

La Carte à Microprocesseur

Un système embarqué en plein essor

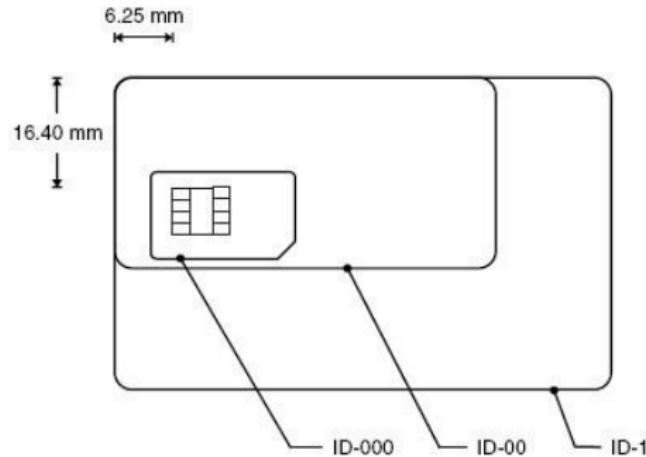
Dr. Tegawendé F. Bissyandé
tegawende.bissyande@fasolabs.org

Cours préparé pour
L'Institut Supérieur de Technologie (IST Burkina)

17 Février 2015

Rappel chapitre 1...

Les fabricants ont la tâche facile!



Critères de classification des cartes à puce

Intelligente ou pas?

- Cartes à mémoire
- Cartes à logique câblée
- Cartes à microprocesseur

Avec quel interfaçage?

- Cartes à contact
- Cartes sans contact
- Cartes dual dual-interface

Critères de classification des cartes à puce

Intelligente ou pas?

- Cartes à mémoire
- Cartes à logique câblée
- Cartes à microprocesseur

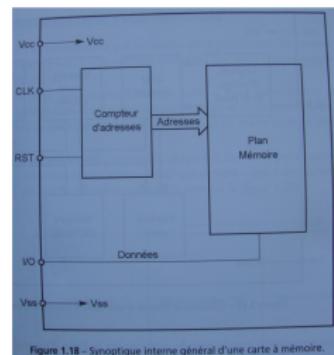
Avec quel interfaçage?

- Cartes à contact
- Cartes sans contact
- Cartes dual dual-interface

Des cartes obsoletes... (1)

Carte à mémoire simple

- 1^{ère} génération de cartes
(Avant 2000, majorité des cartes)
- Une puce mémoire de 1 à 16 Ko
- Une notion de zone :
 - 1 Read-only : zone à valeur fixe [id émetteur]
 - 2 Writable : zone pour lecture [compteur d'unité]
 - 3 fusible : cycle de vie achevé si fusible grillé



Des cartes obsoletes... (2)

Carte à mémoire OTPROM : One Time Programmable

- les dinosaures de la planète carte à puce
- technologie NMOS : 21V pour Vpp
- Circuit intégré programmable 1 seule fois

Télécarte

- Circuit intégré ST 1200 (SGS Thomson)
- Pas rechargeable (parfait pour télécarte)
- Sécurité : programmable 1 seule fois

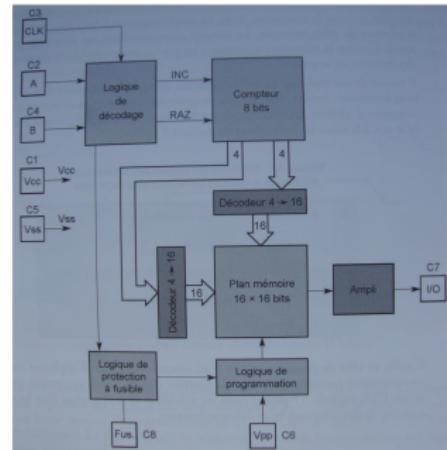
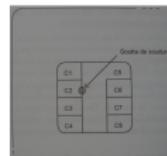


Figure 2.1 ~ Synoptique interne d'une carte à mémoire OTPROM à base de ST 1200.

Facilement piratable...



