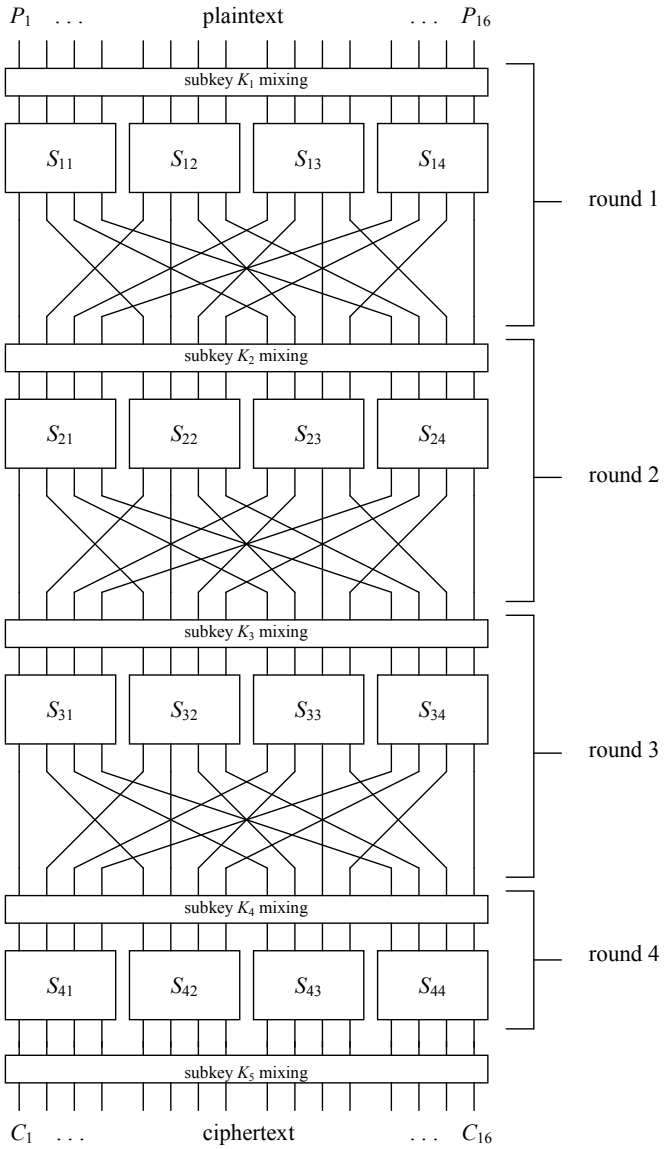
Algebraická kryptoanalýza SPN

Lenka Vábková, Róbert Lórencz

13. listopadu 2018

Osnova

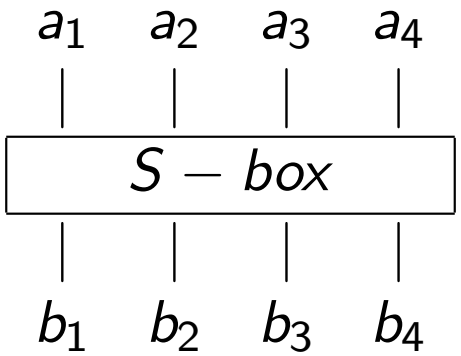
SPN


P_1 . . . plaintext . . . P_{16}
subkey K_1 mixing
S_{11} S_{12} S_{13} S_{14}
round 1
subkey K_2 mixing
S_{21} S_{22} S_{23} S_{24}
round 2
subkey K_3 mixing
S_{31} S_{32} S_{33} S_{34}
round 3
subkey K_4 mixing
S_{41} S_{42} S_{43} S_{44}
round 4
subkey K_5 mixing
C_1 . . . ciphertext . . . C_{16}

S-box

vstup	a_1	a_2	a_3	a_4	výstup	b_1	b_2	b_3	b_4
0	0	0	0	0	E	1	1	1	0
1	0	0	0	1	4	0	1	0	0
2	0	0	1	0	D	1	1	0	1
3	0	0	1	1	1	0	0	0	1
4	0	1	0	0	2	0	0	1	0
5	0	1	0	1	F	1	1	1	1
6	0	1	1	0	B	1	0	1	1
7	0	1	1	1	8	1	0	0	0
8	1	0	0	0	3	0	0	1	1
9	1	0	0	1	A	1	0	1	0
A	1	0	1	0	6	0	1	1	0
B	1	0	1	1	C	1	1	0	0
C	1	1	0	0	5	0	1	0	1
D	1	1	0	1	9	1	0	0	1
E	1	1	1	0	0	0	0	0	0
F	1	1	1	1	7	0	1	1	1

