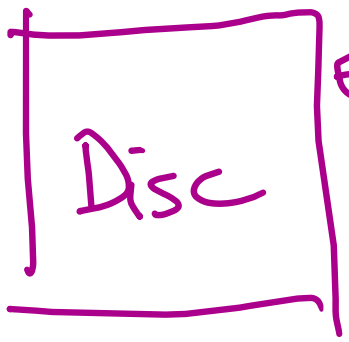
C&S

24.11.2021



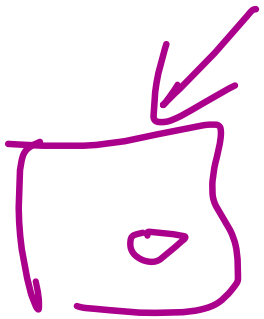
external key:

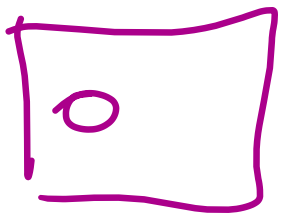
- hardware stick

- password

$= X_1 \otimes X_2$

entropy?

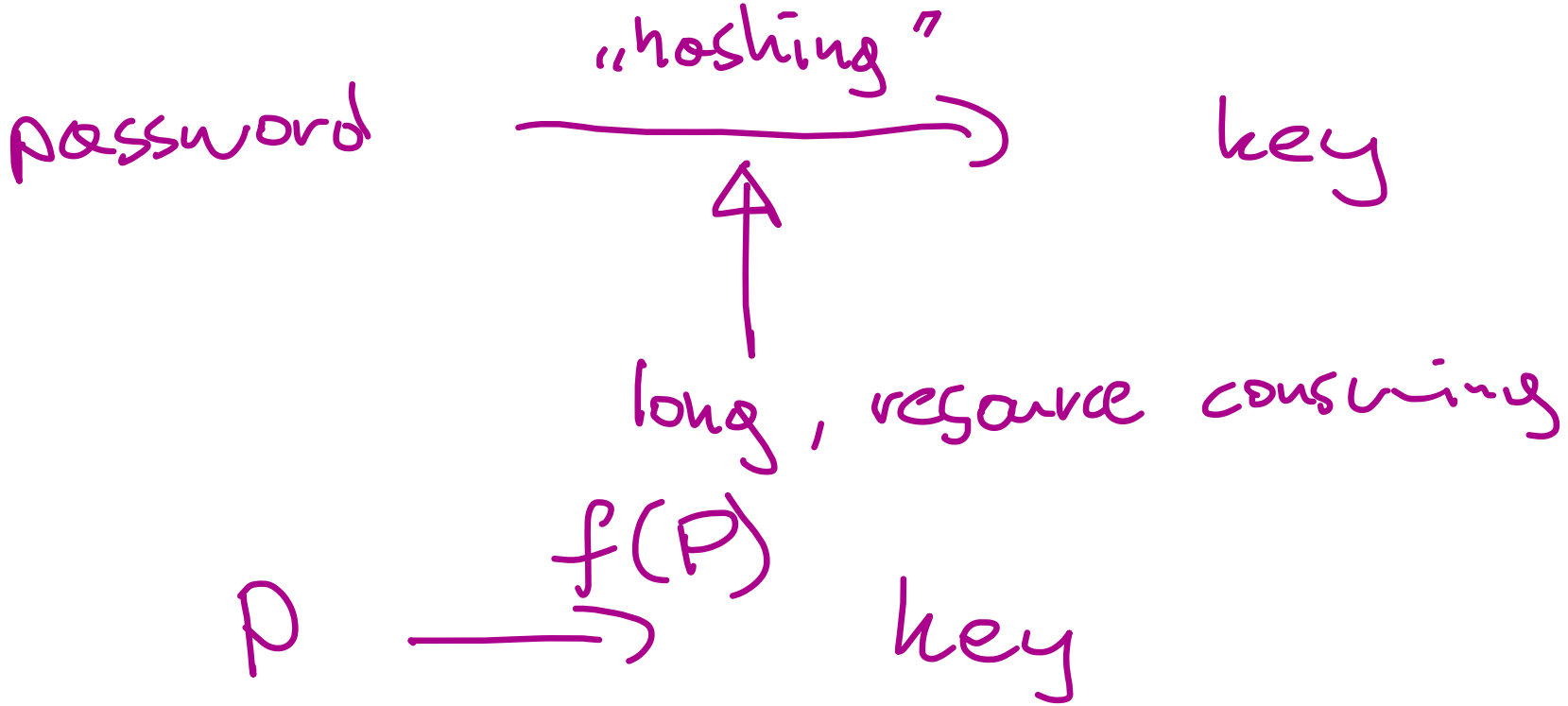




Attack: brute force

try decrypt

if password used as a key



f - space complexity is

~~4~~ 6 GB

time is:

≈ 2 sec.

- flexibility (eg. memory)
- unfriendly to GPU, FPGA, ...

