Návrh a kryptoanalýza šifier - Zadanie 5

Peter Čuřík

24. októbra 2021

1 Lineárna kryptoanalýza

Lineárna 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 lineárnych aproximácií

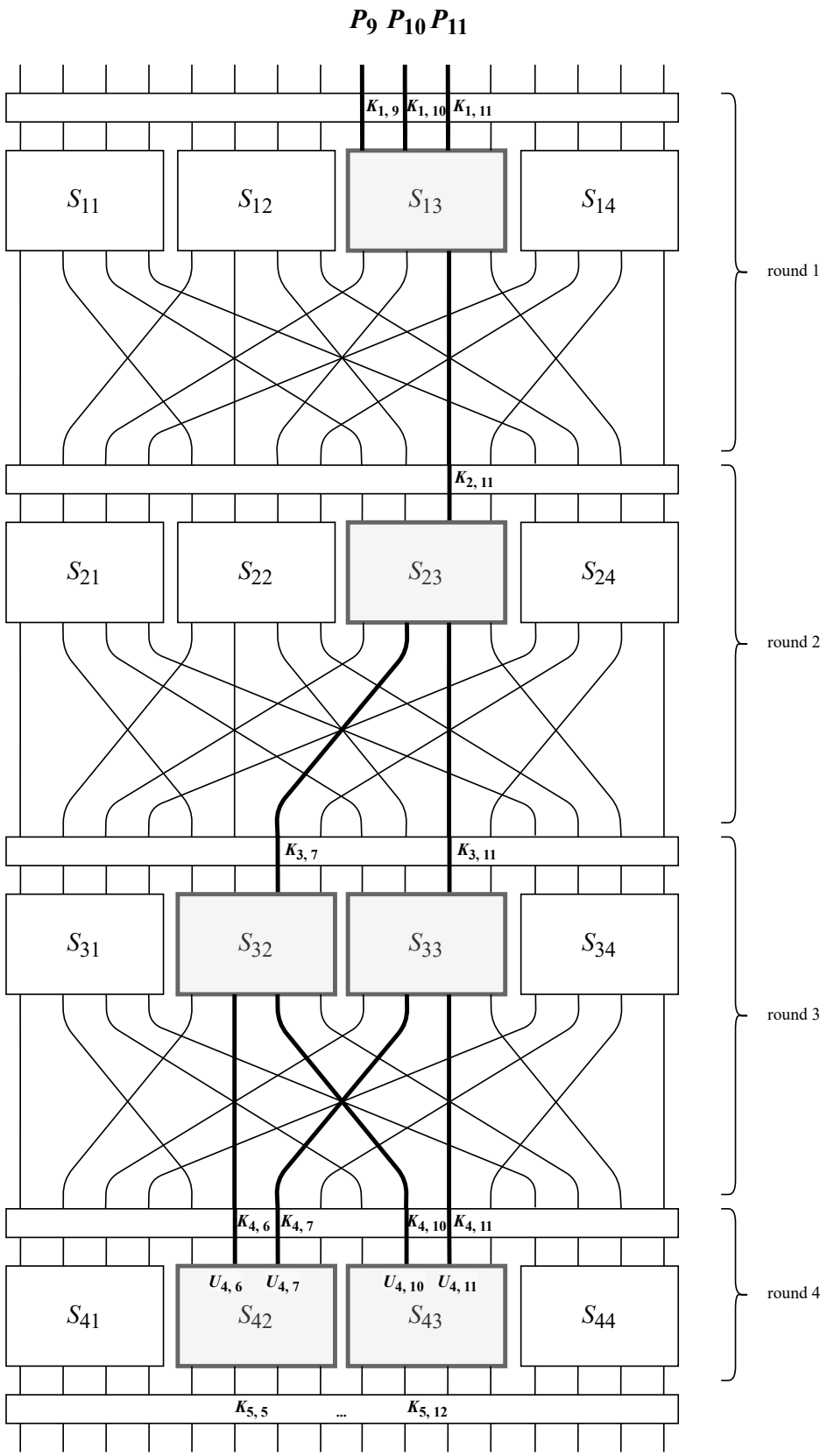
Tabuľka vznikla aplikovaním všetkých možných masiek pre vstupy aj výstupy S-boxu. Vybraté bity boli v každom riadku zoXORované, výsledky jednotlivých výpočtov boli zapísané pre ďalšie kroky. Od počtu prípadov, kedy bol výsledok rovný nule bol zakaždým odpočítaný ideálny stav (práve 8 výsledkov rovných nule). Výsledok tohto odčítania reprezentujú jednotlivé bunky tabuľky.

