Pokročilá kryptologie

Diferenciální kryptoanalýza

prof. Ing. Róbert Lórencz, CSc.

České vysoké učení technické v Praze, Fakulta informačních technologií
Katedra informační bezpečnosti

Obsah přednášky

- Základní vlastnosti
- Analýza S-boxu
- Klíčovaný S-box
- Konstrukce diferenční charakteristiky
- Extrakce bitů klíče - experiment

DK - základní vlastnosti I

- Diferenciální kryptoanalýza (DK) využívá vysokou pravděpodobnost určitých výskytů rozdílů OT a rozdílů v poslední rundě šifry.
- Označme vstupy $X = [X_1 X_2 \ldots X_n]$ a výstupy $Y = [Y_1 Y_2 \ldots Y_n]$ nějakého kryptosystému. Dále mějme dva vstupy do sytému X' a X'' a odpovídající výstupy ze systému Y' a Y''.
- Vstupní rozdíl je definován: $\triangle X = X' \oplus X'' = [\triangle X_1 \triangle X_2 \ldots \triangle X_n]$, kde $\triangle X_i = X_i' \oplus X_i''$, kde i reprezentuje i-ty bit.
- Podobně $\triangle Y_i = Y_i' \oplus Y_i''$ je výstupní rozdíl $\triangle Y = Y' \oplus Y'' = [\triangle Y_1 \triangle Y_2 \ldots \triangle Y_n]$, kde $\triangle Y_i = Y_i' \oplus Y_i''$.
- V ideálním případě náhodné šifry je pravděpodobnost výskytu jednotlivých rozdílů $\triangle Y$ daných $\triangle X$ právě $1/2^n$, kde n je počet bitů X.

DK - základní vlastnosti II

- DK hledá využití možnosti výskytu jednotlivých $\triangle Y$ daných jednotlivými vstupy $\triangle X$ s velmi vysokou pravděpodobnosti p_D větší než $1/2^n$.
- Dvojici $(\triangle X, \triangle Y)$ nazýváme rozdíl - diferenciál.
- Při DK útočník vybírá dvojice vstupu X' a X'', tak aby jednotlivé $\triangle X$ dávali příslušné $\triangle Y$ s vysokou pravděpodobnosti.
- V případě SPN budeme se snažit zkoumat vysoce pravděpodobné diferenciální charakteristiky. Diferenciální charakteristiky jsou sekvence vstupních a výstupních diferencí v rundách, tak, že výstupní diference z jedné rundy je vstupní diferencí další rundy.
- Užitím vysoce pravděpodobných diferenciálních charakteristik nám umožňuje využít informaci přicházející do poslední rundy SPN k odvození bitů poslední vrstvy podklíče.

DK - základní vlastnosti III

- Stejně jako u LK budeme nejdříve zkoumat diferenciální charakteristiky jednotlivých S-boxů s tím, že zjištěné vlastnosti nám pomůže vytvořit celkovou diferenciální charakteristiku.

Analýza S-boxu

- Vstupy S-boxu jsou $X = [X_1 X_2 X_3 X_4]$ a výstupy S-boxu jsou $Y = [Y_1 Y_2 Y_3 Y_4]$.
- Všechny diferenční dvojice S-boxu $(\triangle X, \triangle Y)$ budeme zkoumat a určíme s jakou pravděpodobnosti se vyskytuje $\triangle Y$ pro dané $\triangle X$.
- Pro každou vstupní dvojici $(X', X'' = X' \oplus \triangle X)$ vyjádříme $\triangle Y$, pro které platí $(Y', Y'' = Y' \oplus \triangle Y)$.
- Například pro $X' = 0110$ a ze substituce $Y' = 1011$. Pro $\triangle X = 1011$ je $X'' = X' \oplus \triangle X = 0110 \oplus 1011 = 1101$ a ze substituce potom $Y'' = 1001$ a $\triangle Y = Y' \oplus Y'' = 1011 \oplus 1001 = 0010$