Des cartes obsoletes... (2)

Carte à mémoire OTPROM : One Time Programmable

- les dinosaures de la planète carte à puce
- technologie NMOS : 21V pour Vpp
- Circuit intégré programmable 1 seule fois

Télécarte

- Circuit intégré ST 1200 (SGS Thomson)
- Pas rechargeable (parfait pour télécarte)
- Sécurité : programmable 1 seule fois

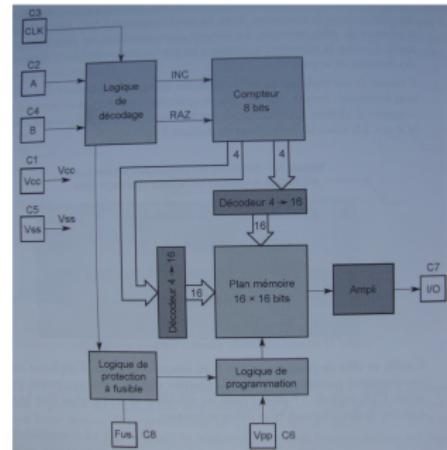
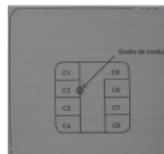


Figure 2.1 ~ Synoptique interne d'une carte à mémoire OTPROM à base de ST 1200.

Facilement piratable...



Résumé sur la carte à mémoire

Caractéristiques

- Stockage de données, pas de CPU
- Logique 1 fois-programmable
- Cycle de vie

Avantages

- Technologie très simple
- Technologie à faible coût ($\approx 1\text{€}$)

Inconvénients

- Dépendance vis-à-vis du lecteur de carte
- Facilement piratable (logique faillible)

Un cadenas ne se ferme pas tout seul...



Résumé sur la carte à mémoire

Caractéristiques

- Stockage de données, pas de CPU
- Logique 1 fois-programmable
- Cycle de vie

Avantages

- Technologie très simple
- Technologie à faible coût ($\approx 1\text{€}$)

Inconvénients

- Dépendance vis-à-vis du lecteur de carte
- Facilement piratable (logique faillible)

Un cadenas ne se ferme pas tout seul...



Résumé sur la carte à mémoire

Caractéristiques

- Stockage de données, pas de CPU
- Logique 1 fois-programmable
- Cycle de vie

Avantages

- Technologie très simple
- Technologie à faible coût ($\approx 1\text{€}$)

Inconvénients

- Dépendance vis-à-vis du lecteur de carte
- Facilement piratable (logique faillible)

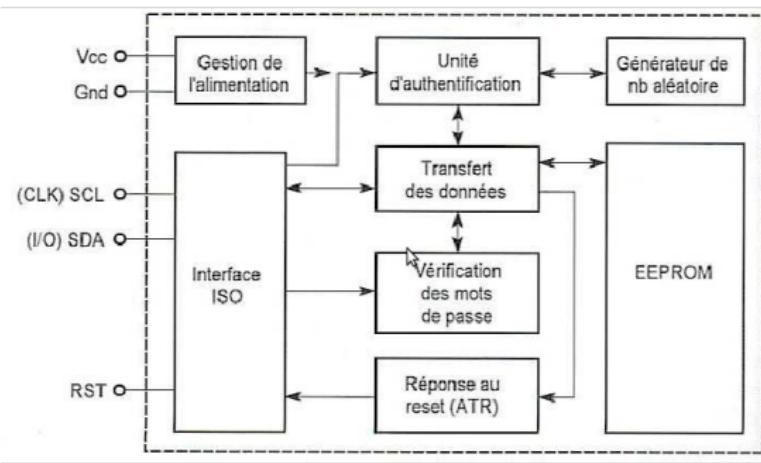
Un cadenas ne se ferme pas tout seul...



Carte à logique cablée

Caractéristiques

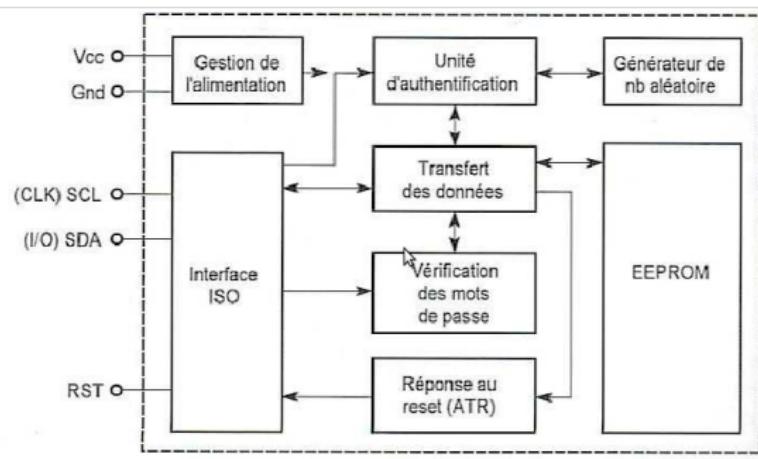
- 2eme génération de cartes
- Zone mémoire + règles d'utilisation de la mémoire
- Logique physiquement implantée dans le silicium de la carte



