

# **Présentation de la carte à puce et son utilisation dans les réseaux informatiques**

Damien Sauveron

[damien.sauveron@unilim.fr](mailto:damien.sauveron@unilim.fr)

<http://damien.sauveron.free.fr/>

*Colloque Franco-Algérien*

*« Applications de l'arithmétique aux télécommunications »*

*14 décembre 2007*

# Plan

## **La carte à puce et les concepts de base**

- Qu'est-ce qu'une carte à puce ?

- Court historique

- La carte à microprocesseur et les technologies de communication

- Les applications

## **Les sécurités**

- Au niveau physique

- Au niveau logicielle

- Au niveau de l'environnement de production

- Méthodes formelles & Test

- Évaluation sécuritaire et certification

## **Les attaques**

- Non invasive

- Invasive

## **Les cartes du futur**

## 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

En 1970, K. Arimura au Japon dépose un brevet sur la carte à puce.

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

## La carte à microprocesseur

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

Microprocesseur (CPU) : 8, 16 ou 32 bits (à architecture CISC ou RISC)

ROM : 32 à 256 Ko

- stocke le COS (Card Operating System) et des données permanentes
- Figée en usine

EEPROM : 32 à 256 Ko

- (Electrical Erasable Programmable Read Only Memory)
- mémoire persistante => stocke les données applicatives
- problèmes : durée de vie limitée et temps d'accès lent

RAM : 1 à 4 Ko

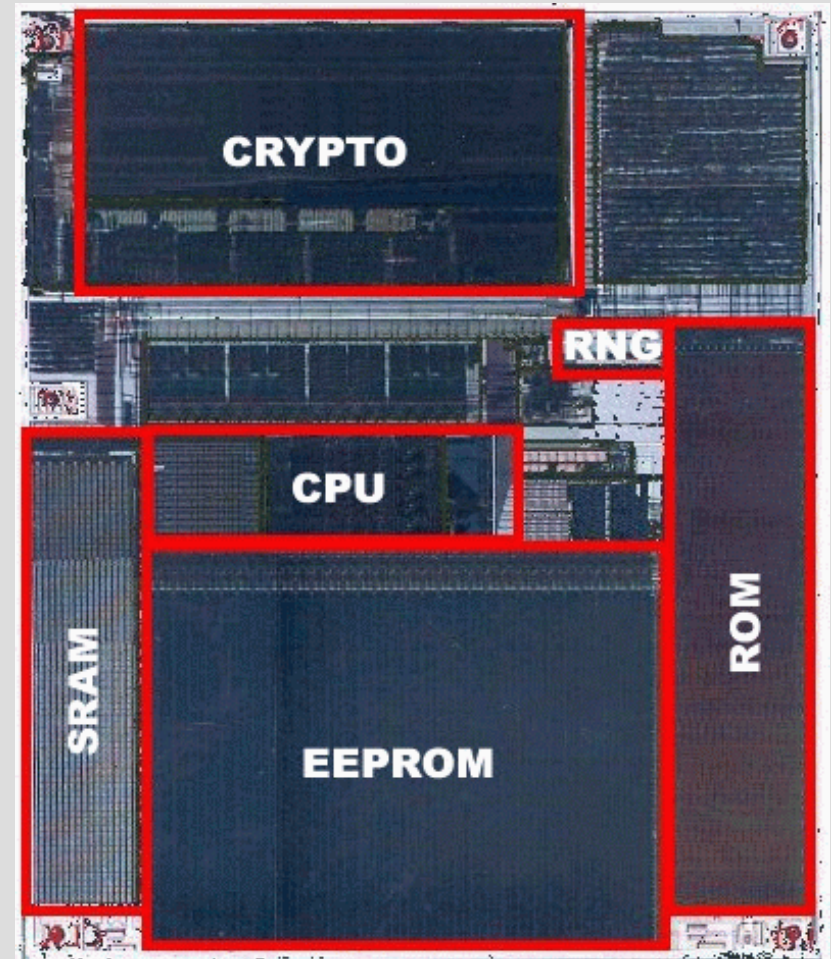
- mémoire de travail
- avantages : durée de vie illimitée et temps d'accès rapide

Coprocasseur cryptographique

Générateur de nombres aléatoires (RNG)

Vers de nouvelles mémoires (+ rapide, + grosse) :

- FeRAM
- Flash
- MRAM



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

## Comparaison d'architecture

|           | Smart Card | Personal Computer | Ratio  |
|-----------|------------|-------------------|--------|
| RAM       | 1 kbyte    | 128 Mbytes        | 130000 |
| Storage   | 64 kbytes  | 6 Gbytes          | 100000 |
| Baud Rate | 192 kbits  | 100 Mbits         | 500    |
| CPU Speed | 20 Mips    | 500 Mips          | 25     |

**les cartes à contact  
versus  
les cartes sans contact  
versus  
les cartes dual-interface**

## Carte à contact

### Suit le standard ISO 7816

Communication série via huit contacts => insertion dans un lecteur de carte

### Problèmes :

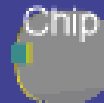
l'insertion et le retrait sont des facteurs d'usure de la carte  
orientation de la carte dans le lecteur

## Contact Smart Card

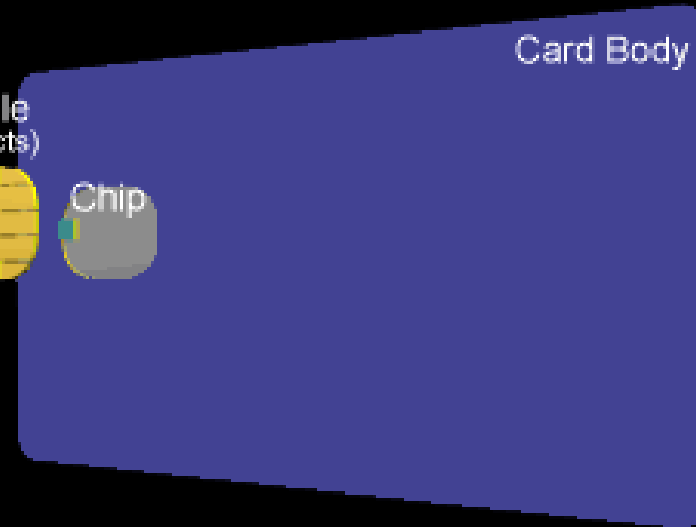
Module  
(Contacts)



Chip



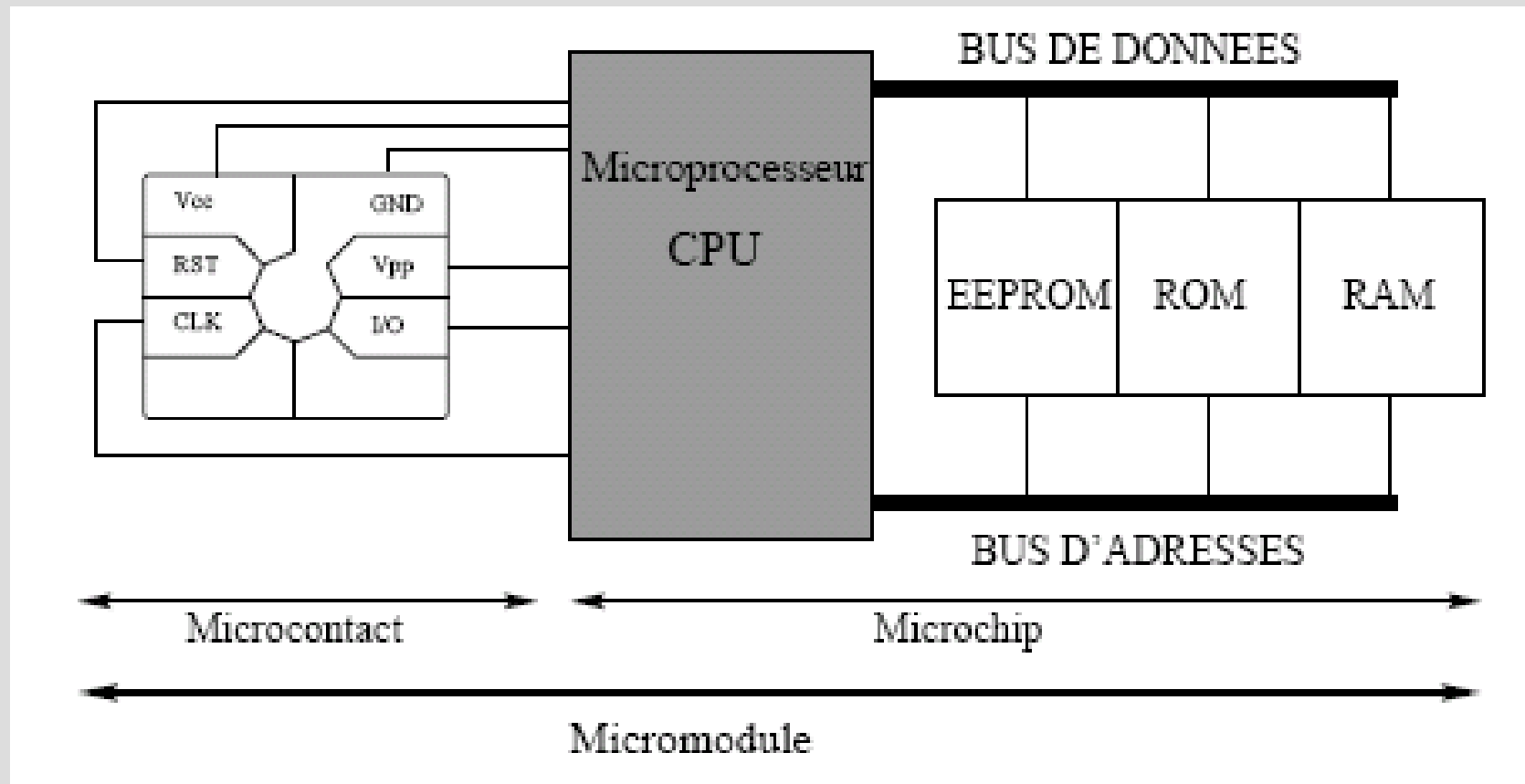
Card Body



## La carte à contact

Son fonctionnement, l'oblige à être insérée dans un lecteur de carte.  
Elle utilise une communication série via huit contacts.

1 seule ligne I/O => semi duplex



## Carte sans contact

Communication via une antenne dans la carte

Récupère son énergie d'un couplage capacitif ou d'un couplage inductif

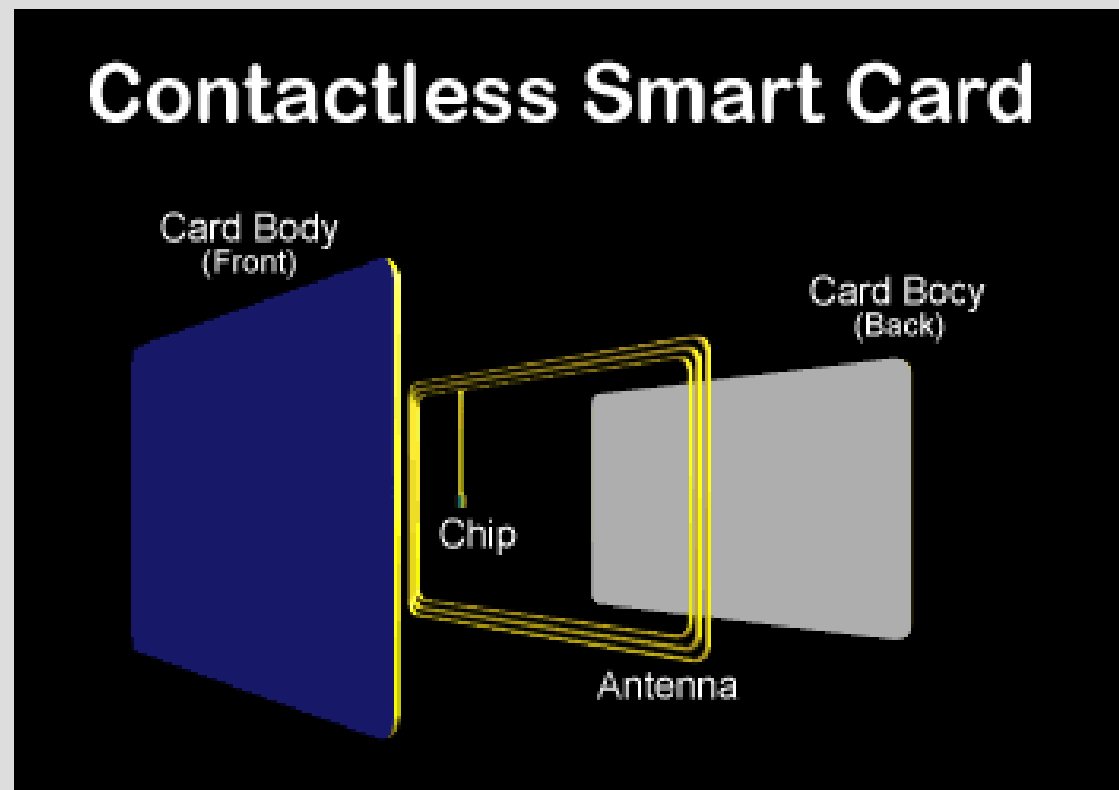
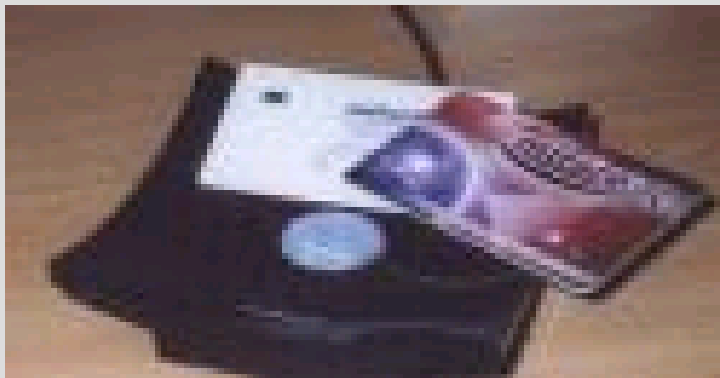
Suit le standard ISO 14443

### Problèmes :

distance de communication limitée (environ 10 cm)

temps de transaction est de l'ordre de 200 ms => limite les données à échanger

le coût élevé



## **La carte combi**

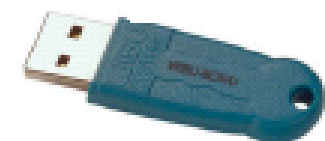
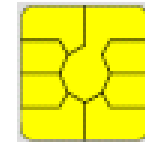
**C'est une combinaison entre :**

la carte à contact  
et la carte sans contact

**Ces deux possibilités de communication en font une carte « idéale ».**

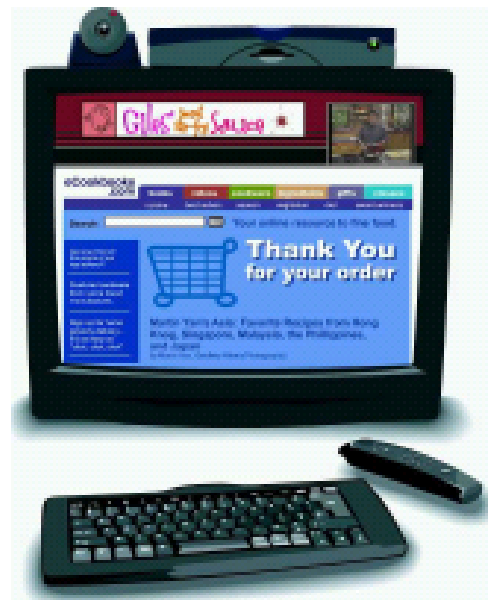
## Les différentes formes et interfaces de communication

- Cartes avec contact (Module SIM GSM)
  - ISO 7810, 7816-1, 7816-2
  - USB ou OTG (USB pour mobile)
- Cartes sans contact
  - Plusieurs normes
- Cartes Hybrides
  - combinaison contact et sans contact
- Boutons
  - Produits iButton (bus DS 1-Wire)
  - JavaRing (iButton monté sur bague)
- Dongle
  - Série, parallèle, USB



## Les terminaux cartes

- Contact / sans contact
- Simple / complexe (keypad, LCD, multi-slot, biometrie ...)



## Pourquoi utiliser la carte à puce ?

### Avantages :

- la sécurité
- la portabilité
- la facilité d'utilisation
- la personnalisation

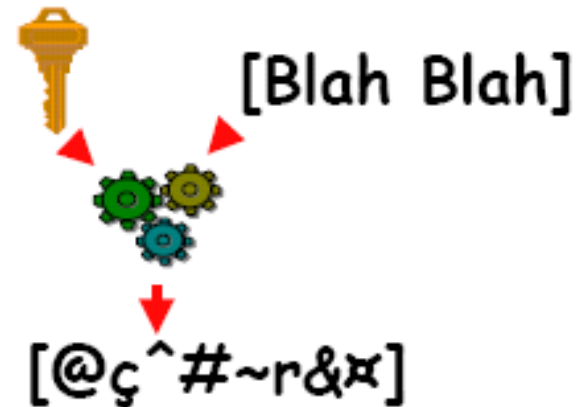
- Tamper resistance
  - Storage



- Portability



- Tamper resistance
  - Processing



- Ease of use
- Onboard key generation
- Cost

# Applications

l'industrie des télécommunications

l'industrie bancaire et monétaire (B0', EMV, Monéo, proton)

le secteur de la santé

l'industrie audiovisuelle avec la télévision à péage, ...

le porte-monnaie électronique (CEPS)

les transports en commun.

le contrôle d'accès physique de personnes à des locaux, ...

l'identification : à des sites sur l'Internet, ...

les applications de fidélité

les "e-services"

Identification gouvernementale (carte d'identité, ...)

## ***Examples of Smart Card Use***



- Mobile Communication



- Banking



- Transport

- Identity Cards

- Physical Access Control

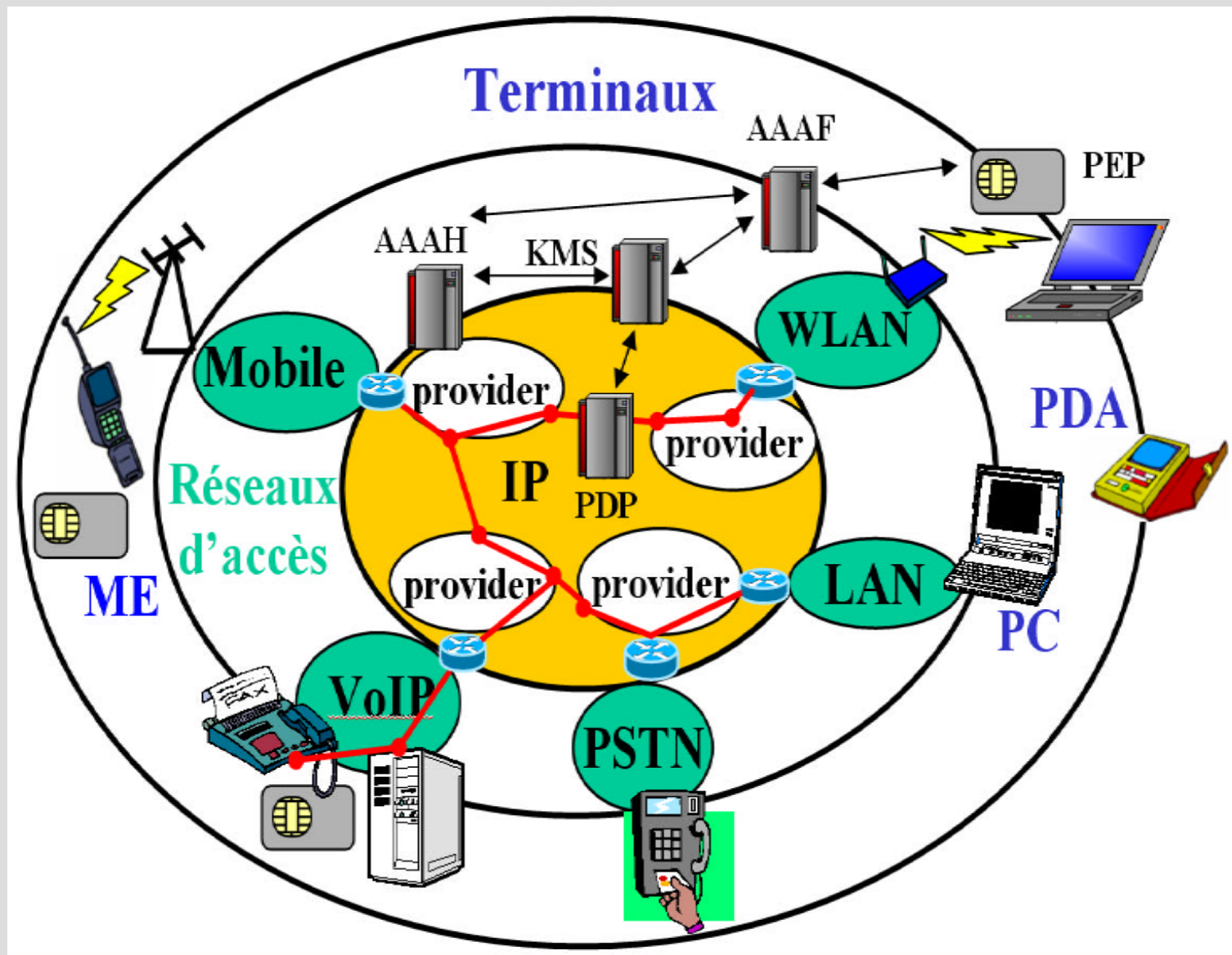


- IT Access Control

- Satellite TV chip card



## La carte : omniprésente !



# Applications de sécurisation

- Sécurité physique :
  - Accès à des locaux : ouverture et fermeture de porte (suivi de passages)
    - ex : Ministère des finances, Gemplus
- Sécurité logique :
  - Contrôle d'accès logique à un serveur
    - Identification, Authentification
  - Protection de messagerie électronique
    - Signature électronique et chiffrement des messages
  - Renforcement de la sécurité des transactions sensibles
    - Ordres de virements internationaux  
(chiffrement de code porteur)
  - Vote électronique

# Applications d 'identification

- Identification d 'une personne :
  - dans une entreprise (contrôle horaire),
  - sur un réseau informatique (login),
  - sur un réseau téléphonique (carte SIM),
  - ou dans la société (carte d 'identité)
- Ex: Le GSM et la carte SIM
  - Abonné localisé par la carte (le terminal utilisé devient celui du porteur)
  - Facturation directe de l 'abonné
  - Sécurité physique (carte)+logique (NIP)
  - Stockage de données personnelles (agenda)
  - 1,22 milliards de cartes SIM livrés en 2005

# Applications Actuelles des Cartes

- Différents secteurs porteurs
  - Les Télécommunications : Cartes Pré-payées, carte SIM
    - Recherche tj + de services,  $\forall$  le coût
  - Les Banques : Porte-monnaie Électronique, Carte Bancaire
    - Recherche de coût de fonctionnement le plus faible
  - La Santé : Carte patient, carte professionnels de santé
    - Recherche la sécurité d ' informations sensibles
- Sous l 'impulsion du GSM,  
la carte doit offrir de + en + de services

# Futures Applications

PARTIELLEMENT DÉJÀ FAIT!

