



Carte à puce

SALS : Supports Amovibles Légers et Sécurisés

SRAD : Sécurité des Réseaux et Applications Distribués

Damien Sauveron

damien.sauveron@xlim.fr

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

La carte à microprocesseur

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

ROM : 256/512 Ko

EEPROM/FeRAM/Flash : 24 à 256 Ko

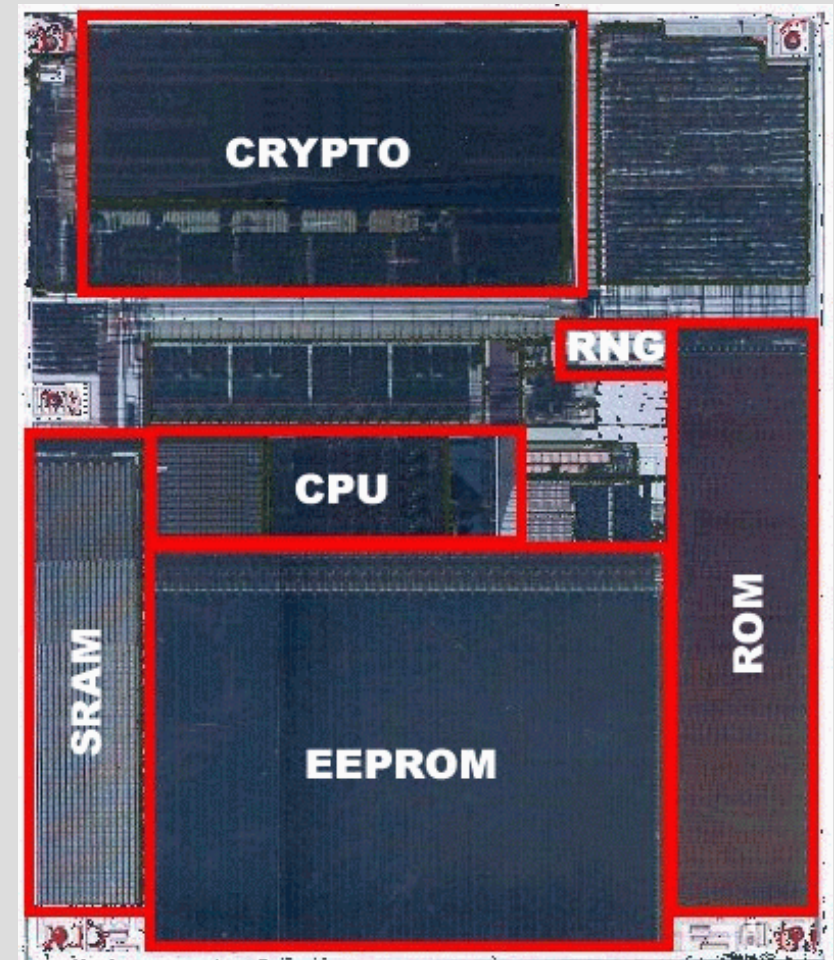
RAM : 1 à 4 Ko

Coprocasseur cryptographique

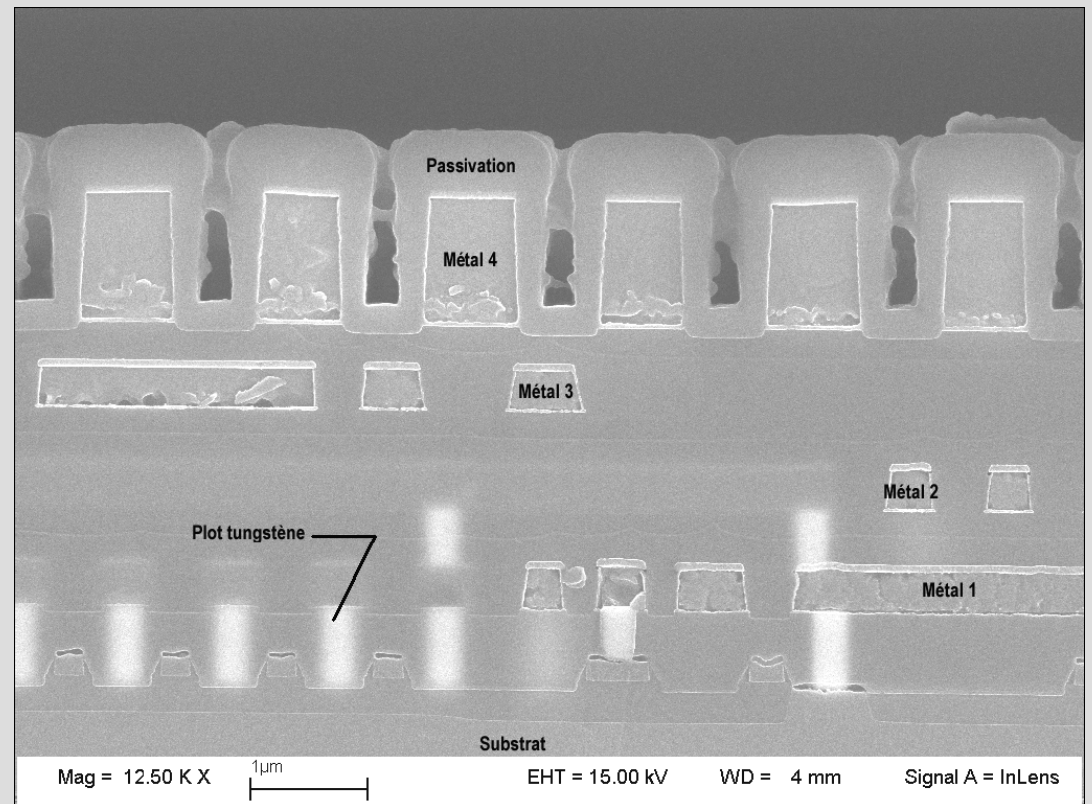
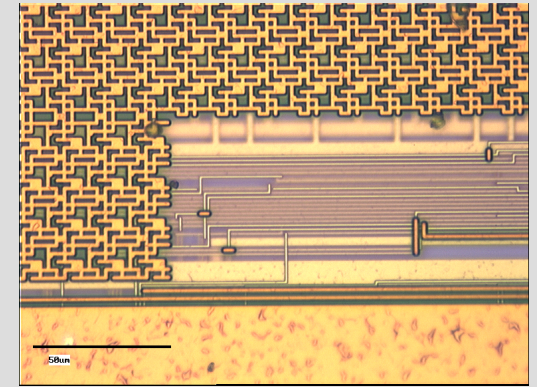
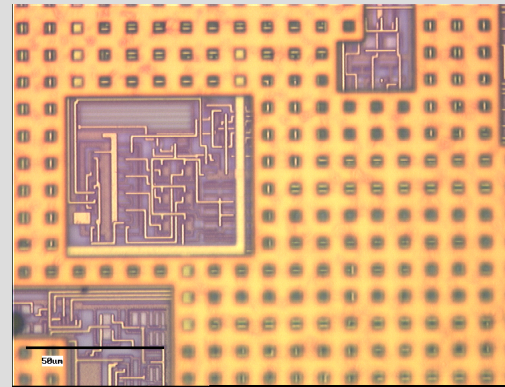
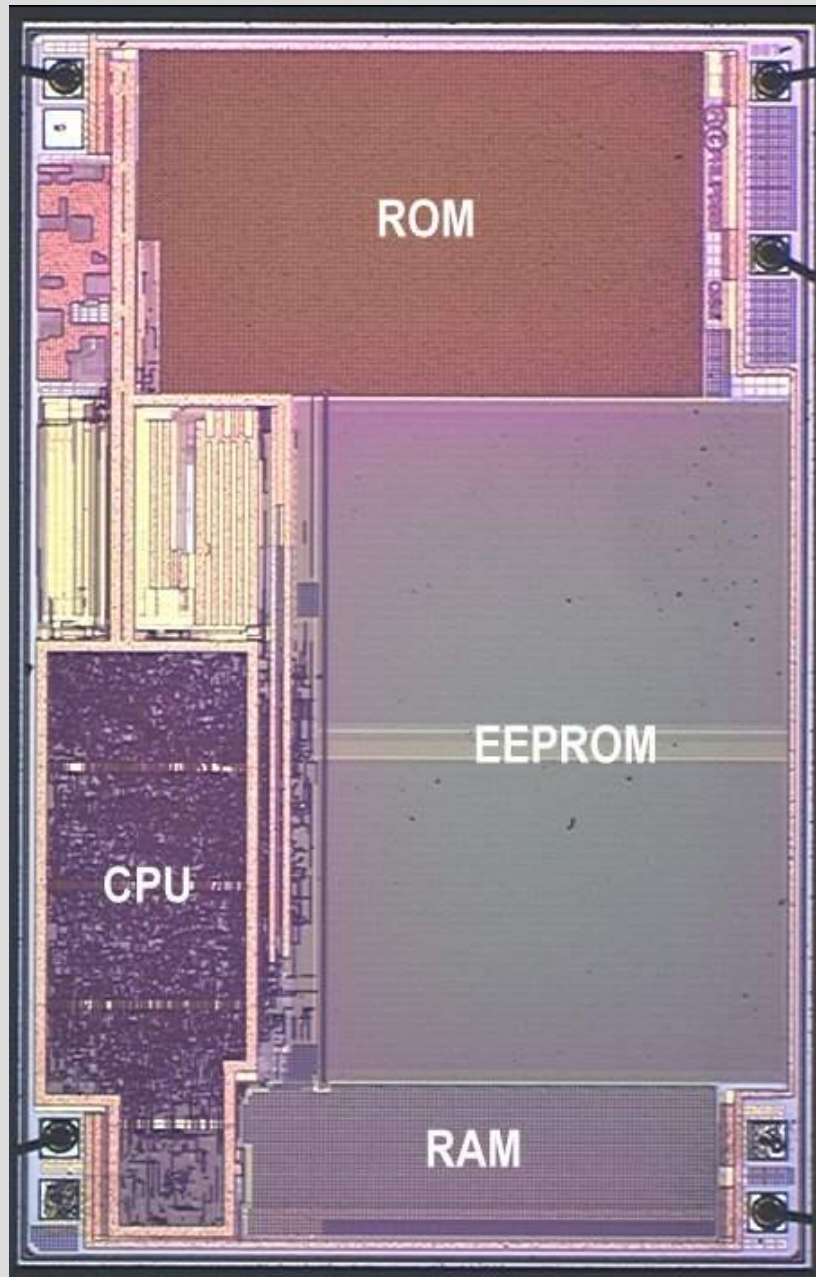
Générateur de nombres aléatoires (RNG)

Détecteur de sécurité, ...