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

Tabuľka 1: Tabuľka lineárnych aproximácií.

1.2 Voľba lineárnej trajektórie

Podľa Tabuľky 1 sme hľadali také lineárne kombinácie vstupov a výstupov jednotlivých S-boxov, aby sme dosiahli výhodný bias a v poslednom kole skončili v práve dvoch S-boxoch. 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. Pri jednotlivých S-boxoch označujeme vstupné bity $X_1...X_4$ a výstupné bity $Y_1...Y_4$ s označením MSB a LSB rovnakým spôsobom. Využívame nasledovné aproximácie S-boxov:



Obr. 1: Lineárna trajektória v SPN.

$$
\begin{array}{ll}
S_{13} : X_1 \oplus X_2 \oplus X_3 = Y_3, & \text{s pravdepodobnosťou } 12/16,\ \varepsilon : 1/4 \\
S_{23} : X_3 = Y_2 \oplus Y_3, & \text{s pravdepodobnosťou } 12/16,\ \varepsilon : 1/4 \\
S_{32} : X_3 = Y_2 \oplus Y_3, & \text{s pravdepodobnosťou } 12/16,\ \varepsilon : 1/4 \\
S_{33} : X_3 = Y_2 \oplus Y_3, & \text{s pravdepodobnosťou } 12/16,\ \varepsilon : 1/4
\end{array}
$$

Výslednú lineárnu aproximáciu možno zapísať ako:

$$U_{4,6} \oplus U_{4,7} \oplus U_{4,10} \oplus U_{4,11} \oplus P_9 \oplus P_{10} \oplus P_{11} \oplus \Sigma_K = 0$$

kde

$$\Sigma_K = K_{1,9} \oplus K_{1,10} \oplus K_{1,11} \oplus K_{2,11} \oplus K_{3,7} \oplus K_{3,11} \oplus K_{4,6} \oplus K_{4,7} \oplus K_{4,10} \oplus K_{4,11}$$

a Σ_K je zafixované na 0 alebo 1. Podľa Piling-Up lemy určíme finálne ε pomocou určenia pravdepodobnosti rovnice vyššie:

$$1/2 + 2^3 * (1/4)^4 = 1/2 + 1/32 = 17/32$$

teda, $\varepsilon = 1/32$.

1.3 Útok

Na prevedenie útoku je nutných úmerne veľa testovacích P/C párov N. Platí, že $N = c * \varepsilon^{-2}$, kde c je konštanta, ktorú stanovíme na hodnotu 8. Potom je nutných 2^{13} párov na prevedenie útoku.

2 Implementácia

2.1 Generovanie tabuľky lineárnych aproximácií

Vlastné riešenie v jazyku Python. Správnosť algoritmu bola otestovaná na príklade z publikácie: *A Tutorial on Linear and Differential Cryptanalysis by Howard M. Heys*. Zdrojový kód je dostupný z: `https://github.com/petercurikjr/Design-and-cryptanalysis-of-ciphers---Assignments/blob/master/05/lin_approximation_table_generator.py`