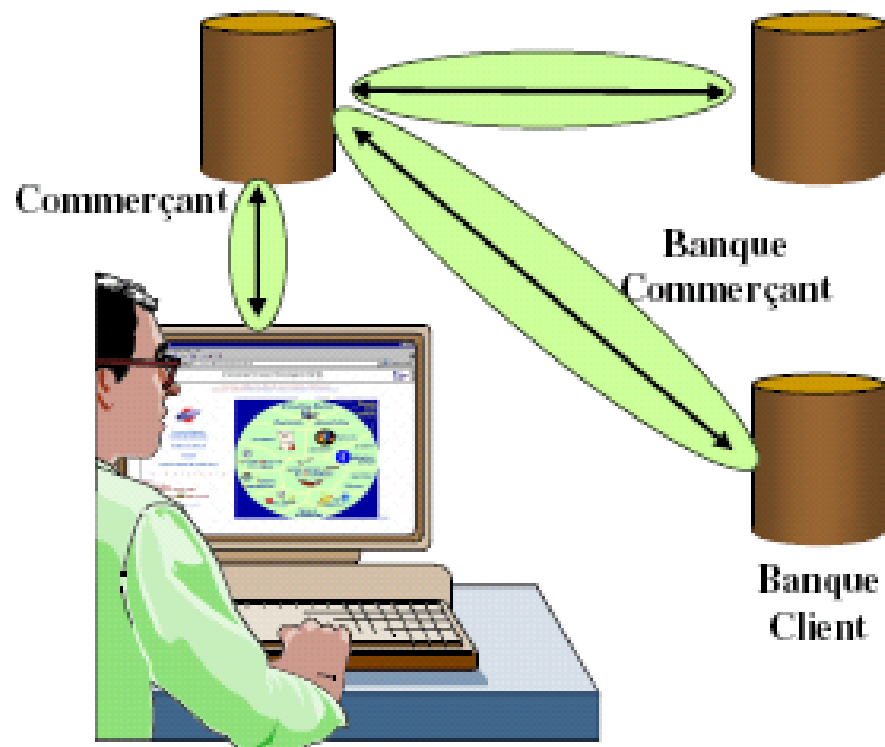
- La Carte « bookmark » ou Portail
  - Toutes les informations propres à l'utilisateur sont stockées dans la carte
  - configuration des serveurs mails et news,
  - liste des signets
  - Liste des mots de passe
- La Carte à Mémoire Etendue
  - La carte contient des liens vers des informations stockées sur des serveurs anonymes
  - Permet de laisser les informations sur le réseau sans problème de sécurité
  - L'information peut être cryptée, et la carte est utilisée pour décrypter
- La Carte pour personnaliser un terminal générique
  - CESURE
  - Déploiement des composants de l'application terminal

DÉJÀ FAIT!

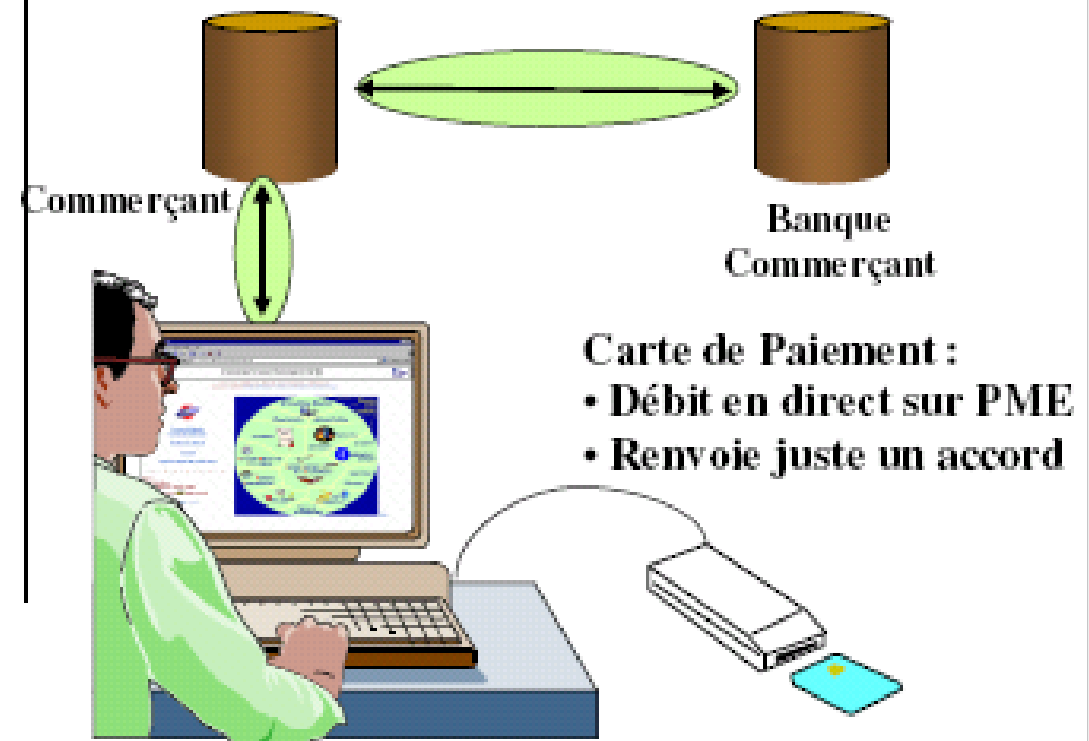
# Futures Applications

- La carte et les paiements distribués

Actuellement



Bientôt



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**

**Le micromodule est monolithique => difficile de distinguer ses différents composants**

**un numéro de série unique**

**l'utilisation de mémoire de type PROM**

**blindage physique du composant (grille, grille active, ...)**

**des détecteurs de conditions anormales (tension, fréquence, température, lumière, ...)**

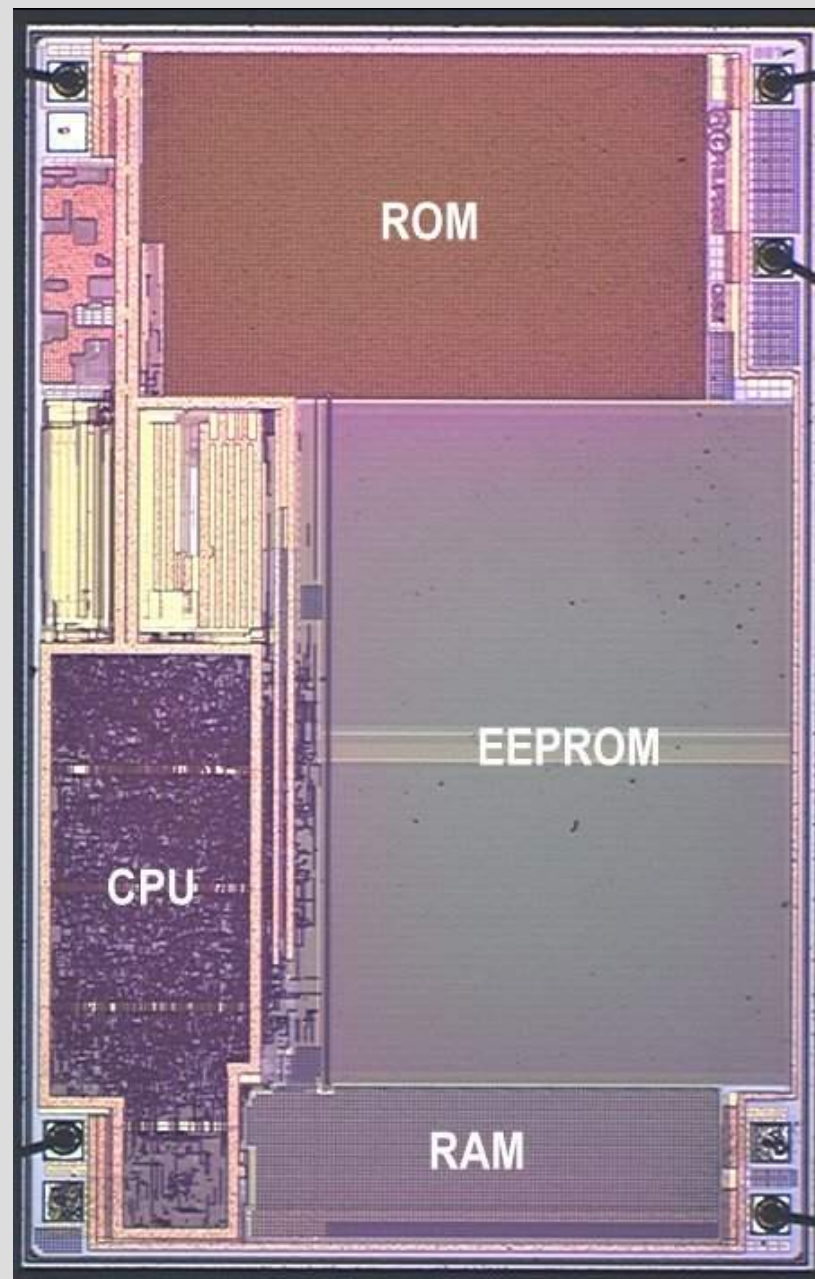
**brouillage des informations dans le composant (mémoire, bus, ...)**

**co-processeurs cryptographiques**

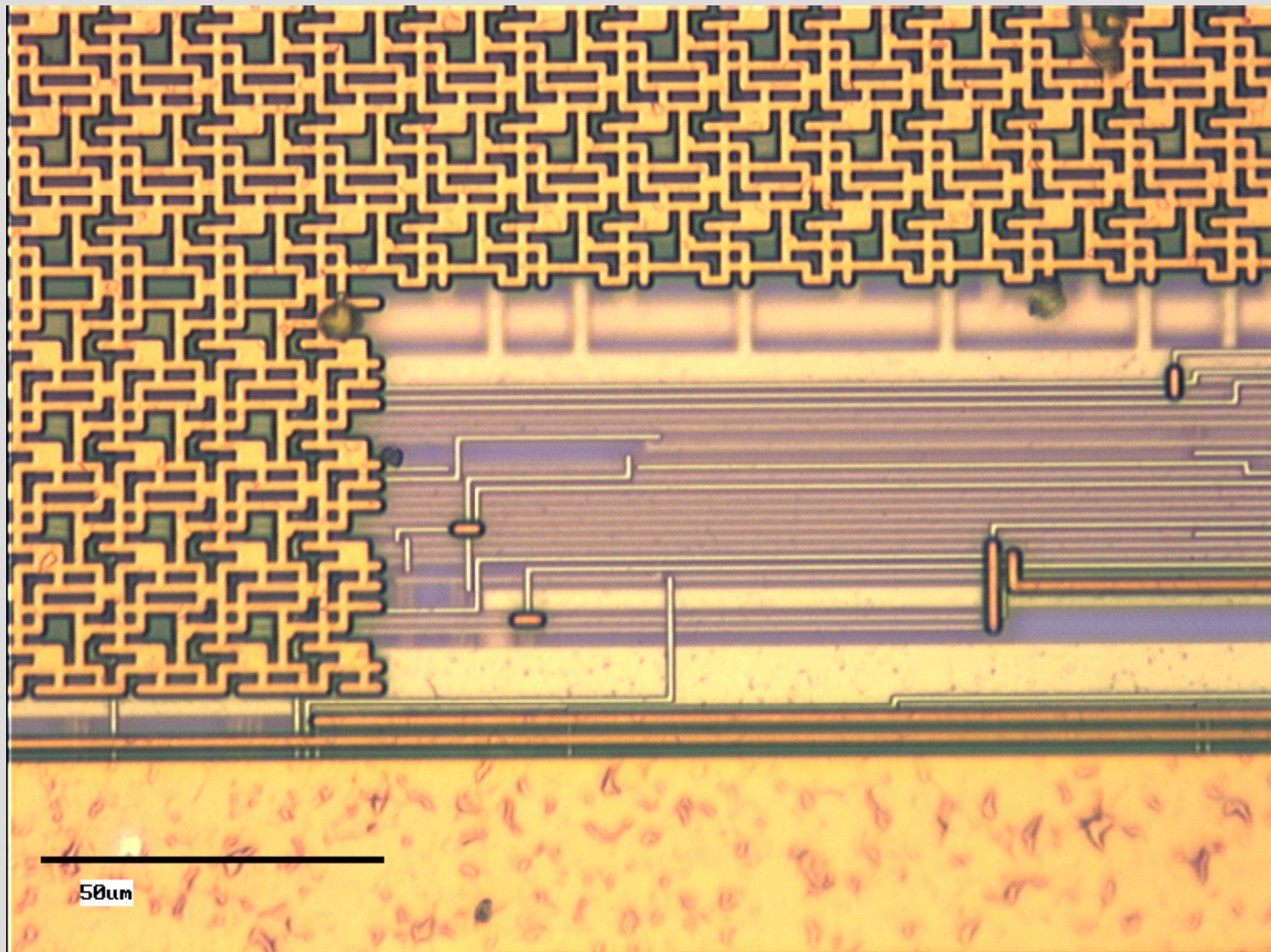
**pompe de charge pour le lissage de la consommation**

**Dual logic, circuit asynchrone**

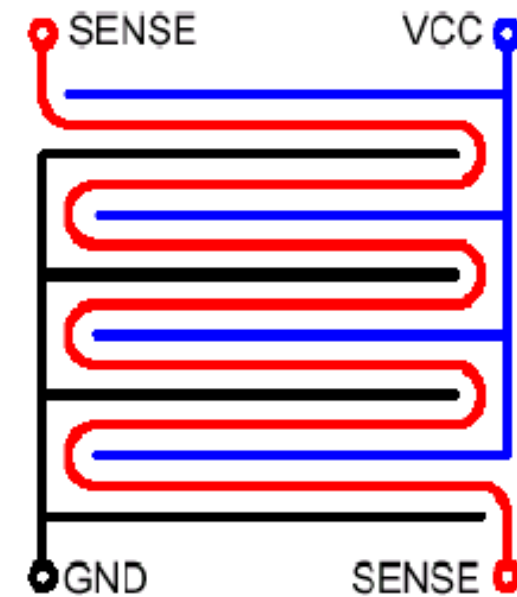
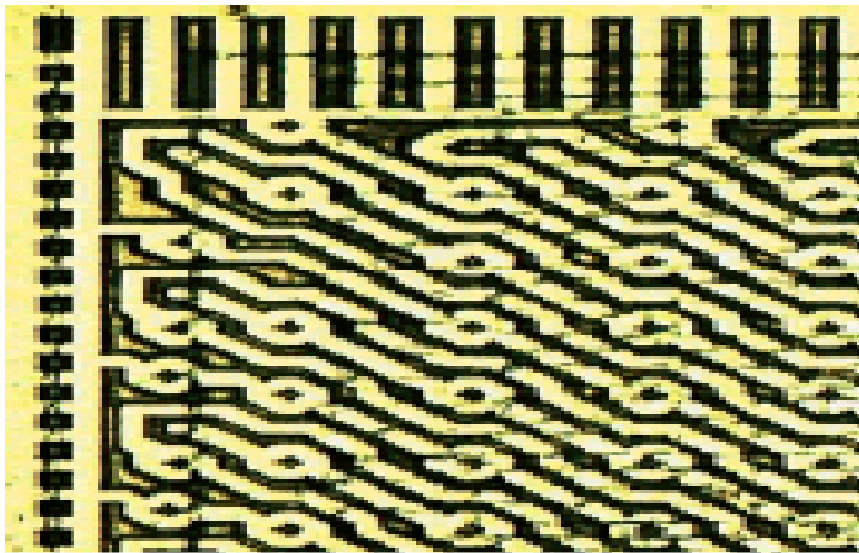
## Une puce



