Differential Cryptography

20 November 2019 20:26

Source: https://www.youtube.com/watch?v=xcBqraHhcJU

→ uses the information about the XOR of two inputs and the XOR of corresponding two outputs
→ CPA : not known plaintext attack.

using on: GIFIG Cipher

Input $x : \{0,1\}^{l_m}$, $K_0 : \{0,1\}^{l_m}$

Output $y : \{0,1\}^{l_m}$

by schedule algorithms generates $(k_0, k_1, \ldots K_{N_R})$

Algorithm:

$w^0 = x$

for $r = 1$ to $N_R - 1$:

$u^r = w^{r-1} \wedge K^{r-1}$

For $i = 1$ to m

do $v_i^r = S(u_i^r)$

permutation ← $w^r = v^r_{P(1)}, v^r_{P(2)}, \ldots, v^r_{P(m)}$

plain substitution of $u^{N_R} = v^{N_R-1} \wedge K^{N_R-1}$

for $i = 1$ to m

do $v^{N_R} = S(u_i^{N_R})$

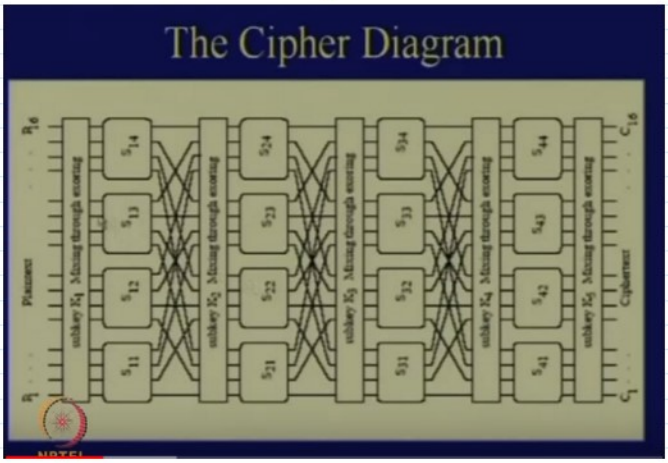
$y = v^{N_R} \wedge K^{N_R}$

Key whitening Step

$N_R - 1$ rounds

last round

for $l = m = N_R = 4$ ∴ PT → 16 bits
→ divided into 4 groups of 4 bits each
→ S box works on each of the 4 bits



Key scheduling

→ key → 32 bits
→ K_r is made by taking 16 successive bits from the key starting at $(4r+1)^{th}$ bit position

Informally:

(1) attacker chooses an input XOR, x'
(2) obtain several tuples : $(x, x^*; y, y^*)$ s.t. $x \wedge x^* = x'$
(3) for each pair of y and y^*, he guesses the key value of last round
(4) decrypts the pair, and checks the XOR at the last but one round
(5) checks the result against most probable outcome
(6) maintains frequency table, for each key noting # of matches
(7) expected that candidate key will have the highest number of matches

for S box : (the real thing)

Let $S : \{0,1\}^m \to \{0,1\}^n$ i.e. $m \times n$ S-box

consider an ordered pair of bit-strings of length m say (x, x^*)

Input : $x \wedge x^*$

Do that for all possible differentials and we get a

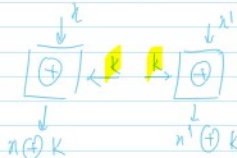
DIFFERENTIAL DISTRIBUTION TABLE

	0	1	2	3	.....	9	A	B	C	...	F
0	16										
1											
2			2					0	0		
			2					0	0		
						0	0	4	0	4	
		0	0	0	0	0					
						0					
F											

Lot of zeros (0)

Entries are denoted by $N_D(\Delta x, \Delta y)$

Thus $N_D(B,2) = 8$



$x \oplus K \quad x' \oplus K$

$x \oplus x'$

∴ keys have no effect on differentials.