	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

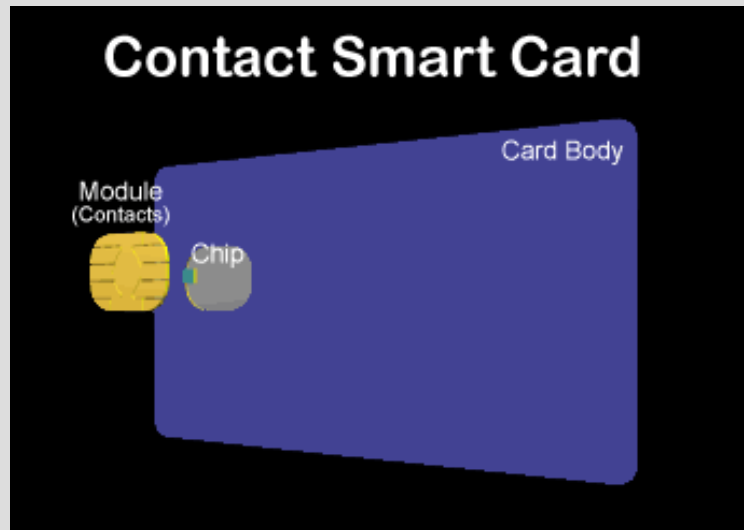


Une puce sous toutes les coutures

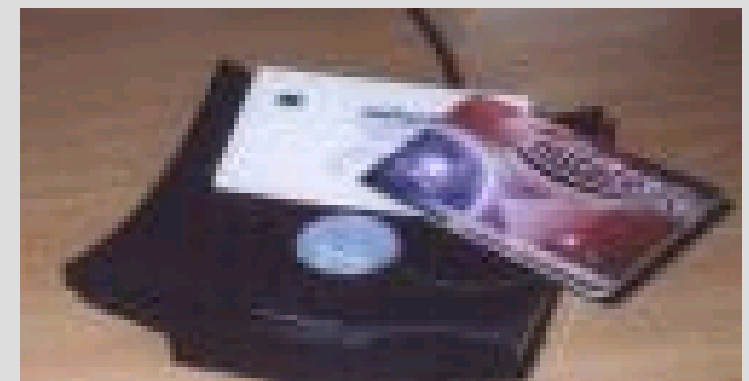
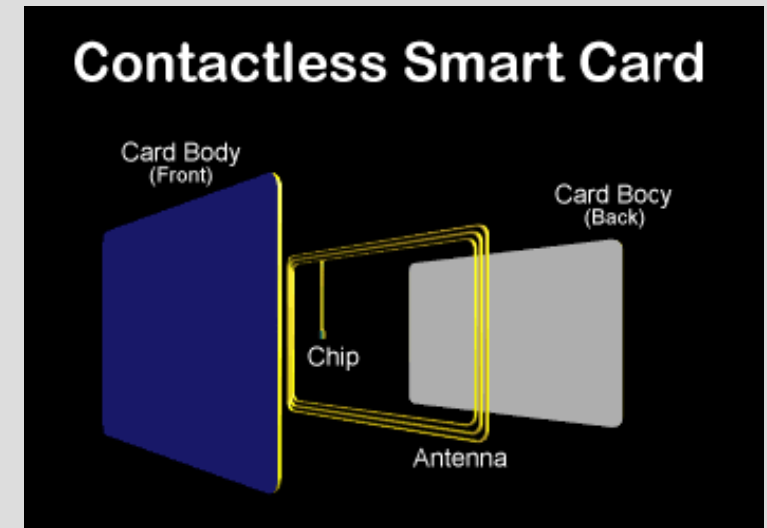


Les cartes à contact, les sans contacts ... et les autres formes

Contact Smart Card

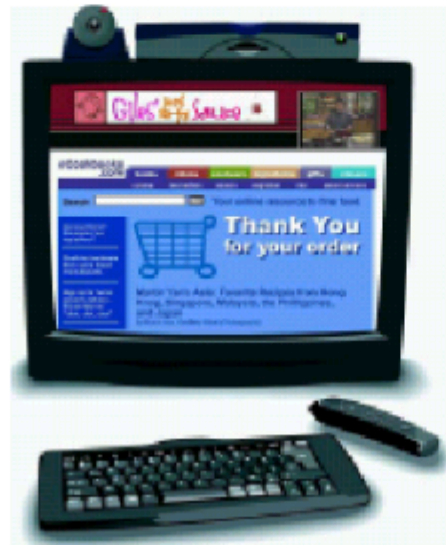


Contactless Smart Card



Les terminaux cartes

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



Pourquoi utiliser la carte à puce ? **Le périphérique le plus sécurisé au monde**

