International Journal of Computer Applications (0975 – 8887)
Volume 131 – No.18, December 2015

Variants of Differential and Linear Cryptanalysis

Mehak Khurana
Department of Computer science
NORTHCAP University
Gurgaon, Haryana, India

Meena Kumari
Department of Computer science
NORTHCAP University
Gurgaon, Haryana, India

ABSTRACT
Block cipher is in vogue due to its requirement for integrity, confidentiality and authentication. Differential and Linear cryptanalysis are the basic techniques on block cipher and till today many cryptanalytic attacks are developed based on these. Each variant of these have different methods to find distinguisher and based on the distinguisher, the method to recover key. This paper illustrates the steps to find distinguisher and steps to recover key of all variants of differential and linear attacks developed till today. This is advantageous to cryptanalyst and cryptographer to apply various attacks simultaneously on any crypto algorithm.

General Terms
Block Ciphers, Cryptography, Cryptanalysis.

Keywords
Boomerang, Differential Cryptanalysis, Higher Order, Impossible, Integral, Linear cryptanalysis, Rectangle, Related Key, Truncated, Zero Correlation

1. INTRODUCTION
Block cipher is one of the cryptographic techniques which are used for integrity, confidentiality and authentication mechanism. Designing a cipher which is secure and immune to all present day attacks is a challenging task. Cryptanalyst has to find statistical and algebraic technique based on mathematical weakness in design with the aim to recover the secret key. Cryptanalytic method consists of analyzing mathematical properties of encryption algorithms with the aim to find the distinguishers which distinguishes the output distribution of cryptographic algorithms from uniform distribution. Based on this property one finds the distinguisher which distinguishes it from randomness and exploits this to find the key. Attack is said to be theoretically successful if cryptanalyst breaks the cipher with less key complexity than exhaustive search. It may not be practically feasible to break with lesser key complexity than exhaustive search. But lesser key complexity than brute force attack shows that the cipher design has some flaws or weakness which can be exploited in future with advent of new attacks.

There are various types of cryptanalytic attacks; based on the attackers access such as ciphertext only attack, known plaintext attack or attacker access to encryption system to generate chosen plaintext and its ciphertext or decryption process to generate plaintexts of chosen ciphertexts. The success of attack can be measured using number of plaintext-ciphertext pairs or operations required to recover secret key or partial key. When for the attack the number of operations required is less than 2^n where n is size of secret key, the cipher is said to be broken.

Biham and Shamir **[1] [2]** proposed the basic differential cryptanalytic technique based on DES, which is probabilistic chosen plaintext attack. Many modifications and extensions have been proposed and analyzed to improve the attacks on various crypto algorithms. In 1993 Biham **[3]** proposed new types of cryptanalytic attacks using related key. In 1994, Lars Knudsen **[4]** proposed truncated differential which predicts only part of the difference in a pair of texts after each round of encryption. In same year he proposed higher order differential based on the concept of higher order derivatives. Knudsen and Wagner **[5]** in 1997 proposed integral cryptanalysis where some part of plaintext is kept constant and rest part is varied with all possibilities. In 1998 Eli Biham, Alex Biryukov, and Adi Shamir used impossible differential to break IDEA and Skipjack block ciphers **[6]** by exploiting differentials that never occurs. In 1999 Boomerang attack was developed by Wagner **[7]** which states, attack is possible even if no differentials with high or low probability is present for whole cipher. This attack was modified and named as Rectangle attack **[8]** in 2001. Related Key attack can be combined with other variants of differential cryptanalysis where knowledge of difference in keys may allow to attack more number of rounds **[9]**.

Linear cryptanalysis was developed by Matsui **[10]** in 1993 to exploit linear approximation with high probability i.e. greater than ${}^{1}/_{2}$. Zero correlation is a variant of linear cryptanalysis developed by Bogdanov and Rijmen **[11]** which tries to construct atleast one non trivial linear hull with no linear trail i.e. with correlation C exactly zero. This attack is countermeasure of impossible differential attack.

To attack a cipher using integral, impossible or zero correlation attack details of S-Box is not required as it is independent of the choice of S-Box. Choosing another S-Box for a cipher will result in almost same cryptanalytic results. Fig. 1 illustrates the different types of attacks developed till today.

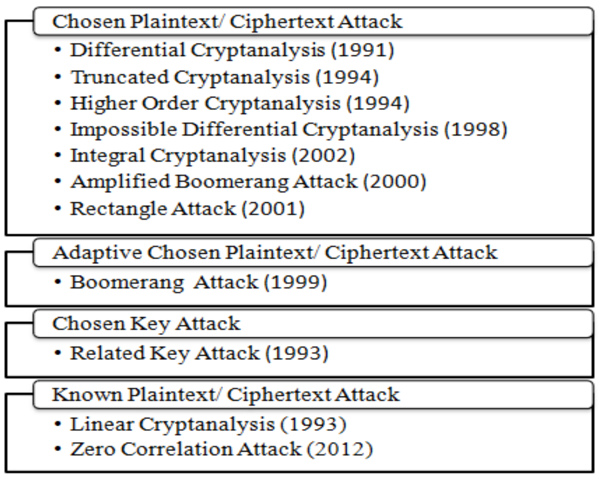

Fig 1: Types of Cryptanalytic Attacks

Differential and Linear cryptanalysis or its variants have been applied on almost all the block ciphers developed till today. The fig. 2 shows various differential and linear based attacks which are developed and their combinations. Block cipher which is resistant to one attack can be attacked by its variants or some combinations of variants. To ease the process of applying these attacks to check resistance to present day cryptanalytic attacks, the simplified steps of each attack are described in next sections.

