An untwisted representation of AES

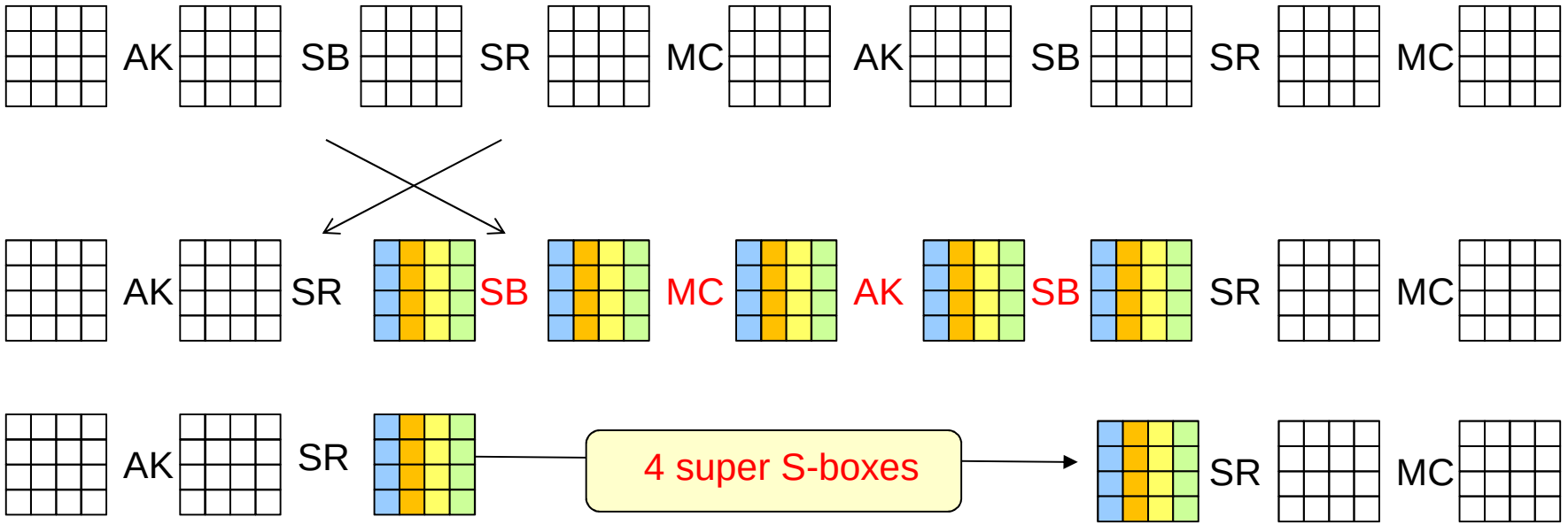
ESC 2013

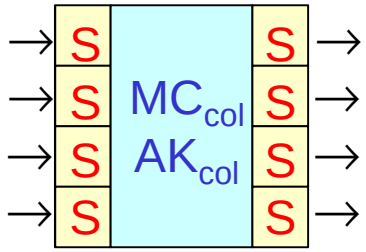
Henri Gilbert, ANSSI

henri.gilbert@ssi.gouv.fr

starting point: super S-box notion [DR06]

- equivalent representation of 2 consecutive AES rounds





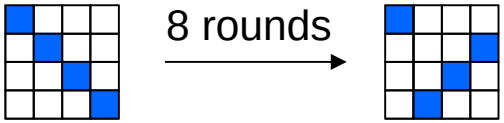
one super S-box

super S-boxes: applications

- analysis of 2-round differentials [DR06]

- extended rebound attacks against AES-like permutations [GP09, LMRRST09]
  - the « known key distinguisher » against 8-round AES of [GP09]

    produces a pair of plaintext blocks that satisfies the truncated differential:



    complexity: about 2^{48} AES operations; 2^{64} for the best known generic attack

