT
   iii |Bias| = |COUNT- M/2 |
3. Construct a table for all sub keys corresponding to. |Bias|
4. From the table, if |Bias| = 0 then TPS is not a correct one. If |Bias| = Expected value, then the TPS is correct.

The implementation of the present algorithm is as shown in fig.36.

4.1 Zero Correlation Linear Cryptanalysis

The Linear cryptanalysis has following variations:

1. Zero Correlation Linear Cryptanalysis
2. Bi-linear cryptanalysis
3. Multiple Linear Cryptanalysis

Bogdanov and Rijmen [78] introduced the Zero correlation linear cryptanalysis. Let F be cryptographic function of cipher X. For any given input A and output B, A → B denotes a linear approximation for F for X at round r.

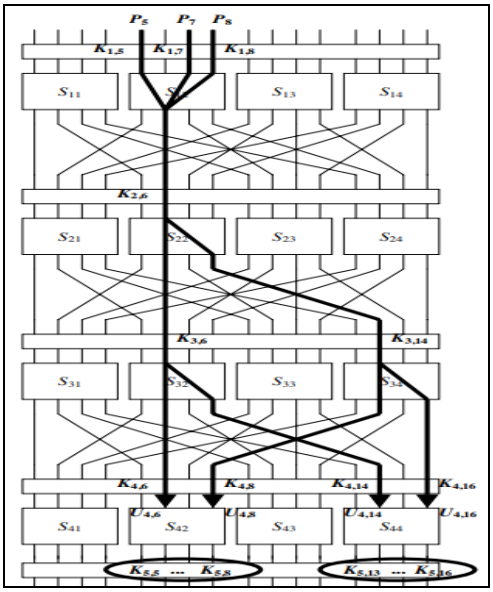


Fig.36 Linear cryptanalysis Attack on cipher

The probability of the linear approximation can be expressed as P = ($^{Pr}_{X}$) (AX = BF(X)). If C is correlation then C = 2P-1 with A≠ 0, B ≠ 0. For a fixed A and B , A → B for any iterative block cipher is denoted as Linear Hull (LH). The sequences of the LH are denoted by linear Trail (LT). This is depicted in fig.37 for any function F=f, input A=a, output B=b, f_i is the function of i^{th} round and u_i's are intermediate values.

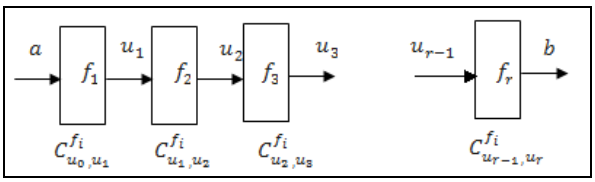


Fig. 37 Linear approximation

The total correlation contribution CU over a cipher is computed as follows:

1. Obtain linear approximations for all rounds $C_U = \pi^r_{i=1} C^{fi}u_{i-1}, u_i$, where $C^{fi}u_{i-1}, u_i$.
2. Concatenate all C_U from step-1 to obtain linear Trails. 3. If $C_U = 0$ for each LT, then C = 0 and it is denoted by a —/ b. Even for one zero correlation linear hull is found, the cipher may be attacked.

The construction of linear crypt distinguisher is given in fig.38 and its implementation is shown in fig.39.

The basic steps for constructing an attack on ciphers are

i) Computation of Distinguisher

1. Select PT, CT and unknown K.
2. Construct LD using zero-correlation C (a — b) = 0.
3. Calculate the contribution of non-zero correlation using the partial trails and obtain LD (a, b).

ii) Key Deduction

1. Compute TPS for all combination of sub k_r.
2. Encrypt and decrypt partially PT and CT for each possible sub key respectively for rounds r_1 and r_1 respectively.
3. For all sub keys and for linear approximations check the correlation during partial encryption decryption.
4. If C= 0, the sub key guess is correct.

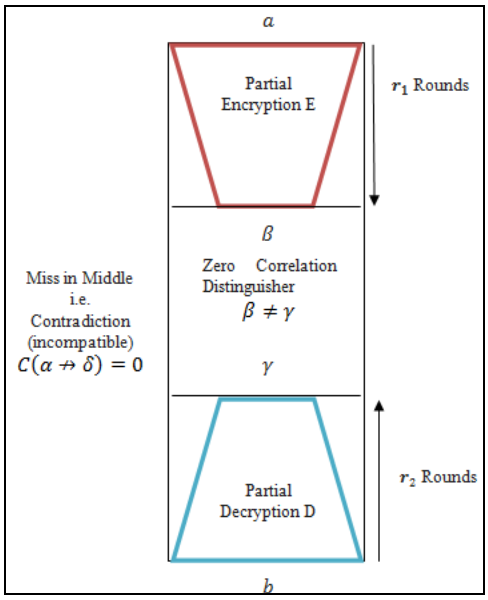


Fig. 38 Construction Linear cryptanalysis

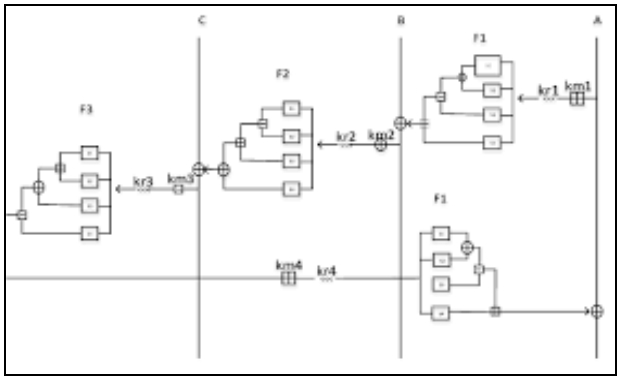


Fig. 39 Implementation of Zero-correlation attack on a cipher

4.2 Bi-linear cryptanalysis

Another variation linear cryptanalysis is Bi-linear cryptanalysis. In general it is implemented on Feistel block ciphers. In this attack the relations between the bilinear functions of plain and cipher text bits are used to obtain the keys. This attack is more effective on some ciphers where ordinary linear cryptanalysis techniques fail. The linear cryptanalysis easily breaks the DES but fails at s5DES cipher [79]. On the other hand the bilinear attack defeats the s5DES

efficiently as it has a bias of ¼ at third round bilinear approximation of s5DES[80]. Also ciphers like Rijndael-type S-box are very tough against linear cryptanalysis (LC) but are easily vulnerable to BLC [81-83].

4.3 Multiple Linear Cryptanalysis:

The Multiple Linear Cryptanalysis attacks were developed by various researchers [84-92]. Kaliski and Robshaw [84] introduced an attack considering several linear approximations. The weakness of this technique is L w∈K Kw. In order to overcome this weakness a new method was developed and successfully implemented for DES and also for cryptanalysis of reduced Serpent [86-88]. Computation of Linear Hulls [80] is another technique implemented for block ciphers like PRESENT [89], Matsui's Algorithm-2 [74] etc. Multiple Linear Hulls (MPH) and Correlation Matrix (CM) are the two important components of the Multiple Linear attacks and incorporating these components several methods can developed[90, 91, 63].

5. NON-LINEAR ATTACKS (ALGEBRAIC ATTACKS)

Algebraic attack is a potential powerful attack on symmetric key block cipher. It had been applied on two algorithm Simplified AES and Baby Rijndael [93]. The algebraic attack procedure is given below:

1. The cipher operations are expressed a set of equations or algebraic expressions of variables.
2. Some variables are substituted with known data.
3. For obtaining the key an algebraic system and set of operators are used.

The main challenge for algebraic attack is non-linearity in selected systems. Like a brute force attack or a code book attack it may not be practical for strong ciphers [94].

6. STATISTICAL CRYPTANALYSIS

Statistical cryptanalysis is a very popular technique in the present cryptanalytic research. In these techniques stastical correlations are significant for recovery of the keys. Most of the time these techniques are implemented on block ciphers but can also be applicable to others. Davies and Murphy [95] designed a stastical attack using stastical correlations to implement on DES. Biham and Shamir implemented the differential cryptanalysis as statistical cryptanalysis for DES [96–98]. The first practical implementation of stastical cryptanalysis on DES was done by Matsui [74, 99]. Vaudenay implemented another statistical cryptanalysis on DES [100]. Partitioning cryptanalysis is another stastical approach on DES by Harpes and Massey [101].