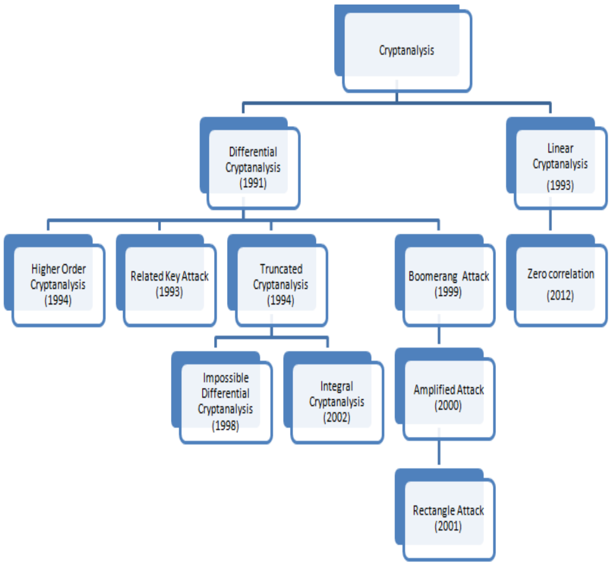

Fig 2: Variants of Cryptanalysis

2. DIFFERENTIAL CRYPTANALYSIS

In differential cryptanalysis, one attacks by exploiting the fact that for some fixed plaintext difference $\Delta \boldsymbol{P} = \boldsymbol{P} \oplus \boldsymbol{P'}$, certain differences in the ciphertext $\Delta \boldsymbol{C} = \boldsymbol{C} \oplus \boldsymbol{C'}$ appear more often than one would expect for secured design and this high probability of occurrence is used to find secret key, where P and P' are two plaintexts and C and C' are corresponding ciphertexts. To apply differential cryptanalysis, one needs to find the high probability of differentials in each S-Box used in block cipher based on Substitution Permutation Network (SPN) and then find products of high probabilities of differential of S-boxes which lead the given plaintext difference $\Delta \boldsymbol{P} = \boldsymbol{P} \oplus \boldsymbol{P'}$ to the ciphertext difference $\Delta \boldsymbol{C} = C \oplus C'$. So in order to determine the differential characteristic, Difference distribution tables are constructed for each S-Box for input difference ΔX and output difference ΔY. Due to the weakness in S-Box (nxm), high probabilities of difference pair $(\Delta X, \Delta Y)$ may be obtained instead of $1/_{2^n}$ as in the case of ideal S-Box, which is not achievable. All difference pairs of input X and output Y of an S-Box can be examined and the high probabilities of input output pairs $(\Delta X, \Delta Y)$ of each S-Boxes are traversed and combined from first round to second last round treating S-Boxes as independent. Once the differential characteristic for second last round with a suitably large enough probability p_D is discovered, it is easy to attack cipher to recover some bits of last round subkey by ex-oring all the possible combinations of all influenced nonzero difference bits TPS (Target Partial Subkeys) entering last round with the ciphertext and running one round backwards through S-boxes. The number of chosen plaintext-ciphertext pairs required for attack will be $1/_{p_D}$.

Differential cryptanalysis is divided into two steps: i) Finding the Distinguisher and ii) Steps for Key Recovery.

i) Finding the Distinguisher

1. Difference distribution table is constructed for each S-Box $(n\,x\,m)$ which contains the number of occurrences of corresponding output difference ΔY for each given input difference ΔX.
2. Find the probability of the each value of input output difference by dividing it by 2^n (number of input bits).
3. Mark S-box difference pairs from round to round so that the nonzero output difference bits from one round correspond to the nonzero input difference bits of the next round with highest probability. Therefore traversing the active S-Box (i.e. non-zero differential with high probability) difference pair from first round till second last round of the cipher. The highest probabilities of input output pairs of active S-boxes are multiplied, to get the differential probability p_D till second last round of the cipher [10].
4. So the differential probability p_D is the distinguisher

During the cryptanalysis process, many pairs of plaintexts for which ΔP will be encrypted. With high probability, the differential characteristic ΔC will occur. Such pairs for $(\Delta P, \Delta C)$ are termed as right pairs. Plaintext difference pairs for which the characteristic does not occur are referred to as wrong pairs.

ii) Steps for Key Recovery

1. Generate N plaintext/ciphertext pairs with given ΔP.
2. If k_r (TPS) is $l - bit$. There are 2^l possibilities. For each TPS value (say TPS*) do the following
   (i) Set count =0
   (ii) For each Ciphertext (i) for $i = 1\ to\ N$ do the partial decryption
      a) Ciphertext (i) ⊕TPS*
      b) Run backward through S-boxes to obtain bits into the last round S-boxes
      c) Check the input difference to the final round determined by partial decryption is the same as expected from the differential characteristic
      d) If same, increment count. The partial subkey value with largest count is considered for each TPS*
3. Obtain a table of partial subkey values and corresponding $prob = count/N$.
4. If probability (prob) as calculated in step 3 is equal to p_D (as expected)⟹ Correct TPS is determined.

For fast implementation, discard those wrong ciphertext pairs of which zeros do not appear in appropriate subblock of the ciphertext difference.

3. VARIANTS OF DIFFERENTIAL CRYPTANALYSIS

In this section variants of differential cryptanalysis are described by illustrating the steps to formulate the distinguisher and steps to recover key.

3.1 Truncated Differential Cryptanalysis

In case of differential cryptanalysis, one exploits the probability of fixed plaintext difference of two plaintexts that produces the predicted Ciphertext difference of the respective ciphertexts, but in case of truncated differential, instead of getting the exact differential in plaintext and Ciphertext, one exploits the probability of subset of plaintext differences and subset of predicted Ciphertext differences [12]. Wherever the value in the difference is not as predicted in Differential cryptanalysis that are denoted by **'?'** (don't care), So the predicted probability of truncated differential increases the number of plaintext and Ciphertext pairs to be counted in the distinguisher, which in turn increases the probability of recovering the key [13]. The attack is as follows:

i) Finding the Distinguisher

1. Let ΔP_α be the subset of non trivial difference ΔP of two inputs to encryption function $f: GF(2^n) \rightarrow GF(2^n)$ upto r rounds, for which only fraction of output difference ΔC i.e. ΔC_δ occurs after r rounds. The truncated differentials $\Delta P_\alpha \rightarrow \Delta C_\delta$