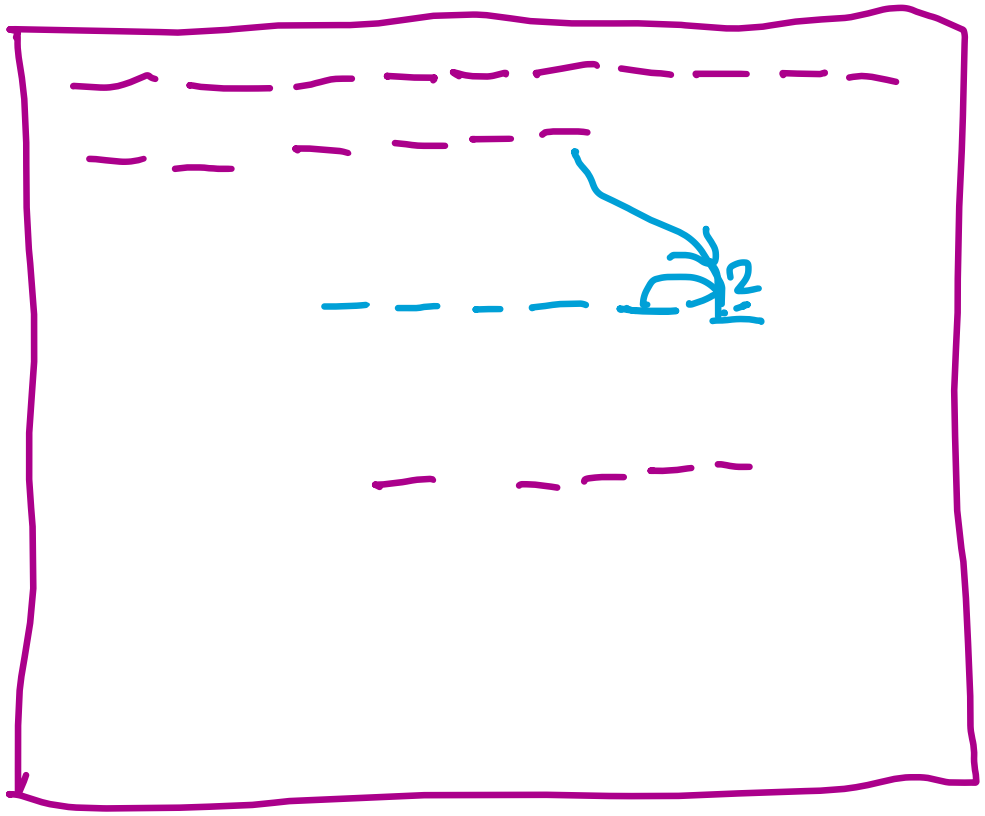
Idea:

hash chain:

