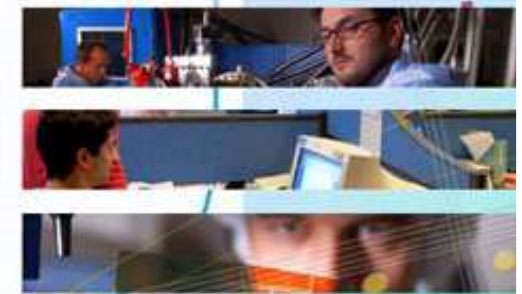


micro and nanoelectronics
microsystems
ambient intelligence
image chain
biology and health



The NFC noisy phone

O. SAVRY



cea

leti

Scenario

- **Business cards sharing**
- Peer to peer
- The best place to store business cards data : **the mobile phone**
- The data exchange should be protected
- Protection against eavesdropping on the communication

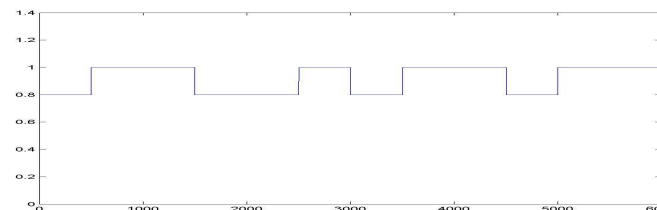
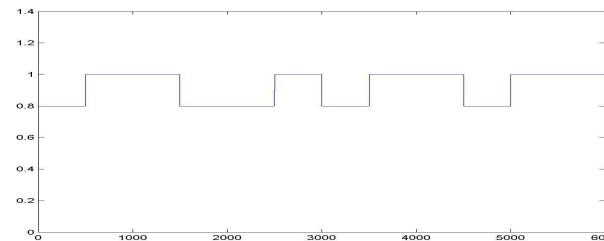
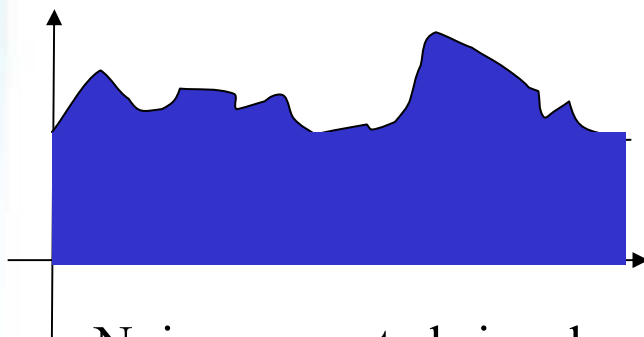
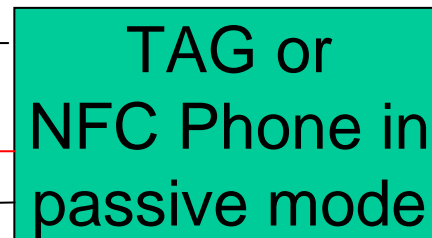
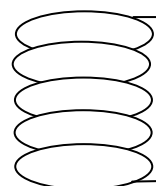
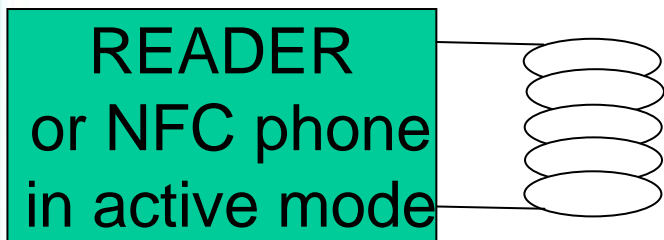
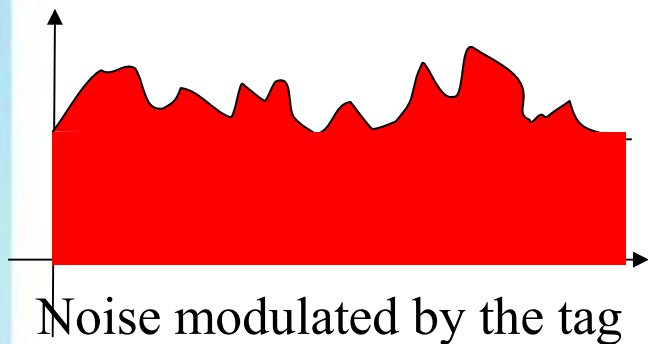