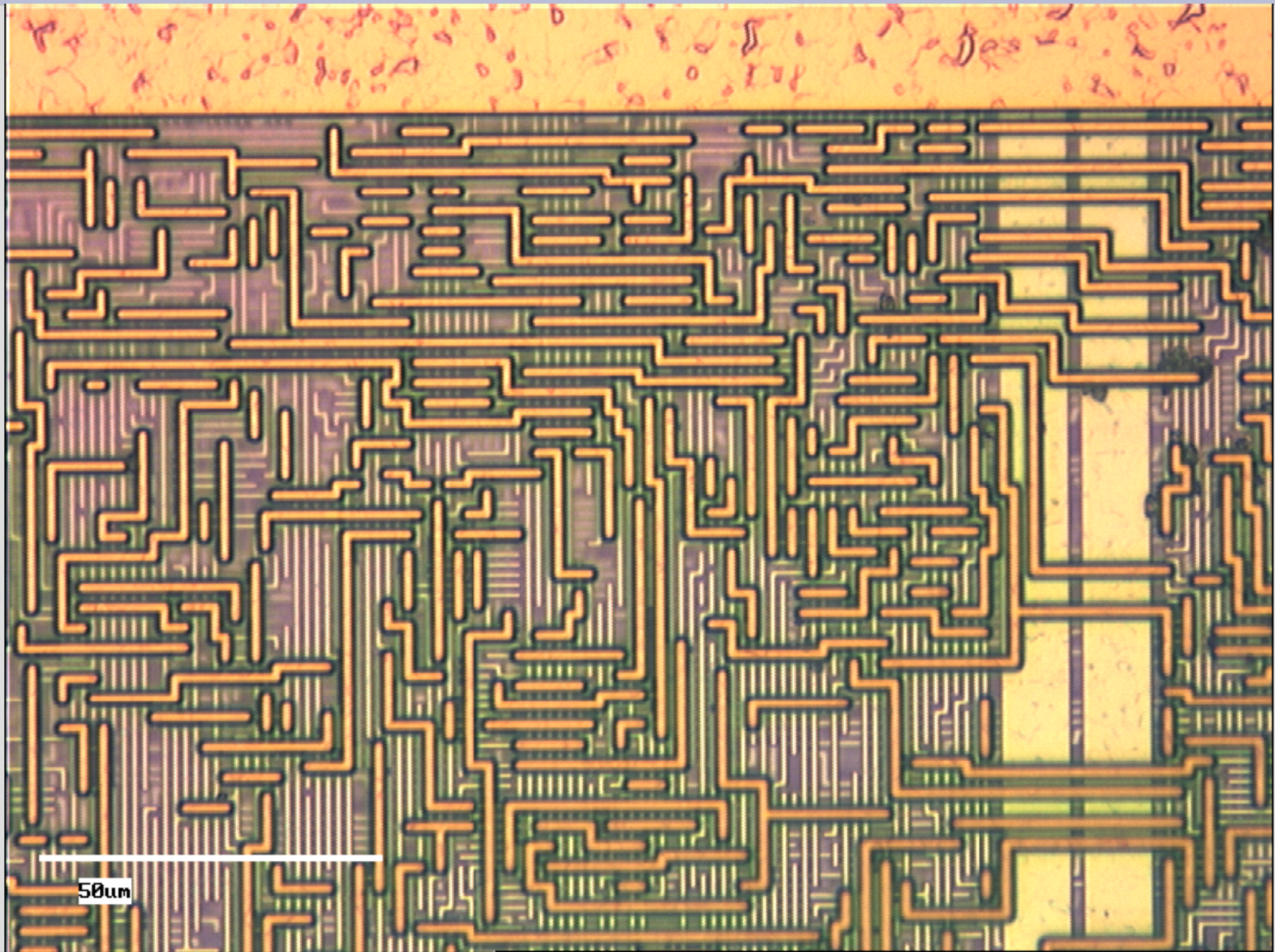
## La grille de protection



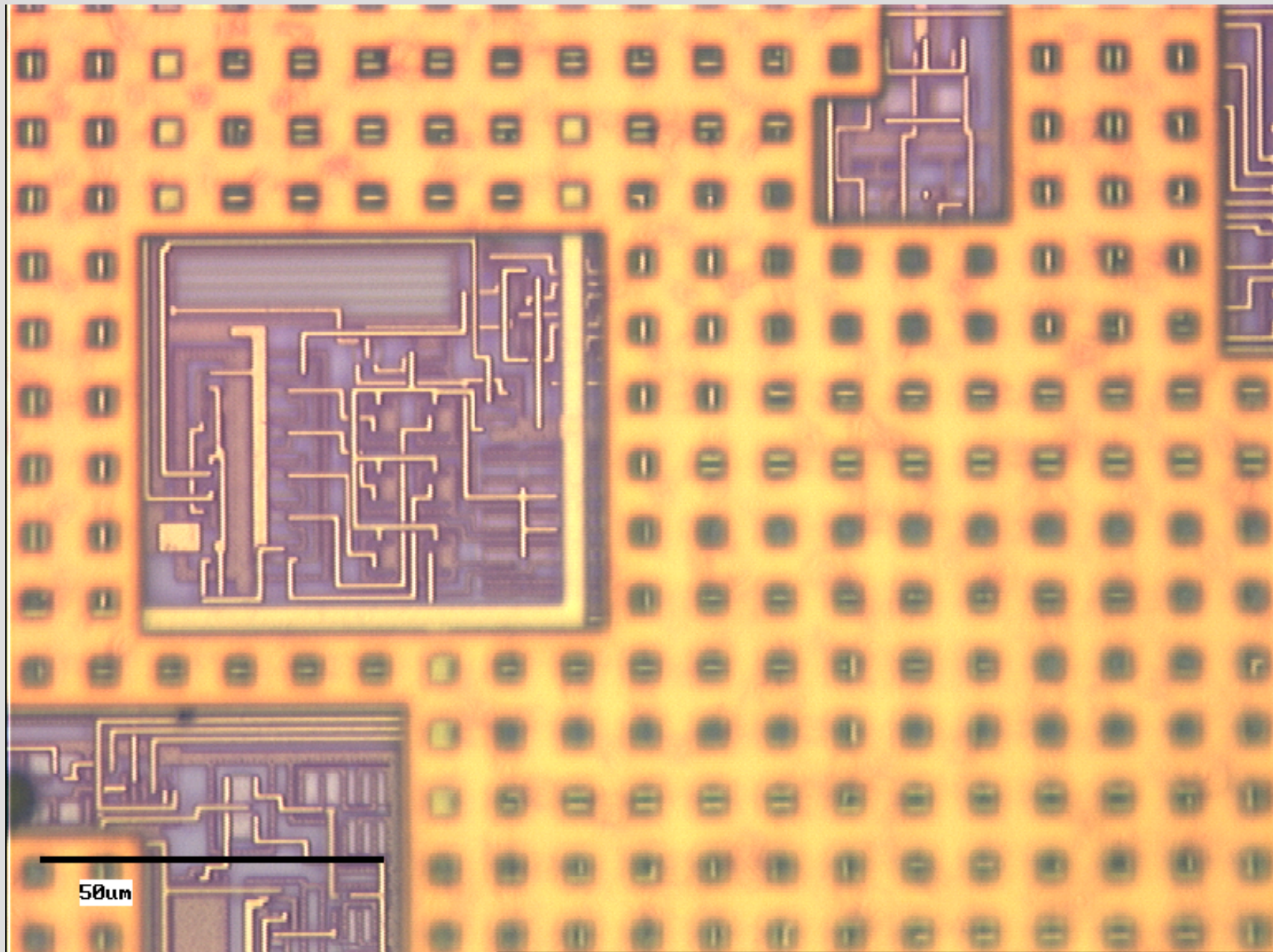
## Grille active



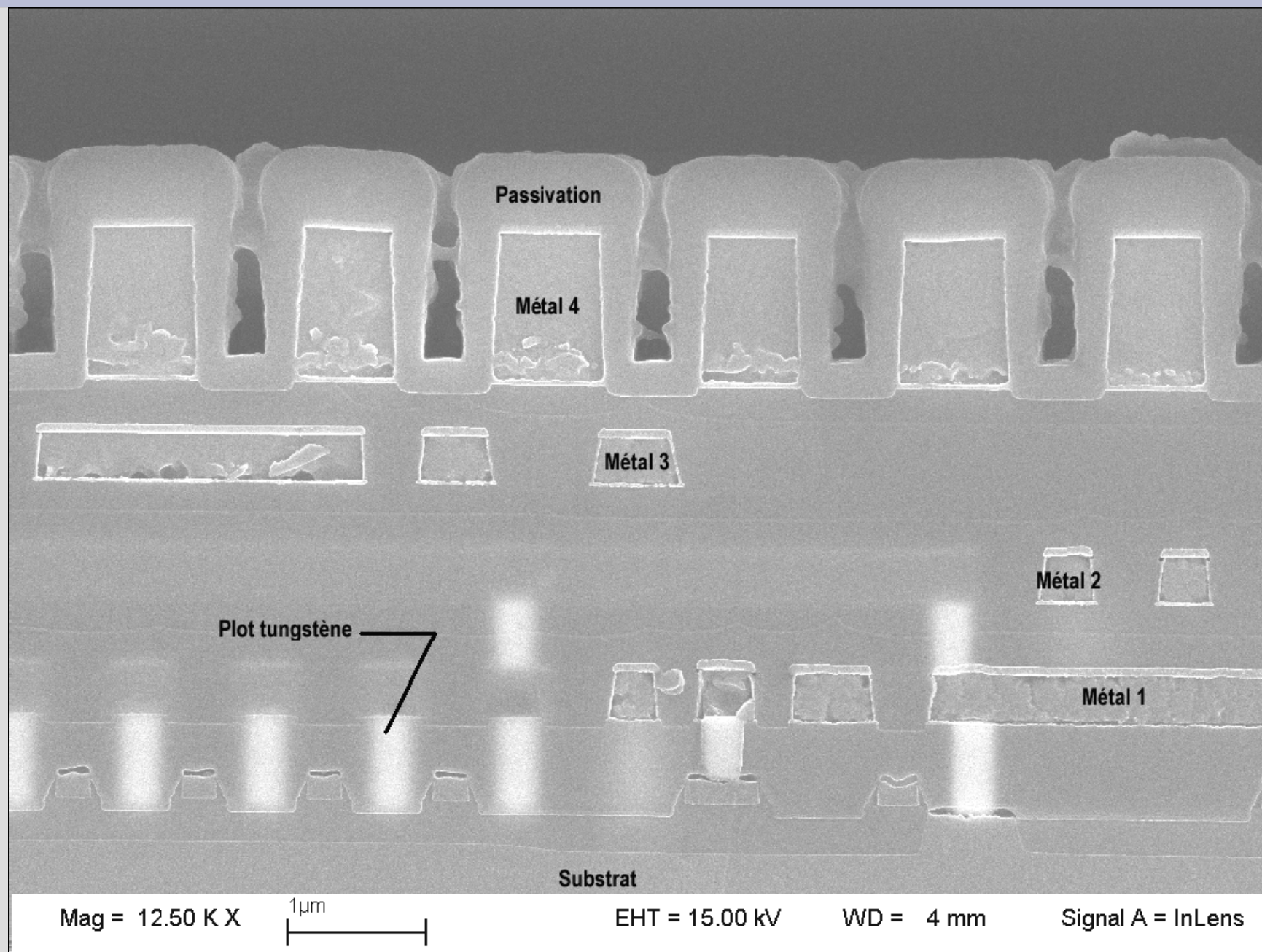
## Le CPU



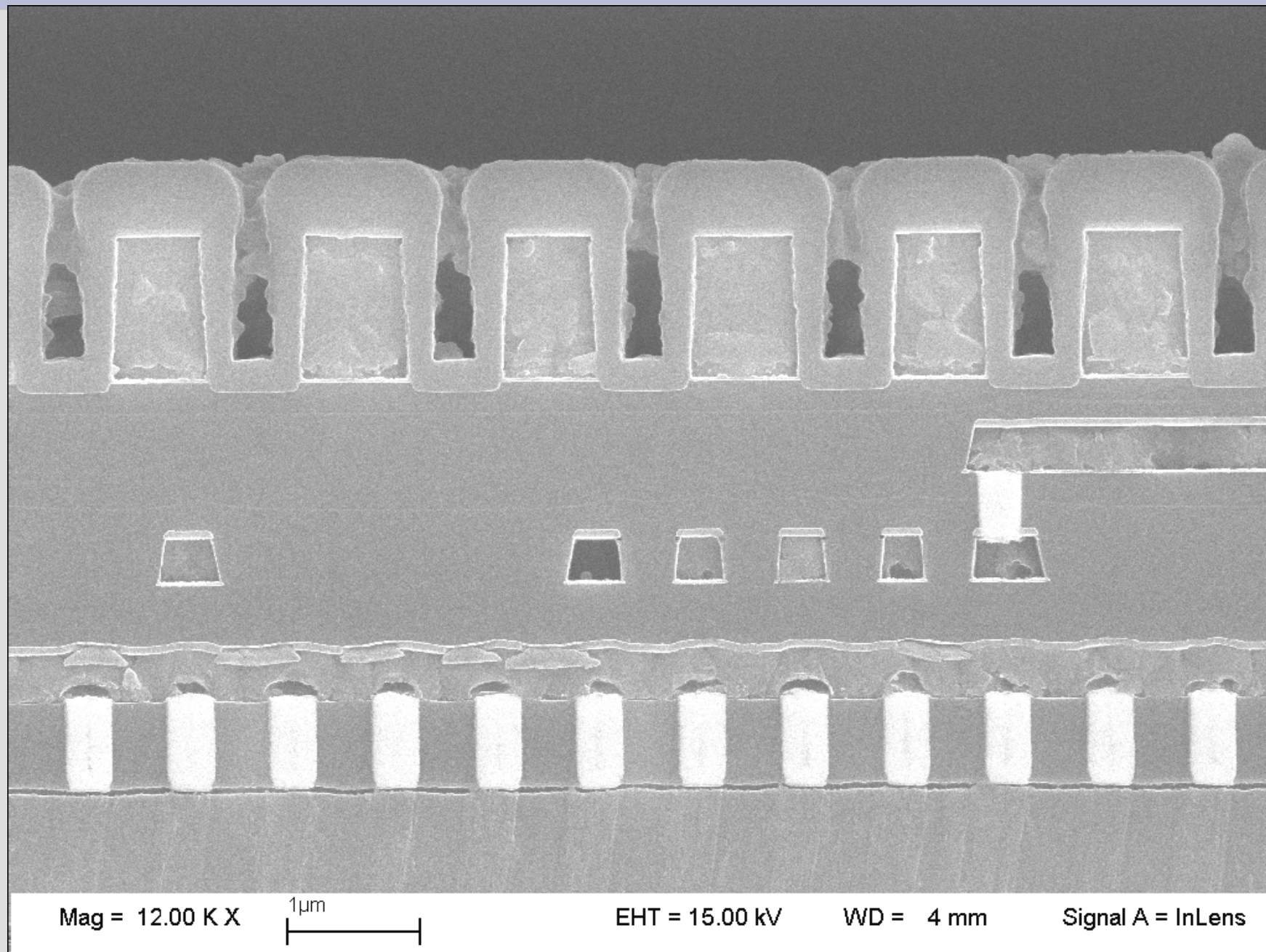
## La partie analogique



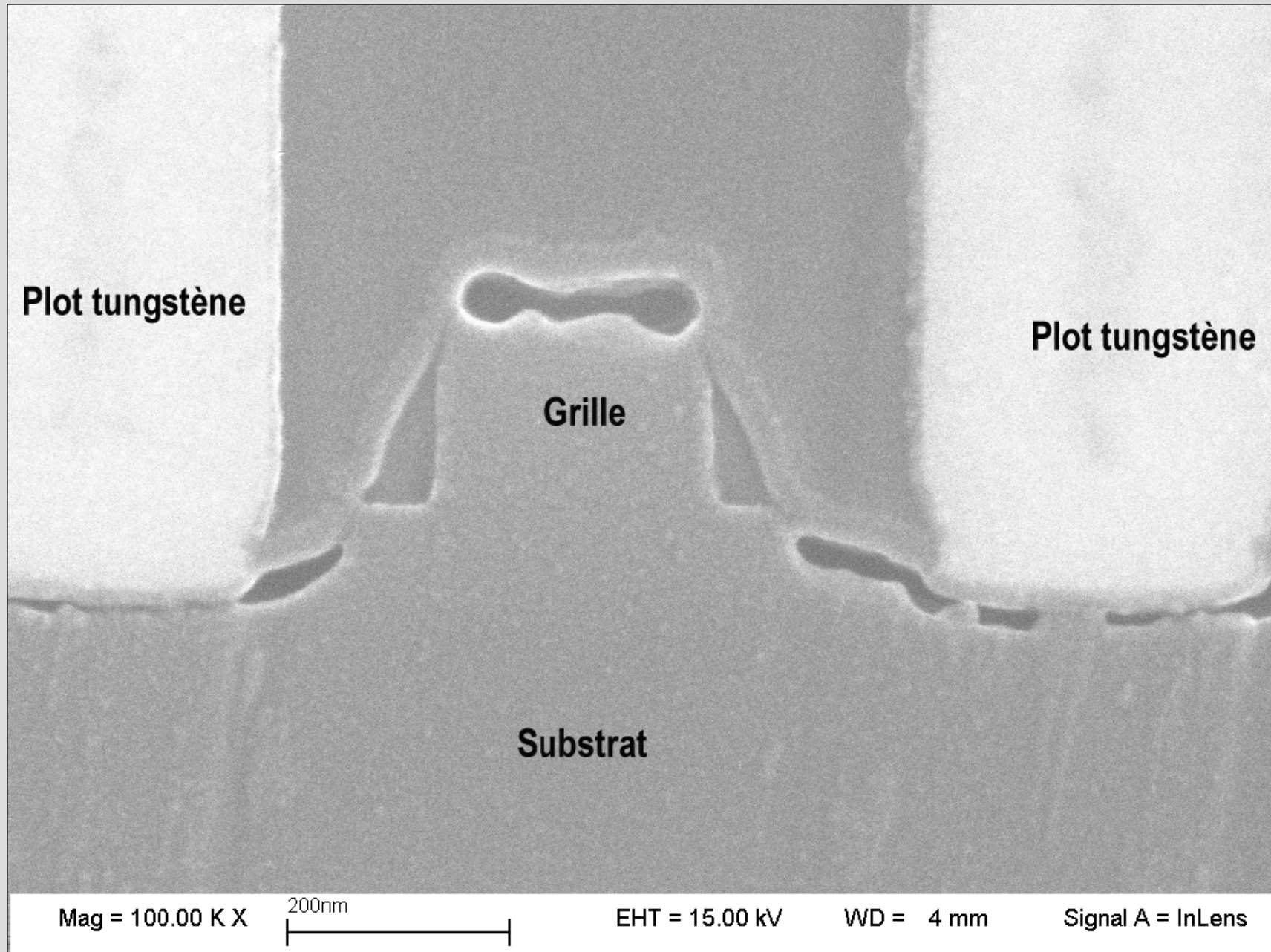
## La coupe d'une puce



## La coupe d'une puce



## La 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 haut niveau de sécurité est assuré  
par la triple alliance de l'électronique,  
de l'informatique et de la cryptographie*

## **Compléments de sécurité : Les méthodes formelles, le test, l'évaluation et la certification sécuritaire**

**Conception formelle de certains partie de l'OS (voire de l'OS complet)**

**Preuve formelle sur des aspects sécuritaire**

**Génération de jeux de tests associés aux spécifications**

**...**

**L'évaluation et la certification sécuritaire**

La carte à puce

—

Les attaques

## Différentes catégories

### **Non invasives**

Le produit reste fonctionnel

### **Invasives**

Le produit est partiellement endommagé

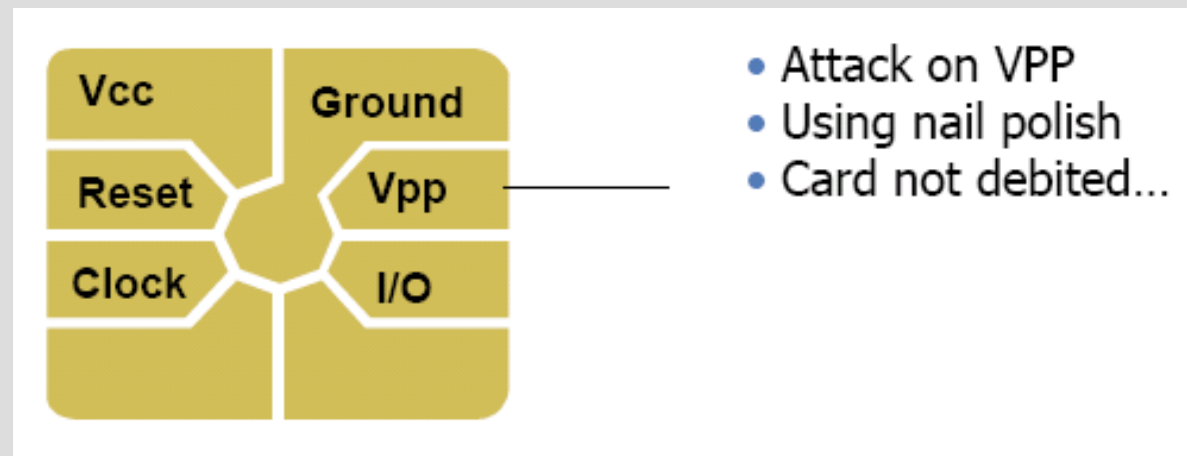
## Non invasives

**modification des conditions opérationnelles ( $V_{cc}$ , F)**

**modification de la température**

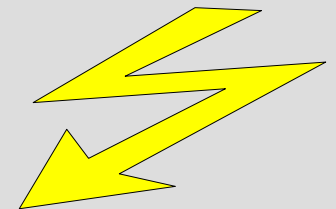
**modification des rayonnements lumineux (UV, rayon X, lumière blanche, IR, ...)**

**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**

=> nombre de cycle d'une instruction ou d'un algorithme.

### **la consommation de courant**

=> 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**

=> Les courants RF entraînent un rayonnement électromagnétique.

## Le matériel

**un oscilloscope numérique,**

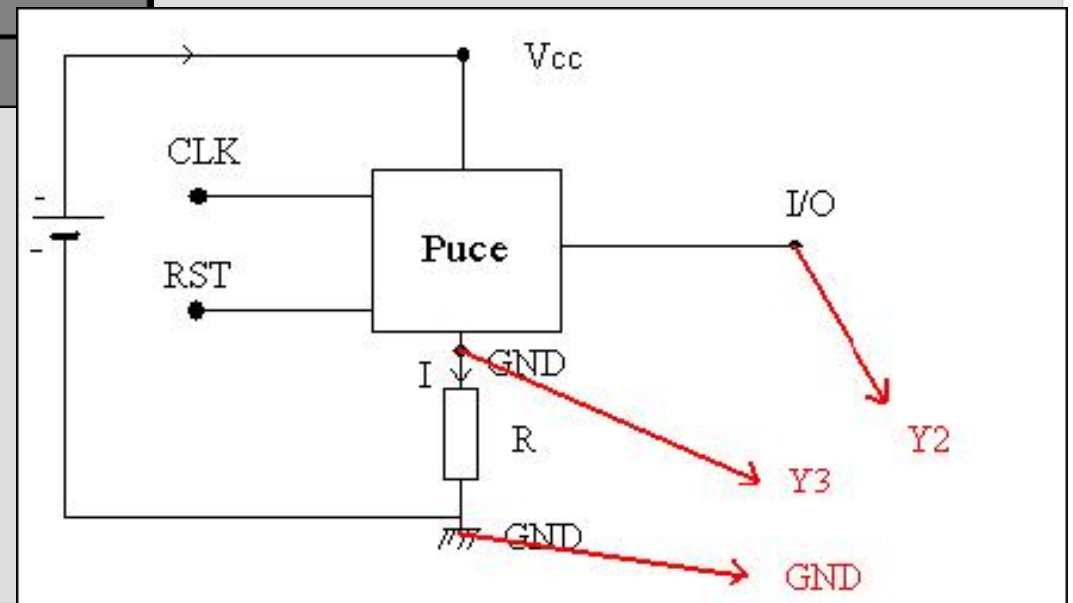
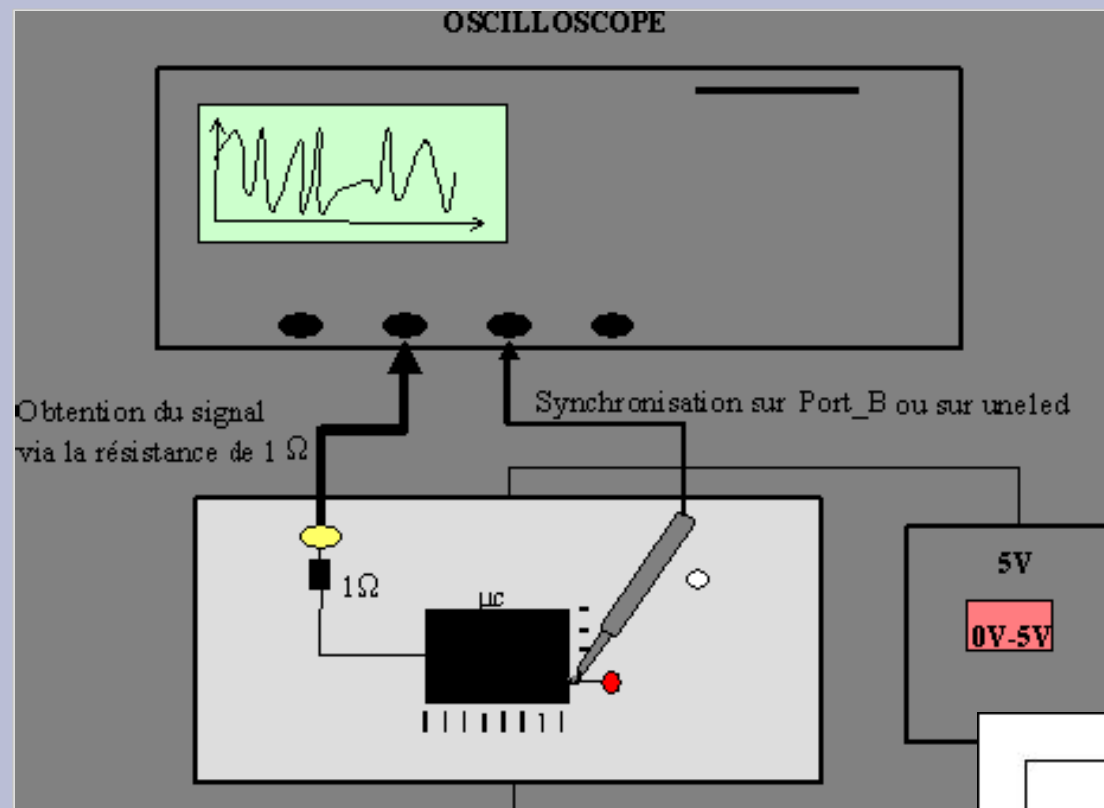
**un lecteur de carte à puce,**

**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 pour suivre la consommation en courant



## La consommation de courant

**Elle est surtout utilisée dans le domaine de la cryptographie.**

**Il existe différentes attaques :**

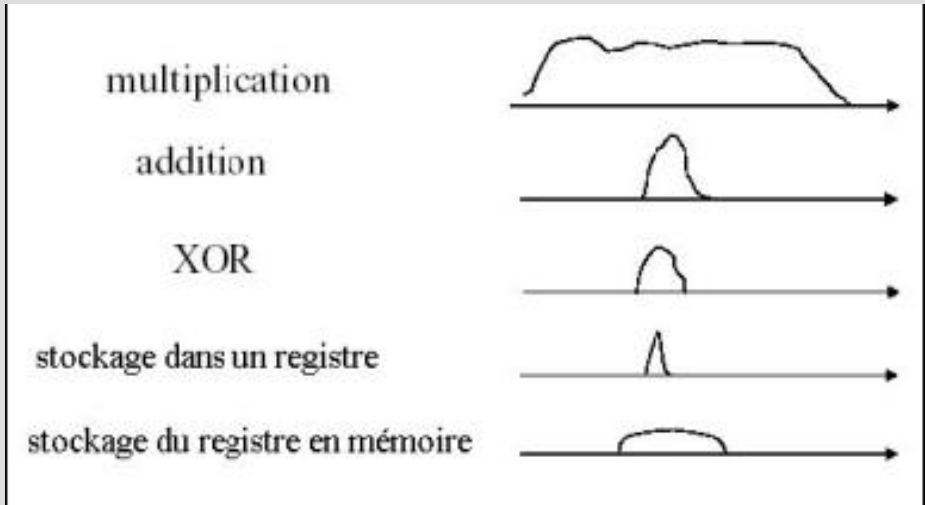
- la SPA (Simple Power Analysis)

- la DPA (Differential Power Analysis)

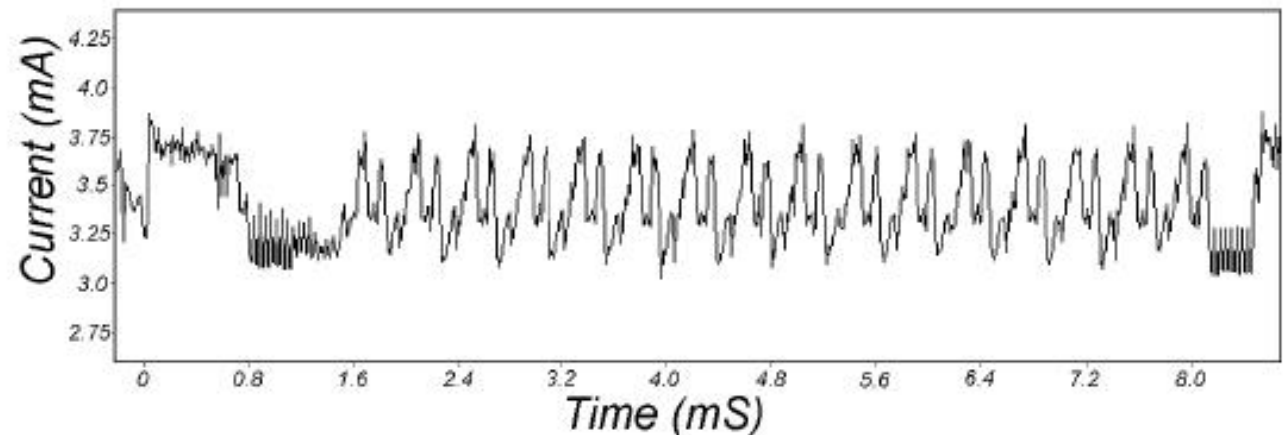
- la HODPA (High Order Differential Power Analysis)

## 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

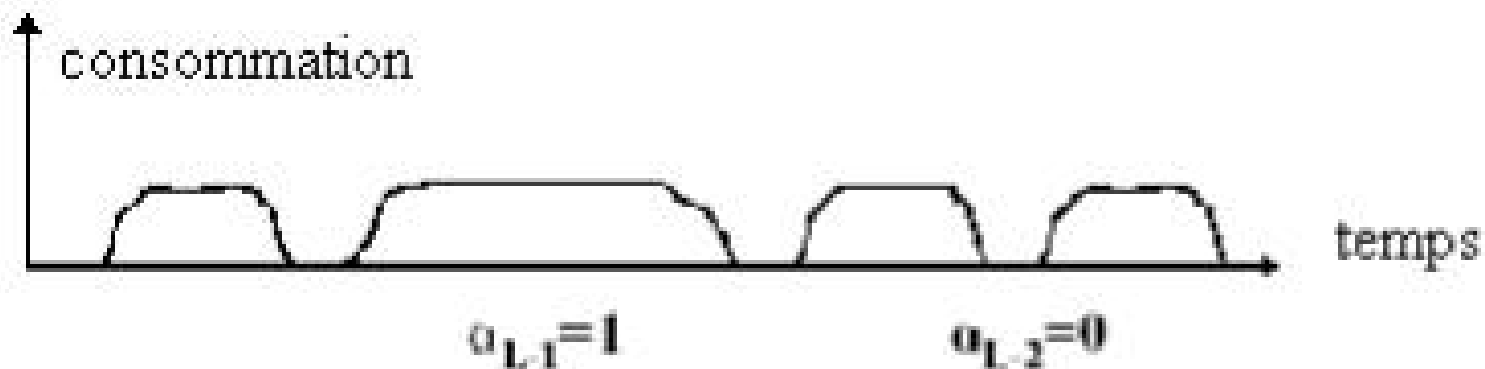
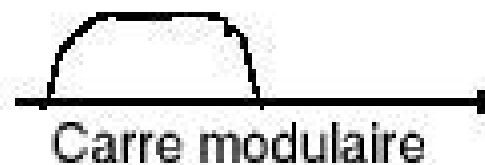
```
s = 1 ;  
for ( i = L - 1 ; i >= 0; i-- ) {  
    s = s*s mod n ;  
    if ( a [ i ] == 1 )  
        s = s*y mod n ;  
}
```