7. A BRUTE FORCE ATTACK

The brute force attack will be the last choice for defeating a cipher. It tries all possible values for keys to attack the cipher. It obtains the information using trial-and-error method. Now-a-days automated software is being used for brute force attack to derive the information. However to overcome this attack several methods are used. Limiting or restricting accessibility to system to a specific number of attempts may be a defence against brute force attack. Generally this mechanism may effective in password protection where attackers try to crack the pass words for accessing the systems [102].

8. A DENIAL-OF-SERVICE (DoS)

Denial-of-service (DoS) attack prevents the authorised user from accessing a service. Dumping or flooding the network with excessive messages, authenticate requests for invalid address are the tricks that are used for DoS attack to make the network server busy and access will be denied for genuine user [102].

9. ATTACK ON TWO-TIME PAD

This is cipher text attack. Using of same stream of characters as key for multiple times makes the system vulnerable to attack as there is possibility of recovering key from reverse operations on the ciphers. The measures against Two-Time Pad are (i) Not using the same stream of characters as keys repeatedly. (ii) Padding some unique bits to the character stream of the secret key. (iii) Using a counter for key with some initial value for the encryption process and increasing its value for every iteration of the algorithm [103].

10. FREQUENCY ANALYSIS

Frequency analysis is a known ciphertext attack. It exploits the stastical repetitive nature some characters of language for attack. By analysing the frequency of occurrence of some characters and related common features it is easy to identify their role in encryption process. Hence it is possible to obtain the correct sequence of characters from jumbled words [104].

11. MAN-IN-THE-MIDDLE ATTACK

Interception of message on open communication system by an unauthorised eavesdropper without knowledge of sender and receiver of the message is known as Man-in-the-middle attack. The attacker may modify exchange or retransmit the message using his own key. Due unawareness communication will be normal between the sender and the receiver. Thus the entire communication on the channel is controlled by the attacker. This attack is also known as a Janus attack or a fire brigade attack [105-107].

12. MEET-IN THE –MIDDLE ATTACK

This attack was proposed by Diffie and Hellman in 1977[108, 109]. It is a known plaintext attacks. The attacker knows some intermediate portions of plaintext and their ciphertexts. This attack breaks the ciphers having multiple keys and

encryptions. The space-time trade-off to is an interesting feature of the attack that drastically reduces the complexity of the multiple-encryption scheme. The multidimensional meet-in-the-middle attack is shown in fig.40.

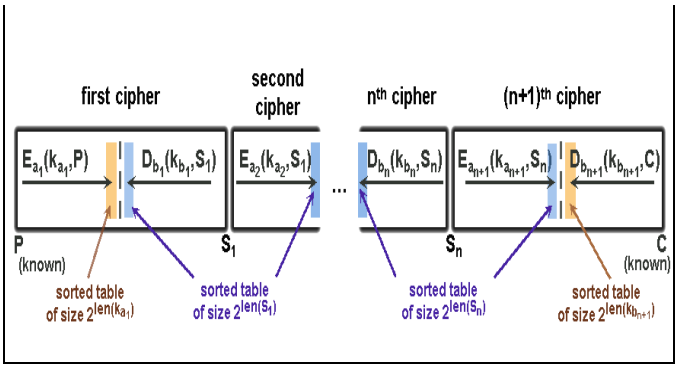


Fig.40 Man-in-the-middle attack

According Diffie and Hellman, the following steps are implemented to attack the cipher.

1. Compute all $E_{a1}(k_{a1},P)$and construct a table with E_{a1} k_{a1} and sort with respect to the values of $E_{a1}(k_{a1},P)$.
2. Compute all $D_{bn+1}(k_{bn+1},C)$ and construct a table with k_{bn+1} and sort with respect to the values of $D_{bn+1}(k_{bn+1},C)$.
3. Do the following for all S_1:
    1. Compute $D_{b1}(k_{b1},S_1)$ and construct a table with k_{b1} and sort with respect to the values of $D_{b1}(k_{b1},S_1)$.
    2. Compute all $E_{a2}(k_{a2},S_1)$ and construct a table with k_{a2} and sort with respect to the values of $E_{a2}(k_{a2},S_1)$.
    3. For all S_2 do the following steps.

1. Compute $D_{b2}(k_{b2},S_2)$ and construct a table with k_{b2} and sort with respect to the values of $D_{b2}(k_{b2},S_2)$

....

n..For all S_n do the following steps.

1. Compute $D_{bn}(k_{bn},S_n)$ and construct a table with k_{bn} and sort with respect to the values of $D_{b2}(k_{bn},S_n)$
2. Compute all $E_{an+1}(k_{an+1},S_n)$ and construct a table with k_{an+1} and sort with respect to the values of $E_{an+1}(k_{an+1},S_n)$.
3. Obtain a pair of keys (k_{ai}, k_{bi})by analysing the above tables that can be potential secret keys.

13. REPLAY ATTACK

In Replay attack an attacker or intruder drops on to the communication system and intercepts communication systems and unauthorizedly gets the information. Later the attacker misuses this information by retransmitting it for a duplicate transaction or false authentication. Digital signature with stamp is one of the measures to counter the replay attack[110].

14. HOMOGRAPH ATTACK

This attack is to deceive the users by using aliases that appear similar to some authorised systems. In general a genuine domain name is spoofed with homoglyphs or homographs. The counter measures are browser tools and in-built security mechanisms [111].

15. BIRTHDAY ATTACK

According to probability theory for a set of randomly chosen people there is always a collision probability that some pairs have same birthday under some assumptions. This is also known as birthday paradox. The Birthday attack exploits this probability to attack a cipher or hash function. The likelihood of collisions is obtained for various random attacks. With the permutations of these collisions secret keys may guessed. Generally, Birthday attack is implemented on Hash functions to determine the collisions. Quantum computations may support Birthday attacks efficiently in breaking the collision resistance [112].

16. RAINBOW ATTACK

The Rainbow attack was proposed by Oechslin [113] and Hellman [114]. In this attack a table is constructed for values for reverse cryptographic hash functions and the table is known as Rainbow Table. In general these tables are precomputed. These tables can be used as tools to attack on hash generated passwords.

V. COMBINED ATTACKS

So far many attacks have been discussed. But all these attacks are mostly individual attacks or single attacks. These attacks have their role in cryptanalysis. It is quite natural that when new attacks are being designed to counter them strong security measures are devised for cryptographic systems. Hence it is obvious that new attacks are to be designed for enhanced security systems. However, it is a continuous and endless process for designing new attacks and new counter measures. But in each aspect new and creative ideas may improve or provide better and efficient techniques. The cryptanalytic tools should be designed and developed taking into consideration of the complexity involved in the processes being implemented and importance of the security infrastructure. In this aspect to design new cryptanalytic tools two procedures may be followed. (1) Inventing new attacks. (2) Extending, generalising and combining already known

cryptanalytic attacks. Research is being done in this direction and several new approaches were reported in the literature. In this paper some of these related approaches have been reviewed. This section mainly focuses on new approaches for combination of attacks. Various combined attacks have been reported in the literature. In the present survey an attempt has been made do discuss some important combined attacks. The theme behind these combined attacks is an assumption that instead of individual attacks combination of various attacks may defeat the security of the systems quickly and efficiently. At the same time the security level of the systems can be further improved by subjecting them to various efficient combined attacks. Also new attacks may be designed from the existing cryptanalytic attacks. Various attacks and their variations can be classified as mentioned below:

I. Main Cryptanalysis Techniques:

1. Related key crypt Analysis (RKC)
2. Differential Crypt Analysis (DC)
3. Linear Crypt Analysis (LC)

II. Variations in Differential Crypt Analysis (DC)

1. Truncated differential cryptanalysis (TDC)
2. Higher order differential cryptanalysis (HODC)
1. Square cryptanalysis (SC)
2. Impossible Differential Cryptanalysis (IDC)
3. Boomerang Cryptanalysis (BC)
4. Rectangle Cryptanalysis (RC)

III. Variations in Linear cryptanalysis

1. Multiple Linear cryptanalysis (MLC)
2. Non Linear Crypt analysis (NLC)
3. Bilinear cryptanalysis (BLC)

From the above mentioned individual cryptanalytic techniques the possible combinations of attacks have been tabulated in Table-II.