Carte à logique cablée

Caractéristiques

- 2eme génération de cartes
- Zone mémoire + règles d'utilisation de la mémoire
- Logique physiquement implantée dans le silicium de la carte



Carte à logique cablée

Caractéristiques

Adresse	Contenu	Rôle
0-15	Card manufacturer area	Identifie le fabricant de la carte
16-23	Issuer reference	Identifie l'organisme délivreur de la carte ou l'application
24-63	Card identification area	Contient le numero de serie de la carte, l'index de la clé secrète, ...
64-103	Abacus counter area	Contient la balance de la carte (les unités)
128-191	Authentication key	Contient la clé secrète de la carte
288-319	Pull-out flags	Sert à restaurer la valeur du compteur final si la transaction est interrompue
320-375	56-bit user defined area	Effacable

La mémoire est subdivisée en X zones (à lecture seule ou à écriture si la carte l'autorise)

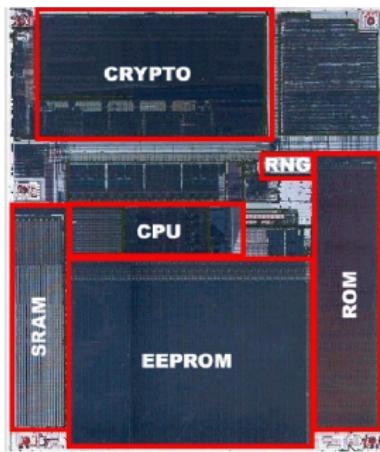
Securité

- 1^{er} niveau : Au niveau de chaque zone mémoire, on peut définir un mot de passe pour la lecture et un autre pour l'écriture
- 2^{eme} niveau : Une authentification mutuelle entre la carte et le lecteur

La vraie carte à puce : Carte à microcontrôleur

Les différentes dénominations

- Cartes à microcontrôleur
- Cartes à microprocesseur
- Cartes intelligentes (*smart cards*)
- **Cartes à puces** (tout court!)

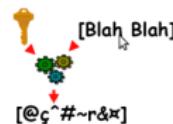


Un microcontrôleur =

- UC + ROM
- RAM + EEPROM
- Interface I/O + processeur cryptographique

Qui fait quoi?

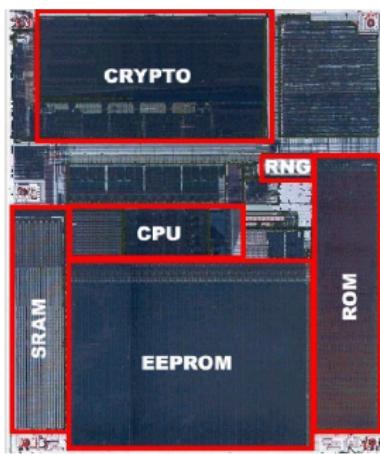
- CPU : 8, 16 ou 32 bits (arch CISC ou RISC)
- ROM : OS et données permanentes (32-256 Ko – Usine)
- RAM : Mémoire vive (1 à 4 Ko – mémoire de travail)
- EEPROM : Mémoire persistante (32-256 Ko – données applicatives)
- coprocesseur cryptographique



La vraie carte à puce : Carte à microcontrôleur

Les différentes dénominations

- Cartes à microcontrôleur
- Cartes à microprocesseur
- Cartes intelligentes (*smart cards*)
- **Cartes à puces** (tout court!)

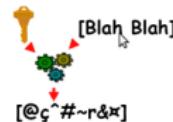


Un microcontrôleur =

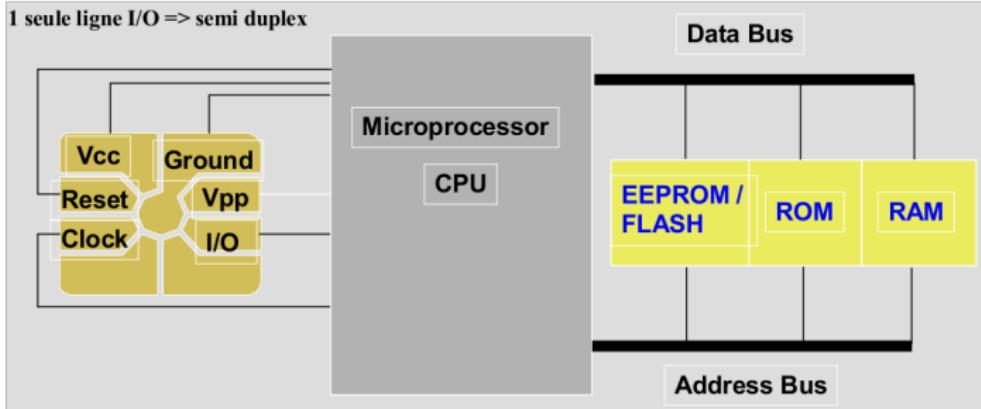
- UC + ROM
- RAM + EEPROM
- Interface I/O + processeur cryptographique

Qui fait quoi?

