Les cartes à puce. Sécurités et Attaques.

Pierre Dusart
dusart@unilim.fr
et
Damien Sauveron
damien.sauveron@unilim.fr
http:/damien.sauveron.free.fr/

3 Mai 2005

Plan

1) La carte à puce

- ➤ Présentation
- ➤ Sa sécurité
- ➤ Les attaques

2) Java Card

- ➤ Présentation
- ➤ Sa sécurité
- ➤ Les attaques

La carte à puce

Présentation

Qu'est ce qu'une carte à puce ?

- ***un morceau de plastique*** de la taille d'une carte de crédit
- ***un circuit électronique*** capable de manipuler (stocker, calculer, etc) des informations

Historique

- En 1968, deux Allemands Jürgen Dethloff et Helmut Grötrupp introduisent un circuit intégré dans une carte plastique
- Entre 1974 et 1978, le français Roland Moreno, ***le père de la carte à puce*** dépose 47 brevets dans 11 pays
- En 1983, apparition des premières cartes téléphoniques à mémoire
- En 1984, adoption par le G.I.E carte bancaire de la " carte bleue "
- Entre 1984 et 1987, normes ISO 7816 (carte à puce à contact)
- En 1997, apparition des premières Java Cards

Deux classements possibles

les cartes à mémoire

☞ versus

les cartes à microprocesseur

les cartes à contact

versus

☞ *les cartes sans contact*

versus

les cartes dual-interface

La carte à mémoire

- Premier modèle de cartes à puce
- Majorité des cartes vendues dans le monde en 1999

Elle possède :

- ***une puce mémoire*** de 1 à 4 Ko
- ***une logique cablée non programmable***

Avantages :

- sa technologie simple
- son faible coût (1$)

Inconvénients :

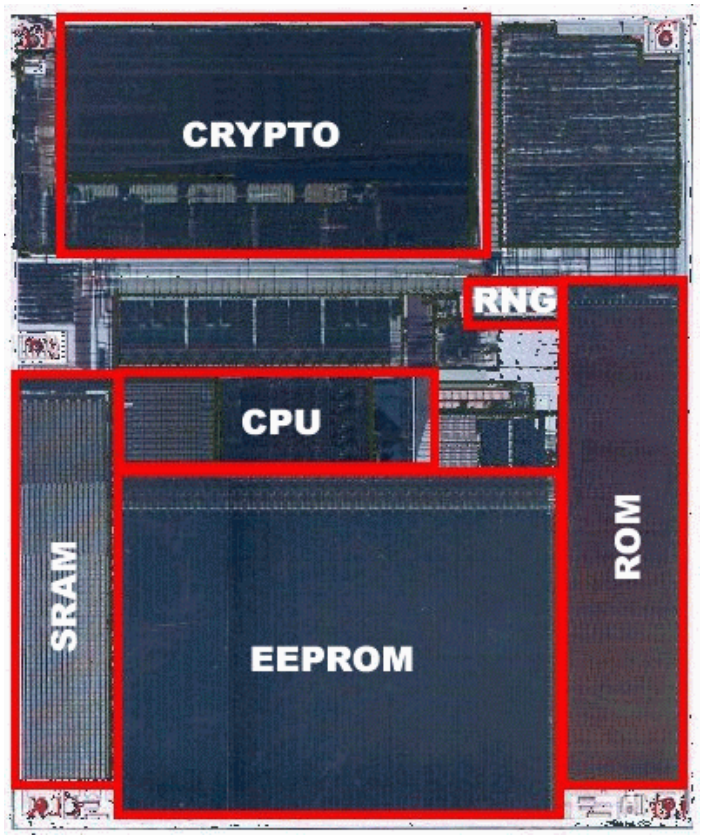
- sa dépendance vis-à-vis du lecteur de carte
- “assez” facile à dupliquer

Les types de carte

La carte à microprocesseur

Taille de la puce : $25mm^2 * 200\mu m$

- ***Microprocesseur*** (CPU) : 8, 16 ou 32 bits (à architecture RISC ou pas)
- ***ROM*** : 16 à 64 Ko
- ***EEPROM/Flash/FeRAM*** : 16 à 64 Ko
- ***RAM*** : 1 à 2 Ko
- Coprocesseur cryptographique
- Générateur de nombres aléatoires (RNG)

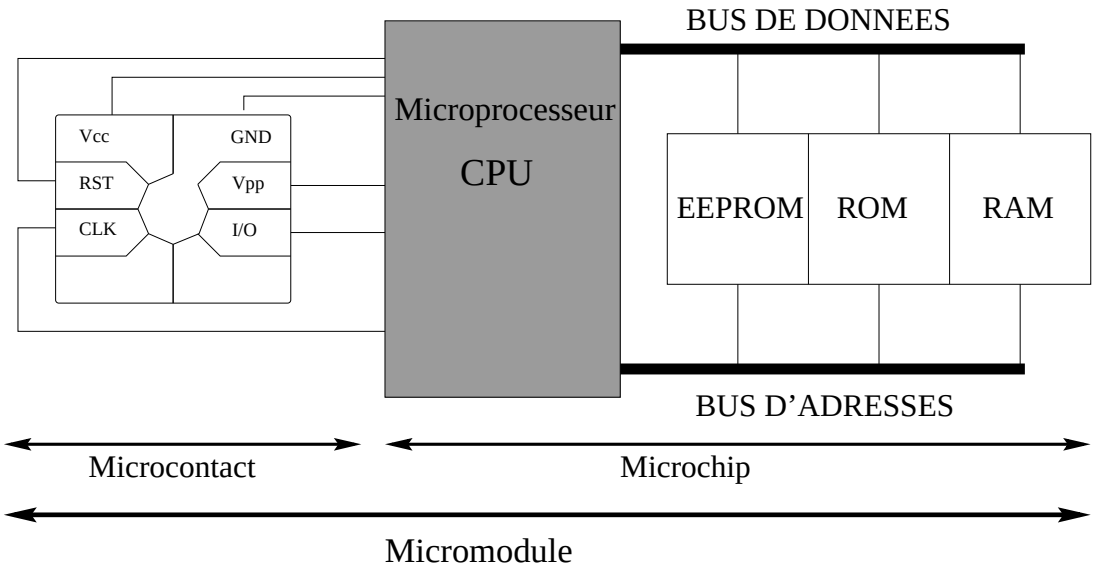


Avantage : le coût acceptable pour tant de sécurité (entre 1$ et 20$).

Les modes de communication

La carte à contact (1/2)

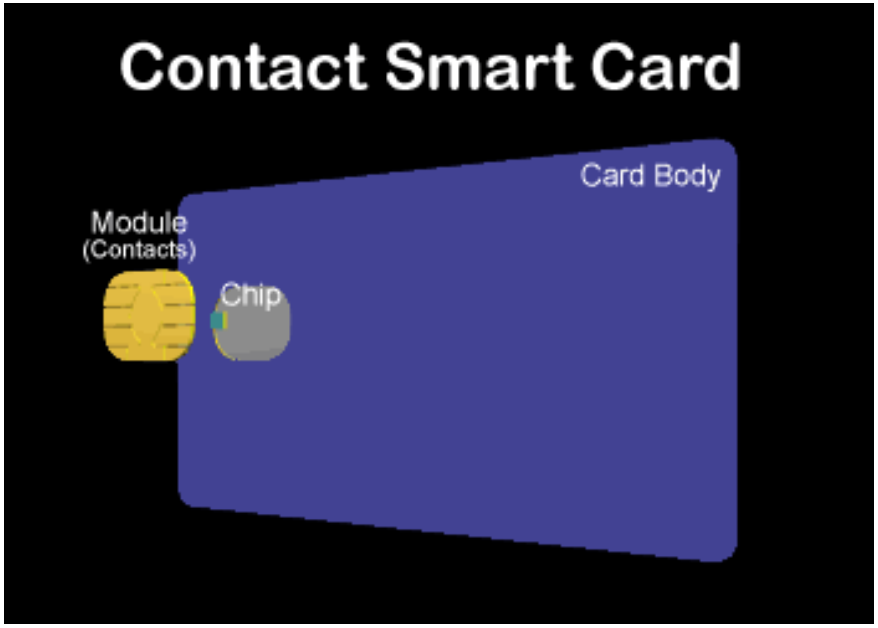
- Suit le standard ***ISO 7816***
- ***Communication série via huit contacts*** $\Longrightarrow$ insertion dans un lecteur de carte



La carte à contact (2/2)

Problèmes :

- l'insertion et le retrait sont des facteurs d'usure de la carte
- orientation de la carte dans le lecteur



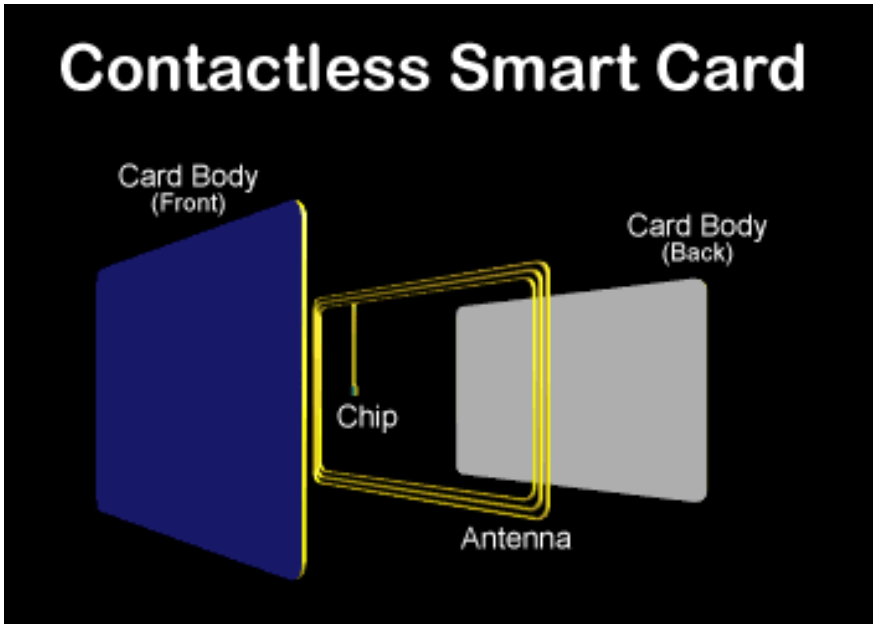
Les modes de communication

La carte sans contact

- ***Communication via une antenne*** dans la carte
- Récupère son énergie d'un couplage capacitif ou d'un couplage inductif
- Suit le standard ***ISO 14443***

Problèmes :

- distance de communication limitée (environ 10 cm)
- temps de transaction est de l'ordre de 200 ms $\Longrightarrow$ limite les données à échanger
- le coût élévé



Les modes de communication

La carte dual-interface

C'est une combinaison entre :

- la carte à contact
- et la carte sans contact

Ces deux possibilités de communication en font une carte "idéale".

