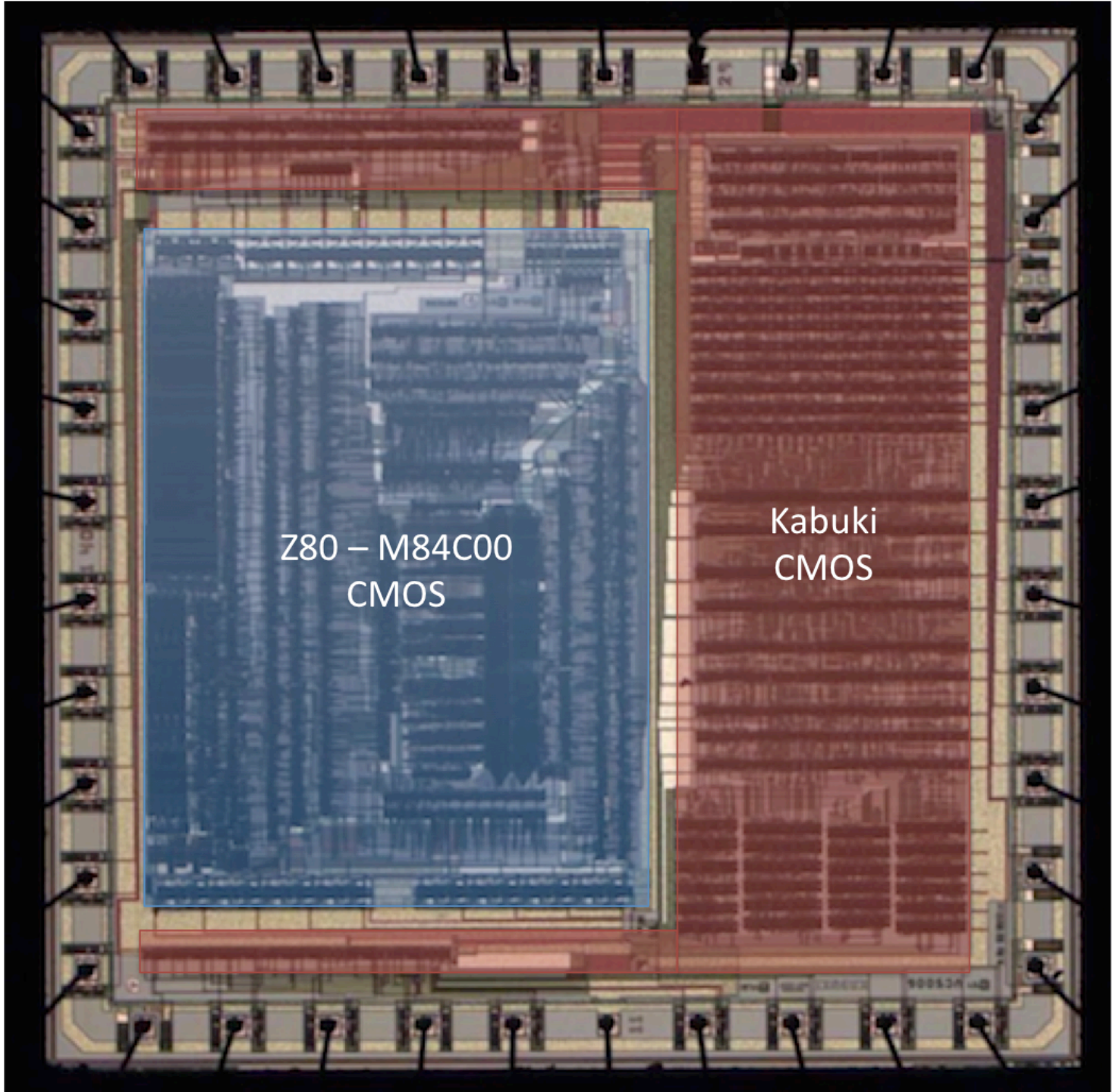
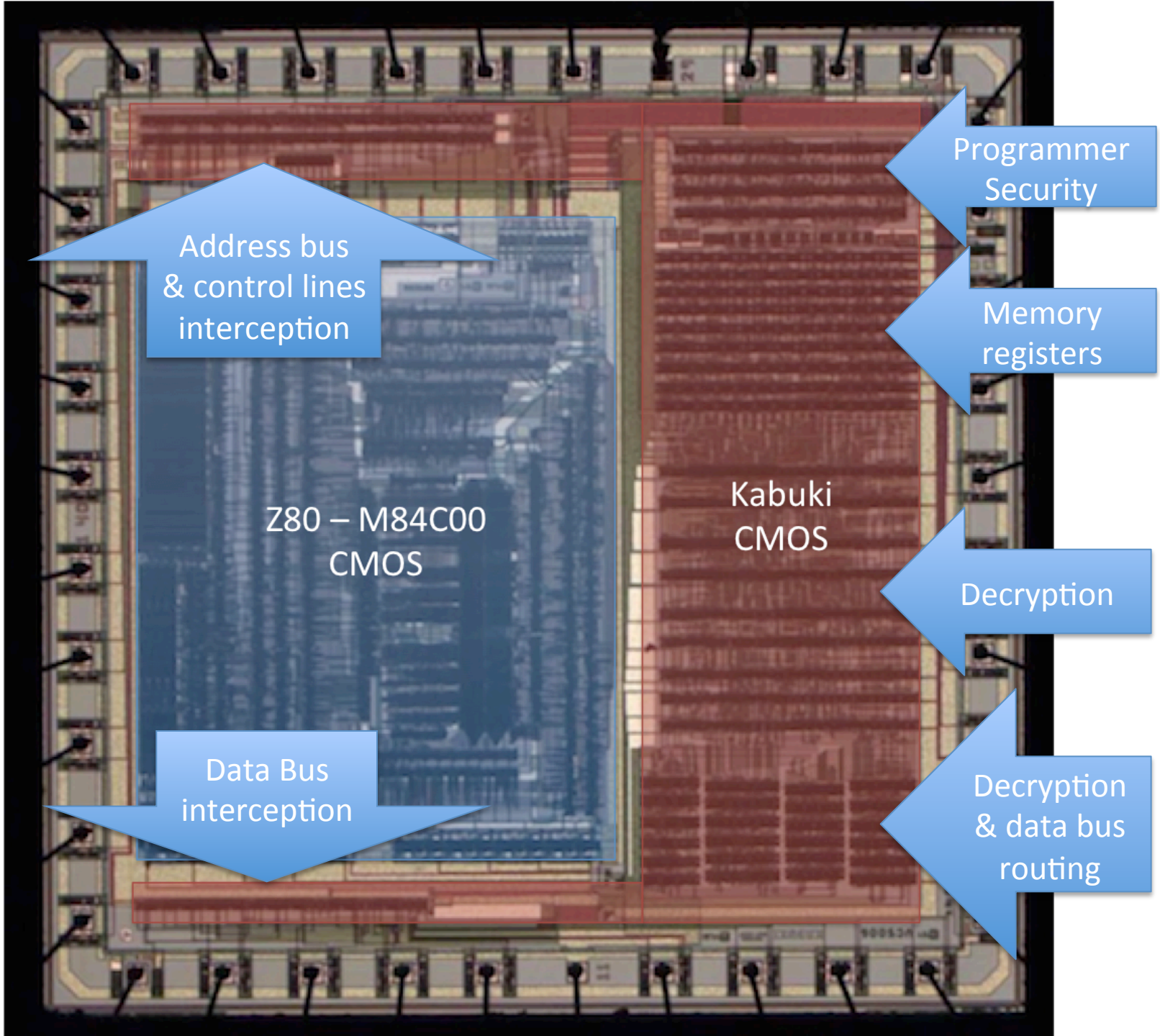
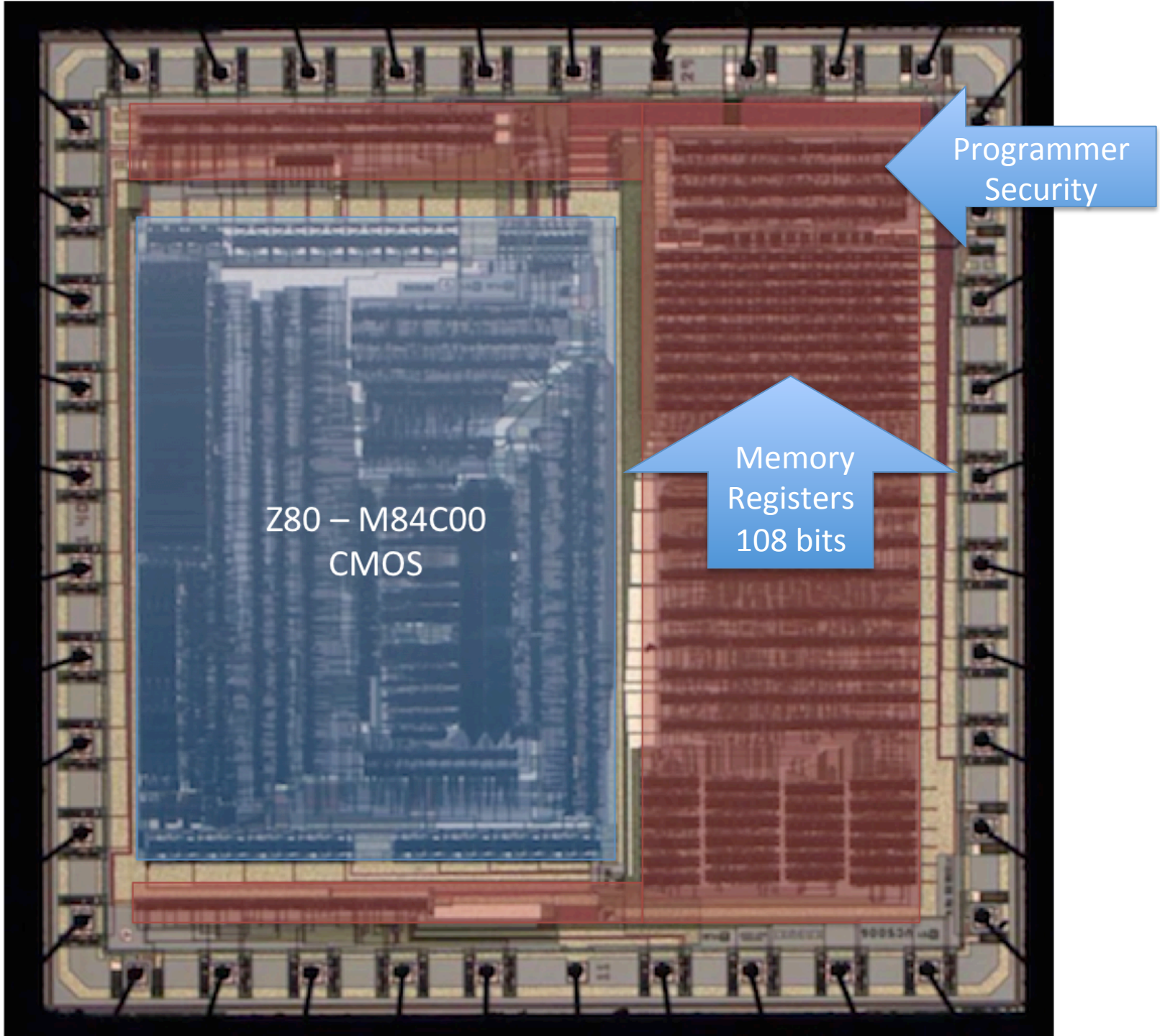