2. Let T be a table of size 2^n which is initialized to zero for all entries.

3. For all possible value of input x, $x \in GF(2^n)$, compute the table T by putting 1 at position $f(x) \oplus f(x \oplus \Delta P_\alpha)$, which gives truncated output ΔC_δ corresponding truncated input ΔP_α, i.e. $T[f(x) + f(x + \Delta P_\alpha)] = 1$. Therefore all possible output differentials corresponding to the truncated differential are marked and known.

ii) Steps for Key Recovery

In order to recover last round key k_r, get truncated differentials and table T values of function f of r round

1. Generate N pair of plaintext P, P' and their corresponding ciphertext C, C' respectively.

2. For all possible value of the last round key k_r, do the following:

   (i) Decrypt one round backwards C, C' using k_r, and obtain the intermediate ciphertexts M, M'

3. For all possible value of the second last round key, k_{r-1} do the following:

   (i) Calculate $t_1 = f(M + k_{r-1})$, $t_2 = f(M' + k_{r-1})$

   (ii) If $T[t_1 + t_2 + M + M'] > 0$, then pair of keys k_{r-1} and k_r are right keys. Here, measuring is done if the truncated differential was seen.

4. By repeating the attack N number of times only one unique pair of keys k_{r-1} and k_r, the right key will be suggested. Then output the values of k_{r-1} and k_r.

5. Output the subkeys for last and second last round $\boldsymbol{k_r}$ and $\boldsymbol{k_{r-1}}$ respectively.

3.2 Impossible Differential Cryptanalysis

Biham et.al. in 1998 developed variant of a truncated differential cryptanalysis called impossible differential cryptanalysis [14] [15] [16] by formulating distinguisher based on the fact that certain differentials never occur (i.e. the differentials with zero probability). It can be applied to the cipher, whose non-linear round function is bijective. To apply impossible differential attack, there is a need to find impossible differential pair $(\alpha \nrightarrow \delta)$ which can be used as distinguisher the differential α can be ΔP the difference of two plaintext P and P' or it can be the difference of two inputs N and N' after encryption of x rounds of P and P' and the differential δ can be ΔC the difference of two ciphertext C and C' or it can be the difference of two outputs M and M' after decryption of y rounds of C and C'. The difference α after $r_1 + r_2$ rounds produces the output difference δ. An impossible differential with miss in middle technique works as a distinguisher to rule out the incorrect keys, where miss in middle technique uses combination of two differentials both of which hold with probability one and do not meet in middle i.e. for r_1 rounds of partial encryption α becomes β and for partial decryption of r_2 rounds δ becomes γ (see Fig 3). If $\beta \neq \gamma$ the difference $\alpha \nrightarrow \delta$ after $r_1 + r_2$ rounds of encryption is impossible because $\alpha \rightarrow \beta \neq \gamma \leftarrow \delta$ and (α, δ) is called impossible differential pair. Keys are eliminated or discarded for which impossible differential characteristic $\beta \neq \gamma$ holds for the subkey of that key.

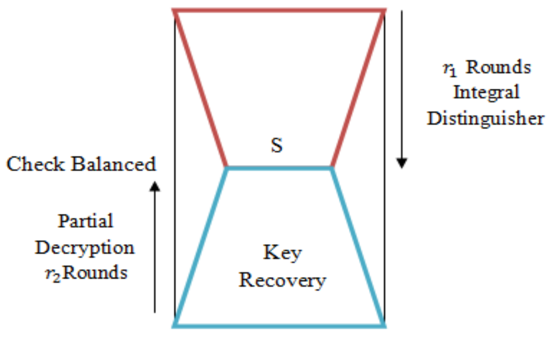

Fig 3: Miss in middle

i) Finding the Distinguisher

To obtain impossible differentials $(\boldsymbol{\alpha \nrightarrow \delta})$

1. Obtain the input differential $\alpha = N \oplus N'$, encrypt N, N' by r_1 rounds to obtain differential β of the outputs i.e. $Pr(\alpha \rightarrow \beta) = 1$

2. For the differential $\delta = M \oplus M'$, decrypt M, M' by r_2 rounds to obtain values with differential γ i.e.$Pr(\delta \rightarrow \gamma) = 1$

3. If $\beta \neq \gamma$ then $\alpha \nrightarrow \delta$ is impossible

4. Repeat above 4 steps for different values (α, δ) to obtain a set ID i.e. $ID = (\alpha_1, \delta_1), (\alpha_2, \delta_2) \ldots.(\alpha_n, \delta_n)$.

ii) Filtering and Key Elimination

For each key, obtain subkey after x rounds and y rounds. Do the following to rule out the invalid subkeys.

1. For input-output pairs (N, M) and (N', M'). Check $N \oplus N' = \alpha$ and $M \oplus M' = \delta$ i.e. $(\alpha, \delta) \in ID$
2. Find the differential β of the values after encrypting N and N' by r_1 round
3. Find differential γ of the value after decrypting M, M' by r_2 rounds
4. Check $\beta \neq \gamma$ then subkey is invalid.
5. Rejecting the invalid keys, the total key space is reduced.

3.3 Integral Cryptanalysis

In 1997, Daemen, Knudsen and Rijmen published new block cipher called SQUARE, and later discovered an attack on it and named as Square Attack which could not be able to attack large number of rounds. This attack was later on named as Saturation Attack. Finally in 2002, Knudsen and Wagner came up with many improvements and modifications by combining different techniques and named it as Integral Cryptanalysis [17]. Block ciphers which uses bijective components are prone to integral cryptanalysis.

The integral is defined as $\int R = \sum_{B \in R} B$, where $B = \{b_1, b_2 \dots . b_n\}$ is a state vector where each $b_i \in GF(2^n)$. R is a multiset of state vectors. In integral 'n' represents the number of words in the plaintext and ciphertext, for example in AES the state vector is of 16 words each of 8 bits. In this attack, attacker tries to predict the values in the integral after certain number of rounds of encryption. The following properties can be observed in output of cipher rounds which play an important role to construct basic model of integral distinguisher to distinguish several rounds of block cipher from random permutation.