La carte à puce

Sa sécurité

La sécurité physique

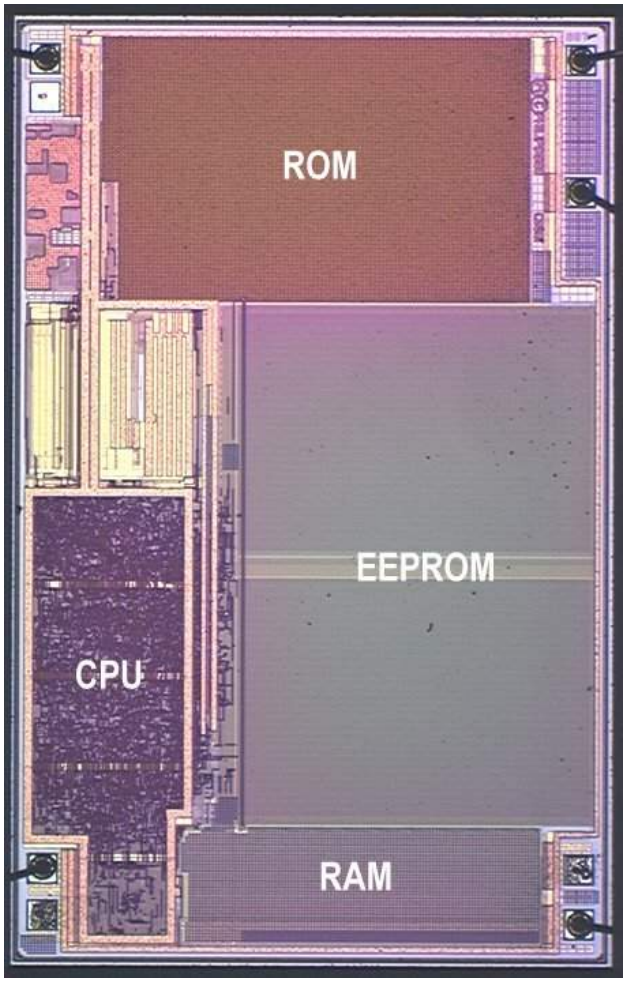
- techniques d'impression sophistiquées
  - différentes couches d'impression
  - hologramme
  - embossage
- procédés d'encollage
- matériaux plastiques
- design du micro-contact

La sécurité hardware

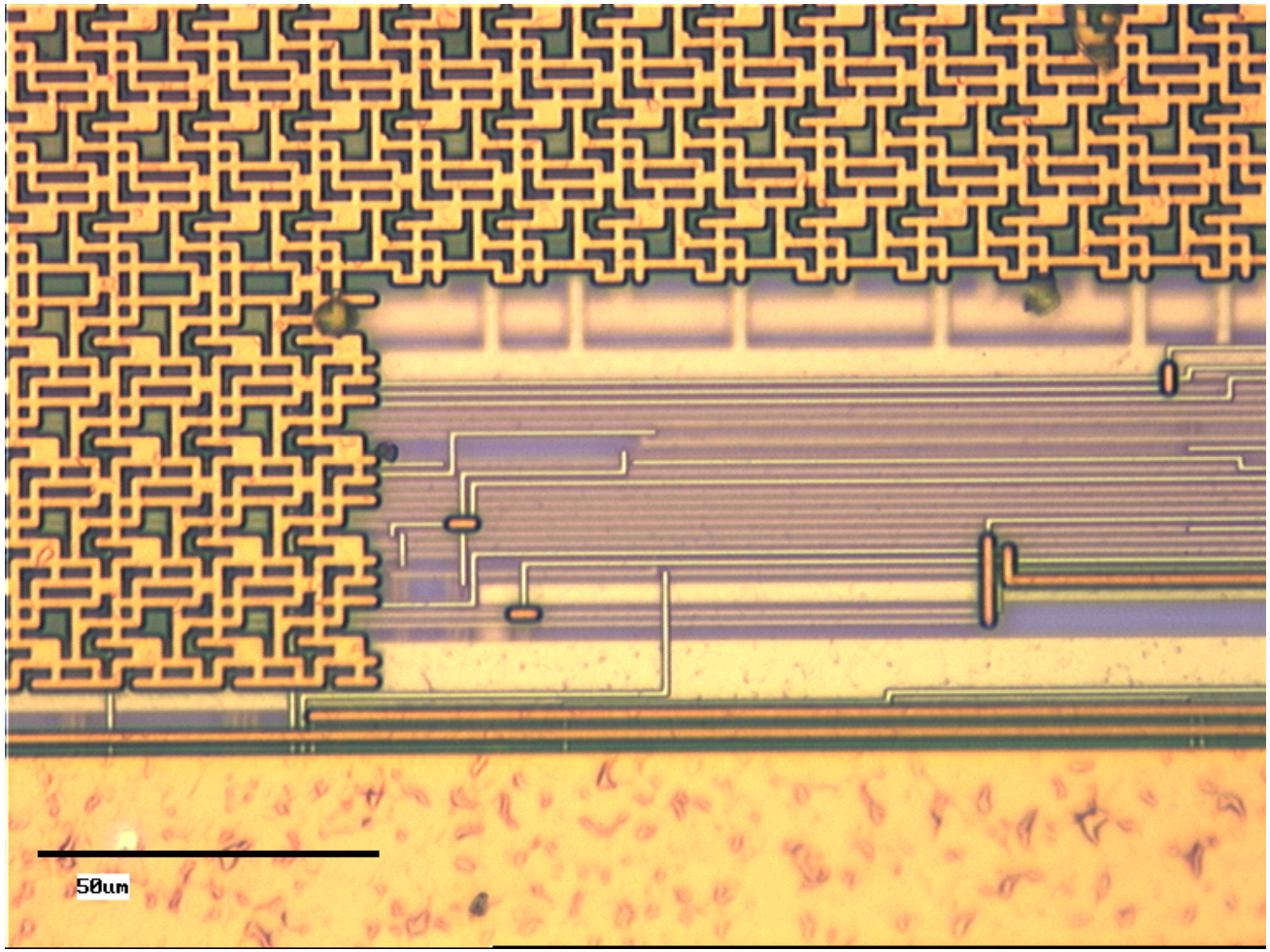
- un numéro de série unique
- l'utilisation de mémoire de type PROM
- blindage physique du composant (grille, grille active, ...)
- des détecteurs de conditions anormales (température, lumière, ...)
- brouillage des informations dans le composant (mémoire, bus, ...)
- co-processeurs cryptographiques
- pompe de charge pour le lissage de la consommation

