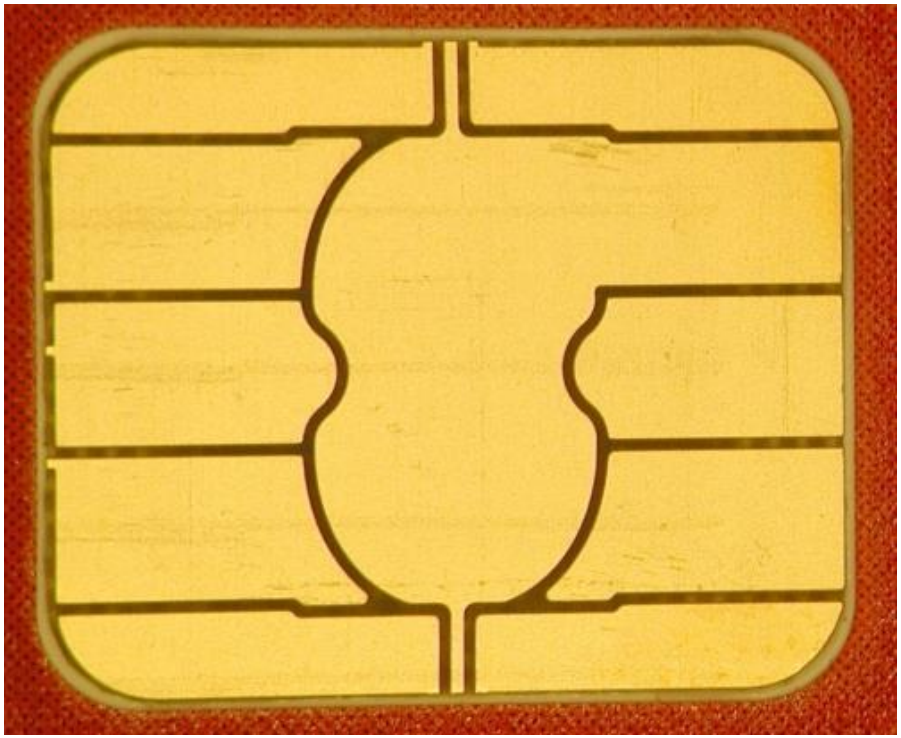
RECALL (LAST SESSION)

- **Smartcard introduction**
  - Applications
  - Design
    - Electronic : What's inside?
    - Architecture scheme (Mux / Demux / registers …)
    - Embedded software
    - Development phases
- **Smartcard Business**
  - Founderies
  - IC Developers
  - Embedded Software Developers
- **Communication**
  - 7816 standard
  - 14443 standard