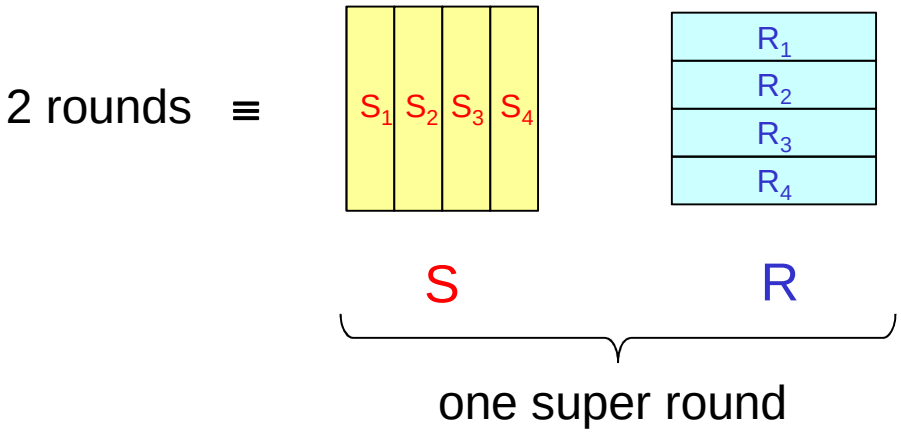
- many applications to the cryptanalysis of AES-like hash functions
  - such as Whirlpool, ECHO, and Grøstl, e.g. [MPRS10], [JNS11], [JNP12]

objective: untwisted 2-round representation

- start from the super S-box representation of 2 rounds

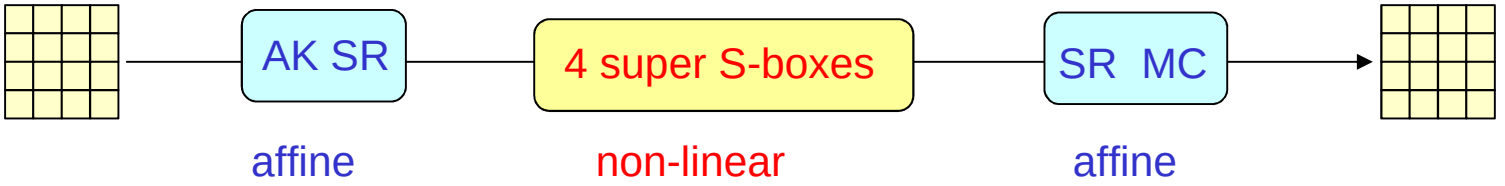
  « eliminate ShiftRows » to get a simplified view

- equivalent view of 2 consecutive rounds as the composition of
  - a nonlinear transformation: essentially 4 parallel « super S-boxes »
  - an affine transformation: essentially 4 parallel « MixRows »



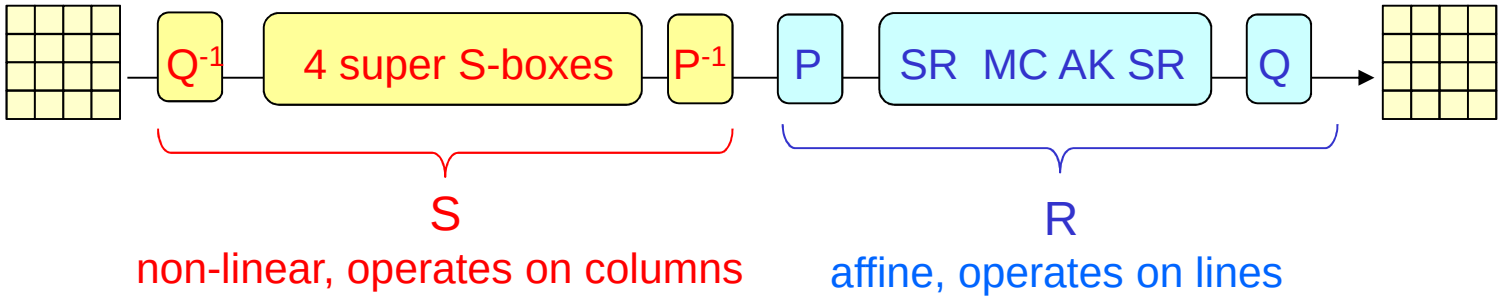
how to move to an untwisted representation (1/2)