La sécurité hardware

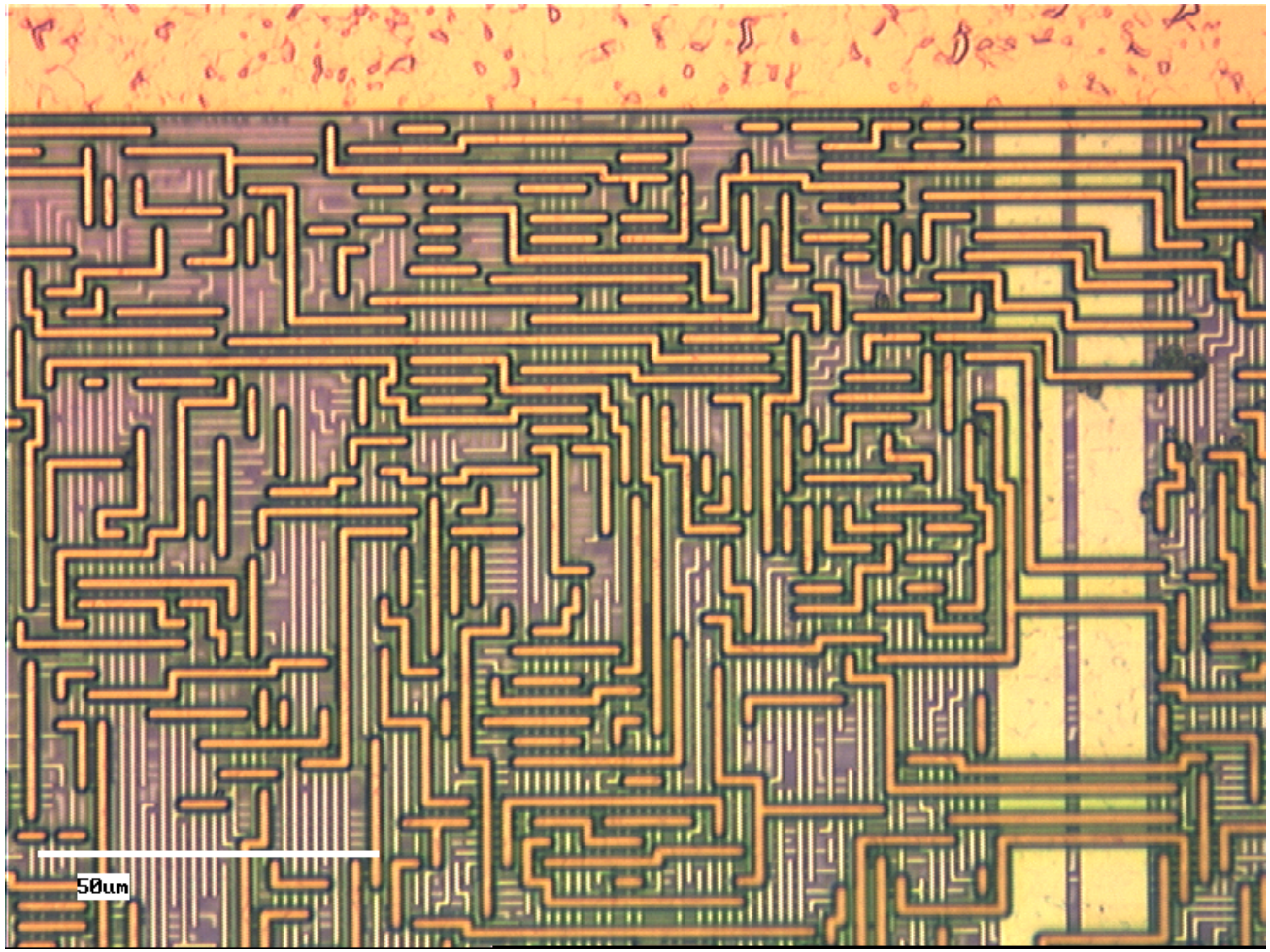
Une puce



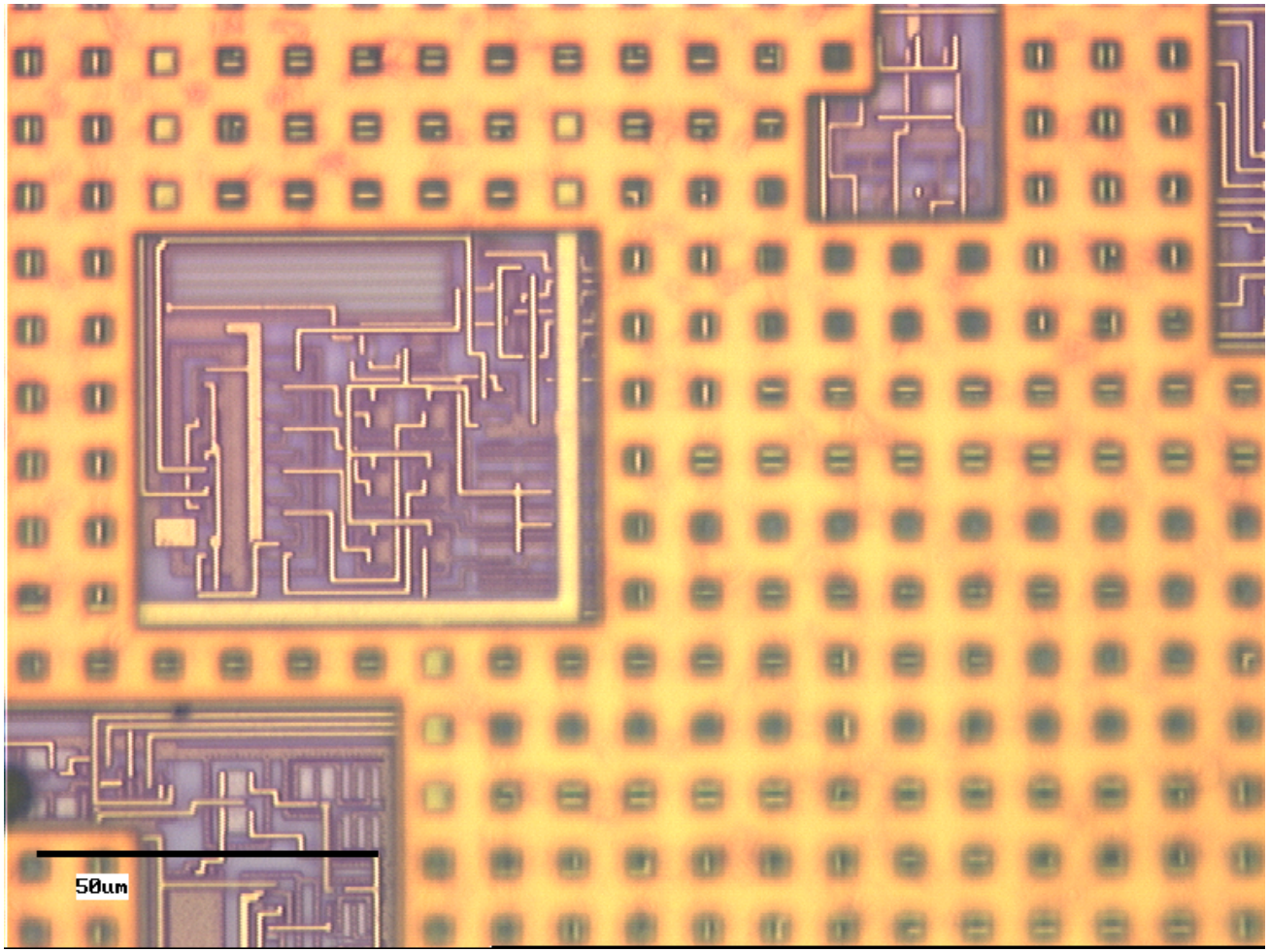
La grille de protection



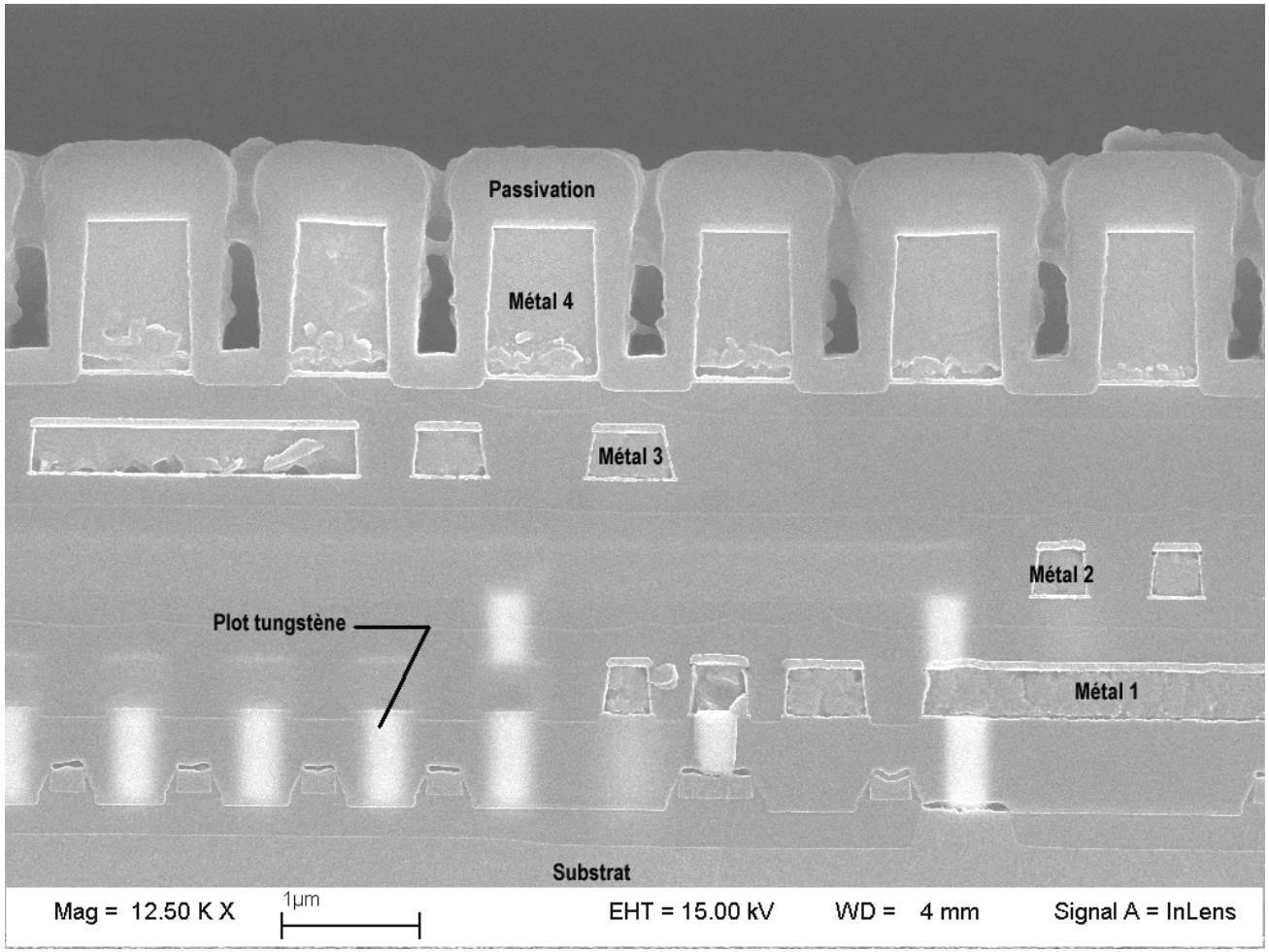
Le CPU



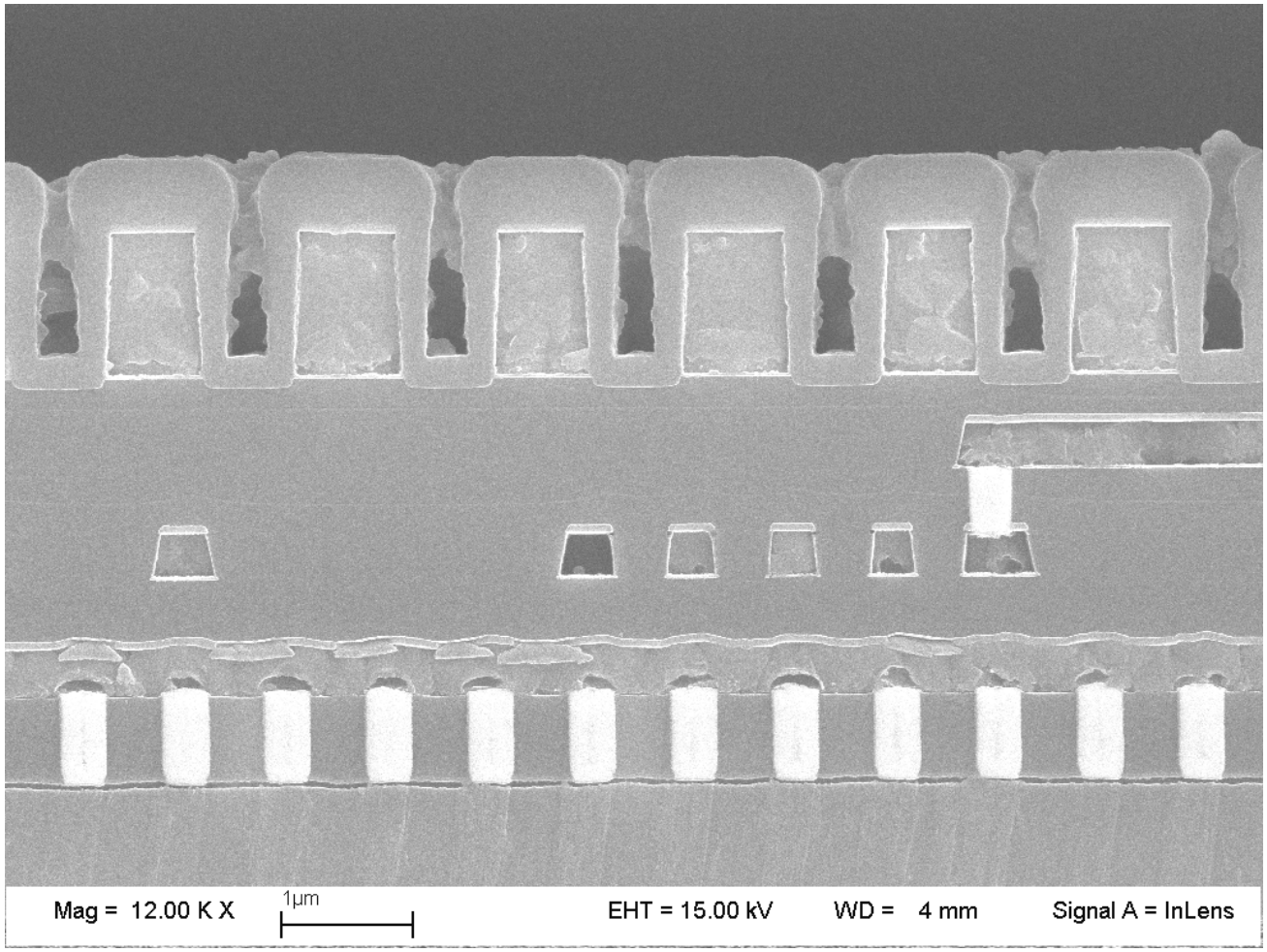
Une partie analogique



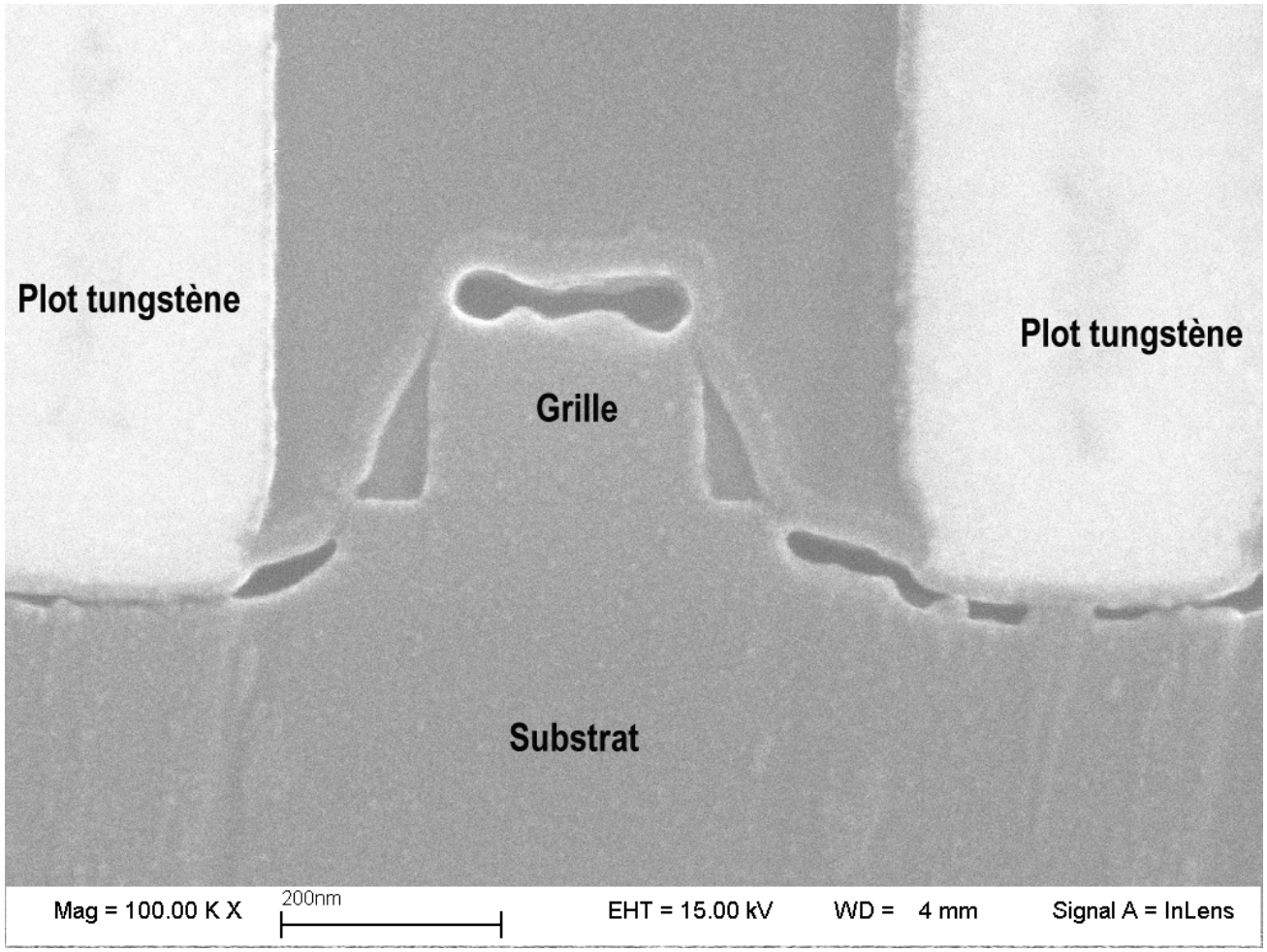
Une coupe de la puce



Une coupe de la puce



Une coupe d'un transistor



La sécurité software

- contrôles d'accès aux données
- maintien de l'intégrité des données
- entrées/sorties sécurisées
- migration du code

La sécurité de l'env. de production

- physiquement sécurisé