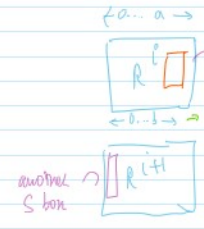
PROPAGATION RATIO

P s.t. input XOR a' gives an output XOR b' pair (a', b') is called differential

$$R_p(a', b') = \frac{N_D(a', b')}{2^m}$$

DIFFERENTIAL TRAIL

→ key have no effect → neglect intermediate keys
→ combine the propagation ratios for which input XOR of differential in any round = output differential of last round differential



$\Delta R^{i-1} = \text{Linear}(\Delta R^{i-1})$

Assumption → hop ratio's are independent
∴ we can just multiply them

Eg: S^1, $R_p(1011, 0010) = 1/2$

S^2, $R_p(0100, 0100) = 3/8$

Let $S: \{0,1\}^m \rightarrow \{0,1\}^n$ i.e. $m \times n$ S-box
consider an ordered pair of bit-strings of length m
say (x, x^*)
Input: $x \wedge x^*$
Output: $y \wedge y^* = S(x) \wedge S(x^*)$

differential set

Define $\Delta(x')$ to be the set of all ordered pairs (x, x^*) s.t. $x \wedge x^* = x'$

formally:

$$\Delta(x') = \{(x, x \oplus x') : x \in (0,1)^m\}$$

elements in set $\rightarrow 2^m$
for each pair in set, # of values within the output XOR can take is 2^n
$\therefore 2^m$ pairs are distributed among 2^n values

this non uniformity WILL BE EXPLOITED (δ)

Eg:

$\Delta(1011) = \{(0000, 1011), (0001, 1010) \cdots (1111, 0100)\}$

x	x^*	y	y^*	y' $(y \wedge y^*)$
		$S(x)$	$S(x^*)$	
0000	1011	1110	1100	0010
⋮	⋮	⋮	⋮	⋮
1111	0100	0111	0010	0101

will have repeated value (δ) and ∴ some values must be missing

frequency table of

0000	0001	0010	.....	0111	.....	1111
0	0	8		2		2

observations:
(1) only 5 out of 16 possible XORs occur
(2) non uniform distribution
had it been uniform all 16 would have occured once
(3) this attacks exploits THIS NON-UNIFORMITY which serve as the DISTINGUISHER

proved that: if $\exists$ DISTINGUISHER $\Rightarrow \exists$ a REAL WORLD ATTACK

Eg: $\Sigma_2^1, R_p(1011, 0010) = 1/2$
$\Sigma_2^2, R_p(0100, 0110) = 3/8$
$\Sigma_2^3, R_p(0010, 0101) = 3/8$
$\Sigma_5^3, R_p(0010, 0101) = 3/8$

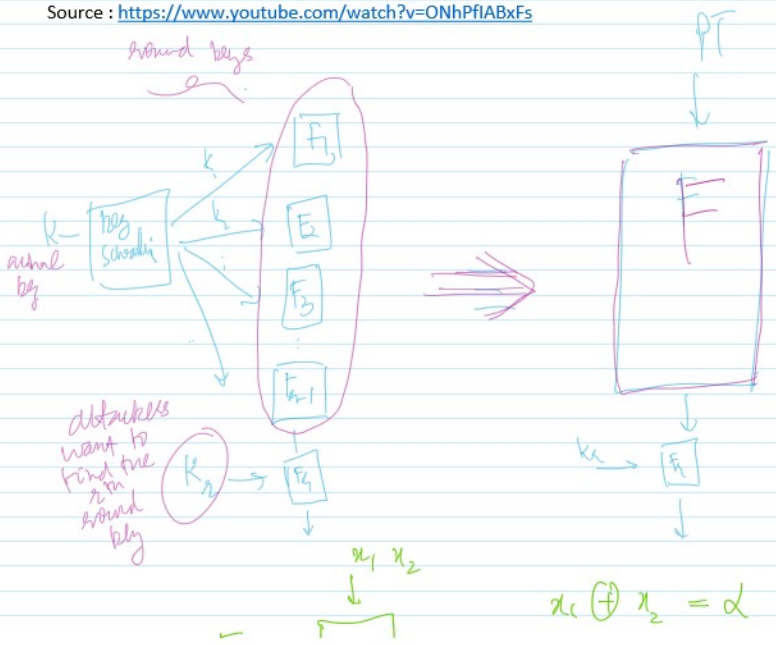
Resultant Hop Ratio is:
$R_p(0000\ 1011\ 0000, \cdots 0000\ 1) = \frac{1}{2} \times \left(\frac{3}{8}\right)^3$