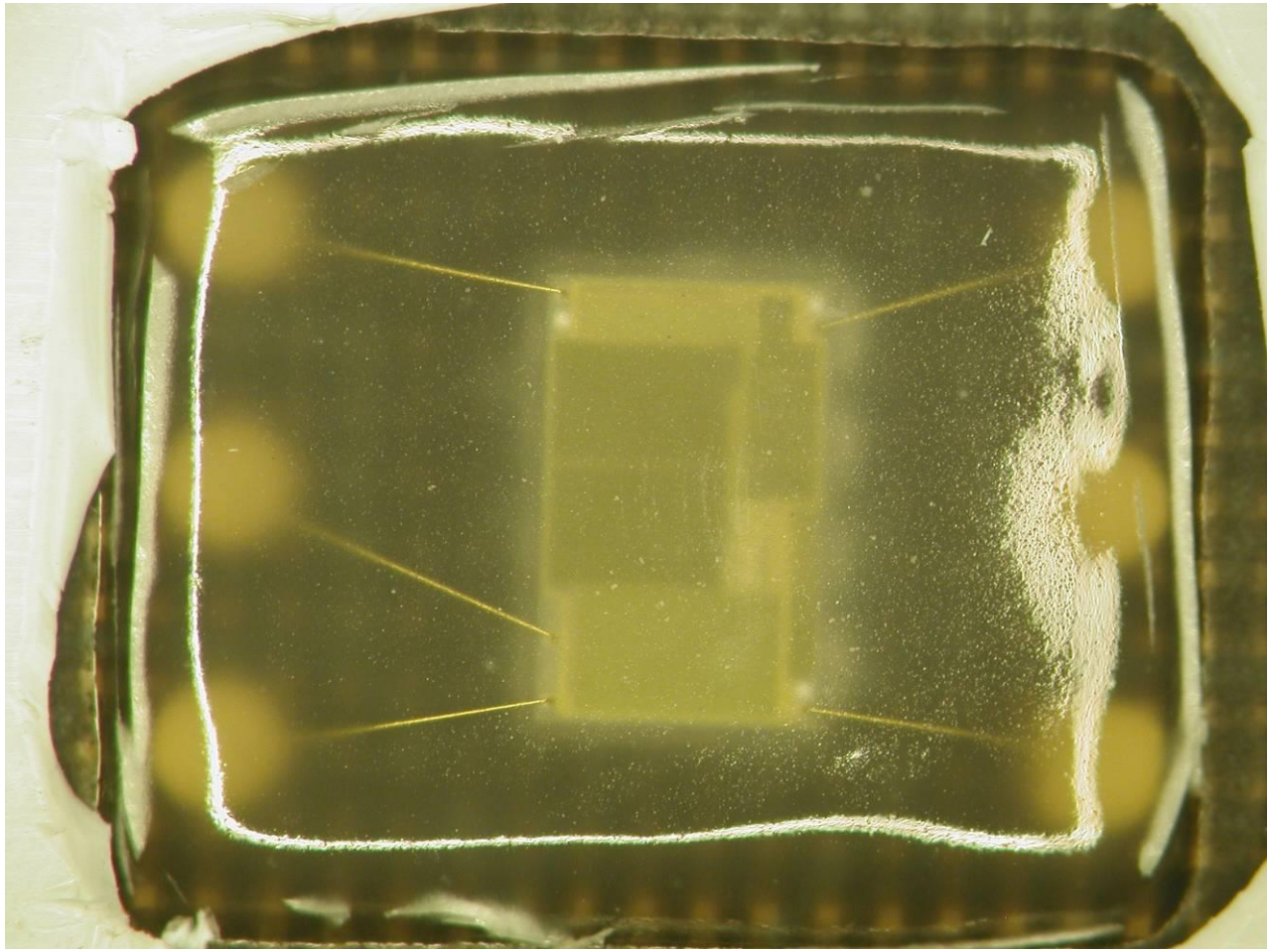
TODAY

- **Physical implementation / Physical Attacks**
  - A famous example
- **Banking protocols**
  - B0’
  - EMV intro
- **fault attacks**
  - intro
  - RSA case