- régulièrement audité

Pour résumer : la triple alliance électronique, informatique et cryptographie assure un très haut degré de sécurité

La carte à puce

Les attaques

Non invasives

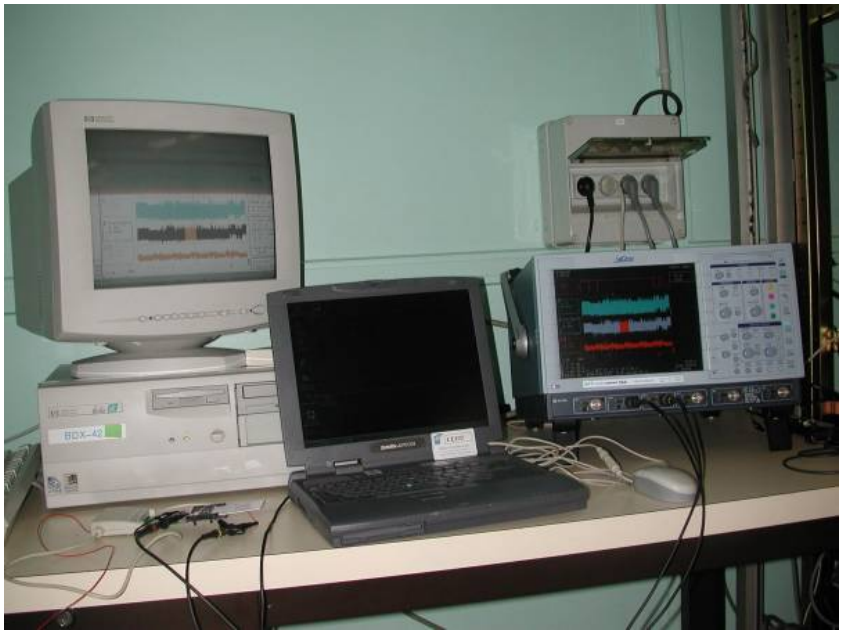
- modification des conditions opérationnelles (Vcc, F)
- modification de la température
- modification des rayonnements lumineux (UV, rayon X, lumière blanche, IR, ...)
- injection de fautes (glitches, rayonnements lumineux)
  (injection de fautes sur la JVM :
  `http://www.cs.princeton.edu/~sudhakar/papers/`)
- attaques sur les canaux cachés

