Radio Frequency Insecure Devices ?

SCRT
Information Security
Switzerland

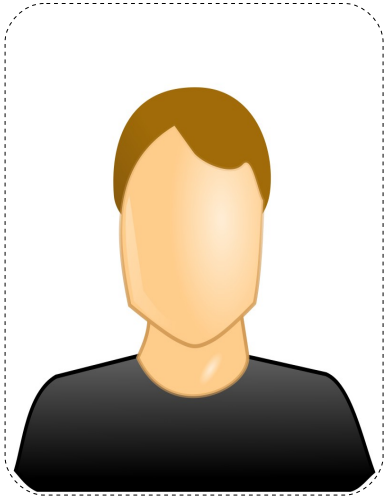
http://www.scrt.ch

Table des Matières

- Introduction
- Systèmes RFID
- Étude de cas: EM410X
  - Applications « typiques »
  - Modèle de sécurité
  - Attaques
- Démonstration(s)
- Conclusions

Introduction

Conférencier



Nom
Alves Domingues
Prénom
Sergio
Profession
Ingénieur Sécurité
Société
SCRT
Contact
sergio (a) scrt.ch

```
SCRT<SUISSE<<<<<<<<<<<<<<<<<<<<<<<<<<<<
ALVES<DOMINGUES<<SERGIO<<<<<<<<<<<<<<<
GLOBAL<SECURITY<DAYS<<2010<<FRANCE<<<<<
```

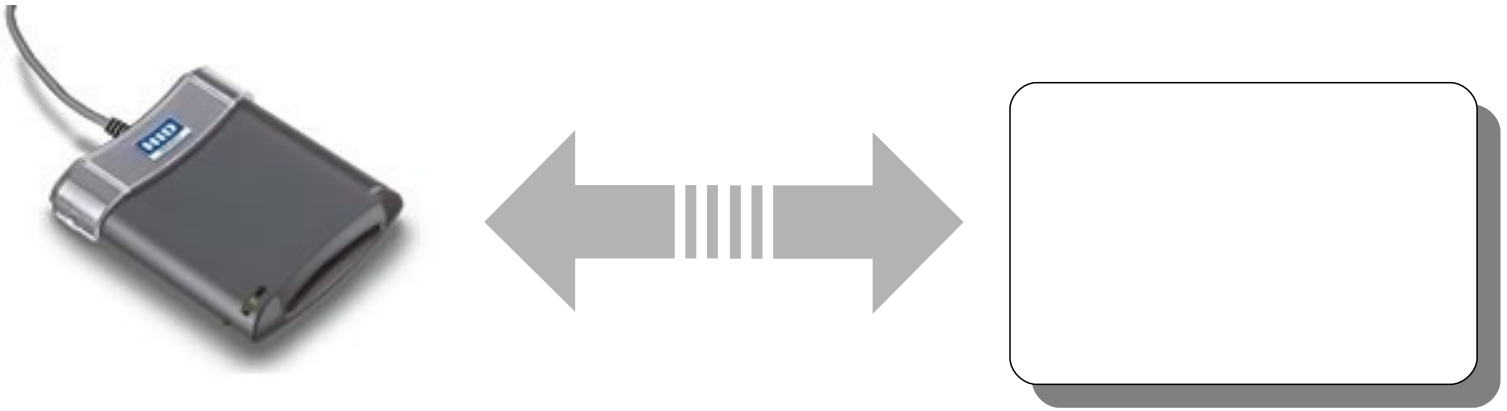
Présentation

- Ce que nous allons aborder
  - Brève présentation des systèmes RFID
  - Quelques exemples d'utilisations
  - Étude de cas d'une utilisation ... à éviter !
  - Démonstration(s)
- Ce que nous n'allons pas aborder
  - Vulnérabilités des systèmes RFID eux-mêmes
  - Mais plutôt, vulnérabilités induites par les choix de leurs applications

Systèmes RFID

Systèmes RFID

- Radio Frequency IDentification
  - Lecteur
  - Transpondeur (« tag ») passif
  - Alimentation par couplage EM
  - Communication par ondes



Systèmes RFID

- Différentes fréquences
  - 125 kHz – 134 kHz (LF)
  - 13.56 MHz (HF)
  - 900 MHz (UHF)
- Nombreux standards
  - ISO14443
  - ISO15693
  - ISO 11784/11785
  - etc ... (plusieurs dizaines) ...