- **step 1:** 2-rounds representation using super S-boxes



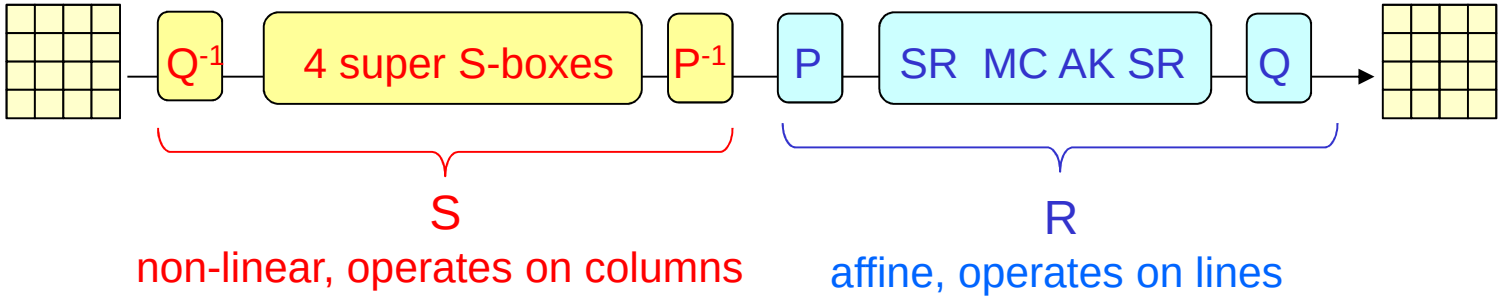
or equivalently (up to a cyclic shift of the periodic 2-round pattern)

- **step 2:** composition with well chosen byte permutations P and Q and their inverses



how to move to an untwisted representation (2/2)

- **problem:** find suitable byte permutations P and Q at step 2



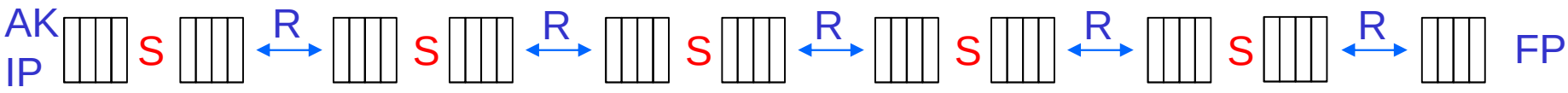
- **solution:** $P = SR\ T\ SR^{-1}$ and $Q = SR^{-1}\ T\ SR\ SC$

  where: T = matrix transposition ; SC (SwapCols) = swapping of columns 2 et 4

- **proof sketch:**
  - P and Q can be shown to operate on columns, therefore **S operates on columns**
  - R can be expressed (after simplification) as: $R = SR\ (T\ MC\ AK\ T)\ SR\ SC$

    since T MC T, SR, and SC operate on lines, **R operates on lines**

equivalent representation of 10-round AES



10 full rounds

IP et FP: initial and final byte permutations (no or little influence on security)

can such a representation be helpful ?

- most natural application target
  - structural cryptanalysis of round-reduced AES or AES-based hash functions

- work in progress on one first application
  - extension of Knudsen and Rijmen's known key distinguisher of [KR07] from 7-round AES to 8-round AES
  - whether this 8-round distinguisher can or not be extended to more rounds requires further analysis

block ciphers attack models (rough outline)

- usual attack model
  - the adversary is given a « black box » (oracle) access to an instance of the primitive associated with a random secret key and its inverse
  - attack purpose: distinguish the primitive from a random permutation

