Advanced cryptology

Differential cryptanalysis

prof. Ing. Róbert Lórencz, CSc.

České vysoké učení technické v Praze, Fakulta informačních technologií
Katedra počítačových systémů

Příprava studijních programů Informatika pro novou fakultu ČVUT je spolufinancována Evropským sociálním fondem a rozpočtem Hlavního města Prahy v rámci Operačního programu Praha — adaptabilita (OPPA) projektem CZ.2.17/3.1.00/31952 – „Příprava a zavedení nových studijních programů Informatika na ČVUT v Praze“.
Praha & EU: Investujeme do vaší budoucnosti

Tato přednáška byla rovněž podpořena z prostředků projektu č. 347/2013/B1a Fondu rozvoje vysokých škol Ministerstva školství, mládeže a tělovýchovy

Contents of lectures

- Basic features
- Analysis of the S-box
- Keyed S-box
- The construction of differential characteristics
- Extraction of key bits - experiment

DC - basic properties I

- Differential cryptanalysis (DC) utilizes a high probability of certain occurrences of PT differences and differences in round of last cipher.
- Let us denote inputs $X = [X_1 X_2 \ldots X_n]$ and outputs $Y = [Y_1 Y_2 \ldots Y_n]$ of any cryptosystem. Next, let us have two inputs to the system $X^{'}$ a $X^{''}$ and the corresponding outputs of the system $Y^{'}$ a $Y^{''}$.
- Input differential is defined by: $\triangle X = X^{'} \oplus X^{''} = [\triangle X_1 \triangle X_2 \ldots \triangle X_n]$, where $\triangle X_i = X_i^{'} \oplus X_i^{''}$, and where i represents i-ty bit.
- Similarly $\triangle Y_i = Y_i^{'} \oplus Y_i^{''}$ is the output difference $\triangle Y = Y^{'} \oplus Y^{''} = [\triangle Y_1 \triangle Y_2 \ldots \triangle Y_n]$, where $\triangle Y_i = Y_i^{'} \oplus Y_i^{''}$.

DC - basic properties II

- Ideally, a random cipher is the probability of occurrence of each differences $\triangle Y$ given $\triangle X$ právě $1/2^n$, where n is the number of bits X.
- DC looks for the operation of the of occurrence of individual $\triangle Y$ given different inputs $\triangle X$ with very high probability p_D greater than$1/2^n$.
- Pair of $(\triangle X, \triangle Y)$ we call difference - differential.
- At DC attacker selects a pair of input $X^{'}$ a $X^{''}$, so that individual $\triangle X$ gave the corresponding $\triangle Y$ with high probability.
- In the case of SPN we will try to examine highly probable differential characteristics. The differential characteristics are a sequence of input and output difference in rounds, so that the output from one is input difference of next round.

DC - basic properties III

- Using highly probable differential characteristics allows us to use the information coming into the last rounds of SPN to derive bits of the last subkey layer.
- As with LC, we will first examine the differential characteristics of individual S-boxes with the fact that the identified properties will help us create the overall differential characteristic.

Analysis of S-box

- The outputs of S-box are $X = [X_1 X_2 X_3 X_4]$ and outputs of S-boxes are $Y = [Y_1 Y_2 Y_3 Y_4]$.
- All differential pairs of box $(\triangle X, \triangle Y)$ we will examine and determine with which probability it occurs $\triangle Y$ for given $\triangle X$.
- For each input pairs $(X^{'}, X^{''} = X^{'} \oplus \triangle X)$ we express $\triangle Y$, for which holds $(Y^{'}, Y^{''} = Y^{'} \oplus \triangle Y)$.

DC - basic properties IV

- for example, for $X^{'} = 0110$ and from substitution $Y^{'} = 1011$. For $\triangle X = 1011$ is $X^{''} = X^{'} \oplus \triangle X = 0110 \oplus 1011 = 1101$ and from the substitution then $Y^{''} = 1001$ a $\triangle Y = Y^{'} \oplus Y^{''} = 1011 \oplus 1001 = 0010$

DC

Demonstration of differential pairs of S-box

X	Y	ΔY		
		$\Delta X = 1011$	$\Delta X = 1000$	$\Delta X = 0100$
0000	1110	0010	1101	1100
0001	0100	0010	1110	1011
0010	1101	0111	0101	0110
0011	0001	0010	1011	1001
0100	0010	0101	0111	1100
0101	1111	1111	0110	1011
0110	1011	0010	1011	0110
0111	1000	1101	1111	1001
1000	0011	0010	1101	0110
1001	1010	0111	1110	0011
1010	0110	0010	0101	0110
1011	1100	0010	1011	1011
1100	0101	1101	0111	0110
1101	1001	0010	0110	0011
1110	0000	1111	1011	0110
1111	0111	0101	1111	1011

DC - basic properties 2 I

Analysis of S-box

- $\triangle Y$ for $\triangle X = 1011, 1000, 0100$ is in previous table.
- From the table we see for instance that for $\triangle X = 1011$ occurs 8 values $\triangle Y = 0010$.
- The full expression of the differences for S-box is the following table.
- Ideal S-box should have for all pairs $(\triangle X, \triangle Y)$ value 1, i.e. only one occurrence (probability $1/2^4 = 1/16$).
- Sum occurrence in rows and columns is equal to 16!