2.2 Útok na SPN

Vlastné riešenie v jazyku C. Riešenie pozostáva z dvoch súborov. Jeden generuje P/C páry do textového súboru. Druhý tento súbor číta a prevádza samotný útok. Výsledky zapíše do textového súboru. Zdrojový kód je dostupný z: `https://github.com/petercurikjr/Design-and-cryptanalysis-of-ciphers---Assignments/tree/master/05/linear_cryptanalysis_attack`

2.3 Vyhodnocovanie a grafy

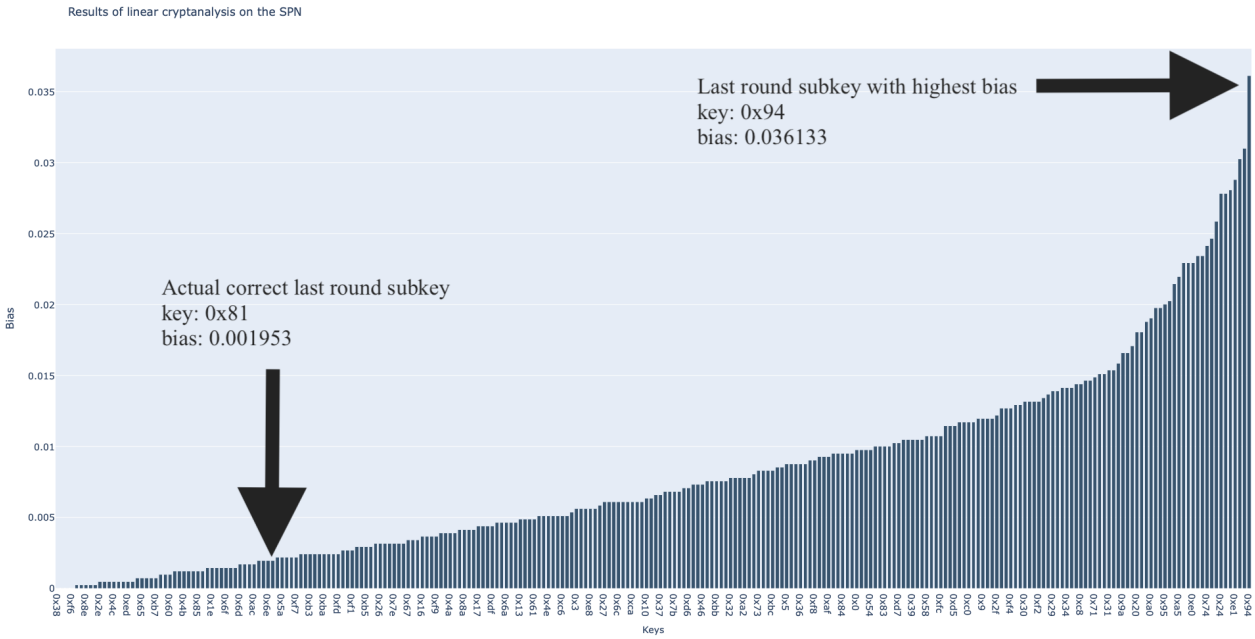
Vlastné riešenie v jazyku Python. Využitie knižnice Plotly na vykresľovanie grafov z dát získaných v textovom súbore, ktorý vytvoril C program zodpovedný za prevedenie útoku. Zdrojový kód je dostupný z: `https://github.com/petercurikjr/Design-and-cryptanalysis-of-ciphers---Assignments/blob/master/05/result_analysis.py`

3 Výsledky

Výstupom útoku je tabuľka, kde ku všetkým 256tim 8 bitovým častiam posledného kolového kľúča je priradený príslušný bias. Tabuľku sme vyniesli do 2D grafu (obrázok nižšie). Na y osi sú usporiadané všetky biasy od najnižšieho pop najnižší. Na x osi sú vynesené všetky kľúče zoradené od kľúčov s najmenším biasom po kľúče s najväčším biasom.