Ukázka diferenčních párů S-boxu

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

DK - základní vlastnosti 2 I

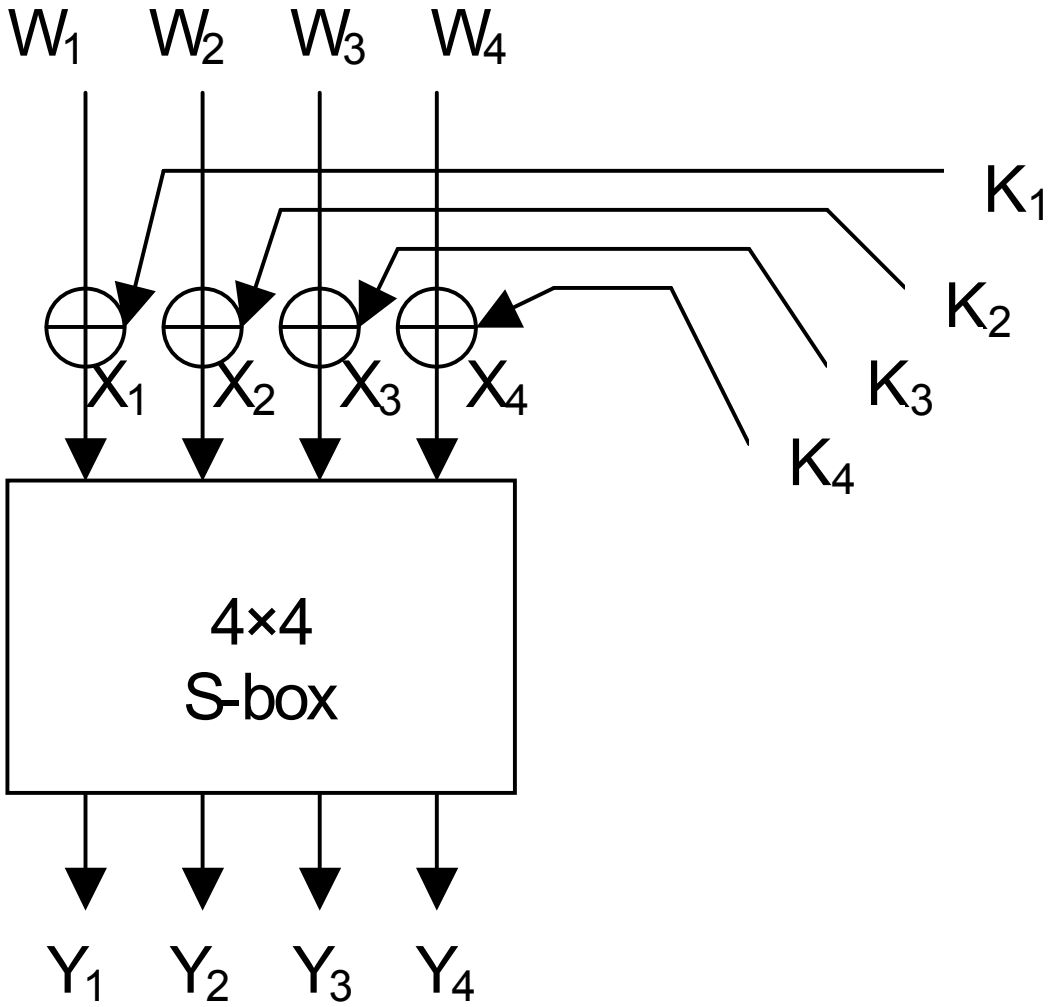
Analýza S-boxu

- $\triangle Y$ pro $\triangle X = 1011, 1000, 0100$ je v předchozí tabulce.
- Z tabulky vidíme například, že pro $\triangle X = 1011$ se vyskytuje 8 hodnot $\triangle Y = 0010$.
- Úplná vyjádření distribuce diferencí pro S-box je následující tabulce.
- Ideální S-box by měl mít pro všechny páry $(\triangle X, \triangle Y)$ hodnotu 1, tj. jediný výskyt (pravděpodobnost $1/2^4 = 1/16$).
- Suma výskytu v řádcích a sloupcích se rovná 16!