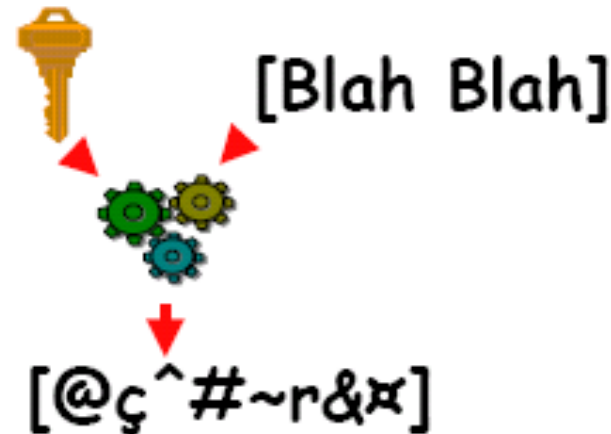
- Tamper resistance
 - Storage



- Portability



- Tamper resistance
 - Processing

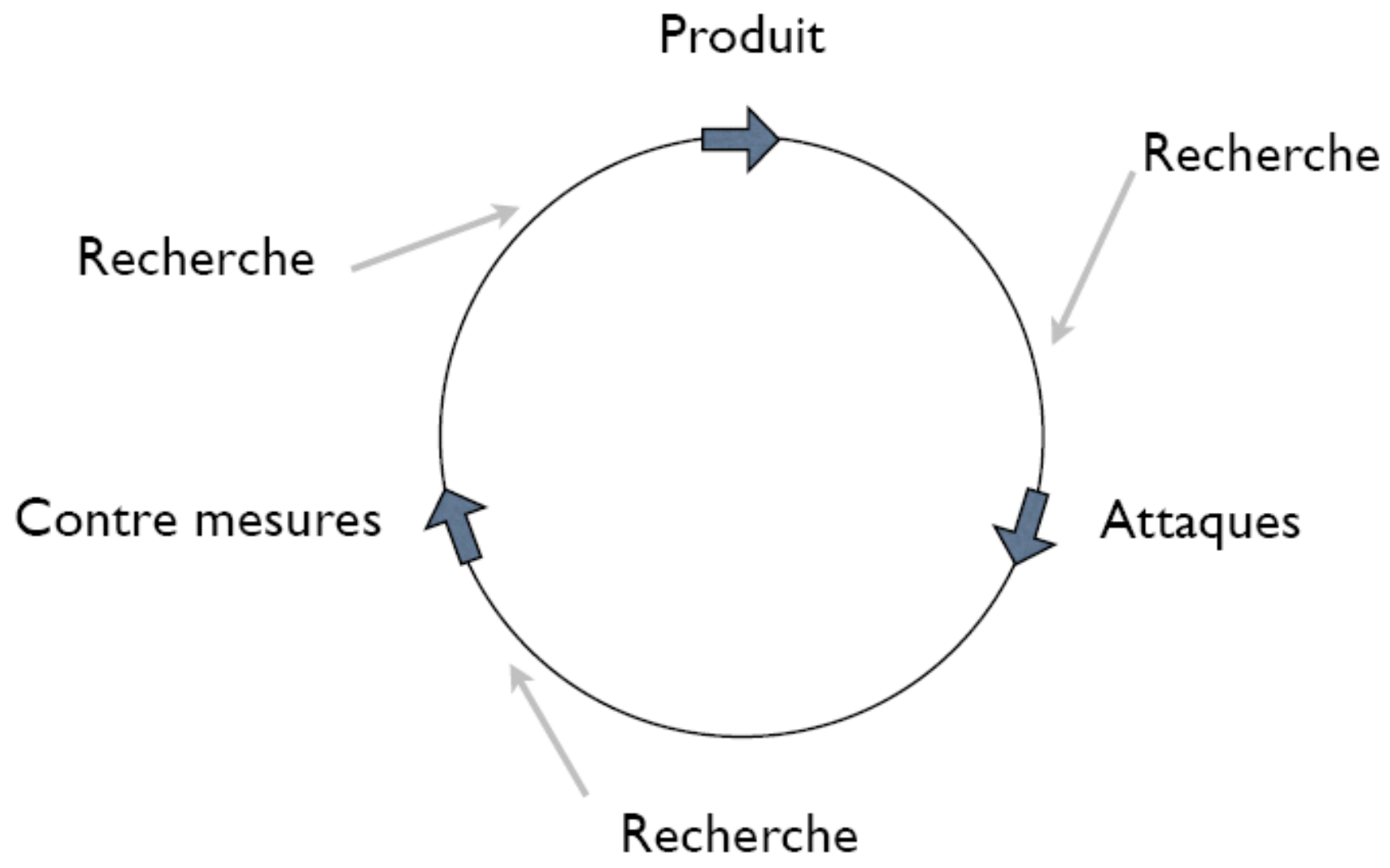


- Ease of use
- Onboard key generation
- Cost

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

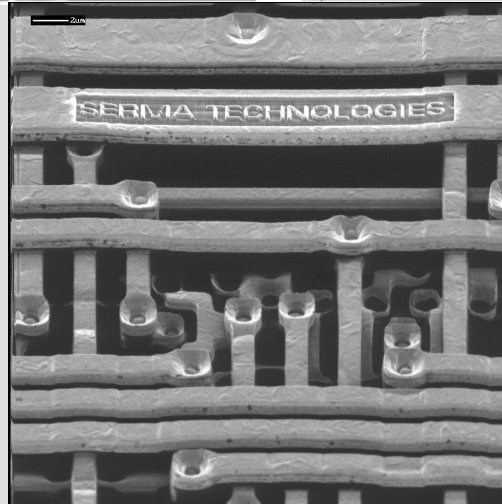
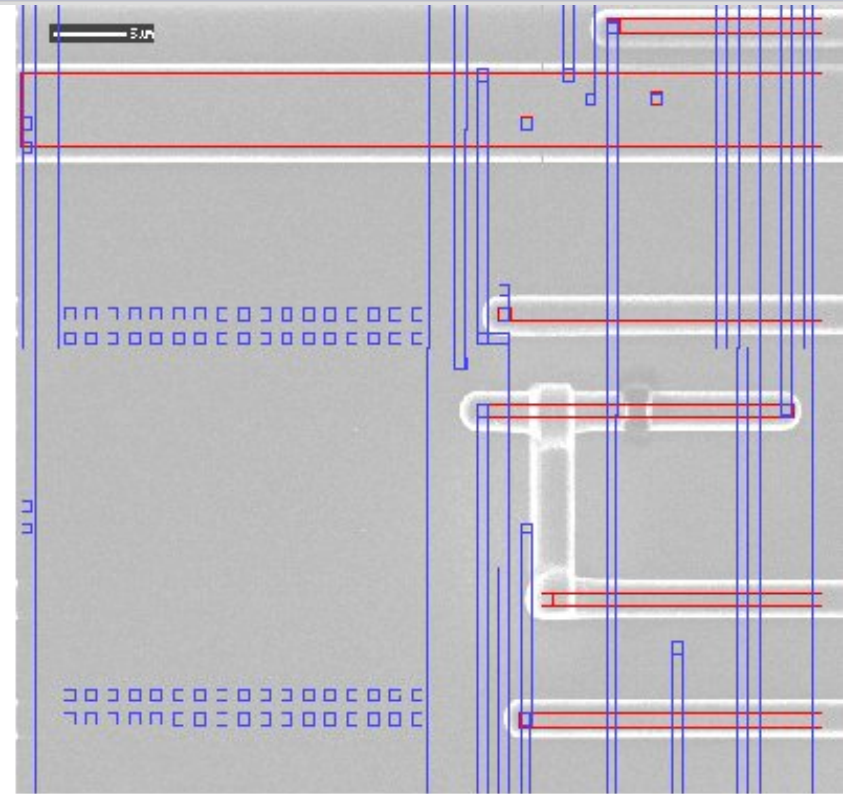
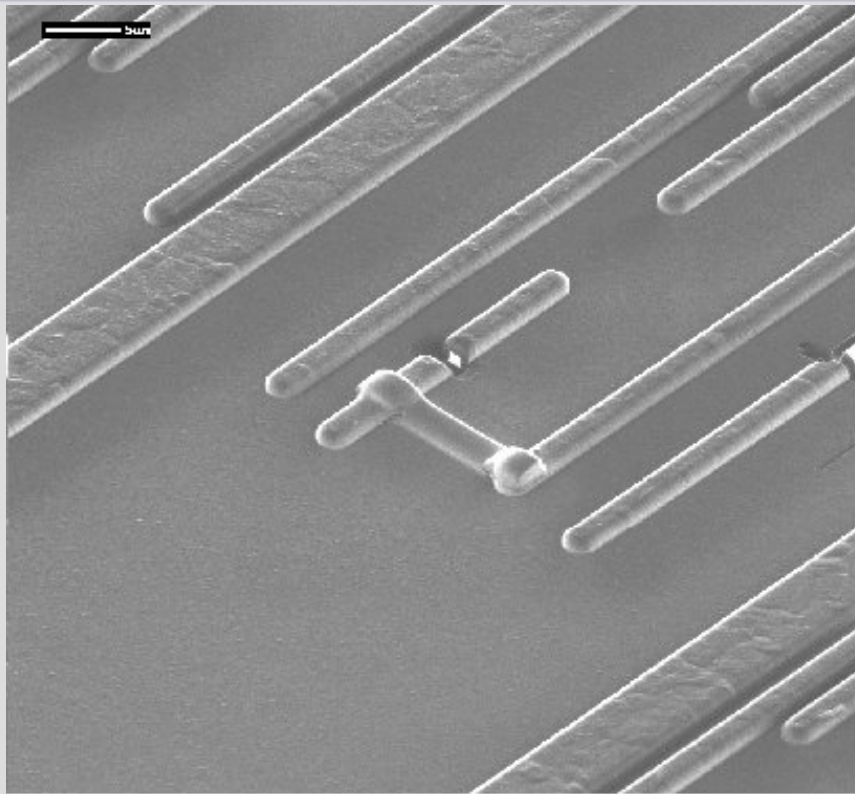
Questions ?

Le cycle infernal



