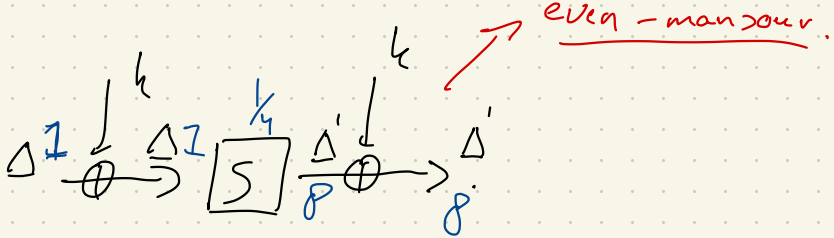
Differential Cryptanalysis

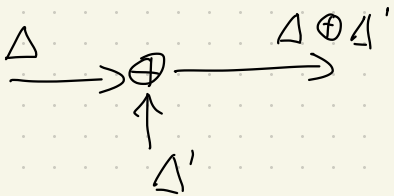
$$\Delta_{in} = p \oplus p' \longrightarrow \boxed{E} \longrightarrow c \oplus c' = \Delta_{out}$$

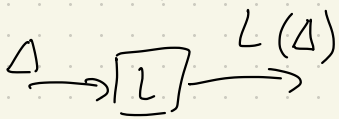
$k \oplus k = 0$

input difference

$$p \oplus p' = \Delta$$







DDT

$$S = \begin{bmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & A & B & C & D & E & F \\ C & 6 & 9 & 0 & 1 & A & 2 & B & 3 & 8 & 5 & D & 4 & E & 7 & F \end{bmatrix}$$

$$\overset{1}{\overset{\shortparallel}{\Delta_{in}}} = x \oplus x' \longrightarrow \boxed{S} \longrightarrow y \oplus y' = \Delta_{out}$$

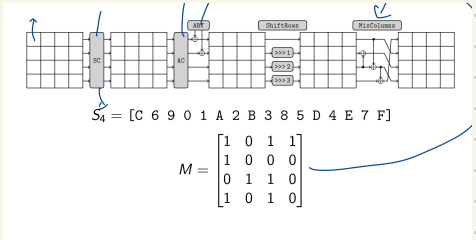
$$S(x) \oplus S(x')$$

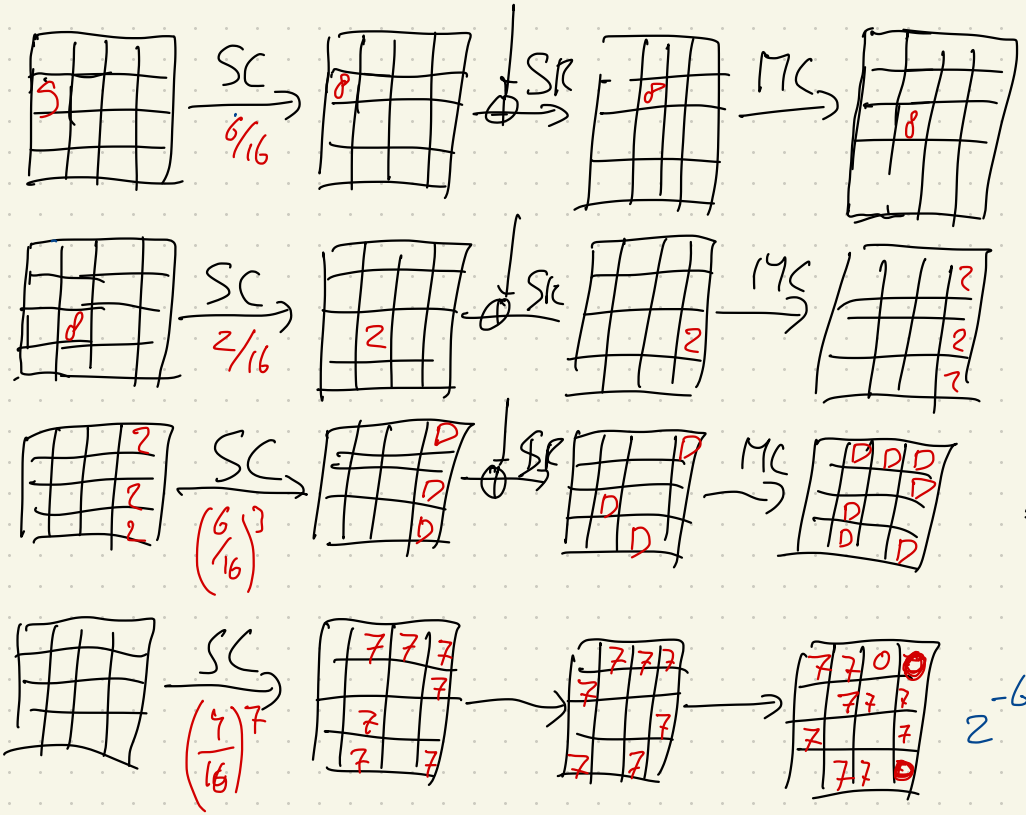
Def DDT, the DDT, difference distr. table maps input differences and output differences to probabilities, s.t. $DDT[\Delta_{in}][\Delta_{out}] = p$, where p is the prob. that this event happens.

