RÉPUBLIQUE
FRANÇAISE
Liberté
Égalité
Fraternité

Communications à grande distance avec un lecteur ISO 14443

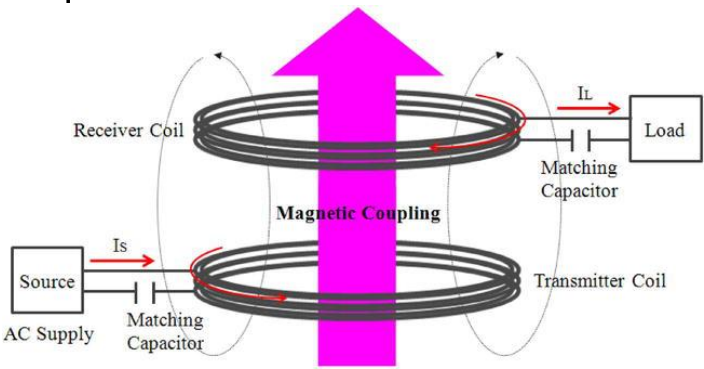
Pierre-Michel Ricordel, Yoan Burny
ANSSI/SDE/ST/LSF

Discussion d'origine

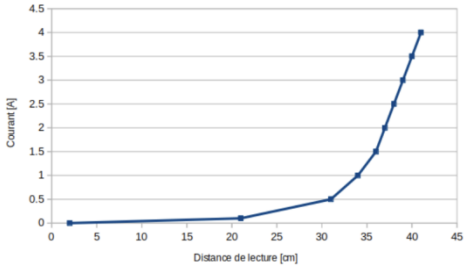
- Q: Nous allons déployer des lecteurs de cartes sans contact dans un environnement sensible pour notre nouveau système d'impression sécurisé.
- R: Non, vous ne pouvez pas déployer un système sans fil dans un environnement sensible
- Q: Mais c'est une interface de proximité qui n'a que 10 cm de portée, comment pouvez-vous le justifier ?
- R: …

La technologie des cartes sans contact

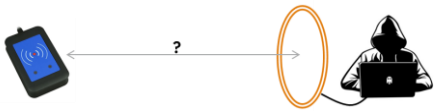
- Le système déployé est un système ISO 14443
  - Standard utilisé pour le paiement, les transports, le contrôle d'accès, le NFC…
  - Le lecteur génère un champ magnétique très intense à 13,56 MHz
    - La carte est alimentée par le champ magnétique
    - Le lecteur envoie des messages en modulant le champ
    - La carte répond en modulant sa consommation
  - Vitesse de communication de base : 106 kbit/s
  - Portée typique : 10 cm
  - Propagation du champ à 13,56 MHz :
    - Longueur d'onde : 22,1 m
    - Zone de champ proche à moins de 3,5 m
      - Décroissance du champ en $1/R^3$



Etat de l'art



- Lecture d'une carte à distance
  - Physiquement très difficile : 27 cm
- Interception des communications à distance
  - Messages du lecteur : ~10 m
  - Messages de la carte : ~1 m
- Attaque par relais
  - Attaque en deux parties proches, sans limite de distance
- Communication à distance avec un lecteur
  - Scénario rarement envisagé



