Návrh a kryptoanalýza šifier - Zadanie 6

Peter Čuřík

31. októbra 2021

1 Diferenciálna kryptoanalýza

Diferenciálna kryptoanalýza bola vykonaná na SP sieti zo zadania číslo 4, s použitím nasledovnej S-box tabuľky (v hexadecimálnom formáte):

vstup	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
výstup	8	C	B	3	7	9	1	4	E	6	0	D	2	F	5	A

1.1 Tabuľka diferenciálnych pravdepodobností

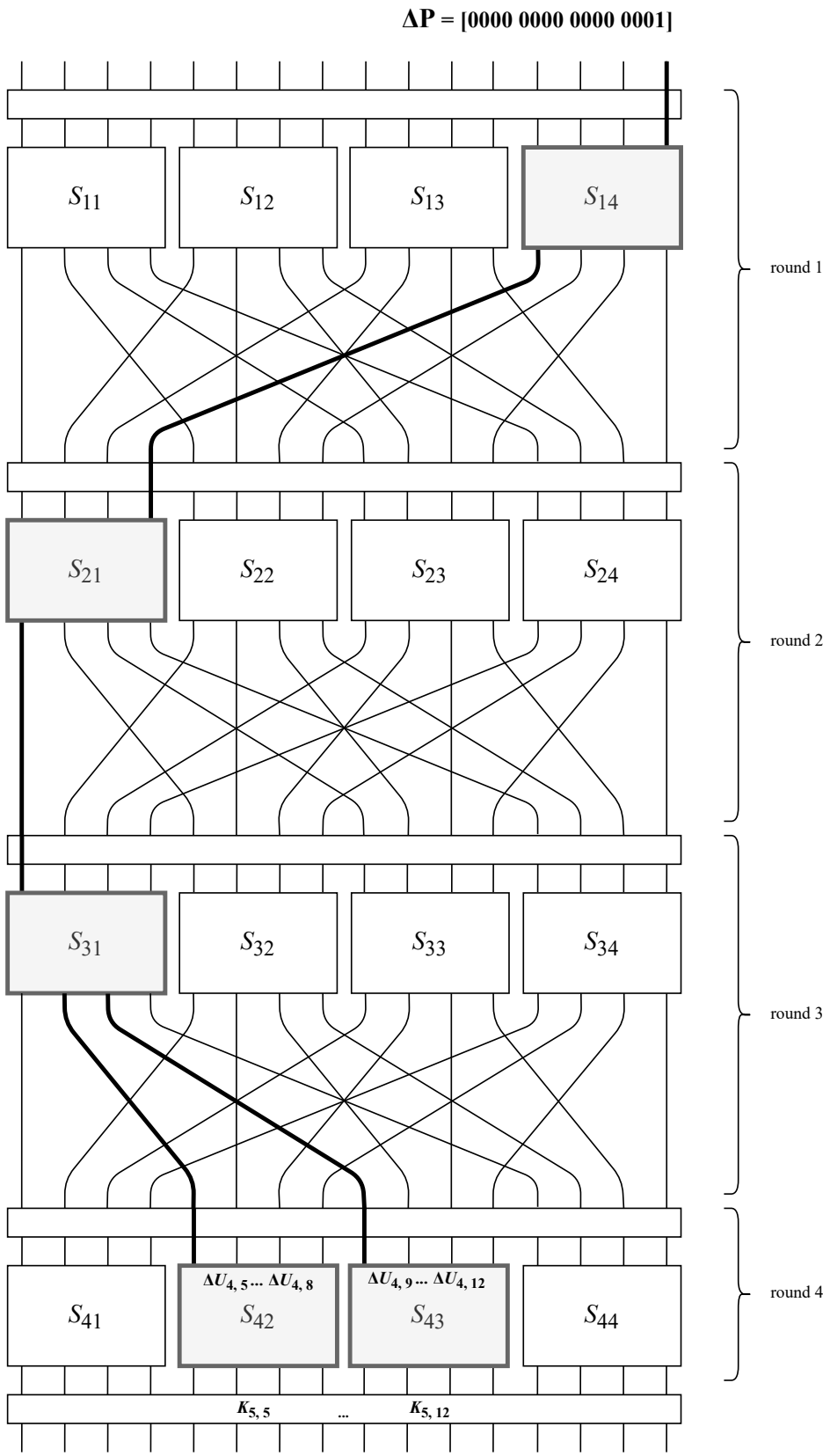
	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**A**	**B**	**C**	**D**	**E**	**F**
0	16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	0	0	0	2	2	0	0	4	0	0	0	0	4	2	2
2	0	0	0	2	0	2	2	2	0	0	0	2	0	2	2	2
3	0	0	0	4	0	0	2	2	4	0	2	2	0	0	0	0
4	0	0	0	0	0	4	0	4	0	2	2	0	2	0	0	2
5	0	4	2	0	2	0	0	0	2	0	2	2	0	0	0	2
6	0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

Tabuľka 1: Tabuľka diferenciálnych pravdepodobností.