Solutions: encryption

- Symmetric/asymmetric cryptographic algorithm
- Expensive in term of computing ressources
- Time consuming
- Contactless devices are limited in energy supply
- Problem of keys management : the users should share a secret ket (or a public key)
- Another secure channel is then required for private key
- Or a certification authority is required for the authentication of a public key
- We propose to solve these problems at the physical layer with a noisy NFC phone

The RFID Noisy Reader Principle

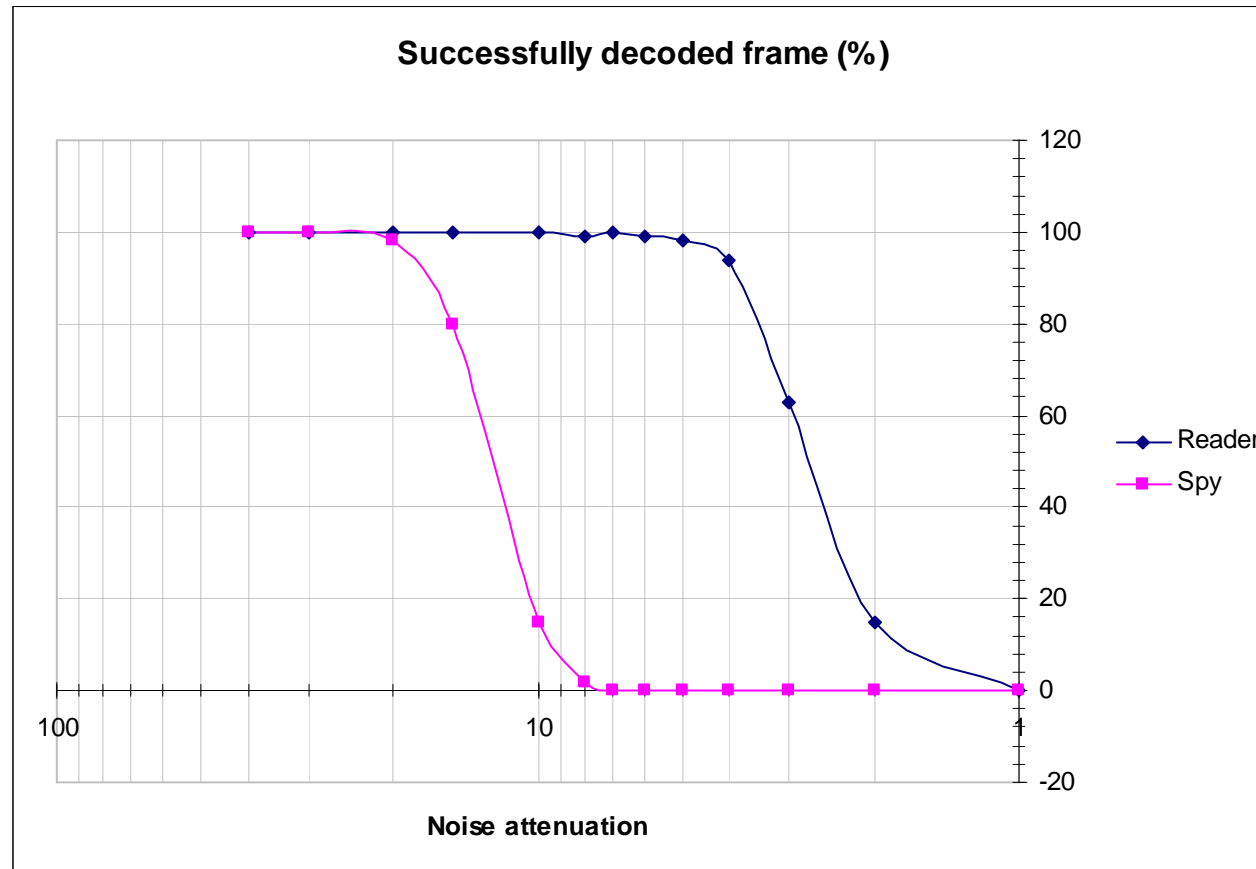
We get back the tag message



Noisy NFC phone Development

- Prototype of a Noisy RFID reader
- ISO 14443 type B
- Noise generation:
 - a PRNG generates 2 random numbers which modulate the subcarrier amplitude and phase
- Noise subtraction:
 - The noise generator emits noise via an antenna in null coupling with the reader antenna
 - ◆ The reader does not see the emitted noise while a spying probe in the field will see it