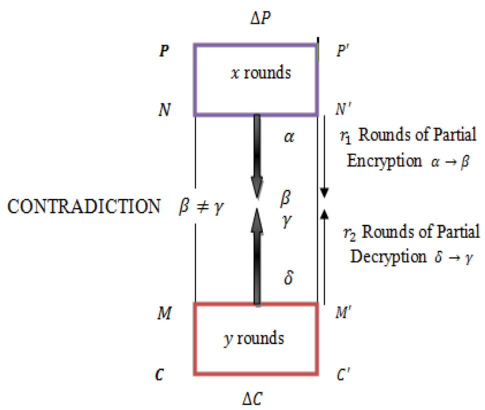

Fig 4: Integral Attack

a) All i^{th} words are equal i.e. $b_i = c$ for all $B \in R$, denoted by symbol $'C'$ Where $c \in GF(2^n)$, are some fixed values (constants)

b) All i^{th} words are different $\{b_i : B \in R\} = GF(2^n)$, denoted by symbol $'A'$.

c) All i^{th} words sum to certain value predicted in advance $\bigoplus_{B \in R} b_i = c'$, denoted by symbol $'S'$ (balanced) Where $c' \in GF(2^n)$, are some fixed values (constants)

d) The sum of words that cannot be predicted i.e. no information can be derived are denoted by symbol '?'

i) Finding the Distinguisher

1. Choose an input multiset R which consists of 2^n chosen plaintexts which have above property such that plaintext with some certain words being A and rest of the words being C. e.g. P = (CCCC*;* CCCC), P' = (*ACCC; CCCC*).
2. Encrypt the multiset, after a few rounds r_1 of encryption check if all the sum (usually exclusive-or) at some word is zero (balanced) i.e. some bytes of output will have state $'S'$ (balanced) with probability one which works as a distinguisher that can distinguish few rounds of cipher from random permutation, see fig. 4.
3. Thus by changing the position of $'A'$ in chosen plaintext, different distinguisher can be obtained.

ii) Steps for Key Recovery

1. Obtain all the possible combination of subkey k_r (TPS).
2. Do the partial decryptions (for r_2 rounds) upto the output of integral distinguisher.
3. If decryption gives exclusive-or sum of the states as zero i.e. balanced, store that subkey. Otherwise, repeat the steps for other possible subkeys.
4. Repeat step 1-3 number of times for all multiset, subkey with maximum count is the correct subkey.

3.4 Higher Order Differential Cryptanalysis

Knudsen introduced higher order differential cryptanalysis based on the concept of higher order derivative proposed by Lai [18] that are applicable to those ciphers that can be expressed by multivariable Boolean functions with low degree [19].

The derivative of function $f: GF(2^n) \to GF(2^m)$ at the point a is $\Delta_a f(x) = f(x + a) - f(x)$ where $a \in GF(2^n)$. For i^{th} derivative of f at the point $\{a_1, a_2, .., a_i\} \in GF(2^n)$ is defined as $\Delta^{(i)}_{a_1, \dots, a_i} f(x) = \Delta_{a_i}\left(\Delta^{(i-1)}_{a_1, \dots, a_{i-1}}\right) f(x)$, where $\Delta^{(i-1)}_{a_1, \dots, a_{i-1}} f(x)$ is the $(i-1)^{th}$ derivative of f at $\{a_1, a_2, \dots . . a_{i-1}\}$, the 0^{th} derivative of f is defined to be $f(x)$ itself, also $\deg(\Delta_a f(x)) \leq \deg(f(x)) - 1$. For any $x \in GF(2^n)$, let $L[a_1, \dots, a_i]$ be the list of all 2^i possible combinations of $a_1, \dots, a_i$ [20]. Then

$$\Delta^{(i)}_{a_1, \dots, a_i} f(x) = \bigoplus_{v \in L[a_1, \dots, . a_i]} f(x \oplus v)$$

If a_i is linearly independent of $a_1, \dots . , a_{i-1}$, then. $\Delta^{(i)}_{a_1, \dots, a_i} f(x) = 0$. In iterated block cipher of block size n and r rounds, Attack is possible, when it is known that the total degree deg(f) of the output of the $(r-1)^{th}$ round. To attack $(r-1)$ rounds of cipher, find the order of $(r-1)$ rounds for which derivative $\Delta_{a_1, a_2, \dots, a_{r-1}} f(x) = c\ (constant) \forall x \in GF(2^n)$ i.e. independent of round keys $k_1, k_2, \dots, k_{r-1}$. The steps to find the order are given in [21]. The attack is based on the property that the d^{th} derivative of a multivariate polynomials f with degree d is a constant and $(d+1)^{th}$ derivative is zero.

i) Finding the Distinguisher

1. Randomly choose a plaintext $P \in GF(2^n)$
2. Encrypt plaintexts $P \oplus v, \forall v \in L[a_1, \dots, .a_i]$ to obtain their corresponding ciphertexts c_v.
3. Compute $\bigoplus_{v \in L[a_1,\dots,a_i]} f(x \oplus v)$
4. If $\bigoplus_{v \in L[a_1,\dots,a_i]} f(x \oplus v) = c$ (constant) $\forall x \in GF(2^n)$, for $(r-1)$ round with any round keys $k_1, k_2, \dots, k_{r-1}$.This will work as a distinguisher to recover the key.

ii) Steps for Key Recovery

1. Generate N plaintext randomly. For each plaintext P, do the following
2. For all the possible combination of last round influenced bits k_r (TPS), if k_r is $l - bits$, there are 2^l possibilities for each k_r value, for each value of TPS (say TPS*) Do the following
   (i) Decrypt all ciphertexts c_v one round backwards using TPS*
   (ii) The value of TPS* for which $\bigoplus_{v \in L[a_1,\dots,a_i]} f_{k_r}^{-1}(c_v)$ becomes constant $\forall v \in L[a_1, \dots, .a_i]$, store that TPS* value in a table T and reject TPS* if $\bigoplus_{v \in L[a_1,\dots,a_i]} f_{k_r}^{-1}(c_v)$, $\forall v \in L[a_1, \dots, .a_i]$ is not constant.
2. Repeat the step 2 for N plaintexts and the key in the table T with highest probability is the correct last round key. Output that key k_r.