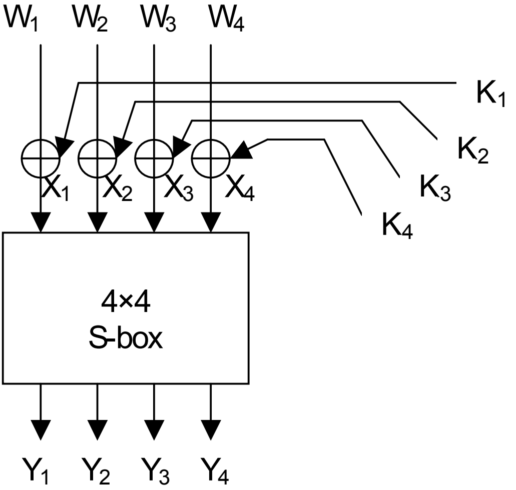
DC

Differential distribution table

		Output Difference															
		0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
Input Difference	0	16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	1	0	0	0	2	0	0	0	2	0	2	4	0	4	2	0	0
	2	0	0	0	2	0	6	2	2	0	2	0	0	0	0	2	0
	3	0	0	2	0	2	0	0	0	0	4	2	0	2	0	0	4
	4	0	0	0	2	0	0	6	0	0	2	0	4	2	0	0	0
	5	0	4	0	0	0	2	2	0	0	0	4	0	2	0	0	2
	6	0	0	0	4	0	4	0	0	0	0	0	0	2	2	2	2
	7	0	0	2	2	2	0	2	0	0	2	2	0	0	0	0	4
	8	0	0	0	0	0	0	2	2	0	0	0	4	0	4	2	2
	9	0	2	0	0	2	0	0	4	2	0	2	2	2	0	0	0
	A	0	2	2	0	0	0	0	0	6	0	0	2	0	0	4	0
	B	0	0	8	0	0	2	0	2	0	0	0	0	0	2	0	2
	C	0	2	0	0	2	2	2	0	0	0	0	2	0	6	0	0
	D	0	4	0	0	0	0	0	4	2	0	2	0	2	0	2	0
	E	0	0	2	4	2	0	0	0	6	0	0	0	0	0	2	0
	F	0	2	0	0	6	0	0	0	0	4	0	2	0	0	2	0

DC

Keyed S-box



DC - keyed S-box I

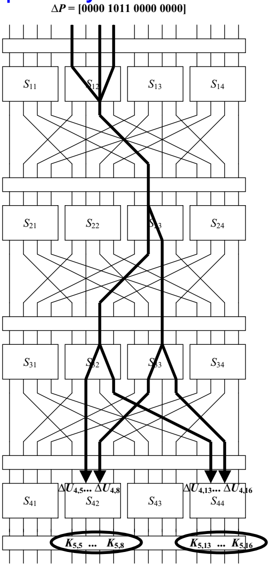
- The key is applied to each input in round and at the end of 4th round. Let $\triangle W = [W_1^{'} \oplus W_1^{''}, W_2^{'} \oplus W_2^{''}, \ldots, W_n^{'} \oplus W_n^{''}]$ is a difference of input to the S-box. Then

$$\triangle W_i = W_i^{'} \oplus W_i^{''} = (X_i^{'} \oplus K_i) \oplus (X_i^{''} \oplus K_i) = X_i^{'} \oplus X_i^{''} = \triangle X_i$$

- Key bits have no impact on the input differentiated value and can be ignored.
- keyed S-box has the same the differential distribution table as not keyed S-box.

DC

Example of differential cryptanalysis



DC - construction of differential characteristics I

Example

- Based on description of differential characteristics of an S-box in SPN we can create differential characteristic of whole cipher by mutual connecting of S-boxes in individual rounds.
- In following example is created differential characteristic, which involves S-boxes S_{12}, S_{23}, S_{32} and S_{33}.
- On a picture of differential characteristic of SPN (previous slide) is shown a creation of differential characteristic of SPN.
- Diagram illustrates influence of nonzero bit differences in connection network with S-boxes.
- Bold is a route through S-boxes, which are active and has a nonzero difference.
- Differential characteristic is executed over first 3. rounds. Last round serves for incorporation of last subkey and thus also its reveal.