**Signature RSA :  $y^a \bmod n$**

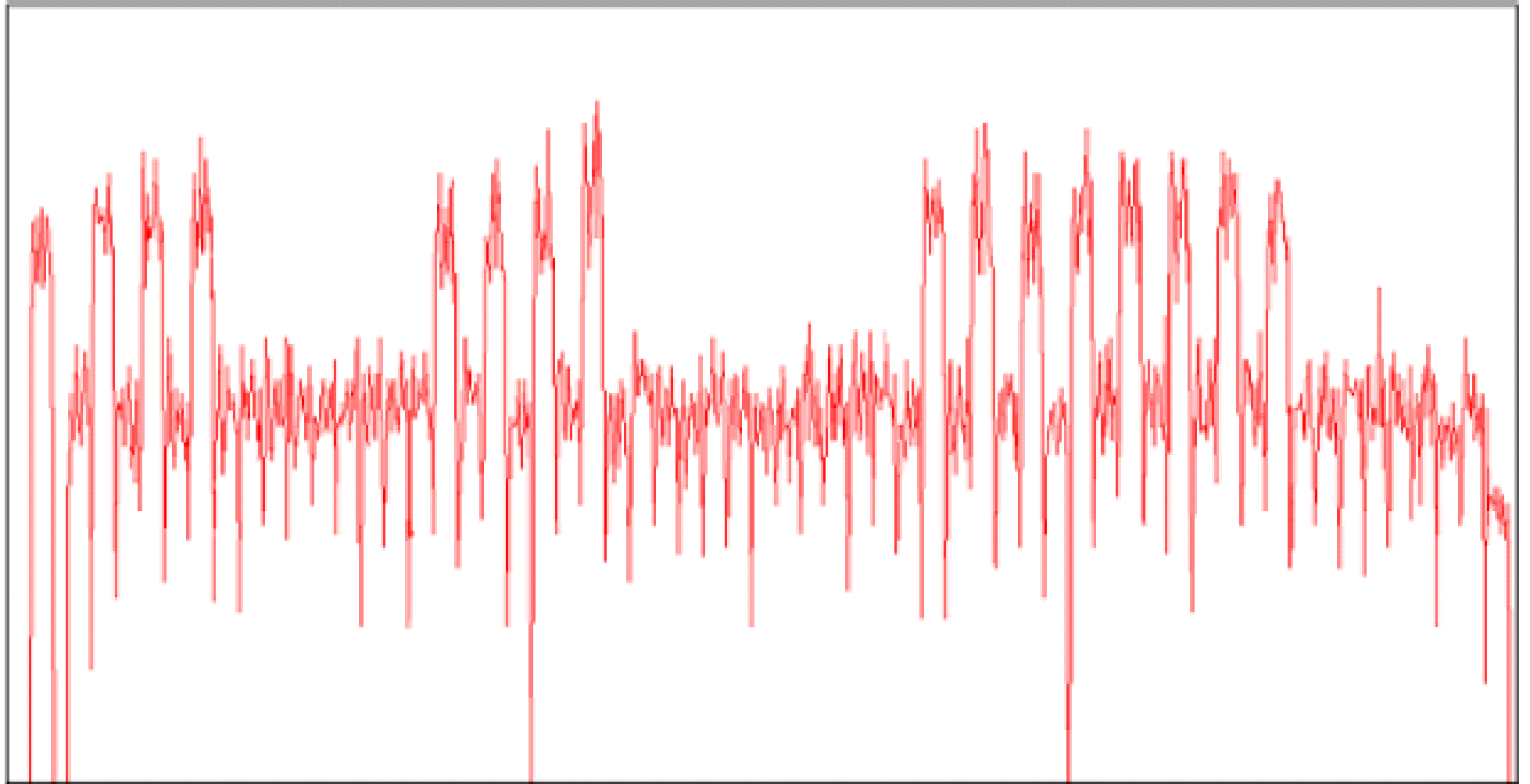
**y** est le message à signer,

**n** est public,

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

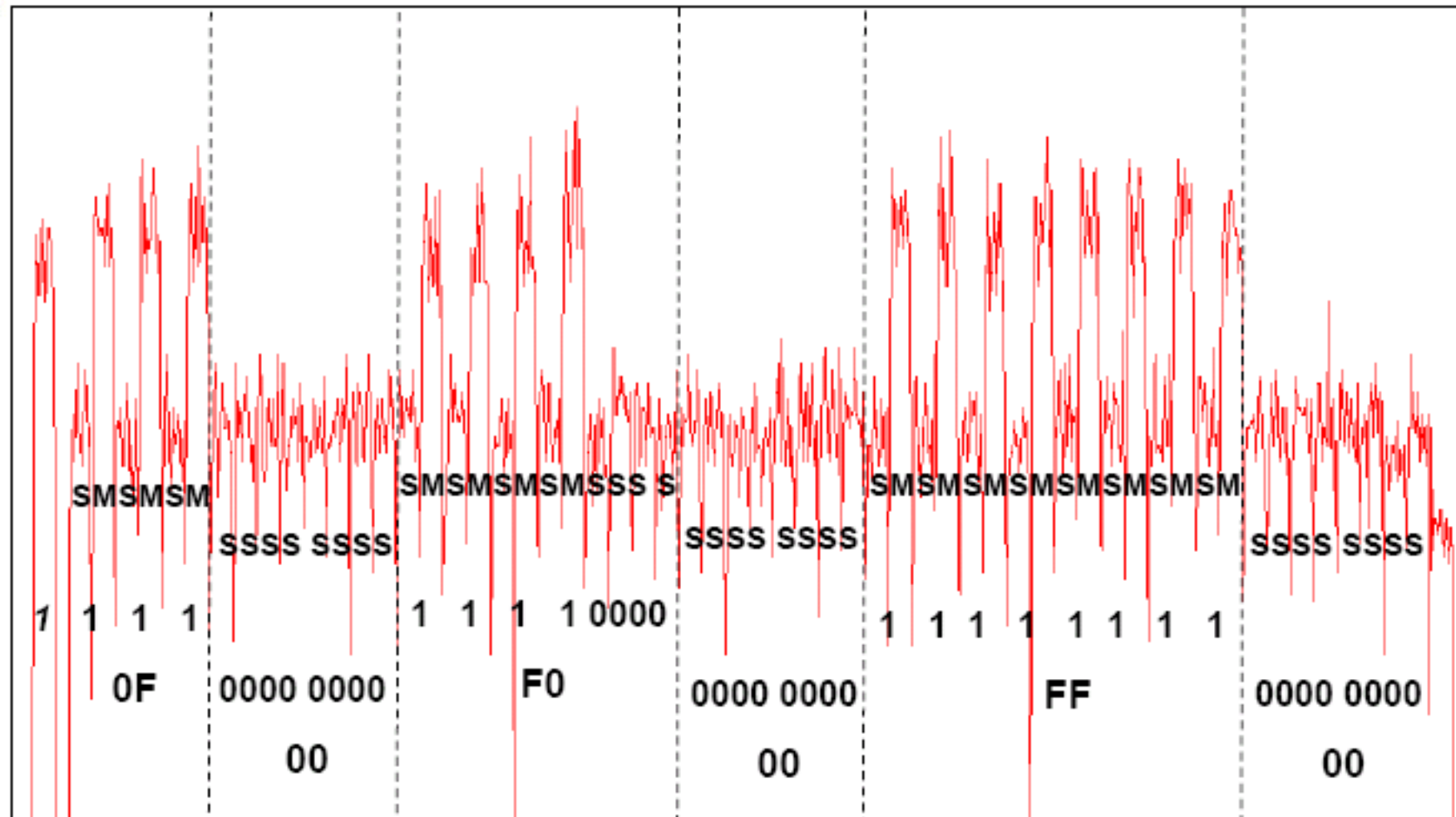


## Exemple « réel »

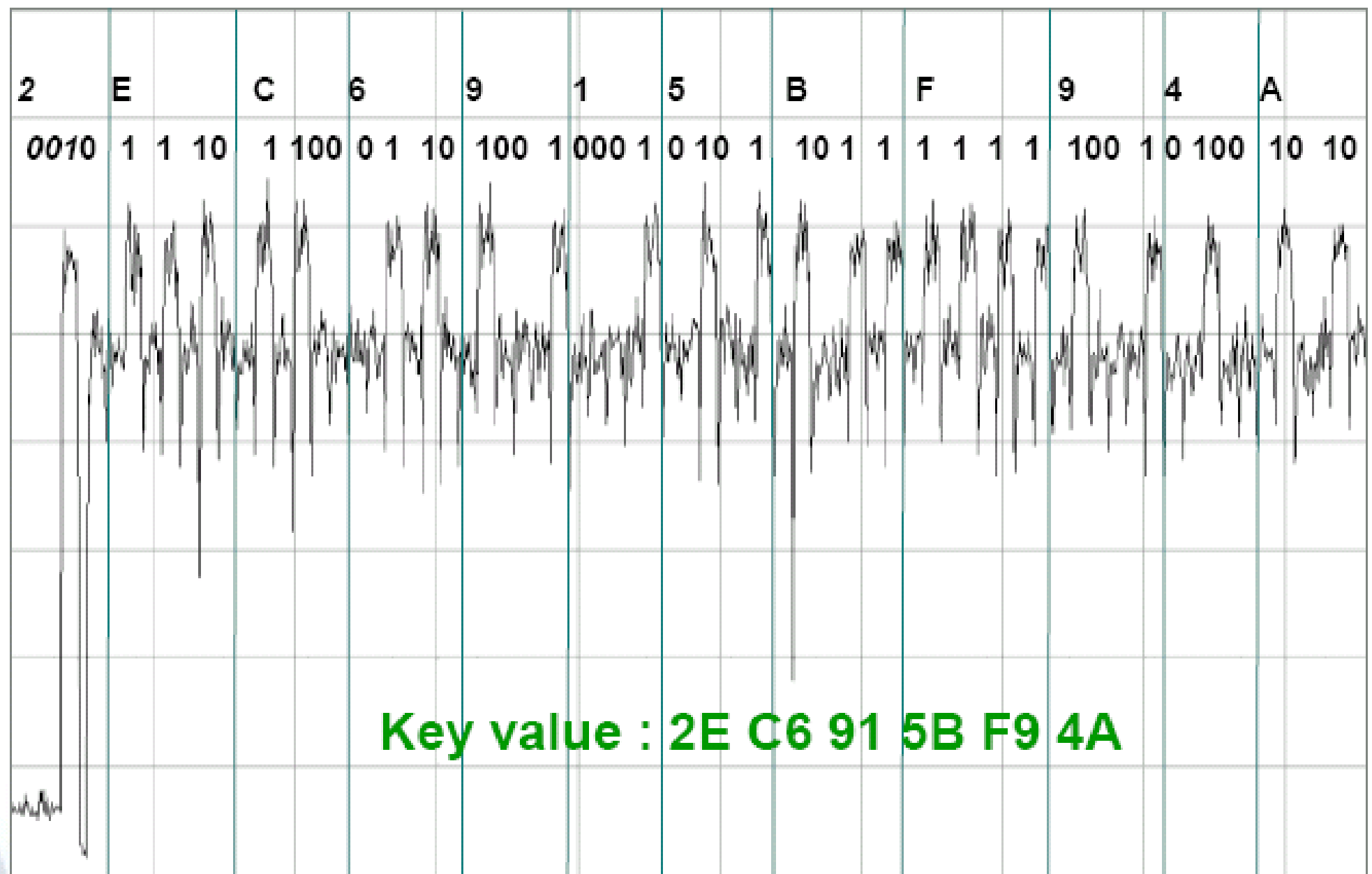


## Exemple « réel »

Test key value : 0F 00 F0 00 FF 00



## Exemple « réel »



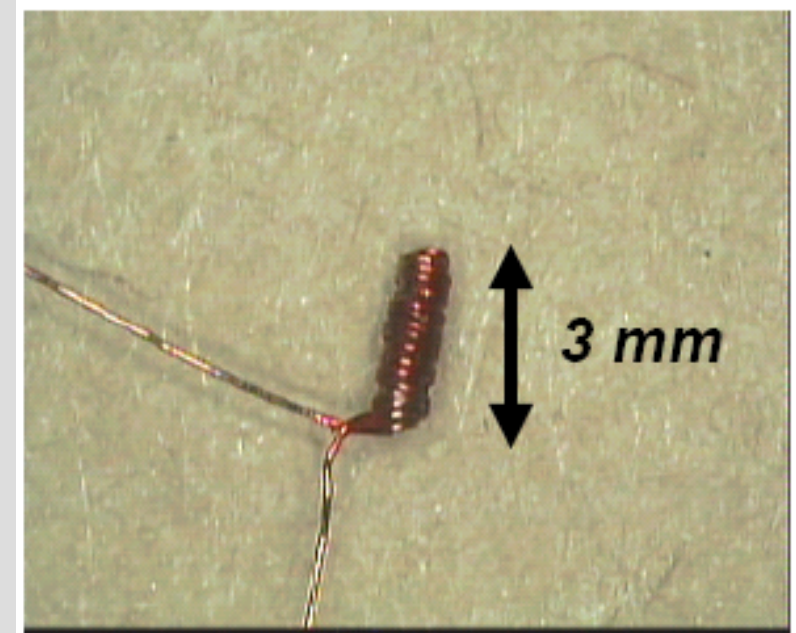
## Les émissions EM

**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.

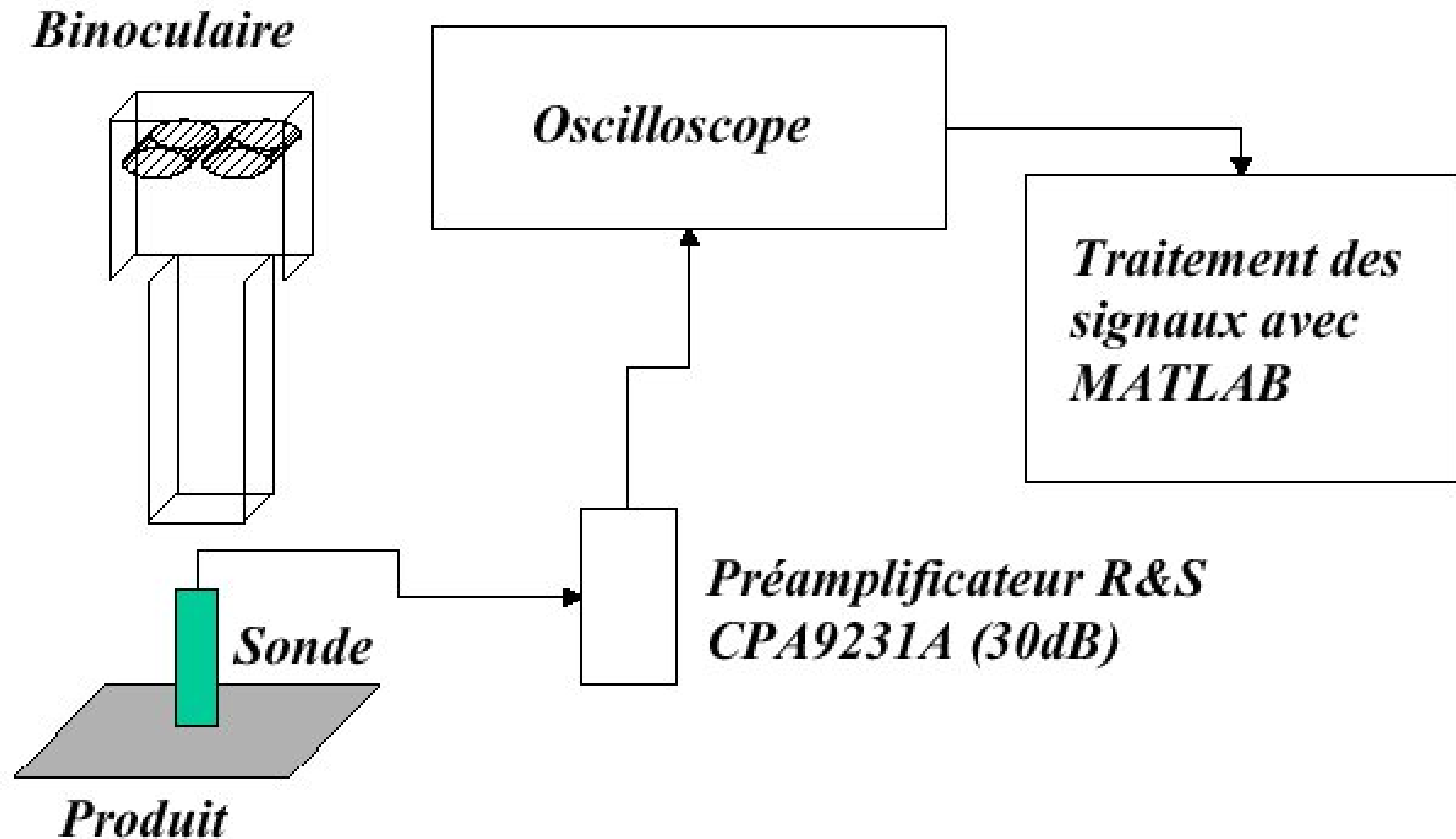
**Différence :** L'information est plus locale. On peut déplacer la micro-sonde électromagnétique au dessus de la zone qui nous donnera le plus d'informations (exemple : co-processeur cryptographique).

**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.

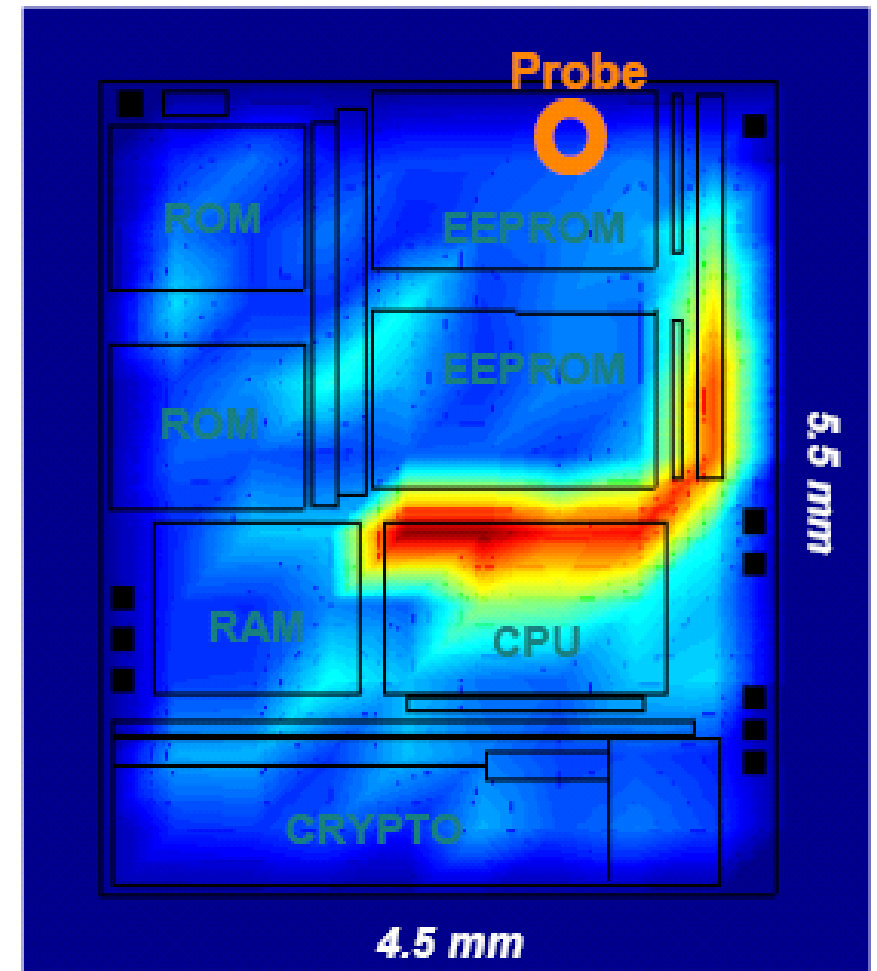
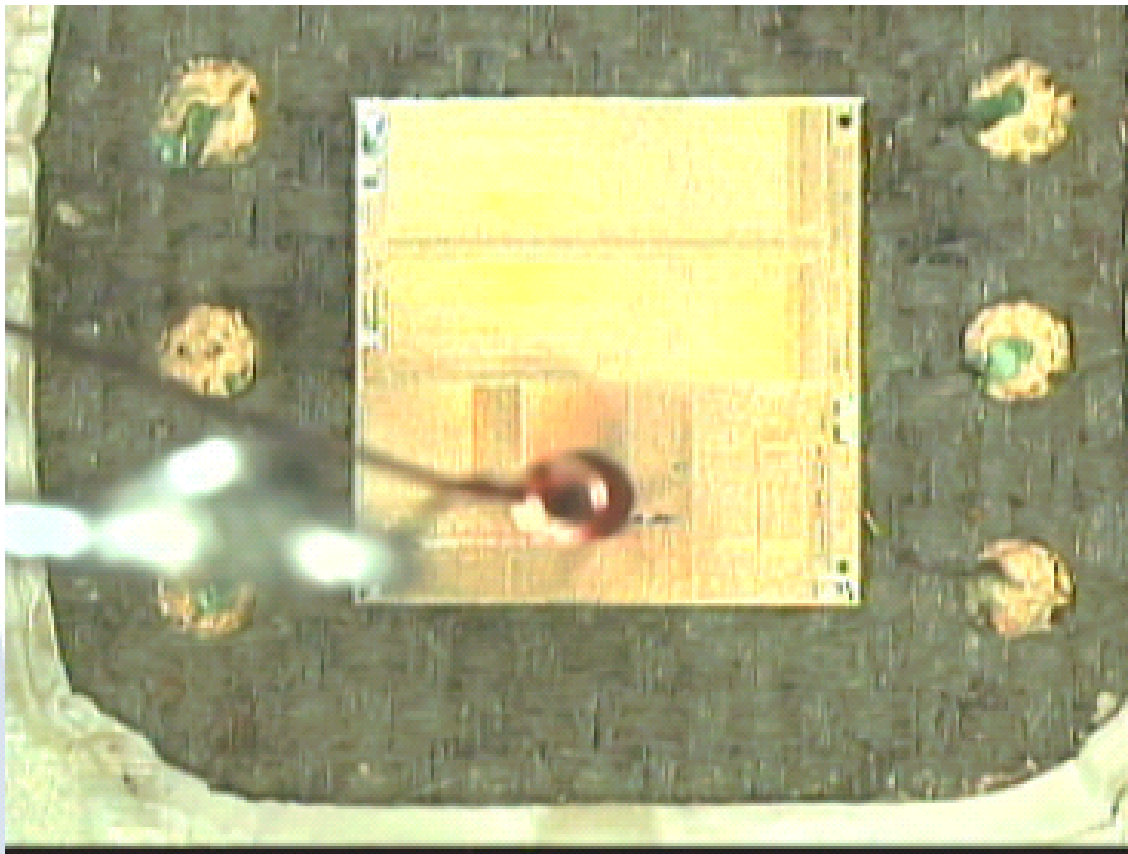