Table -II possible combinations of attacks

RKC	DC	LC	Combined Attacks so far implemented	Other combinations for future study
	TDC	MLC	D-NLC	D-LC, D-NLC, S-LC, S-NLC, RK-D-LC, RK-D-NLC
	HODC			RK-RC, RK_BC, D-BLC, HOD-LC, D-L-BC,
	SC	NLC	RK-RC	D-BL-BC
	IDC			D-MLC, HOD-MLC, D-NL-BC, D_L_RC, RK-D-MLC
	BC	BLC	RK-BC	RK-D-L-BC, RK-BL-BC, RK-D-NL-BC, RK-D-NL-RC,
	RC			

The objective of these combined attacks should be accurate and reliable evaluation of cryptographic algorithms shown in Table-III.

Table-III Cryptographic algorithms

Block Cipher	Hash Functions	MAC Algorithms
SHACAL-1	MD4	HMAC
SHACAL-2	MD5	NMAC
DES	HAVAL	
Triple DES	SHA-0	
AES	SHA-1	
Blowfish		
Variations of Blowfish		
RC6		
CAST		
IDEA		
Others		

From above combinations some of the combined attacks have been considered for review in present work.

5.1. The Differential-Linear Cryptanalytic Attack

Longford and Hellman [115] had proposed a combined attack known as the differential-linear cryptanalysis attack. It is a combination of differential cryptanalysis and linear cryptanalysis. In this combined attack first differential characteristic of a part of block cipher is determined with probability 1. For the immediately following rounds of the cipher linear approximation is obtained. Thus a differential-linear distinguisher may be constructed to any chosen plain text. The complete description of this attack has been discussed in detail elsewhere [115]. Here, the idea of the attack is briefly described.

1. Let E be a chosen cipher and E_0 and E_1be two sub cipher of E such that $E=E_0$ o E_1.
2. For any input α and corresponding output β, $(\Delta\alpha \rightarrow \Delta\beta)$ is a differential with probability 1 for E_0
3. Let X may be a chosen plaintext defined over a set $\{0,1\}^n$. Then γ and δ are defined as $\gamma= E_0(X \oplus \alpha)$ and $\delta E(X) = \delta E(X \oplus\alpha)$ with probability 1.
4. The linear approximation with bias for E1 is defined as $\Gamma\ \gamma \rightarrow \Gamma\ \delta$.
5. The differential –linear distinguisher is given by the pair $(\Delta\alpha \rightarrow \Delta\beta, \Gamma\ \gamma \rightarrow \Gamma\ \delta)$

Longford and Hellman applied this attack on DES for 8 rounds with 512 chosen plaintext and recovered 10 bit key. Biham etal [116,117] introduced another combined attack with more number of rounds. In the frame work of Longford and Hellman Differential-linear attack, Kim [118] implemented the attack for small size text that may be supplement previous attacks.

Jiqiang Lu [119,120] devised a new and more reasonable method considering the two assumptions of Hellman and excluding the assumption of Biham of earlier models has shown some edge over the previous models.

5.2. The Differential-Nonlinear Attack

Kim [118] developed a new combined attack known as Differential-Nonlinear attack. Most of the procedure is same as the differential-linear attack introduced by Longford and Hellman [115] but the difference is in differential calculation. In this attack a non-linear distinguisher is designed and used instead of linear one. The nonlinear approximation is appended to differential characteristic to obtain the distinguisher.

1. Let E be a chosen cipher and E_0 and E_1 be two sub cipher of E such that $E=E_0$ o E_1.
2. For any input α and corresponding output β, ($\Delta\alpha \rightarrow \Delta\beta$ is a differential with probability p for E_0
3. Let X may be a chosen plaintext defined over a set $\{0,1\}^n$
4. Let $\lambda_I .I \oplus F(C, K')=0$ and $\lambda_I .I^* \oplus F(C^*, K')=0$ be the conditions for non-linear approximation with probability ½ +q" for a non linear function $\lambda_I \rightarrow F$ for E_1.
5. Let the one bit equation be $F(C;K') \oplus f(C^*;K') = F(E_1K(E_0{}^K(X));K_0) \oplus F(E_1{}^K(E_0K(P^*));K_0) = a$ with probability ½ + 2p . q"^{2}
6. Mask the non-linear approximation as linear approximation.

The implementation is shown in fig.41.By using above procedure the attack can be applied to various systems particularly for hash functions [121-123].

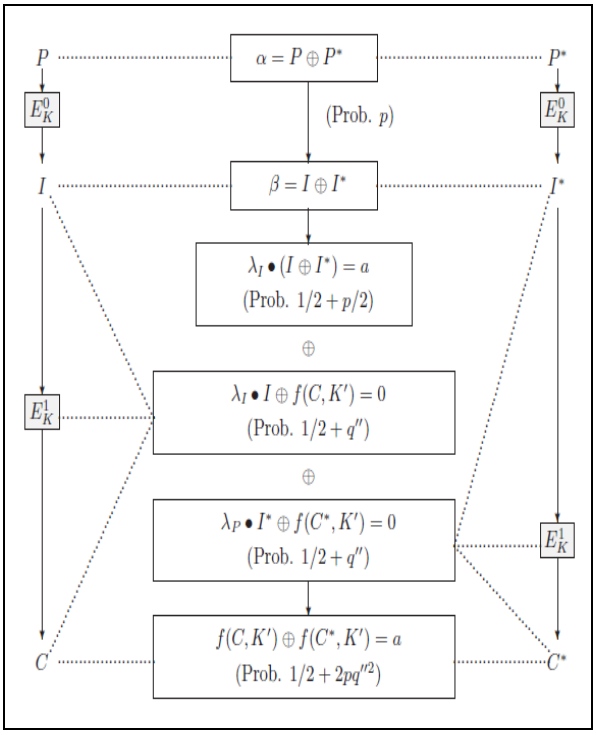


Fig.41 Differential-Nonlinear Distinguisher

5.3. The Square-(Non) linear Attack

In this section, the square-linear and square-nonlinear attacks that combine the square attack with the linear and nonlinear attacks, respectively will be discussed.. These attacks are similar to the differential-(non)linear techniques. The square attack was introduced when the block cipher SQUARE was pro-posed [124]. After this attack was introduced, it has been extended and generalized to the multiset attack [53] and the integral attack [125]. The basic idea behind this attack is the same as that of the higher-order differential attack [29]. It exploits a square characteristic whose input data consist of a set of plaintexts in which some bits are formed of a saturated set, and whose output data have a property like balancedness in some bits.

1. Let l be a bit length. Let us consider a set $W= \{0, 1\}^l$. if any value of W exists only once in the set W then W is said to be saturated.
2. If the sum of all the elements is zero in the set then it is said to be balanced.
3. For any sub cipher E_0 , each square-linear attack considers a square characteristic with some inputs and corresponding some balanced outputs.
4. Compute $\lambda_{C*}((\bigoplus^{2^{m-1}}_{i=0} C_i) = \lambda_C *(\bigoplus^{2^{m-1}}_{i=0} E^1{}_K(E^0{}_K(P_i))) = 0$ with probability $1/2 + 2^{2^{m-1}}q'^{2m}$ · with probability $1/2 + 2^{2^{m-1}}q'^{2m}$.

This attack requires $O((2^{2n_i1}q"2^n)^{-2})$ chosen plaintext sets to work. The extended attack is known as the square-nonlinear attack [126].

