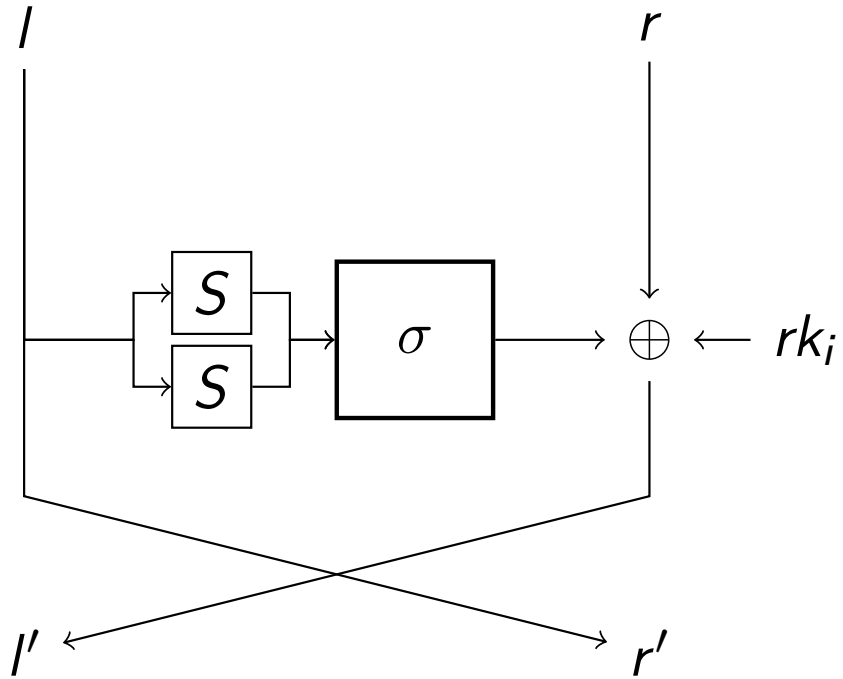
Linear Cryptanalysis

May 22, 2019

TC05 (mini)



With Sbox (different from TC05):

$S = (12,\ 1,\ 10,\ 7,\ 13,\ 8,\ 9,\ 4,\ 6,\ 15,\ 11,\ 2,\ 0,\ 14,\ 3,\ 5)$

and bit permutation:

$$\sigma = \left(\begin{array}{cccc|cccc} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 6 & 0 & 1 & 7 & 2 & 4 & 5 & 3 \end{array}\right)$$

LAT

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

Next week

- The designs are uploaded to `https://cryptanex.hideinplainsight.io/tcc/`.
- Small exercise: compute LAT of `TC05` Sbox and linear characteristic.
- More about Linear cryptanalysis.
- Ask questions early and often.