Z80 – M84C00
CMOS
Kabuki
CMOS


Programmer Security
Address bus & control lines interception
Memory registers
Z80 – M84C00 CMOS
Kabuki CMOS
Decryption
Data Bus interception
Decryption & data bus routing


Programmer
Security
Z80 – M84C00
CMOS
Memory
Registers
108 bits

Kabuki Programmer

- Gatekeeper
  - Controls writing to memory registers
- Security
  - Prevents outsiders from reprograming the cpu

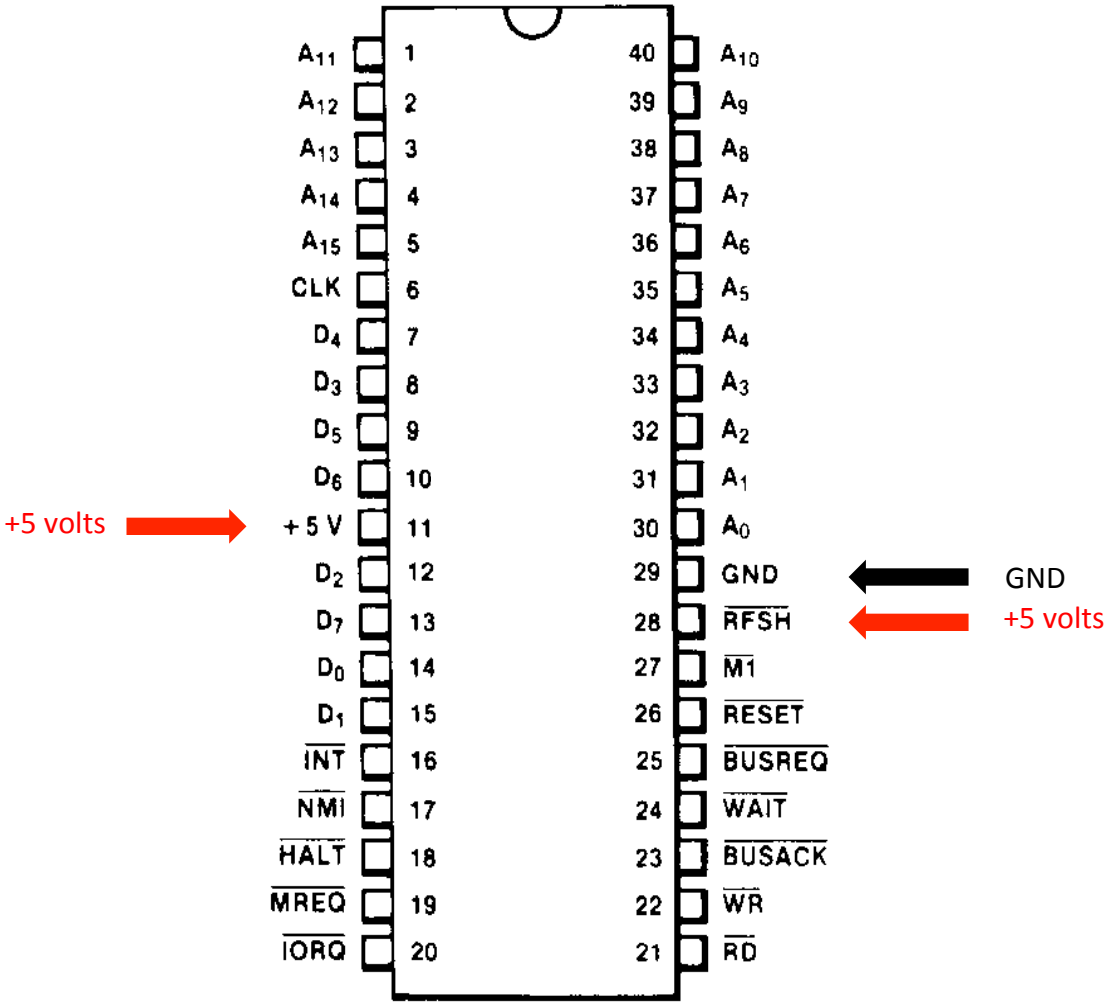
Kabuki Memory registers

- 108 x 1 bit registers
  - Layout: Serial in. Parallel out.
  - 72 bits: Decryption keys
  - 16 bits: Memory decryption area definition
  - 20 bits: Working memory