Risques d'une communication à grande distance avec un lecteur

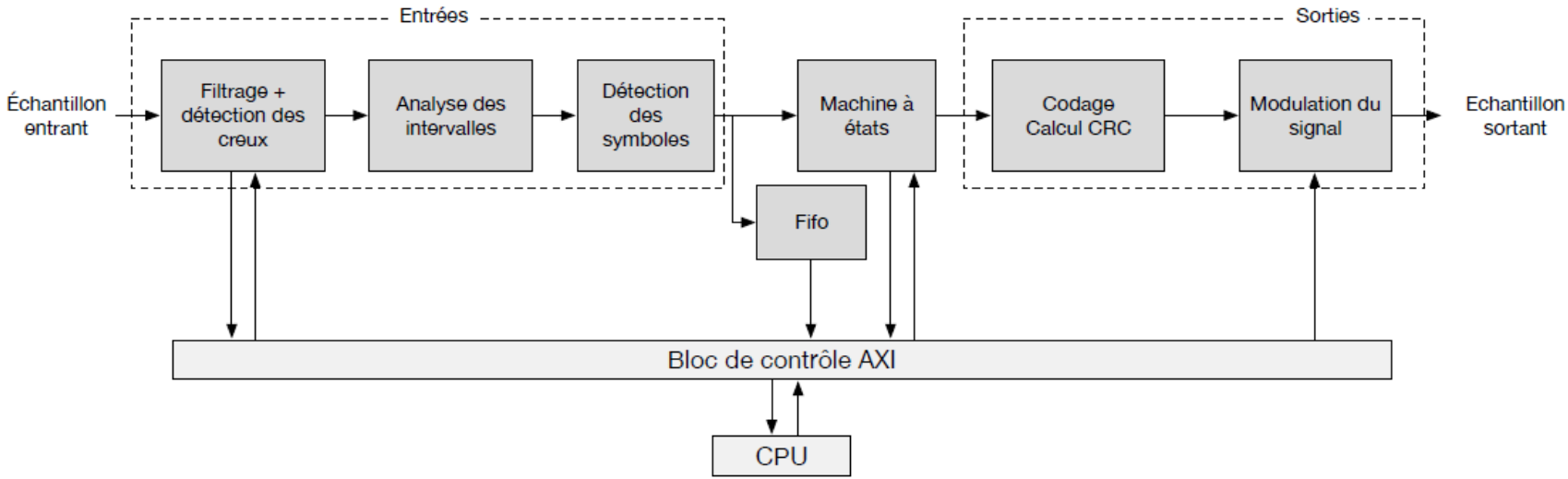
- Les circonstances sont favorables
  - Le lecteur émet fort et peut être reçu d'assez loin
  - L'attaquant peut émettre un signal fort qui va interférer avec le champ du lecteur pour lui donner l'illusion d'un signal de conso
- Différentes attaques peuvent être envisagées sur le lecteur
  - Reconfiguration ou mise à jour du firmware
  - Exploitation de vulnérabilités
  - Injection de données corrompues qui sont interprétées par les systèmes sous-jacents

Réalisation d’un démonstrateur

- Besoin d’un émulateur de carte avec des E/S analogiques 50 Ohm large bande
- Difficulté : le protocole ISO 14443 requiert un temps de réponse très court et très précis (~90µs)
- Solution : implémentation du protocole en VHDL, sur le FPGA de l’ADALM2000

Analog Devices ADALM2000 :
-Xilinx Zynq7000 (FPGA+ 2x ARM Cortex A9)
-2x CAN 100ME/s, 2x CNA 150ME/s
-Buildroot Linux
-Faible coût : 220€