## Le dispositif de cartographie EM



## Le dispositif de cartographie EM

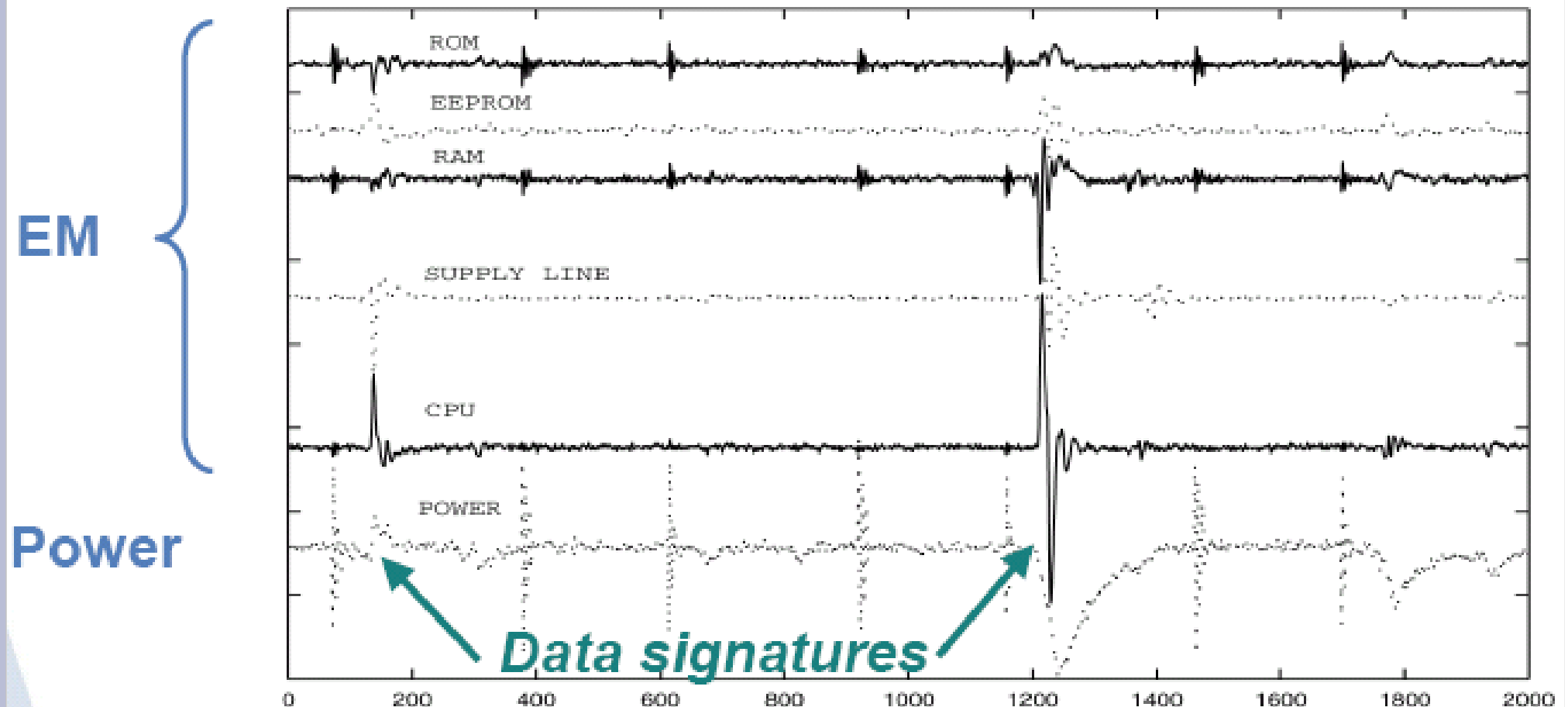
- Horizontal cartography (XY plane)
  - to pinpoint instruction related areas
  - better if automated



## Différence EM/Power

- EM signals versus XY probe position

Differential traces between (00h  $\oplus$  00h) and (FFh  $\oplus$  00h) picked up at different locations



## Attaques EM

**la SEMA (Simple EM Analysis)**

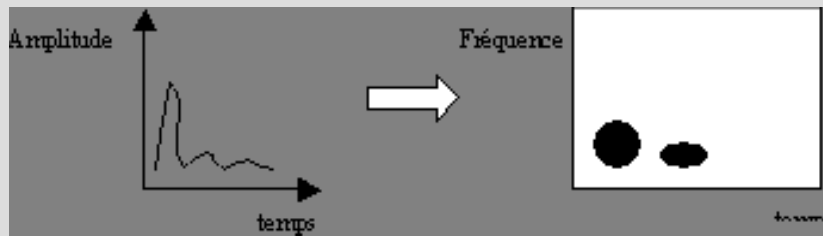
**la DEMA (Differential EM Analysis)**

**=> 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.

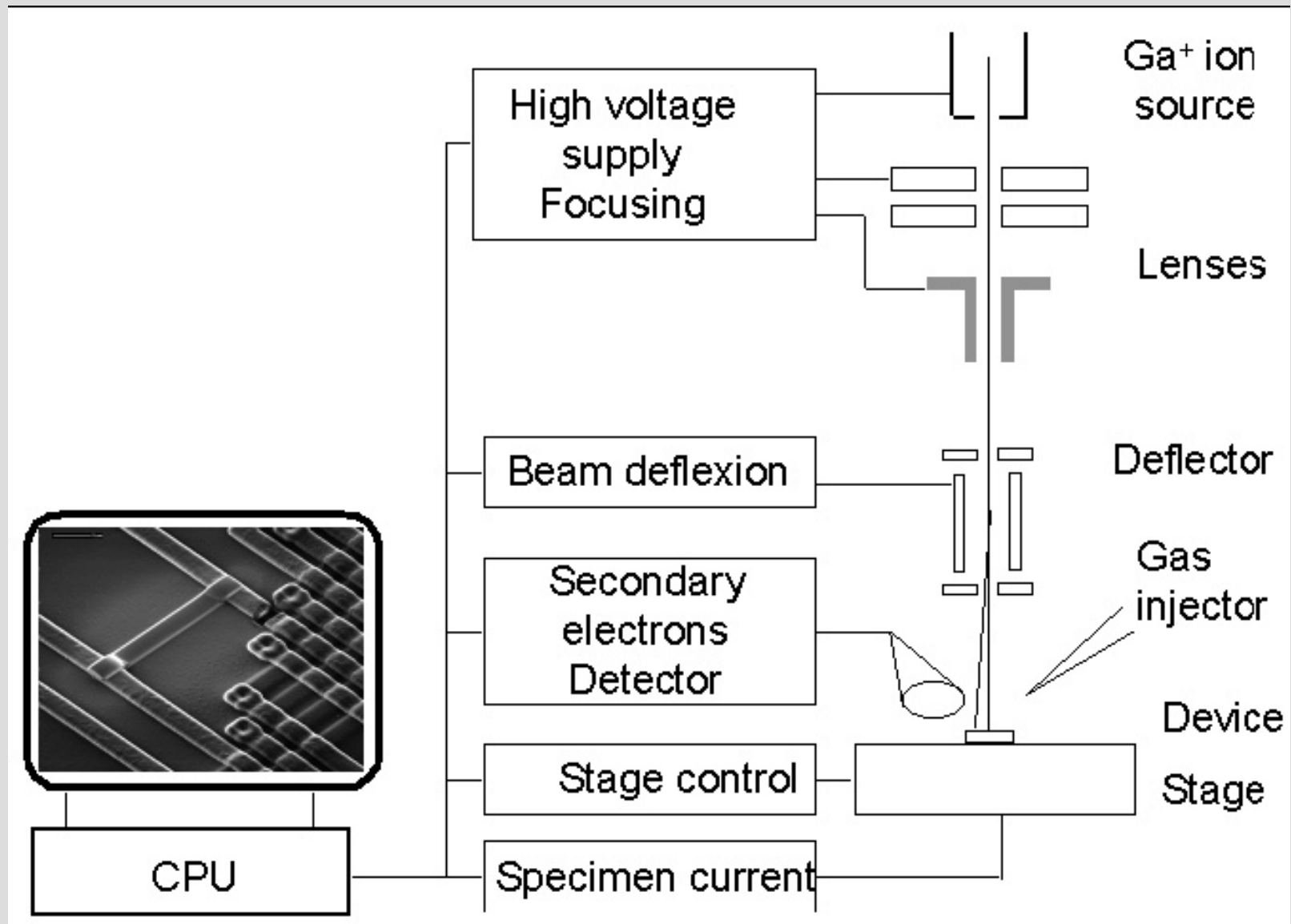
## **Invasives**

**micro-probing**

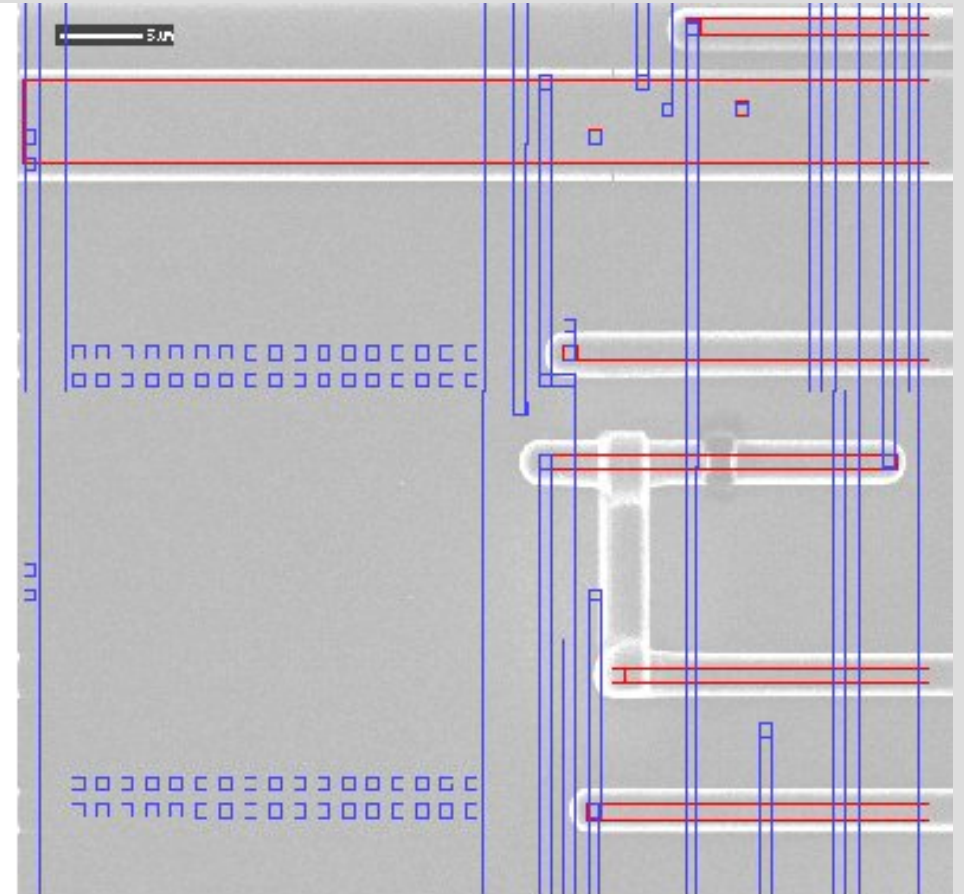
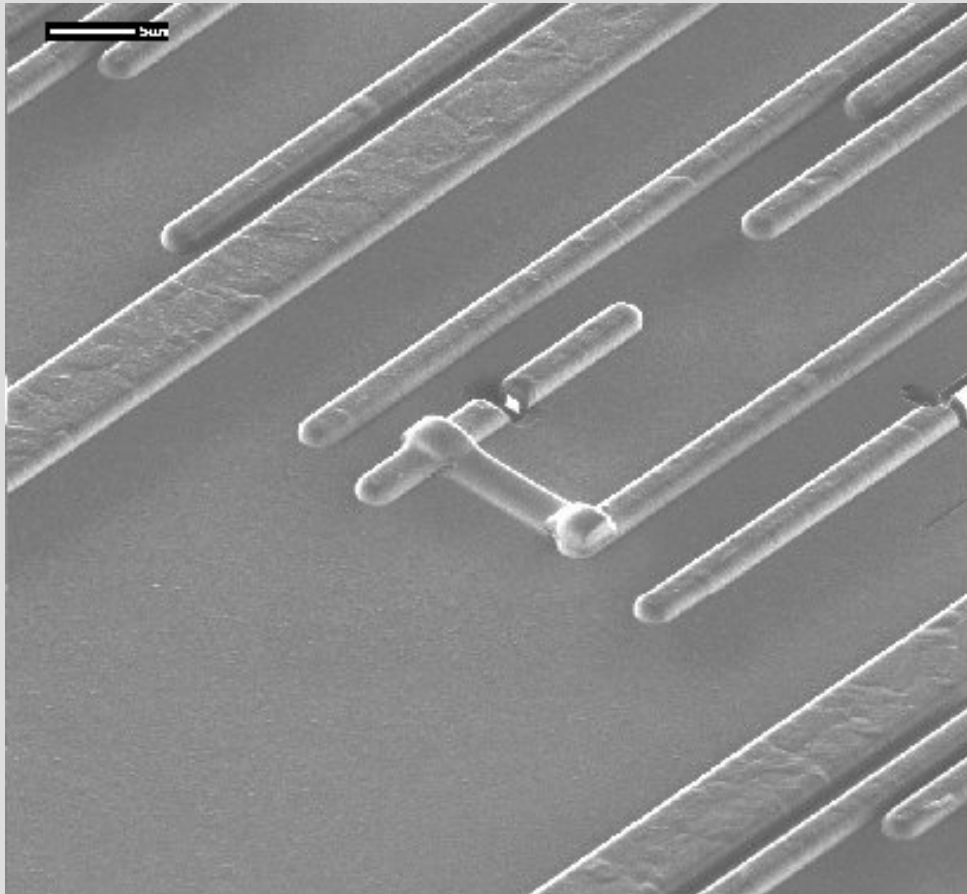
**modification de circuit (FIB)**

**réetro-conception du circuit**

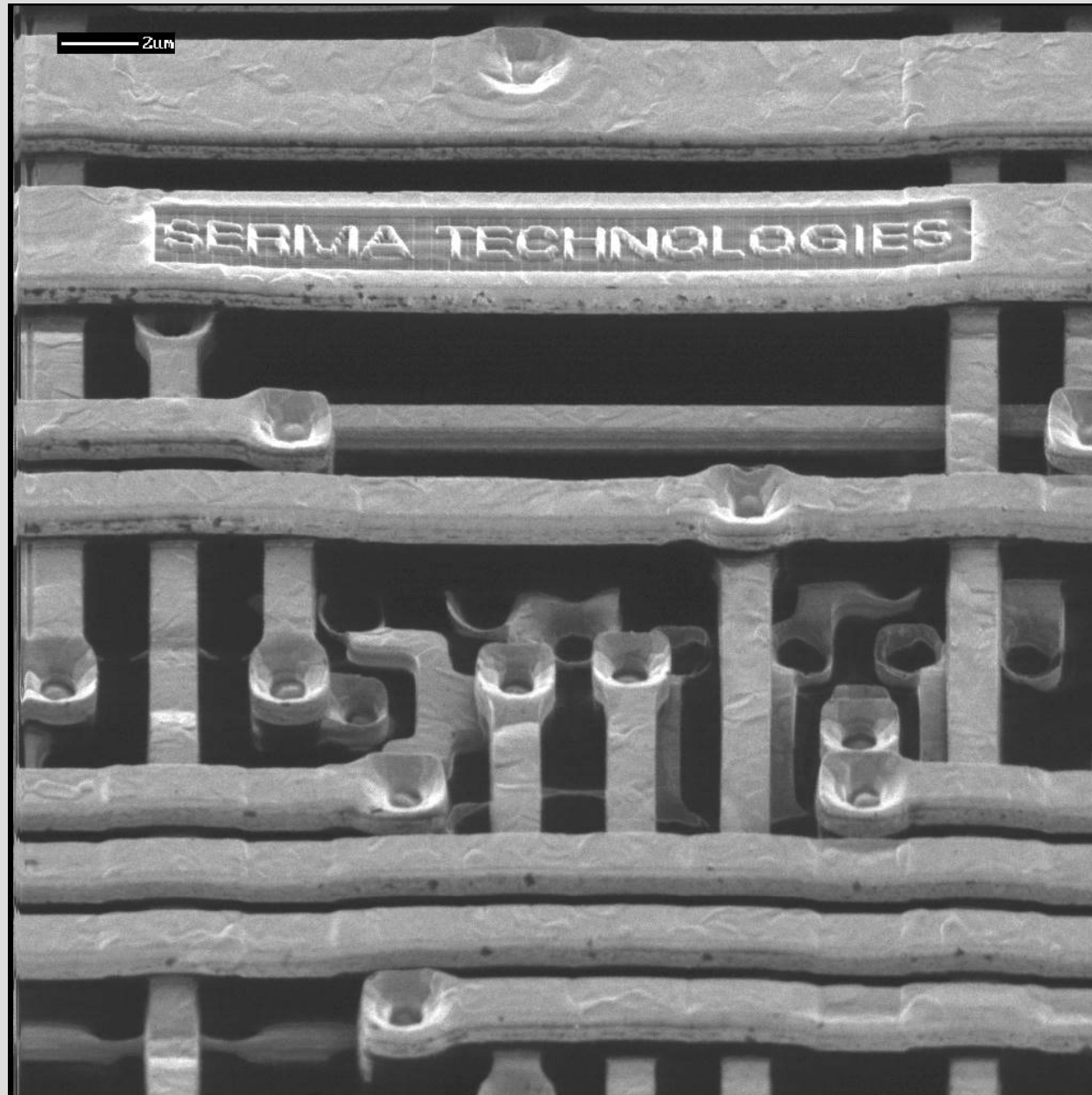
## Le FIB (Focused Ion Beam)



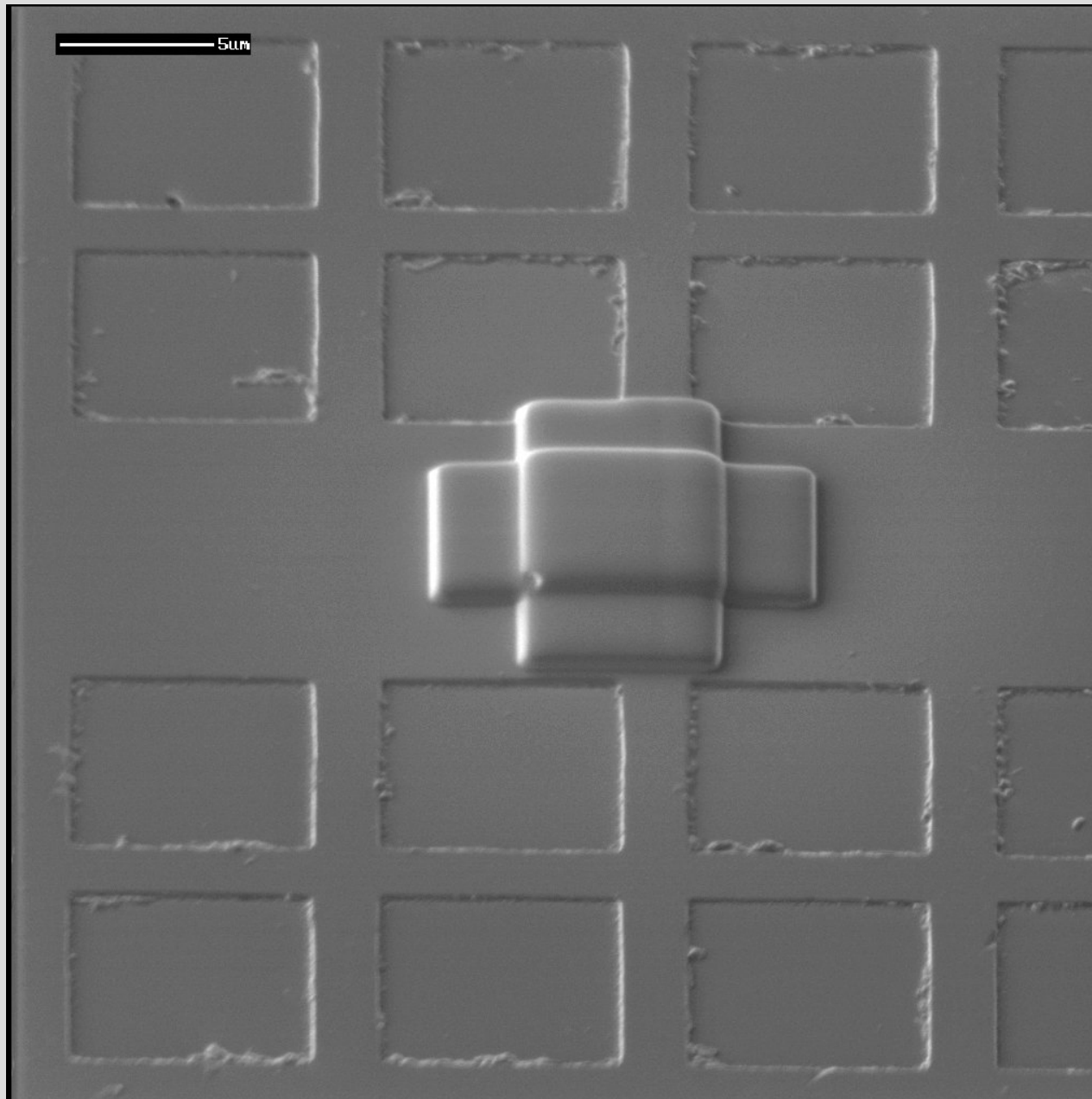
## Modifications de circuits (1/2)



## Modifications de circuits (2/2)

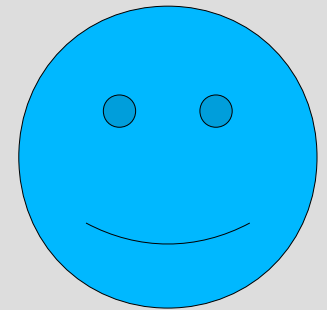


## Micro-probing



# Très cher !

- If you have more money or if you are a student.