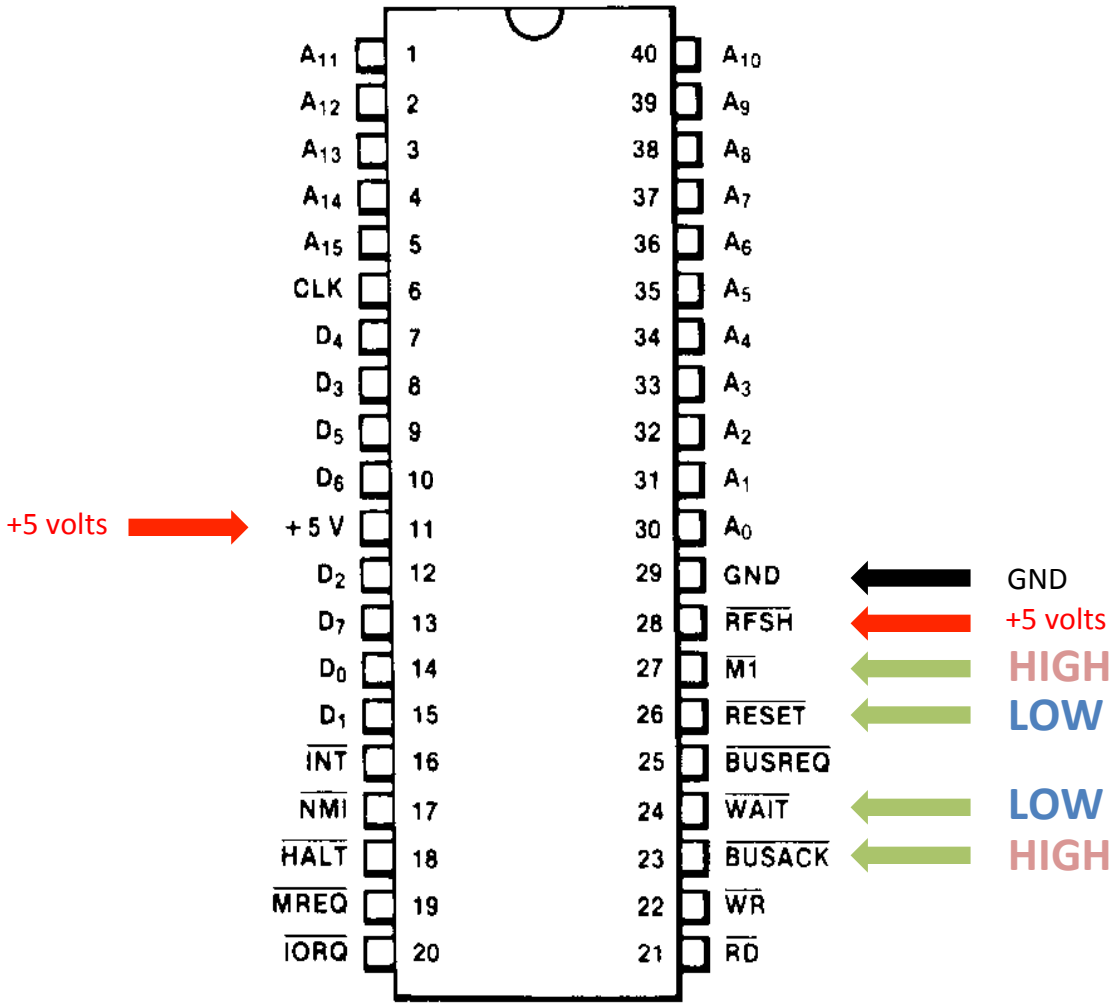
Kabuki Programmer

- Security implementation
  - Not trivial: multi stage with significant obfuscation
  - Required de-processing of several cpu layers
  - Security Stages
    - **#1** Signal setup
    - **#2** Secret Door knock 1
    - **#3** 20 bit Secret key – Hardware obfuscated
    - **#4** Secret Door knock 2