Higher order cryptanalysis can be applied to maximum 5 feistel rounds of cipher i.e. cannot defeat ciphers with large or more than 6 rounds.

3.5 Boomerang Cryptanalysis

In 1999, Boomerang was developed by Wagner **[7]** which states that even if there is no differential with either high or low probability for whole cipher, it may still be vulnerable to Boomerang attack. It is an adaptive chosen plaintext/Ciphertext attack in which attacker finds two short differentials with high probabilities instead of one whole differential with low probability.

The block cipher encryption $E: \{0,1\}^n X \{0,1\}^k = \{0,1\}^n$ is decomposed into two halves $E = E_0 \, o \, E_1$ where E_0 represents first half and E_1 represents second half. Differential characteristic for E_0 is $\alpha \rightarrow \beta$ with probability p and for E_1^{-1} the differential characteristic is $\delta \rightarrow \gamma$ with probability q [7]. In boomerang attack, to find all plaintexts sharing a desired difference that depends on the choice of the differential is the distinguisher [22].

i) Finding the Distinguisher

1. The attacker randomly chooses two plaintexts P, P' and computes $\alpha = P' \oplus P$
2. Encrypt P and P' by E_0 to obtain middle ciphertext $M = E_0(P)$ and $M' = E_0(P')$ and further encrypt for E_1 to obtain ciphertext $C = E_1(M)$, $C' = E_1(M')$.
3. Obtain new ciphertexts D, D' from ciphertexts C, C' with difference δ i.e. $D = C \oplus \delta$ and $D' = C' \oplus \delta$ such that by decrypting C, C' by $E_1^{-1}$and D, D' by E_1^{-1} the difference γ is obtained i.e. $E_1^{-1}(C) \oplus E_1^{-1}(D) = E_1^{-1}(C') \oplus E_1^{-1}(D') = \gamma$
4. Decrypt these Ciphertext D and D' for E_1^{-1} partially to get N, N' and further decrypt it for E_0^{-1} to get O and O' i.e. $O = E_0^{-1}(N)$ and $O' = E_0^{-1}(N')$.
5. Finally for each pair (O, O') check whether O and O' differ by same differential α i.e. $O \oplus O' = \alpha$. If this condition is satisfied, it means it has formed a right quartet (P, P', O, O'). If so, store the quartet.
6. Repeat these steps with other set of plaintext to find other pairs that form right quartets and store it in a table (Boomerang distinguisher).

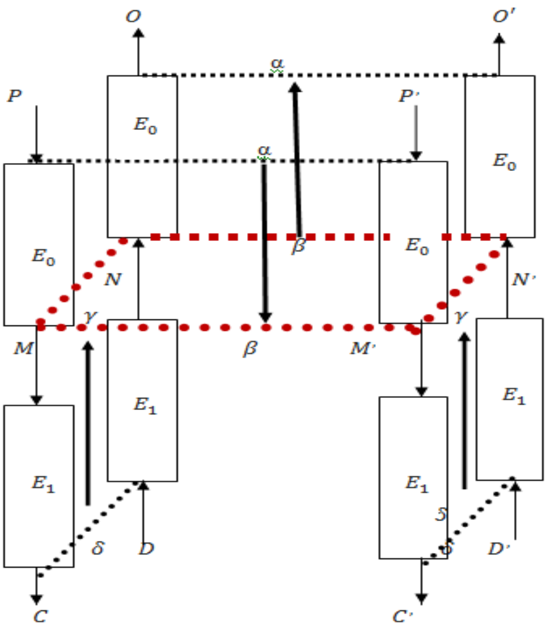

Fig 5: Structure of Boomerang Attack

ii) Steps of Key Recovery

1. From set of boomerang distinguisher, for each obtained right quartets (P, P', O, O')
2. Find all possible values for nonzero influenced difference bits entering last round (TPS).
   (i) For all the possible values TPS (k_r) i.e. if k_r is $l - bits$, there are 2^l possibilities for each k_r value, Do the following Set count =0.
   (ii) Encrypt (P, P', O, O') and obtain the corresponding ciphertext quartet (C, C', D, D') respectively.
   (iii) Then do the one round partial decryption d_k under key k_r

a) $\bar{C} = d_{k_r}(C), \bar{C}' = d_{k_r}(C')$ and $\bar{D} = d_{k_r}(D), \bar{D}' = d_{k_r}(D')$

b) Check the difference by partial decryption $\bar{C} \oplus \bar{C}'$ and $\bar{D} \oplus \bar{D}'$ is the same as expected from the differential characteristic.

c) If difference is same in both the pairs then increment the count

3. Value of TPS which has maximum count for right quartet is correct TPS and output that value.

3.6 Rectangle Cryptanalysis

Boomerang uses adaptive chosen plaintext/ciphertext due to which many of the ciphers that were developed through the years cannot be attacked by boomerang distinguishers and key recovery attack cannot be applied [8], which led to the development of its chosen plaintext variant called amplified attack [23]. This was later modified and named as rectangle attack.

