S38
Lineárna kryptoanalýza

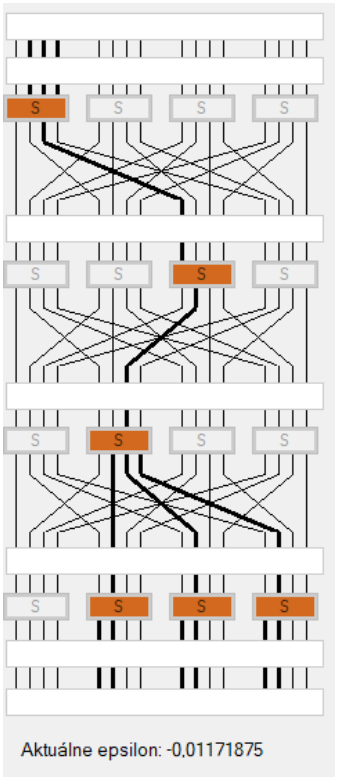
Viliam Mihálik

1. Analýza S-boxu:

a\b	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	-4	2	-2	-2	-2	0	0	0	0	-2	-2	-2	2	4	0
2	0	0	-2	2	2	2	0	-4	-2	2	0	0	0	4	2	2
3	0	0	0	4	0	-4	0	0	-2	-2	-2	2	-2	2	-2	-2
4	0	-2	-2	0	2	0	0	2	2	0	0	2	4	2	2	-4
5	0	-2	0	2	0	2	0	-2	-2	0	2	0	-2	-4	2	-4
6	0	2	0	2	0	2	0	2	4	2	0	-2	-4	2	0	-2
7	0	-2	-6	0	-2	0	0	2	0	-2	2	0	-2	0	0	2
8	0	-2	2	4	-4	2	-2	0	2	0	0	2	2	0	0	2
9	0	2	0	-2	-2	4	-2	0	-2	-4	-2	0	0	2	0	-2
10	0	2	0	2	-2	0	6	0	0	-2	0	-2	2	0	2	0
11	0	2	-2	0	0	-2	-2	-4	4	-2	-2	0	0	-2	2	0
12	0	0	0	0	2	2	2	2	0	0	-4	4	-2	-2	2	2
13	0	0	-2	-2	-4	0	2	-2	0	4	-2	2	0	0	-2	-2
14	0	0	2	-2	0	0	2	-2	2	-2	4	4	-2	2	0	0
15	0	-4	0	0	2	2	2	-2	2	-2	-2	-2	0	0	-4	0

Tab. 1: Lineárny profil S-boxu

Maximálna výchylka: -0.375 = -6/16



Obr. 1: Lineárna trajektória odlišovača

Počet aktívnych S-boxov: 6
Odchýlky aktívnych S-boxoch:

1. -3/8
2. -1/4
3. -1/4
4. 5. 6. 1/4

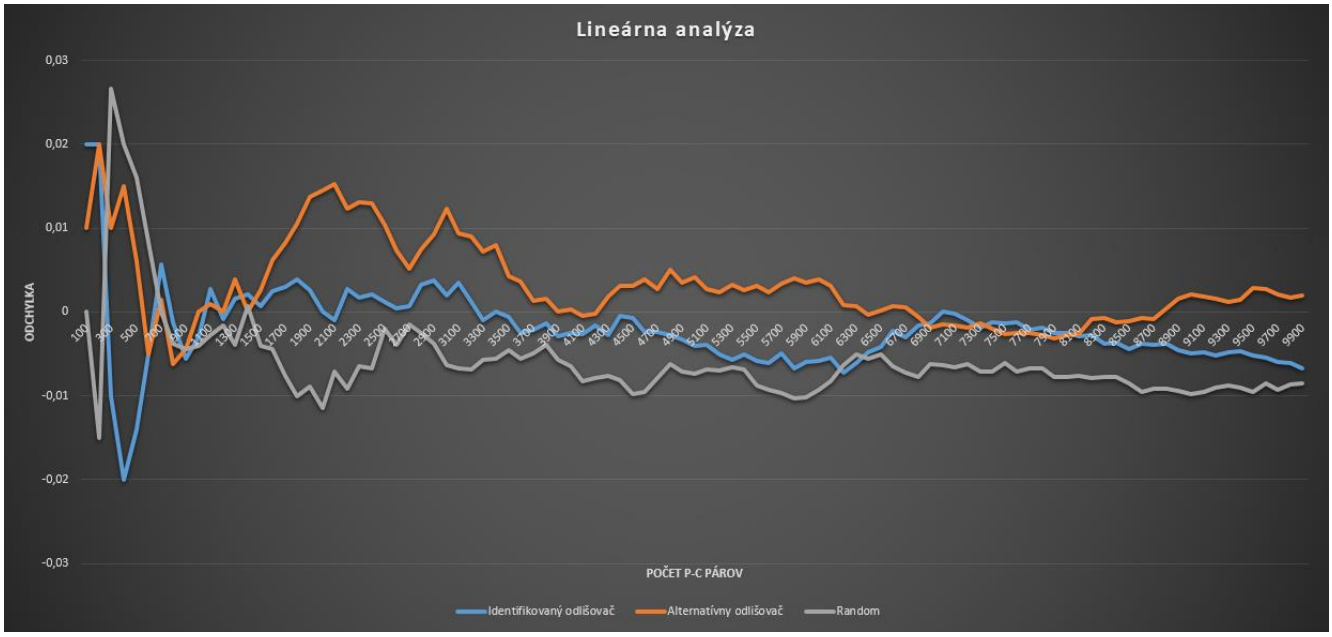
Výsledný odlišovací test(+ je XOR):
*LA : **P2 + P3+ P4 = U5 +U6 + U9 +U10 + U13 + U14***

Alternatívny test:
LA : P4 = U10 + U12

Celková odhadnutá odchýlka:
Odlišovací test: **-0.01171875** Alternatívny test: -0.001953125

Odhad počtu P-C párov: 7282

3. Testovanie odlišovača:



Obr. 2: Graf závislosti nameranej odchýlky od počtu testovaných P-C párov pre (Séria1) odlišovací test, (Séria 2) iný náhodne zvolený test, (Séria 3) odlišovací test na srand()/rand() kombináciu

4. Vyhodnotenie výsledkov: *Slovná sumarizácia a vyhodnotenie výsledkov. Aká je zhoda teórie a praxe?*

Môžeme vidieť že pri použití poznatkou o sboxe sme dokázali korigovať epsilon a tým aj počet P-C párov, ktoré je potrebné vygenerovať. Graf nám ukazuje že identifikovaný odlišovač, ktorý by mal byť najlepší má vo väčšine prípadov najmenšiu odchylku. Avšak taktiež aj alternatívny odlišovač pri väčšom množstve P-C párov pracuje dobre.