- known key model [KR07]
  - the adversary is given a « white box » access to a random instance of the primitive and its inverse, i.e. to a random key value
  - attack purpose: exhibit a difference of behaviour with a random permutation Π^*

    by constructing «abnormally correlated » (input, output) pairs

- other attack models (not addressed here)
  - chosen key attacks: exhibit a difference of behaviour with an ideal cipher (Π_K^*)

    by constructing «abnormally correlated » (key, input, output) triplets
  - related key attacks: chosen modifications of unknown keys…

known key attack (informal definition)

known key attack of order t and distinguisher R against a block cipher E

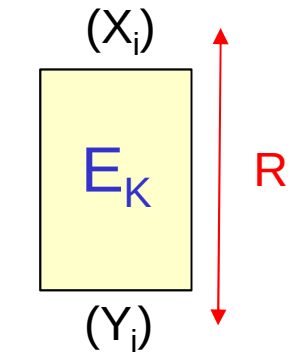
- an algorithm A that on input a key K derives in time T:

  - a t-tuple $X = (X_i)$ of n-bit plaintext blocks;

  - a t-tuple $Y = (Y_i)$ de of ciphertext blocks,

  related

  - by $Y_i = E_K(X_i)$ [i=1 to t] **and** by a relation X R Y named a distinguisher

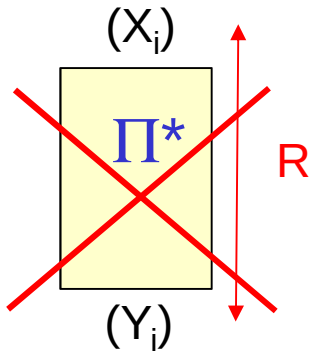


- the relation R must be:

  - independent of key K;
  - efficiently checkable;
  - « abnormal » : given a random permutation Π^* of $\{0,1\}^n$

    it must be impossible to construct $X = (X_i)$ and $Y = (\Pi^*(X_i))$ s. t.. X R Y

    in time T with a significant success probability



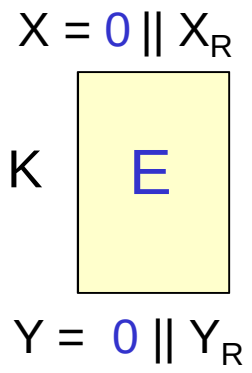
known key attacks: examples

- example of an attack of order 1

(X,Y) that satisfies the following distinguisher R:

$X_L = Y_L = 0$

derived from K in time $T << 2^{n/2}$



- example of an attack of order 2 and link with hashing

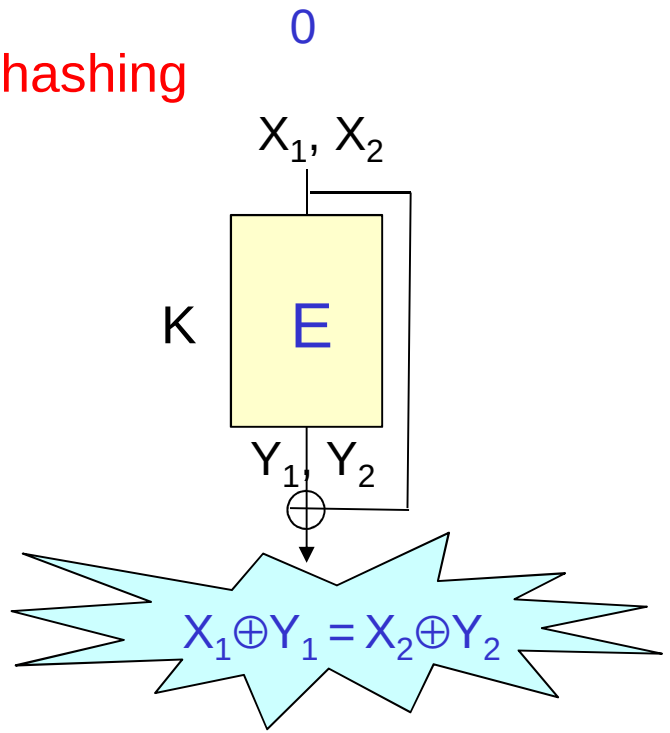
(X_1,Y_1) et (X_2,Y_2) that statisfy the following distinguisher R:

$X_1 \oplus Y_1 = X_2 \oplus Y_2$ and $X_1 \neq X_2$

derived from K in time $T << 2^{n/2}$

$\rightarrow$ the Davies-Meyer construction applied to E

is not collision resistant



resistance against known key attacks

- closely related to the notion of « correlation intractability » [CGH04]

- no block cipher s.t. |key| ≤ |block| is secure under these notions !

  let us for instance assume |key| = |block| = n bits

  let us consider R defined by: X R Y iff $Y = E_X(X)$

  - given K, X = K et the associated ciphertext $Y = E_K(K)$ are related by R
  - given Π^*, finding X, Y s.t. X R Y, i.e. $\Pi^*(X) = E_X(X)$ is difficult

- how to circumvent this difficulty in the case of AES-128 ?
  - stating that the former relation R is artificial is unsatisfying…
  - broaden the key space

    by incorporating both K and arbitrary S-boxes into the key

    the considered distinguishers are then « structural »

    i.e. satisfied by a larger family of algorithms that possess the same overall structure

this solution wil be retained in the sequel

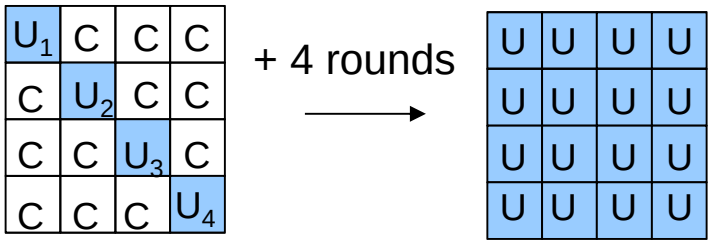
known key attack against $AES_{7rounds}$ [KR07] (1/2)

exploits « integral » properties of the encryption and decryption functions

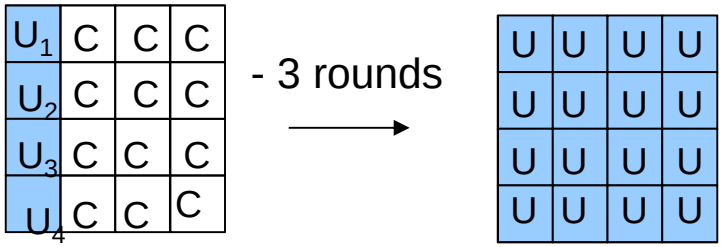
notation: one considers the encryption or decryption of $N = 2^{8t}$ blocks

- a byte is marked C (constant) it takes one single constant value
- a byte x is marked U (uniform) if each of the 256 possible byte values occurs N/256 times
- a quartet (x_1, x_2, x_3, x_4) is marked (U_1, U_2, U_3, U_4) if each of the 2^{32} possible quartet values occurs $N/2^{32}$ times

encryption, $N = 2^{32}$ or a multiple of 2^{32}

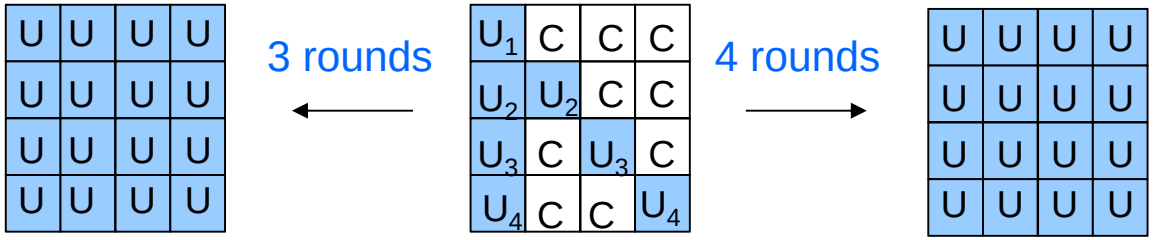


decryption, $N = 2^{32}$ or a multiple of 2^{32}



known key attack against $AES_{7rounds}$ [KR07] (2/2)