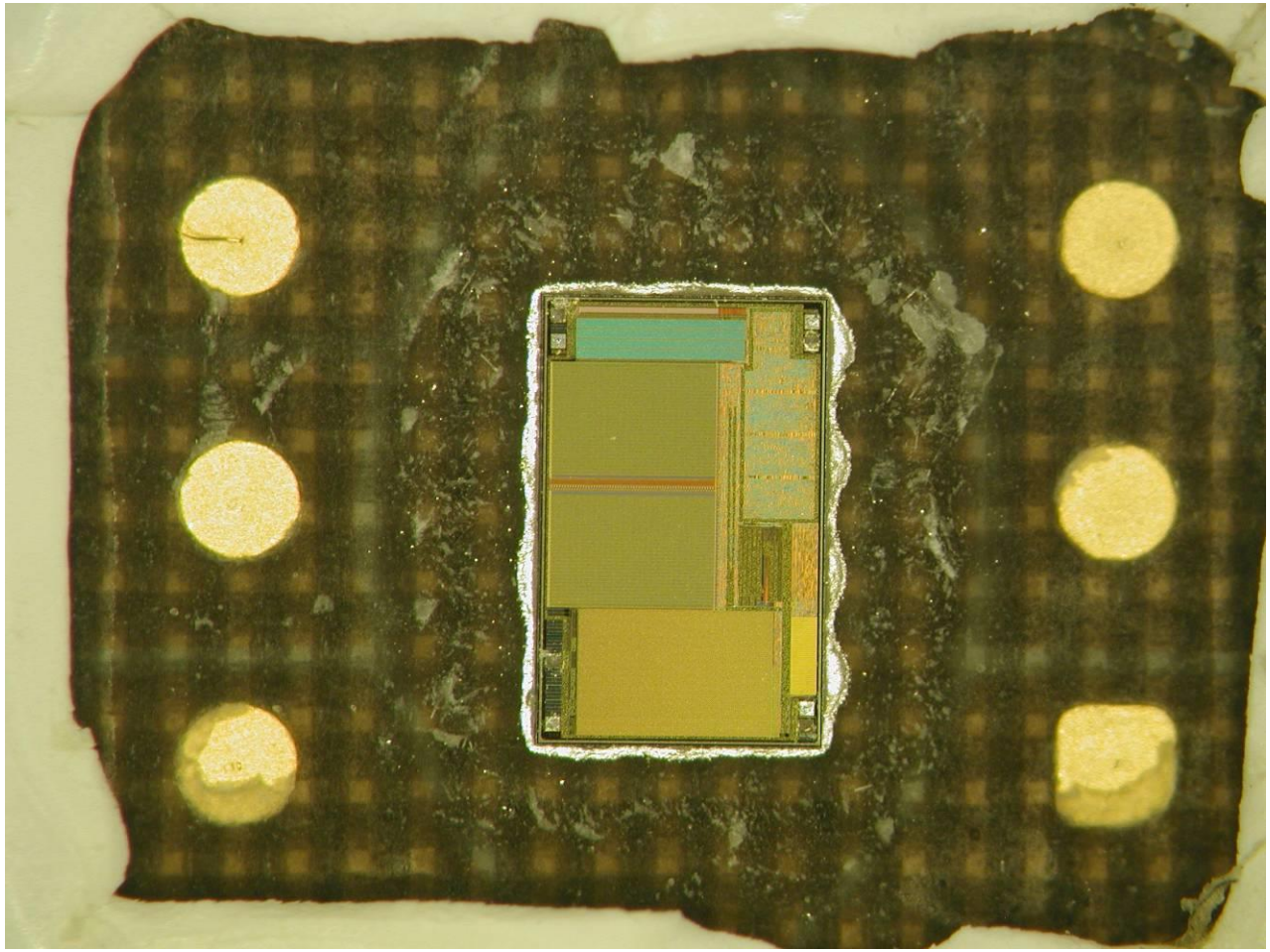
WHAT IS A SMART CARD? MICRO-MODULE



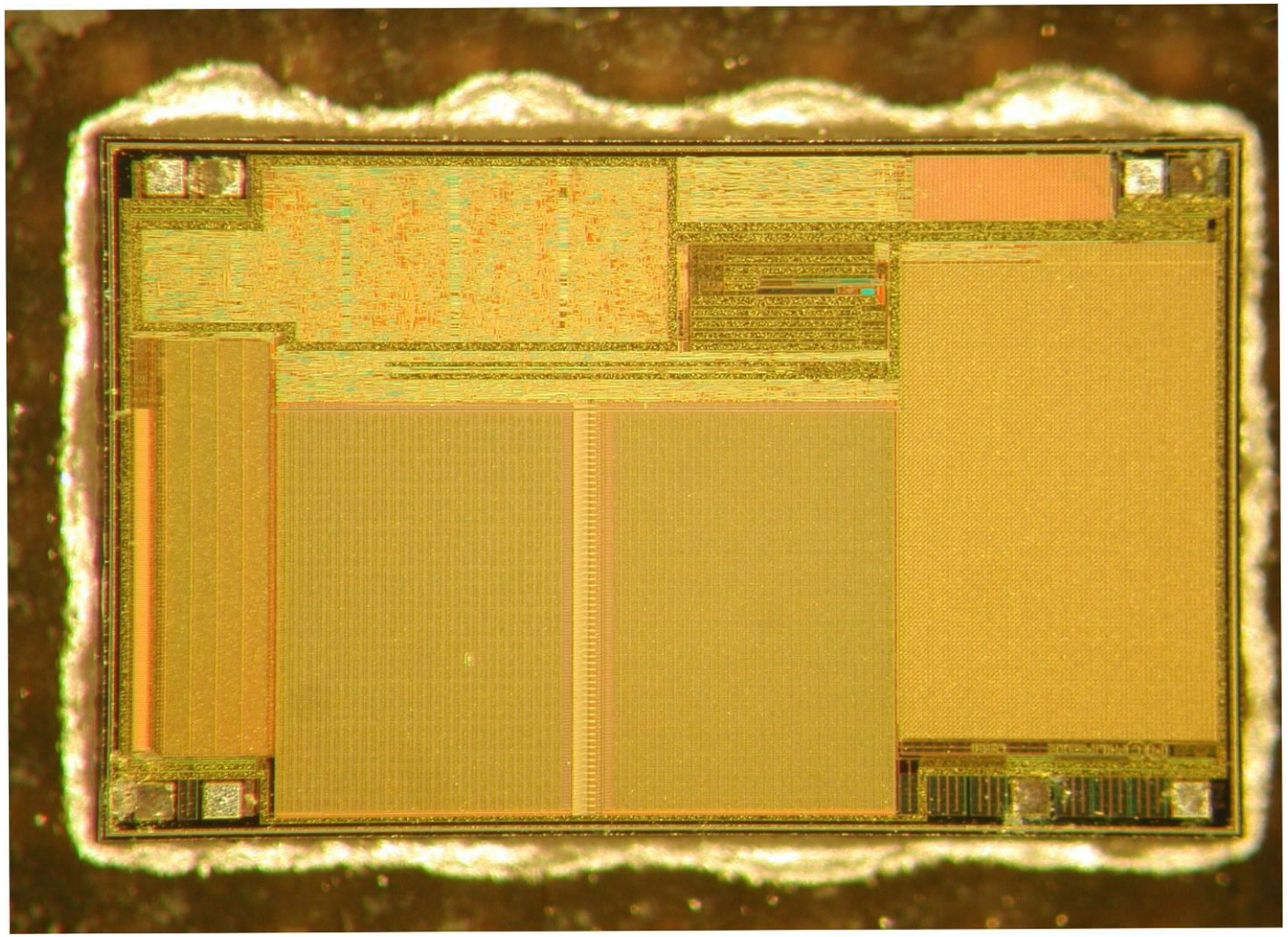
WHAT IS A SMART CARD…