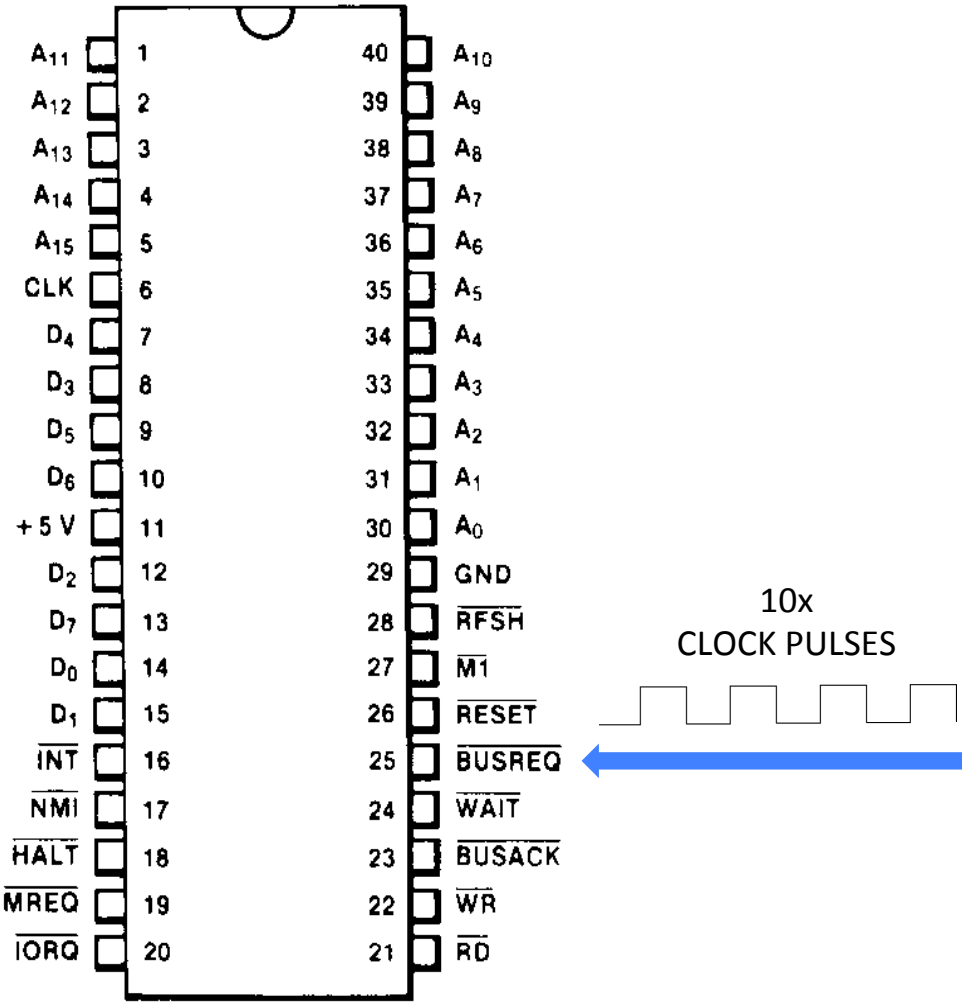
Stage 1 – Signal setup



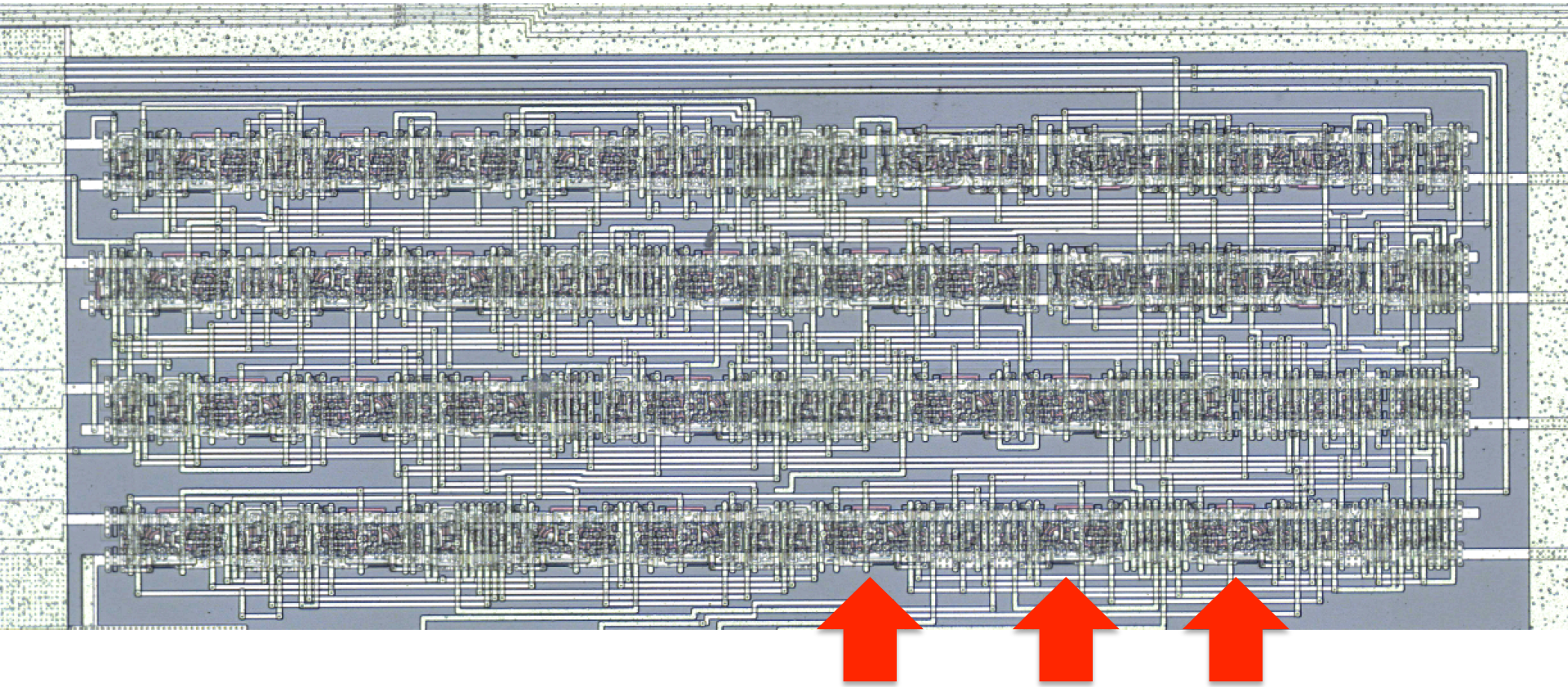
Stage 1 – Signal setup



Stage 2 – Door knock 1

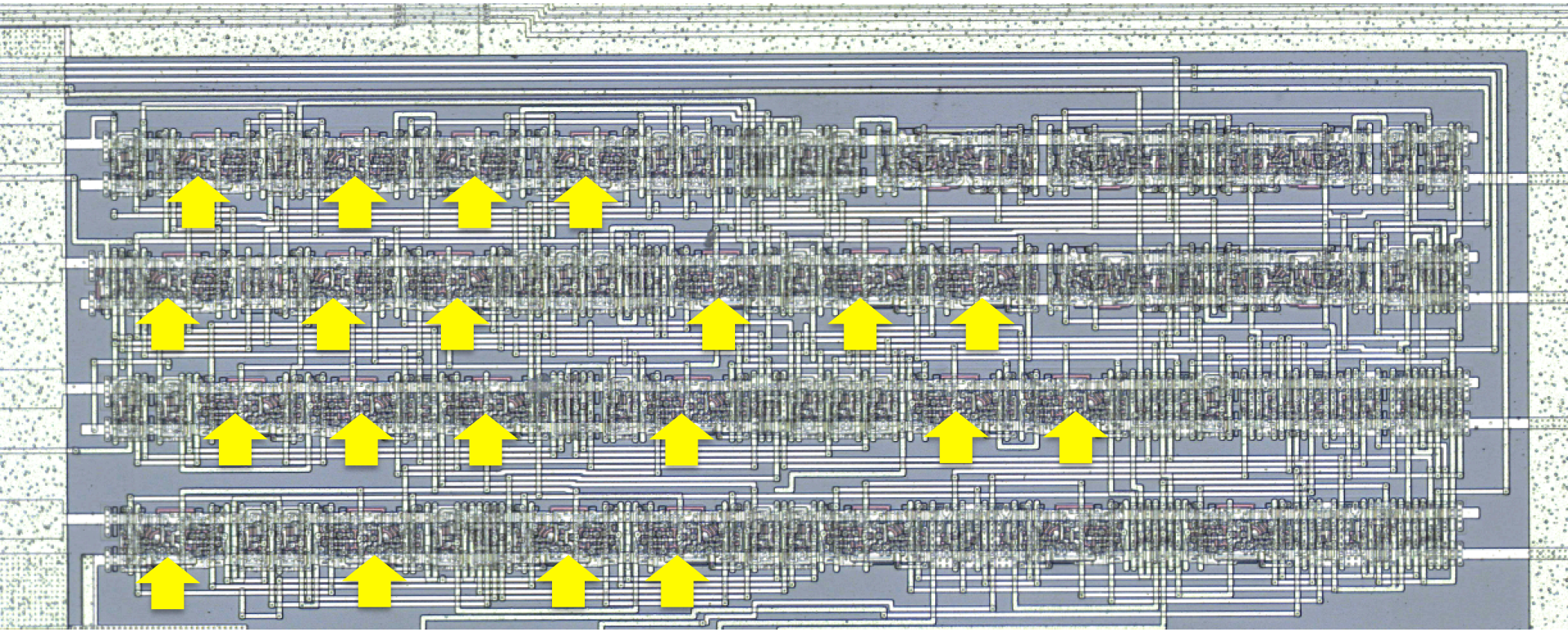


Stage 2 – Door knock 1



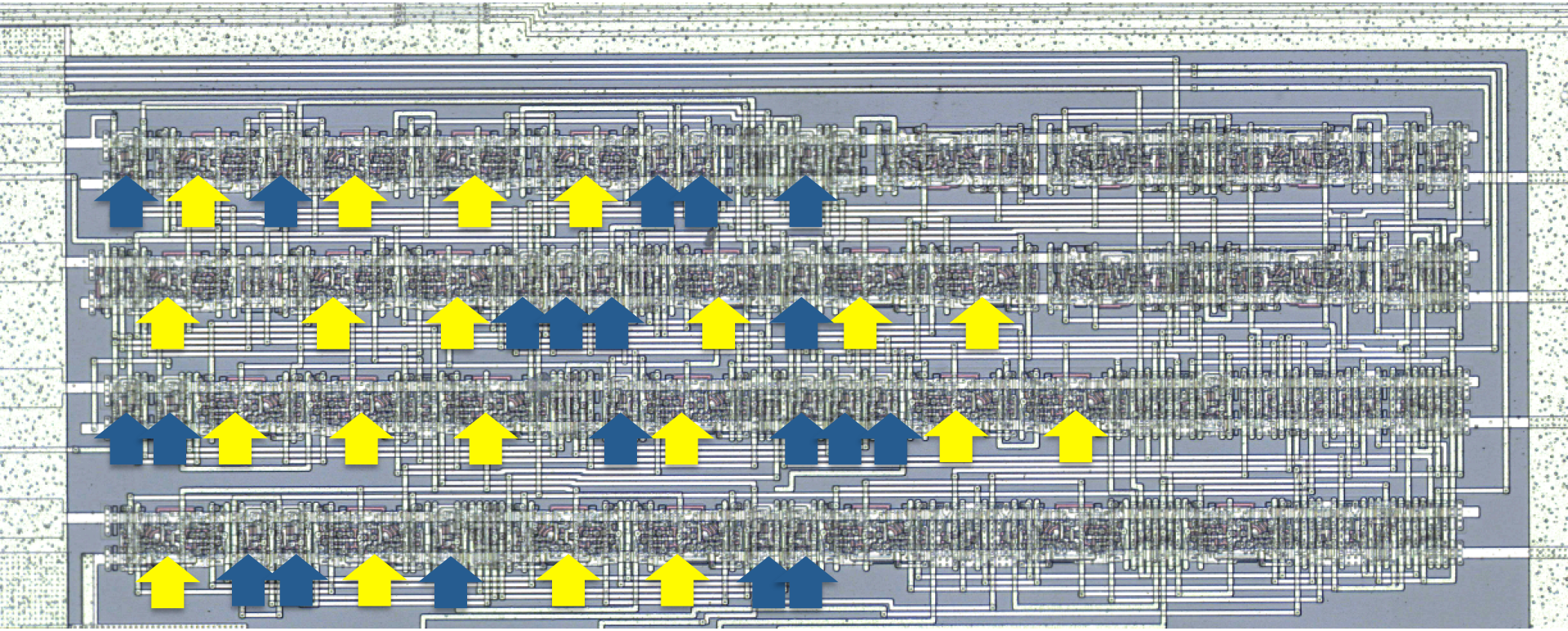
