DC(Differential Cryptanalysis)

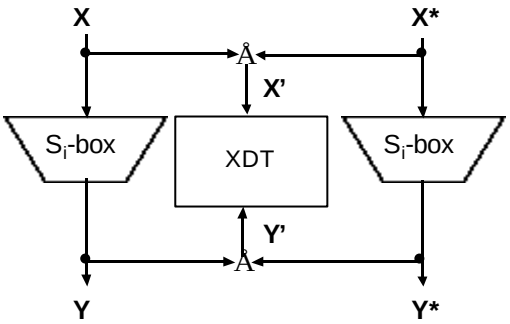
- **Introduction**
  - Biham and Shamir : CR90, CR92
  - Efficient than Key Exhaustive Search
  - Chosen Plaintext Attack
  - O(Breaking DES_{16}) ~ 2^{47}
  - ***Utilize the probabilistic distribution between input XOR and output XOR values Iteratively***
  - Stimulate to announce hidden criteria of DES [Cop92]
  - Apply to other DES-like Ciphers

* E.Biham, A. Shamir,"Differential Cryptanalysis of the Data Encryption Standard ", Springer-Verlag, 1993

DC of DES

- **Discard linear components(IP, FP)**
- **Properties of XOR ($X' = X \oplus X^*$)**
  - {E,P,IP} : $(P(X))' = P(X) \oplus P(X^*) = P(X')$
  - XOR : $(X \oplus Y)' = (X \oplus Y) \oplus (X^* \oplus Y^*) = X' \oplus Y'$
  - Mixing key : $(X \oplus K)' = (X \oplus K) \oplus (X^* \oplus K) = X'$
  - differences(=xor) are linear in linear operation and in particular the result is key independent.

XOR Distribution Table(I)



- X' = {0,1, ..63}, Y' = {0,1, ..15}
- For a given S-box, pre-compute the number of count of X' and Y' in a table

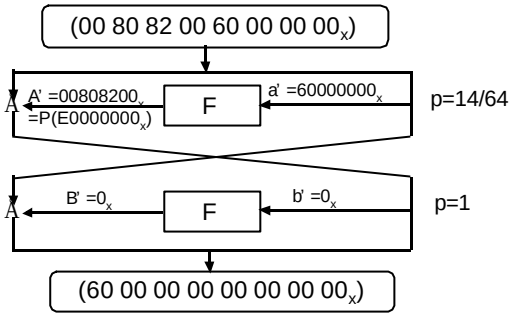
* % of entry in DES S-boxes : 75 ~ 80%

XOR Distribution Table(II)

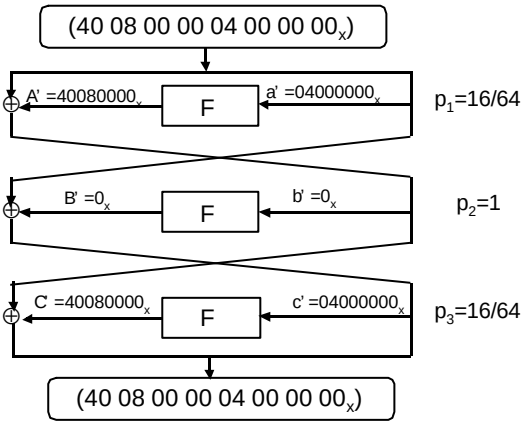
- **S-box in DES**
  - **At the first row (X' =0), Y' =0 for all 64 pairs**
  - **The remaining rows : average= 4, sum 64, range= 0 ~16**
  - **If the value is "0", there are no corresponding X' and Y'**
  - **If the value is "16", it occurs with probabilty 16/64**
  - **Denoted as X' --> Y' with p_1**
  - **Use 0--> 0 with 1 or "16" (higher value) for DC**

Differential Characteristic

- 2-round characteristic in S_1 box ($0C_x$ --> E_x with 14/64)



3-round characteristic



Holding Probability = $p_1\, p_2\, p_3 = 1/16$

Searching Way for round keys

(1) Choose suitable Pt XOR.

(2) Get 2 PTs for chosen pt XOR and obtain the corresponding Ct by encryption

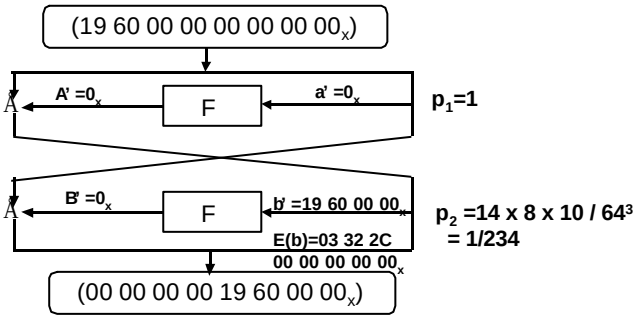
(3) From Pt XOR and pair of Ct, get the expected output XOR for the S-box of final round.