Systèmes RFID

- Différents types
  - Lecture seule
  - Lecture/écriture
- Différentes capacités
  - Stockage seul
  - Capacités de calcul et traitement
  - Fonctions cryptographiques

} Similaires aux cartes à puce « standard »

Applications

- De nombreux systèmes RFID différents impliquent de nombreuses applications possibles ..
  - Tracking
  - Identification
  - Contrôle d'accès
  - Abonnements (transports)
  - Paiement (cartes de crédit)
  - Passeports électroniques

Applications

- ... toutefois, tous les systèmes ne sont pas adaptés à toutes les applications
  - Capacités et limitations différentes
  - Modèles de sécurité différents
  - Niveaux de robustesse différents
- Parfois les systèmes s'avèrent vulnérables
- Souvent, ils sont simplement mal utilisés !

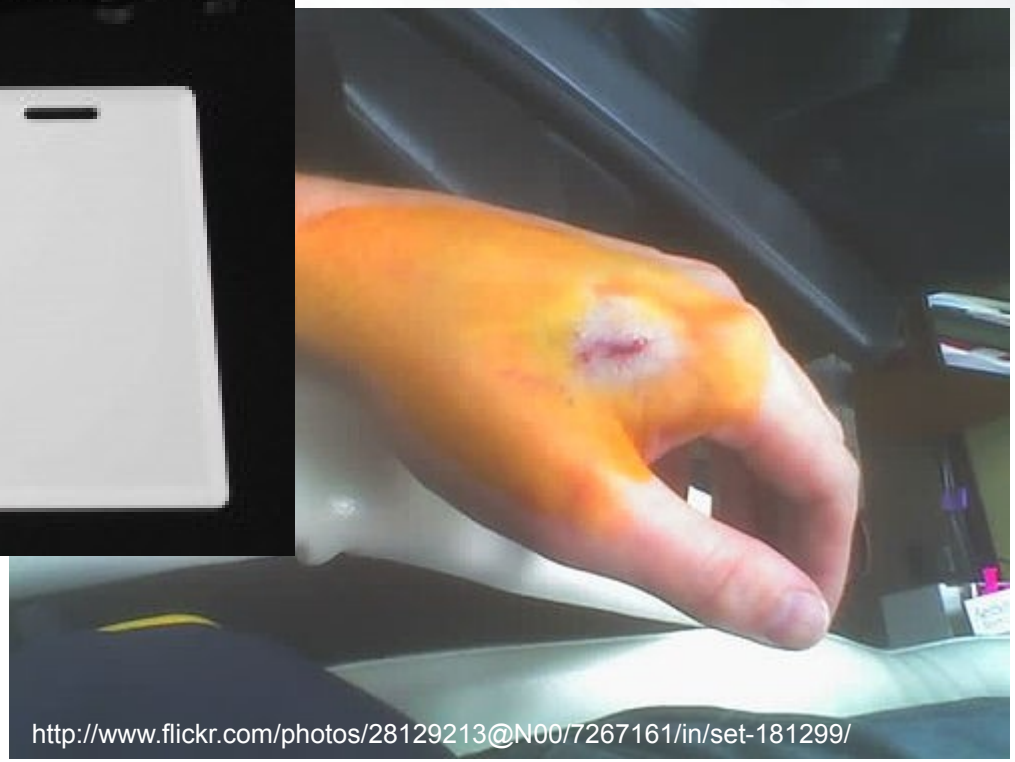
Étude de cas: EM410X

EM410X

- Produit par EM MICROELECTRONIC – Marin SA
- Basse fréquence (125 KHz)
- 64 bits en lecture seule (40 bits « utiles »)
  - Identifiant unique, gravé à la fabrication
- Récemment (~2008) remplacés par EM4200 ...
  - Technologie analogue
  - Rétro-compatible
- ... mais toujours largement utilisé

EM410X

- Nombreux formats différents



http://www.flickr.com/photos/28129213@N00/7267161/in/set-181299/

Applications

- Applications suggérées (fiche technique)

Read Only Contactless Identification Device

Description

The EM4102 (previously named H4102) is a CMOS integrated circuit for use in electronic Read Only RF Transponders. The circuit is powered by an external coil placed in an electromagnetic field, and gets its master clock from the same field via one of the coil terminals. By turning on and off the modulation current, the chip will send back the 64 bits of information contained in a factor programmed memory array.