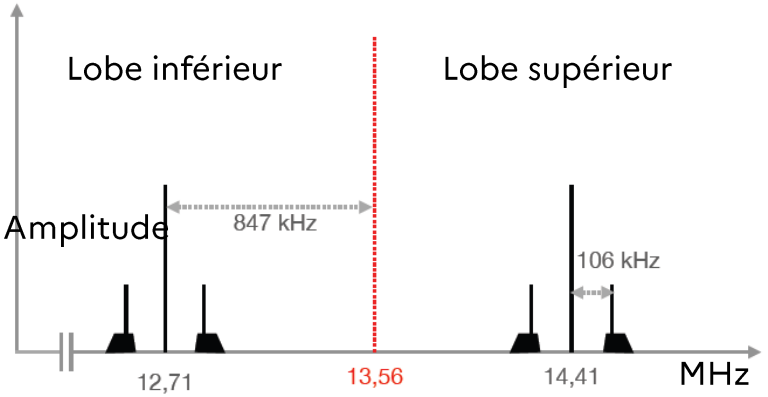
Implémentation VHDL



Choix de conception et modulation de charge active

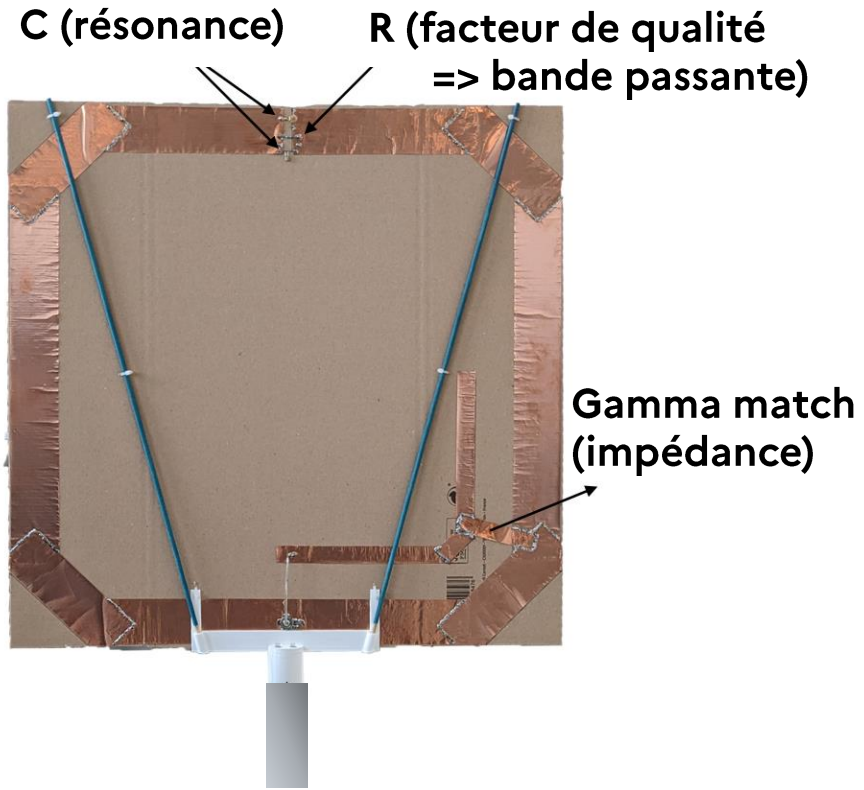
- Les signaux sont traités en bande de base
- L'émulateur et le lecteur ne sont pas synchrones
- La modulation de charge active se fait en ne transmettant que le lobe supérieur de la sous-porteuse
  - Elimine les problèmes de battement du signal
  - Réduit la bande passante du signal, ce qui permet d'optimiser l'antenne
  - L'antenne des lecteurs est toujours plus sensible aux fréquences supérieures (compensation de l'influence de l'inductance mutuelle en présence d'une carte)

La modulation de charge utilise une sous-porteuse à 847 kHz

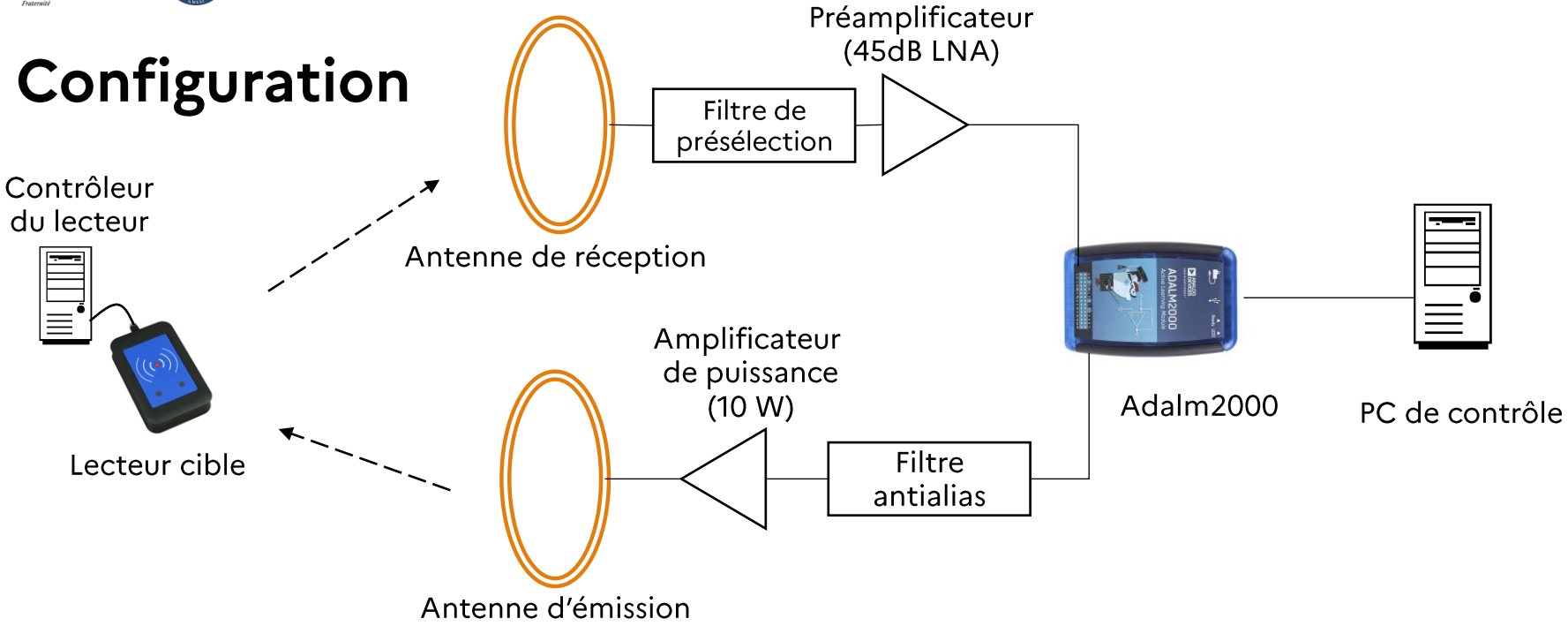


Conception d'antennes

- Antennes boucle résonantes
  - 58 cm x 58 cm
- Résonance optimisée
  - 13.56 MHz pour le RX
  - 14.40 MHz pour le TX
- Facteur de qualité optimisé
  - Bande passante = 200kHz