x	$x' = \Delta_{in} \oplus x$	$S(x)$	$S(x')$	$S(x) \oplus S(x')$
0	1	C	6	A
2	3	9	0	9
4	5	1	A	B
6	7	2	B	9
8	9	3	8	B
A	B	5	D	8
C	D	4	E	A
E	F	7	F	8

ALG Compute DDT(S_{2^n}).

```
DDT[2^n][2^n] = (0)  # fill with zeroes.
for Δin ∈ F_2^n:
    for x ∈ F_2^n:
        x' = Δin ⊕ x
        Δout = S(x) ⊕ S(x')
        DDT[Δin][Δout] ++.
```





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

Δ_{out}

Δ_{in}

	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

2^{-64}

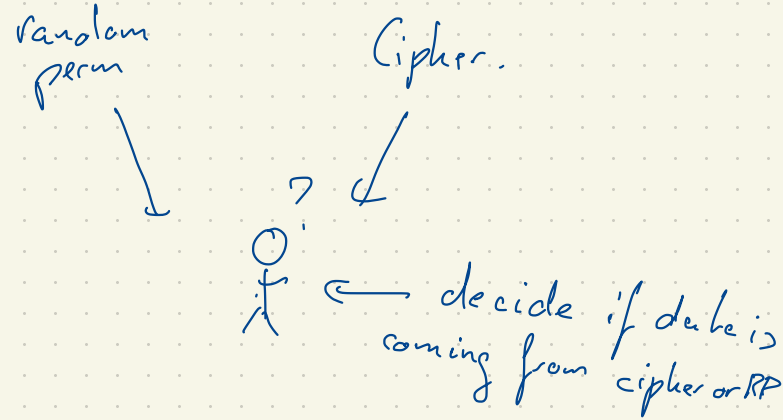
$$\left(\frac{6}{16}\right)^4 \cdot \left(\frac{4}{16}\right)^7 \cdot \frac{2}{16} = 2^{-25.\ldots}$$

Differential Cryptanalysis 2

Schedule:

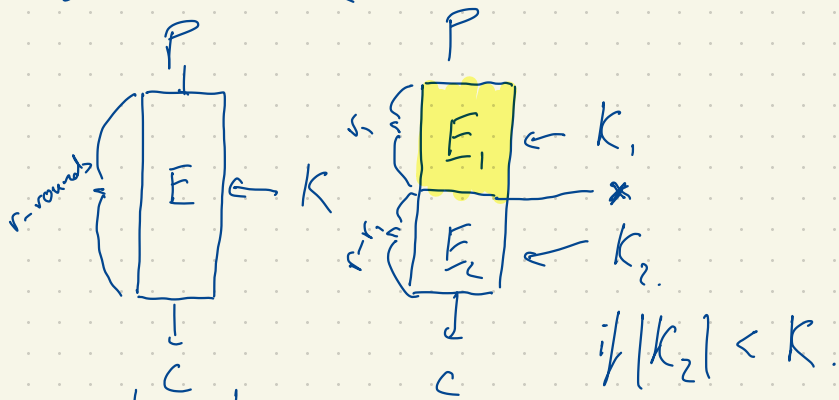
- Recap of last week.
- key recovery attacks.
- Truncated differentials.

