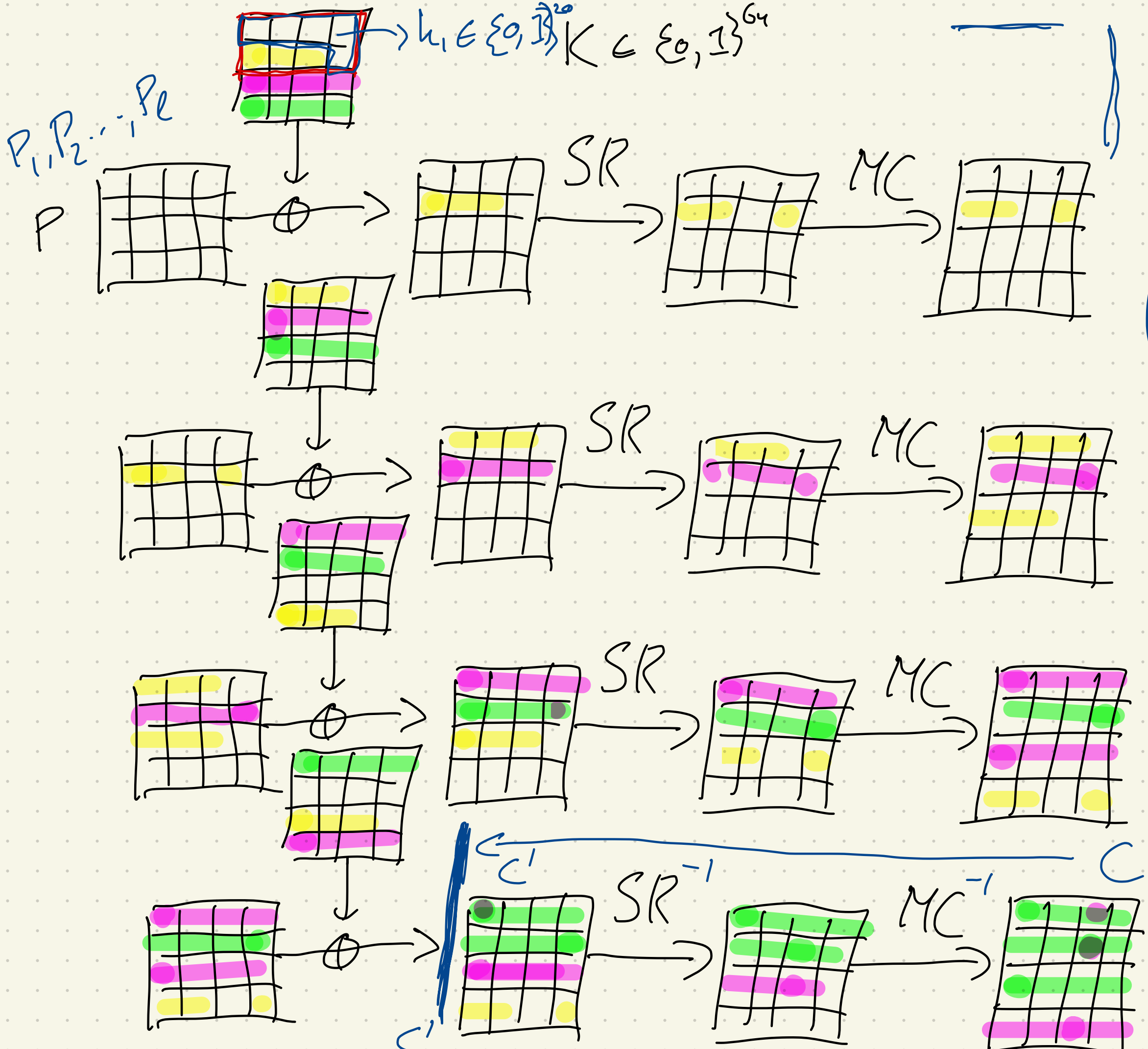
Lecture 3

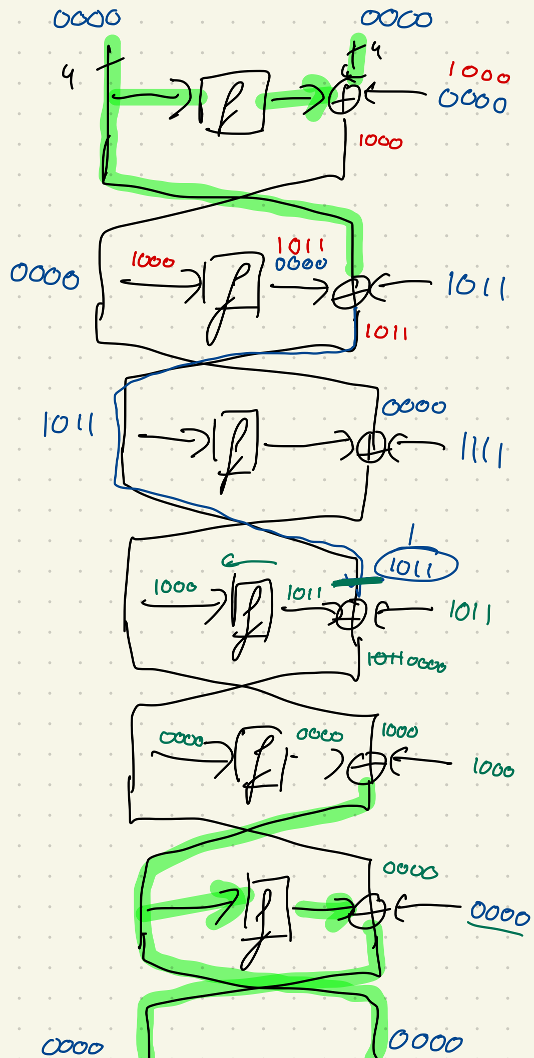


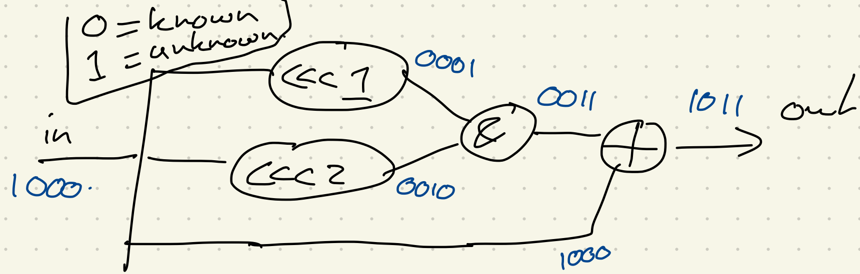
C

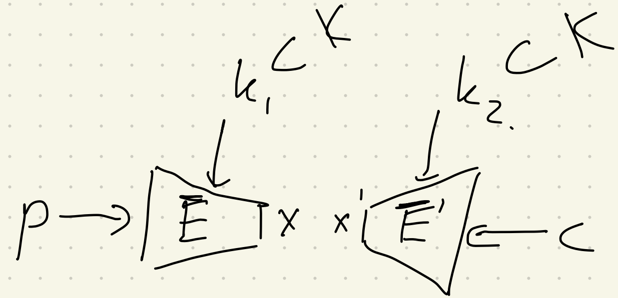
$$M = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix} = \begin{pmatrix} a \oplus c \\ b \oplus c \\ a \oplus d \\ c \end{pmatrix}$$

$$M \cdot \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}$$