The programming of the chip is performed by laser fusing of polysilicon links in order to store a unique code on each chip.

The EM4102 has several metal options which are used to define the code type and data rate. Data rates of 64, 32 and 16 periods of carrier frequency per data bit are available. Data can be coded as Manchester, Biphase or PSK.

Due to low power consumption of the logic core, no supply buffer capacitor is required. Only an external coil is needed to obtain the chip function. A parallel resonance capacitor of 78 pF is also integrated.

Features

- 64 bit memory array laser programmable
- Several options of data rate and coding available
- On chip resonance capacitor
- On chip supply buffer capacitor
- On chip voltage limiter
- Full wave rectifier on chip
- Large modulation depth due to a low impedance modulation device
- Operating frequency 100 - 150 kHz
- Very small chip size convenient for implantation
- Very low power consumption

Applications

- Animal implantable transponder
- Animal ear tag
- Industrial transponder

Applications

- Applications typiques

Chip Parameters

IC Type	EM4100/4102
Frequency	125KHz
Mode	R/O
Protocol	/
Memory	64 bit
Operating Distance	Up to 50mm (depending on antenna geometry)
Anticollision	no
Applications	Access control systems, Time attendance systems, Loyalty program, Mass transportation ticketing, Staff identification

Customizations

- Print: offset, silkscreen, thermal printing
- Serial number printing: thermal or inkjet format
- Signature panel, Scratch off, Hologram, Laser film
- Magnetic stripe: LoCo 300 Oe, HiCo 2750 Oe or 4000 Oe
- Embossing, Hot-stamping, Hole punching
- Encoding, UV printing, Color photo printing

To Know More >>

Ordering Information

Delivery Term

- By express, by air or by sea
- <10k pcs: within 15 working days
- ≥10k pcs: to be negotiated

Payment term

- TT in advance or L/C
- Others on request

Sécurité

- Modèle de Sécurité
  - Lecture seule
  - Identifiant « unique »
- Modèles d'attaque
  - Collisions ← Trouver deux transpondeurs avec le même identifiant
  - Clonage ← « Copier » un transpondeur
  - Émulation ← « Fabriquer » un transpondeur

Collisions

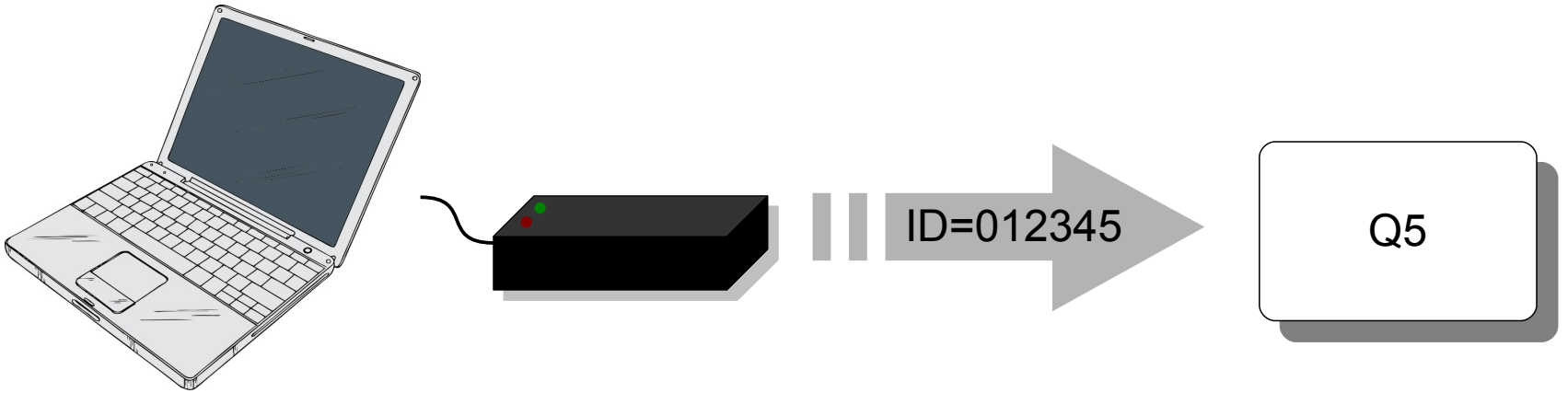
- Problème?
  - 2 transpondeurs avec le même identifiant
- Identifiant sur 40 bits
  - 2^{40} = 1 099 511 627 776 possibilités
- Aspect dépendant uniquement du fabriquant
- Difficile à exploiter
  - Trouver les transpondeurs identiques

Clonage

- Problème ?
  - Copier l'ID d'un transpondeur sur un autre
- EM410X: transpondeurs en lecture seule
  - Oui ... mais!
- Il existe des transpondeurs capables de « se faire passer » pour des EM410X!
  - Hitag2
  - Q5
  - ... autres ...