The Rectangle attack is divided into two steps: 1) Finding the distinguisher 2) Key Recovery (same as Boomerang) [24]

i) Finding the Distinguisher

1. The attacker randomly chooses two plaintext pairs $(P, P'), (O, O')$ with same difference α such that $\alpha = P' \oplus P$ and $\alpha = O' \oplus O$.
2. Encrypt (P, P') and (O, O') to obtain middle ciphertexts i.e. $M = E_0(P)$ and $M' = E_0(P')$ and $N = E_0(O)$ and $N' = E_0(O')$, we are interested in the cases where $M \oplus M' = \beta$, $N \oplus N' = \beta$ and $M \oplus N = \gamma$, which leads to $M' \oplus N' = (M \oplus \beta) \oplus (N \oplus \beta) = \gamma$.
3. Two pairs ($M \oplus N$ and $M' \oplus N'$) each with the difference γ are received. When encrypting $(M, M'), (N, N')$ by E_1, i.e. $C = E_1(M), C' = E_1(M')$ and $D = E_1(N), D' = E_1(N')$ then in some of the cases γ becomes δ. And look for those cases where both difference become $C \oplus D = \delta$ and $C' \oplus D' = \delta$ after E_1. The quartet satisfying these differential requirements forms a right quartet.
4. Repeat these steps to find the pairs that form right quartets (P, P', O, O') and save it in a table (distinguisher).

ii) Steps of Key Recovery

1. From set of distinguisher, for each obtained right quartet (P, P', O, O').
2. Find all possible values for nonzero influenced difference bits entering last round (TPS).
3. For all the possible values TPS (k_r) i.e. if k_r is $l - bits$, there are 2^l possibilities for each k_r value, Do the following for each right quartet.

(i) Set count =0

(ii) Do the partial decryption by one round.

(iii) Check the input difference by partial decryption is the same as expected from the differential characteristic.

(iv) If same, increment count for that TPS.

4. TPS which has maximum count value for right quartet that is correct and output that value.

3.7 Related Key Cryptanalysis

In key schedule algorithm of block cipher, if the relations between pairs of keys in different rounds exist then all the subkeys can be shifted one round backward and a new set of subkeys can be obtained, these key relations can be used to attack the block ciphers. The attack where keys are unknown, but relation is known to the attacker is called chosen key attacks. The attacks are not dependent on number of rounds of a cipher **[25]**.

The Chosen Key Attacks

Several plaintexts are encrypted by these related keys. After encryption the corresponding ciphertexts are obtained under these related keys which have some relation between them, this relation is used by attacker to find both the keys. Chosen Key attack can be further divided into

- Chosen Key Known Plaintext Attack
- Chosen Key Chosen Plaintext Attack

In chosen key known plaintext attack, attacker exploits only relation between the keys and in chosen key chosen plaintext attack, the relation between keys and plaintext are exploited by the attacker. The process of recovering the keys is almost same in both cases.

i) Steps for Key Recovery

1. The attacker chooses such a plaintext pair P and P^* such that right half of P equals the left of P^* i.e. $P_R = P_L^*$.
2. P is encrypted with key K and result of encryption of P is obtained before next round which may be the same as P^* encrypted with key K^* after first round.
3. For plaintexts P and P^* corresponding ciphertext C and C^* is obtained after encryption after all rounds and if these ciphertexts satisfies the relation $C_L = C_R^*$, then it has high probability to find expected pair (by birthday paradox).
4. If attacker find such pairs then P, P^*, C, C^* and K, K^* can be used to recover secret key bits with less trails than brute force attack.

For chosen plaintext attack $2^{n/4}$Chosen plaintexts are required and for known plaintext attack $2^{n/2}$ known plaintexts are required.

4. LINEAR CRYPTANALYSIS

Matsui in 1993 developed linear attack to attack DES by exploiting linear approximation with high probability of input and second last round output of DES cipher by known plaintext approach. In this attack linear expression of u bits of input and v bits of output which holds high or low probability is exploited to find the key. The bias probability ($\varepsilon = |p_L - 1/2|$) is amount it deviates from probability $1/2$ where p_L is the probability of holding the linear expression. The higher the magnitude of the bias $|p_L - 1/2|$, poorer the randomization ability of the 0 cipher and weak is the system, so with fewer known plaintext this attack can be applied. If $P_L > 1/2$ expression $X_{i_1} \oplus X_{i_2} \oplus X_{i_3} \ldots \oplus X_{i_u} \oplus Y_{i_1} \oplus Y_{i_2} \oplus Y_{i_3} \ldots \oplus Y_v = 0$ between u input bits and v output bits of second last round is called linear approximation and if $p_L < 1/2$ it is called affine approximation. Distinguisher for the attack is the bias probability of holding the linear attack of plaintext bits and the second last round of cipher; following are the steps to find distinguisher of SPN cipher with $\boldsymbol{r}$ rounds.

i) Finding the Distinguisher

1. Generate the linear approximation table of order $2^n\ x 2^m$ for each S-Box of size nxm by

(i) Form a table for each nxm S-Box where the elements of the table represent the number coincides between linear relation $a.x = a_1x_1 \oplus a_2x_2 \oplus \dots\ a_nx_n$ of input and the linear relation $b.y = b_1y_1 \oplus b_2y_2 \oplus \dots\ b_my_m$ of the output where a, b represents n and m bit numbers respectively for $0 \le a \le 2^n - 1$ and $0 \le b \le 2^m - 1$. In a table the binary value of $a_1a_2a_3 \dots a_n$ (a_1 the MSB) represents row no, the binary value of $b_1b_2b_3 \dots b_m$ (b_1 the MSB) represents column no.

(ii) Calculate the coincidence probability p_L by dividing the elements of linear approximation table by 2^n (number of input bits).

(iii) Calculate the bias probability ε for each high coincidence probability p_L of each S-Box for each round by using formula $\varepsilon = |p_L - {}^1\!/_2\,|$.

2. Mark the linear trail for the whole cipher by considering those elements of S-Boxes with highest bias probability ε in each round till second last round.