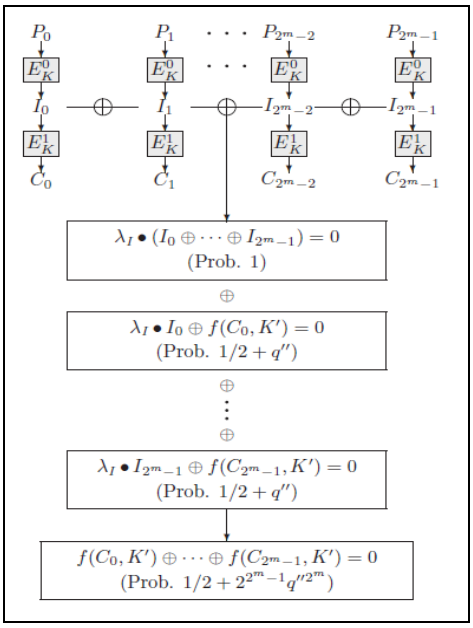


Fig.42 Square-Nonlinear Distinguisher

5.4. The Related-Key Differential-(Non) linear Attack

As the name suggests, the attack is combination of related key and differential-linear attack which was proposed by Hawkes [66]. Based upon related-key differential probability the

attack may be related key and differential-linear attack or related key and differential- non-linear attack. The attack with related key differential probability is 1 and linear approximation bias is ½ , then the attack is related key and differential-linear attack. If bias is less than ½ and differential probability is less than 1 then the attack is related key and differential- non-linear attack. Kim [118] also further extended the attack as given below.

1. Let P and P* be a pair plain texts.
2. Let K and K* be two different related keys.
3. Let $\alpha \rightarrow \beta$ be the related-key differential for E^0 with a probability $p^* = Pr_{X,K}[E^0_K(X) \oplus E^0_{K^*}(X^*) = \beta \mid X \oplus X^* = \alpha \mid K \oplus K^* = \Delta K|$ where ΔK is a specific key difference.
4. Let $\lambda_I \rightarrow \lambda_C$ be linear approximation for E^1 with a probability of ½.+ q'.
5. Let $\lambda_I * (E^0_K(P) \oplus E^0_K * (P^*)) = a$ with probability ½ + p*/2 (= p*. 1+(1-p*) . ½), where $P \oplus P^* = \alpha$ be the one bit equation for differential- linear attack.
6. Obtain the linear approximations (i) $\lambda_I * E^0_K(P) \oplus \lambda_C * E^1_K(E^0_K(P)) \oplus \lambda_k * K^0 = 0$ (ii) $\lambda_{I^{*2}} E^0_K{}^* (P^*) \oplus \lambda_c * E^1_K{}^* (E^0_K{}^* (P^*)) \oplus \lambda_K *$. K'= 0 with probability ½ + q'
7. Obtain $\lambda_c * E_K(P) \oplus \lambda_c * E_{K^*}(P^*) = 0$ with bias $2p^*q'^2$.
8. Obtain $f(E_K(P), K') \oplus f(E_{K^*}(P^*), K^{*'}) = 0$ with bias $2p^*q''^2$ for nonlinear approximation $\lambda \rightarrow$ f with a probability of q".
9. Implement the attack is shown in fig. 43.

The attack requires $O(p^{*-2}q^{"-4})$ related-key chosen plaintexts to succeed [118].

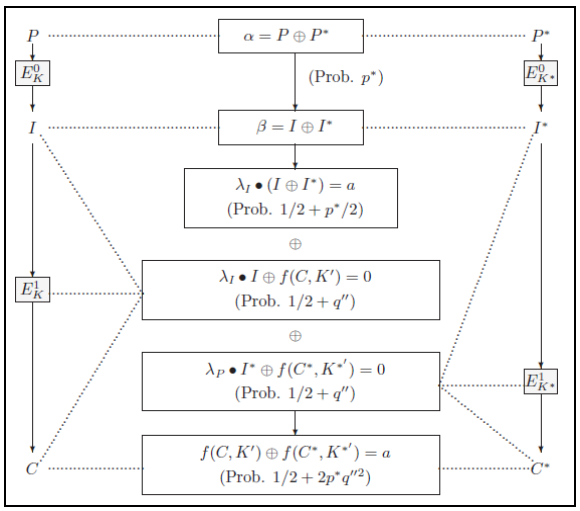


Fig.43 Related-Key Differential-Nonlinear Distinguisher

5.5. Related-Key Rectangle and Boomerang attacks

Kim [118] proposed another combined attack namely Related-Key Rectangle and Boomerang attacks. To implement this attack Kim has devised different distinguishers based upon the type of differentials and number of related keys. Mainly three types of distinguishers were proposed[118].

Type-1: Related key Differentials in first sub cipher and regular differential in second sub cipher.

Type-2: Regular differential in first sub cipher and related key differential in second sub cipher.

Type-3: Related-key differentials in both sub-ciphers.

Procedure:

1. Select two random plaintexts of size n-bit say P and P*.
2. compute $P^* = P \oplus \alpha$ and $P'^* = P' \oplus \alpha$ for a constant α.
3. Derive cipher-texts $C = E_K(P)$, $C^* = E_K{}^*(P^*)$, $C' = E_K{}'(P')$ and $C'^* = E_K{}'^*(P'^*)$,where $K^* = K \oplus \Delta K$, $K' = K \oplus \Delta K'$, $K'^* = K \oplus \Delta K \oplus \Delta K'$ (i.e., $K \oplus K^* = K' \oplus K'^* = \Delta K$ and $K \oplus K' = K^* \oplus K'^* = \Delta K'$) and ΔK, $\Delta K'$ are key differences.
4. Verify if $C \oplus C' = C^* \oplus C'^* = \delta$ or $C \oplus C'^* = C^* \oplus C' = \delta$.
5. Compute right quartets as given below:
   (i) For TYPE 1 $\Delta K \neq 0$ and $\Delta K' = 0$ (or $\Delta K = \Delta K' \neq 0$)
   (ii) For TYPE 2 $\Delta K = 0$ and $\Delta K' \neq 0$
   (iii) TYPE 3 $\Delta K \neq 0$, $\Delta K' \neq 0$ and $\Delta K \neq \Delta K'$
   (iv) Construct right quartets ($P\ P^*; P', P,^*$) satisfying the following conditions
   a) Differential Condition 1: $P \oplus P^* = P' \oplus P'^* = \alpha$
   b) Differential Condition 2: $I \oplus I^* = I' \oplus I.^* = \beta$
   c) Differential Condition 3: $I \oplus I' = \gamma$ (or $I \oplus I'^* = \gamma$
   d) Differential Condition 4: $C \oplus C' = C^* \oplus C'^* = \delta$

These distinguishers have been shown in fig.44 [118].

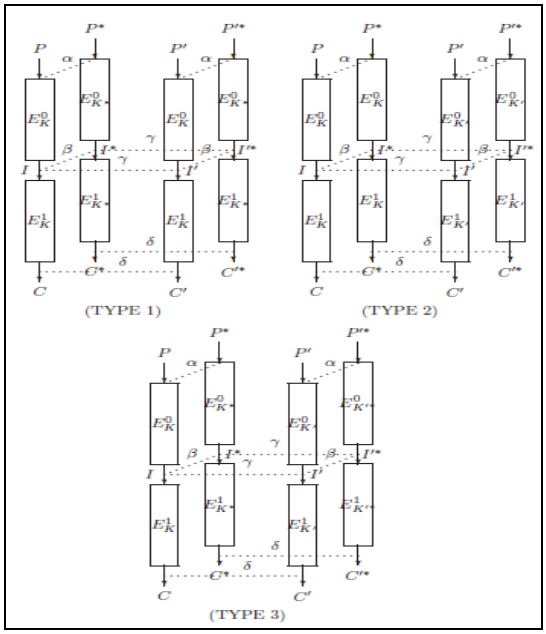


Fig.44 Related-Key Rectangle Distinguishers

5.6. Combined algebraic side-channel attacks

Side-channel attacks are powerful cryptanalytic techniques. Generally they target a specific implementation rather than an abstract algorithm. These attacks are implemented for security of embedded devices. Renauld et al proposed a new combined attack of cryptanalysis against block ciphers known as algebraic side-channel attack [127]. In this method a set of lower degree equations are used to express the block cipher and some physical information is provided. Hence, the algebraic cryptanalysis becomes very efficient to break various block ciphers.