$$X \cap X' \neq \emptyset$$

Phase 1

$H: X \to k_1$

for $k_1 \in K_1$:
- $x = [\,]$
- for $p \in P$:
  - $x \mathrel{+}= \overline{E}_{k_1}(p)$
- $H[x] \to k_1$

Phase 2

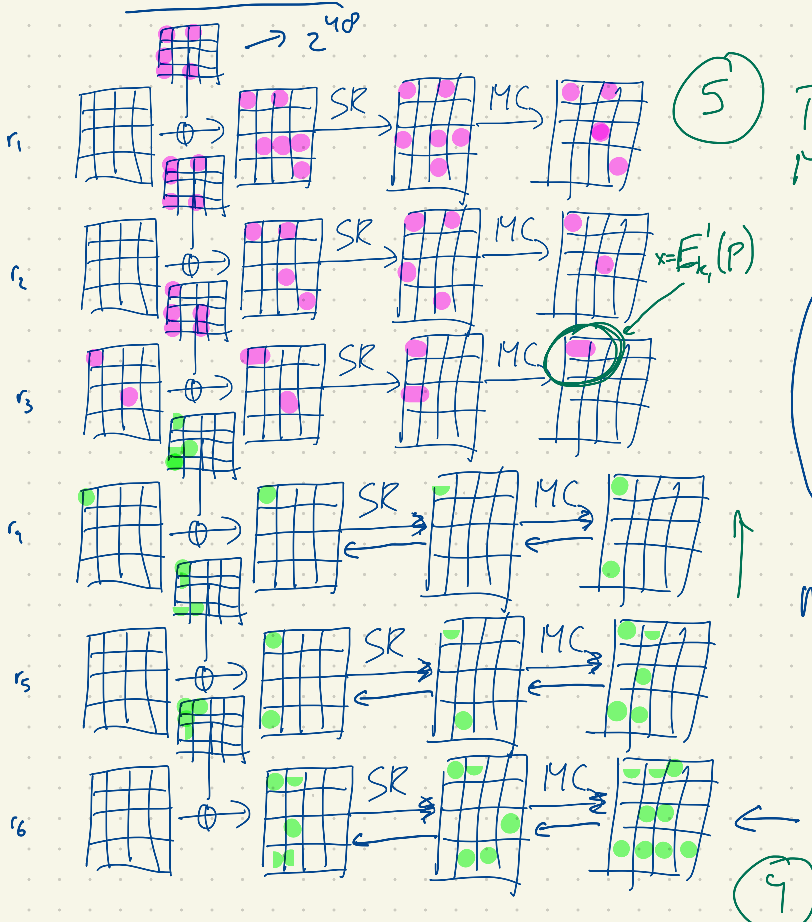
for $k_2 \in K_2$:
- $x' = [\,]$
- for $c \in C$:
  - $x' \mathrel{+}= \overline{E}_{k_2}(c)$
  - if $x' \in H$:
    - output $H[x']$, k_2 prob.