# Le futur de la carte à puce

# ***The Winning Platform...***

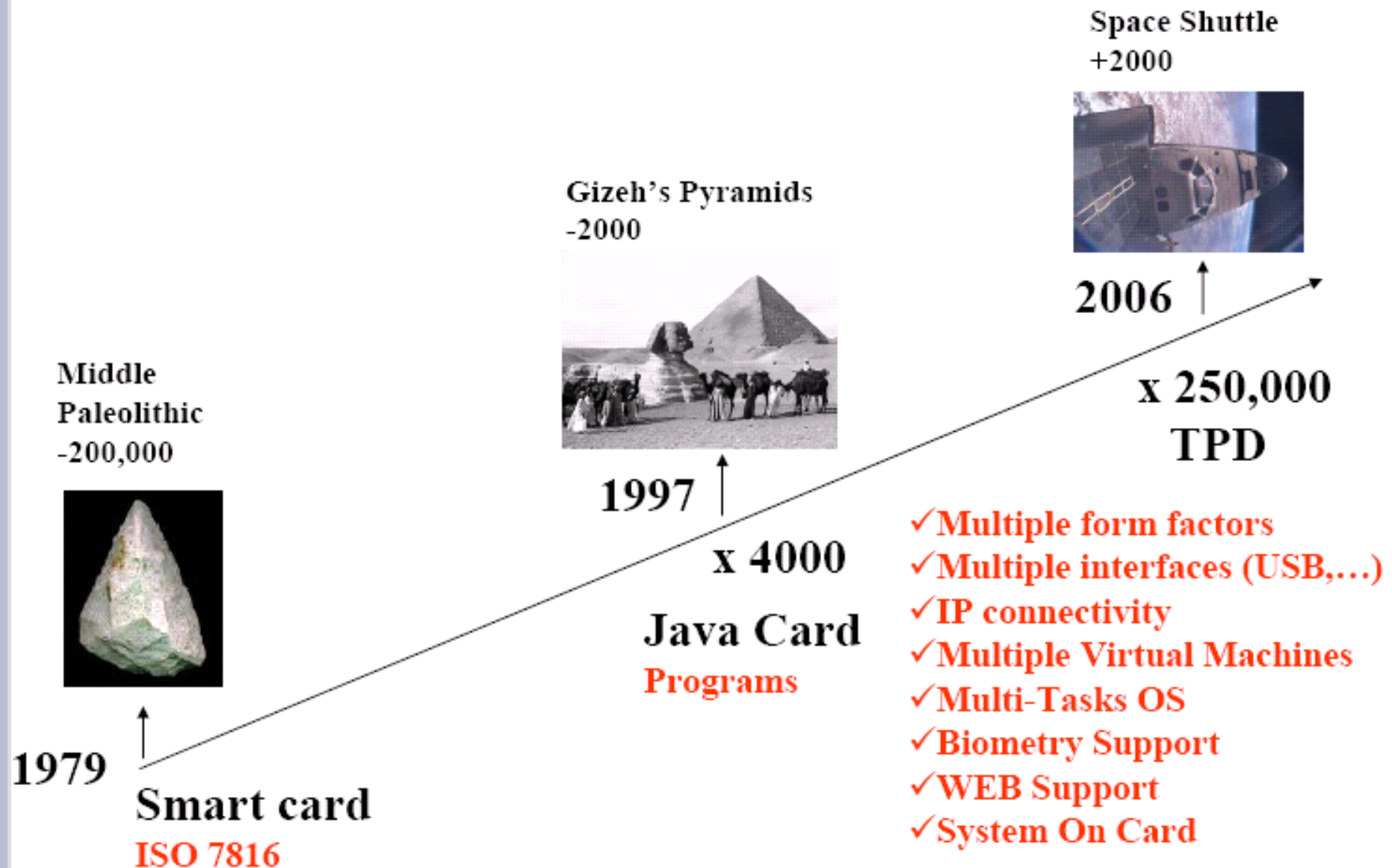


# L'évolution fonctionnelle

*D'après Bertrand du Castel*

- 1997 JavaCard
- 1998 JavaCard+GSM SIM
- 1999 JavaCard+RSA
- 2000 WAP MicroBrowser
- 2001 Biometric (FingerPrint)
- 2002 RMI
- 2003 .NET Card
- 2004 TCP/IP Full Duplex
- 2005 Linux
- 2006 Multi-Channel (STIP)
- 2007 Streaming (full TV satellite)
- 2008 Spontaneous networking (JINI)
- 2009 GRID

# Moore's Law

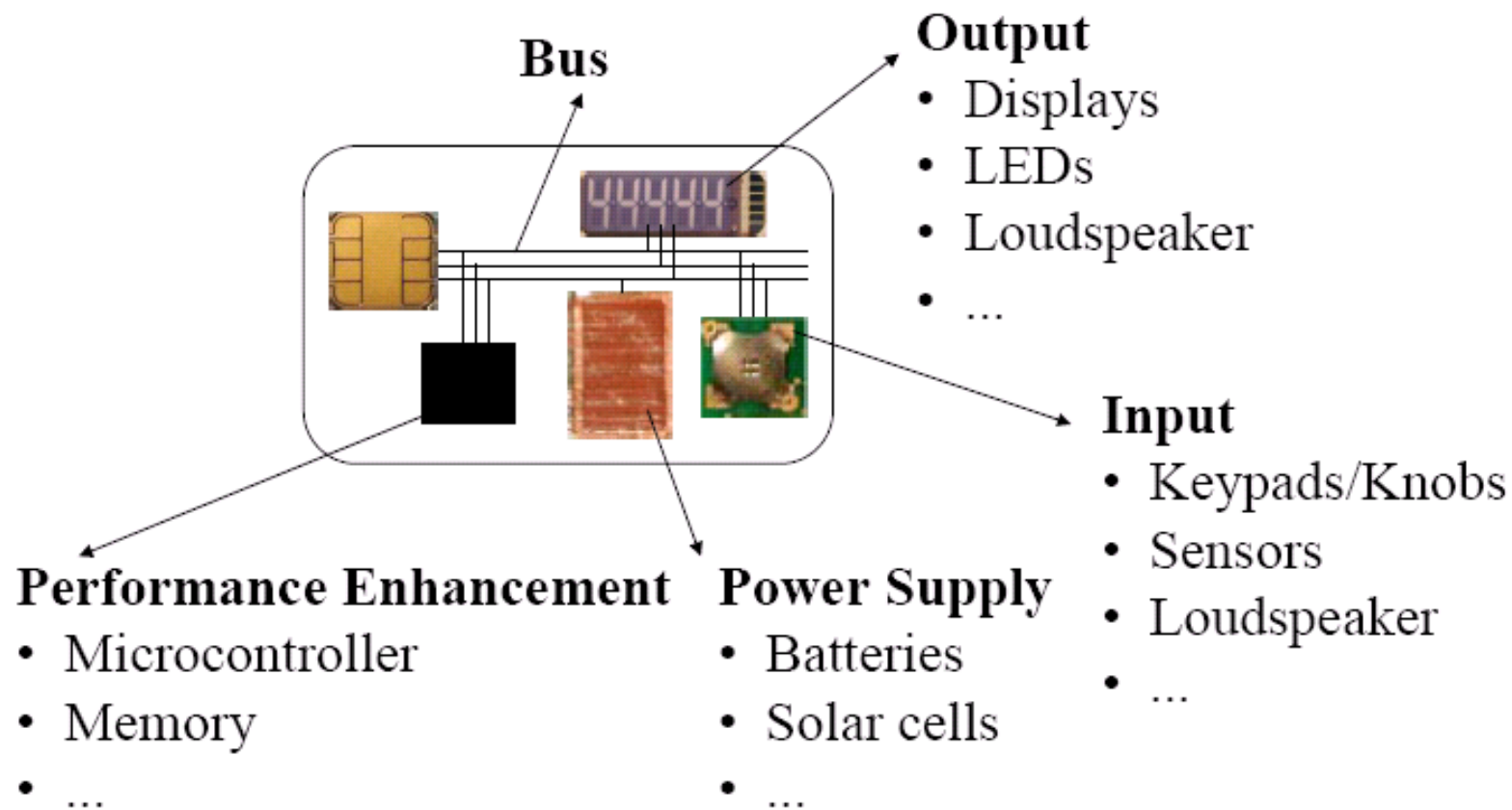


## L'évolution matérielle

*D'après Bertrand du Castel*

- 2004 100Mhz E2+ & FullDuplex 1MB RSA2048 en 50ms
- 2006 200Mhz Bluetooth/UWB 4MB RSA2048 en 10ms
- 2008 400Mhz Bluetooth/UWB 16MB
- 2010 800Mhz Dynamic Display 50MB
  - Microphone
  - Battery (2003 : CEA Grenoble 500µm d'épaisseur)
  - FingerPrint Sensor
  - Pad
  - Rock-n-roll interface (scrolling avec la gravité)

# About System on Card (SoC)



# L'évolution matérielle : Exemple : Java-Powered iButton



- <http://www.ibutton.com>
- Packaging : capsule étanche en métal
  - Peut-être monté sur bague (cf « La nuit des temps » de René Barjavel)
- Communication : 1-Wire
  - Un fil pour les échanges et l'alimentation
  - Débit : 16,6 Kbit/s et 144 Kbit/s
- Horloge temps réel (Secure timestamping)
- Mémoire
  - 64Ko de ROM (OS+JVM)
  - 6Ko à 135Ko de NV-RAM à 100 ns (Non Volatile RAM : 10 ans)
- API JavaCard 2.0
  - Entiers 32 bits
  - javacardx.crypto : Crypto SHA-1, RSA DES, 3DES
- Coté terminal
  - OCF, OneWireContainer
  - PKCS#11, MS CSP, X509, Win2000 log on

### L'évolution matérielle : Exemple: Cyberflex eGate

- Axalto (ex Schlumberger)
- Brevet WO0016255
- Capacité
  - 32 de FlashRAM
- Format
  - ISO7816-1, GSM11.11
- Interface
  - USB/OTG (de 1.5 Mbits/s à 12 Mbits)
  - TCP/IP+USB pour la couche physique (bulk mode)
  - Full duplex
- Crypto :
  - RSA, DES, AES (très haut débit)
- Programmation
  - JavaCard
  - Mini-Serveur HTTP et SOAP



### L'évolution matérielle : Exemple

- Un afficheur, un clavier
  - protection contre les terminaux trafiqués
- Une horloge
  - éviter les attaques temporelles
- Une batterie
  - la mémoire volatile est plus dure à observer !
  - Le processeur peut être réveiller pour rappeler des événements au porteur



source Alien Technology <http://www.alientechnology.com/>

# Java Card Grid Project

# Présentation des grilles de calculs

**Grille** : ensemble de machines interconnectées.

**Principe** :

Partager de GROS calculs entre plusieurs machines.

**Utilisateurs** :

Organismes de la défense, CEA, laboratoires de recherche et universités, ...

**Domaine d'utilisation** :

Cryptographie, physique des particules, bio-informatique, observation de la terre, ...

Un des problèmes important : *La sécurité !*

# Quelques projets utilisant la grille

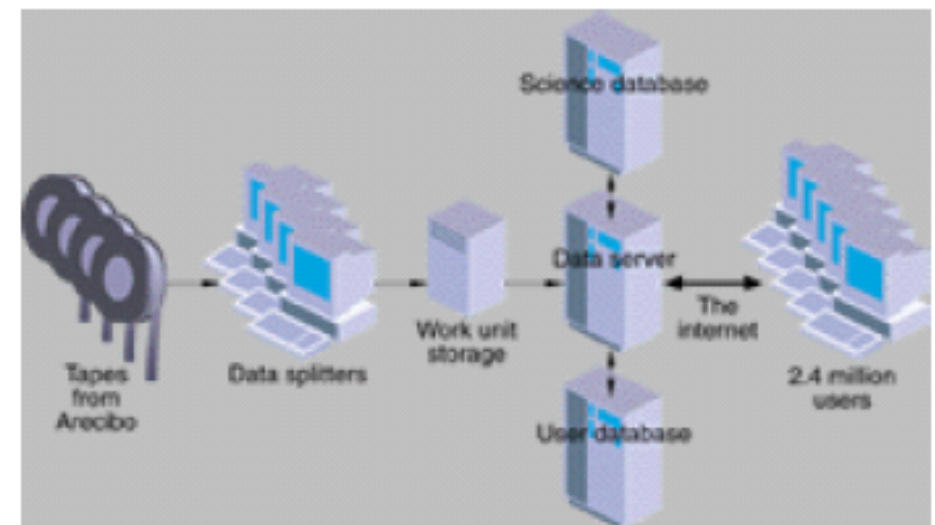
---



Décrypton

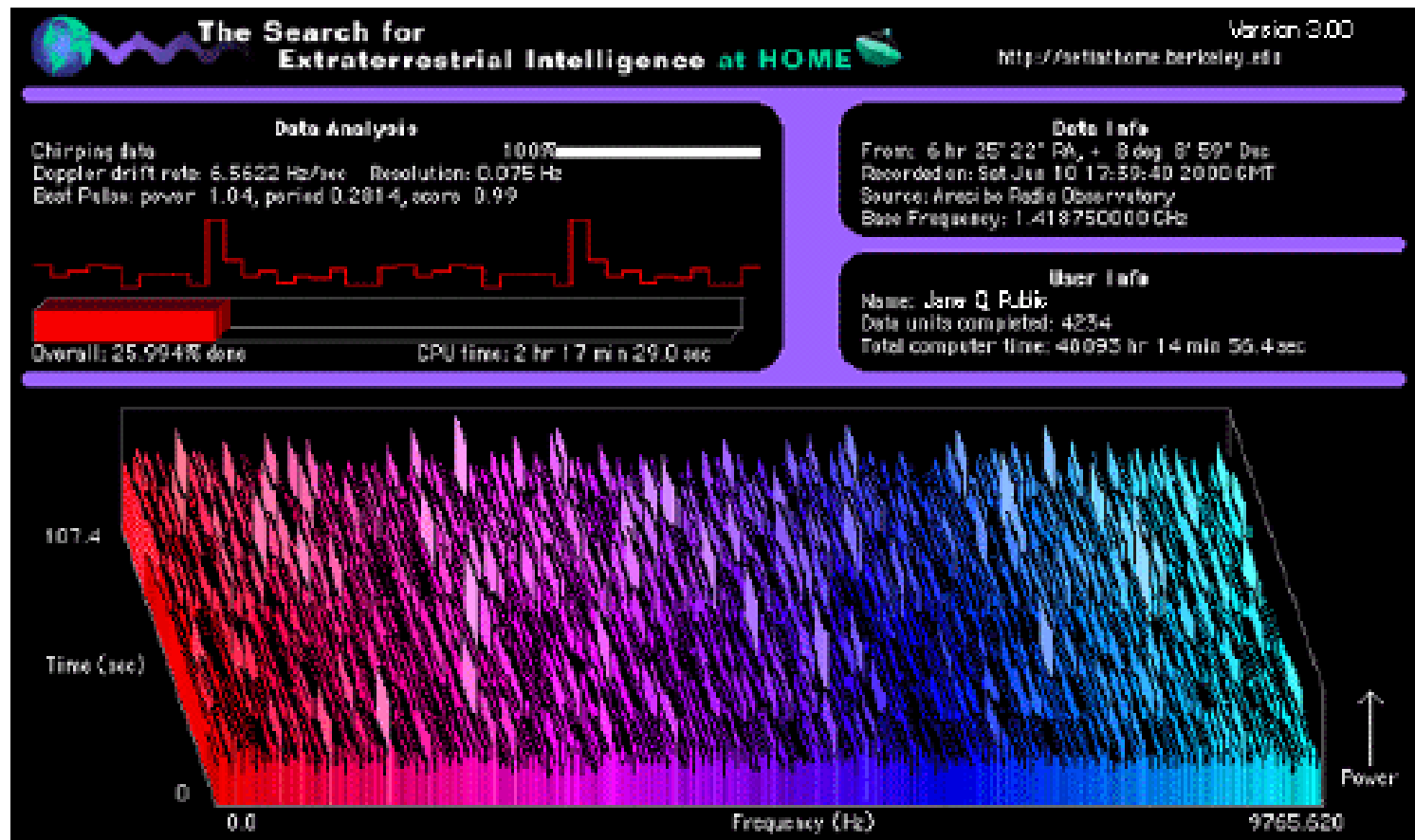
# Seti@home

*But* : Recherche de signaux extra-terrestres.

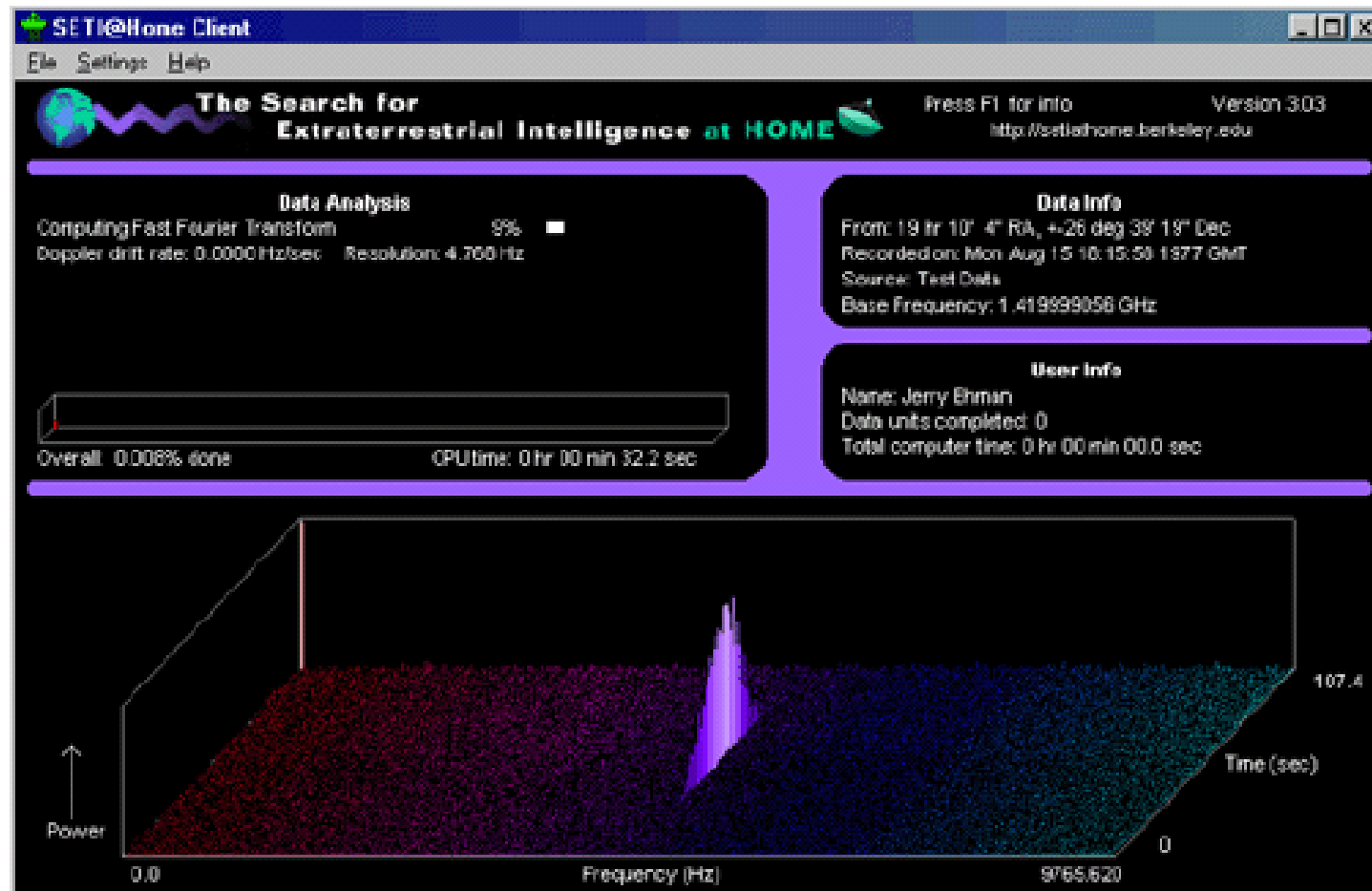


# Les calculs

L'utilisateur télécharge un screensaver puis les données.



# Les résultats



Nous ne  
sommes PAS  
SEULS dans  
l'univers ?

SI!  $\Rightarrow$  Il s'agit de résultats truqués! :-)

# Les problèmes

## Côté Seti@home :

- ☞ Les résultats positifs ou négatifs ne sont pas sûr.  
⇒ *solution* : Faire calculer les mêmes données plusieurs fois par différents utilisateurs

## Côté utilisateur final :

- ☞ Code source non disponible.  
⇒ éviter les faux résultats.
- ☞ Que fait le code sur la machine de l'utilisateur ?

# Le projet “Java Cards Grid”

## Objectifs :

- ☞ Garantir la sécurité du code et des calculs sur la grille.
- ☞ Proposer un framework logiciel exploitant du matériel sécurisé pour assurer la confiance des utilisateurs.

## Avantages pour :

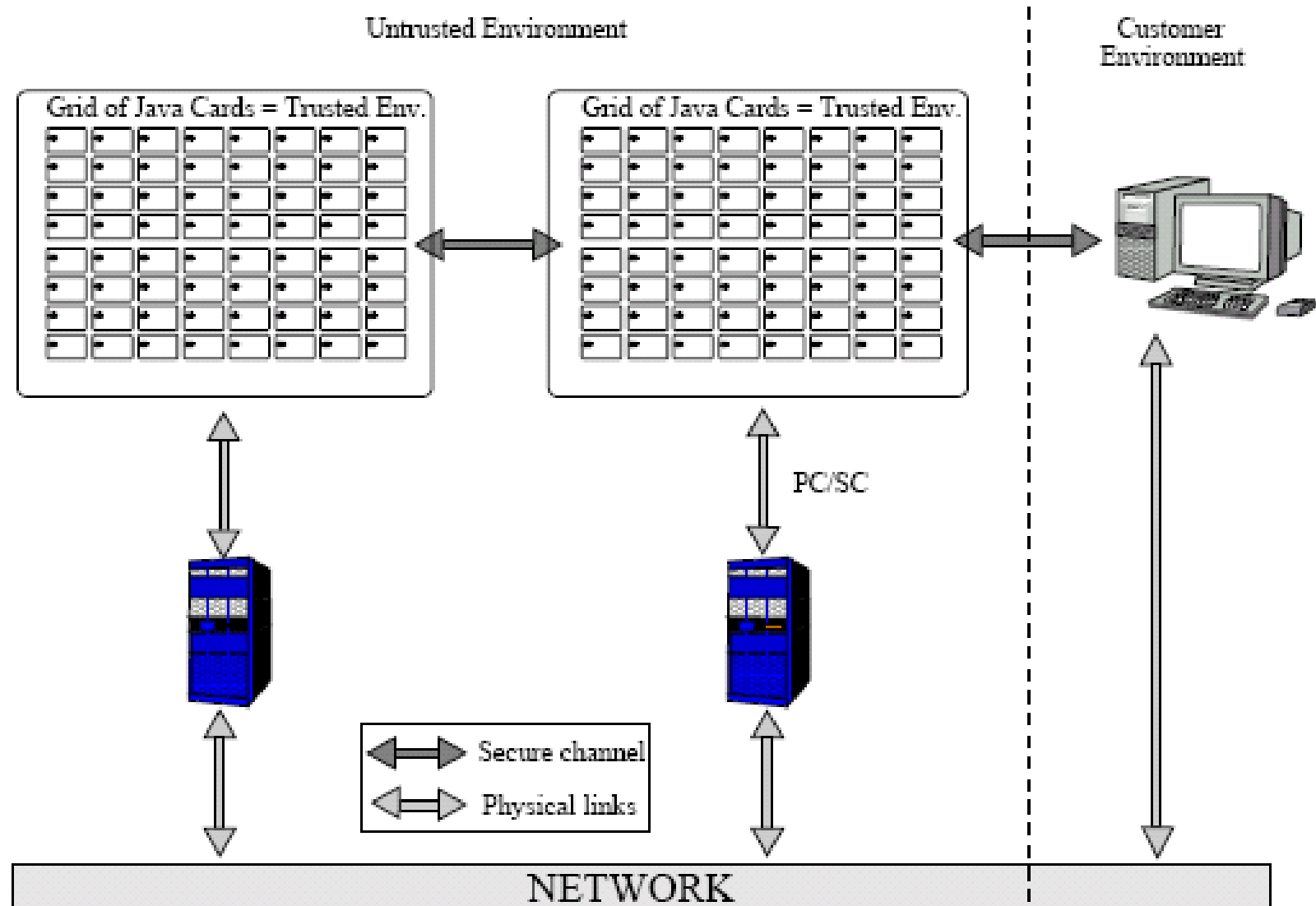
- les utilisateurs du *distributed computing* : une plus grande confiance dans le fournisseur des ressources de calculs ;
- les fournisseurs des ressources de calculs : accroître son marché avec des nouveaux clients comme le CEA, ...