5.7. Differential-Bilinear Attack

Biham et al proposed a new attack by combining a bilinear attack with differential attack yielding Differential-Bilinear Attack. The attack enciphers some pairs of plaintexts, and checks whether the computed pair of ciphertexts satisfy some bilinear approximation or not. This attack has been applied to eight round 5DES for a set of using 384 chosen plaintexts [128].

5.8. Higher-Order Differential and Linear combined Attack

It is combination of higher-order differentials with linear approximations. The XOR values of various sets of masked bits of elements of the cipher are compared with value with the XOR of the masked ciphertext bits in all of the encryptions. The attack uses the higher order differential to predict the XOR value of the sets of masked bits. The square-nonlinear attack was used to attack reduced round version of SHACAL-2 [128]

5.9. Combining the Boomerang Attack with Linear and Bilinear Techniques

A new attack was proposed by Kim [118] to exploit the β difference between the intermediate decryption values X3 and X4 of the encryptions whose ciphertexts are C3 and C4. If there is a differential-bilinear approximation for $E^{-1}{}_{0,}$ then the pair (X3, X4) has the required input difference, and thus, there is some bilinear relation between X3 and X4 whose probability not equal zero [128].

VI. CRYPTANALYTIC TOOLS

Several crypt analytics tools have been reported from time to time. Most of the tools are application specific based. But for cryptanalysis using differential cryptanalysis etc there are no directly applicable cryptanalytic software. The general procedures are to be moulded for requirement. The general approach for development of cryptanalytic tools is shown in fig. 44. Table-IV presents some software for cryptanalysis.

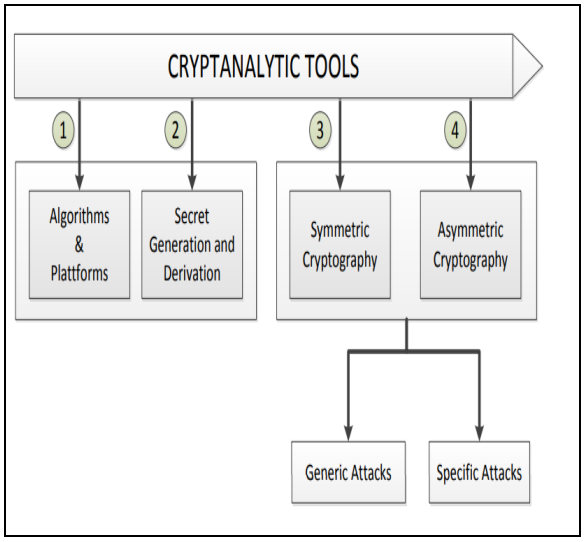


Fig.45 Cryptanalytic tool development approach

Table IV Crypt analytical Tools [126,129]

Tool	Utility
CrypTool1	It includes asymmetric ciphers like RSA, elliptic curve cryptography. CrypTool1 (CT1) experiments with different algorithms and runs on Windows. It was developed in C++ language.
CT2	It runs on Windows. It has an improved GUI and more than hundred crypto logical functions. It is developed in .NET &C#
JCrypTool	It is platform independent. CT works on Linux, MacOS, and Windows. JCT is both a function – centric as well as a document – centric tool
EverCrack	It is open source software, implemented on web. The algebraic design of kernel of this software enables to attack unilateral, monoalphabetic ciphers. instantaneously.
Cryptol	It is useful in design and implementation of new ciphers and evaluation any cryptographic algorithm.
Alpha Peeler	Alpha Peeler is a powerful tool for learning cryptology and is a free software. It may be implemented on classical ciphers and a few modern ciphers such ass MD5, SHA – 1, RSA key generation, RIPEMD – 16, Playfair etc.
Crypto Bench	It can be implemented for various cryptanalytic functions for generation hash, encryption and decryption.
Ganzúa	It is a java based tool a cryptanalysis.
EPDR	It is a password recovery tool for Word and Excel documents.
Jipher	It is a cryptanalytic tool for classical ciphers..

Tool	Utility
Linear trails	It detects the linear characters.
MILP	S-Box Mixed-Integer Linear Programming tool
Hash Clash	It can used for attacks MD5 & SHA-1.
ARX Toolkit	The ARX toolkit is a set of tools to study ARX ciphers and hash functions
Linear Hull Cryptanalysis of PRESENT	A tool to compute linear hulls for PRESENT cipher
Automated Algebraic Cryptanalysis	A simple tool for the automatic algebraic cryptanalysis of a large array of stream- and block ciphers
CryptoSMT	A tool for cryptanalysis of symmetric primitives like block ciphers and hash functions

VII CONCLUSION

In the present paper we have reviewed various cryptanalytic attacks that include both basic attacks and combined attacks. The summery of the review is given below.

1. The main objective all the attacks are to deduce the secret key to defeat the cryptosystems.
2. It is essential to find the weakness or flaws in the crypto system to break the cipher.
3. Also, cryptanalysis is a process of attempting to discover plain text or key or both.
4. The strategy used by the cryptanalysis depends on the nature of the encryption scheme and the information available to the cryptanalyst.
5. Differential cryptanalysis, linear cryptanalysis and related key cryptanalysis are prime cryptanalytic techniques.
6. Block ciphers are the prime subjects for all types cryptanalysis when compared to stream ciphers.
7. Differential cryptanalysis exploits the high probability of certain occurrences of plaintext differences and cipher text differences into the last round of the cipher.
8. Linear cryptanalysis tries to find highly probable linear expressions involving plaintext bits, ciphertext bits and the sub key bits to break ciphers.
9. A related-key attack is an operation on a cipher with several different keys whose values are initially unknown, but where some mathematical relationship connecting the keys is known to the attack.
10. Differential and Linear cryptanalysis have several variations adopting new strategies.
11. Linear cryptanalysis is a simpler attack when compared Differential cryptanalysis and Related key crypt analysis. But most of the ciphers are vulnerable to differential cryptanalysis.
12. In addition to individual attacks several combined attacks were reported. The motivation for these combined attacks is an assumption that instead of individual attacks, combination of various attacks may defeat the security of the systems quickly and efficiently.
13. The combined attacks may lead to new attacks that may be designed from the existing cryptanalytic attacks, with improved security level.
14. The Differential-Linear Cryptanalytic Attack, the Differential-Nonlinear Attack, The Square-(Non) linear Attack, The Related-Key Differential-(Non) linear Attack, Related-Key Rectangle and Boomerang attacks, Combined algebraic side-channel attacks, Differential-Bilinear Attack and Combining the Boomerang Attack with Linear and Bilinear Techniques are some combined attacks reported in the literature. These attacks have been applied to block ciphers, hash functions, message digests and message authentication algorithms.
15. It is observed that the combined attacks more effective for cryptanalysis. Due to the possibility of numerous combinations of the attacks, there will be commendable scope for further research in this direction.
16. Also some useful cryptanalytic tools have been referred.
17. Overall review of the cryptography and cryptanalysis observes that the cryptanalysis is being implemented using hardware, software and combinations of both.
18. It has also been viewed that Cryptanalysis tools are not general but application specific.
19. Individual has to design their own attack using the available techniques as per requirement of the ciphers.
20. Recently stastical approaches becoming more prominent than the traditional cryptanalytic tools.
21. The combination of statistical methods and combined attacks model may have scope for developing new techniques.
22. New fields like Cloud computing, Mobile computing, Distributed systems, Data Science & Data analytics, IoT, Adhoc networks, WSN etc are emerging and providing enormous scope for potentially advance research for cryptanalysis.