Diferenční distribuční tabulka

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

Klíčovaný S-box



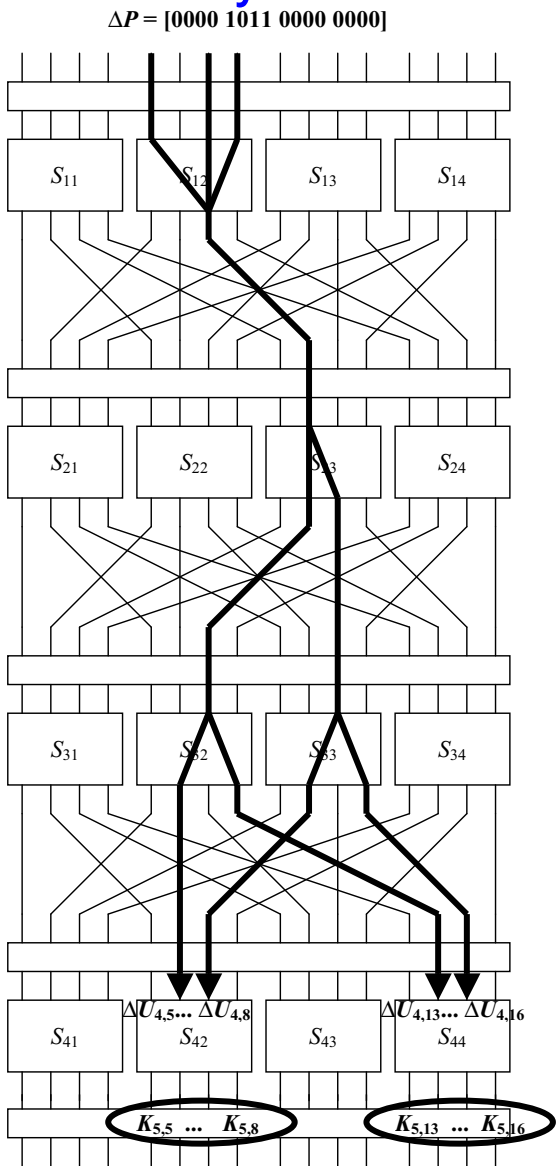
DK - klíčovaný S-box I

- Klíč je aplikovan na každý vstup v rundě a nakonci 4. rundě. Nechť $\triangle W = [W_1' \oplus W_1'', W_2' \oplus W_2'', \ldots, W_n' \oplus W_n'']$ je diference vstupu do S-boxu. Potom

$$\triangle W_i = W_i' \oplus W_i'' = (X_i' \oplus K_i) \oplus (X_i'' \oplus K_i) = X_i' \oplus X_i'' = \triangle X_i$$

- Bity klíče nemají žádny impakt na vstupní diferencovanú hodnotu a můžou být ignorovány.
- Klíčovaný S-box má stejné diferenční distribuční tabulku jako neklíčovaný S-box.

Ukázka diferenciální charakteristiky



DK - konstrukce diferenční charakteristiky I

Příklad

- Na základě popisu diferenciálních charakteristik S-boxu v SPN můžeme vytvořit diferenciální charakteristiku celé šifry vzájemným propojením S-boxů v jednotlivých rundách.
- V následujícím příkladu je vytvořena diferenciální charakteristika, která zahrnuje S-boxy S_{12}, S_{23}, S_{32} a S_{33}.
- Na obrázku diferenciální charakteristiky SPN (předchozí slide) je znázorněná tvorba diferenciální charakteristiky SPN.
- Diagram ilustruje vliv nenulových diferencí bitů v propojovací sítí s S-boxy.
- Tlustě je vyznačená cesta S-boxy, které jsou aktivní a mají nenulový rozdíl.
- Diferenciální charakteristika je prováděná přes první 3. rundy. Poslední runda slouží pro zapracovaní posledního podklíče a tím i jeho odhalení.

DK - konstrukce diferenční charakteristiky II

- Použijeme následující diferenční páry S-boxů:
  - $S_{12} : \triangle X = B \rightarrow \triangle Y = 2$ s pravděpodobností $8/16$
  - $S_{23} : \triangle X = 4 \rightarrow \triangle Y = 6$ s pravděpodobností $6/16$
  - $S_{32} : \triangle X = 2 \rightarrow \triangle Y = 5$ s pravděpodobností $6/16$
  - $S_{33} : \triangle X = 2 \rightarrow \triangle Y = 5$ s pravděpodobností $6/16$
- Všechny ostatní S-boxy mají nulové vstupní diference a tím i nulové výstupní diference.
- Vstup diferenci do šifry je vstupem do 1. rundy

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

- Výstup z prvních S-boxů je

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

DK - konstrukce diferenční charakteristiky III

- a po permutaci v 1. rundě dostáváme vstup do 2. rundy

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

- Výstup s 1. rundy je dán s pravděpodobnosti $8/16 = 1/2$ dané diference $\triangle P$ OT.
- Výstup s 2. S-boxů (aktivní S_{23}) je

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

a po permutace vstup do 3, rundy máme

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

s pravděpodobnosti $6/16$ dané $\triangle U_2$ a pravděpodobnosti $8/16 \times 6/16 = 3/16$ danou $\triangle P$ OT.