Lecture 4

$$M \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

$$M^{-1} \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 \end{pmatrix}$$

6 - mitm



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

Time : 2^{20}

Mem : 2^{20}

$H[x] \to k_1$

$$M \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

$x = E'_{k_1}(p_1) \,|\, E'_{k_1}(p_2) | \dots | E'_{k_1}(p_\ell)$

$x' = D' \dots\dots$

$$\begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix} \xrightarrow{M^{-1}} \begin{pmatrix} ad \\ bd \\ d \\ acd \end{pmatrix}$$

$4 \cdot 16 = 64$

$$\begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix} \Rightarrow \begin{pmatrix} ac \\ bc \\ ad \\ c \end{pmatrix}$$

$$M^{-1} \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 \end{pmatrix}$$

Time : $2^{4 \cdot 4} = 2^{16}$

$$\begin{tikzcd} & K_1 \subseteq K \arrow[d] & & K_2 \subseteq K \arrow[d] & \\ P \arrow[r] & \boxed{E'} \arrow[r] & x & \boxed{D'} \arrow[l] & c \arrow[l] \end{tikzcd}$$

until now $\Rightarrow$ $K_1 \cap K_2 = \emptyset$

$\Rightarrow$ $K_1 \cap K_2 = K_{12}$

Time comp:

$$|K_{12}| \cdot \left(|K_1| - |K_{12}| + |K_2| - |K_{12}| \right)$$

Mem comp

$$|K_1| - |K_{12}|$$

MitM adv.

for $k_{12} \in K_{12}$:

  // forw. pass

  Initialize H

  for $k_1' \in K_1 \setminus K_{12}$:

    $k_1 = k_1' \oplus k_{12}$.

    $x = E'_{k_1}(p)$

    $H[x] = k_1'$

  1 Time: $|K_1| - |K_{12}|$ Mem: $|K_1| - |K_{12}|$

  // backw.

  for $k_2' \in K_2 \setminus K_{12}$:

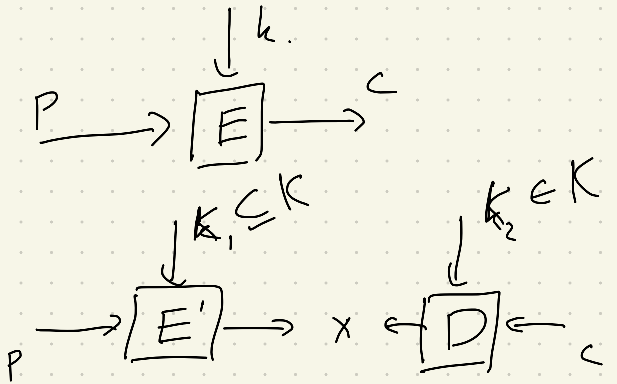
    $k_2 = k_2' \oplus k_{12}$

    $x' = D'_{k_2}(c)$

    if $x' \in H$:

      return prob key is $k_{12}, k_2, H[x']$

  2 Time: $|K_2| - |K_{12}|$ Mem: 0



H :

$$\boxed{K_1 \cap K_2 = K_{12}}$$

Time K_{12}

```
for k_12 ∈ K_12 :
    // forward phase
    Initialize hashmap H.
    for k_1' ∈ K_1 / K_12 :
        k_1 = k_12 ⊕ k_1'
        x = E'_{k_1}(p)
        H[x] = k_1'
    // backward phase.
    for k_2' ∈ K_2 / K_12 :
        k_2 = k_12 + k_2'
        x = D'_{k_2}(c)
        if x ∈ H :
            return k_12, k_2', H[x].
```

often just an OR.

Mem: $K_1 \setminus K_{12}$

Time: $K_1 \setminus K_{12}$

Time: $K_2 \setminus K_{12}$

Total:

Mem: $|K_1 \setminus K_{12}|$

Time: $(|K_1 \setminus K_{12}| + |K_2 \setminus K_{12}|)\,|K_{12}|$

$= K_1 + K_2$

What to use for H

- Hashmap → Random access writes + reads.
- Array + Sort → Seq access writes + RA reads.

→ does it fit in Memory

- Array + Sort (x2) → Seq access writes + reads. → if it doesn't fit in memory.
  1. store all forward entries + sort
  2. store all backward entries + sort
  3. find matches between forward and backward entries.

It depends

A whole field of study on its own.

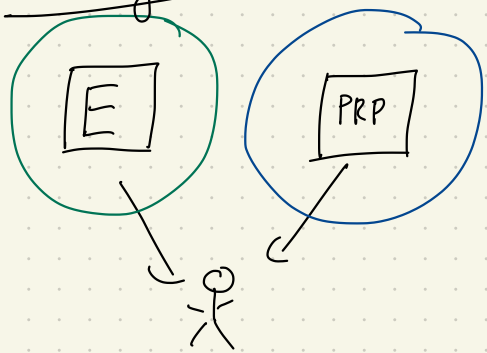
	insert	Read	Space	processing	
Hashmap	$O(1)$	$O(1)$	$c \cdot O(N)$	X	⇒ High constants/overheads
Array + Sort	$O(1)$	$O(\log(n))$	$O(N)$	$O(n \cdot \log(n))$	⇒ + Very low overhead + High I/O efficiency - processing can get too expensive.

