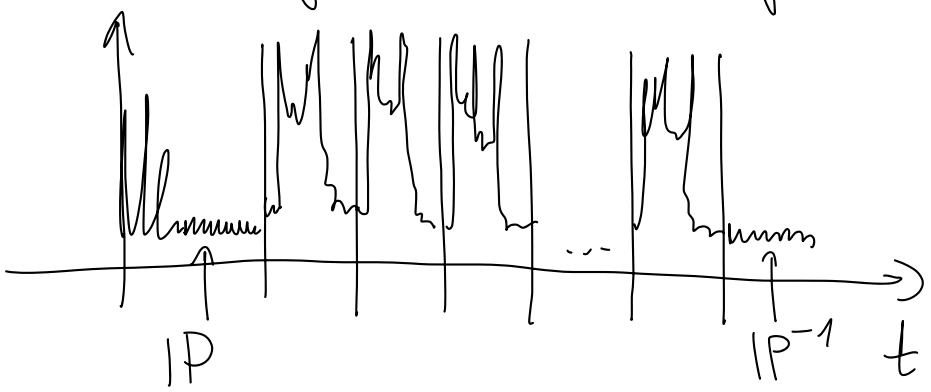
DES

1) Side channel attacks

- czas enc / dec
- zużyta energia (natężenie prądu)



- CPU / zdarzenie / pompa code

2) Fault attacks

Wymuszenie błędu

Wniosek: NIE WYMYŚLAJ I NIE IMPLEMENTUJ KRYPTOSYSTEMÓW

---

3) Atak kwantowy

1) Algorytm Shora : faktoryzacja
2) Algorytm Grovera : wyszukiwanie

DES 2^{56}

Grover → $2^{56/2} = 2^{28}$

$f: \underbrace{X}_{n \text{ el.}} \to \{0,1\}$

$f(x) = 1 \Rightarrow x$?

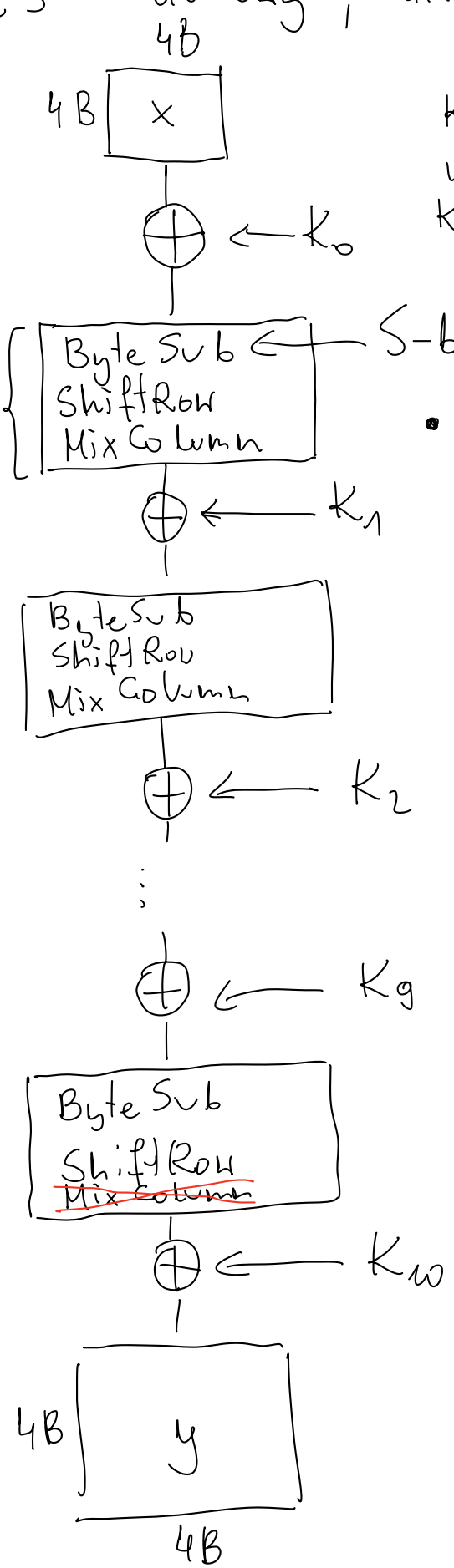
$\sqrt{n}$

$$f(k) = \begin{cases} 1, & e(k,x) = y \\ 0, & \text{w pozostałych} \\ & \text{razie} \end{cases}$$

AES (Advanced enc. standard)