Les canaux cachés

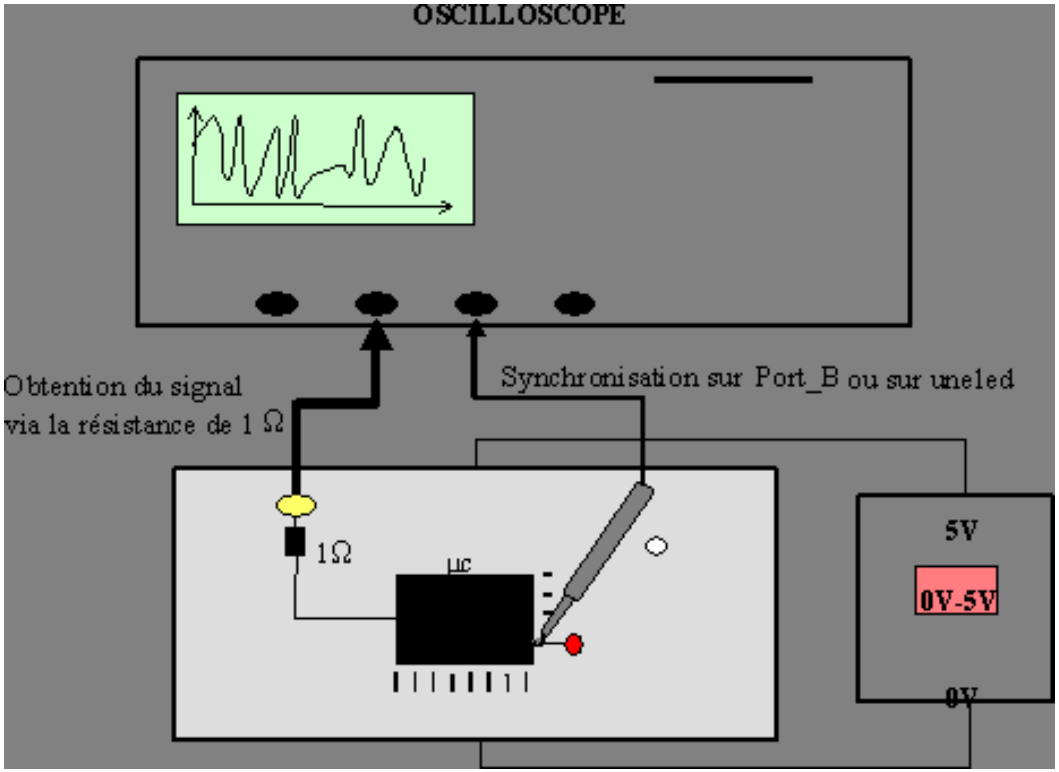
- le temps d'exécution
  $\Longrightarrow$ nombre de cycle d'une instruction ou d'un algorithme.
- la consommation de courant
  $\Longrightarrow$ Les modifications rapides de la tension et de l'intensité du courant au sein du même composant sont à la base des émissions du circuit car ils conduisent des courants RF à l'intérieur et à l'extérieur du chip.
- les émissions électromagnétiques
  $\Longrightarrow$ Les courants RF entraînent un rayonnement électromagnétique.

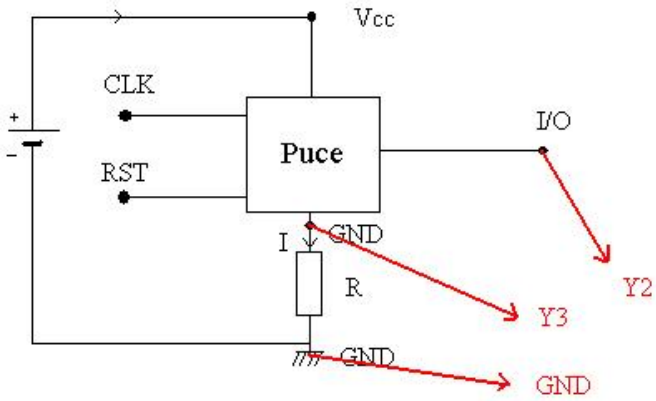
Le matériel

- un oscilloscope numérique,
- un lecteur de carte à puce,
- un pc équipé de cartes d'acquisition et de logiciels mathématique pour le traitement des données,
- une sonde CEM si on veut étudier les émissions électromagnétiques.



Le montage


OSCILLOSCOPE
Obtention du signal
via la résistance de 1 Ω
Synchronisation sur Port_B ou sur uneled
1Ω
µc
5V
0V-5V
0V


Vcc
CLK
RST
Puce
I/O
I
GND
R
GND
Y2
Y3
GND

La “timing attack”

Cette attaque consiste à mesurer le temps d’exécution d’un algorithme.
$\Longrightarrow$ Révèle des informations sur les opérations et/ou les opérandes.

Nécessite souvent :

- ☞ un grand nombre d’exécution à messages choisis,
- ☞ un traitement statistique des résultats obtenus.

La “timing attack” sur le PIN (1/2)

```
for(i = 0; i <= 7; i++)
  if (pinCarte[i] != pinPresente[i])
    return false;
return true;
```

Présentons un PIN quelconque et déroulons le programme :

- ☞ cas du premier octet FAUX

```
i = 0
(pinCarte[i] != pinPresente[i]) ? OUI
return false
```

- ☞ cas du premier octet VRAI

```
i = 0
(pinCarte[i] != pinPresente[i]) ? NON
i <= 7 ? NON
i++
(pinCarte[i] != pinPresente[i]) ? OUI
return false
```

La “timing attack” sur le PIN (2/2)

```
for(i = 0; i <= 7; i++)
  if (pinCarte[i] != pinPresente[i])
    return false;
return true;
```

- Présenter les n valeurs possibles de pinPresente[0] (256 valeurs) (n,0,0,0,0,0,0,0).
- Mesurer la durée d'exécution de la commande τ pour les n valeurs.
- Calculer $\tau[n_0]$ le maximum des τ
  - $\tau[n_0] = max(\tau[n]), n = 0, ..., 255$
- • n_0 est la solution pour pinCarte[0]
- Itérer sur tous les pinPresente[i]

Nombre d'essais : $8 * 256 = 2048$ (contre 256^8 en force brute)

Exemples de protection (1/2)

```
alea = random(0,7); // alea situé dans l'intervalle [0; 7]

for(i = 0; i <= 7; i++) {
  octet = (alea + i) mod 8;
  if (pinCarte[octet] != pinPresente[octet])
    return false;
}
return true;
```

Nombre d'essais en moyenne : $8 * 2048$ (contre 256^8 en force brute)

Possibilité d'attaque de type MasterMind.

Exemples de protection (2/2)

```
boolean test = true;

for(i = 0; i <= 7; i++) {
  test = test;
  if (pinCarte[i] != pinPresente[i])
    test = test && false;
  else
    test = test && true;
}
return test;
```

équivaut à :

```
boolean test = true;

for(i = 0; i <= 7; i++)
  test = test && (pinCarte[i] == pinPresente[i]);
return test;
```

La consommation de courant

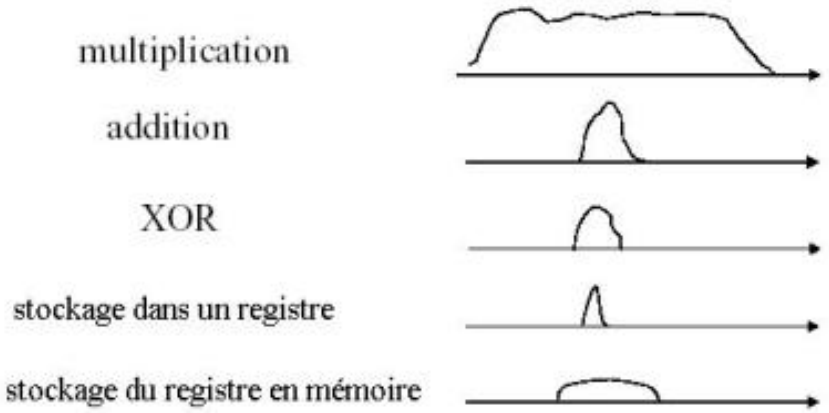
Elle est surtout utilisée dans le domaine de la cryptographie.

Il existe différentes attaques :

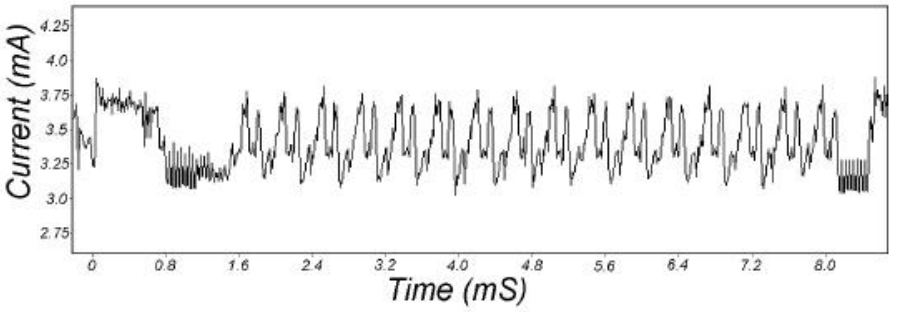
- la SPA (Simple Power Analysis)
- la DPA (Differential Power Analysis)
- la HODPA (High Order Differential Power Analysis)

La SPA (Simple Power Analysis)

Principe : Des instructions différentes ont une trace différente.



Consommation en courant d'un DES. On peut voir la permutation initiale, suivie des 16 tours.