Kľúč, pomocou ktorého bola vygenerovaná vzorka P/C párov, bol 0xC825881F. V poslednom kole je z tohto kľúča odvodený kolový kľúč 0x881F. Keďže sledujeme S-boxy S_{42} a S_{43}, správny kľúč pre tento útok je 0x81.

Tento kľúč má avšak nízky bias, ako vidno na obrázku. S hodnotou 0.001953 sa dostáva medzi najmenej pravdepodobné kľúče na úspešný útok. Najúspešnejší kľúč, u ktorého zároveň zaznamenávame najvyšší nárast oproti predchádzajúcemu kľúču, je kľúč 0x94, s biasom 0.036133.

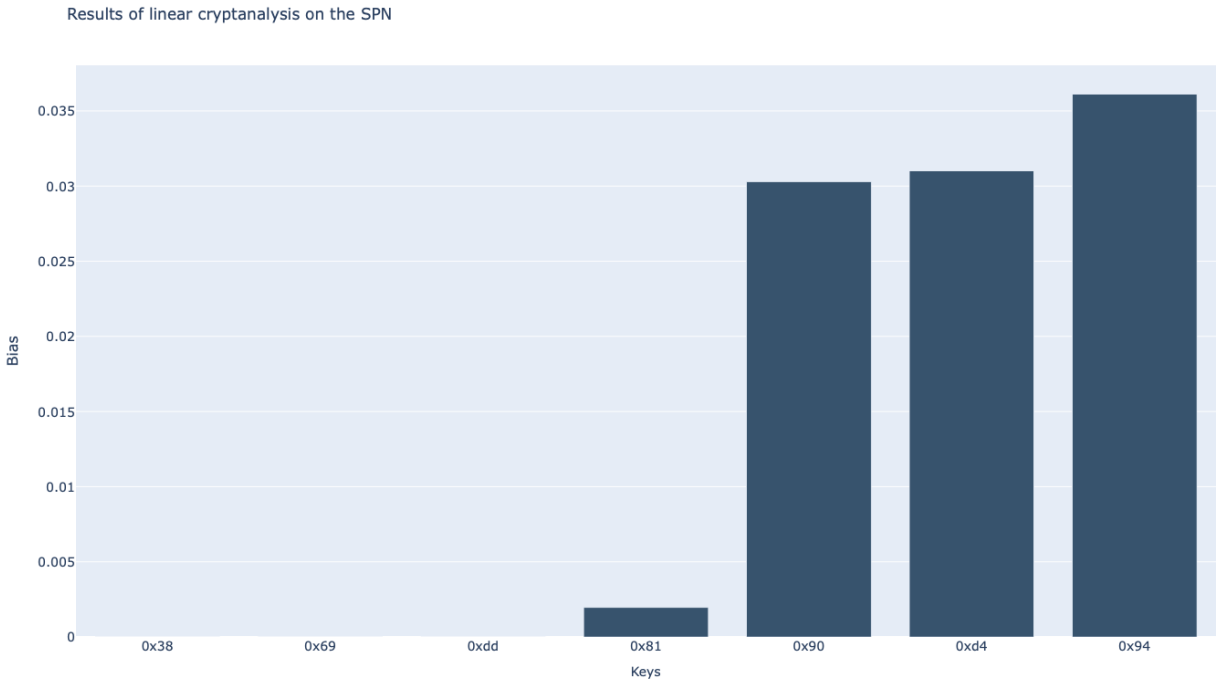


Obr. 2: Výsledky útoku na SPN.

Pre lepšiu prehľadnosť sme vytvorili druhý graf, kde sme vyniesli iba troch najpravdepodobnejších a troch najnepravdepodobnejších adeptov a správny kľúč.

4 Záver

Namerané hodnoty sú v očakávanom rozsahu. Bolo očakávané, že kľúč 0x81 bude mať najvyšší bias, respektíve bude medzi adeptami s najvyššou pravdepodobnosťou. V tomto prípade sú namerané hodnoty ďaleko od očakávaných.



Obr. 3: Výsledky útoku na SPN.