Clonage

- Hitag2, Q5, ...
  - Transpondeurs paramétrables
  - Modulation, identifiant, etc.
  - Compatibles avec les lecteurs EM410X (lecture)
  - Nécessitent un lecteur spécifique (écriture)



Clonage

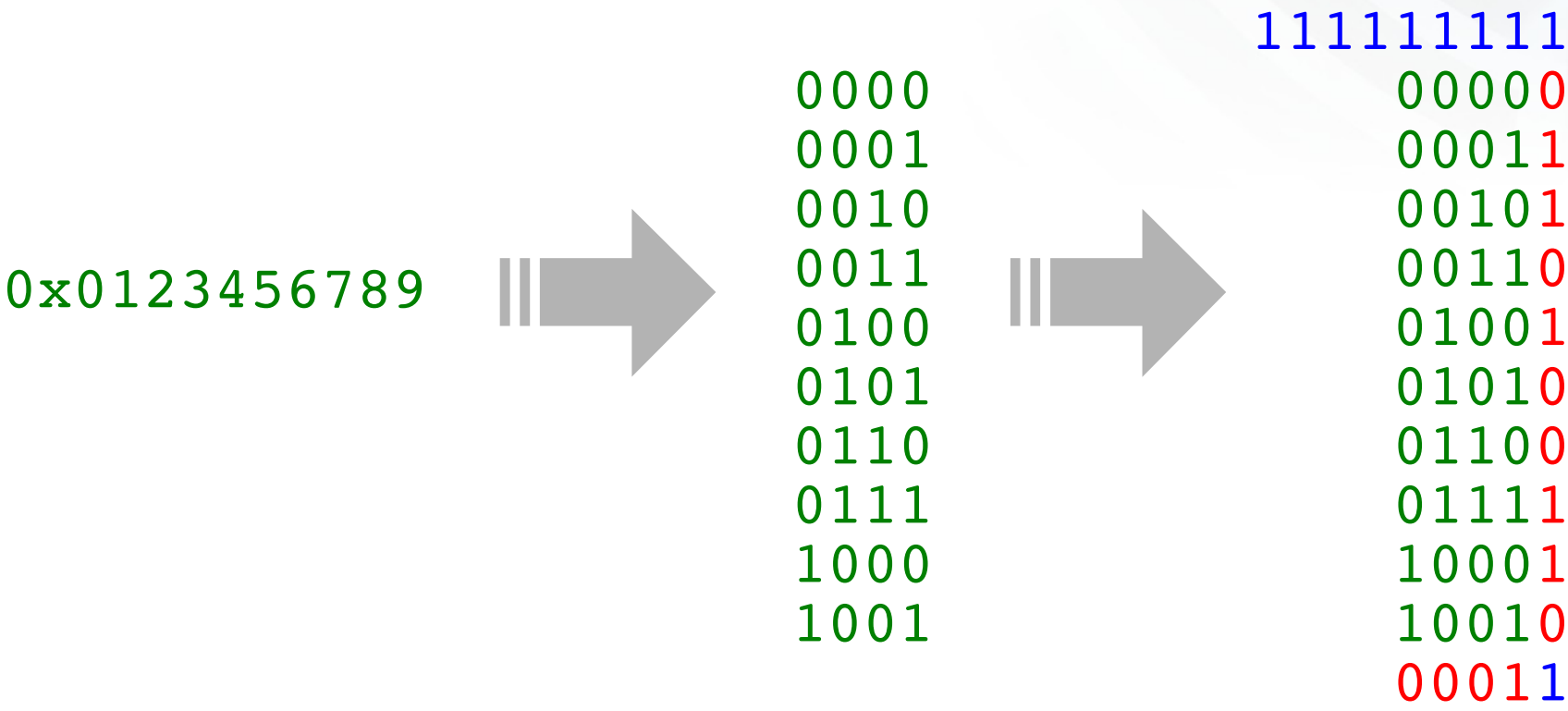
- Systèmes « autonomes » de copie
  - Peu chères (~ 60$)
  - Autonomes (pas besoin d'ordinateur)
  - Très simples d'utilisation
  - Utilisent des transpondeurs spéciaux (similaires aux Q5 ou Hitag2)
  - Nécessitent l'accès au transpondeur original

