Les cartes à puces

Mise à jour le 30 septembre 2006

Un petit bouquet de l'offre commerciale...

Introduction

La carte à puce est une invention française. Notre étude s'intéressera plus particulièrement aux **télécartes françaises** de première génération. Elle ne visera pas à pirater notre cher ami France Télécom mais à lire les informations contenues en leur coeur et à leur trouver (Aux cartes !) des utilités telle que la fabrication d'une serrure codée à lecteur de cartes.

Description

En règle générale, une carte à puce est composée d'une carte en plastique de 5,4 cm de haut par 8,6 cm de long dans laquelle vient se loger une puce, ou "micromodule" composé de 8 contacts.

Contrairement aux cartes à puces de type "carte bleue" et autres cartes plus sécurisées, où la puce est en fait un véritable mirco-processeur, les cartes téléphoniques utilisent une simple mémoire, une EEPROM, (Une ancêtre de la mémoire flash contenue dans les clefs USB) qui est capable de stocker 256 bits de données, sans alimentation, pendant au moins 10 ans (garantie constructeur).

Brochage

Vous l'avez sans doute remarqué, depuis maintenant quelques années, la puce se trouvant initialement en haut à gauche de la carte à été ramené au milieu, de plus, la puce semble "inversée". Cette première disposition, hérité des premières cartes à puces françaises est appelée position AFNOR, elle à été progressivement remplacé par la position ISO.

La photo ci-dessous montre les deux types de cartes, ainsi que le nom des brochages :

Brochage des cartes à puces

Bon, voyons maintenant à quoi correspondent ces broches, vous allez voir, il n'y a rien de compliqué!

N'oubliez pas que je vous ais dit que cette puce est en fait une mémoire, et une mémoire, ça à besoin d'une alimentation pour lire et écrire des données dedans.

C'est le rôle de la broche Vcc : On alimente la puce en 5 V continus entre Vcc et la masse (0 v).

Vpp est une tension servant uniquement en mode "programmation" de la mémoire, elle est de 21 V dans ce cas là, autrement, elle est de 5 V. Les nouvelles générations de télécartes T2G, (Télécartes de 2eme Génération) ne nécessite plus cette tension pour pouvoir y changer des données, cette broche est donc inutilisée et sera supprimée.

La broche E / S est le bus de donnée de la mémoire, en fait, à un fil, c'est donc une mémoire de type série, c'est à dire que l'on va utiliser un compteur pour incrémenter l'adresse dans la mémoire (là, ou l'on veut lire ou écrire un bit) et ce bit sera appliqué à cette entrée / sortie (E / S).

Pour incrémenter notre compteur d'adresse, on utilise l'entrée CLK, l'horloge. Chaque front positif sur cette broche incrémentera le compteur d'adresse.

Il n'est pas possible de décrémenter ce compteur, donc de revenir en arrière dans la mémoire, par contre, on peut le remette à 0, grâce à la broche RAZ, (Remise A Zéro), ainsi,on revient sur le premier bit stocké en mémoire, et vous avez bien deviné, l'état de ce bit est présent sur la broche E / S.

Bien sûr, là il était question de lecture de la mémoire.

Pour choisir si l'on veut lire ou écrire dans la mémoire, il faut appliquer un état logique sur l'entrée R/W.

+ 5 V sur cette broche place la mémoire en écriture (Elle recopie l'état logique présent sur la passe E/S)

Attention, c'est là que des protections rentrent en jeu :

- Les 96 premiers bits de la mémoire (qui en compte 256) sont protégés en écriture, ils contiennent des informations sur la carte, j'y reviendrais...

- Il est théoriquement impossible de faire passer un bit de l'état "1" à "0". Par contre, l'inverse est possible, et c'est cette opération qui décompte les unités de téléphone. Donc, on peut décharger une télécarte neuve !

0 V sur cette broche place la mémoire en lecture (E/S passe à 5 V si le bit à l'adresse actuelle est à "1", 0 V si il est à 0)

La broche fusible : En y appliquant une tension, un fusible interne est grillé. La présence de ce fusible, en bon état, permettait de pouvoir écrire dans les 96 premiers bits de la mémoire. Ce fusible est grillé en usine: Les 96 premiers bits de la carte sont donc exclusivement en lecture seule.