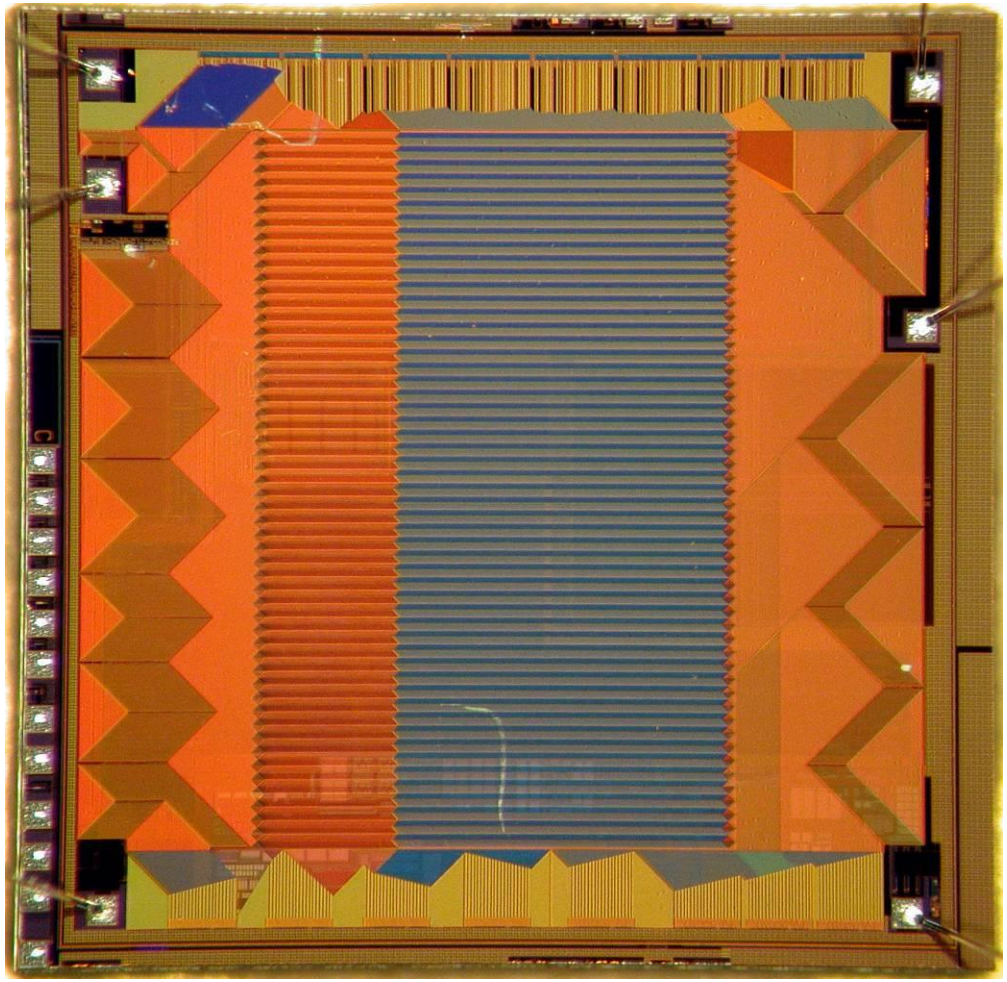
WHAT IS A SMART CARD…



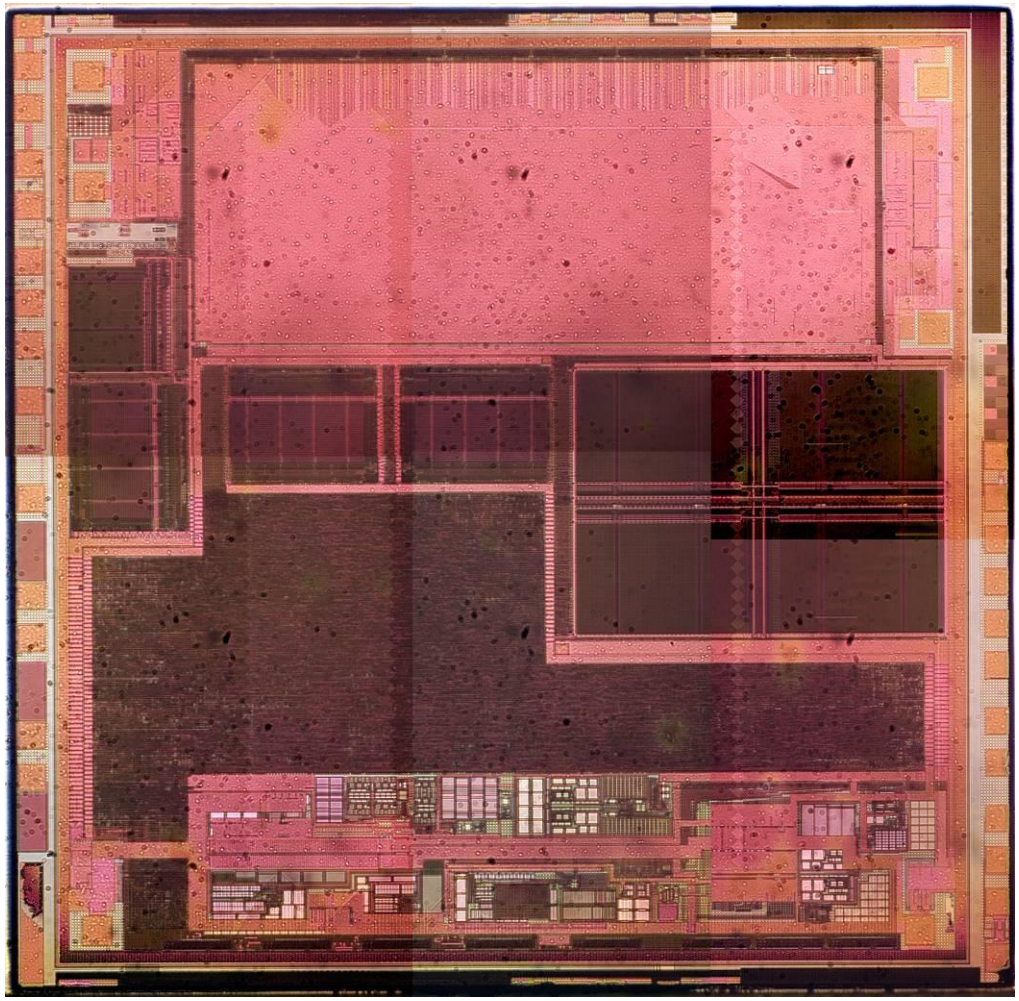
WHAT IS A SMART CARD…