$x, H(x), H(H(x)), \ldots$

$x, H(x), H(H(x), x), \ldots$

memory

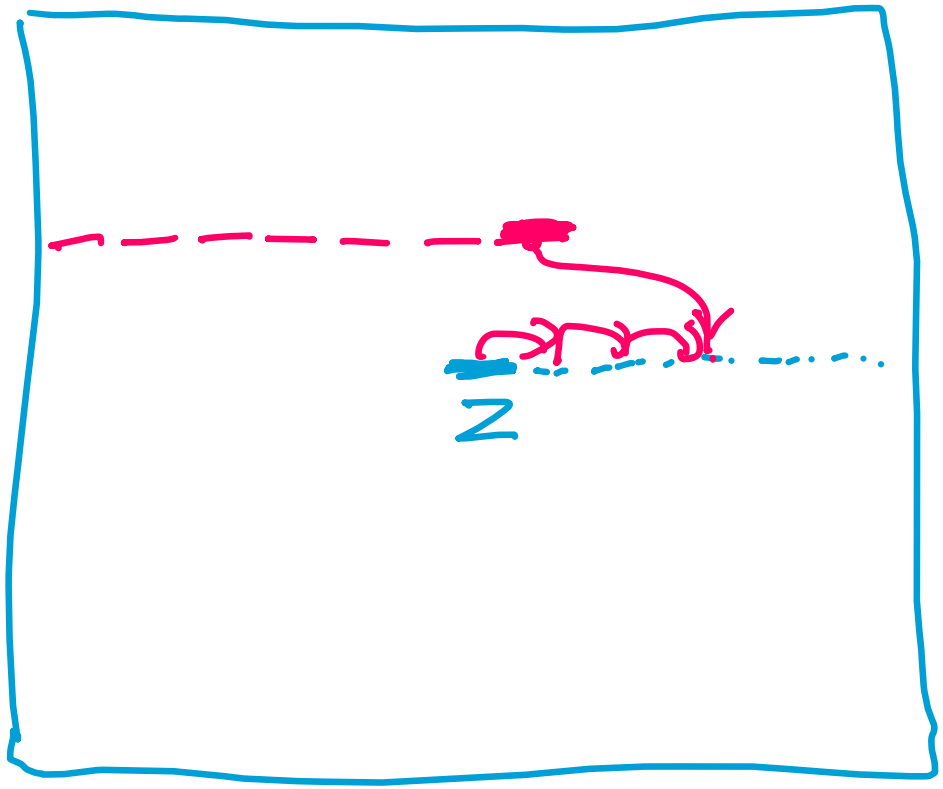


1) fill sequential

$H^k(x) = z$

$|z| = 128$

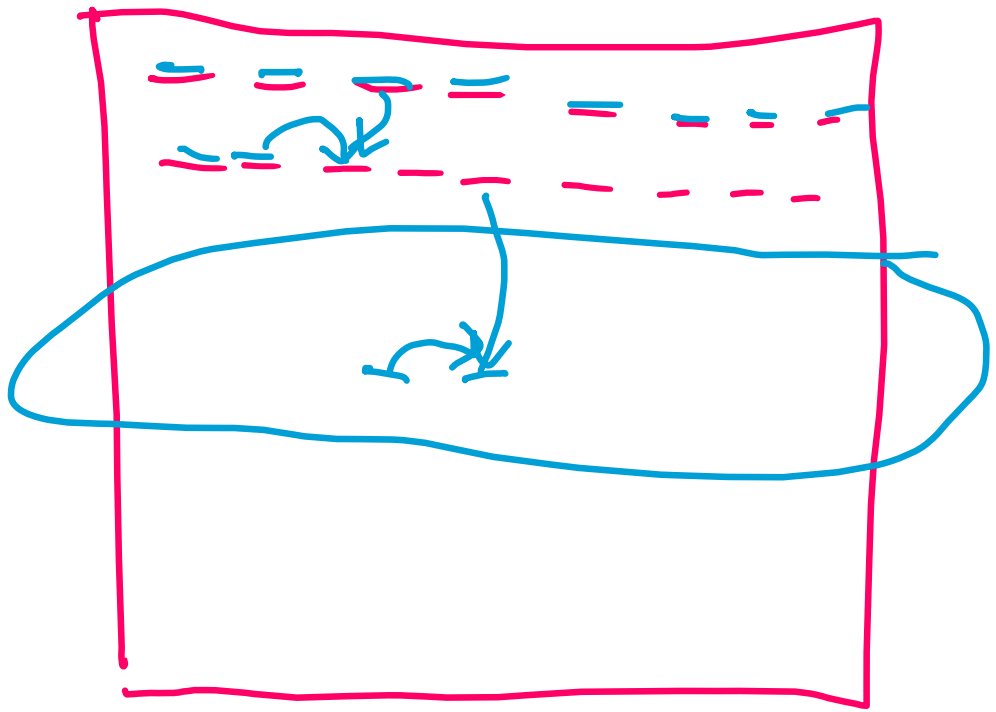
~~2^{128}~~



z

2^{128}

Transformation



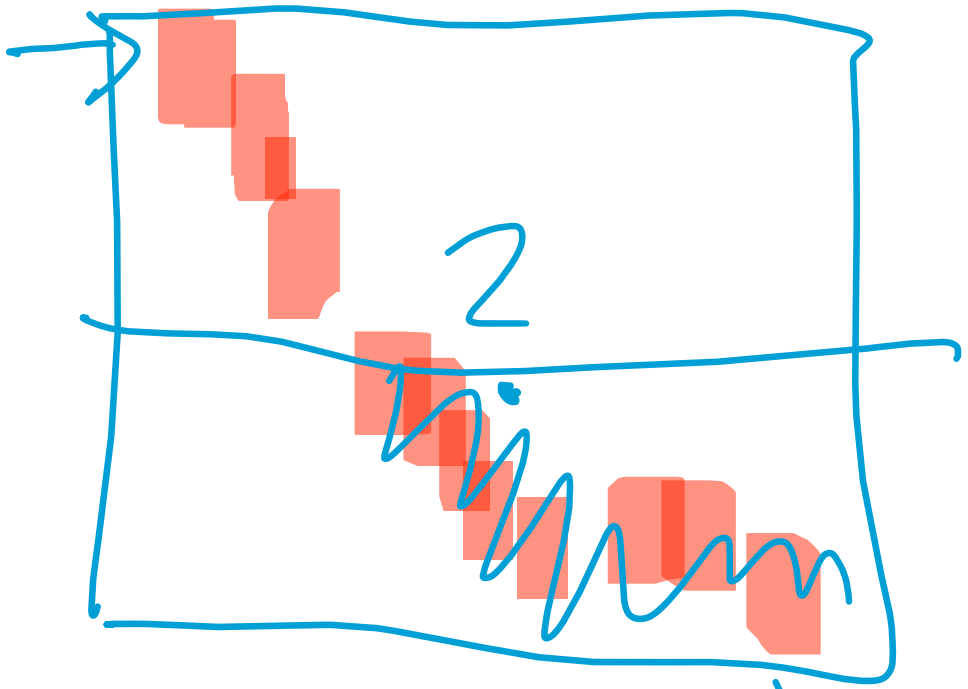
attacks:

trade-off:

recompute

Many transformation

cannot forget



h( ) → key

last round must be executed

- computation in place

encrypt in place