(4)Count the maximum potential key at the final round using the estimated key

(5) right key is subkey of having large number of pairs of expected output XOR

Iterative Characteristic

- **Self concatenating probability**
- **Best iterative char. of DES**



DC of DES_{16}

- 1st round : j --> n
- Till 13 round, use 2-round best iterative characteristics 6.5 times : prob. $=(1/234)^6 \approx 2^{-47.2}$
- Final 2 rounds (2R attack), compute 13 round values from ciphertext in the reverse direction ->no effect to overall prob.
- Total complexity : $(p)^{-1} \approx 2^{47}$

DC of DES per round

Round	# of chosen plaintext		
4	2^4		
6	2^8		
8	2^{18}		2^{14}
10	2^{35}		2^{24}
12	2^{43}	CR90[1]	2^{31}
14	2^{51}	CR92[2]	2^{39}
15	2^{52}		2^{47}
16	2^{58} 2^{61} *		2^{47}

*** Assume independent round key**

1. "Differential Cryptanalysis of DES-like Cryptosustems",Proc. of Crypto90, LNCS537, pp.2-21
2. "Differential Cryptanalysis of the full 16-round DES",Proc. of Crypto' 92, LNCS740,pp.487-496

Additional result of DES by DC

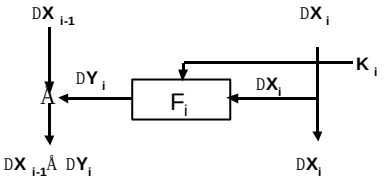
- P Permutation : can' t strengthen DES
- order of S-box : can weaken much or strengthen only up to 2^{48}
- Replacement XORs by addition : can weaken much in some cases
- Modifying S-boxes
  - random : 2^{18} - 2^{20}
  - modifying one entry (i.e.,S(0) ->S(4)) : 2^{33}
  - uniform distribution table : 2^{26}

LC(Linear Cryptanalysis)

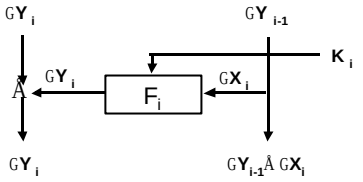
- Introduction
  - Matsui : EC93[1], CR94[2]
  - Known Plaintext Attack
  - O(Breaking DES_{16}) ~ 2^{43}
    - 12 HP W/S, 50-day operation
  - ***Utilize the probabilistic distribution between input linear sum and output liniear sum values Iteratively***
  - Duality to DC : XOR branch vs.three-forked branch
  - Apply to other DES-like cryptosytems

1. M.Matsui,"Linear Cryptanalysis Method for DES Cipher", Proc. Of Eurocrypt' 93,LNCS765, pp.386-397
2. M.Matsui,"The First Experimental Cryptanalysis of the Data Encryption Standard", Proc. Of Crypto' 94,LNCS839, pp.1-11.

XOR branch vs. 3-forked branch



XOR branch after f-ft. i.e.,
DC goes downstream through f-ft.
$\Delta X_i = \Delta X_{i-2} \oplus \Delta Y_{i-1}$ $(3 \le i \le n)$
with $\Pi_{\{i=1\}}^{n} p_i$
DX_i : X_i's Differential value



3-forked branch before f-ft. i.e.,
LC goes upstream through f-ft.
$\Gamma Y_i = \Gamma Y_{i-2} \oplus \Gamma X_{i-1}$ $(3 \le i \le n)$
with $2^{n-1}\Pi_{\{i=1\}}^{n} |p_i - 1/2|$
$G X_{i-1}$: X_{i-1}'s Masking value

Basic principle of LC

(Goal) : Find linear approximation)
$P[i_1,i_2, ..,i_a]$ Å $C[j_1,j_2, ..,j_b]=K[k_1,k_2, ..,k_c]$
with significant prob. p (1 ½)
where, A[i,j, ..,k]=A[i] Å A[j] Å …Å A[k]
(Algorithm)MLE(Maximum Likelihood Estimation)
(Step 1) For given P,C, compute $X=P[i_1,i_2, ..,i_a]$ Å $C[j_1,j_2, ..,j_b]$
(Step 2) if |X=0| >1/2 (# of P),
and if p > 1/2, $K[k_1,k_2, ..,K_c]=0$ else 1.
if |X=0| < 1/2 (# of P)
and if p >1/2 $K[k_1,k_2, ..,k_c]=1$ else 0.