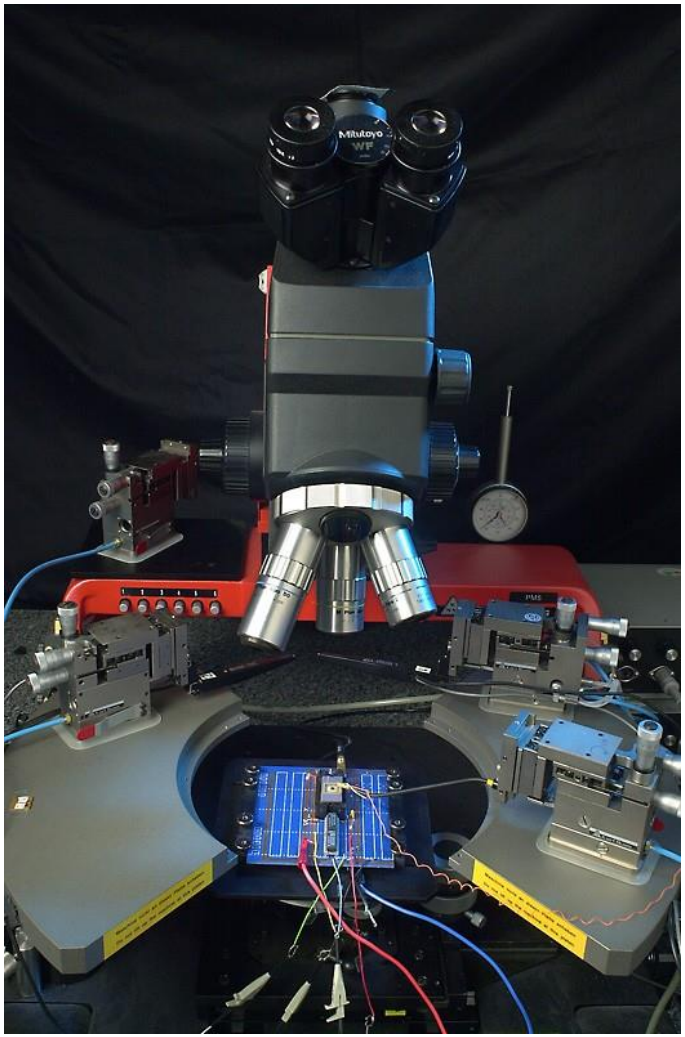
WHAT IS A SMART CARD… ANTI-PROBING LAYER



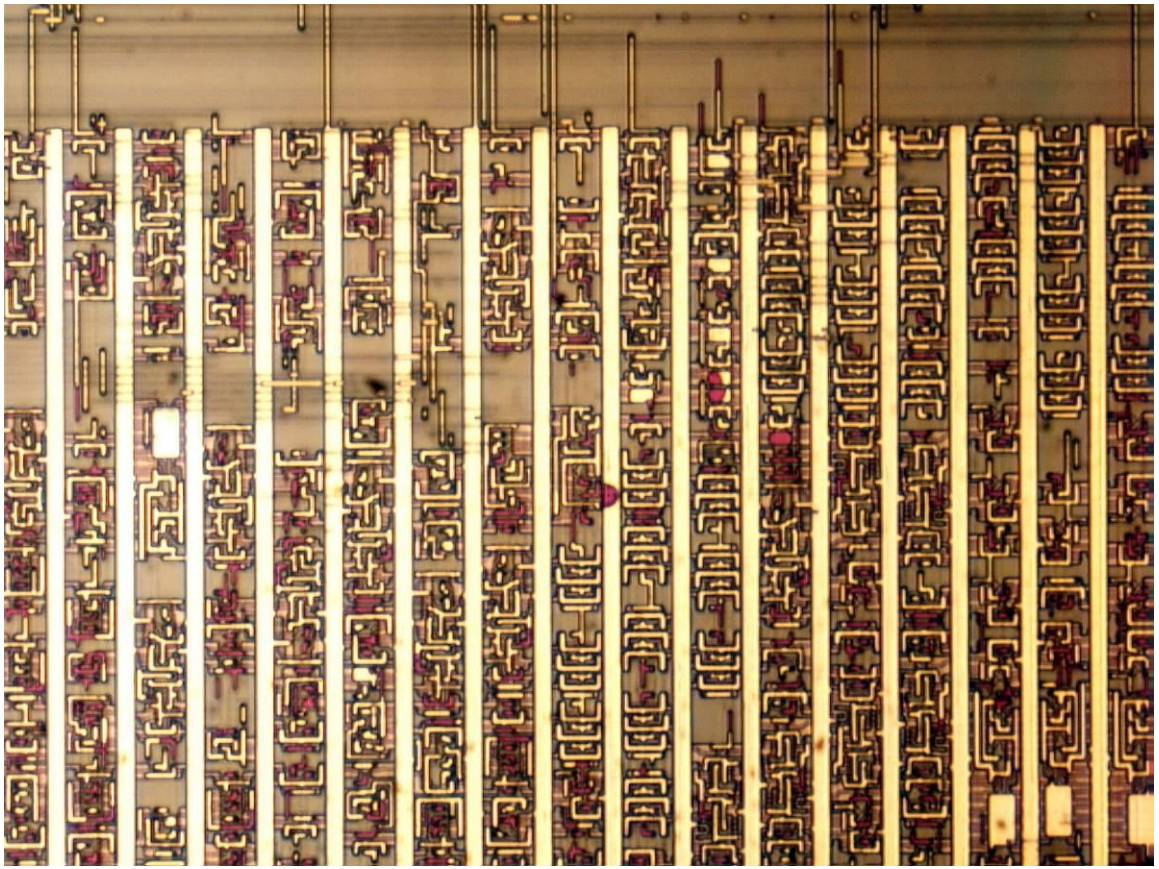
WHAT IS A SMART CARD?