La SPA sur la signature RSA

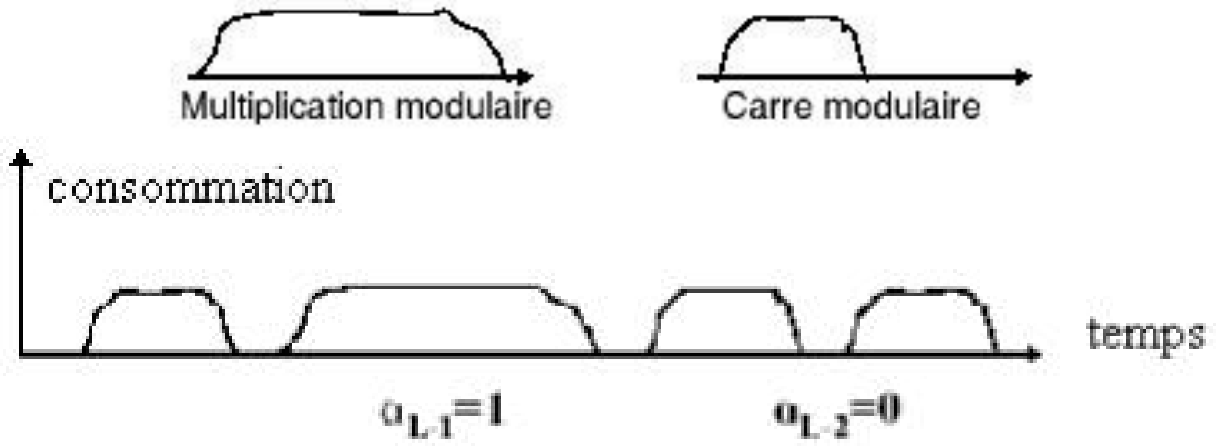
```
s = 1;
for(i = L - 1; i >= 0; i--) {
   s = s*s mod n;
   if (a[i] == 1)
      s = s*y mod n;
}
```

Signature RSA : $y^a \ mod \ n$

y est le message à signer,

n est public,

a, l'exposant peut être considéré comme la clé secrête.



La DPA (Differential Power Analysis)

Principe : La consommation dépend des opérations effectuées (les instructions) mais aussi des opérandes.

Elle utilise des **fonctions statistiques** adaptées à l'algorithme visé qui font ressortir des **corrélations entre un bit** intermédiaire a (ne dépendant que d'un fragment K_r de r bits de la clé et du message d'entrée M) **et la consommation de courant**.

La HODPA (High Order DPA)

La HODPA ou DPA d'ordre n est aussi basée sur une étude statistique de la consommation de courant de la carte.

Différence : elle utilise des corrélations entre la consommation de courant et n variables intermédiaires ne dépendant que d'un fragment de la clé et du message d'entrée.

Elle est beaucoup plus difficile à réaliser, mais beaucoup plus puissante.

Les émissions EM

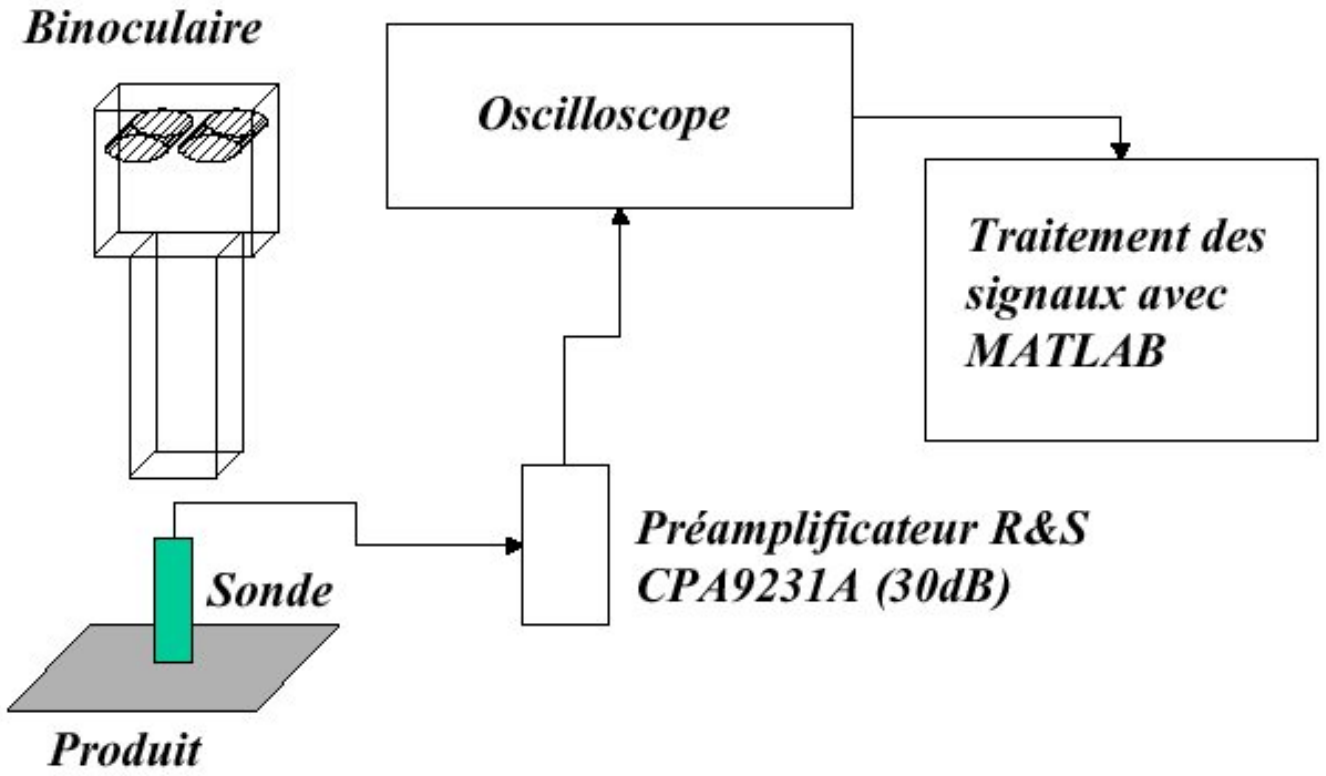
Principe : Les courants qui circulent dans la puce induisent des champs électromagnétiques qui sont susceptibles de donner le même type d'information que le courant.

Différence : L'information est plus locale. On peut déplacer la micro-sonde électromagnétique au dessus de la zone qui nous donnera le plus d'informations (exemple : co-processeur cryptographique).

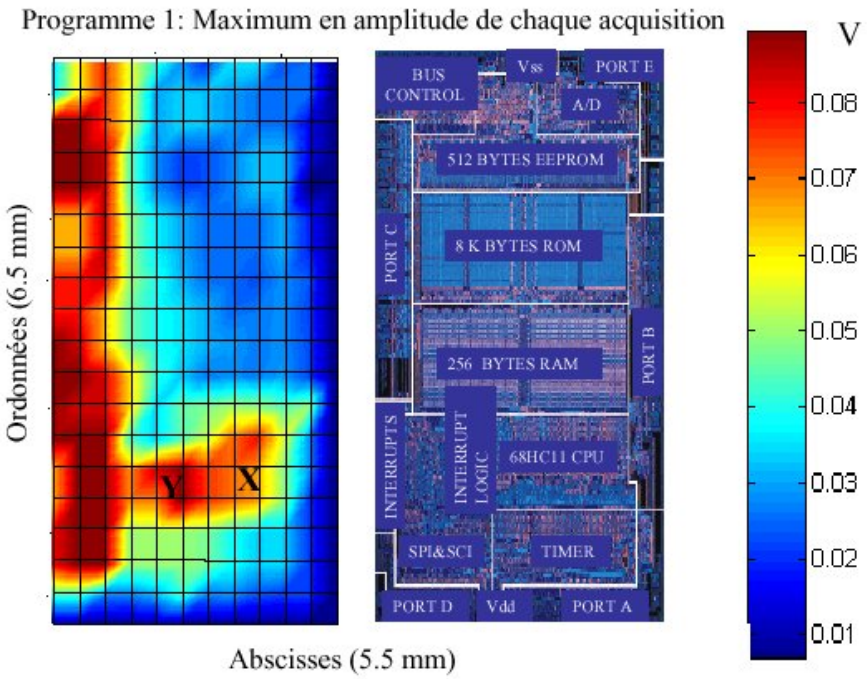
Avantage : Insensible aux contre-mesures physiques tels que l'ajout de bruit en sortie ou le lissage de la consommation globale de courant.

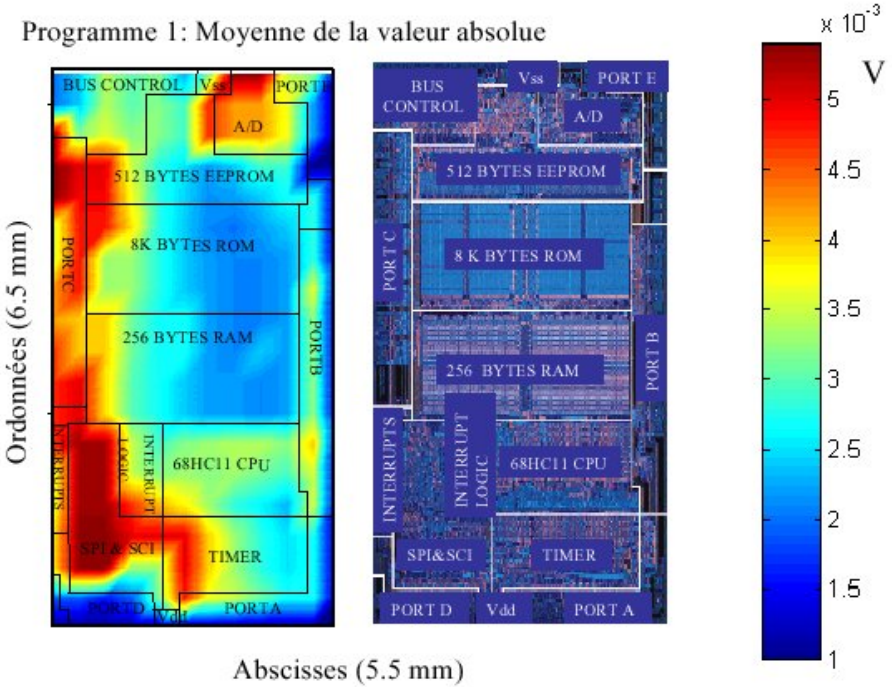
Inconvénient : La reproductibilité des mesures est difficile.