Distinguisher.



Given a Diff Characteristic with prob p we can distinguish the cipher using $\frac{1}{p}$ pairs with the correct input diff.

Key recovery.



if $|K_2| < K$.

we pick K_2

if K_2 is the correct key.

$\Rightarrow$ distinguisher reports cipher

if K_2 is wrong

$\Rightarrow$ distinguisher reports RP

<u>Assumption</u> Wrong key randomization Assumption.

If we use the wrong key for enc./dec. the resulting state is random.

<u>Alg</u>

given distinguisher $\pi(p, x)$

$\Rightarrow$ Cipher / RP.

1. Pick $k_2 \in K_2$.
2. compute $x = E_2^{-1}(c, k_2)$
3. if $\pi(p, x) = RP$

   $\Rightarrow$ go to 1

   if $\pi(p, x) =$ Cipher

   $\Rightarrow$ return k_2 as a candidate key.

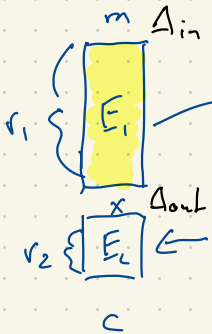
<u>Complexity</u>

Time : $O(|K_2|)$

Mem : $O(1)$

Data : $O(1)$.

Differential Char as a Dist.



Diff char with prob p.

$$\Delta_{in} \xrightarrow{p} \Delta_{out}$$

k_2.

Time:

$$O\left(|K_2| \cdot \frac{1}{p}\right)$$

Memory/Data:

$$O\left(\frac{1}{p}\right)$$

ALG Key recovery.

Given $\Delta_{in} \to \Delta_{out}$ with p.

pairs = [ ].

for i in $0 \ldots \frac{1}{p} \cdot c$:

  pairs += $(m, m \oplus \Delta_{in}, E(m), E(m \oplus \Delta_{in}))$

given.

for $k_2 \in K_2$:

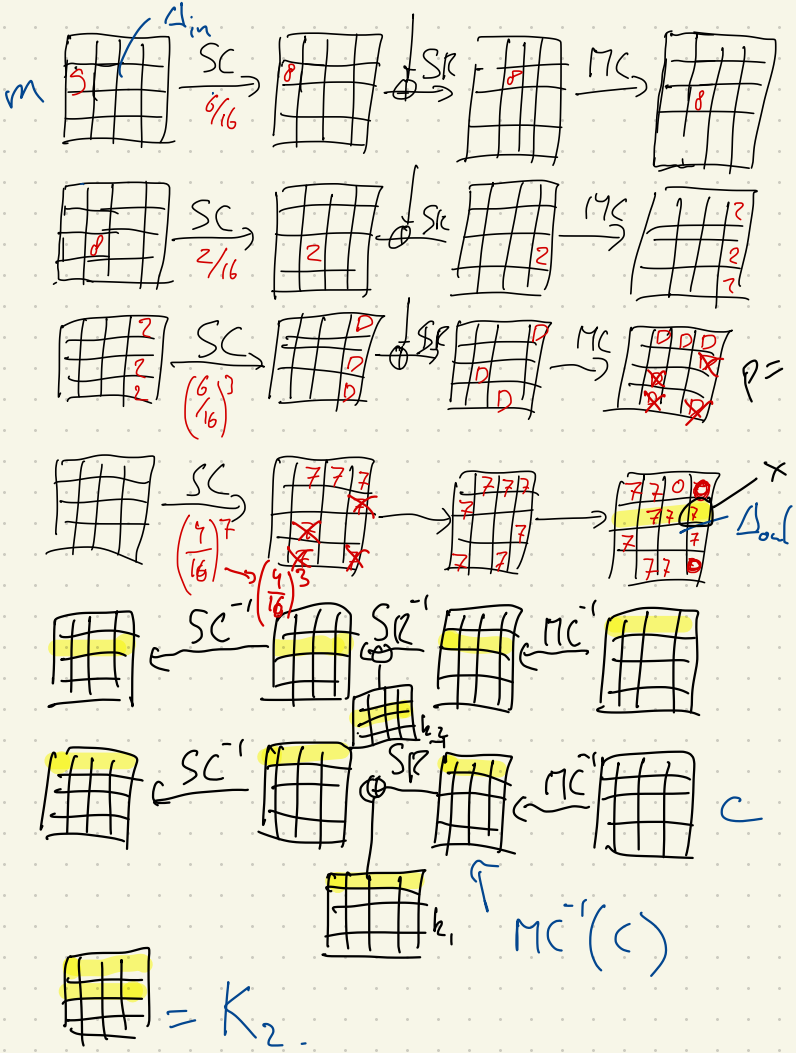
  for m, m', c, c' in pairs:

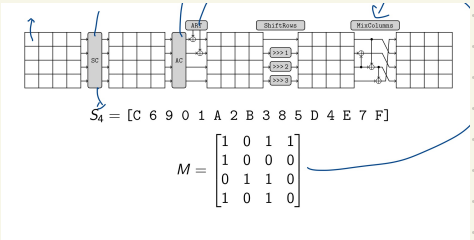
    $x = E_2^{-1}(c, k_2)$

    $x' = E_2^{-1}(c', k_2)$

    if $x \oplus x' = \Delta_{out}$:

      return k_2 as a candidate.

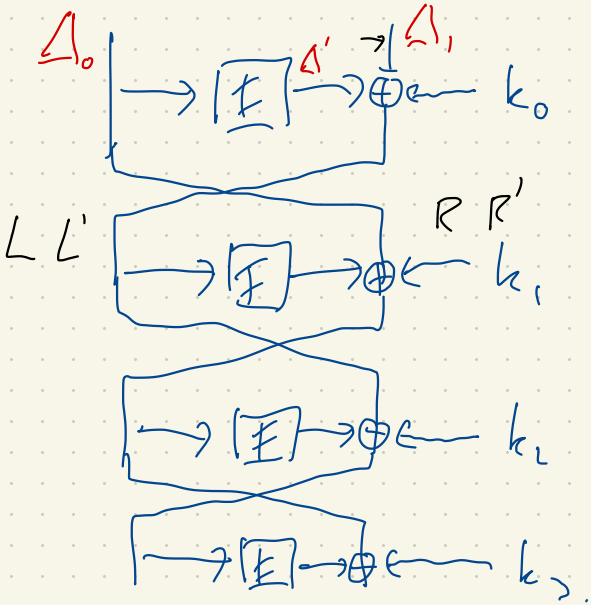




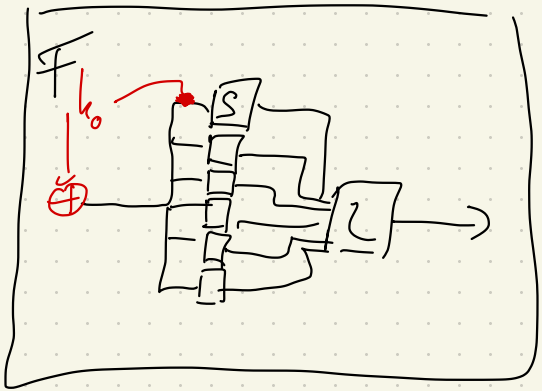
Given 2^{26} pairs (m, m', c, c') with $m \oplus m' = \Delta_{in}$