- CPU : 8, 16 ou 32 bits (arch CISC ou RISC)
- ROM : OS et données permanentes (32-256 Ko – Usine)
- RAM : Mémoire vive (1 à 4 Ko – mémoire de travail)
- EEPROM : Mémoire persistante (32-256 Ko – données applicatives)
- coprocesseur cryptographique

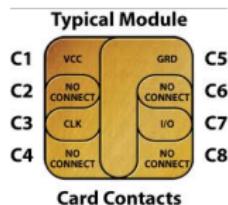


Cartes à contact

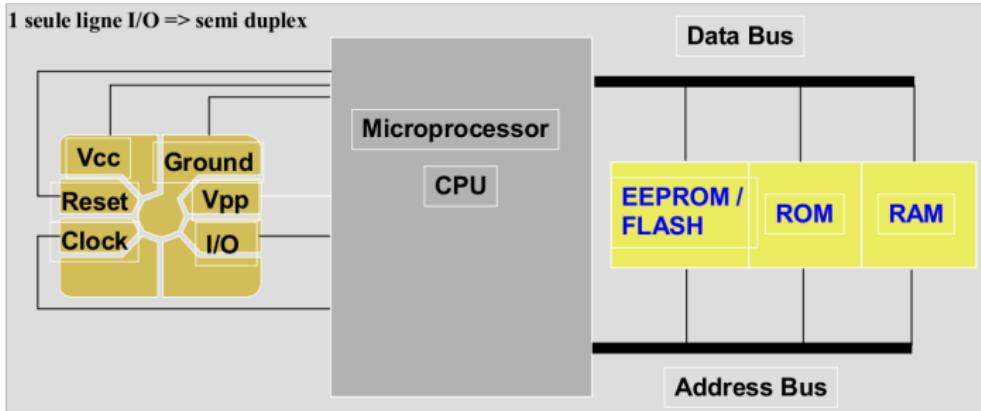


En bref...

- Suit le standard 7816
- Communication série via 8 contacts
- Les insertions/retraits sont des facteurs d'usure
- orientation contraignante de la carte dans le lecteur

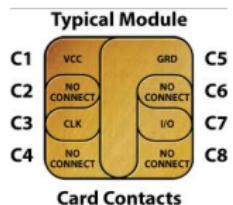


Cartes à contact

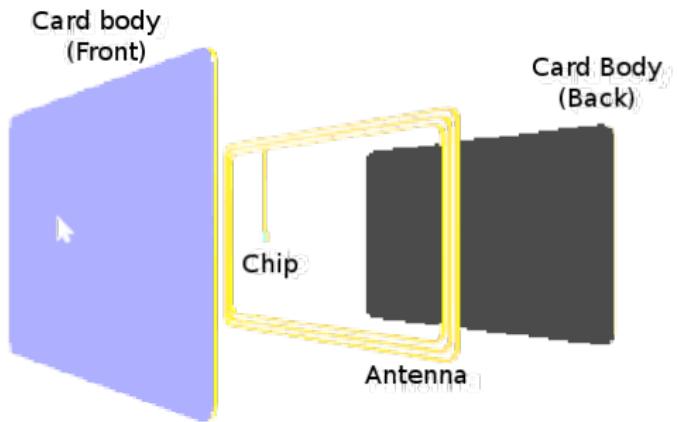


En bref...