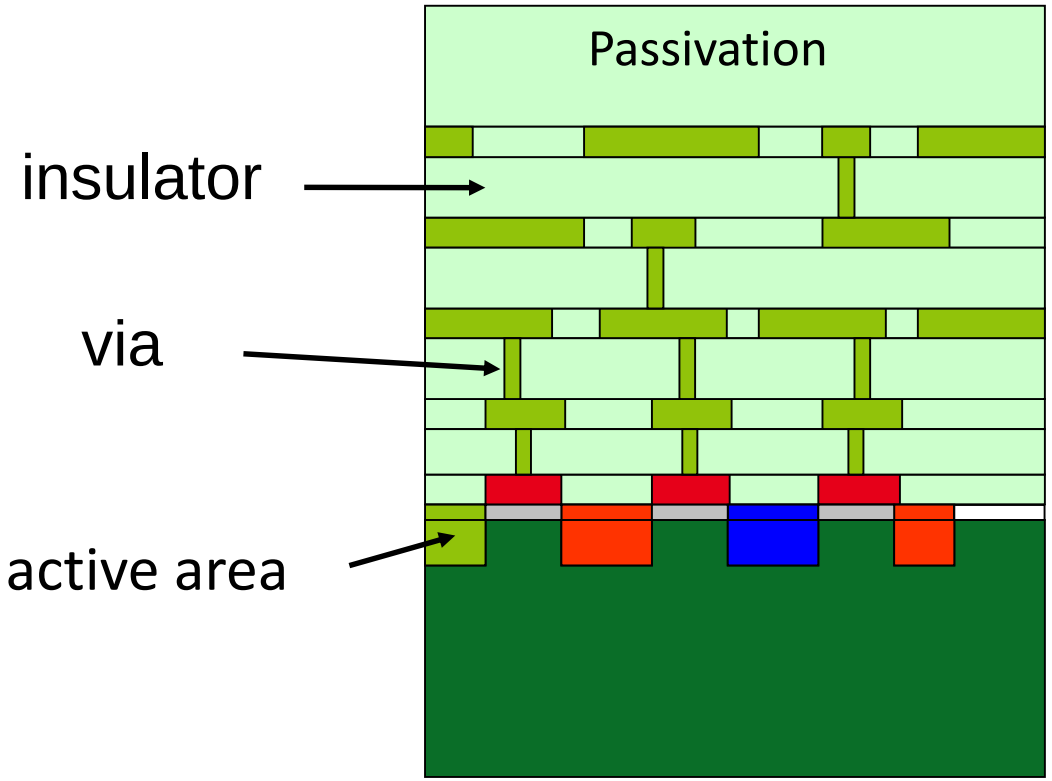
WHAT IS A SMART CARD… MICRO-PROBING



WHAT IS A SMART CARD?