Linear Distribution Table(I)

- **For a S-box S_a,(a=1,2, ..,8) of DES**

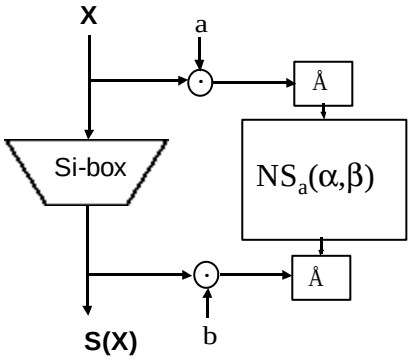
  $NS_a(a, b) = \#\{x \mid 0 \le x < 64, \quad parity(x \cdot a) = parity(S(x) \cdot b)\}$

  $1 \le a \le 63$, $1 \le b \le 15$, $\cdot$: dot product (bitwise AND)

- **Ex) $NS_5(16,15) = 12$**
  - **The 5-th input bit at S5-box is equal to the linear sum of 4 output bits with probability 12/64.**
  - **X[15] Å F(X,K)[7,18,24,29]=K[22] with 0.19**
  - **X[15] Å F(X,K)[7,18,24,29]=K[22] Å 1 with 1-0.19=0.81**

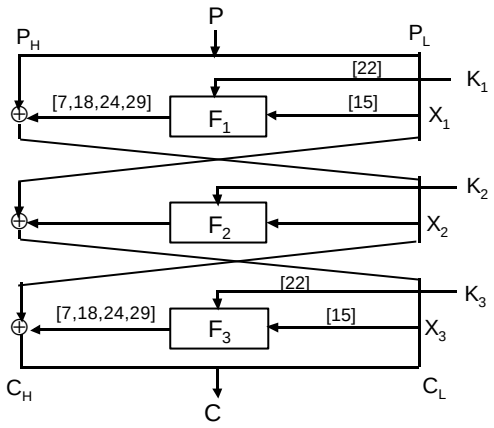
(Note) least significant at the right and index 0 at the least significant bit

Linear Distribution Table(II)



- $NS_a(\alpha,\beta)$ has even values.
- If $\alpha = 1, 32(20_x), 33(21_x)$, $NS_a(\alpha, \beta) = 32$
- $NS_a(\alpha, \beta)$ varies from 0 to 64

3-round DES by LC



$X_2[7,18,24,29] \oplus P_H[7,18,24,29] \oplus P_L[15] = K_1[22]$ ---------- (1)

p_1=12/64

$X_2[7,18,24,29] \oplus C_H[7,18,24,29] \oplus C_L[15] = K_3[22]$ ---------- (2)

p_3=12/64

(1) ⊕ (2) => $X_2[7,18,24,29] \oplus C_H[7,18,24,29] \oplus C_L[15] \oplus X_2[7,18,24,29] \oplus P_H[7,18,24,29] \oplus P_L[15] = K_1[22] \oplus K_3[22]$ holding prob. = $(p_1 * p_3) + (1 - p_1 * p_3)$

* Discard IP and FP like DC

Piling-up lemma in LC

- If independent prob. value, X_i ($1 \le i \le n$) have prob p_i to value 0, prob $(1-p_i)$ to value 1, $p = \{prob(X_1 \oplus X_2 \oplus \ldots \oplus X_n) = 0\}$ is

  $p=2^{n-1} \prod_{i=1}^{n}(p_i - 1/2) + 1/2.$

- The number of known pt for LC with success prob. 97.7% is $|p - 1/2|^{-2}$

LC of DES_{16}

- (Preparation) Use the best iterative linear iteration
- (Search stage)
  - Data Counting : count the effective number of pt and ct and derive key : effective keys (13-bit + 13-bit)
  - Exhaustive Search : the remaining 30 bits of a key

LC of DES

Round	# of Known Plaintext	
8	2^{21}	EC93
12	2^{33}	EC93
16	2^{47}	CR94 2^{43}

Variation of DC/LC

- **Multiple LC : Kaliski & Robshaw [CR94]**
- **Differential-Linear Cryptanalysis : Langford & Hellman [CR94]**
- **Truncated and Higher order DC : Knudsen [FSE95]**
- **Nonlinear Approximation in LC : Knudsen [EC96]**
- **Partitioning Cryptanalysis : Harpes & Massey [FSE97]**
- **Interpolation Attack : Jakobsen & Knudsen [FSE97]**
- **Differential Attack with Impossible Characteristics : Biham [EC99]**

DFA(Differential Fault Attack)

- **DeMillo, Boneh, Lipton (Bellcore), "***On the Importance of Cheking Computations***", 1996**
- **(Assumption) Make an artificial error in algorithm working inside IC**
- **If 200 pairs of Pt and Ct' s are given, succeed to find a key in DES**
- **Highly theoretical attack, however, need attention**