Émulation

- Problème ?
  - Fabriquer un transpondeur valide
- Il est relativement simple de construire un circuit (transpondeur) « compatible » EM410X
  - Basse fréquence
  - Fonctionnement très simple
- Peu de connaissances préalables nécessaires
  - Goooooooogle !
  - Différents projets existants (et documentés)

Émulation

- Encodage de l'identifiant
  - Documenté dans la fiche technique de EM4102



Émulation

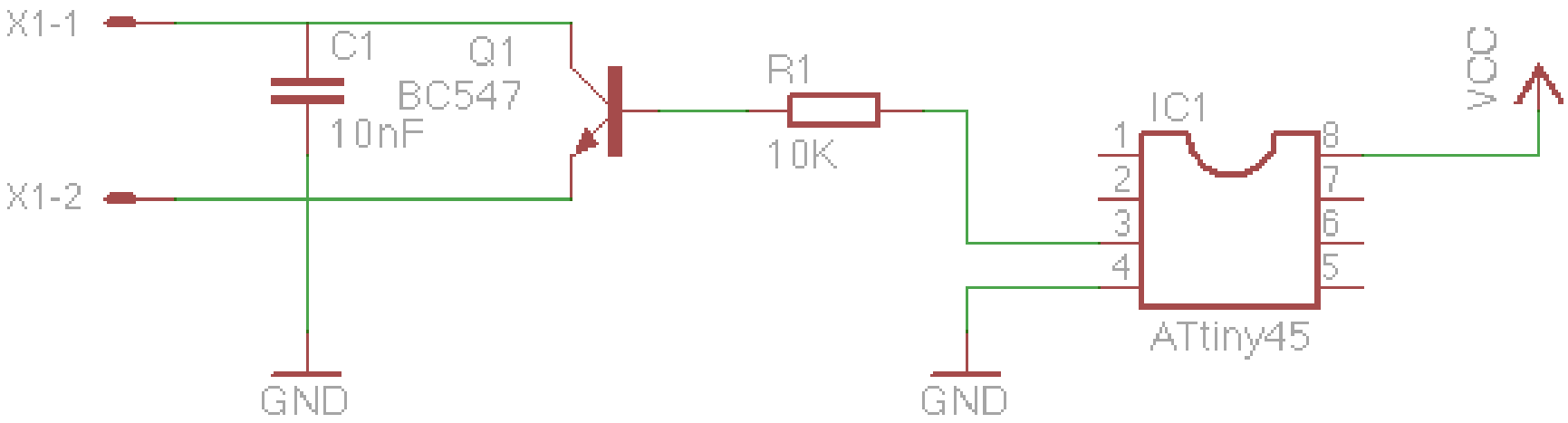
- Transmission des données
  - Documentée dans la fiche technique
  - Encodage Manchester
  - RF/64 (autres possibles)
- Alimentation et synchronisation
  - Passive, par couplage EM ...
  - ... mais des techniques « empiriques » bien plus faciles à implémenter fonctionnent très bien !

Émulation

- Matériel utilisé
  - 1 microcontrôleur Atmel ATtiny45
  - 1 résistance 10K
  - 1 transistor NPN (BC547)
  - 1 condensateur 10nF
  - du fil de cuivre émaillé (0.25mm de diamètre)
- Quelques € au détail

Émulation

- Circuit
  - Très simple !
  - Alimentation par régulateur (LM7805) ou ...
  - ... simplement 3 piles AAA!



Émulation

- Transmission RF
  - Circuit résonnant (LC)
  - Piloté par un transistor NPN
  - Choisissons C = 10nF, donc L = 160 uH