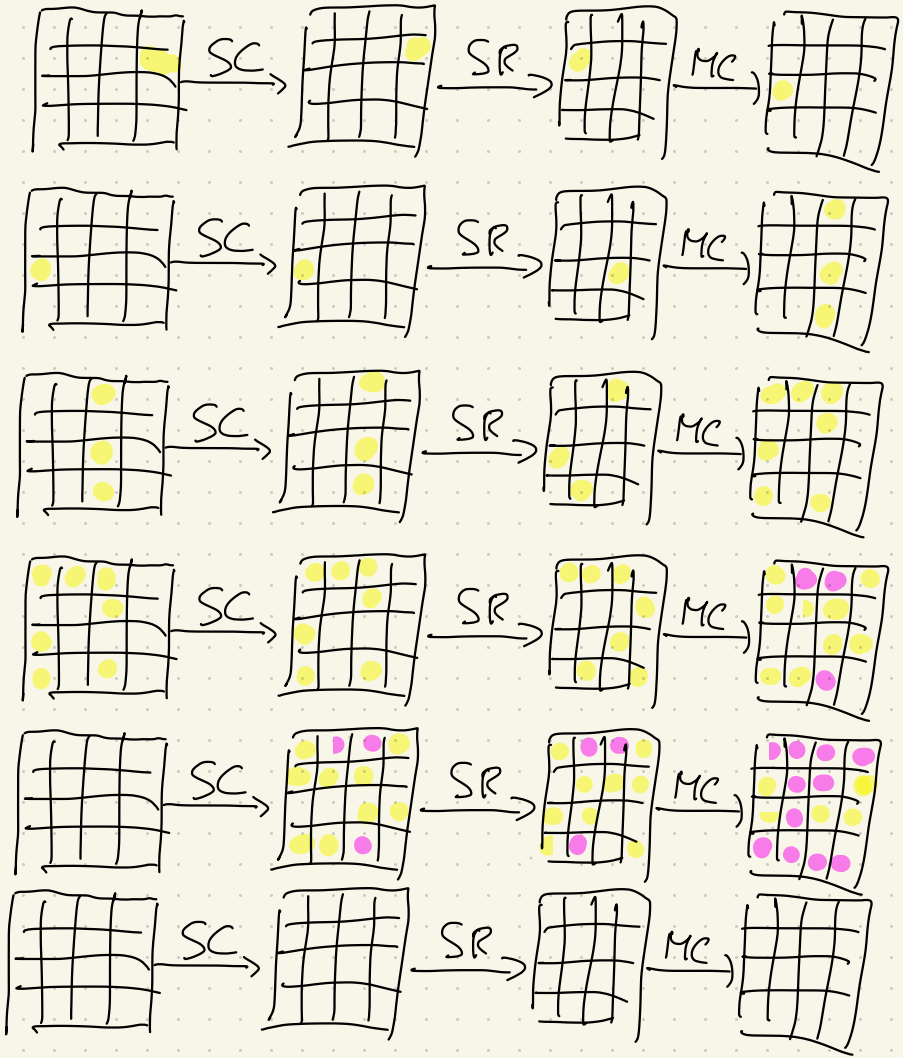
for

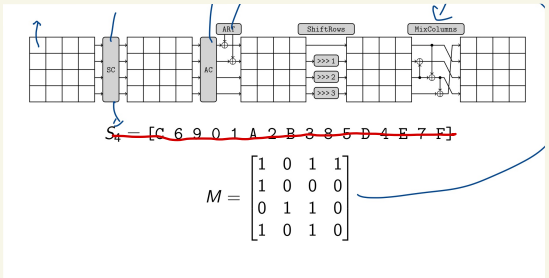
1. Project.
   - a. Cryptanalysis Competition.
   - b. Analysis of ciphers using SMT.
2. Key recovery.
3. Truncated Diff.
4. Differentials.



$$\Delta_1 = (L \oplus L') \oplus \Delta' \oplus k_0 \oplus k_0.$$







$\square \longrightarrow$ zero diff.

$\square \longrightarrow$ non-zero diff.

$\square \longrightarrow$ unknown.