# Buts de notre projet

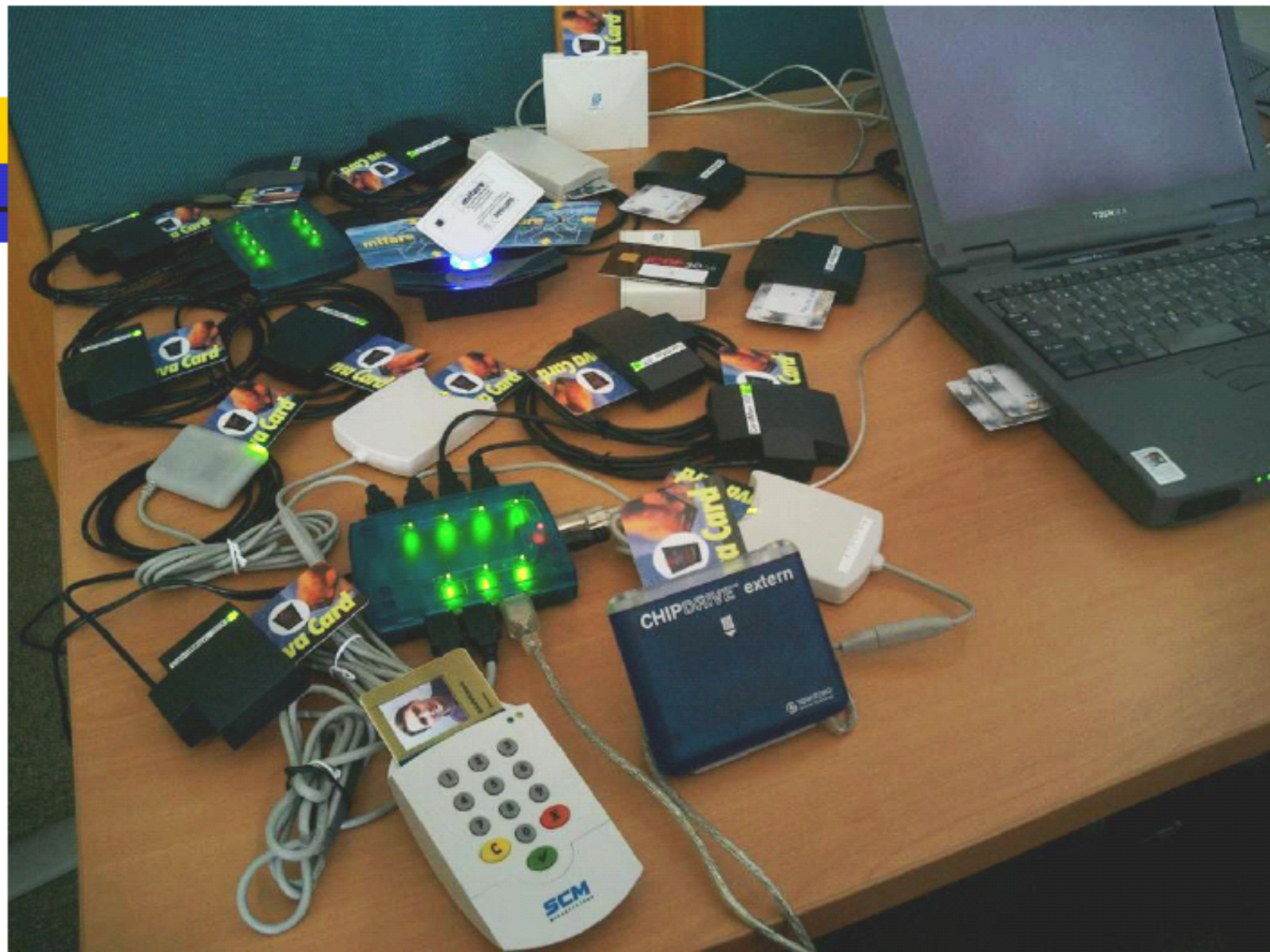
---

- Premier but : Fournir un environnement sécurisé pour partager des ressources (matérielles, logicielles) et de la puissance de calcul
- Second but : Fournir une plate-forme pour expérimenter sur les réseaux ad hoc

# Notre proposition



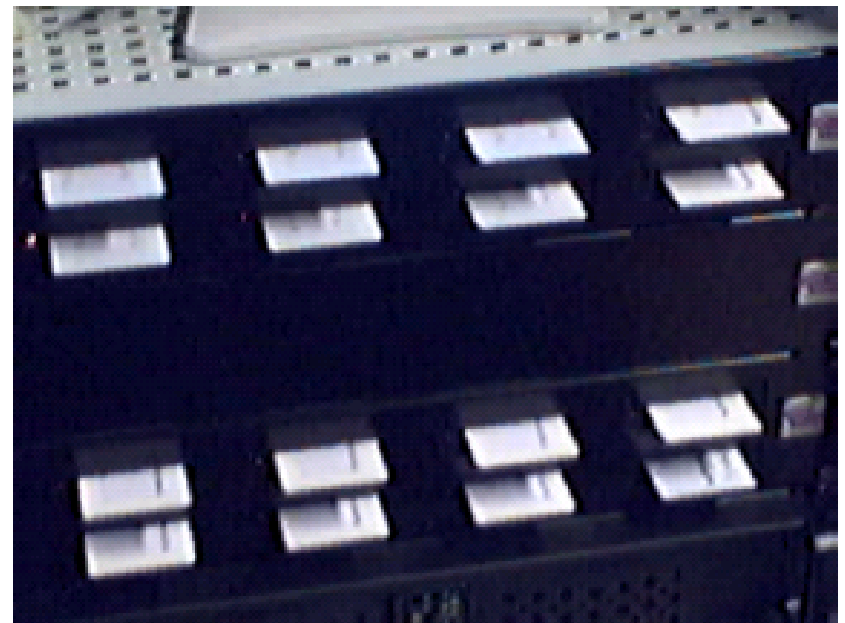
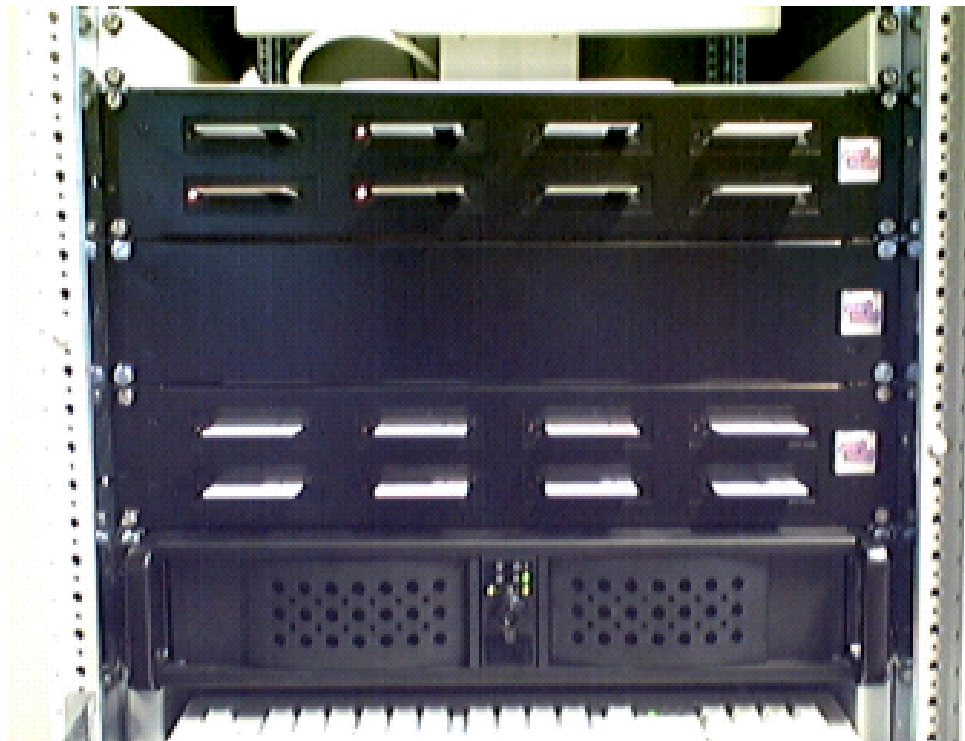
## Mon bureau il y a en 2003/2004



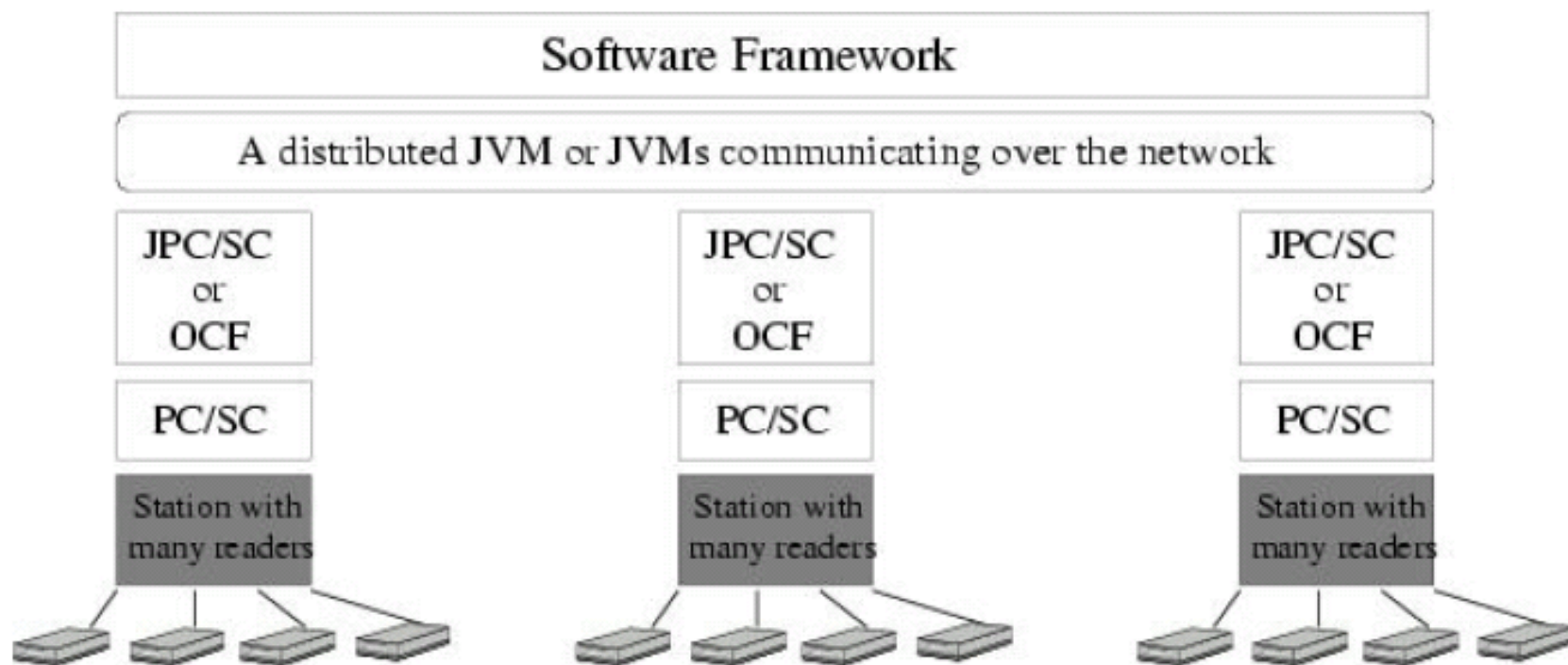
# La Plate-forme Actuelle



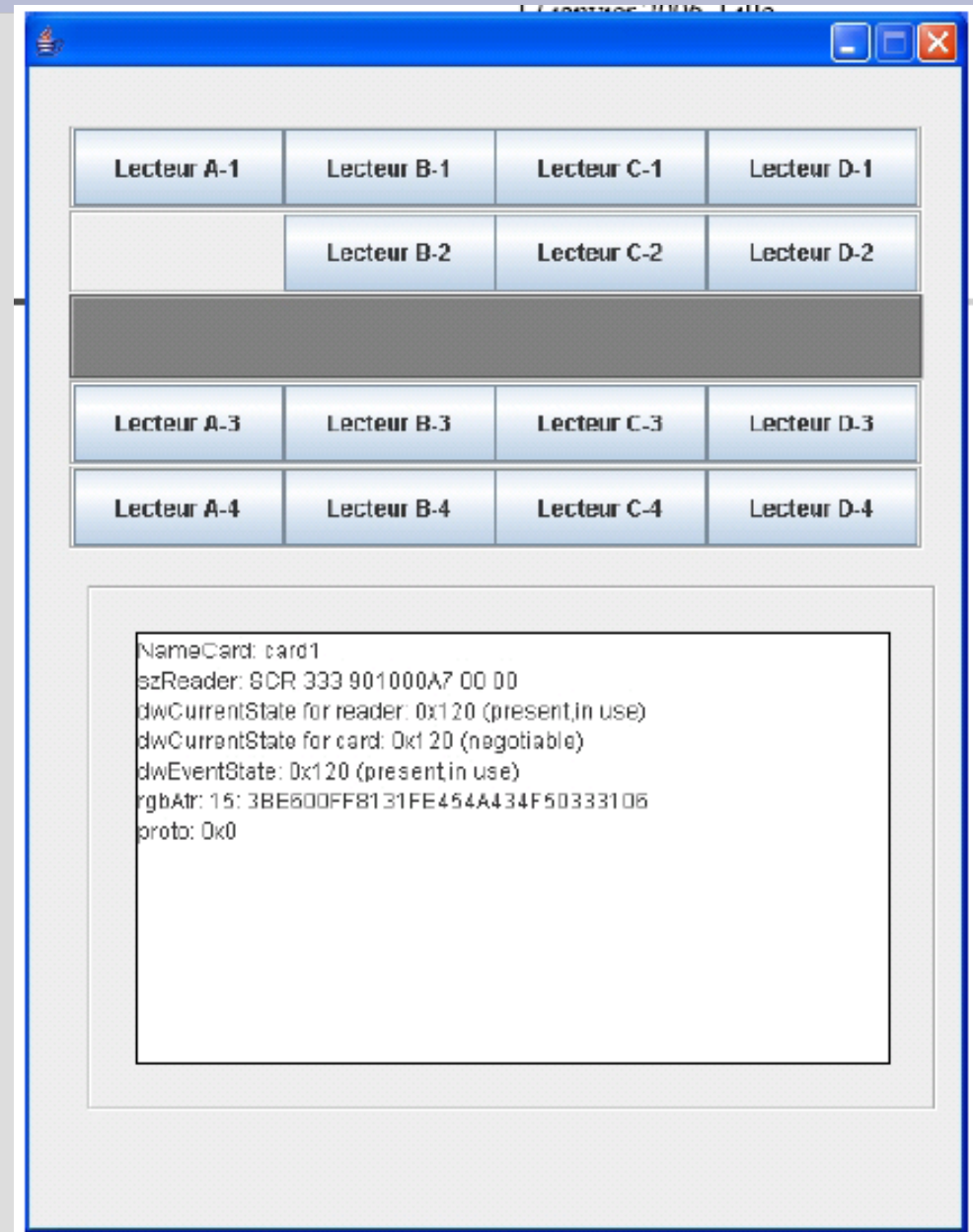
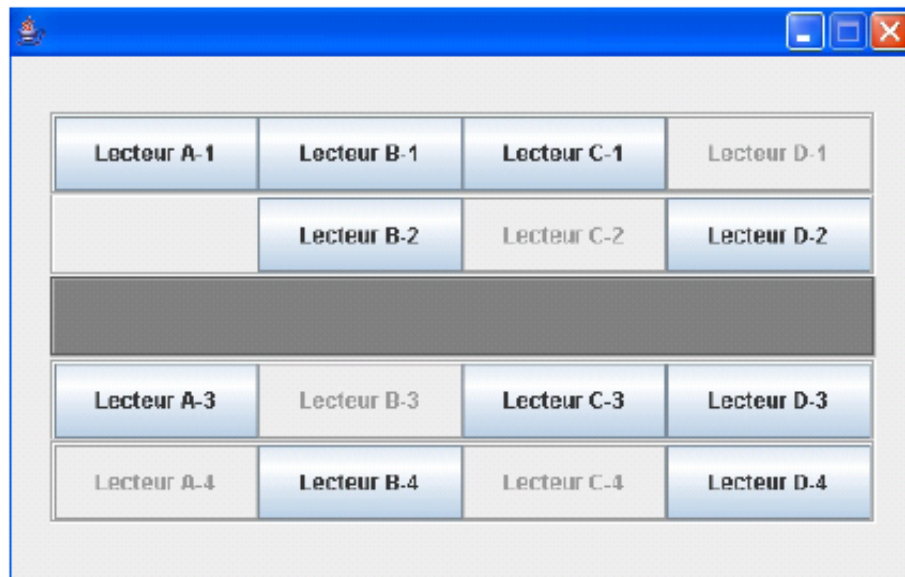
- 2 fois
  - 1 PC
  - 16 lecteurs de cartes
  - 1 point d'accès Wi-Fi
- Les deux machines sont connectées entre elles (réseau filaire)



# L'environnement logiciel



## L'environnement d'administration



# Première démonstration

The screenshot displays the JFractal Java applet interface, which is divided into several sections:

- Java Applet Window:** Displays a fractal image on a dark blue background.
- JFractal Controls:** Contains various controls and monitoring information.
  - Buttons:** Start, Stop, Reset.
  - Parameters:**
    - Iterations: 20
    - Precision: 5
    - Subdivisions: 100
    - Steps: ≤ 6
    - Points: ≤ 5460
    - Points/Size: ≤ 14 @0
    - Area ratio: 0 25 50 75 100 (with a slider)
  - Monitoring:**
    - Progress:** Progress bar at 100%.
    - Elapsed time:** 04:10:53.932
    - Remaining time:** 00:00:00.000
    - Estimated time:** 04:10:53.932
    - Time stats:**
      - Computed time min: INFINITY
      - Computed time max: -INFINITY
      - Computed time average: 00:00:02.723
      - Computed time total: 1 day.
    - Iterations stats:**
      - Min: 1
      - Max: 20
      - Average: 4
      - Total: 173547
    - Engine:**
      - FCS size: 9 (with a Manage... button)
      - Schedulers: qfractalSmartScheduler (dropdown menu)
      - ☐ details
  - Log:** A text area showing the execution log, including messages like "Starting...", "733 bytes have been freed invoking System.gc()", and "Starting the computation of FractalData[geometry: 200x200+0-0]".
  - Footer:** Checkboxes for ☒ Verbose mode, ☒ Debug mode, and ☒ Progress mode.

# Quelques benchmarks

|                                           |         |
|-------------------------------------------|---------|
| 9 Java Card onto Fujitsu mb94r215b (FRAM) | 122 min |
| 9 GemXpresso Pro R3 E32PK                 | 202 min |
| 9 JCOP31bio                               | 253 min |
| 9 GemXpresso Pro R3 64PK                  | 376 min |
| 9 SmartC@fé Expert                        | 389 min |

TAB. 1 – Benchmarks sans secure channel

*Scalabilité* en cours d'expérimentation.

1 Java Card onto Fujitsu mb94r215b (FRAM)  $\implies 18heures = 9 * 120min$

# Application CBP/Air France

- On imagine (☺) que le *US Customs and Border Protection* (CBP) souhaite fouiller les fichiers passagers des compagnies aériennes comme Air France, pour les vols utilisant un aéroport US.
- Problème : la CEE interdit explicitement la diffusion d'informations confidentielles sur les passagers.

# Les Contraintes du Problèmes

- Code de fouille du CBP
  - Distribué sur les cartes
  - Doit demeurer confidentiel
- Fichier passagers d'Air France
  - Distribué sur les cartes
  - Doit demeurer confidentiel

# Etat Actuel et Travaux en Cours

- État actuel
  - La plate-forme est opérationnelle
  - Prix « Best innovative technology » à e-smart 2005
- Travaux en cours
  - Gestionnaire de swap sécurisé
- Autres travaux liés :
  - Aspects liés au ad hoc
    - une thèse en cours avec la DGA

# Perspectives

---

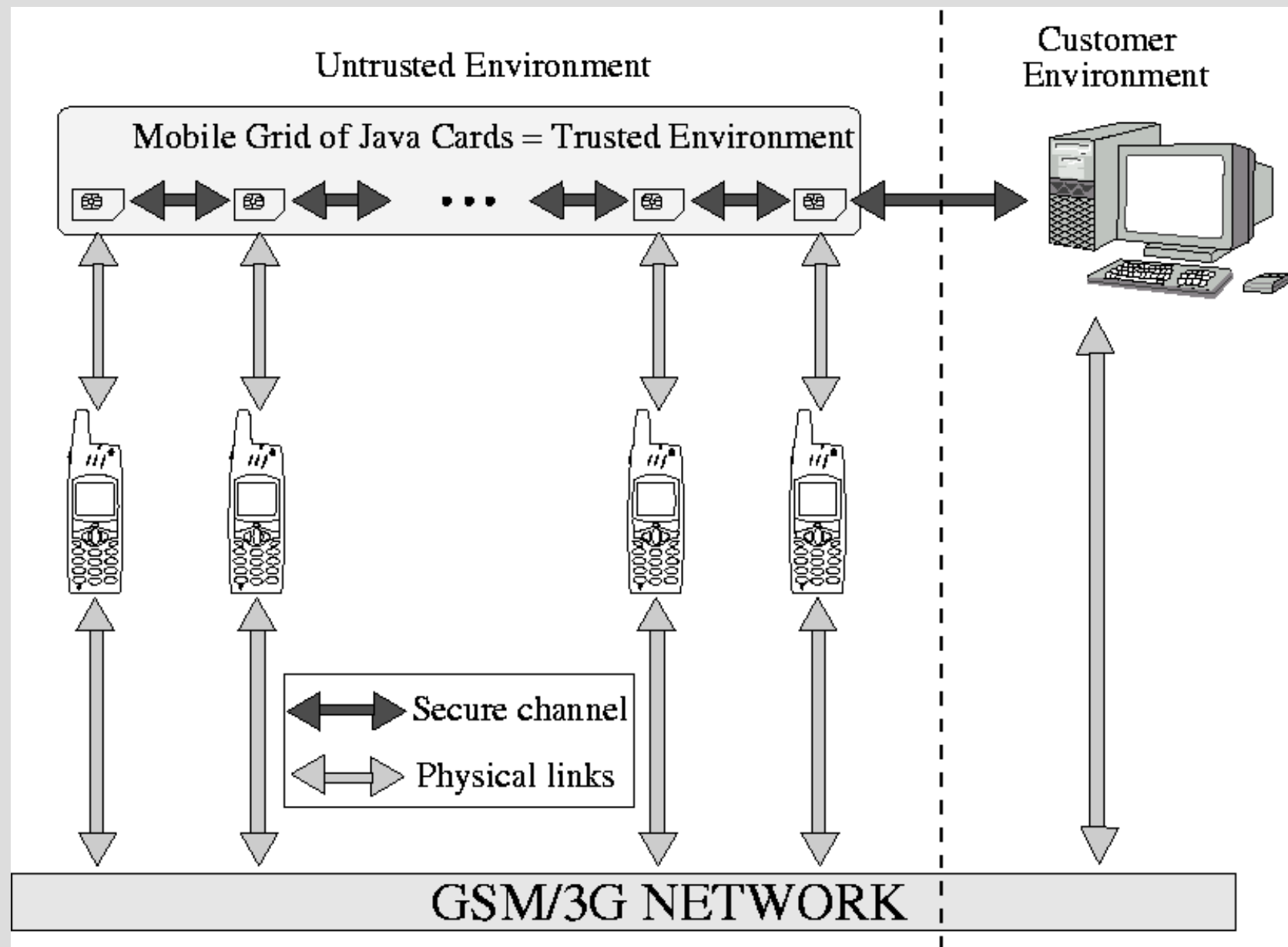
- Aspects logiciels
  - Gestion des pannes
  - Assemblage de composants
  
- Passage à l'échelle
  - Avec plus de cartes:
    - 1000 lecteurs envisagés
    - Sera mené avec un industriel
      - (confidentiel pour l'instant)
  - Avec de vrais processeurs
    - Trusted Computing Group

# Soutiens industriels

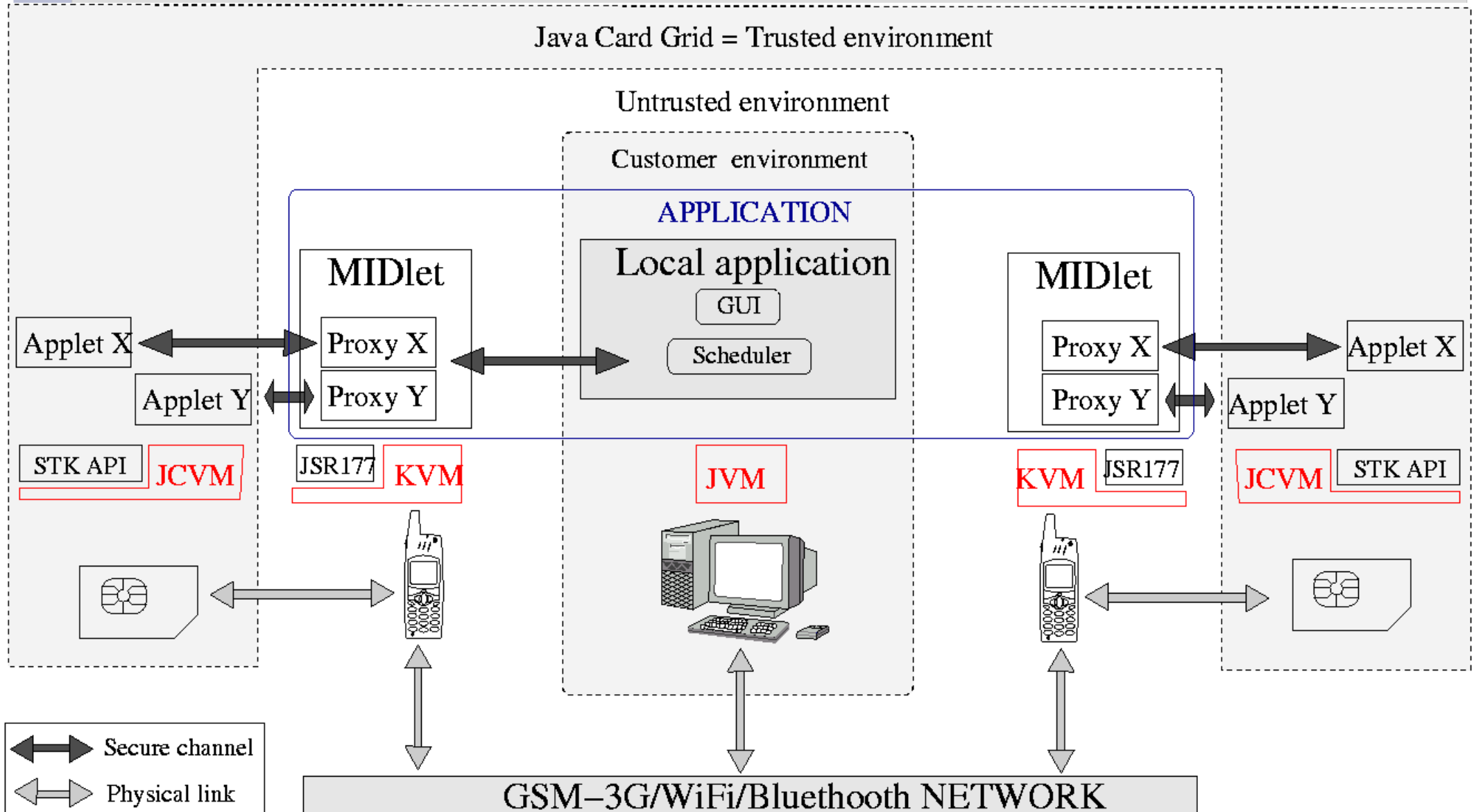
- Sun Microsystems
  - IBM
  - Oberthur
  - Gemplus
  - Schumberger
  - Smartmount
  - SCM
  - Giesecke & Devrient GmbH
- Fujitsu