 - A correlation of the received signal with the noise enables to retrieve the tag message

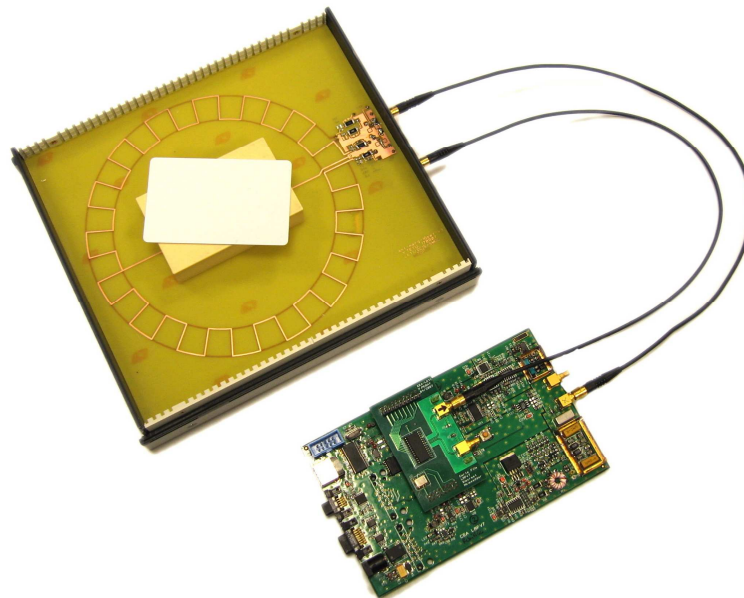
Performance measurement of the noisy reader



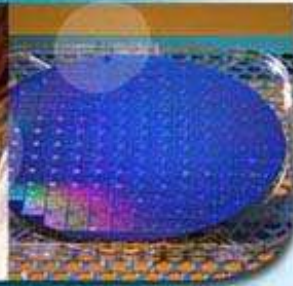
© CEA 2009. All rights reserved
 Any reproduction in whole or in part on any medium or use of the information contained herein
 is prohibited without the prior written consent of CEA.

Conclusion

- Performances
 - Null coupling + correlation required
 - A factor 1000 on the BER between the reader and a spying probe
 - Real time protection on the physical layer
 - The ISO standards are not modified

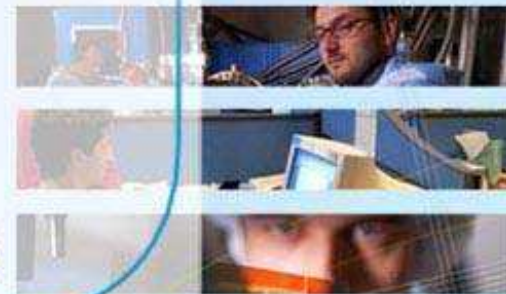


micro and nanoelectronics
microsystems
ambient intelligence
biology and health
image chain



Innovation for industry

Loyalty
Entrepreneurship
Team work
Loyalty Innovation
Entrepreneurship
Team work
Innovation



leti

MINATEC

INSTITUT
CARNOT
CEA LETI

cea