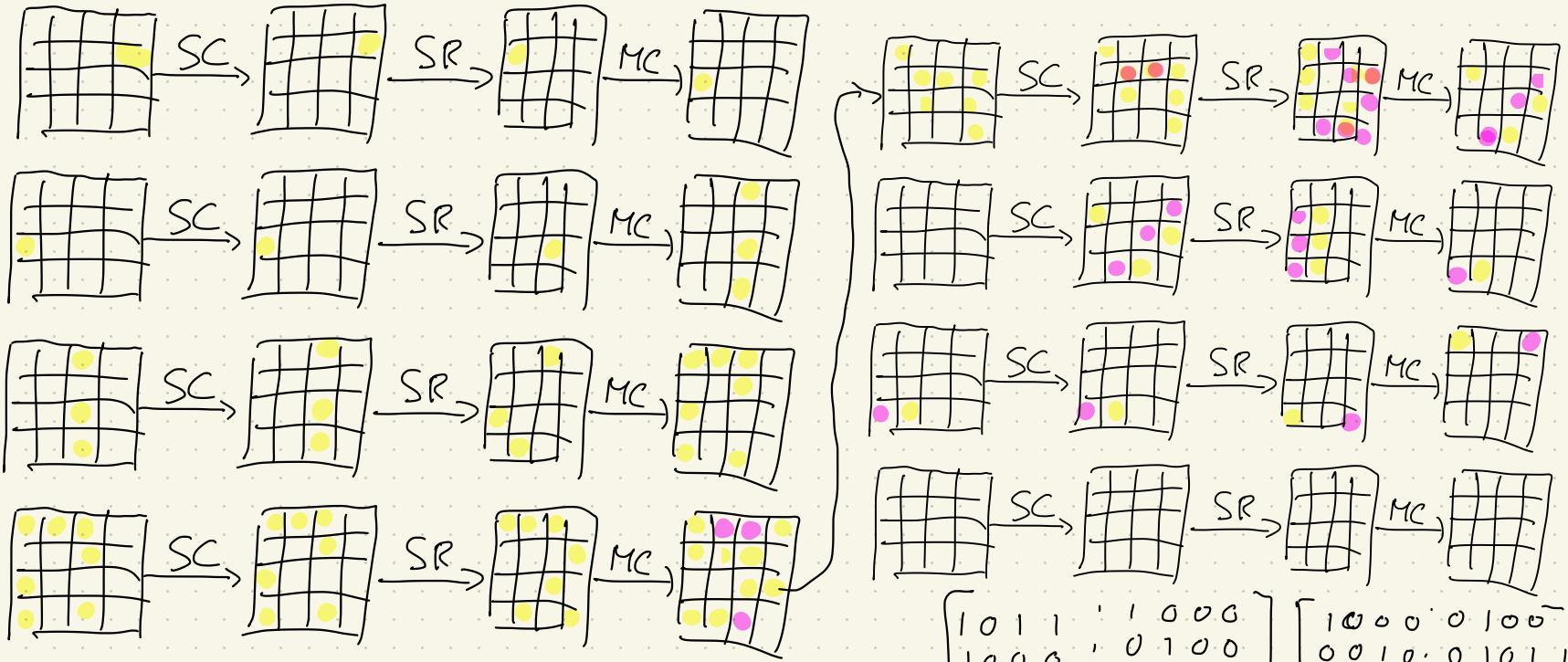
$(2^{-4})^4 = 2^{-16}$

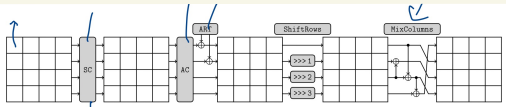
$\square \oplus \square = \square$

$\square \oplus \square = \square$

$S(\square) = \square$

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





$\cancel{S_4 = [C\ 6\ 9\ 0\ 1\ A\ 2\ B\ 3\ 8\ 5\ D\ 4\ E\ 7\ F]}$

$$M = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 \end{bmatrix}$$

$$\left[\begin{array}{cccc|cccc} 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \end{array}\right] \quad \left[\begin{array}{cccc|cccc} 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \end{array}\right]$$

$$\left[\begin{array}{cccc|cccc} 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \end{array}\right] \quad \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 \end{bmatrix}.$$

Differential char.

$$\Delta_{in} \to \Delta_0 \to \Delta_1 \to \Delta_{out}.$$

$$\begin{tikzcd}
 & \Delta_0' \arrow[r] & \Delta_1' \arrow[dr] & \\
\Delta_{in} \arrow[ur, "P_n"] \arrow[dr, "P_0"'] & & \vdots & \Delta_{out}. \\
 & \Delta_0 \arrow[r] & \Delta_1 \arrow[ur] &
\end{tikzcd}$$

$\boxed{\text{Bonus points}}$ if you check your characteristic for the diff. effect.

$P_0 + \dots + P_n$