Differential Cryptanalysis

Roy Laurens
Information Networking Institute

Introduction

- Difference - the real essence
- Characteristic - chaining the difference

Notations and Definition

- Numbers (n_x), plaintext (P), ciphertext (T)
- The difference ($X' = X_1 \oplus X_2$)
- Inputs and outputs of the F func. ($A,B,\ldots,J$) and ($a, b, \ldots, j$)
- Subkeys (K_i)
- Input and output of the S box
  $Si_{IX} = Si_{Ex} \oplus Si_{Kx}$
  $Si_{ox} = Si(Si_{IX})$

Overview

- Analyzing the differential behaviour of S-box function
- (Known) design rules of S-boxes
  - 1 input bit $\rightarrow$ 2 output
  - S(X) and S(X$\oplus$1100) $\rightarrow$ 2 output
- Difference Distribution Table
  - X $\rightarrow$ Y : X may caused Y
  - X $\rightarrow$ Y : X may not caused Y
- Small example

Characteristic

- Definition : observation of difference pattern between rounds
- Right pair vs. Wrong pair
- A 3-round characteristic example
- Iterative characteristic
- 3R, 2R and 1R-Attacks

Differential Cryptanalysis on DES-4

- Characteristic used
- Subkeys calculation
- Can be extended to 6 and 8 round

Improvement on DES

- Random S-boxes
- Uniform difference S-box
- Modifying P
- Modifying S-box order

Random & Uniform S-boxes

- Flaw : (high probability of) private input bits modification causing zero output XOR
- Characteristic : (1/16)
  $\Omega_P = 60\ 00\ 00\ 00\ 00\ 00\ 00\ 00_x$

Results

- Actual result on DES4 and DES6 : < 1 sec. + 14 bit brute force

Nbr. of Round	Needed pairs	Analyzed pairs	Found bit	Characteristic		S/N		Chosen plains
4	2^{3}	2^{3}	42	1	1	16	[16]	2^{4}
6	2^{7}	2^{7}	30	3	1/16	2^{16}	*	2^{8}
8	2^{15}	2^{13}	30	5	1/10486	15.6	[24]	2^{16}
9	2^{25}	2^{24}	30	6	1/1000000	1.0	[30]	2^{26}
10	2^{34}	4	18	9	$2^{-31.5}$	2^{33}	*	2^{35}
11	2^{35}	2^{11}	48	9	$2^{-31.5}$	2^{21}	*	2^{36}
12	2^{42}	4	18	11	$2^{-39.4}$	2^{25}	*	2^{43}
13	2^{43}	2^{19}	48	11	$2^{-39.4}$	6	[30]	2^{44}
14	2^{50}	4	18	13	$2^{-47.2}$	2^{17}	*	2^{51}
15	2^{51}	2^{27}	48	13	$2^{-47.2}$	4	[42]	2^{52}
16	2^{57}	2^{5}	18	15	$2^{-55.1}$	2^{9}	*	2^{58}

Conclusion

- Generality for Feistel cipher
- Probabilistic result
- Countermeasure : Round increment and less difference