Memory registers
1 bit each

Stage 3 – 20 bit secret key



Memory registers serially connected

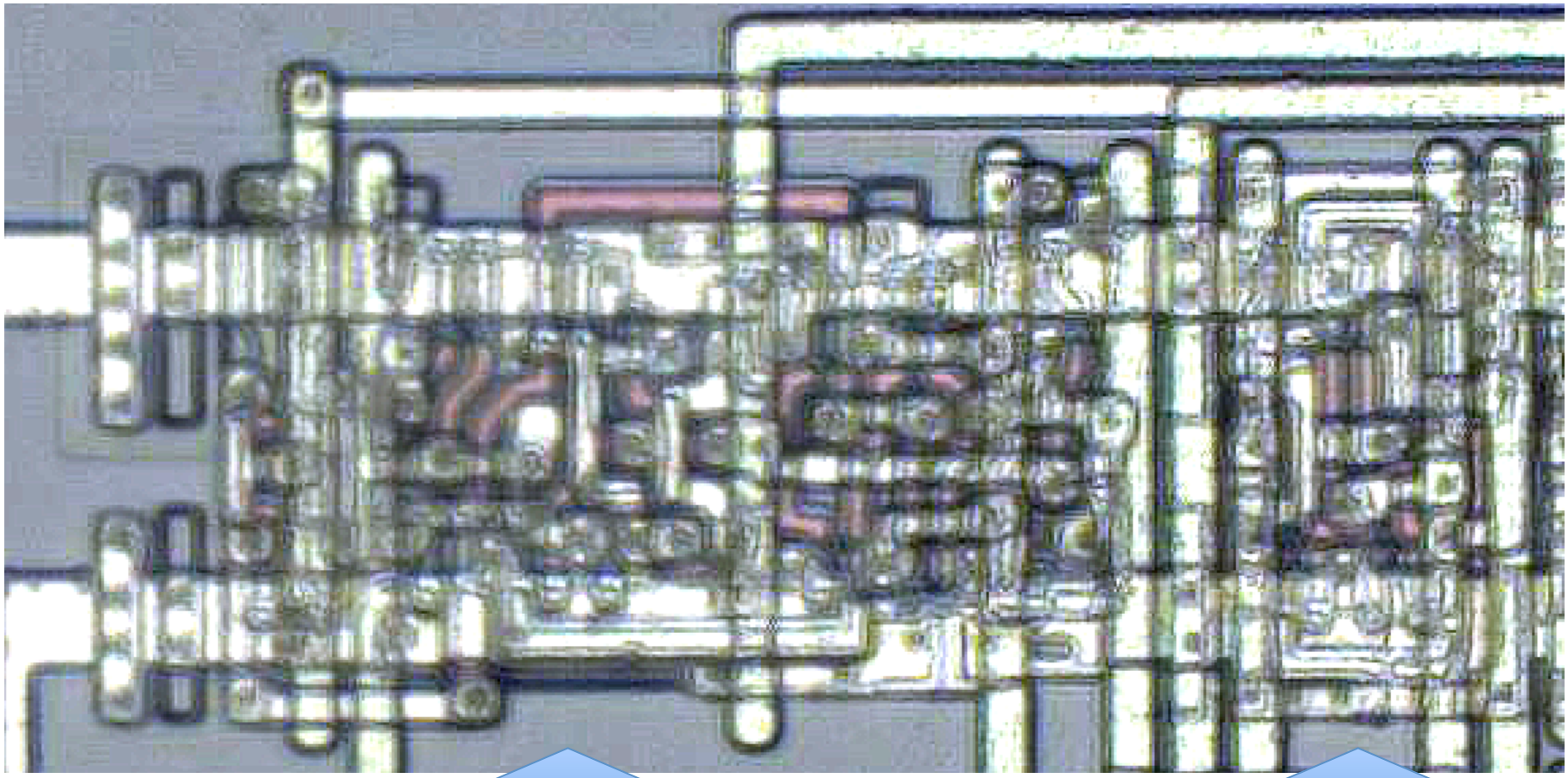
Stage 3 – 20 bit secret key



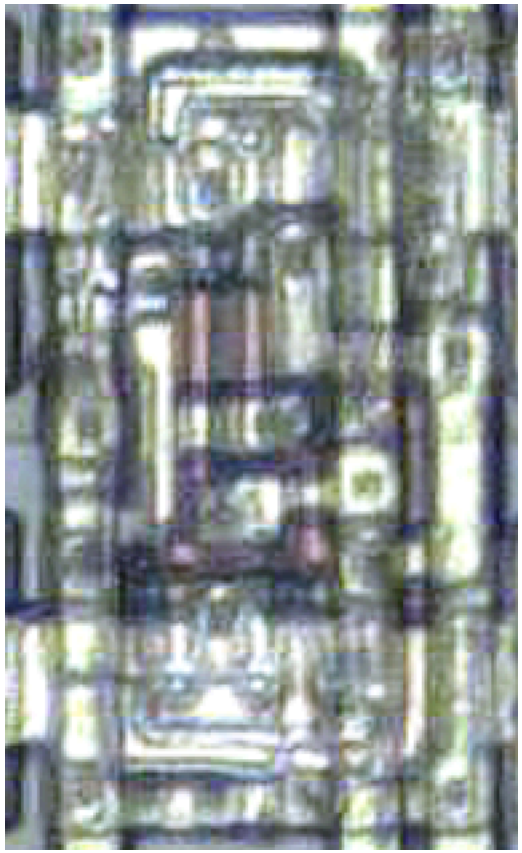
Memory registers serially connected

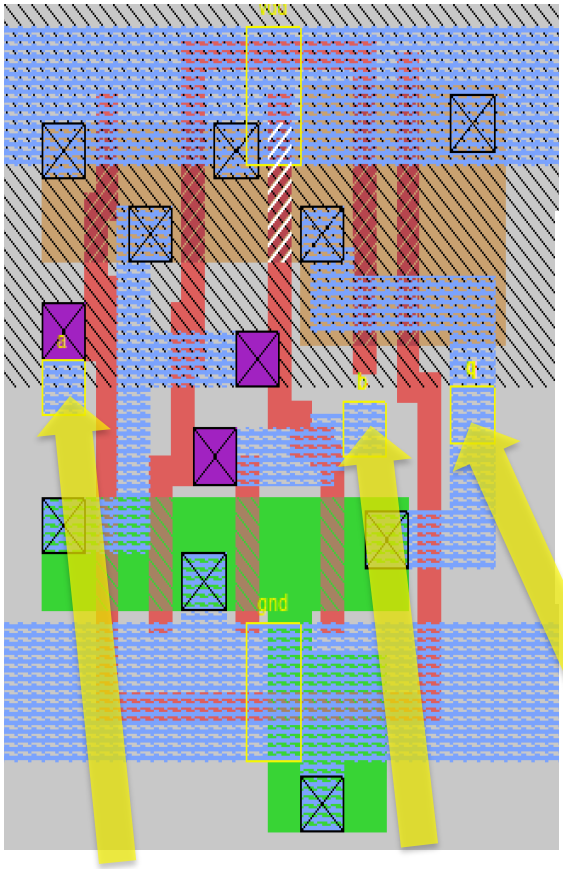