Le dispositif de cartographie EM

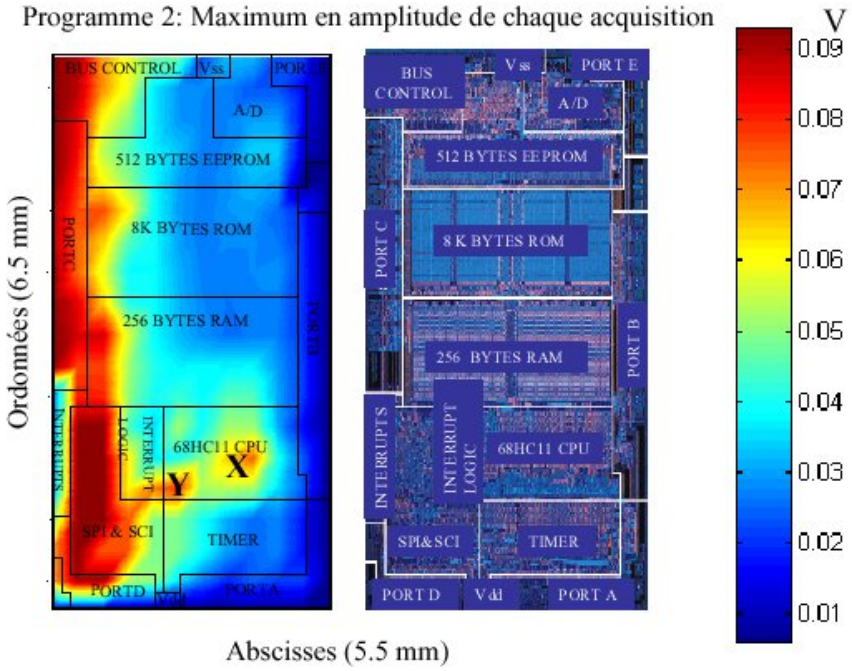


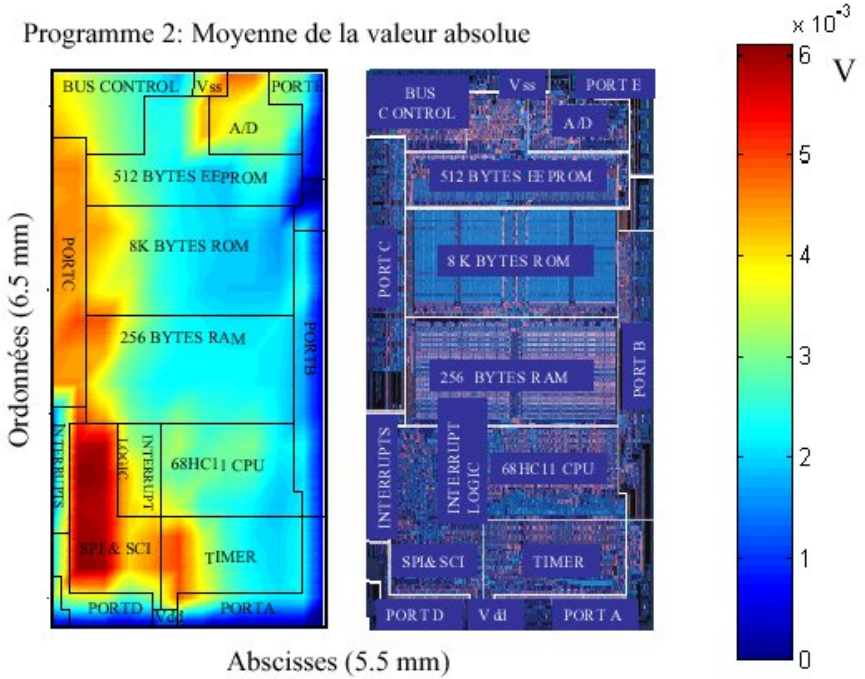
Cartographie pour l'algo 1





Cartographie pour l'algo 2





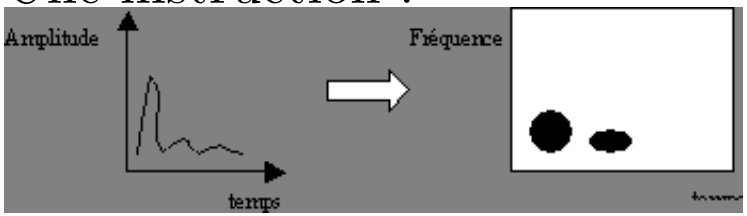
Attaques EM

- ☞ la SEMA (Simple EM Analysis)
- ☞ la DEMA (Differential EM Analysis)
  $\Longrightarrow$ nécessite moins d'acquisitions

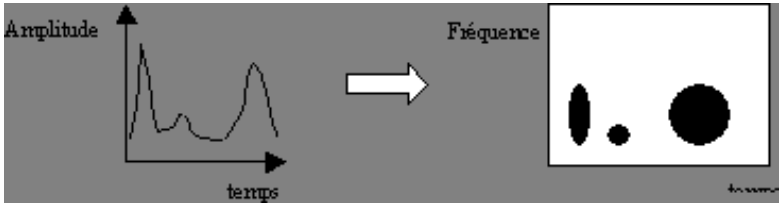
La rétro-conception logicielle

méthode du "dictionnaire" :

Une instruction :



Une autre instruction :



La séquence des deux :

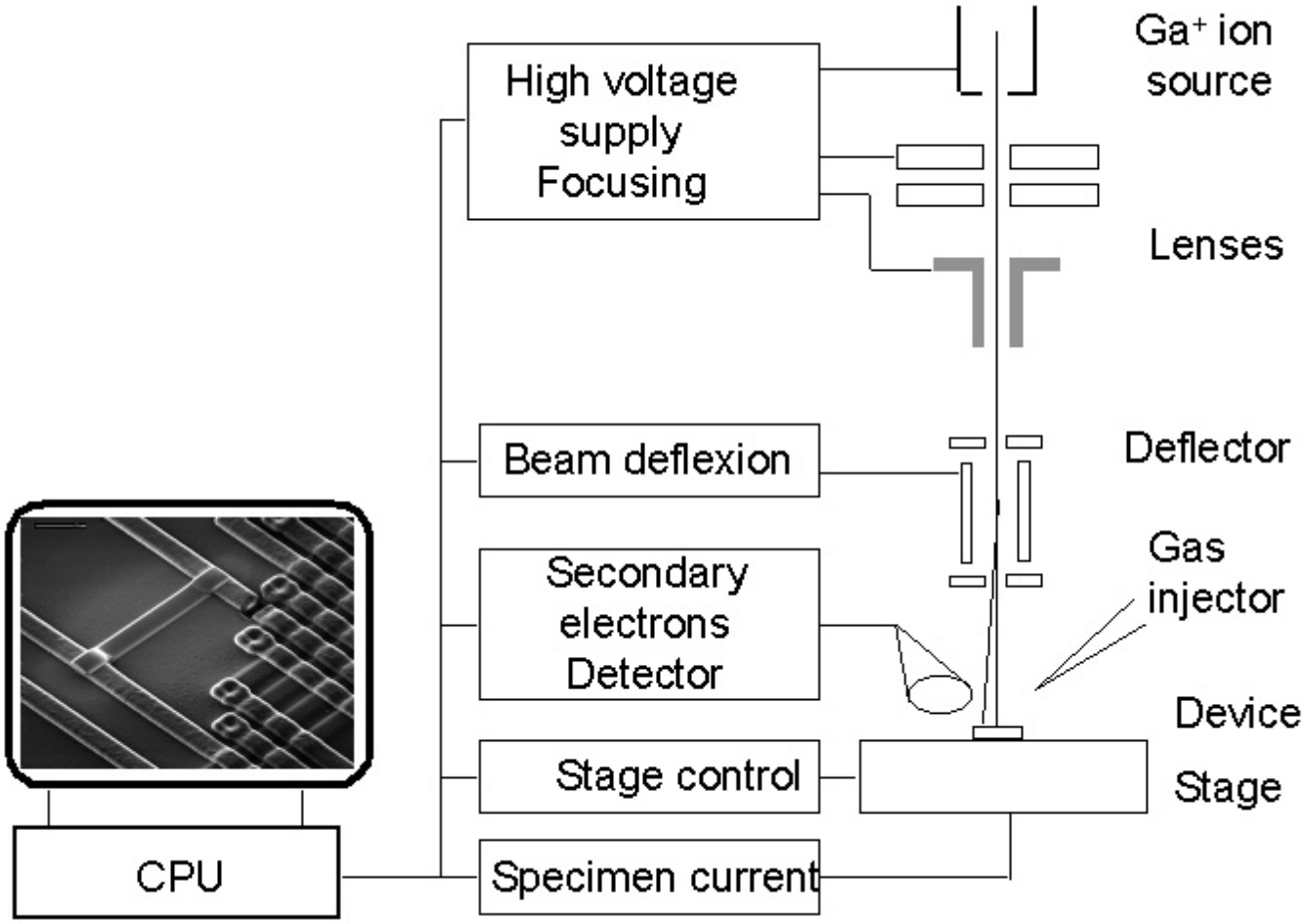
Utilisation possible de la consommation en courant ou des émissions EM.