3. Calculate the expected bias probability p_D of holding the linear expression between input and the last round cipher by using pilling up lemma, considering all S-Boxes as independent. For each round function the linear expression which hold with high coincidence probability and calculate bias probability by subtracting from ½ and combine this linear expression with next round linear expression with highest coincidence probability and go on calculating ε_i for each round and at last probability of

$$p_D(x_1 \oplus x_2 \oplus \dots \oplus x_n = 0) = {}^1\!/_2 + 2^{k-1} \prod_{i=1\ to\ k} \varepsilon_i$$

where $\varepsilon_{1,2\dots k} = 2^{k-1} \prod_{i=1\ to\ k} \varepsilon$.

ii) Steps to Recover Key

1. Generate N plaintext / ciphertext pairs
2. If TPS is l-bit. There are 2^l possibilities
3. For each TPS value (say TPS*) do the following

(i) Set $count\ = 0$

(ii) For each ciphertext(i) for i=1 to N do the partial decryption

(a) ciphertext (i) ⊕ TPS*

(b) Run backward through S-boxes to obtain bits into the last round S-boxes

(c) XOR the Bits of plaintext (i) with XOR of the bits obtained in step (b)

(d) If expression in (c) is zero

(e) Increment count

(iii) $|Bias| = |count - N/2|$

4. Obtain a Table of partial subkey values and corresponding $|Bias|$
5. If $|Bias| = 0 \Rightarrow$ Incorrect TPS
   If $|Bias| \approx Expected\ value \Rightarrow$ Correct TPS

5. VARIANTS OF DIFFERENTIAL CRYPTANALYSIS

5.1 Zero Correlation Cryptanalysis

Zero correlation linear cryptanalysis was proposed by Bogdanov and Rijmen **[11]** for an iterative block cipher is a counterpart of impossible differential cryptanalysis. This attack exploits the linear approximation $a \to b$ of the cryptographic function f of the cipher of r rounds where a and b are input sum and output sum selection pattern. The probability $p = \Pr_x\{ax = bf(x)\}$ for linear approximation $a \to b$ over all input x is exactly ${}^1\!/_2$ which amounts to correlation C zero because $C = 2p - 1$ with $a \neq 0,\ b \neq 0$. The linear approximation $a \to b$ for an iterative block cipher from fixed input a to fixed output b is called a Linear Hull which contains all possible sequences of linear approximation. These set of sequences are called Linear Trails [26]. See fig 5, where f_i is the function of ith round and $u_i{}'s$ are intermediate values.

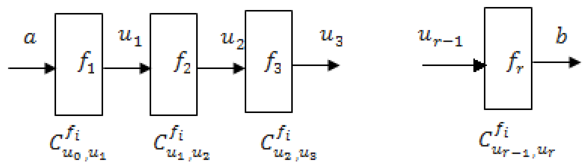

Fig 6: Linear Trail

According to pilling up lemma, the total correlation contribution $\boldsymbol{C_U}$ over a cipher of a linear trail $\boldsymbol{U}$ is a computed by identifying strong linear approximation trail by concatenating approximations from round to round and calculated by doing product of these correlation for all rounds and is defined as

$C_U = \prod_{i=1}^{r} C_{u_{i-1},u_i}^{f_i}$, where $C_{u_{i-1},u_i}^{f_i}$ is correlation for each intermediate value $u_{i-1} \to u_i$

For a linear hull $a \to b$, total correlation over a cipher is computed by summing the correlation contribution C_U of all its possible linear trails U.

$$C = \sum_{U = u_0 = a, u_1, u_2, \dots u_r = b} C_U$$

To construct zero correlation ($C = 0$) linear hull, input a and output b is selected in such a way that no linear trail exists with non-zero correlation contribution C_U i.e. if correlation contribution $C_U = 0$ for each linear trail, then correlation over the entire iterative cipher is exactly zero, $C = 0$ and it is denoted by $a \nrightarrow b$. For correlation contribution to be zero $C_U = 0$ for each trail, construct each trail with at least one intermediate $C_{u_{i-1},u_i}^{f_i}$ linear approximation $u_{i-1} \to u_i$ over the rounds to be zero since the product of all correlation values with intermediate zero correlation value will result in zero correlation $C = 0$ for this linear hull. If $C_{u_{i-1},u_i}^{f_i} = 0$ for a linear trail U, the pair of selection pattern u_{i-1} and u_i for a trail is called incompatible. If even one zero correlation linear hull (distinguisher) exists, the cipher can be attacked.

The basic steps for constructing an attack on ciphers are

i) Finding the Distinguisher

1. Choose plaintext and ciphertext pairs with fixed unknown key K.
2. Construct linear distinguisher with correlation zero $C(a \nrightarrow b) = 0$ by using miss in middle technique. This can be done by encrypting fixed input a to obtain output β for r_1 rounds of cipher, decrypting fixed output b to obtain γ for r_2 rounds of cipher.
3. Obtain the partial trails with non zero correlation contribution. If both the partial trails do not match in middle $\beta \neq \gamma$, this contradiction ensures the correlation zero therefore $r_1 + r_2$ rounds must be a zero-correlation linear hull i.e. $C = 0$. Thus correlation of linear hull is exactly zero and linear distinguisher (a, b) is obtained.

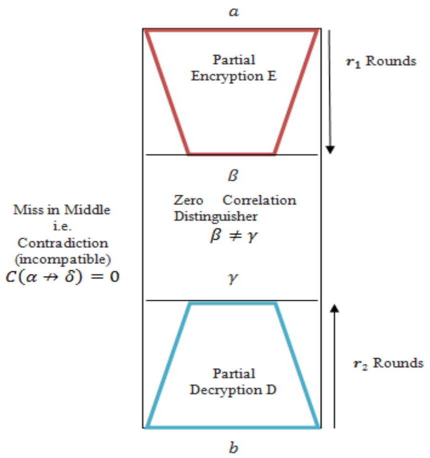

Fig 7: Zero correlation Linear Cryptanalysis Structure

ii) Steps to Recover Key

1. Obtain all the possible combination of subkey k_r (TPS) to compute encryption and decryption.
2. For each possible subkey, partially encrypt each plaintext (for r_1 rounds) and partial decrypt each ciphertext (for r_2 rounds) upto the input and output boundaries of the distinguisher (zero correlation linear approximation boundaries)
3. Evaluate the correlation for partial encryption decryption of all linear approximations for each possible subkey by counting number of times $ax \oplus bf(x) = 0$
4. If the correlation C is 0, the subkey guess is correct

The correlations for distinct linear hulls were evaluated to reduce the error probability.