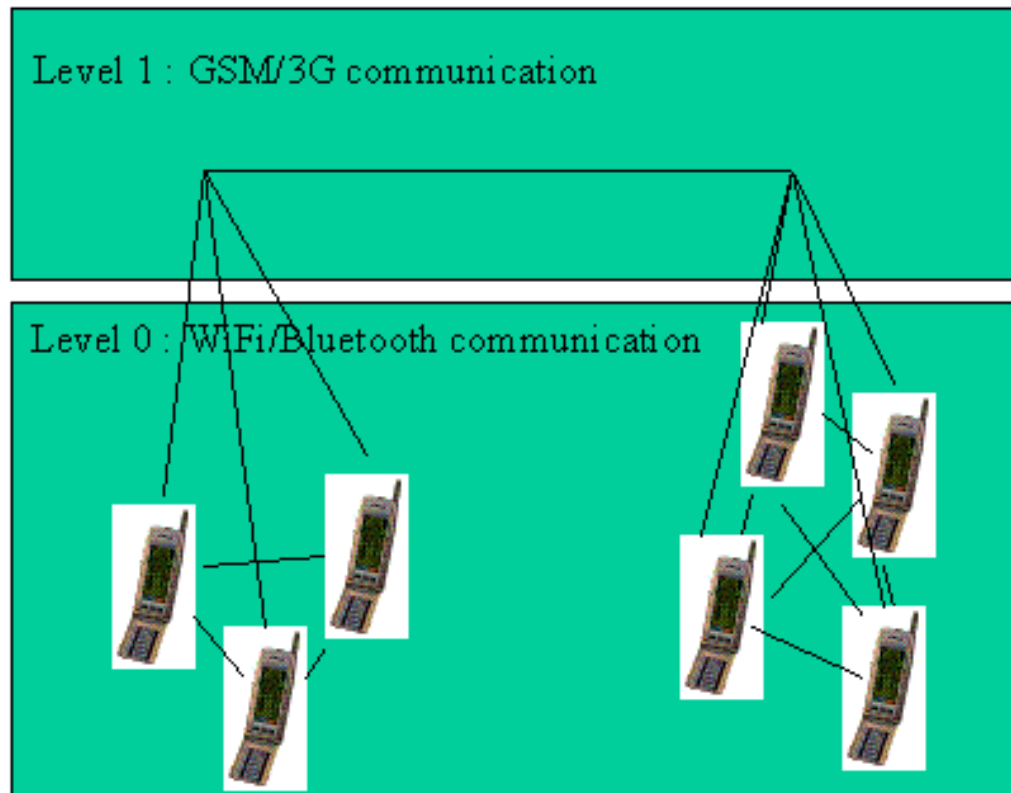
## La mobile Java Card Grid



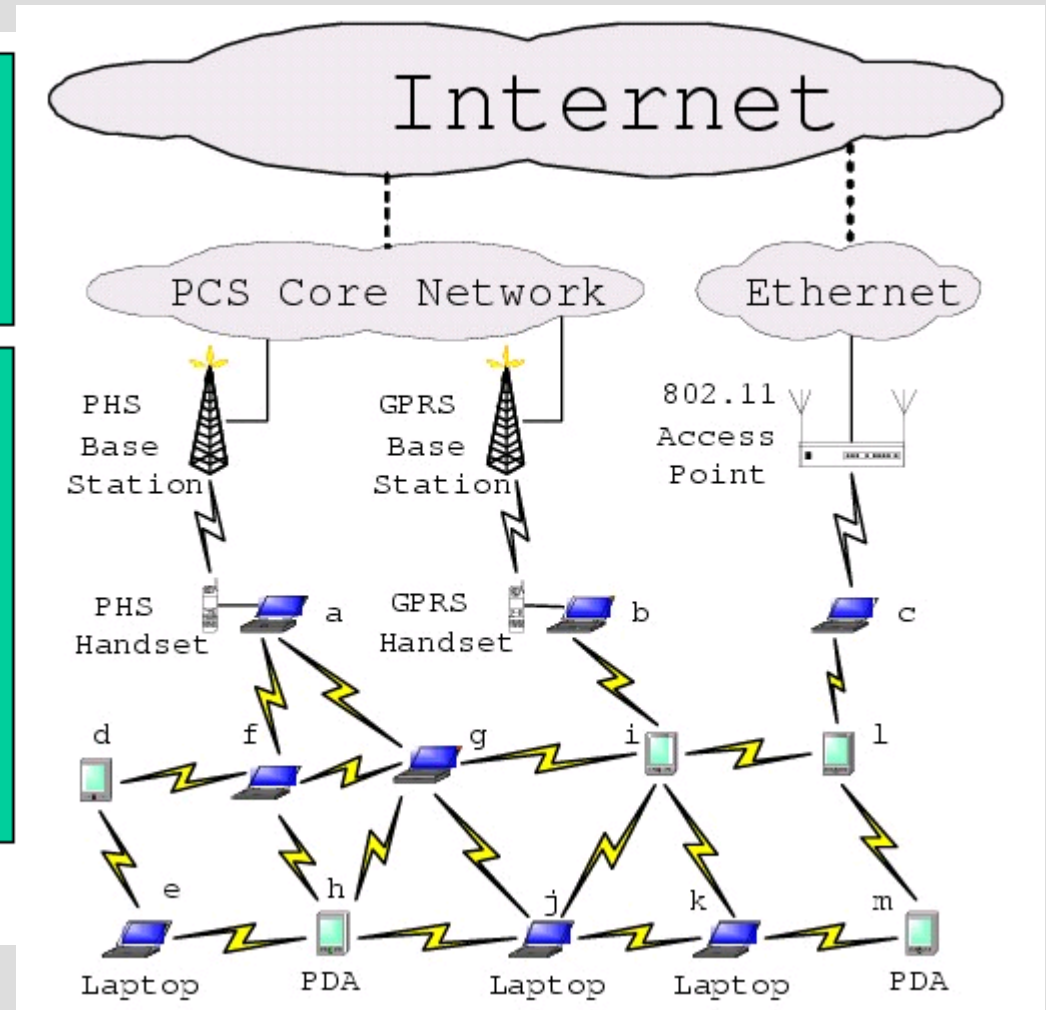
# La multilevel Java Card Grid (1/2)



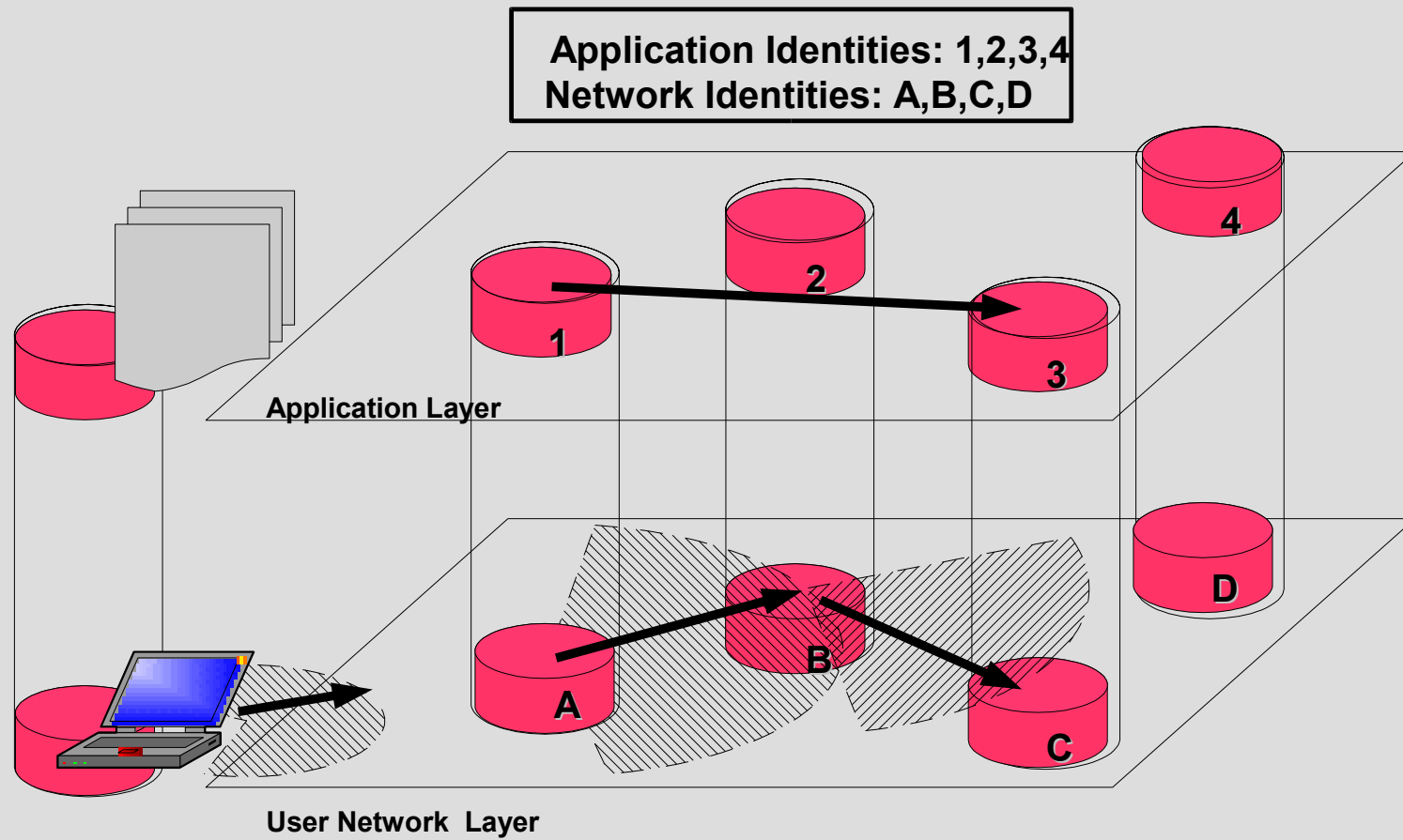
## La multilevel Java Card Grid (1/2)



Multilevel Java Card Grid

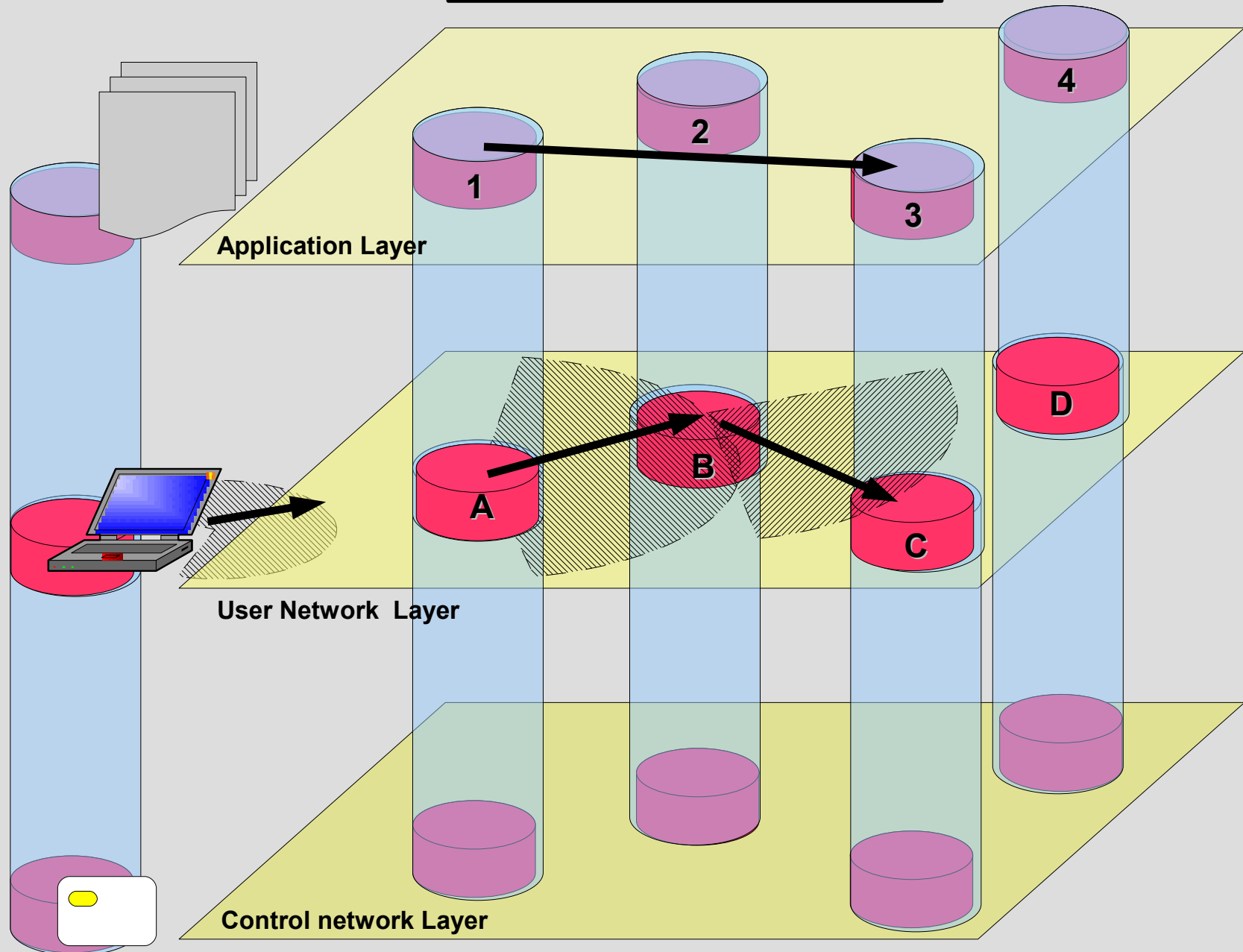


## Les réseaux ad hoc

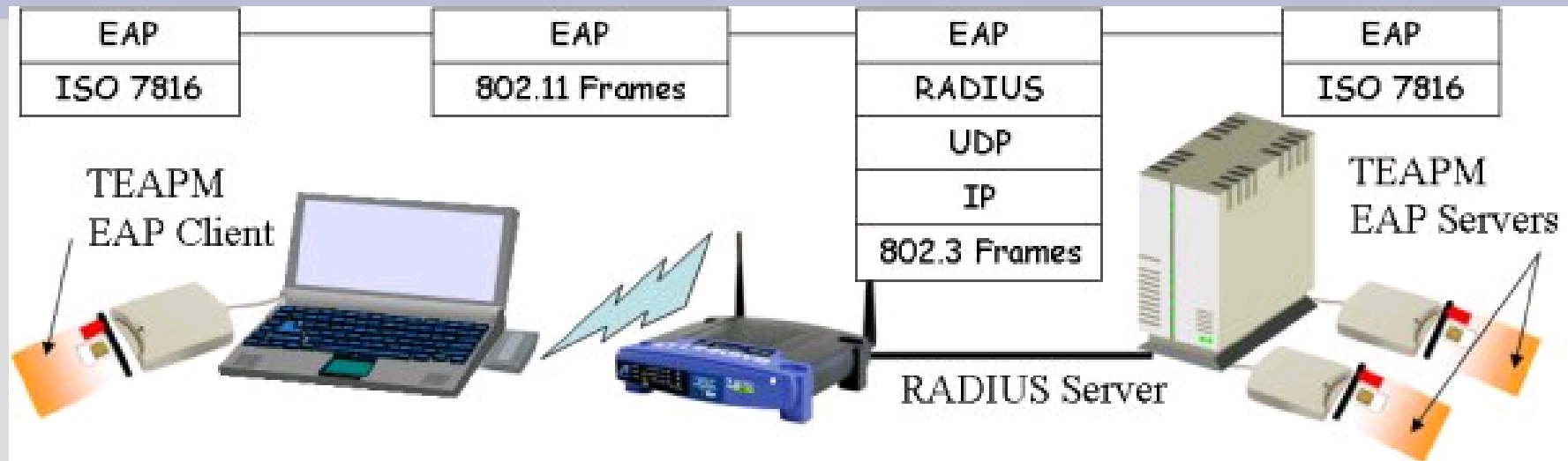


## Une solution de sécurisation

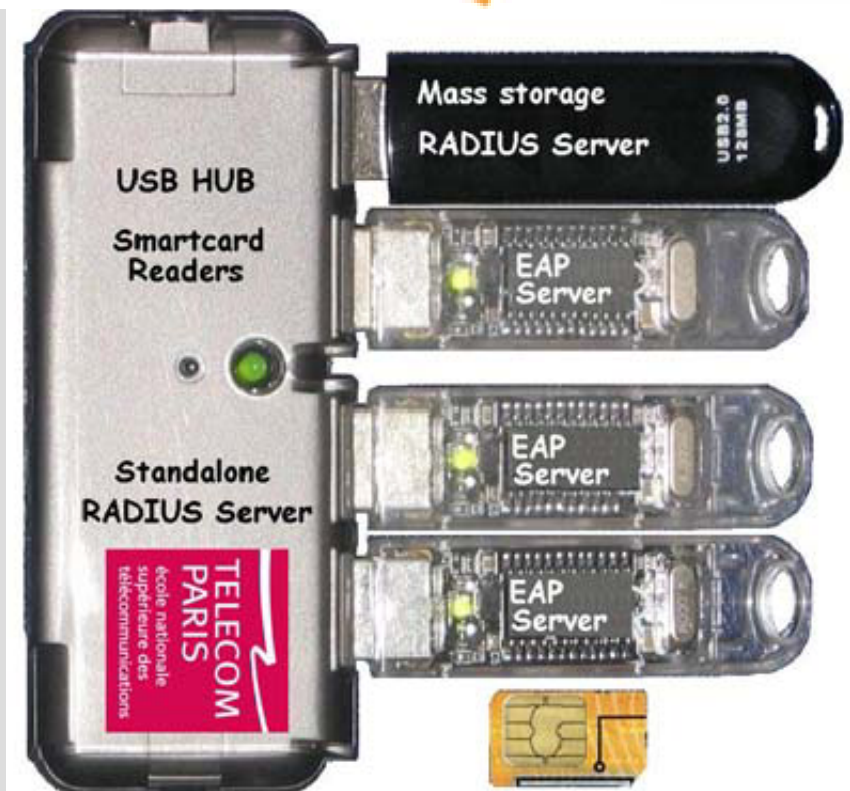
Application Identities: 1,2,3,4  
Network Identities: A,B,C,D



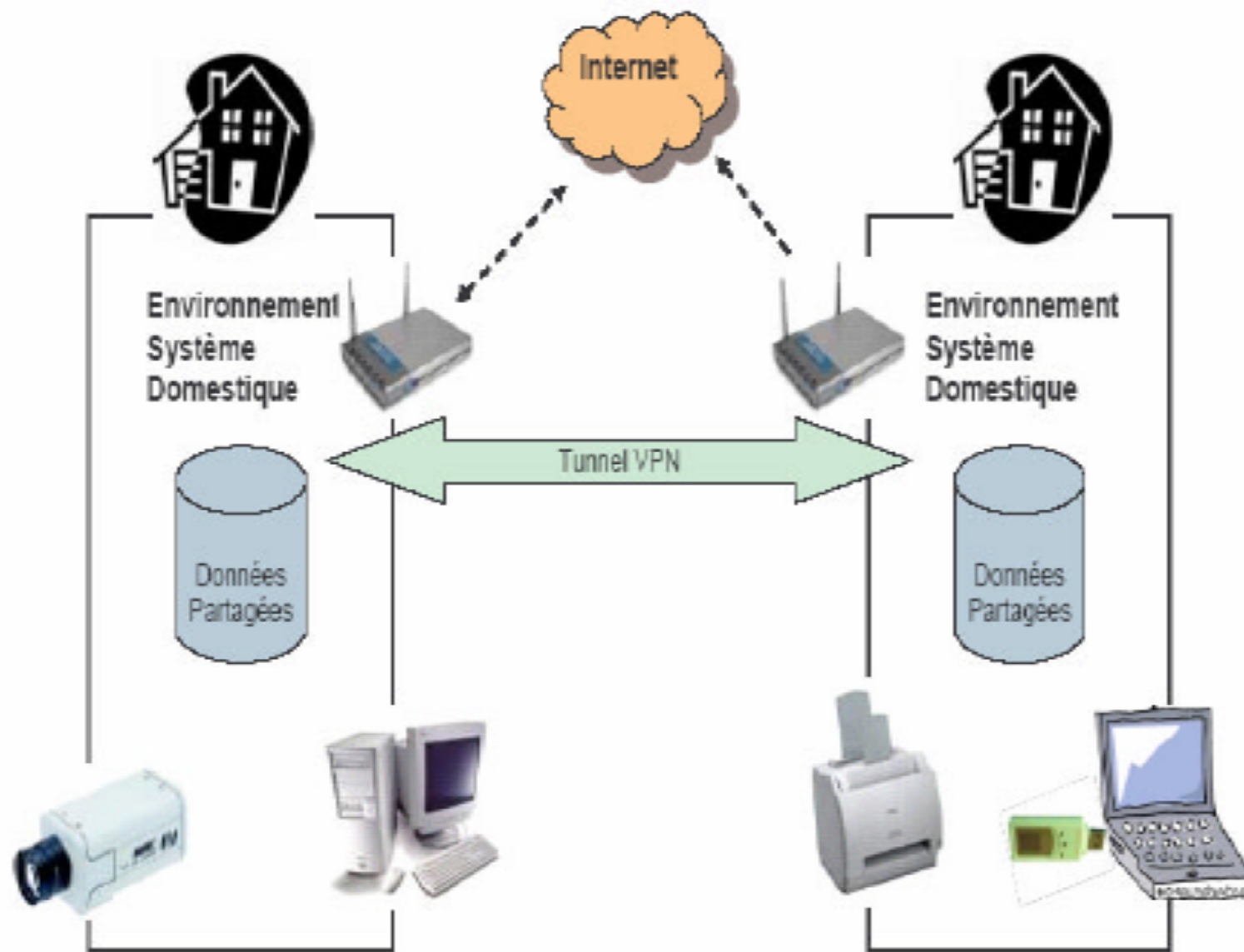
## Sécurisé le réseau WiFi avec EAP



**EAP: Extensible Authentication Protocol**



## Réseaux domestiques



**La carte  
=  
un élément fondamental  
pour assurer la sécurité des réseaux  
(et applications)**