- **SALS : Supports Amovibles Légers et Sécurisés**
- Objectifs : les attaques et les contre-mesures

Modifications de circuits (avec un FIB)



Le matériel pour nos attaques

Oscilloscope numérique et un lecteur de carte à puce,

PC équipé de cartes d'acquisition et de logiciels mathématique de traitement des données,

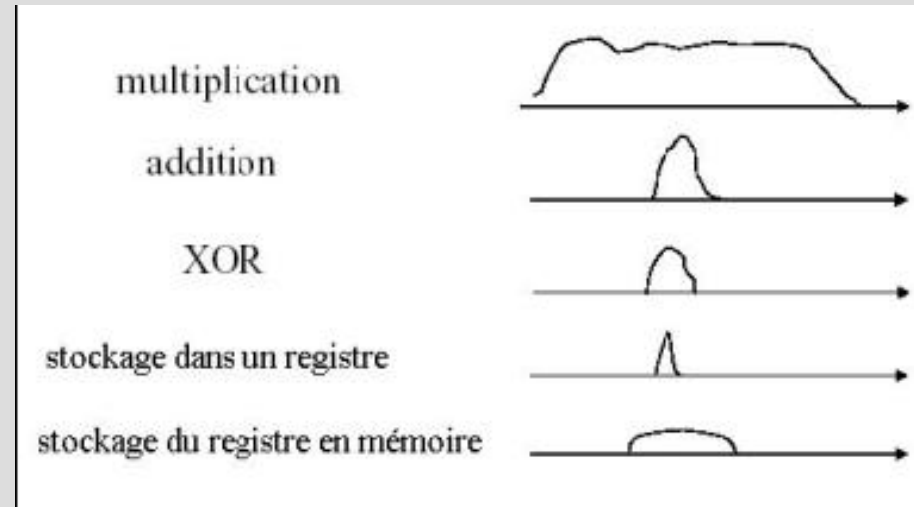
Sonde CEM si on veut étudier les émissions électromagnétiques