Acknowledgements

Dr. B. Srinivasa Rao is very much thankful to Dr. L. Pratap Reddy, Professor, Department of Electronics and Communication Engineering, JNTUH, Hyderabad for his supervision of my research work and valuable suggestions. He is also thankful to the management of Gokaraju Rangaraju Institute of Engineering and Technology, Bachupally, Hyderabad for encouragement and cooperation.

REFERENCES

[1] Rescorla E.**,** SSL and TLS: Design and Building Secure System, Addison Wesley Professional, U.S.A. 2001

[2] Ooi S.K. and. Vito C.B., Cryptanalysis of S-DES, University of Sheffield Centre, Taylor's College, 1st April 2002

[3] Noorman, J., Van Bulck, J., Muehlberg, T.J., Piessens, F., Maene, P., Preneel, B., Verbauwhede, I., Goetzfried, J., Mueller, T., and Freiling, F., "Sancus 2.0: A Low-Cost Security Architecture for IoT Devices," ACM Transactions on Privacy and Security PP (99), 32 pages, 2017.

[4] Schneier B., Applied Cryptography, Ed.2, John Wiley and Sons. 1996

[5] Schneier B.et. al., The Two fish Encryption Algorithm, John Wiley and Sons. 1999

[6] Yeun C.Y., Design Analysis and applications of cryptographic techniques, Ph.D. Thesis, Department of Mathematics, Royal Holloway University of London. 2000

[7] Schaefer E., A Simplified Data Encryption Standard Algorithm, Cryptologia 96 1996

[8] Mirzan F., Block Ciphers and Cryptanalysis, Department of Mathematics, Royal Holloway University of London 2000

[9] Schulzrinne H., Network Security: Secret Key Cryptography, Columbia University, New York 2000

[10] Heys M. H., A Tutorial on Linear and Differential Cryptanalysis, Memorial University of Newfoundland, Canada 2000

[11] Kilian J. and Rogaway P., How to Protect DES against Exhaustive Key Search, NEC Research Institute U.S.A. 2000

[12] Aoki K., et. al. Camellia: A 128-Bit Block Cipher Suitable for Multiple Platforms, NTT Corporation and Mitsubishi Electric Corporation 2000

[13] Pierson G. L., Comparing Cryptographic Modes of Operation using Flow Diagrams, Sandia National Laboratories, U.S.A. 2000

[14] Garrett P., Making, Breaking Codes, Prentice Hall, U.S.A. 2001

[15] Singh S., The Science of Secrecy, Fourth Estate Limited 2000

[16] Landau S., Standing the Test of Time: The Data Encryption Standard, Sun Microsystems 2000

[17] Kiljan S., De Cock D., Simoens K., Van Eekelen M., and Vranken H., A Survey of Authentication and Communications Security in Online Banking," ACM Computing Surveys 49(4), 35 pages, 2017.

[18] De Cnudde T., and Nikova S., Securing the PRESENT Block Cipher Against Combined Side-Channel Analysis and Fault Attacks, IEEE Transactions on Very Large Scale Integration (VLSI) Systems 25(10), pp. 1-11, 2017.

[19] Chen Y., Luykx A., Mennink B., and Preneel B., Efficient Length Doubling From Tweakable Block Ciphers, IACR Transactions on Symmetric Cryptology 2017(3), pp. 253-270, 2017.

[20] Luykx A., Mennink B., and Paterson K.G., Analyzing Multi-Key Security Degradation, In Advances in Cryptology – ASIACRYPT 2017, Lecture Notes in Computer Science, T. Peyrin, and T. Takagi (eds.), Springer-Verlag, 30 pages, 2017.

[21] Perrin L., Udovenko A., Biryukov A. (2016) Cryptanalysis of a Theorem: Decomposing the Only Known Solution to the Big APN Problem. In: Robshaw M., Katz J. (eds) Advances in Cryptology – CRYPTO 2016. CRYPTO 2016. Lecture Notes in Computer Science, vol 9815. Springer, Berlin, Heidelberg

[22] Stallings W., Cryptography and Network Security, Ed.4, Pearson prentice Hall, 2006

[23] Forouzan B. A., Cryptography and Network Security, Tata Mc Graw-Hill, Special Edition, 2007.

[24] Schneier B., Applied Cryptography, Ed.2, John Wiley & Sons, 1996

[25] https://www.tutorialspoint.com

[26] http://www.crypto-it.net/eng/attacks/index.html

[27] Biham E. and Shamir A., Differential Cryptanalysis of DES-like Cryptosystems, Advances in Cryptology, LNCS 537, pp. 2-21, Springer-Verlag, 1990.

[28] Heys M. H., A Tutorial on Linear and Differential Cryptanalysis. http://www.cs.bc.edu

[29] Khurana M. and Kumari M., Variants of Differential and Linear Cryptanalysis, International Journal of Computer Applications, 131, 18, pp20-28, 2015

[30] Goyal R. and Khurana M., Cryptographic Security using Various Encryption and Decryption Method I.J. Mathematical Sciences and Computing, 3, 1-11 2017

[31] Knudsen L., Truncated and higher order differentials, in Preneel B.,(Eds.), FSE, LNCS 1008, pp.196-211, Springer-Verlag 1995

[32] Swenson C., Modern Cryptanalysis: Techniques and Advanced Code Breaking, Indianapolis: Wiley Publishing 2008

[33] Knudsen R. L. And Robshaw J. B. M., The Block Cipher Companion, Springer-Verlag 2011

[34] https://en.wikipedia.org/wiki/Truncated differential cryptanalysis

[35] Knudsen L., Truncated and Higher Order Differentials in 2nd International Workshop on Fast Software Encryption (FSE1994), Leuven: Springer-Verlag.pp. 196–211 1994

[36] Knudsen L. and Berson T., Truncated Differentials of SAFER, 3rd International Workshop on Fast Software Encryption (FSE 1996). Cambridge: Springer-Verlag. pp. 15–26. 1996

[37] Borst J., Knudsen R.L. and Rijmen V., Two Attacks on Reduced IDEA, Advances in Cryptology EUROCRYPT '97, Konstanz: Springer-Verlag. pp. 1–13. 1997

[38] Knudsen R. L., Robshaw M.J.B. and Wagner D.,Truncated Differentials and Skipjack, Advances in Cryptology- CRYPTO '99, Santa Barbara, California: Springer-Verlag. pp. 165–180 1999

[39] Matsui M., and Tokita T., Cryptanalysis of a Reduced Version of the Block Cipher E2, 6th International Workshop on Fast Software Encryption (FSE 1999), Rome: Springer-Verlag. pp. 71–80 1999

[40] Moriai S. and Yin L. Y., "Cryptanalysis of Two fish (II)" (PDF) 2000(Retrieved 2013-01-14)

[41] 41 Crowley P., Truncated differential cryptanalysis of five rounds of Salsa20 2006

[42] 42 La X., Higher Order Derivatives and Differential Cryptanalysis, Communications and Cryptography, (Ed. Blahut R. et al), Kluwer Academic Publishers, pp227-2331994

[43] Harpes C., Notes on High Order Differential Cryptanalysis of DES, Internal report, Signal and Information Processing Laboratory Swiss Federal Institute of Technology August 12, 1993

[44] Biham E., Higher Order Differential Cryptanalysis Preliminary draft August 13, 1993

[45] Duan M., and Lai X., Higher Order Differential Cryptanalysis Framework and its Applications, in International Conference on Information Science and Technology, Nanjing, Jiangsu, China, March 26-28, 2011

[46] Duan M., Lai X., Yang M., Sun X. and Zhu B., Distinguishing Properties of Higher Order Derivatives of Boolean Functions, in IEEE Transactions on Information Theory, 2010

[47] Canteaut A. and Videau M., Degree of Composition of Highly Nonlinear Functions and Applications to Higher Order Differential Cryptanalysis, in Knudsen R. L. (Ed.): EUROCRYPT 2002, LNCS 2332, pp. 518-533, Springer-Verlag (2002)