WHAT IS A SMART CARD… SIDE VIEW



Antiprobing layer M_4

M_3

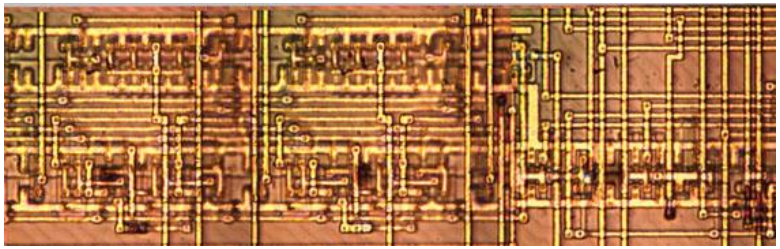
M_2

M_1

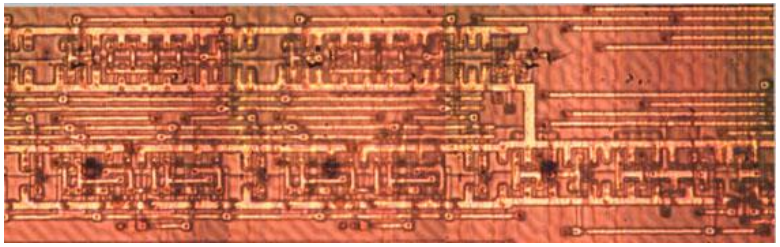
poly

REVERSE ENGINEERING

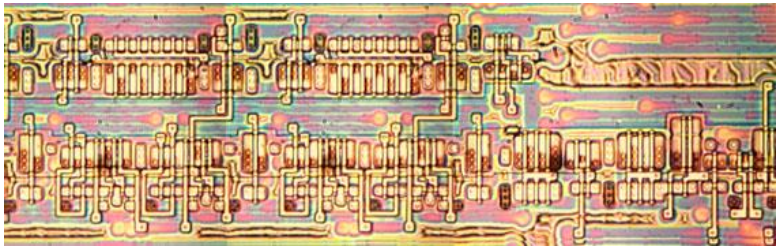
Example with a 3 metal layer techno, M3 used for anti-probing layer



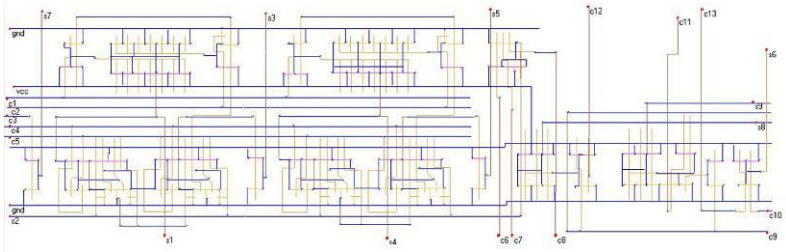
1 : **removing of the anti-probing layer (M3), view of M2**



2 : **removing of M2, view of M1**

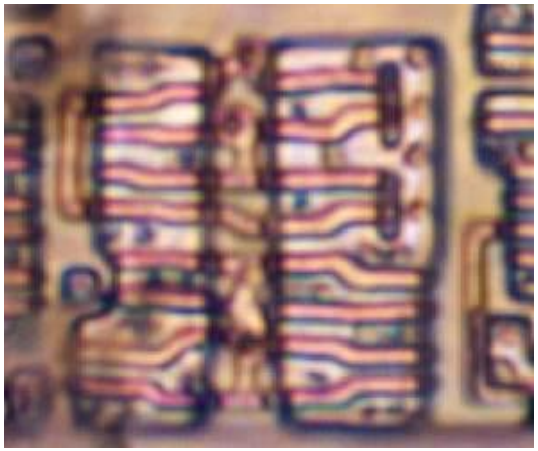


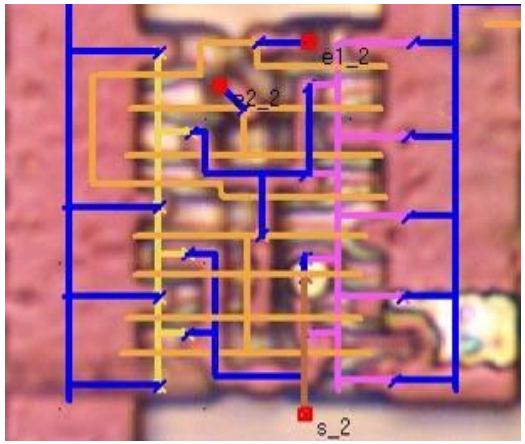
3 : **removing of M1, view of active area and poly**

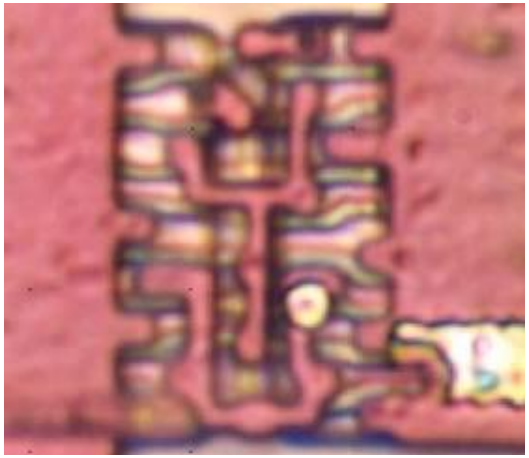


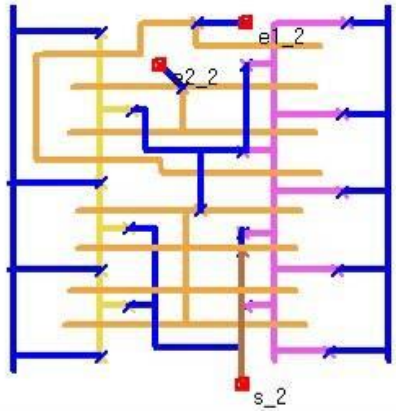
4 : **schematic reconstruction**

WHAT IS A SMART CARD? REVERSE ENGINEERING



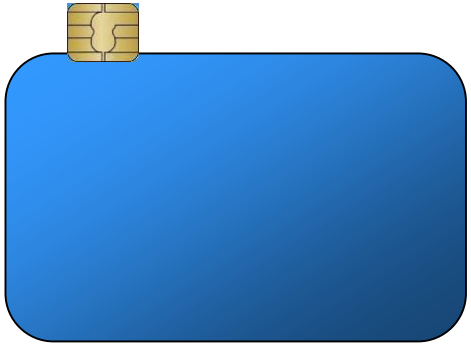






MIFARE BREAK (CASE STUDY)