Platine motorisée 3D

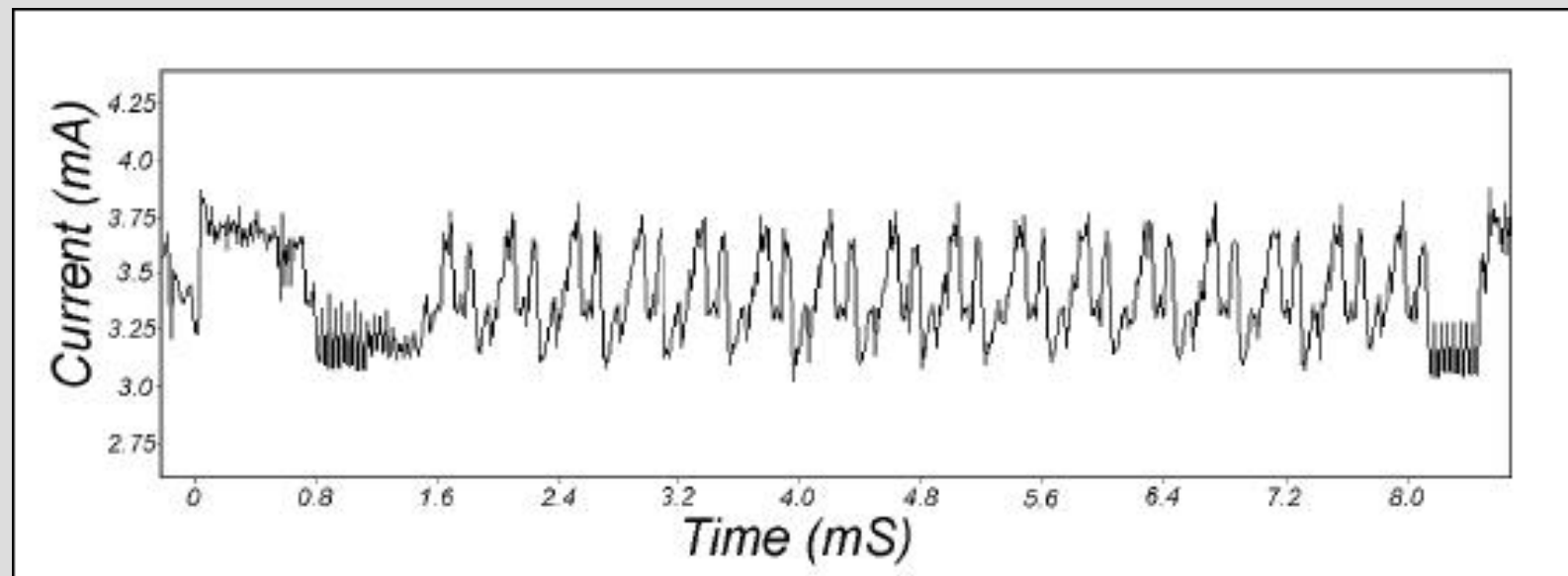


Attaque SPA (Simple Power Analysis)

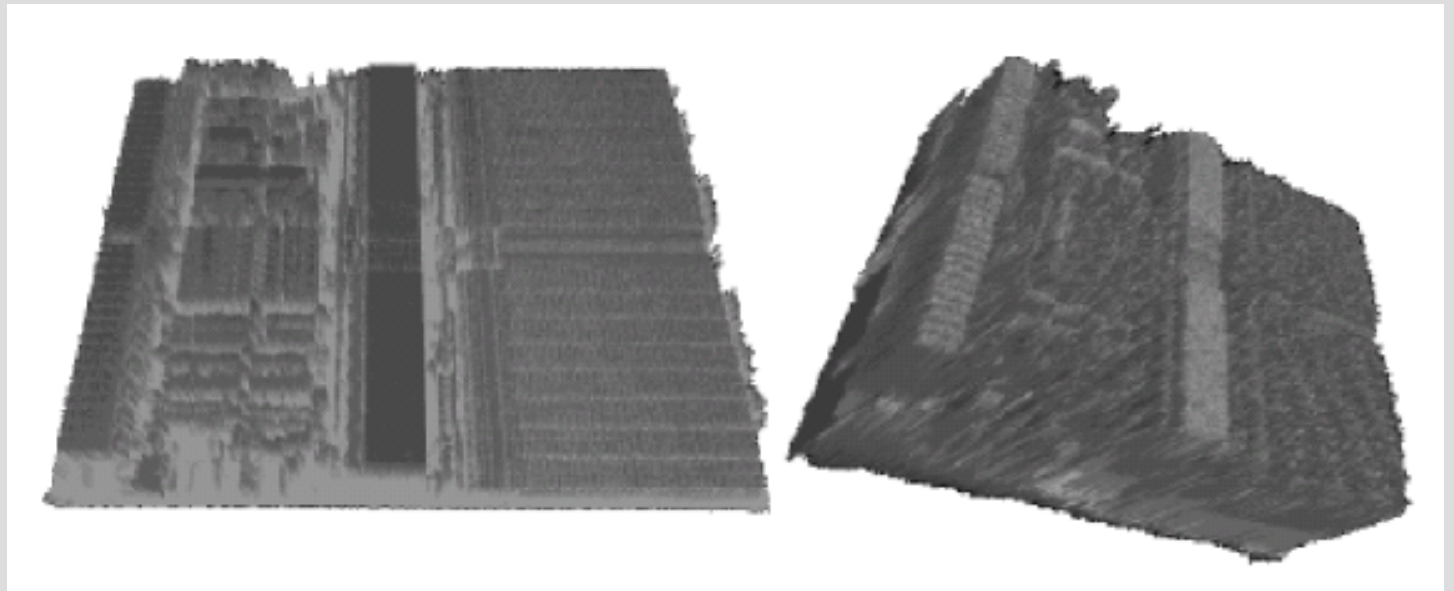
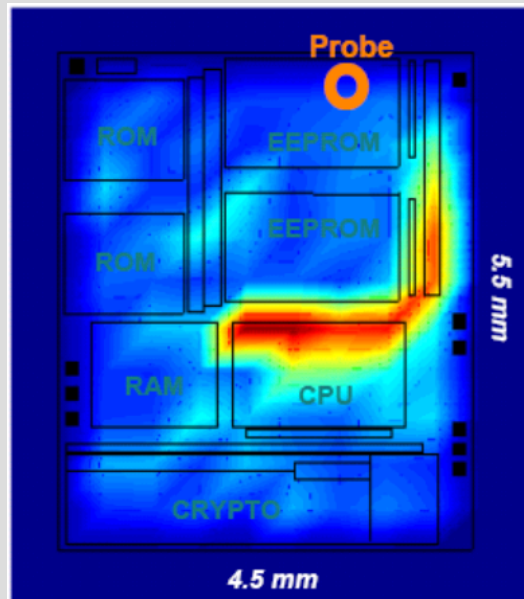
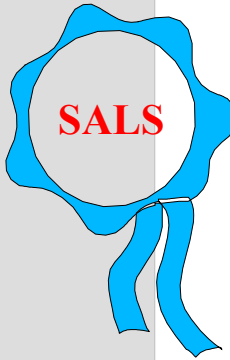
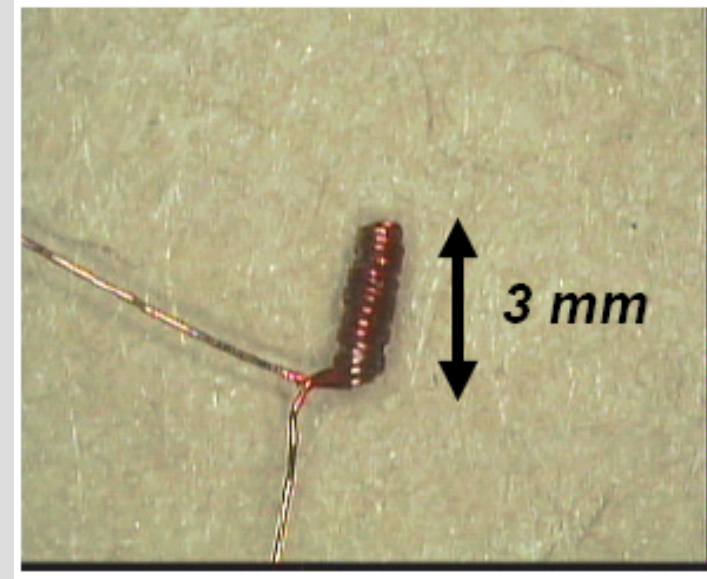
Principe : Des instructions différentes ont une trace différente.