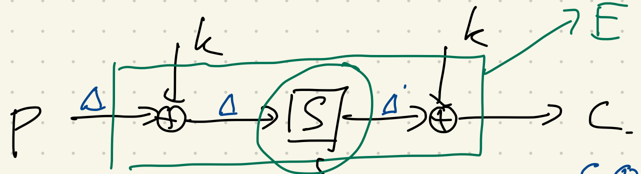
Actually since we have uniform random entries ⇒ $\log \log (n)$

We can do sorting in $O(N)$

Differential Cryptanalysis

Distinguisher





Lemma: given some PRP σ, σ'

$\sigma \oplus \sigma'$ is a PRF

$C_1 \oplus C_2 = \Delta_{out}$

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

$P_1 \oplus P_2 = \Delta_{in}$

$1 \rightarrow \Delta_{in}$

P_1	$P_1 \oplus \Delta$	$S(P_1) \oplus S(P_1 \oplus \Delta)$
0	1	$E \oplus B = 5$ (x2)
2	3	$4 \oplus 6 = 2$ (x2)
4	5	$A \oplus D = 7$ (x2)
6	7	$7 \oplus 0 = 7$
8	9	$3 \oplus 8 = B$
A	B	$F \oplus C = 3$
C	D	$5 \oplus 9 = C$
E	F	$1 \oplus 2 = 3$

$\uparrow \Delta_{out}$

$\Delta_{in} = 1 \qquad P_1 \oplus P_2 = 1$

$$\Delta_{out} = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & A & B & C & D & E & F \\ 0 & 0 & 2 & 4 & 0 & 2 & 0 & 4 & 0 & 0 & 0 & 2 & 2 & 0 & 0 & 0 \end{pmatrix} \rightarrow \text{sum} = 16.$$

Alg:

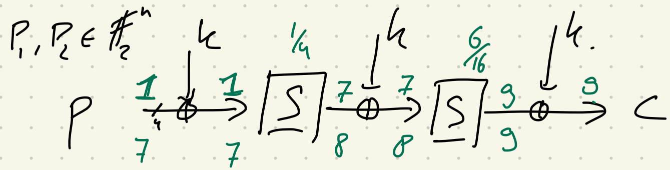
take P_1

compute $E(P_1) \oplus E(P_1 \oplus 1) = \Delta_{out}$

if $\Delta_{out} = 7$:

counter ++

$P_1, P_2 \in \mathbb{F}_2^n$



P_1, P_2

$\Delta_{in} = 1$

$$\begin{array}{l} \\ \Delta_{out} = \end{array} \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & A & B & C & D & E & F \\ 0 & 0 & 2 & 4 & 0 & 2 & 0 & 4 & 0 & 0 & 0 & 2 & 2 & 0 & 0 & 0 \end{pmatrix} \rightarrow \text{sum} = 16.$$

$7 \rightarrow 9$ with prob $\frac{36}{256} \geq \frac{1}{\rho}$.

$\frac{1}{\rho} = \frac{32}{256}$.

DDT → Difference Distribution Table.

Alg

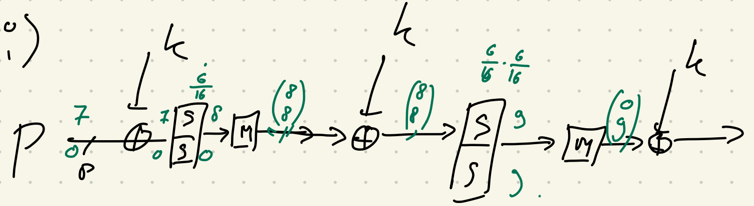
for all Δ_{in} :
  Init array of counters. Row
  for $x \in X$:
    $Row[S(x) \oplus S(x \oplus \Delta_{in})]$++.
  Add Row to DDT.
return DDT.

TC05 sbox DDT

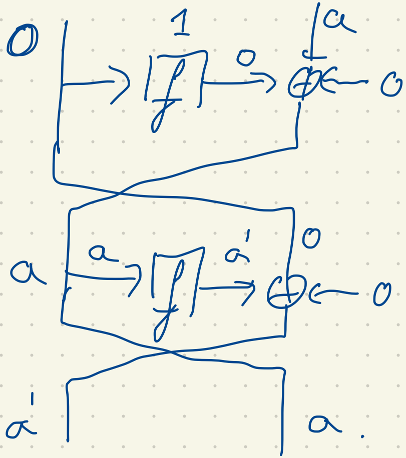
$4 \rightarrow 6$ $2 \rightarrow D$ $5 \rightarrow D$
$7 \rightarrow 9$ $9 \rightarrow 8$.