Funkce



$$b_i(a_1, a_2, a_3, a_4) = \tag{1}$$
$$c_0 +$$
$$c_1 a_1 + c_2 a_2 + c_3 a_3 + c_4 a_4 +$$
$$c_{12} a_1 a_2 + c_{13} a_1 a_3 + c_{14} a_1 a_4 + c_{23} a_2 a_3 + c_{24} a_2 a_4 + c_{34} a_3 a_4 +$$
$$c_{123} a_1 a_2 a_3 + c_{124} a_1 a_2 a_4 + c_{134} a_1 a_3 a_4 + c_{234} a_2 a_3 a_4 +$$
$$c_{1234} a_1 a_2 a_3 a_4$$

Hledáme koeficienty c_0 až $c_{1234} \in \{0, 1\}$ pro b_1, b_2, b_3, b_4.

Koeficienty

S-boxu pro vstup = '0','1','2' atd. má $b_1 = 1, 0, 1$ atd. má vyraz (1) tvar:

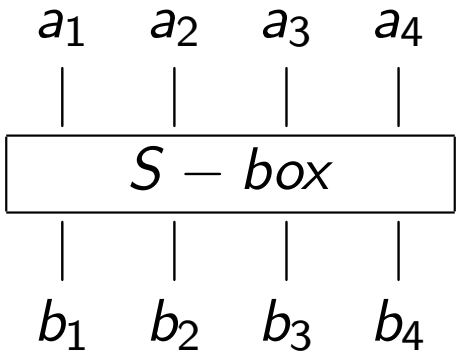
$$
\begin{aligned}
1 &= c_0 \\
0 &= c_0 + c_4 \\
1 &= c_0 + c_3 \\
0 &= c_0 + c_3 + c_4 + c_{34} \\
0 &= c_0 + c_2 \\
1 &= c_0 + c_2 + c_4 + c_{24} \\
1 &= c_0 + c_2 + c_3 + c_{23} \\
1 &= c_0 + c_2 + c_3 + c_4 + c_{23} + c_{24} + c_{34} + c_{234} \\
0 &= c_0 + c_1 \\
1 &= c_0 + c_1 + c_4 + c_{14} \\
0 &= c_0 + c_1 + c_3 + c_{13} \\
1 &= c_0 + c_1 + c_3 + c_4 + c_{13} + c_{14} + c_{34} + c_{134} \\
0 &= c_0 + c_1 + c_2 + c_{12} \\
1 &= c_0 + c_1 + c_2 + c_4 + c_{12} + c_{14} + c_{24} + c_{124} \\
0 &= c_0 + c_1 + c_2 + c_3 + c_{12} + c_{13} + c_{23} + c_{123} \\
0 &= c_0 + c_1 + c_2 + c_3 + c_4 + c_{12} + c_{13} + c_{14} + c_{23} + c_{24} + c_{34} + \\
&\quad c_{123} + c_{124} + c_{134} + c_{234} + c_{1234}
\end{aligned}
$$

S-box

Tabulka vstupů a výstupů:

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

Funkce:



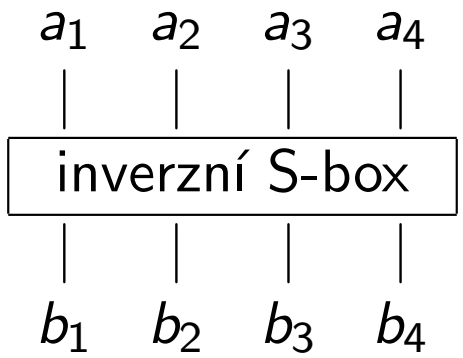
$$b_1 = 1 + a_1 + a_2 + a_4 + a_1a_2 + a_2a_3 + a_1a_2a_3 + a_2a_3a_4$$
$$b_2 = 1 + a_1 + a_2 + a_1a_3 + a_2a_4 + a_3a_4 + a_1a_3a_4$$
$$b_3 = 1 + a_3 + a_4 + a_1a_2 + a_1a_3 + a_1a_4 + a_2a_3 + a_2a_4 + a_3a_4 + a_1a_2a_3 + a_1a_2a_4$$
$$b_4 = a_1 + a_3 + a_1a_4 + a_2a_4 + a_1a_3a_4$$

inverzní S-box

Tabulka vstupů a výstupů:

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

Funkce:



$$b1 = 1 + a_1 + a_2 + a_3 + a_4 + a_2a_3a_4$$
$$b2 = 1 + a_2 + a_4 + a_1a_4 + a_1a_3 + a_1a_3a_4 + a_1a_2a_3$$
$$b3 = 1 + a_3 + a_2 + a_1a_4 + a_1a_2 + a_1a_2a_4$$
$$b4 = a_1 + a_2 + a_4 + a_3a_4 + a_2a_3 + a_2a_3a_4 + a_1a_4 + a_1a_2 + a_1a_2a_4$$

Vstupy kryptoanalýzy

$$
\begin{aligned}
ot &= \{0,1,0,1,0,0,1,0,0,1,0,0,0,0,0,1\} \\
ct &= \{1,1,1,1,0,0,0,1,0,1,1,1,1,1,1,0\} \\
klic &= \{k_1,k_2,k_3,k_4,k_5,k_6,k_7,k_8,0,0,1,1,0,1,0,0\}
\end{aligned}
$$

Všechny rovnice platí modulo 2.

Rovnice I.

- $k_1(1+k_2)(1+k_3)+k_4+k_2k_4+k_5+k_4k_5+k_4k_6k_7+k_5k_6k_7+k_4k_5k_6k_7+k_4k_8+k_6k_8+k_4k_6k_8+k_4k_6k_7k_8+(1+k_2)k_3(1+(1+k_4)k_5(1+k_6k_7)+k_8+k_4k_8+(1+k_4)k_6(k_7+k_8+k_7k_8))=k_1+k_3k_4+k_2(k_3+k_4+k_3k_4)+k_6+k_7$
- $1+(1+k_4+k_2k_4+k_4k_5+k_2k_4k_5+k_4k_6+k_2k_4k_6+k_5k_6+k_3(1+k_4)(1+k_5+k_6)+k_1(1+k_3k_4)(1+k_5+k_6))k_8+k_7(1+k_4+k_2k_4+k_8+k_4k_8+k_2k_4k_8+k_5k_8+k_4k_5k_8+k_2k_4k_5k_8+k_4k_6k_8+k_2k_4k_6k_8+k_5k_6k_8+k_3(1+k_4)(1+(1+k_5+k_6)k_8)+k_1(1+k_3k_4)(1+(1+k_5+k_6)k_8))=k_3k_4+k_2(1+k_3)(1+k_4)+k_6+k_7+k_6k_7+k_8+k_6k_7k_8$
- $1+k_2k_3k_4+k_7+k_8+k_6(1+k_7+k_7k_8)=k_2+k_1(1+k_2(k_3+k_4))$
- $k_2(1+k_4)(1+k_5+k_7+k_6k_8+k_5k_7k_8)+k_3(1+k_1+k_1k_4)(1+k_5+k_7+k_6k_8+k_5k_7k_8)+k_4(k_5+k_7+k_6k_8+k_5k_7k_8+k_1(1+k_5+k_7+k_6k_8+k_5k_7k_8))=k_7+k_8+k_6(1+k_7+k_7k_8)$

Rovnice II.

- $k_1(1+(1+k_2+k_2k_3)k_4)+k_4(k_5+k_5k_6k_7+k_8+k_6(k_7+k_8+k_7k_8))=k_2k_3+k_3k_4+k_5k_6k_7+k_8+k_5k_8+k_5k_7k_8$
- $1+k_6+k_5k_6k_7+k_8+k_1(-1+k_2+k_3+k_2k_3-k_7k_8-k_3k_4k_7k_8)+k_2(1+k_3-k_4(1+k_7k_8))=k_6k_8+k_7(1+(1+k_3)(1+k_4)k_8)$
- $(1+k_1)k_2(1+k_3)+k_4+(1+k_1)k_3(1+k_4)+k_8+k_5k_7k_8=1+k_5k_7+k_7k_8+k_6(1+k_7+k_8+k_5k_8)$
- $k_2+k_3+k_1k_3+k_4+k_1k_4+k_2k_4+k_1k_3k_4=1+k_5(1+k_6k_7+k_8+k_7k_8)$

Rovnice III.