La lecture de la mémoire

On peut incrémenter le compteur d'adresse et le remettre à 0.

Les données sont disponibles sur la broche E / S.

- **Vpp : (5 V)**
- **E / S : Sortie données**
- **Fusible : Non Connecté**

R/W	RAZ	CLK	Instruction
0	0	front montant	Reset du compteur d'@
0	1	front montant	Compteur d'@ + 1

L'écriture dans la mémoire

On peut incrémenter le compteur d'adresse et le remettre à 0.

Les données sont introduites en série sur la broche E / S.

Si R/W est à "1" le bit présent est lu.

- **Vpp : (21 V)**
- **E / S : Entrée données**
- **Fusible : Non Connecté**

R/W	RAZ	CLK	Instruction
0	0	front montant	Reset du compteur d'@
0	1	front montant	Compteur d'@ + 1
1	1	impulsion positive	Progr (0 => 1)

La structure de la mémoire d'une télécarte

Voici le contenu de la mémoire d'une télécarte 50 unités neuve :

Les 256 bits ont été regroupés par paquets de 4,(des quartets) donc, pour plus de lisibilité.

Les 96 premiers bits interdits en écriture sont en gris foncés.

Les autres, en gris clair. C'est là que sont "stockés" les unités de tchatche !

1100	0011	0000	0101	0101	1001	0001	0100
1100	0011	0010	0010	1000	1000	0011	0011
1011	1111	1110	1110	0001	0000	0000	0110
1111	1111	0000	0000	0000	0000	0000	0000
0000	0000	0000	0000	0000	0000	0000	0000
0000	0000	0000	0000	0000	0000	0000	0000
0000	0000	0000	0000	0000	0000	0000	0000
0000	0000	0000	0000	0000	0000	0000	0000

Ces 96 premiers bits sont uniques à chaque carte, ils renferment un "message d'authenticité", un numéro de série, le nombre de tirages du dessin de la carte (je rappelle que chaque puce est unique), et la date de fabrication.

Voici ce que j'ai identifiés :

- Les bits 1 à 4 sont toujours à "1100" (?)
- Les bits 9 à 12 forment le "code application" de la carte. Ses valeurs vont de 03 à 06 hexadécimal. Mais il sera toujour superieur à 80 pour une autre application. En effet le bit 9 sera toujours programmé à 1 pour une carte à puce autre qu'une télécarte. (Ah ! cher France Télécom !) :o)
- Les bits 13 à 16 déterminent l'année 199X. Où X est donc codé sur 4 bits ! (Attention au bug !)

  0000 => 1990; 0001 => 1991; 0010 => 1992; 0011 => 1993... etc.

Nous voila donc avec un code propre à chaque carte, donc une potentielle clef unique pour une serrure codée, les cartes à puces étant normalement incopiables !

Les bits 96 à 256 sont affectés au comptage d'unités (bit à "0" = une unité, bit à "1" = pas d'unité), ce qui veut dire qu'une telle carte pourrait contenir 160 unités or, le maximum dans le commerce est de 120. Sur ces 160, on en grille 10 en usine pour tester la carte, il en reste donc 150, ensuite, les autres bits sont ignorés, car dans nos 96 premiers bits, est inscrit la capacité (commerciale) de la carte. Ainsi sur une carte à 5 unités il restera 160 - 10 - 5 = 145 bits qui resteront à "0" alors que la carte sera considerrée comme vide. En fait il en restera que 137 comme décrit plus loin !

Il est possible de programmer (mettre à "1") ces bits restants pour personnaliser sa carte !

Voici donc le contenu de notre télécarte mais "épuisée" :

En rouge, les modifications.

1100	0011	0000	0101	0101	1001	0001	0100
1100	0011	0010	0010	1000	1000	0011	0011
1011	1111	1110	1110	0001	0000	0000	0110
1111	1111	1111	1111	1111	1111	1111	1111
1111	1111	1111	1111	1111	1111	1111	0000
0000	0000	0000	0000	0000	0000	0000	0000
0000	0000	0000	0000	0000	0000	0000	0000
0000	0000	0000	0000	0000	0000	1111	1111

Notez que les 8 derniers bits passent à "1" quand la carte est épuisée.