Statut : recherches en cours.

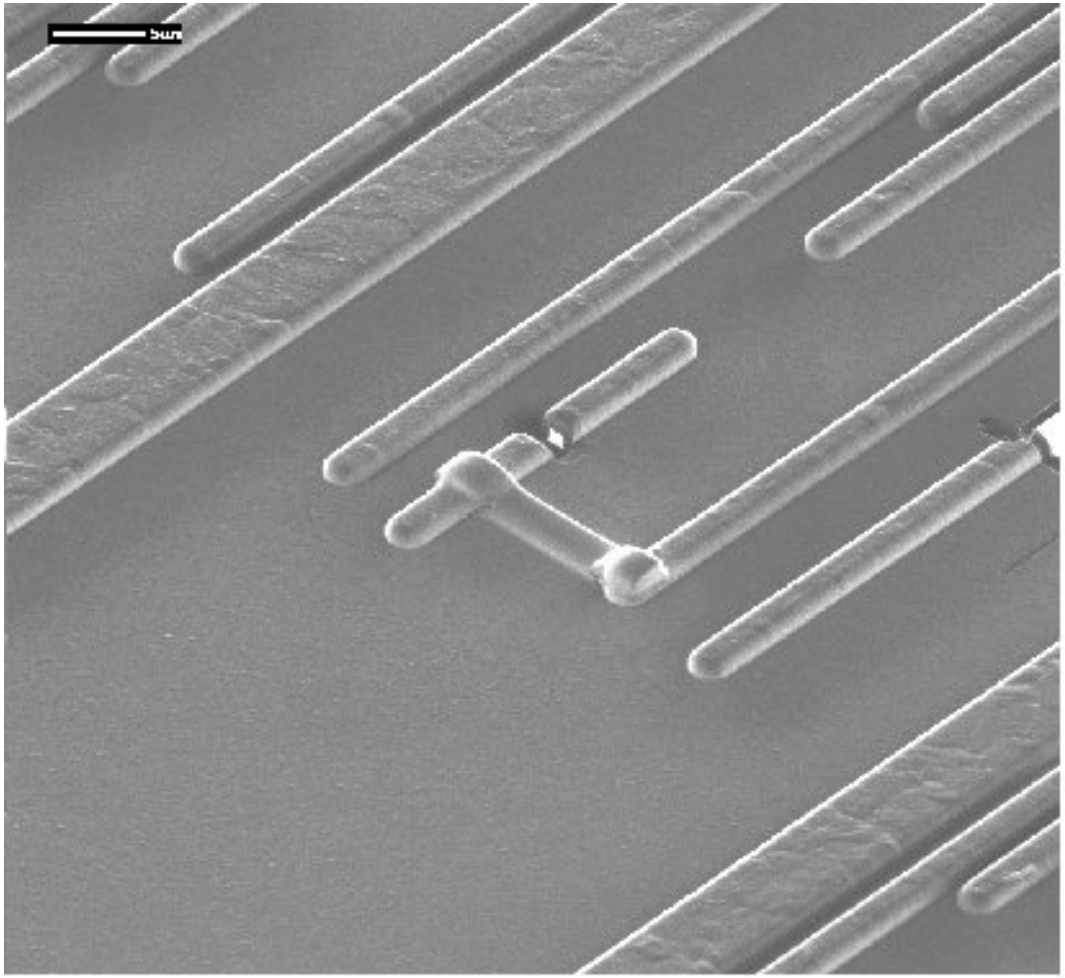
Invasives

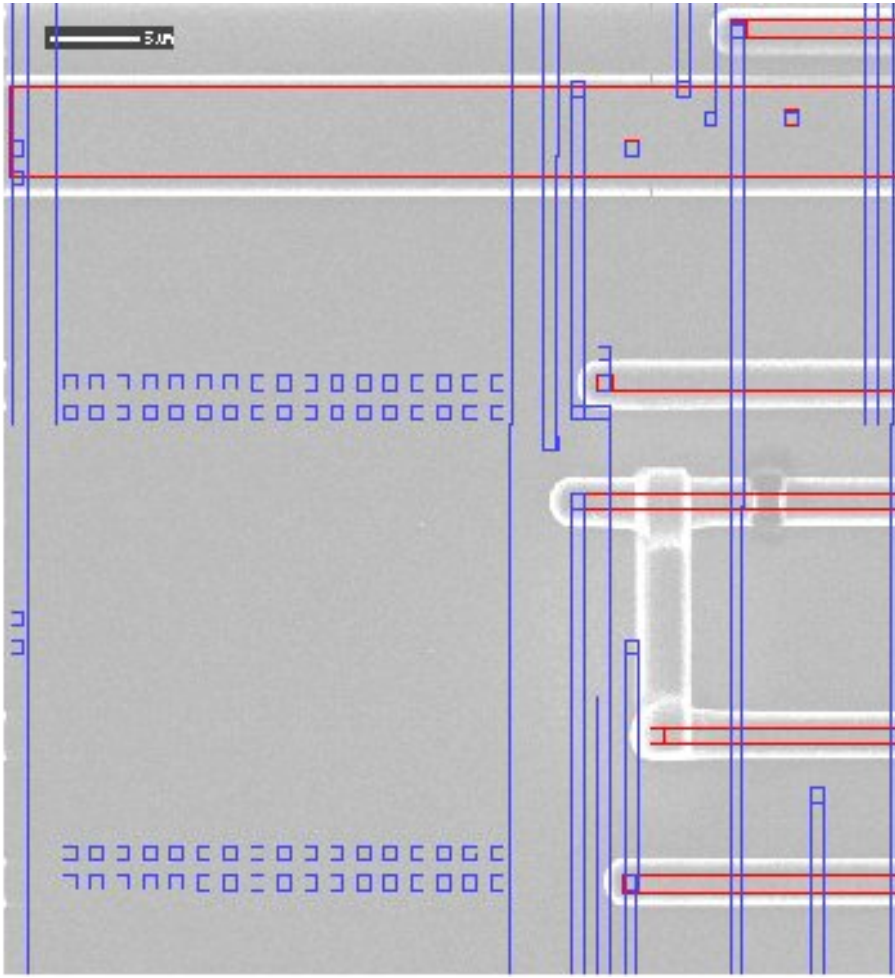
- micro-probing
- modification de circuit (FIB)
- rétro-conception du circuit

Le FIB


High voltage
supply
Focusing
Ga+ ion
source
Lenses
Beam deflexion
Deflector
Secondary
electrons
Detector
Gas
injector
Device
Stage control
Stage
CPU
Specimen current

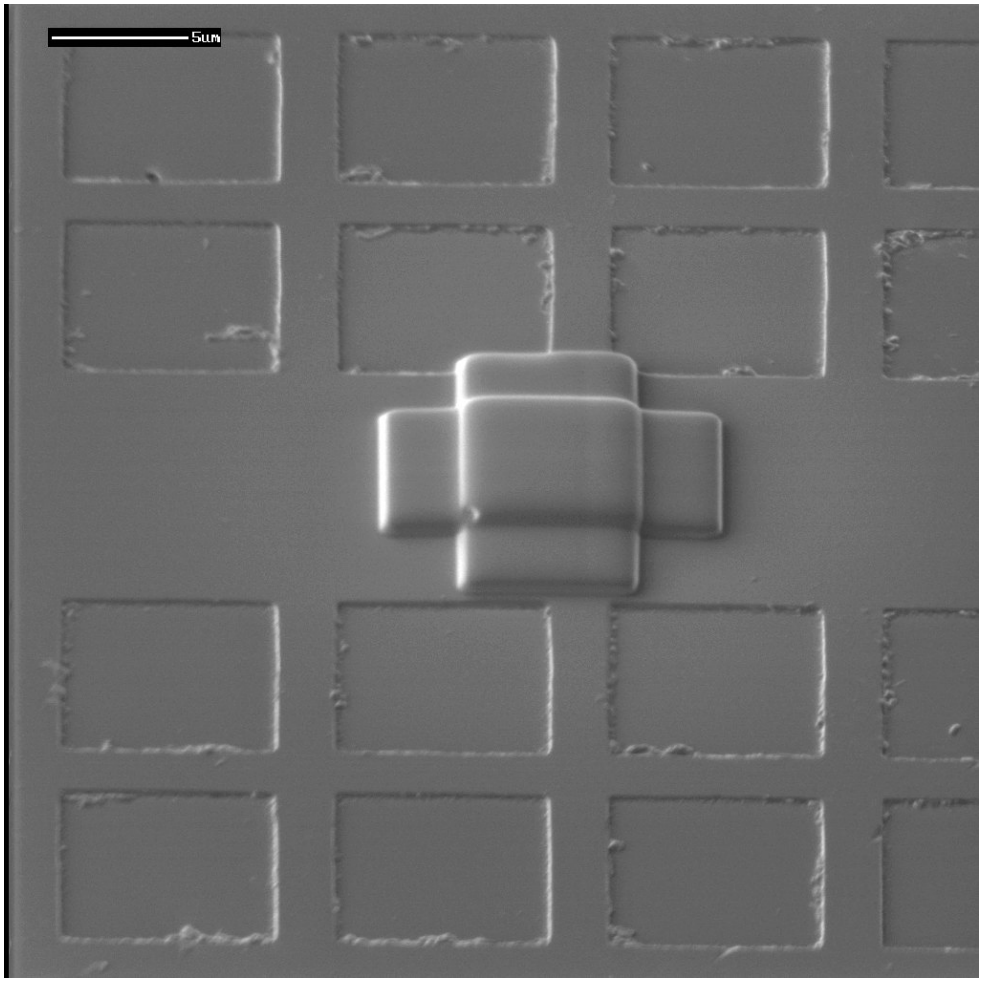
Modifications de circuits (1/2)





Modifications de circuits (2/2)

Micro-probing



Coût

Très cher !