Configuration

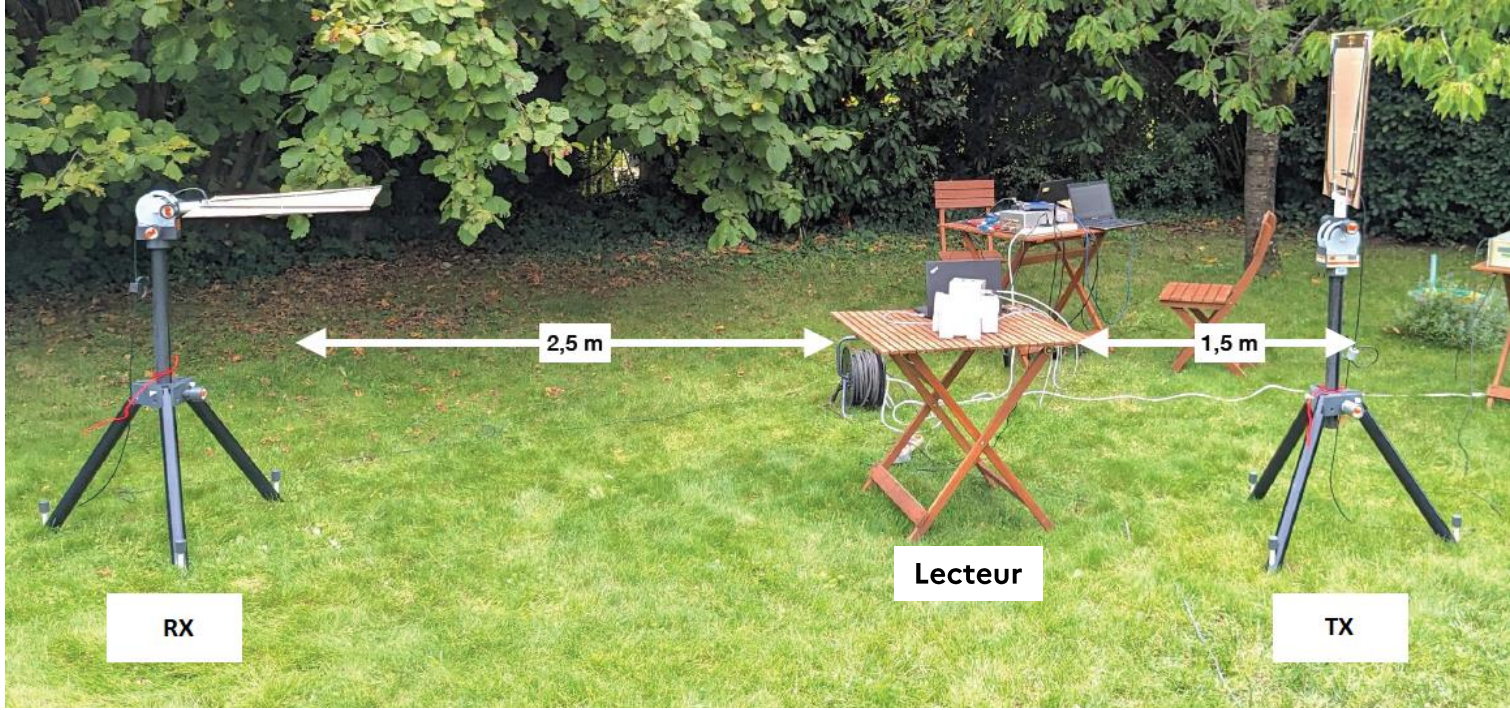


- Les antennes doivent être éloignées pour éviter d'endommager le préamplificateur avec les signaux de l'amplificateur

Résultats
Mode rayonné

- Au labo (murs métalliques et présence d'autres lecteurs)
  - Réception uniquement : 1.5 m (trop de signaux parasites ambiants)
  - Emission uniquement : 3.5 m (les murs aident à concentrer le champ)
- Pièce trop exigüe et trop de facteurs de perturbation…