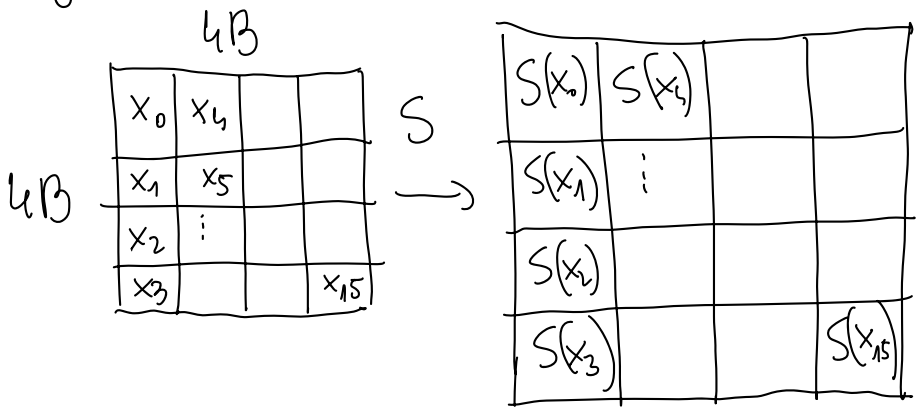
2.01.1997	NIST AES?	128 b. bloku
12.09.1997	wymagania NIST	(128, 196, 256 b. ← dł. klucza)
15.06.1998	21 kandydatów	
20.08.1998	15 — " —	(Pierwsza konf. kandydatów)
03.1999	Druga konf. kand.	
08.1999	5 finalistów: MARS, RC6, Rijndael, Serpent, Twofish	
04.2000	Trzecia konf.	
2.10.2000	Wybór Rijndael	(Daemen, Rijmen)
28.02.2001	Ogłoszenie standardu NIST	(do dyskusji)
26.11.2001	Przyjęcie standardu AES.	

AES blocuri, dl. bloc 128 b. / dl. cheie 128 / 196 / 256
Lizibe runde: 10, 12, 14

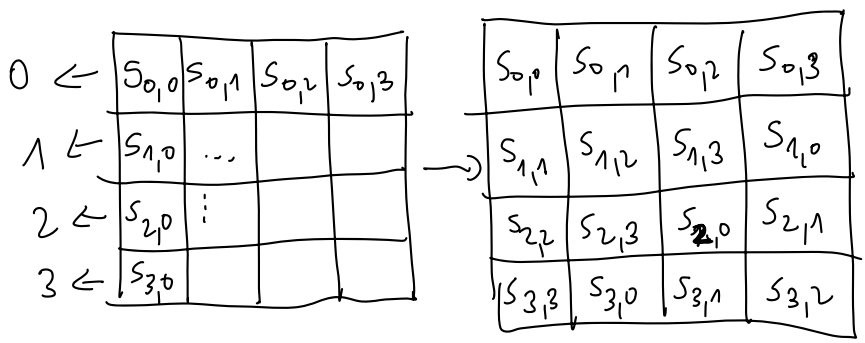


K - 128 b 16B
↓
$K_0, K_1, \dots, K_{10}$ ← $11 \cdot 16B = 176B$

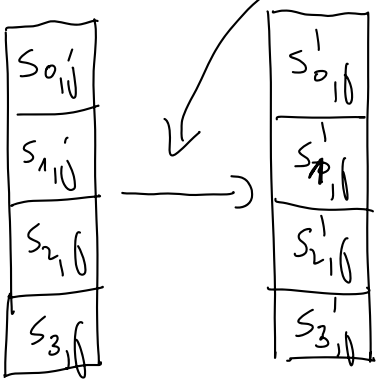
• Byte Sub S-box $S: \{0,1\}^8 \to \{0,1\}^8$



• Shift Row



• Mix Column — înmulțire prin matrice



$M_{4\times4} \cdot \begin{bmatrix} s_{0,0} \\ s_{1,0} \\ \vdots \end{bmatrix} = \begin{bmatrix} s'_{0,0} \\ \vdots \end{bmatrix}$

Kompromis między wielkością kodu a szybkością

code size vs performance tradeoff

	code size	perf
tablicowany wszystko 24KB 4KB	duży	najszybsze
tablicowany S-box	mały	wolny / szybki
bez obliczeń wstępnych	najmniejszy	najwolniejszy

Intel, AMD

x86

- aesenc ← runda 1..9
- aesenclast ← ostatnia runda
- aeskeygenassist ← klucz

GB/s

14 x szybsze niż software

SSD