CONTACT MODE : START-UP AND COMMANDS



supplies power and reset signal →

← sends ATR

← and wait for a command

sends a command →

deals with the command…

← … sends the response

fully described in norm ISO 7816

COMMAND FORMAT : APDU

Application Protocol Data Unit:

CLA INS P1 P2 Lx + DATA

5 bytes + data displayed with hexadecimal notation

example : SELECT command

00 A4 04 00 xx + AID

AID = A0 00 00 00 42 10 10

APDU : 00 A4 04 00 07 A0 00 00 00 42 10 10

A BRIEF HISTORY…

1968 - 1972: several patents (Japan, Germany, GB, USA) on plastic cards with electronic circuits and memories

1974: Roland Moreno‘s patent (memory cards)

1977 - 1978: Michel Ugon’s patents (microcontroller cards)

1979: manufacturing of the first smart card (two components)

1981: first microcontroller card with one component

1983: launch of the first french « Télécarte » (phone card)

1989: B0’ banking application

1992: all french banking cards have a chip

1996: EMV application but not use…

1999: Humpich case

2007: EMV in all french banking cards

2010: “Chip and PIN is Broken” (Murdoch, Drimer, Anderson, Bond)

B0' DATA

- **internal data of the card**
  - readable data:
    name
    date of issue
    account details
    maximum amont for debit
    log of previous transactions
    VA = selected readable data
    VS = RSA signature of VA compute at personalisation time
    N (RSA modulus) 320 bits (GIE CB – same key for all cards)
    public key (3)
  - unreadable data:
    DES keys

B0' AUTHENTICATION

$Vs = E_{kpriv}(H(data))$ -- **Specifications were not public**

Offline Authentication

- Alice (A) inserts the card (C) in the Terminal (T)
- C sends (data, Vs) to T
- T compares H(data) with $D_{KPub}(Vs)$
- T asks for the code
- A gives her code
- T sends the code in clear to C
- C answers to the reader if the code is OK

Online Authentication : T initiate with the Bank (B) a session

- B sends a random x
- C computes $y = E_{KDES}(x)$ and sends to B
- B answers if the transaction is authenticated or not

HUMPICH CASE - 1997

- **French engineer**
- **Discovered the 2 weaknesses**
  - Yes cards
  - Crypto : Modulus of 320 bits. It's been factored
    - ~2hours with factorint (pari/gp) on my old laptop
- **Goes to GIE-CB to sell its know-how**
  - GIE CB refuses to believe him
- **He proved the attack buying underground tickets**
  - Police search
  - Jail for few days
  - Judicial process -> 10 months of jail (suspended sentence)

HUMPICH CASE

- **The private exponent magically appeared on internet**

- **The modulus has been raised to 768 bits**
- **Until May 2007 Yes cards attack still worked**
  - Last fraud : feb 2007 ~600 000 euros

EMV

- The purpose and goal of the EMV standard is to specify interoperability between EMV compliant IC cards and EMV compliant credit card payment terminals throughout the world.

Source : wikipedia

- Public specification, see *www.emvco.com*
  EMV Integrated Circuit Card Specifications for Payment Systems
  Book 1: Application Independent ICC to Terminal Interface
  Book 2: Security and Key Management
  Book 3: Application Specification
  Book 4: Cardholder, Attendant, and Acquirer Interface Requirements

- **EMV specifications are public.**
  VISA, MASTERCARD, JCB, AMEX use EMV and customized it…

EMV

- Book 1: Application Independent ICC to Terminal Interface
  - signals
  - reset and ATR
  - APDU
  - command READ RECORD and SELECT
- Book 2: Security and Key Management
  - authentification : SDA, DDA and CDA
  - PIN management
  - Application cryptogram
  - secure messaging
  - session key and ATC
- Book 3: Application Specification
  - GET PROCESSING OPTIONS
  - VERIFY
  - INTERNAL AUTHENTICATE, EXTERNAL AUTHENTICATE
  - GENERATE AC
- Book 4: Cardholder, Attendant, and Acquirer Interface Requirements

EMV : DYNAMIC DATA AUTHENTICATION

- The card has
  - Public data
    - Data cardholder: data
    - S_{EMV}(data)
    - S_{EMV}($kpub_{card}$)
  - Private data
    - Card private key kpriv (card specific, unreadable)

- 1. Card (C) sends
  - data, S_{EMV}(data), S_{EMV}($kpub_{card}$)
- 2. T computes
  - 2a. V_{EMV}(S_{EMV}(data)) != data
  - 2b. V_{EMV}(S_{EMV}($kpub_{card}$) = $kpub_{card}$ => It gets $kpub_{card}$
- 3. T generates a random challenge R and sends it to C
- 4. C sends R2=S_{card}(R)
- 5. T computes and checks Pcard(R2)