$N = 2^{56}$ blocks



resulting known key attack:

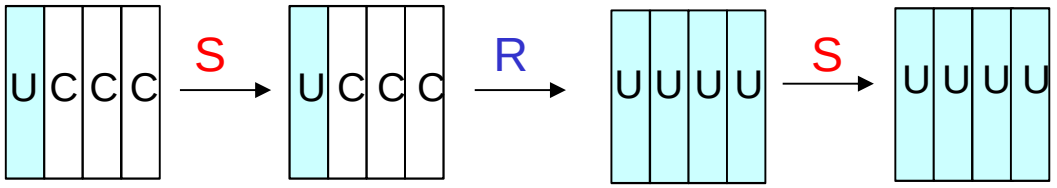
- distinguisher: input and output property U
- complexity: $T = 2^{56}$
- it is conjectured (not proven) that no generic attack with the same distinguisher and the same complexity exists

generalisation: 7 to 8 rounds of Rijndael for blocksizes of 160 to 256 bits [MPP09]

extension: known key attack against $AES_{8rounds}$

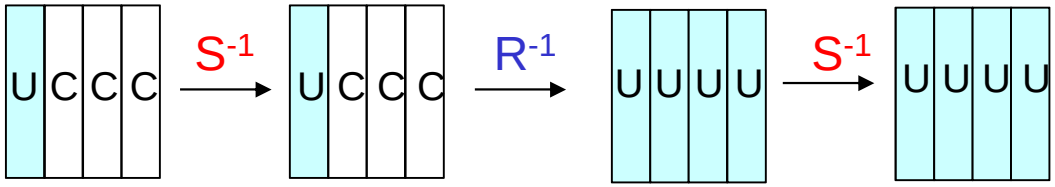
encryption of a structure X made of 2^{32} blocks

$X = \{(x_i,a,b,c)\}$



decryption of a structure Y made of 2^{32} blocks

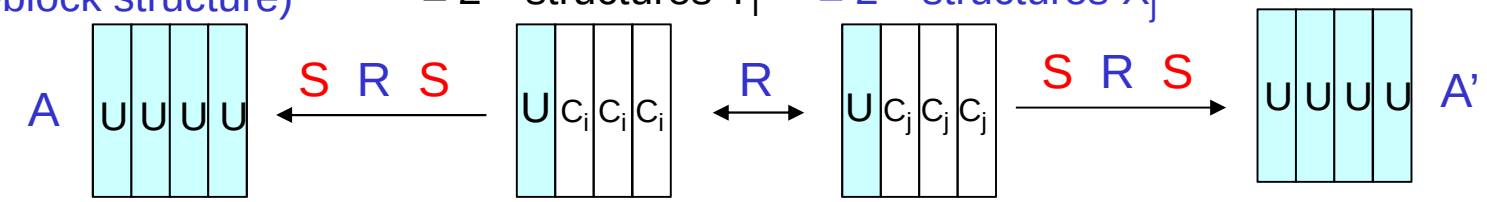
$Y = \{(y_j,e,f,g)\}$



Z: melting of X and Y
(2^{64} -block structure)

$R^{-1}(Z) = Y+L^{-1}(X)$
$\equiv 2^{32}$ structures Y_i

$Z = X+RY = X+LY+cst$
$\equiv 2^{32}$ structures X_j



- distinguisher: input and output property U up to the affine mappings A and A'
- complexity: $T = 2^{64}$
- it is conjectured (not proven) that for this distinguisher no generic attack in time T exists

concluding remarks

- the former 8-round distinguisher is outperformed by the one of [GP10]
- work in progress: analyse whether it can be extended to more rounds