- $1+k_3+k_5+k_6k_7+k_5k_6k_7+k_8+k_6k_8+k_6k_7k_8+k_1(1+k_2)(1+k_3)(1+(1+k_4)k_5(1+k_6k_7)+k_8+k_4k_8+(1+k_4)k_6(k_7+k_8+k_7k_8))+k_2((1+k_4)(1+k_5+k_5k_6k_7+k_8+k_6(k_7+k_8+k_7k_8))+k_3(1+(1+k_4)k_5(1+k_6k_7)+k_8+k_4k_8+(1+k_4)k_6(k_7+k_8+k_7k_8)))=1+k_1+k_2+k_2k_4+k_1k_2k_4+k_5+k_6+k_5k_8+k_5k_6k_8$
- $k_4+k_2k_4+k_5+k_7+k_4k_5k_7+k_2k_4k_5k_7+k_8+k_4k_8+k_2k_4k_8+k_5k_8+k_4k_5k_8+k_2k_4k_5k_8+k_6k_8+k_4k_6k_8+k_2k_4k_6k_8+k_5k_6k_8+k_4k_7k_8+k_2k_4k_7k_8+k_4k_6k_7k_8+k_2k_4k_6k_7k_8+k_5k_6k_7k_8+k_3(1+k_4)(1+(1+k_6)(1+k_7)k_8+k_5(k_7+k_8))+k_1(1+k_3k_4)(1+(1+k_6)(1+k_7)k_8+k_5(k_7+k_8))=(1+k_1+k_2+k_2k_4+k_1k_2k_4)(k_6+k_5(1+k_8+k_6k_8))$
- $1+k_3(1+k_2+k_1k_2+k_4)+k_6k_8+k_7(1+k_5+k_6+k_5k_6+k_8)=(k_1+k_2+k_2k_4+k_1k_2k_4)(k_6+k_5(1+k_8+k_6k_8))$
- $1+k_2+k_3+k_1k_3+k_4+k_1k_4+k_2k_4+k_1k_3k_4+k_5+k_7+k_6k_8+k_5k_7k_8=1+k_2(1+k_4)(k_6+k_5(1+k_8+k_6k_8))+k_1(1+k_2k_4)(k_6+k_5(1+k_8+k_6k_8))$

Rovnice IV.

- $1 + k_1(1 + k_3 + k_2(1 + k_3 - k_4)) + k_2(-1 + k_3 + k_4 - k_3k_4) + k_5 + k_4k_5 + k_6k_7 + k_4k_6k_7 + k_5k_6k_7 + k_4k_5k_6k_7 + k_8 + k_4k_8 + k_6k_8 + k_4k_6k_8 + k_4k_6k_7k_8 = k_3 + k_6 + k_7 + k_5k_8 + k_5k_6k_8 + k_7k_8$
- $k_6 + k_7 + k_5k_6k_8 + k_6k_7k_8 + k_2(1 + k_1k_4 + k_3k_4 - k_4k_7 - k_4k_8 - k_4k_7k_8) = (k_1 + k_4)(k_7 + k_8 + k_7k_8) + k_3(-1 + k_8 + k_4k_8 + k_1k_4k_8 + (1 + k_4 + k_1k_4)k_7(1 + k_8))$
- $k_1 + k_1k_2k_3 + k_3k_4 + k_2(k_3 + k_4 - k_3k_4) = 1 + k_6 + k_7 + k_5k_8 + k_5k_6k_8 + k_7k_8 + k_6k_7k_8$
- $(k_5 + k_7)k_8 + k_6(1 + k_5k_8 + k_7k_8) = k_5 + k_6k_8 + k_5k_7k_8$

Vyřešením dostaneme nezmámé bity klíče:

$$\begin{aligned} k_1 &= 0 \\ k_2 &= 0 \\ k_3 &= 0 \\ k_4 &= 1 \\ k_5 &= 0 \\ k_6 &= 0 \\ k_7 &= 1 \\ k_8 &= 0 \end{aligned}$$