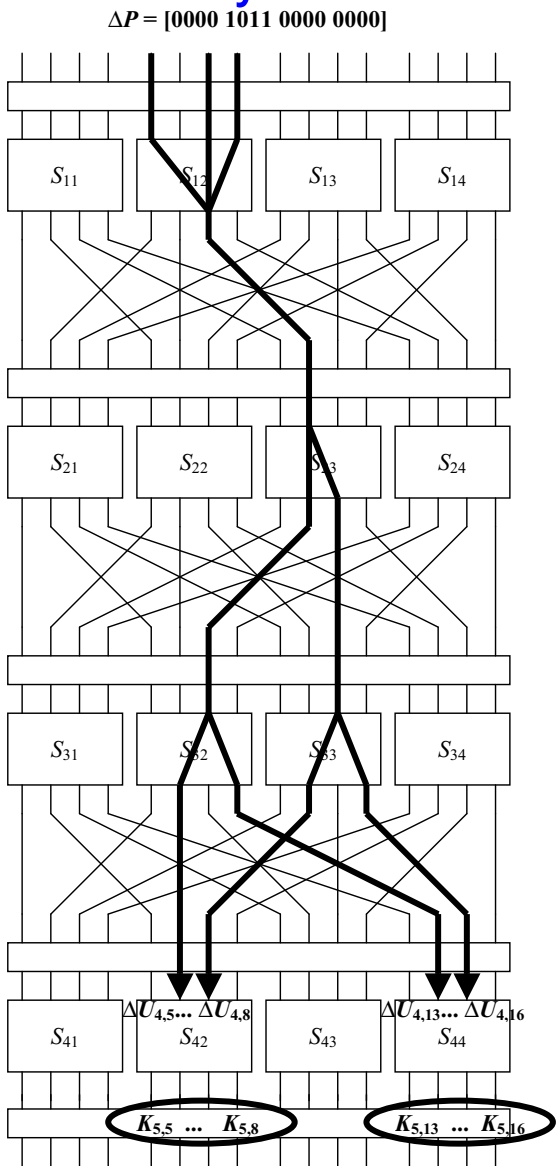
DK - konstrukce diferenční charakteristiky IV

- Předpokládáme přitom, že diferenciál 1. a 2. rundy jsou nezávislé, potom celková pravděpodobnost je součin obou pravděpodobnosti.
- Pro S-boxy S_{32} a S_{33} permutaci v 3. rundě dostáváme

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

  s pravděpodobnosti $(6/16)^2$ danou $\triangle U_3$ a potom pro pravděpodobnost $8/16 \times 6/16 \times (6/16)^2 = 27/1024$ danou diferenci $\triangle P$ a kde opět předpokládáme nezávislost mezi jednotlivými S-boxy ve všech rundách.
- V procesu kryptoanalýzy budeme uvažovat dvojice OT (a jejich ŠT) takových, kterých $\triangle P = [0000\ 1011\ 0000\ 0000]$. Výskyt takových dvojic je $27/1024$ pravděpodobný.
- Takové dvojice budeme nazývat pravé dvojice a dvojice, které nevyhovuji této podmínce budeme nazývat nepravé dvojice.

Ukázka diferenciální charakteristiky



DK - extrakce bitů klíče I

- V případě existence diferenciální charakteristiky pro $R-1$ rund šifry SPN můžeme provést kryptoanalýzu šifry s cílem extrahovat některé bity podklíče K_5.
- Tento proces vyžaduje částečnou dešifraci ŠT xorovaného s podklíčem K_5 z dvojice OT/ŠT.
- Hodnoty diferenciálů $\triangle U_{4,5} \ldots \triangle U_{4,8}$ a $\triangle U_{4,13} \ldots \triangle U_{4,16}$ daných diferenční charakteristikou z hodnot $\triangle P$ pravých dvojic OT porovnáváme s diferencemi hodnot získaných částečnou dešifraci hodnot ŠT (příslušných k pravým dvojicím OT) a xoru vybraných bitů K_5.
- Toto srovnávaní děláme pro každou pravou dvojici OT (a jejich ŠT) se všemi možnými hodnotami 8 bitů podklíče K_5 ($256 hodnot$) - $K_{5,5} \ldots K_{5,8}$ a $K_{5,13} \ldots K_{5,16}$.
- Pokud nastane shoda, potom inkrementujeme čítač pro danou kombinaci bitů podklíče.

Experimentální výsledky DK

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

DK - extrakce bitů klíče - experiment I

- V tabulce na předchozím slide je tabulka s některými hodnotami podklíče s pravděpodobnosti "shody"v experimentu s 5000 pravými dvojicemi.
- Pravděpodobnost je vypočtena z: $prob = count/5000$.
- Z tabulky je zřejmé, že podklíč hex 24 má největší pravděpodobnost shod (0,0244) blízkou teoretické stanovené hodnoty 27/1024 = 0,0264.