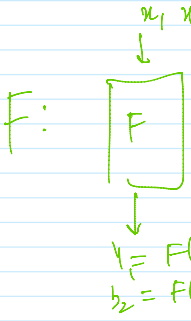
Obtain the differential for $r-1 = 3$ rounds
$(V^3)' = (U^4)'$

The Attack:
Choose Large no of PT say 5000,
obtain corresponding CT.
↓
guess key (note we only need to guess 8 bits of key)
↓
Apply last round & verify whether differential at input of last round S-box is 0000 0110 0000 0110
↓
make frequency table for keys.

IMMUNITY AGAINST DC:
(1) build S-Box with a uniform distribution
(2) # of PT-CT required $\propto \frac{1}{\text{probability of differential}}$

Source : https://www.youtube.com/watch?v=ONhPfIABxFs





$x_1 \oplus x_2 = \alpha$

$x_1 = 1101 \ldots\ldots 01$

$x_2 = 1011 \ldots\ldots 011$

$011 \ldots\ldots$

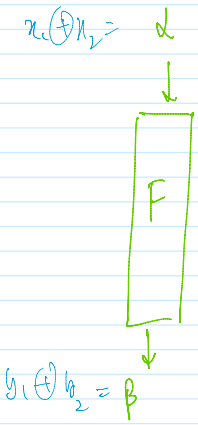
$y_1 \oplus y_2 = \beta$

DIFFERENTIAL TRIAL $\Rightarrow \alpha \to \beta$

if $\exists\ \alpha, \beta$ s.t. probability if we α the output difference will be β is more than 50%.

$\Downarrow$

DA is applicable



suppose such α, β exist then the ATTACK is as FOLLOWS:

Choose $x_1 = x$, $x \in \{0,1\}^l$

$x_2 = x \oplus \alpha$

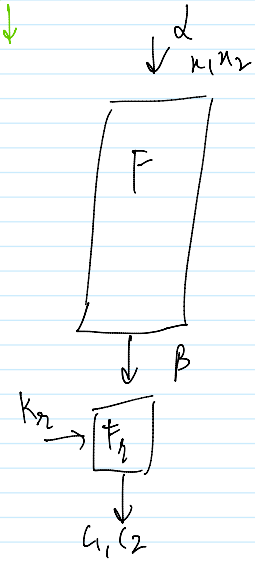
i.e. $x_1 \oplus x_2 = x \oplus (x \oplus \alpha)$