Consommation en courant d'un chiffrement DES.



La cartographie EM et attaques EM (passive/active)



Questions ?

SRAD : Sécurité des Réseaux et Applications Distribués

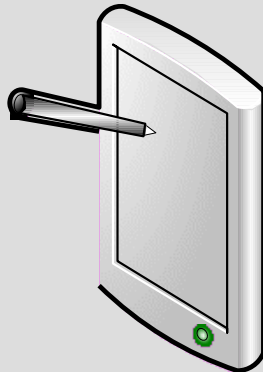
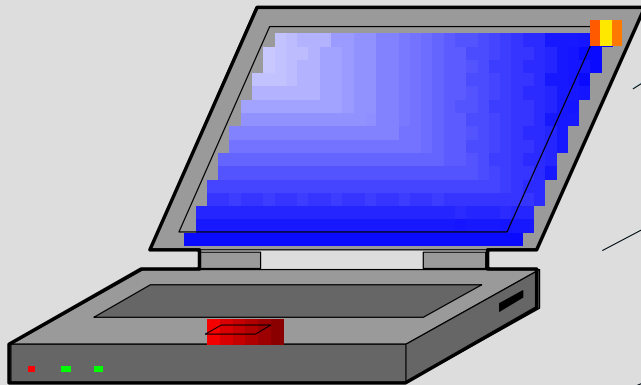
Projet ANR SARAH (*Services distribués Asynchrones pour Réseaux Ad Hoc*)

- VALORIA (Vannes)
- LITIS (Le Havre)
- LaBRI (Bordeaux)
- XLIM (Limoges)

Projet MADNESS (*Mobile Ad Hoc Network with Embedded Secure System*)

Les cibles des réseaux ad hoc

UMPC, PDA, Laptop, ...