XNOR

Stage 3 – 20 bit secret key



Stage 3 – 20 bit secret key



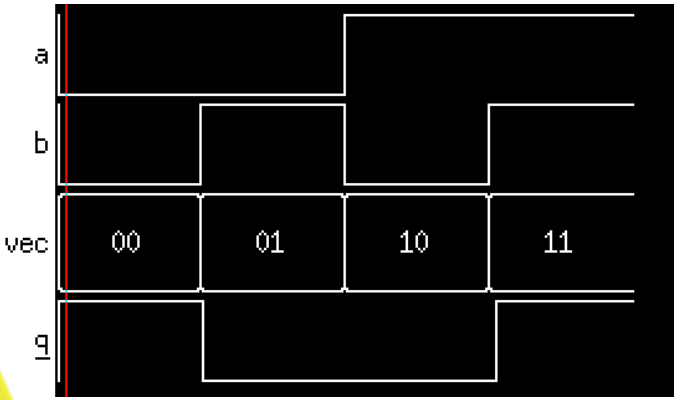


Input A

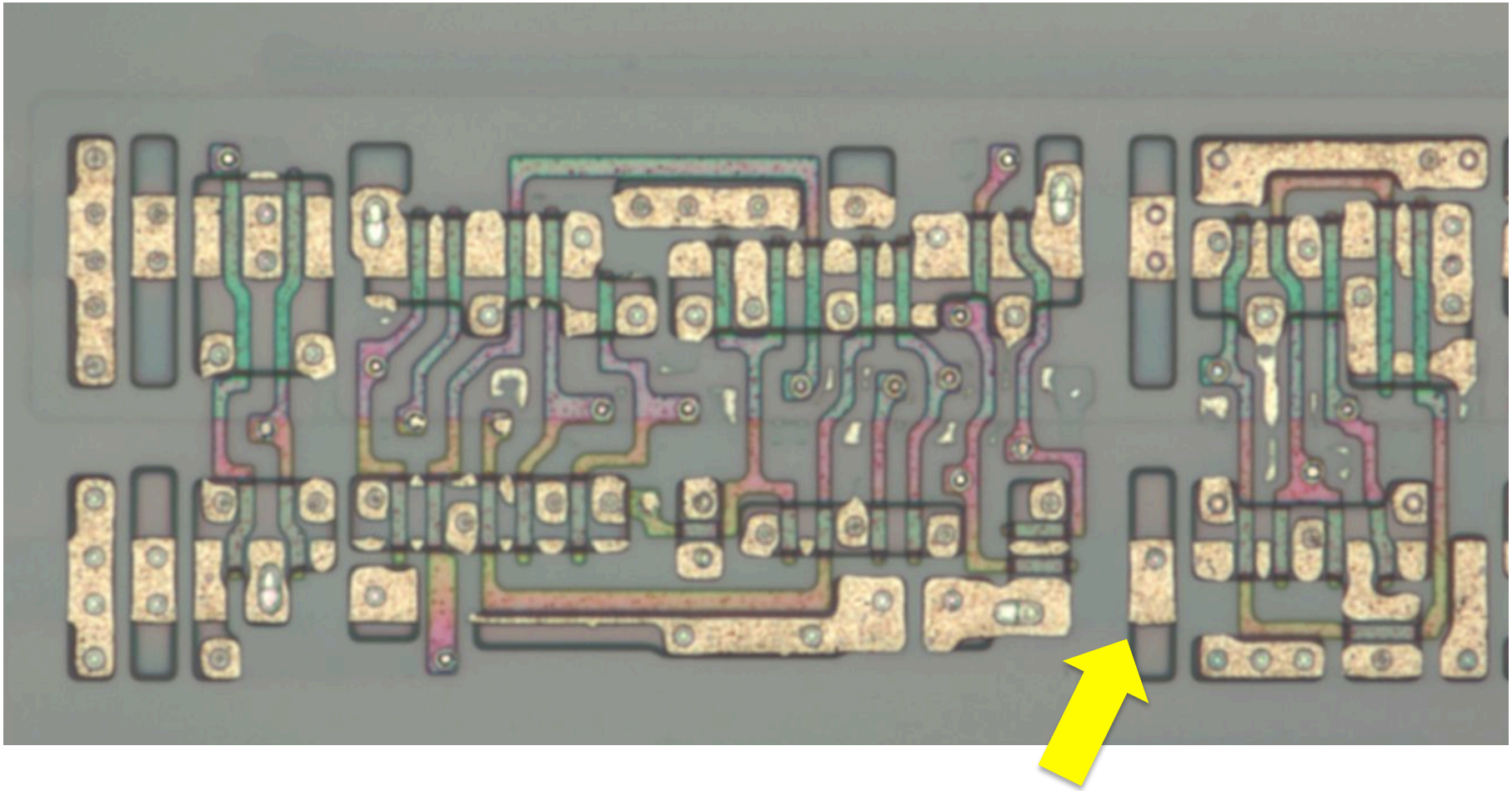
Input B

Output

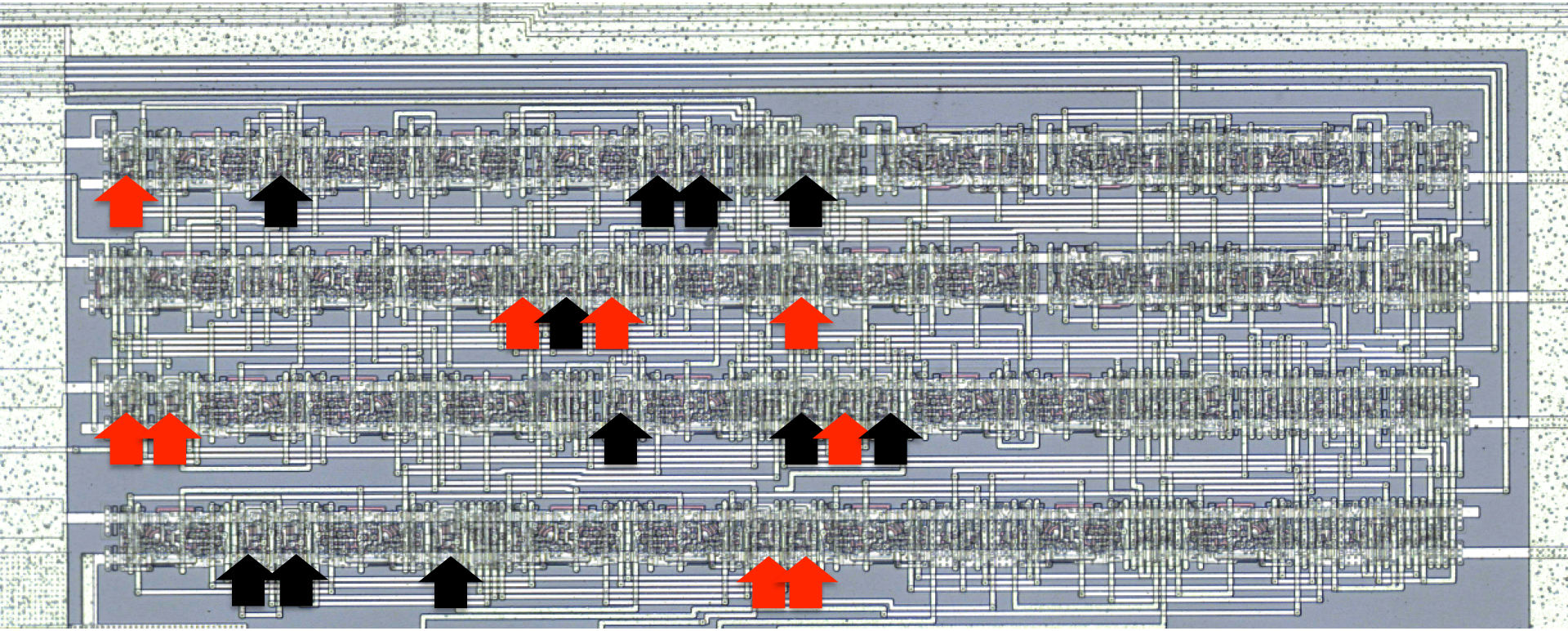
XNOR



Stage 3 – 20 bit secret key