[48] Standaert F., Piret G. and Quisquater J. J., Cryptanalysis of Block Ciphers: A Survey," UCL, Groupe Crypto, http:// www.dice.ucl.ac.be/crypto/, Belgium 2003

[49] Hidema T. and Toshinobu K., Journal of the National Institute of Information and Communications Technology Vol.52 Nos.1/2 2005

[50] Biham E., Biryukov A., and Shamir A., Cryptanalysis of Skipjack Reduced to 31 Rounds Using Impossible Differentials, J. Stern (Ed.): EUROCRYPT'99, LNCS 1592, pp. 12–23, 1999

[51] Ben-Aroya I. and Biham E., Differential Cryptanalysis of Lucifer, Lecture Notes in Computer Science, Advances in Cryptology, proceedings of CRYPTO'93, pp. 187– 199, 1993

[52] Matsui M., Linear Cryptanalysis Method for DES Cipher, Lecture Notes in Computer Science, Advances in Cryptology, proceedings of EUROCRYPT'93, pp. 386–397, 1993

[53] Liu Y., Gu D., Liu Z., and Li W., Impossible Differential Attacks on Reduced Round LBlock, in ISPEC 2012, LNCS 7232, pp. 97-108, 2012(Springer-Verlag Berlin Heidelberg)

[54] Boura C., Naya-Plasencia M., Suder V., Scrutinizing and Improving Impossible Differential Attacks: Applications to CLEFIA, Camellia, LBlock and Simon, Asia crypt2014, LNCS Volume 8873, pp 179-199,Springer-Verlg 2014

[55] 55. Li R., B. Sun B. and C. Li C., Impossible Differential Cryptanalysis of SPN ciphers, https: //eprint.iacr.org/ 2010/ 307 2010

[56] Biham E. and Shamir A., Differential Cryptanalysis of the Data Encryption Standard, Springer-Verlag, 1993

[57] Knudsen L. and Wagner D., Integral Cryptanalysis, Daemen J. and Rijmen V. (Eds.): FSE 2002, LNCS 2365, pp. 112–127, 2002.

[58] Yeom Y., Integral Cryptanalysis and Higher Order Differential Attack," in Trends in Mathematics, Information Centre for Mathematical Sciences, Volume 8, Number 1, Pages 101-118 2005

[59] Biryukov A. and Shamir A., Structural Cryptanalysis of SASAS, Advances in Cryptology - EUROCRYPT 2001, LNCS 2045, Springer-Verlag, pp. 394–405, 2001

[60] Biham E. and Chen R., Near-Collisions of SHA-0. In M.K. Franklin, editor, Advances in Cryptology – CRYPTO 2004, volume 3152 of Lecture Notes in Computer Science, pages 290–305, Springer-Verlag, 2004.

[61] Joux A. and Peyrin T., Hash Functions and the (Amplified) Boomerang Attack, https://www.iacr.org/ archive/ crypto2007/ 46220242/46220242.pdf

[62] Anderson R., E. Biham E., Knudsen R. L., Serpent: A Proposal for the Advanced Encryption Standard, NIST AES Proposal, 1998

[63] Biham E., Dunkelman O. and Keller N.,The Rectangle Attack – Rectangling the Serpent Pfitzmann B. (Ed.): EUROCRYPT 2001, LNCS 2045, pp. 340–357, 2001

[64] Kelsey J., Kohno T., Schneier B., Amplified Boomerang Attacks against Reduced-Round MARS and Serpent, New York FSE 2000, pp. 75-93, 2000

[65] Fleischmann E., Gorski M. and Lucks S., Attacking Reduced Rounds of the ARIA Block Cipher, https://eprint.iacr.org/2009/334.pdf, Germany 2009

[66] Wagner D., The Boomerang Attack., in Knudsen R.L., editor, Fast Software Encryption – FSE'99, volume 1636 of Lecture Notes in Computer Science, pages 156–170. Springer Verlag, 1999.

[67] https://en.wikipedia.org/wiki/Related-key_attack

[68] Biham E., New types of cryptanalytic attacks using related keys, Journal of Cryptology 7.4, 229-246 1994

[69] Knudsen, L.R., Cryptanalysis of LOKI91, in: Zheng, Y., Seberry, J. (eds.) AUSCRYPT 1992. LNCS, vol. 718, pp. 196–208. Springer, Heidelberg 1993

[70] Dunkelman O., Related Key attack, http:// www.cs.haifa. ac.il /~orrd/RK-Attacks.pdf, 2011

[71] Tardy-Corfdir A. and Gilbert H., A Known Plaintext Attack of FEAL-4 and FEAL-6. In Feigenbaum J. (Eds), Advances in Cryptology - CRYPTO '91, 11th Annual International Cryptology Conference, Santa Barbara, California, USA, August 11-15, 1991, Proceedings, volume 576 of Lecture Notes in Computer Science, pages 172–181. Springer, 1991

[72] 72.Biryukov A., Wagner D. (1999) Slide Attacks. In: Knudsen L. (eds) Fast Software Encryption. FSE 1999. Lecture Notes in Computer Science, vol 1636. Springer, Berlin, Heidelberg

[73] Darakhshan J. M. and Vora l. P. Related-Key Statistical Cryptanalysis,. https://eprint.iacr.org/2007/227.pdf 2007

[74] Matsui M., Linear Cryptanalysis Method for DES Cipher, in Helleseth T., (Eds.), Advances in Cryptology - EUROCRYPT '93, Lecture Notes in Computer Science, 765, pp 386–397, Springer, 1993

[75] Cho J.N, Hamelin M. and Nyberg K.., A New Technique for Multidimensional Linear Cryptanalysis with Applications on Reduced Round Serpent, in Lee P.J. and Cheon J.H.,(Eds.), Information Security and Cryptology - ICISC 2008, 5461, Lecture Notes in Computer Science, pp383–398.,Springer, 2008.

[76] Hakala R.M. and Nyberg K., Linear Distinguishing Attack on Shannon, in Mu Y., Susilo W., and Seberry J. (Eds.), information Security and Privacy, Lecture Notes in Computer Science, 5107, pp 297–305, Springer, 2008

[77] Nakahara Jr. J., Preneel B., and Vandewalle J., Linear cryptanalysis of reduced-round versions of the SAFER block cipher family, in Schneier B.(Eds.), Lecture Notes in Computer Science, 1978, pp 244–261, Springer, 2000

[78] Bogdanov A., and Rijmen V., Zero Correlation Linear Cryptanalysis of Block Ciphers, IACR Eprint Archive Report 2011, 123, 2011

[79] Kim K., Lee S., Park S. and Lee D., How to Strengthen DES against Two Robust Attacks, proceedings of Joint Workshop on Information Security and Cryptology, 1995

[80] Gilbert H. and Handschuh H., (Eds.): FSE 2005, LNCS 3557, pp. 126–144, 2005.

[81] Courtois N T., The Inverse S-box, Non-linear Polynomial Relations and Cryptanalysis of Block Ciphers, in AES 4 Conference, LNCS 3373, pp. 170-188, Springer, 2004

[82] Courtois N T., Feistel Schemes and Bi-Linear Cryptanalysis, https://eprint.iacr.org/2005/251.pdf 2005

[83] 83.Kowalczyk L., Lewko A.B. (2015) Bilinear Entropy Expansion from the Decisional Linear Assumption. In: Gennaro R., Robshaw M. (eds) Advances in Cryptology -- CRYPTO 2015. CRYPTO 2015. Lecture Notes in Computer Science, vol 9216. Springer, Berlin, Heidelberg

[84] Kaliski Jr. B.S. and Robshaw M.J.B... Linear Cryptanalysis Using Multiple Approximations, in Desmedt Y. (Eds.), Advances in Cryptology - CRYPTO '94,Lecture Notes in Computer Science , 839, pp 26–39, Springer 1994.