Il reste bien 160 - 10 - 50 - (les 8 derniers bits mis à 1) = 92 bits à programmer.

Un lecteur de télécartes pour 3 Euros

Voici comment réaliser en 15 minutes un appareil qui vous permettra de lire le contenu d'une télécarte, que la puce soit en position ISO ou Afnor.

La lecture de la mémoire se fera en appuyant sur un bouton poussoir muni d'un système anti-rebond (le bouton poussoir génère des micro impulsions parasites pouvant êtres prises en compte par la télécarte) pour éviter de "sauter" des bits. La lecture des bits se fera grâce à une led piloté par un transistor, car la carte à puce n'a pas assez de puissance pour la commander directement. L'archivage se fera grâce à deux dispositifs dont la fiabilité n'est plus à démontrer... quoi que... à savoir la feuille de papier et le crayon. Rassurez vous, ces 2 composants se trouvent assez facilement dans diverses boutiques spécialisées.

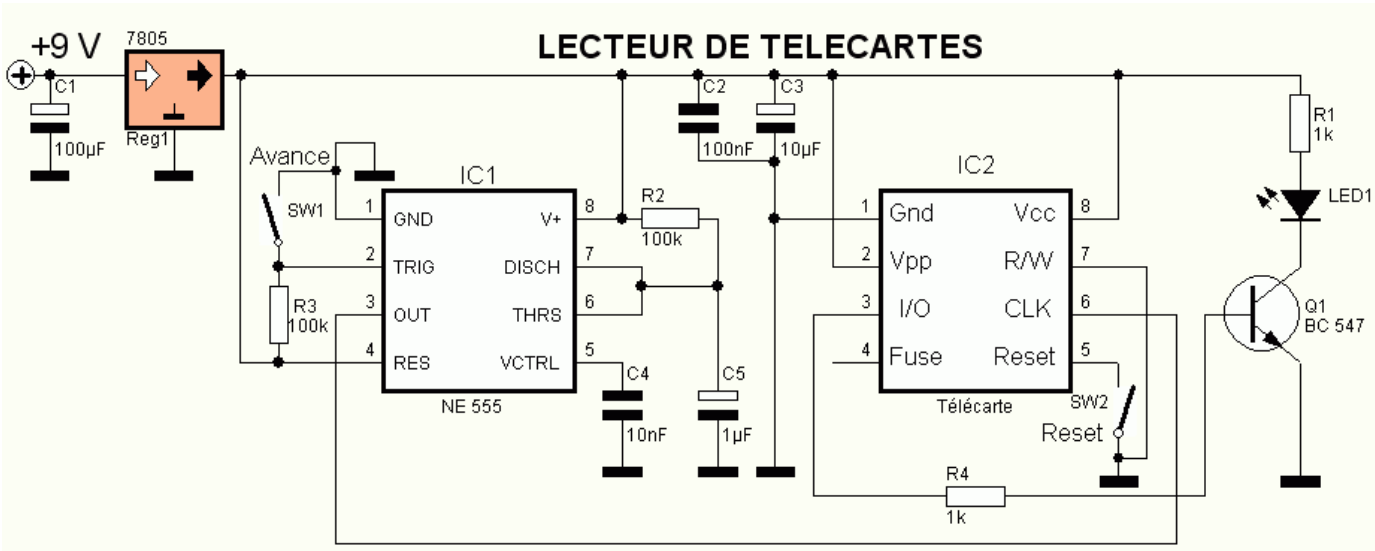

Schéma d'un lecteur de télécartes rustique

Mode d'emploi :

Appuyez sur RESET pour mettre le pointeur en début de mémoire (bit 0).

Appuyez sur AVANCER pour incrémenter le pointeur d'adresse et ainsi parcourir la mémoire de la carte.

Notez et comparez les images mémoire, vous pourrez même savoir combien d'unités il reste dans la télécarte !

Note :

- Ce montage n'altère en rien le contenu et le fonctionnement de la carte.

- Il est possible que vous tombiez sur une télécarte de 2eme génération, auquel cas le montage ne marchera pas.

http://Matthieu.weber.free.fr