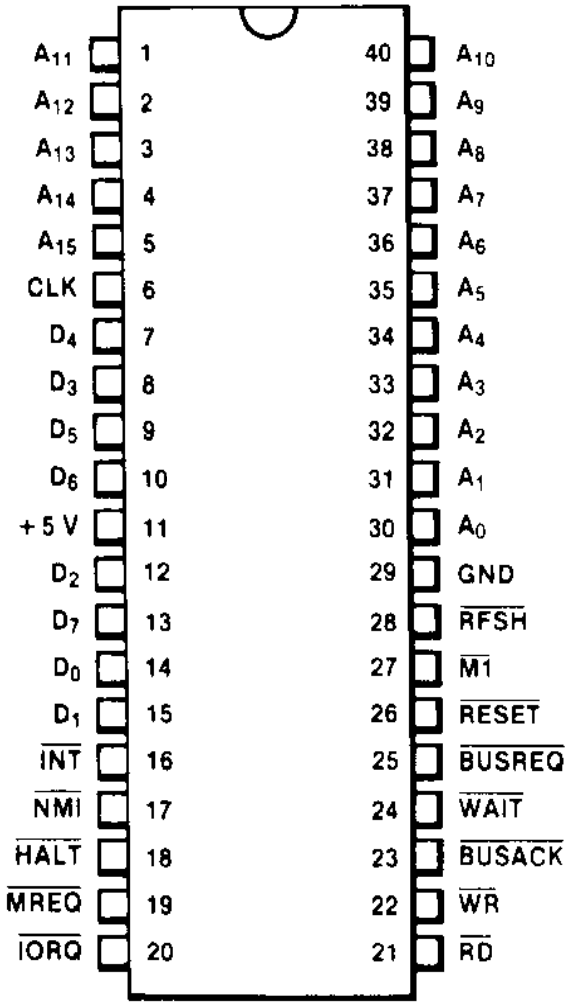
Stage 3 – 20 bit secret key



XNOR connected to VCC (+5) rail

XNOR connected to VDD (ground) rail

Stage 3 – 20 bit secret key



20 bit key sequence

1011 0111 1010 0100 0101

1 x Clock pulse with each bit

Key significance?