6. CONCLUSION

Cryptographers as well as cryptanalysts all over the world have been applying the latest attacks to already published or newly designed crypto algorithm. To design a highly secure block ciphers which are immune to the present day attacks, one needs to analyze the possibility of any weakness in the design which can be exploited by all the variants of differential and linear attacks. The steps described in this paper, to find the distinguisher and to recover the key of each cryptanalytic attack will be of great help to cryptanalyst. With the advent of HPC and Distributed computing, these attacks will make cryptanalysis efficient. All the attacks described in this paper can be applied on SPN, feistel and generalized feistel structure with the additional condition that the round function should be bijective for impossible, integral and zero correlation. The following Table 1 consolidates the ciphers which have been attacked by variants of linear and differential cryptanalysis till today.

The proposed work, helps to apply simultaneously all the variants of differential attacks to a block ciphers. These steps of finding distinguisher and steps to recover key eases the task of cryptanalysts to apply the attack on cipher simultaneously.

CIPHER / ATTACK	DES	AES	CAMELLIA	CAST	IDEA	SAFER	LBLOCK	FEAL	TEA, XTEA	PRESENT	MISTY	SKIPJACK	CLEFIA	ARIA	KASUMI	SERPENT
Differential	*			*	*	*		*		*						
Truncated			*							*		*		*		
Higher Order	*		*	*						*	*				*	
Integral		*	*			*	*			*	*	*	*	*		*
Impossible		*	*	*			*				*	*	*	*		
Boomerang		*	*	*			*	*				*		*		
Rectangle			*													
Related Key	*	*		*			*		*						*	*
Linear	*					*		*		*						*
Zero Correlation		*	*	*			*		*			*	*			

Table 1: List of Attacks and ciphers

The steps of key recovery described in this paper on the latest zero correlation attack which is a variant of linear cryptanalysis will also help to check the weakness in the design. Future work will be to apply these attacks on various algorithms and to do comparison on basis of time and data complexity.

7. REFERENCES

[1] E. Biham, A. Shamir, “Differential Cryptanalysis of DES-like Cryptosystems,” Journal of Cryptology, Vols. 4, no.1, pp. 3-72, 1991.

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

[3] E. Biham, "New Types of Cryptanalytic Attacks Using Related Keys," Journal of Cryptology, Springer-Verlag, vol. 7, no. No. 4, p. 229–246, 1994.

[4] L. Knudsen, "Truncated and higher order differentials," in In B.Preneel,editor, FSE, LNCS 1008, pp.196-211, Springer,1995., 1995.

[5] L. Knudsen, D. Wagner, “Integral Cryptanalysis (Extended Abstract),” in FSE 2002, LNCS 2365, pp. 112–127, Springer-Verlag, 2002.

[6] E. Biham, A. Biryukov, A. Shamir, “Cryptanalysis of Skipjack Reduced to 31 Rounds using Impossible Differentials,” in Advances in Cryptology: EUROCRYPT'99 LNCS 1592, pp. 12-23, Springer Verlag, 1999.

[7] D. Wagner, "The Boomerang Attack," in Fast Software Encryption, FSE’99 (L. R.Knudsen, ed.) Springer-Verlag, vol. 1636 of Lecture Notes in Computer Science, p. 156–170, 1999.

[8] E. Biham, O. Dunkelman, N. Keller, "The Rectangle Attack - Rectangling the Serpent," EUROCRYPT 2001 LNCS, Springer, Heidelberg (2001), vol. 2045, pp. 340-357, (2001).

[9] E. Biham, O. Dunkelman, N. Keller, "Related-Key Boomerang and Rectangle Attacks.," EUROCRYPT 2005, LNCS, Springer, Heidelberg (2005), vol. 3494, pp. 507-525, 2005.

[10] Howard M. Heys, A Tutorial on Linear and Differential Cryptanalysis.

[11] A. Bogdanov, V. Rijmen, “Zero Correlation Linear Cryptanalysis of Block Ciphers,” IACR Eprint Archive Report 2011/123, March 2011.

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

[13] Lars R. Knudsen, Matthew J.B. Robshaw, The Block Cipher Companion, Springer-Verlag, 2011.

[14] Y. Liu, D. Gu, Z. Liu, Wei Li, “Impossible Differential Attacks on Reduced Round LBlock,” in ISPEC 2012, LNCS 7232, pp. 97–108, 2012, Springer-Verlag Berlin Heidelberg 2012, 2012.

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

[16] R. Li1, B. Sun1 and C. Li, "Impossible Differential Cryptanalysis of SPN Ciphers," https://eprint.iacr.org/2010/307.pdf, 2010.

[17] Y. Yeom, “Integral Cryptanalysis and Higher Order Differential Attack,” in Trends in Mathematics, Information Center for Mathematical Sciences, Volume 8, Number 1, June, 2005, Pages 101-118, 2005.

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

[19] M. Duan, X. Lai, Mohan Yang, X. Sun, B. Zhu, “Distinguishing Properties of Higher Order Derivatives of Boolean Functions,” in IEEE Transactions on Information Theory, Jul 2010.

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

[21] Francois-Xavier Standaert, Gilles Piret, Jean-Jacques Quisquater, “Cryptananlysis of Block Ciphers: A Survey,” UCL, Groupe Crypto, http://www.dice.ucl.ac.be/crypto/, Belgium, 2003.

[22] E. Biham, O. Dunkelman, N. Keller, "New Results and boomerang and rectangle attack," in Proceeding of Fast Software Encryption, LNCS 2365, Springer verlag, pp 1-16, 2002.

[23] J. Kelsey, T. Kohno, B. Schneier, Amplified Boomerang Attacks Against Reduced-Round MARS and Serpent, New York : FSE 2000, Springer-Verlag. pp. 75–93, 2000.

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

[25] E. Biham, “New Types of Cryptanalytic Attacks Using Related Keys,” Journal of Cryptology, Springer-Verlag, vol. 7, no. No. 4, p. 229–246, 1994.

[26] A. Bogdanov and V. Rijmen, “Linear hulls with correlation zero and linear cryptanalysis of block ciphers,” Designs, Codes and Cryptography, vol. 70 , no. 3, pp. 369-383, March 2014 .