$$f_0 = \frac{1}{2\pi\sqrt{LC}}$$

Émulation

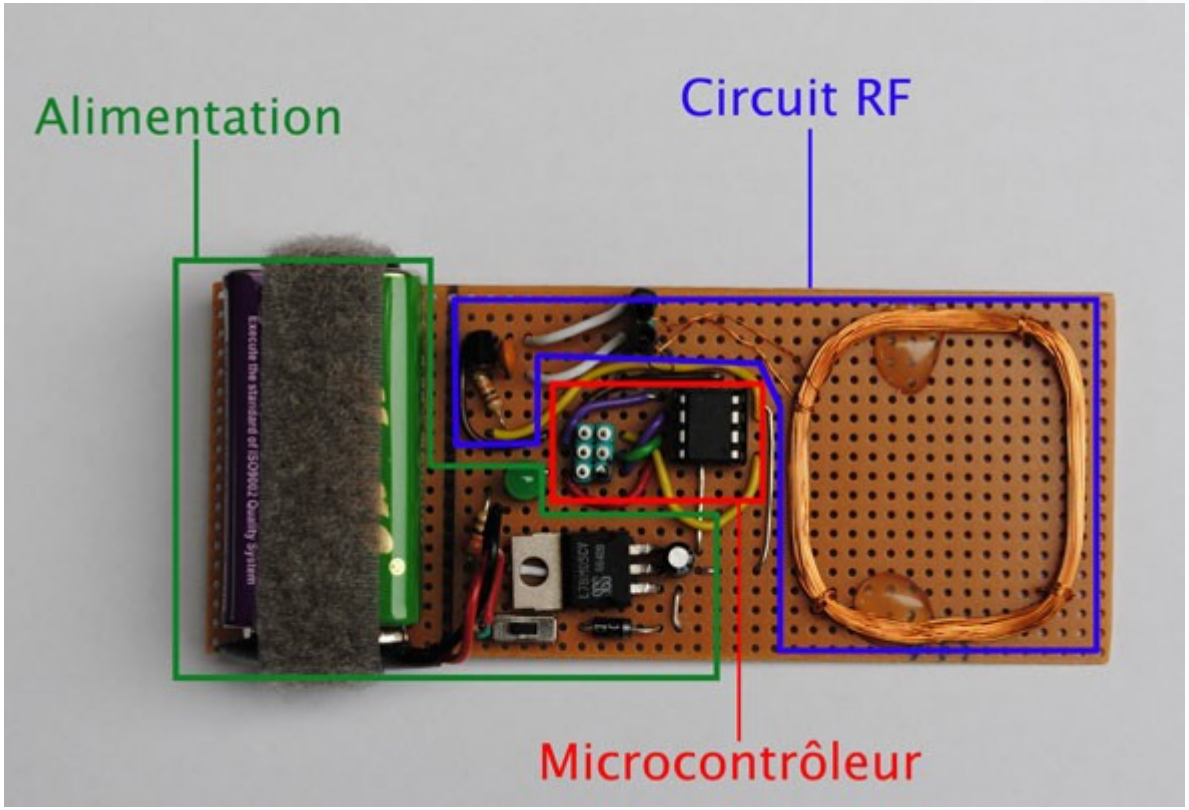
- Antenne
  - Le L dans LC :-)
  - Une « simple » bobine de fil
  - Éventuellement possible à trouver toute prête
  - Mais probablement plus simple à fabriquer
  - d = 0.25mm, D = 40mm, L = 160 uH => N = 43

$$L = \frac{\mu \cdot N^{(1.9)} \cdot D}{2} \cdot \ln\left(\frac{D}{d}\right)$$

où $\mu = 4 \cdot \pi \cdot 10^{-7}$

Émulation

- Réalisation
  - Firmware disponible sur http://blog.scrt.ch



Démonstration(s)

Conclusions

Conclusions

- Large palette de systèmes RFID disponibles
- Très répandus depuis quelques années
- Certains sont très robustes ...
  - Cartes à puce avec interface RFID
  - Mécanismes de sécurité
- ... mais d'autres le sont beaucoup moins
  - Systèmes simples tels que EM410X
  - Pas de mécanisme de sécurité prévus

Conclusions

- Il faut être conscient des limitation de chacun
  - RFID != RFID
  - Applications diverses et non équivalentes
- Mauvais choix = fausse impression de sécurité
  - Éventuellement, moins robustes que le système qu'ils remplacent
  - Exemple: EM410X | clé « standard »

http://blog.scrt.ch

Références

- http://www.rfidiot.org/
- http://www.alexanderguthmann.de/en/emulator.html
- http://en.wikipedia.org/wiki/Radio-frequency_identification
- http://www.emmicroelectronic.com/webfiles/Product/RFID/AN/AN411.pdf
- http://fr.wikipedia.org/wiki/Circuit_LC
- http://en.wikipedia.org/wiki/Manchester_code