1011 0111 1010 0100 0101

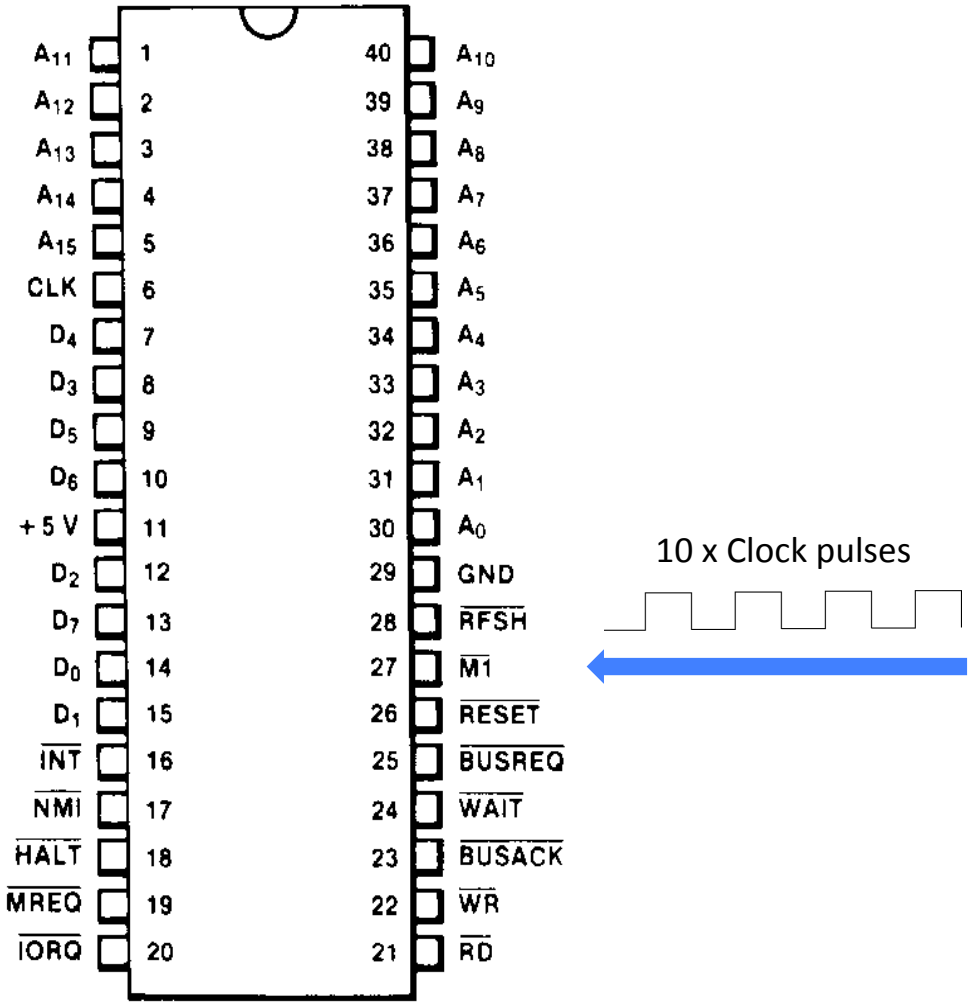
Decimal: 752197

Hex: 0xB7A45

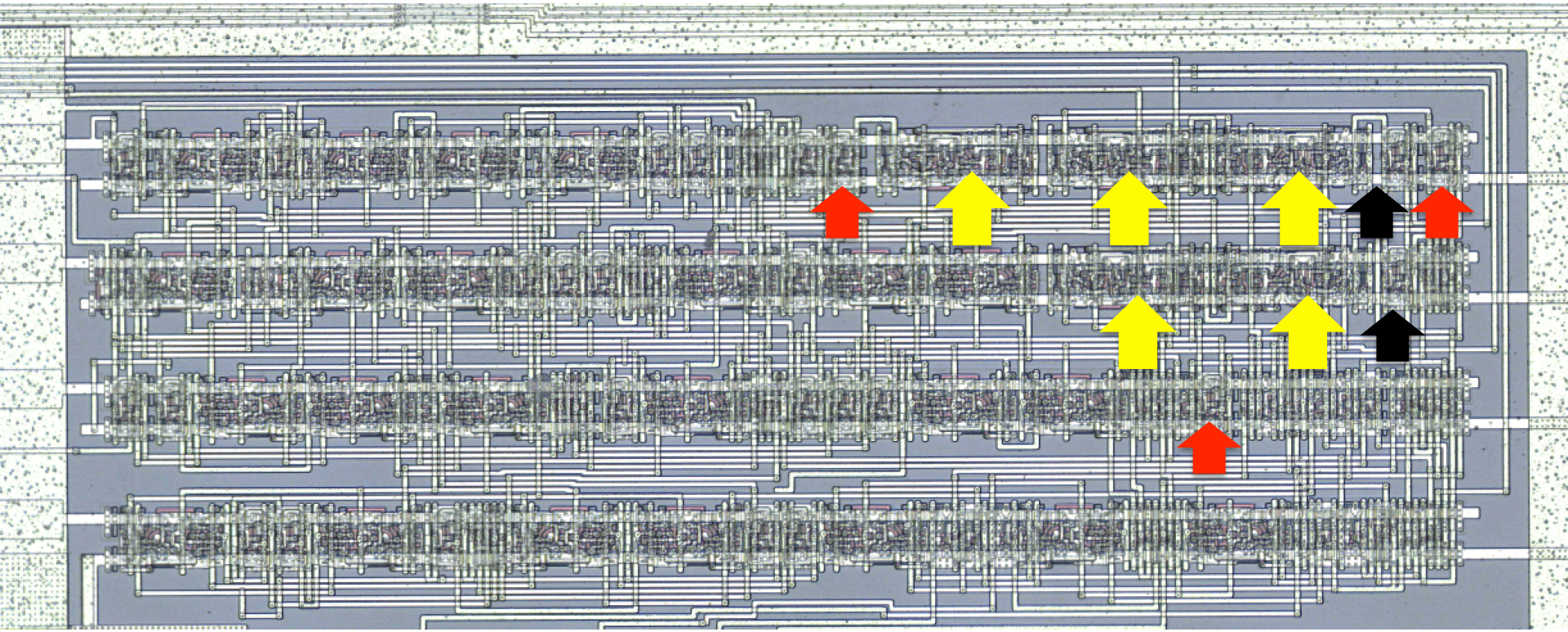
Reversed

BIN 1010 0010 0101 1110 1101 DEC 665069 HEX 0xA25ED

Stage 4 – Door knock 2



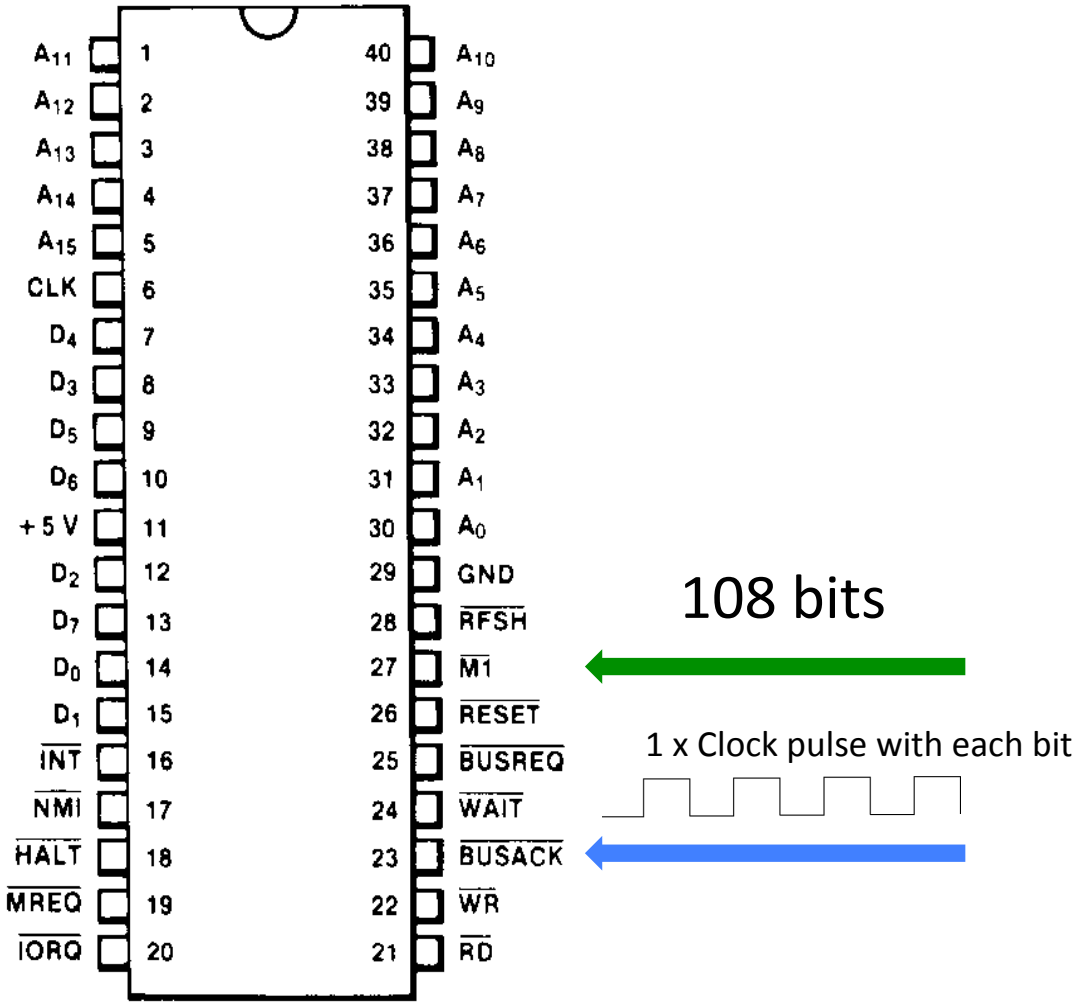
Stage 4 – Door knock 2



5 x Memory registers
1 bit each

5 x XNOR

Programming



What to program
Capcom Block Block Example

Work bits – default them to zero
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0

Address Key
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0

Swap Key #2
1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1

Swap Key #1
0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1

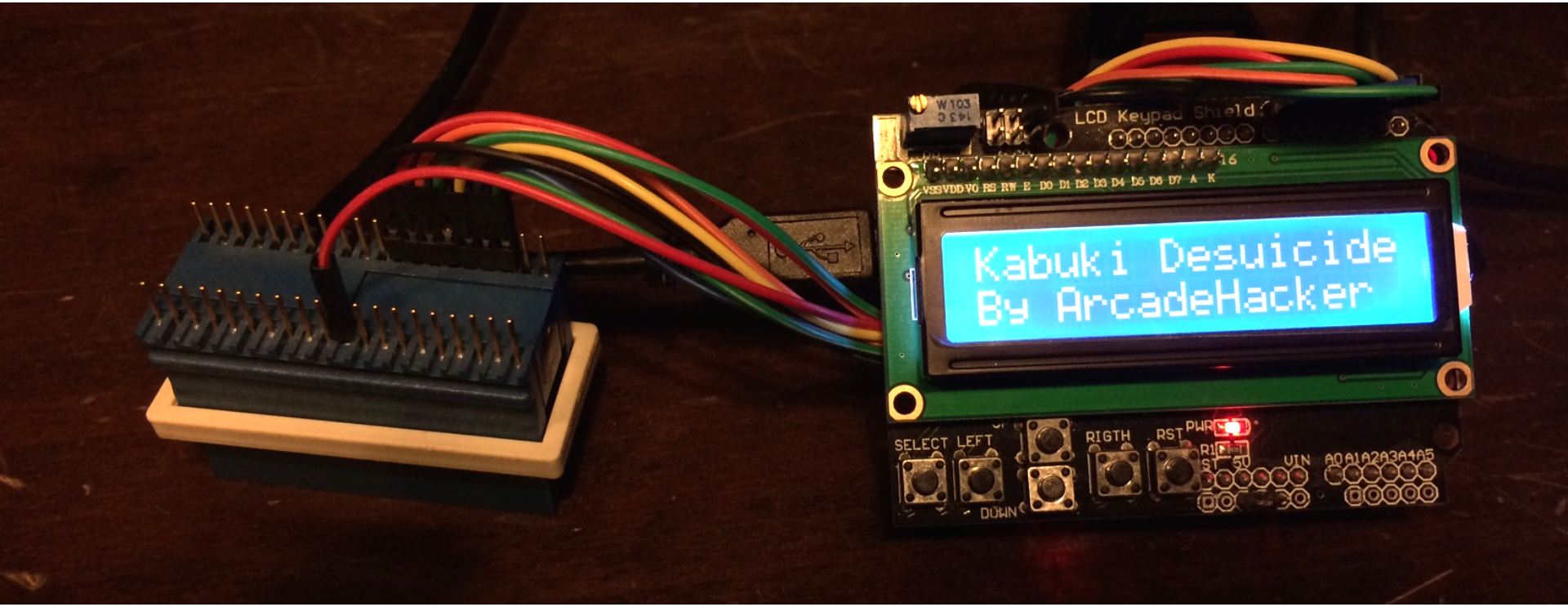
XOR Key
0, 0, 0, 0, 0, 0, 0, 1

Memory decryption area mask
1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0

Decryption keys

https://github.com/mamedev/mame/blob/master/src/mame/machine/kabuki.c

Kabuki Desuicider



edcross+arcadehacker@gmail.com