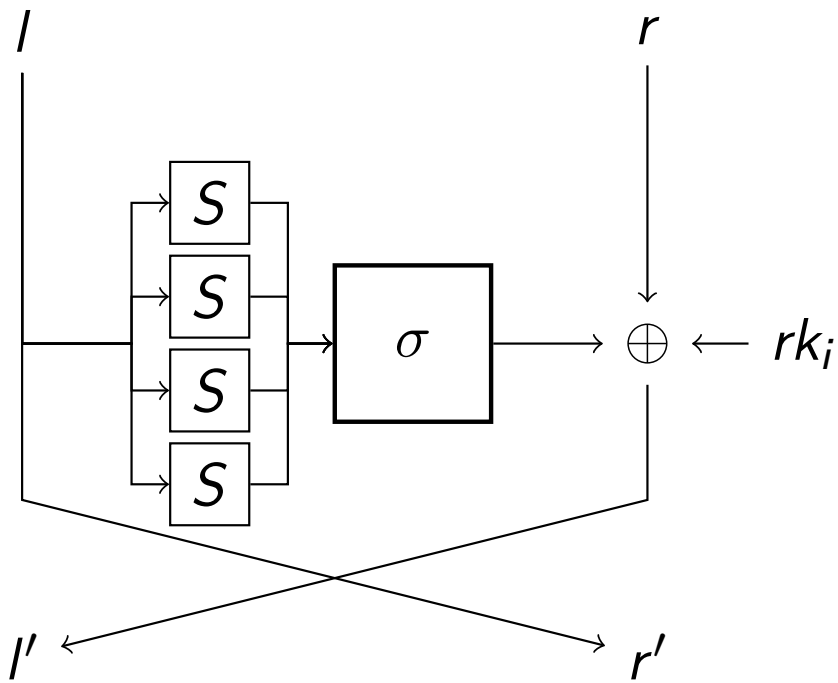
Breaking 10 rounds of TC05

May 1, 2019

Plan de campagne

- Find suitable differential distinguisher with prob. $\ll 2^{-10}$
- Design the key recovery attack, s.t. we can run it on our own computers.
- Some non-trivial optimisations.

TC05



TC05

The sbox S is defined as follows:

$$S = (\texttt{E}, \texttt{B}, \texttt{4}, \texttt{6}, \texttt{A}, \texttt{D}, \texttt{7}, \texttt{0}, \texttt{3}, \texttt{8}, \texttt{F}, \texttt{C}, \texttt{5}, \texttt{9}, \texttt{1}, \texttt{2})$$

and the bit permutation σ is defined as follows:

$$\sigma = \left(\begin{array}{cccc|cccc|cccc|cccc} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & A & B & C & D & E & F \\ 6 & 0 & 1 & 7 & E & 8 & 9 & F & 2 & 4 & 5 & 3 & A & C & D & B \end{array}\right)$$

Given master key $K = k_0|k_1|k_2|k_3$ the round key k_i is defined as follows:

$$k_{i+1} = k_{i-3} \oplus k_i \oplus \sigma(k_{i-1}) \oplus 0xC$$

TC05 sbox DDT

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

Optimizing TC05

- We can combine the σ and S-box layer into tables to reduce the round functions to two table lookups.
- We create two 8×32-bit lookup tables one for the upper half of the state and one for the lower half of the state.

```
uint32_t SBOX8_0[256];
uint32_t SBOX8_1[256];

void compute_SBOX8_sigma(){
    uint32_t s0, s1;
    for(uint32_t x=0; x < 256; x++){
        s0 = (apply_sbox(x) & 0xFF);
        s1 = (apply_sbox(x) << 8) & 0xFF00;
        SBOX8_0[x] = sigma(s0);
        SBOX8_1[x] = sigma(s1);
    }
}
```

Nextnext week

- Next week **no** lecture.
- Project design deadline is for next class.
- Ask questions early and often.