Léger

Communication radio

Ultra mobile

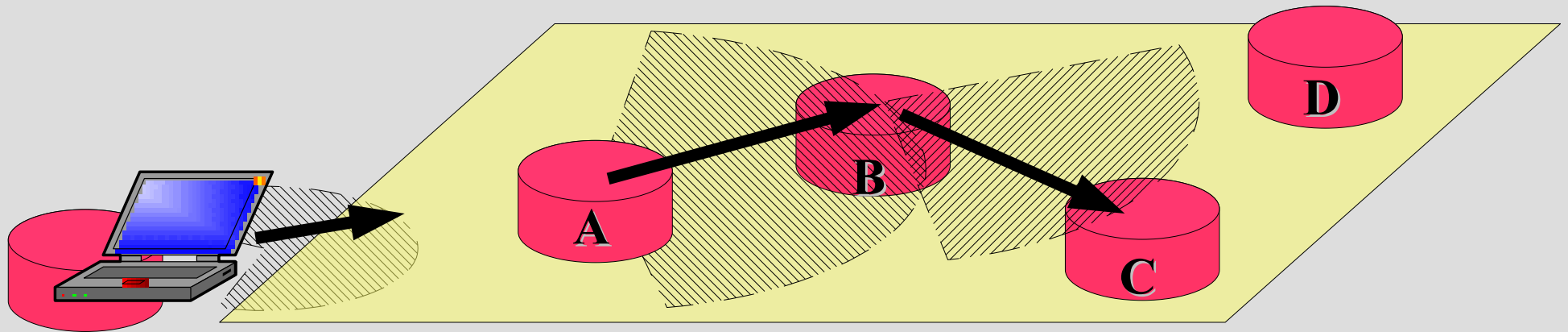
Ultra personnel

Puissance de calcul limitée

Autonomie limitée

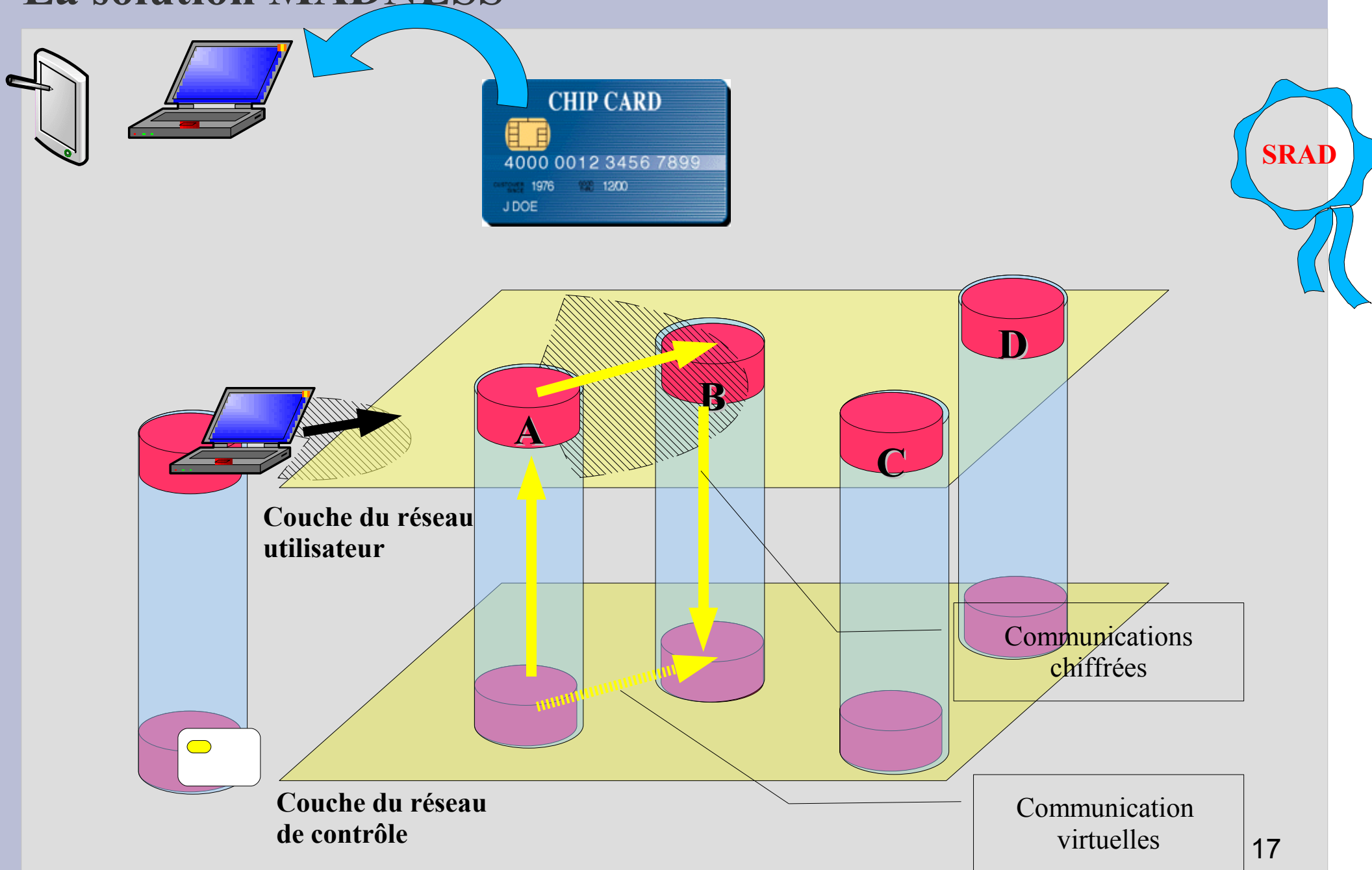
Communications dans un réseau ad hoc

La portée radio étant limitée, on passe par des noeuds intermédiaires



Problème : B peut être égoïste, malveillant, défectueux

La solution MADNESS



Questions ?

Les personnes

– SALS

Pierre Dusart (Responsable scientifique)
François Arnault
Bruno Barelaud
Denis Peyrat (Doctorant)
François Torrès
Damien Sauveron
Georges Younis (Post-doctorant)

– SRAD

Pierre-François Bonnefoi (Responsable scientifique)
Carlos Aguilar Melchor (ATER)
François Arnault
Ève Atallah (Doctorante)
Céline Burgod (Doctorante)
Julien Cartigny
Pierre Dusart
Damien Sauveron

– Quelques partenaires

Institutionnels : CEA-LETI, CEDRIC, LaBRI, LIFL, LITIS, Royal Holloway

University of London, VALORIA

Privés : EADS, RFI Global Service, SERMA Technologies, Pro-Active, Thomson R&D

COPYRIGHTS

Merci à:

Pierre-François Bonnefoi
Didier Donsez
Pierre Paradinas
David Samyde
Gemalto
SERMA Technologies
UCL

Les droits associés aux illustrations sont leurs propriétés.