$= \alpha$

we get c_1, c_2 → # Chosen Plaintext Attack

$c_1 = E(x_1)$

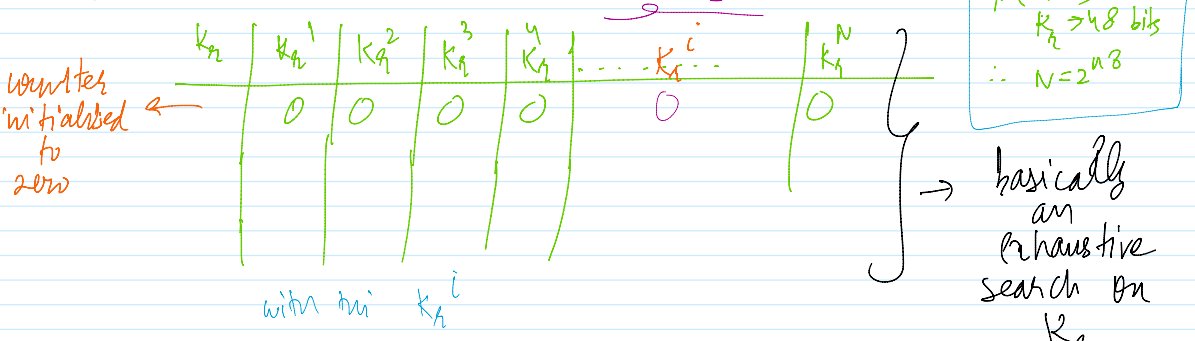
$c_2 = E(x_2)$



how if $y_1 = F(x_1)$

$y_2 = F(x_2)$, then

most probabably: $y_1 \oplus y_2 = \beta$



for DES $K_2 > 48$ bits

$\therefore N = 2^{48}$

→ basically an exhaustive search on K_2

$F_2^{-1}(K_2^i, c_1) = y_1^i$

$F_2^{-1}(K_2^i, c_2) = y_2^i$

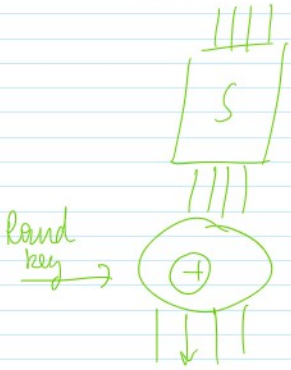
$F_k^{-1}(k_8^i, z) = y_2^i$

we try $y_1^i \oplus y_2^i$ if it $= \beta$, then we increase counter by +1

we do this for all plaintext

then the $k_{r_1}^j$ with MAXIMUM FREQUENCY is MOST PROBABLY THE r^{th} round KEY

how to find such α and β ??

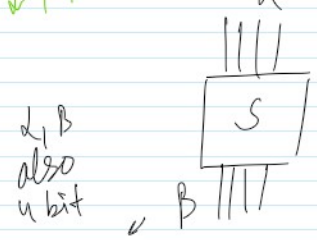


$S: \{0,1\}^4 \to \{0,1\}^4$

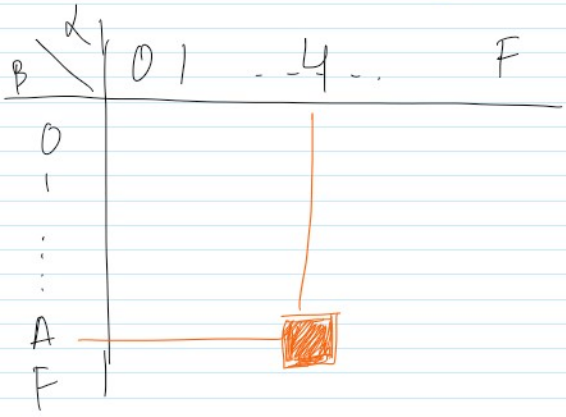
we want to find α, β for this (α, β)

S box : $2^4 \to 16$ entries

0	1	2	.....	9	A	..	F
3	A	F	....	.	.	..	.



α, β also 4 bit



to find:

$x_1 = x \in \{0,1\}^4$ here α is 4

$x_2 = x \oplus \alpha$ s.t. $x_1 \oplus x_2 = \alpha$

compute

$y_1 = F(x_1)$ $y_2 = F(x_2)$

F is here is just S box

for a fixed α

β	0	1	2	.....	B	..	F
counter initialised to zero	0	0	0	0	+1	0	0

counter initialised to zero

0	0	0	0	0	p	p	p	0
					+1			

$y_1 = f(x_1)$ $y_2 = f(x_2)$

f is here is just S box

s.t. $y_1 \oplus y_2 = \beta$ lets assume β here is $\vec{B}$

↓

increment counter

Store back the differential table