[85] Biryukov A., Canni`ere C.D., and Quisquater M., On Multiple Linear Approximations, in Franklin M.K, editor, Advances in Cryptology - CRYPTO 2004, Lecture Notes in Computer Science, 3152,pp 1–22., Springer, 2004

[86] Collard B., Standaert F.C., and Quisquater J.,Improved and Multiple Linear Cryptanalysis of Reduced Round Serpent, in Pei D.,Yung M., Lin D., and Wu C., (Eds), Information Security and Cryptology, Lecture Notes in Computer Science, 4990,pp 51–65, Springer 2007.

[87] Collard B., Standaert F.C., and Quisquater J., Experiments on the Multiple Linear Cryptanalysis of Reduced Round Serpent, Nyberg K. (Eds.) Fast Software Encryption, Lecture Notes in Computer Science,5086 , pp382–397. Springer, 2008

[88] Nyberg K. Linear Approximation of Block Ciphers, Santis A.D. (Eds), Lecture Notes in Computer Science, 950, 1995

[89] Leander G., on linear hulls, statistical saturation attacks, PRESENT and a cryptanalysis of PUFFIN, in Paterson K.G.(Eds.), Advances in Cryptology - EUROCRYPT 2011, Lecture Notes in Computer Science, 6632, pp303–322, Springer, 2011

[90] 90. Hermelin M.and Nyberg K., Linear Cryptanalysis Using Multiple Linear Approximations, https://eprint.iacr.org/ 2011/093.pdf 2011

[91] Knudsen L.R., and Robshaw M.J.B., Non-Linear Approximations in Linear Crypt analysis, Maurer U. (Ed.): Advances in Cryptology - EUROCRYPT '96, LNCS 1070, pp. 224-236, 1996.

[92] 92.Coron JS., Lee M.S., Lepoint T., Tibouchi M. (2016) Cryptanalysis of GGH15 Multilinear Maps. In: Robshaw M., Katz J. (eds) Advances in Cryptology – CRYPTO 2016. CRYPTO 2016. Lecture Notes in Computer Science, vol 9815. Springer, Berlin, Heidelberg

[93] Tianingrum S. and Indarjani S. Algebraic attack on Mini-AES algorithm, AIP Conference Proceedings 1729, 020003 2016, https://doi.org/10.1063/1.4946906

[94] http://en.citizendium.org/wiki/Algebraic_attack

[95] Davies D. and Murphy S.. Pairs and triples of DES S-boxes. Journal of Cryptology, 8(1):1{25, 1995.

[96] Biham E. and Shamir A., Differential cryptanalysis of DES-like cryptosystems , in Menezes A. and Vanstone S.(Eds.), Advances in Cryptology, Crypto'90, Lecture Notes in Computer Science, 537, pp 2-21., Springer-Verlag, 1990

[97] Biham E. and Shamir A., Differential cryptanalysis of DES-like cryptosystems. Journal of Cryptology, 4,1, pp3-72, 1991.

[98] Biham E. and Shamir A., Differential Cryptanalysis of the Data Encryption Standard. Springer-Verlag, 1993

[99] 99.Matsui M., The first experimental cryptanalysis of the Data Encryption Standard, in Desmedt Y.,(Eds.) Advances in Cryptology, Crypto'94: Lecture Notes in Computer Science, 839, pp 1-11. Springer-Verlag, 1994

[100] Vaudenay S., An experiment on DES Statistical cryptanalysis. In 3rd ACM Conference on Computer and Communications Security, pp 139-147, ACM Press, 1996

[101] Harpes C. and Massey J., Partitioning cryptanalysis, in Biham E.,(Eds.), Fast Software Encryption(FSE'97), Lecture Notes in Computer Science, 1267 ,pp 13-27, Springer-Verlag, 1997.
[102] https://www.techopedia.com /definition/18091/ brute-force-attack
[103] http://www.crypto-it.net/eng/attacks/two-time-pad.html
[104] http://www.cryptoit.net/eng/attacks/frequencyanalysis.
[105] https://www.techopedia.com/definition/4018/man-in-the-middle-attack-mitm
[106] http://stephanemoore.com/pdf/meetinthemiddle.pdf
[107] Lyubashevsky V., Masny D. (2013) Man-in-the-Middle Secure Authentication Schemes from LPN and Weak PRFs. In: Canetti R., Garay J.A. (eds) Advances in Cryptology – CRYPTO 2013. CRYPTO 2013. Lecture Notes in Computer Science, vol 8043. Springer, Berlin, Heidelberg
[108] Diffie, Whitfield; Hellman, Martin E. (June 1977). Exhaustive Cryptanalysis of the NBS Data Encryption Standard"(PDF). *Computer*. **10** (6): 74–84. doi:10.1109/C-M.1977.217750.
[109] 109.Derbez P., Fouque PA. (2016) Automatic Search of Meet-in-the-Middle and Impossible Differential Attacks. In: Robshaw M., Katz J. (eds) Advances in Cryptology – CRYPTO 2016. CRYPTO 2016. Lecture Notes in Computer Science, vol 9815. Springer, Berlin, Heidelberg
[110] https://www.pcmag.com/encyclopedia/term/50439 /replay-attack
[111] https://blog.malwarebytes.com /101/2017/ 10/ out-of-character-homograph-attacks-explained/
[112] Gilles B., Peter H. and Alain T., Quantum cryptanalysis of hash and claw-free functions, Springer, Berlin, Heidelberg. pp. 163–169, doi: 10.1007/BFb0054319, (Retrieved 29 October 2017)
[113] Oechslin, P. Making a Faster Cryptanalytic Time Memory Trade-Off, Advances in Cryptology, LNCS, 2729. Pp 617doi:10.1007/978-3-540-45146-4_36, 2003
[114] Hellman, M. E., A cryptanalytic time-memory trade-off, IEEE Transactions on Information Theory. 26, 4, pp401–406; doi:10.1109/TIT.1980.1056220 (1980).
[115] Langford, S.K., Hellman, M.E.: Differential-linear cryptanalysis, in Desmedt, Y. (ed.) CRYPTO 1994. LNCS, vol. 839, pp. 17–25. Springer, Heidelberg (1994)
[116] Biham, E., Dunkelman, O., Keller, N.: Enhancing differential-linear cryptanalysis, in Zheng, Y. (ed.) ASIACRYPT 2002. LNCS, 2501, pp. 254–266. Springer, Heidelberg (2002)
[117] Dunkelman, O., Techniques for cryptanalysis of block ciphers. PhD thesis, Technion -Israel Institute of Technology, 2006
[118] Kim, J., Combined differential, linear and related-key attacks on block ciphers and MAC algorithms. PhD Thesis, Katholieke Universiteit Leuven, 2006.
[119] Lu, J., Cryptanalysis of block ciphers. PhD thesis, University of London, UK 2008
[120] Lu, J., New methodologies for differential-linear cryptanalysis and its extensions., Cryptology ePrint Archive, Report 2010/025, http://eprint.iacr.org/2010/025 2010
[121] Wei, Y.Z., Hu, Y.P. and Chen, J. Differential-nonlinear attack on 33-round SHACAL-2, 2010
[122] Xie J., Dianzi Keji Daxue Xuebao, Journal of Xidian University, 37. 102-106+118. 10.3969/j.issn.1001-2400.2010.01.018.
[123] Chao L. and Wenling W., HU Pengsong Front. Electr. Electron. Eng. China, 2, 4, 435–439 DOI 10.1007/s11460-007-0081-0 2007
[124] J. Daemen, L.R. Knudsen and V. Rijmen, The Block Cipher Square, Proceedings of FSE 1997, LNCS 1267, pp. 149-165, Springer-Verlag, 1997
[125] Knudsen L.R. and. Wagner D, Integral Cryptanalysis, Proceedings of FSE 2002, LNCS 2365, pp. 112-127, Springer-Verlag, 2002.
[126] https://resources.infosecinstitute.com/cryptanalysis-tools
[127] https://pdfs.semanticscholar.org
[128] Biham E., Dunkelman O. and Keller N.: New Combined Attacks on Block Ciphers in Gilbert H. and Handschuh H.(Eds.): FSE 2005, LNCS 3557, pp. 126–144, 2005
[129] https://github.com/Deadlyelder/Tools-for-Cryptanalysis