1.2 Voľba diferenciálnej trajektórie

Podľa Tabuľky 1 sme hľadali také kombinácie vstupných diferencií ΔX a výstupných diferencií ΔY jednotlivých S-boxov, aby sme dosiahli výhodné pravdepodobnosti a v poslednom kole skončili v práve dvoch S-boxoch. Zároveň hľadáme cestu v SP sieti s minimálnym počtom aktívnych S-boxov, pre maximálnu možnú diferenciálnu pravdepodobnosť P. Výber trajektórie možno vidieť na obrázku nižšie. Bity označujeme zľava doprava číslami 1...16, kde most significant bit (MSB) je vľavo a least significant bit (LSB) vpravo. Využívame nasledovné páry diferencií S-boxov:

$$
\begin{aligned}
S_{14} &: \Delta X = \mathrm{B} \rightarrow \Delta Y = 2, \qquad \text{s pravdepodobnosťou } 4/16 \\
S_{21} &: \Delta X = \mathrm{B} \rightarrow \Delta Y = 2, \qquad \text{s pravdepodobnosťou } 4/16 \\
S_{31} &: \Delta X = \mathrm{B} \rightarrow \Delta Y = 2, \qquad \text{s pravdepodobnosťou } 4/16
\end{aligned}
$$



Obr. 1: Diferenciálna trajektória v SPN.

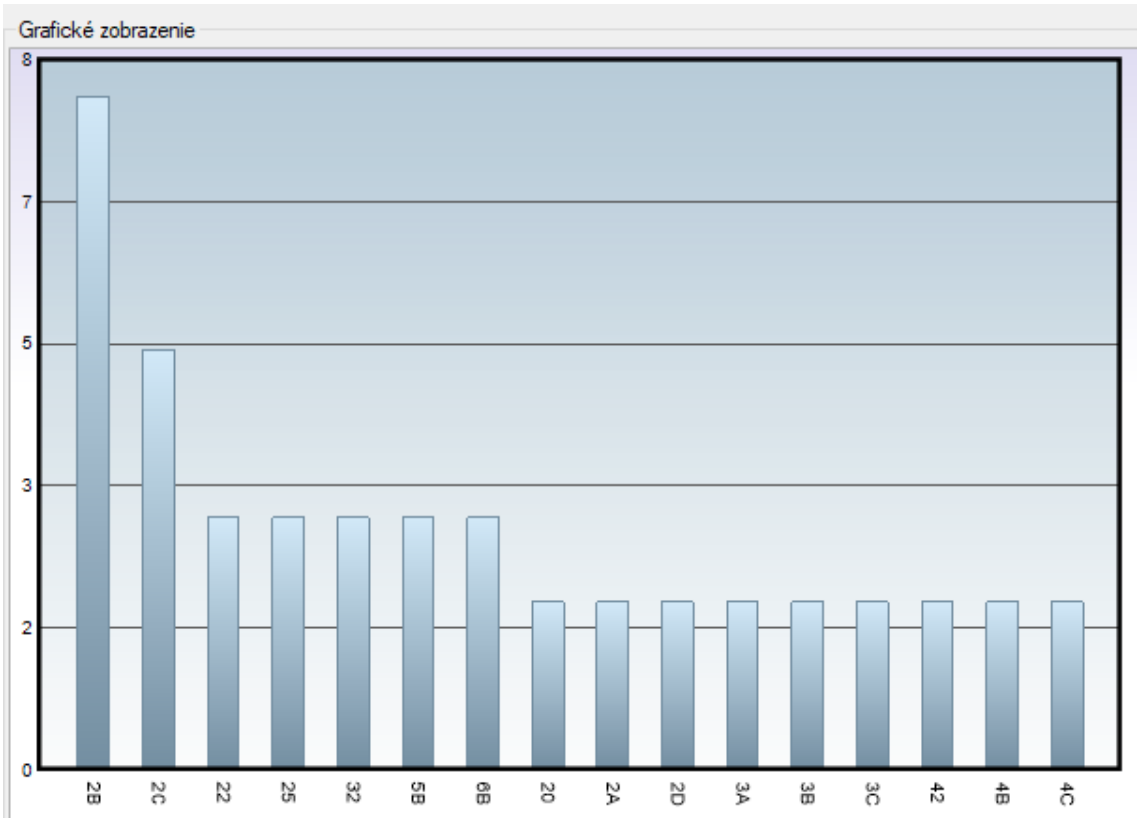
Výsledná diferenciálna pravdepodobnosť bude: $(4/16)^3$. Teda $P = 1/64$.

2 Implementácia

Na konštrukciu tabuľky, prevedenie útoku a generovanie výsledkov bol použitý software dostupný z Moodlu. Ide o .NET PC aplikáciu implementujúcu diferenciálnu kryptoanalýzu.

3 Výsledky

Najpravdepodobnejších adeptov na správny kľúč sme vyniesli do 2D grafu (obrázok nižšie). Na y osi je počet nameraných výskytov hľadanej diferencie. Na x osi je 16 rôznych 8 bitových častí posledného kolového kľúča s najväčším počtom nameraných výskytov hľadanej diferencie zo všetkých 256tich.



Obr. 2: Výsledky útoku na SPN.

4 Záver

Na prevedenie útoku bol zvolený kľúč 0x12BC. Keďže sledujeme S-boxy S_{42} a S_{43}, správna 8 bitová časť kľúča pre tento útok je 0x2B. Táto hodnota je zároveň v grafe na prvom mieste, s najväčším počtom zhôd diferencií. Útok považujeme za úspešný, pretože sme z neho získali rozlišovač tejto šifry.