DC - construction of differential characteristics II

- We are going to use following difference pairs of S-boxes:
  - $S_{12} : \triangle X = B \rightarrow \triangle Y = 2$ with probability $8/16$
  - $S_{23} : \triangle X = 4 \rightarrow \triangle Y = 6$ with probability $6/16$
  - $S_{32} : \triangle X = 2 \rightarrow \triangle Y = 5$ with probability $6/16$
  - $S_{33} : \triangle X = 2 \rightarrow \triangle Y = 5$ with probability $6/16$
- All other S-boxes has zero input differences and thus also zero output differences.
- Input of a differences into cipher is an input into 1st round

$$\triangle P = \triangle U_1 = [0000\ 1011\ 0000\ 0000]$$

- Output from first S-boxes is

$$\triangle V_1 = [0000\ 0010\ 0000\ 0000]$$

DC - construction of differential characteristics III

- and after permutation in 1st round we got input into 2nd round

$$\triangle U_2 = [0000\ 0000\ 0100\ 0000]$$

- Output from 1st round is given with probability $8/16 = 1/2$ if given difference $\triangle P$ PT.
- Output from 2nd S-boxes (active S_{23}) is

$$\triangle V_2 = [0000\ 0000\ 0110\ 0000]$$

and after permutation the input into 3rd round we have

$$\triangle U_1 = [0000\ 0010\ 0010\ 0000]$$

with probability $6/16$ given by $\triangle U_2$ and probability $8/16 \times 6/16 = 3/16$ given by $\triangle P$ PT.

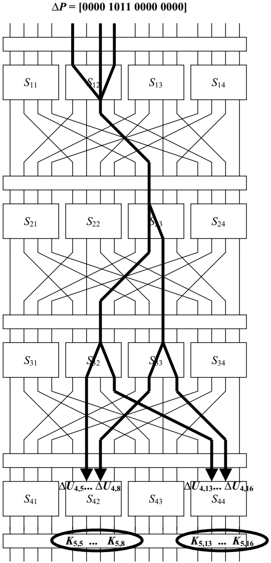
DC - construction of differential characteristics IV

- While we assume, that differential of 1st and 2nd round are independent, then complete probability is a product of both probabilities.
- For S-boxes S_{32} and S_{33} permutation in 3rd round we got

  $$\triangle V_3 = [0000\,0101\,0101\,0000] \text{ and } \triangle U_4 = [0000\,0110\,0000\,0110]$$

  with probability $(6/16)^2$ given by $\triangle U_3$ and then for probability $8/16 \times 6/16 \times (6/16)^2 = 27/1024$ given difference $\triangle P$ where again we assume independence between individual S-boxes in all rounds.
- In cryptanalysis process be assume couples of PT (and their CT) such, that $\triangle P = [0000\ 1011\ 0000\ 0000]$. Occurrence of these couples is $27/1024$ likely.
- Such couples we call true couples and couples, which does not comply with this condition we are going to call false couples.

Example of differential characteristic



DC - Extraction of key bits I

- In case of differential characteristic existence for $R-1$ rounds of SPN cipher, we can execute cipher cryptanalysis with a goal of extracting some subkey bits K_5.
- This process requires partial decryption of CT xored with subkey K_5 from couple PT/CT.
- Values of differentials $\triangle U_{4,5} \dots \triangle U_{4,8}$ and $\triangle U_{4,13} \dots \triangle U_{4,16}$ given by differential characteristic from values $\triangle P$ we compare trues couples of PT with differences of values gained by partial decryption of CT values (corresponding with true couples of PT) and xor of chosen bits K_5.
- This comparison we are doing for each true couple of PT (and their CP) woth all possible values of 8 bits of subkey K_5 $(256 hodnot)$ - $K_{5,5} \dots K_{5,8}$ and $K_{5,13} \dots K_{5,16}$.
- If the match occur, then we increment the counter for given combination of subkey bites.

Experimental results of DC

partial subkey $[K_{5,5}...K_{5,8}, K_{5,13}...K_{5,16}]$	prob	*partial subkey* $[K_{5,5}...K_{5,8}, K_{5,13}...K_{5,16}]$	prob
1 C	0.0000	2 A	0.0032
1 D	0.0000	2 B	0.0022
1 E	0.0000	2 C	0.0000
1 F	0.0000	2 D	0.0000
2 0	0.0000	2 E	0.0000
2 1	0.0136	2 F	0.0000
2 2	0.0068	3 0	0.0004
2 3	0.0068	3 1	0.0000
2 4	**0.0244**	3 2	0.0004
2 5	0.0000	3 3	0.0004
2 6	0.0068	3 4	0.0000
2 7	0.0068	3 5	0.0004
2 8	0.0030	3 6	0.0000
2 9	0.0024	3 7	0.0008

DC - extraction of subkey bites - experiment I

- In table on previous slide is a table with some values of subkey values, with probability of a "match"in experiment with 5000 true couples.
- Probability is calculated from: $prob = count/5000$.
- From table it is obvious, that subkey hex 24 has the biggest probability of a match (0,0244) close to theoretical stated value 27/1024 = 0,0264.