	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

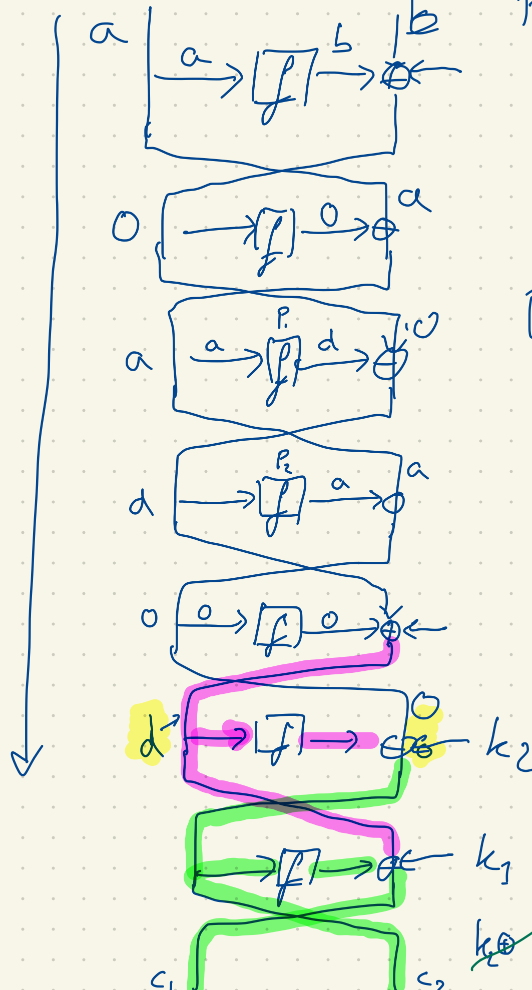
$M = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$



$2^{7} \cdot 2^{-4.25} = 2^{3} \cdot \left(\frac{6}{16}\right)^{3} \approx 2^{-4.25}$



plaintext



ciphertext

$P_1 \cdot P_2$.

for each k_1

if Eq 1:

add point to k_1

pick the k_1 with highest points

Eq 1

$$\cancel{k_2 \oplus}\ f\big(f(c_2)\oplus c_1 \oplus k_1\big) \oplus f\big(f(c_2')\oplus c_1' \oplus k_1\big) \cancel{\oplus k_2} = c_2 \oplus c_2'$$

Project

$\boxed{\text{vote for project}}$

1. LWC candidates $\Rightarrow$ analyze.
2. Competition
   - $\rightarrow$ You desing a cipher.
   - $\rightarrow$ Others analyse your cipher.
3. Automated analysis.

$\Rightarrow$ Individual.

The sbox S is defined as follows:

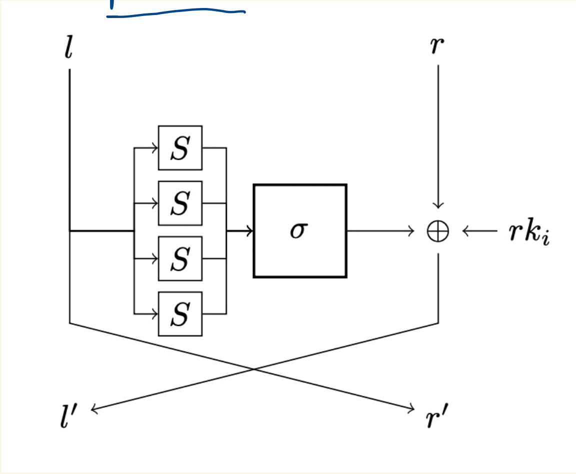
$$S = (\texttt{E, B, 4, 6, A, D, 7, 0, 3, 8, F, C, 5, 9, 1, 2})$$

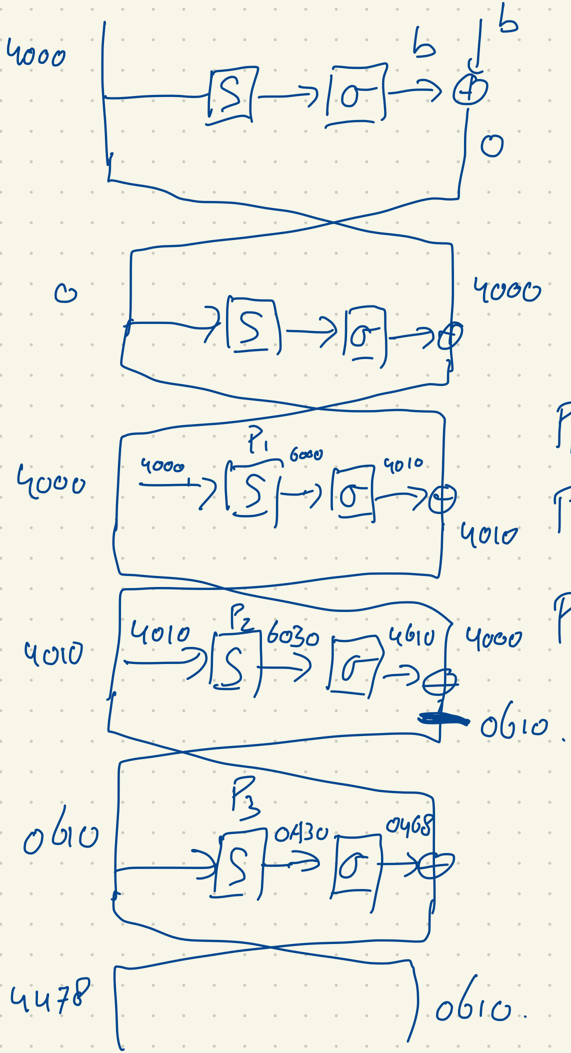
and the bit permutation σ is defined as follows:

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

```
[16  0  0  0  0  0  0  0  0  0  0  0  0  0  0  0]
[ 0  0  2  4  0  2  0  4  0  0  0  2  2  0  0  0]
[ 0  0  0  0  4  0  0  0  0  0  2  2  2  6  0  0]
[ 0  0  0  0  0  0  0  4  4  0  4  0  0  0  0  4]
[ 0  2  0  2  2  0  6  0  0  0  0  0  0  0  4  0]
[ 0  4  0  2  2  0  0  0  0  0  2  0  0  6  0  0]
[ 0  0  2  0  0  2  0  0  0  2  4  4  0  0  2  0]
[ 0  2  0  0  0  0  2  0  0  6  0  0  4  0  2  0]
[ 0  0  2  2  2  0  2  0  0  0  2  2  0  2  0  2]
[ 0  2  0  2  0  2  2  0  6  2  0  0  0  0  0  0]
[ 0  2  2  0  0  0  0  4  0  2  0  2  0  0  2  2]
[ 0  0  2  0  2  4  0  0  2  0  0  0  4  0  2  0]
[ 0  0  2  0  2  4  0  0  2  2  0  2  2  0  0  0]
[ 0  0  2  0  0  0  2  4  0  0  0  2  0  0  4  2]
[ 0  4  0  0  2  2  0  0  2  2  0  0  0  0  0  4]
[ 0  0  2  4  0  0  2  0  0  0  2  0  2  2  0  2]
```

TC05





$2^{32}.$

$P_1 = \frac{6}{16}$

$P_2 = \frac{6}{16} \cdot \frac{4}{16}$

$P_3 = \frac{4}{16} \cdot \frac{4}{16}.$

$$P_1 \cdot P_2 \cdot P_3 = \left(\frac{6}{16}\right)^2 \cdot \left(\frac{4}{16}\right)^3 = 9 \cdot 2^{-12} = 2^{-8.83}$$

		1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
	[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]

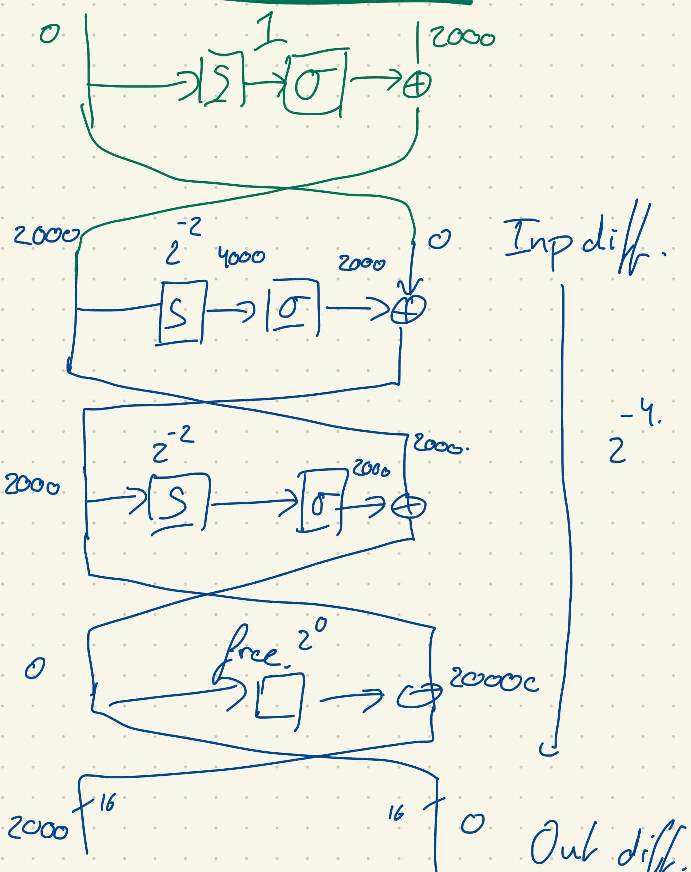
The sbox S is defined as follows:

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

and the bit permutation σ is defined as follows:

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

Lecture 6.



		1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
	[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]

The sbox S is defined as follows:

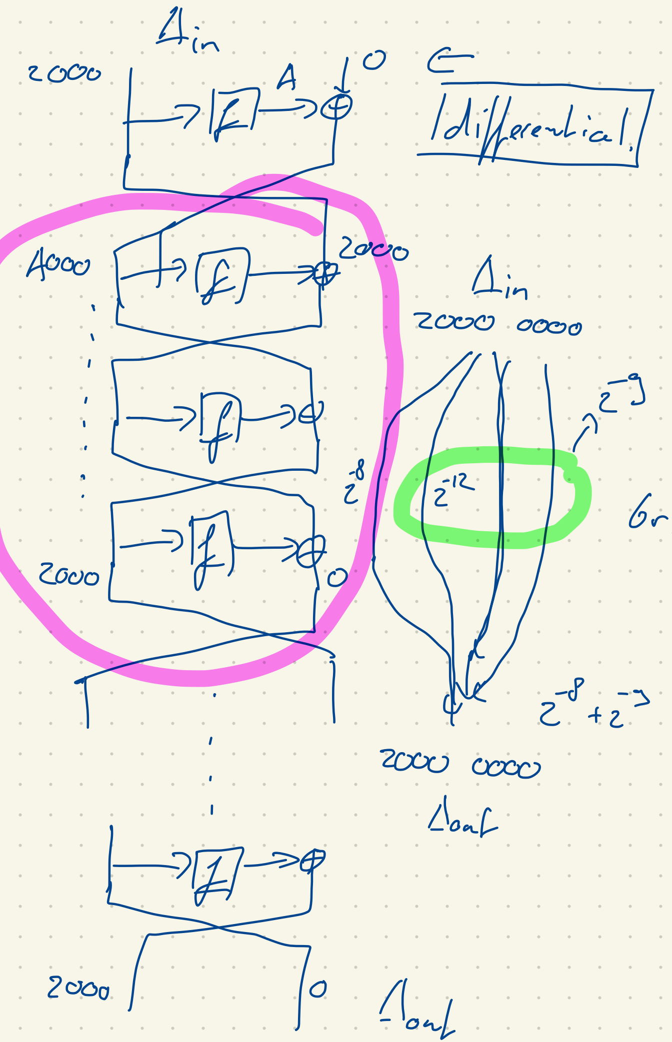
$$S = (\mathtt{E},\ \mathtt{B},\ \mathtt{4},\ \mathtt{6},\ \mathtt{A},\ \mathtt{D},\ \mathtt{7},\ \mathtt{0},\ \mathtt{3},\ \mathtt{8},\ \mathtt{F},\ \mathtt{C},\ \mathtt{5},\ \mathtt{9},\ \mathtt{1},\ \mathtt{2})$$

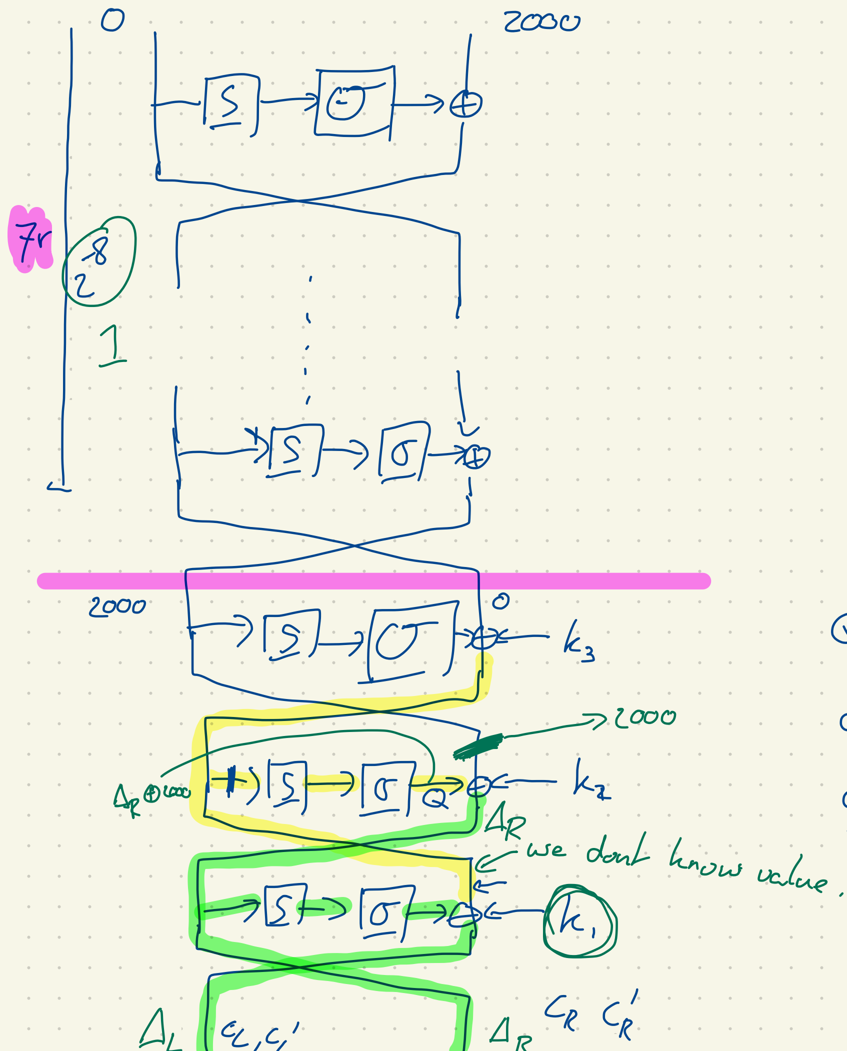
and the bit permutation σ is defined as follows:

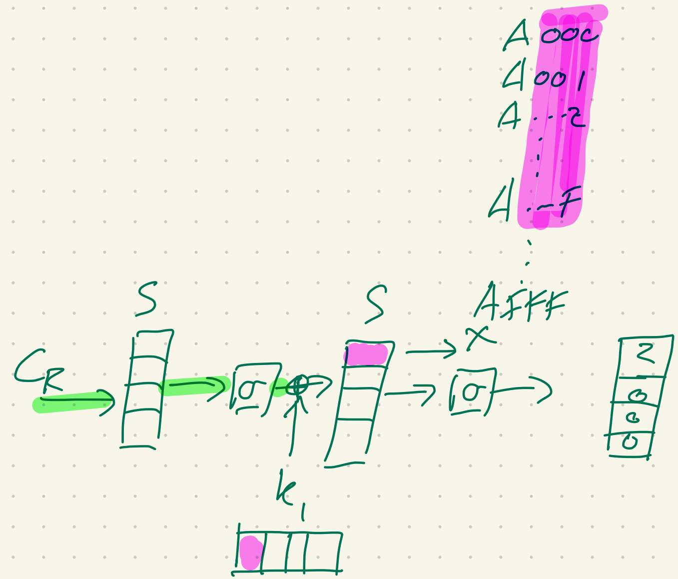
$$\sigma = \left(\begin{array}{cccc|cccc|cccc|cccc} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & A & B & C & D & E & F \\ 6 & 0 & 1 & 7 & E & 8 & 9 & F & 2 & 4 & 5 & 3 & A & C & D & B \end{array}\right)$$

$4000 \longrightarrow 2000$

```
test_diff_char(inp_diff, out_diff, nrof_samples):
    counter = 0
    for i ≤ nrof_samples:
        pick P1 uniform random.
        P2 = P1 ⊕ inp_diff.
        C1 = encrypt(P1)
        C2 = encrypt P2
        Δout = C1 ⊕ C2
        if Δout == out_diff:
            counter ++.
    return counter/nrof_samples.
```







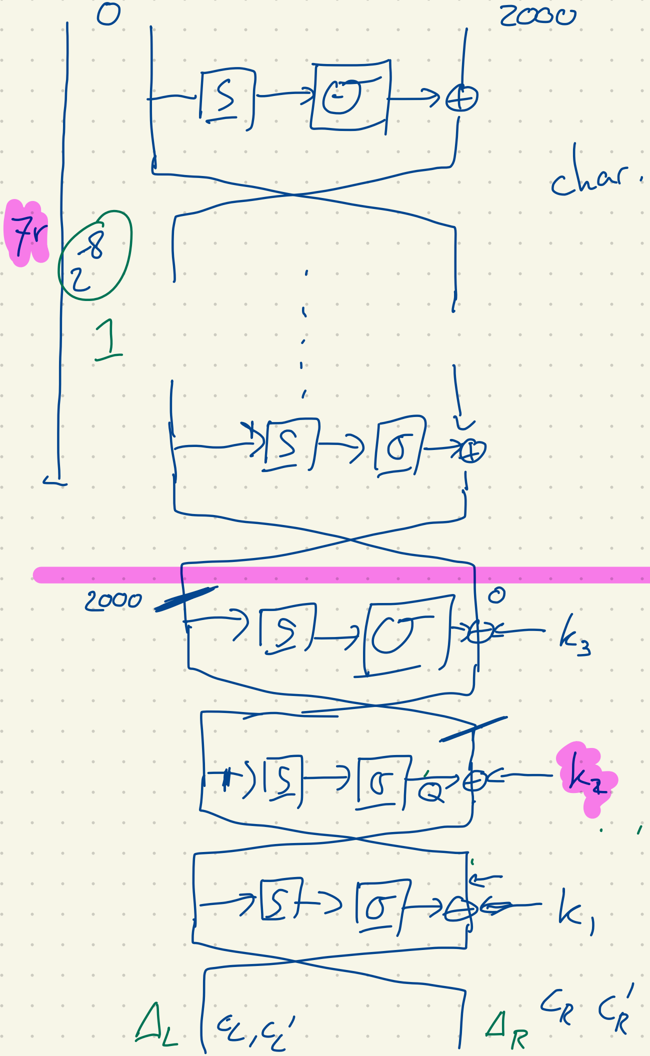
$$Q = q \oplus q'$$

$$q = \sigma(S(\sigma(S(C_R)) \oplus k_1 \oplus C_L))$$

$$q' = \sigma(S(\sigma(S(C'_R)) \oplus k_1 \oplus C'_L))$$

$$Q = \Delta_R \oplus 2000$$

↳ candidate for k_1



attack(Δ_{in}, Δ_{out}, char. rounds, pairs):

- for $k_1 \in K_1$:
  - counter = 0
  - for p_1, p_2, c_1, c_2 in pairs:
    - c_1' = decrypt(c_1, k_1, 10-cr.)
    - c_2' = ...
    - if $c_1' \oplus c_2' = \Delta_{out}$:
      - counter++
  - if counter $\geq 2^{-8} \cdot |pairs|$:
    - output k_1 as prob key.

m-bits of the key

Prob p charact.

T: $2^m \cdot \frac{1}{p} \cdot c$

M: P

Data: P

Implementation Guide:

1. encrypt / decrypt + test.
2. design attack. → test the characteristic.
3. implement partial encrypt/decrypt. + test.
4. Implement the attack w. key guessing.
   ↳ run with known key.

$k_1 = 0x1234$

2^{16}

for $k_1 \in K_1$

for $k_1 \in [0x1230 \ldots 0x123F]$