- Suit le standard 7816
- Communication série via 8 contacts
- Les insertions/retraits sont des facteurs d'usure
- orientation contraignante de la carte dans le lecteur



Cartes sans contact

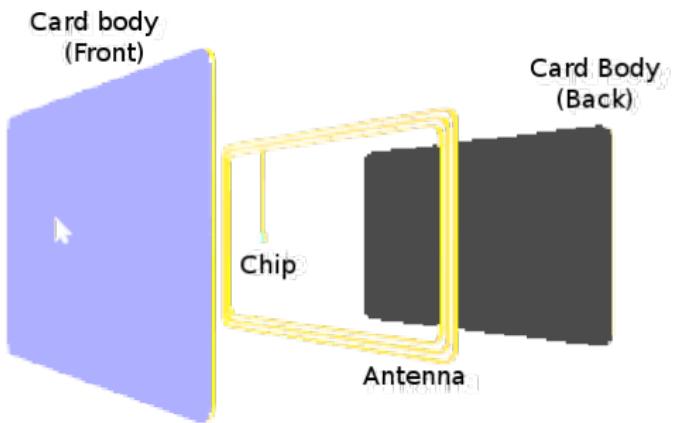


En bref...

- Suit le standard 14443
- Communication série via une antenne embarquée
- Energie fournie par un couplage capacitif ou inductif
- La distance de communication est limitée ($\approx 10\text{cm}$)
- Temps de transaction de 200ms, donc limitations dans les échanges de données
- Coût élevé



Cartes sans contact

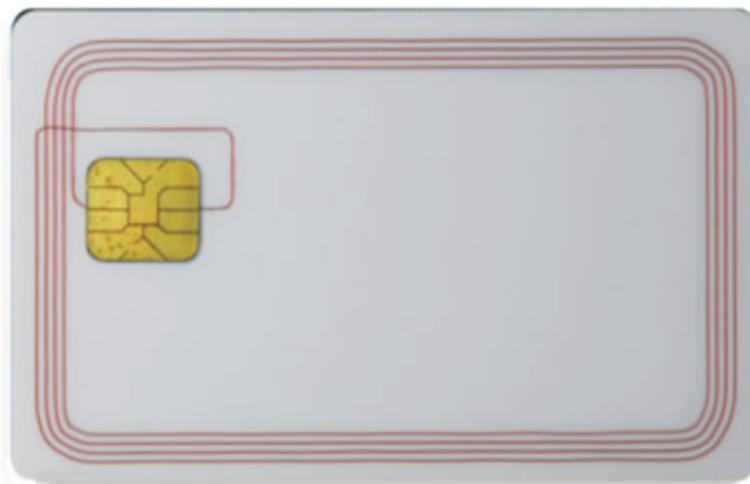


En bref...

- Suit le standard 14443
- Communication série via une antenne embarquée
- Energie fournie par un couplage capacitif ou inductif
- La distance de communication est limitée ($\approx 10\text{cm}$)
- Temps de transaction de 200ms, donc limitations dans les échanges de données
- Coût élevé

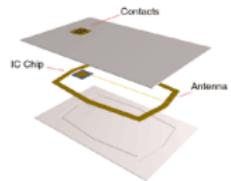


Cartes dual interface & Cartes hybrides

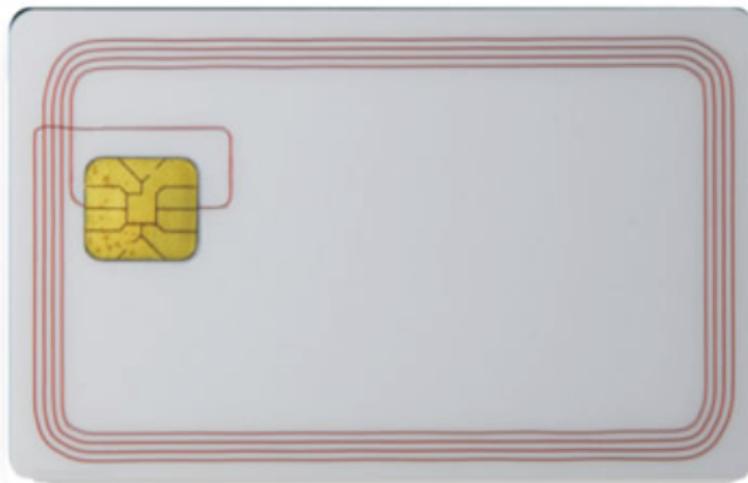


En bref...

- Une combinaison gagnante entre la carte à contacts et celle sans contacts
- Cartes hybrides : deux puces (chips) non interconnectés (une pour la carte à contacts et l'autre pour la carte sans contacts)
- Cartes dual-interface : une seule puce (chip) connectée aux deux interfaces.



Cartes dual interface & Cartes hybrides



En bref...

- Une combinaison gagnante entre la carte à contacts et celle sans contacts
- Cartes hybrides : deux puces (chips) non interconnectés (une pour la carte à contacts et l'autre pour la carte sans contacts)
- Cartes dual-interface : une seule puce (chip) connectée aux deux interfaces.