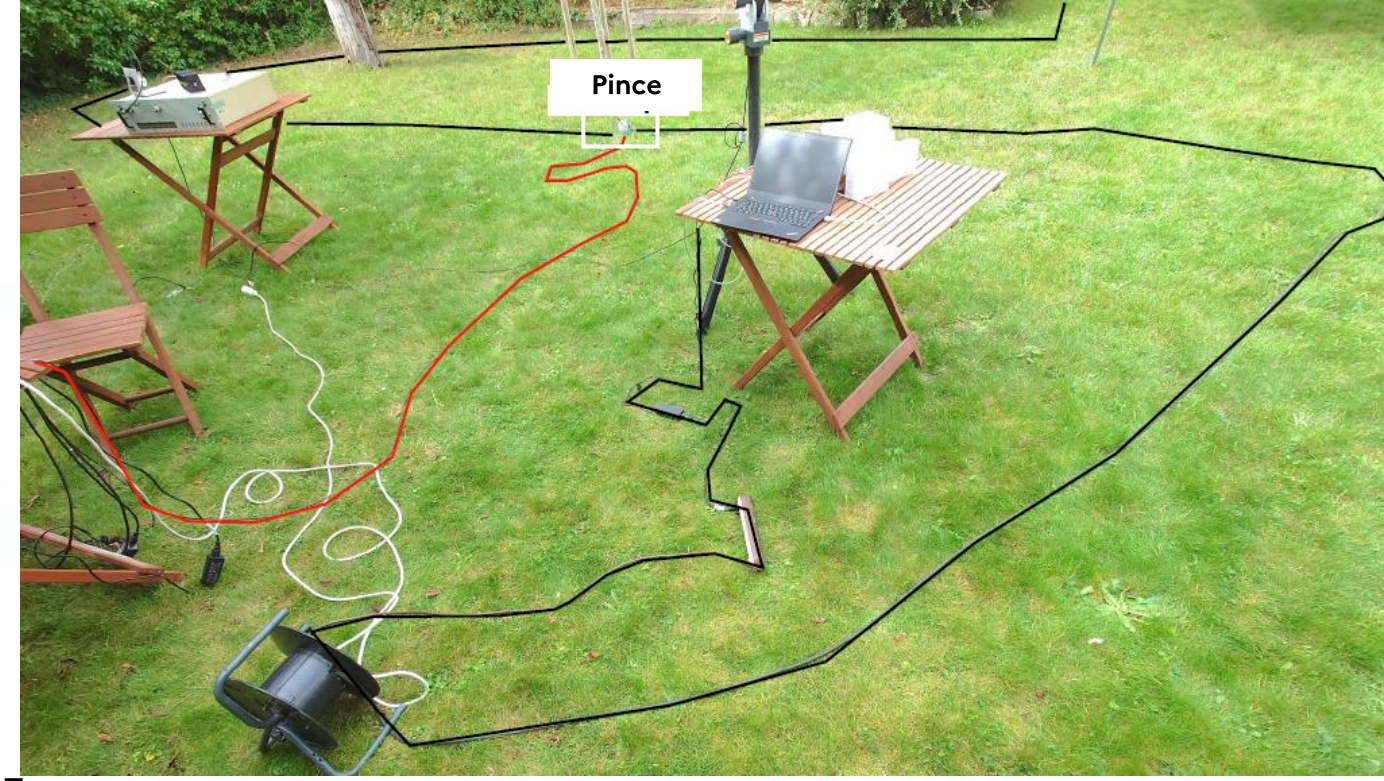
Résultats
Mode rayonné



- A la recherche d'espace libre… dans le jardin
  - Réception: 2.5 m
  - Emission: 1.5 m

Résultats
Mode conduit

Pince de couplage



- En extérieur:
  - Réception seulement : 17 m
  - Emission seulement : 6 m
- Beaucoup de couplages parasites sur les câbles environnants
- En intérieur c'est encore plus imprévisible

Conclusion

- Nous avons démontré la faisabilité de la communication avec un lecteur ISO 14443 à plusieurs mètres de distance
  - Dans les études de risque, les lecteurs ISO 14443 doivent être considérés comme des interfaces capables de communiquer à grande distance
- Cette étude a été faite dans une durée très limitée :
  - Nous avons développé la solution la plus simple possible
  - La majorité du temps a été dédiée au développement du code VHDL du FPGA
  - Peu de temps restait pour les expérimentations
- En conséquence, les résultats que nous avons obtenus sont probablement améliorable avec un effort plus conséquent
- Beaucoup plus de détails sont dans l'article publié sur le site du SSTIC