# 28ème entretiens Jacques Cartier
# Colloque “Objets Connectés”

# La sécurité des objets connectés
## *les défis matériels*

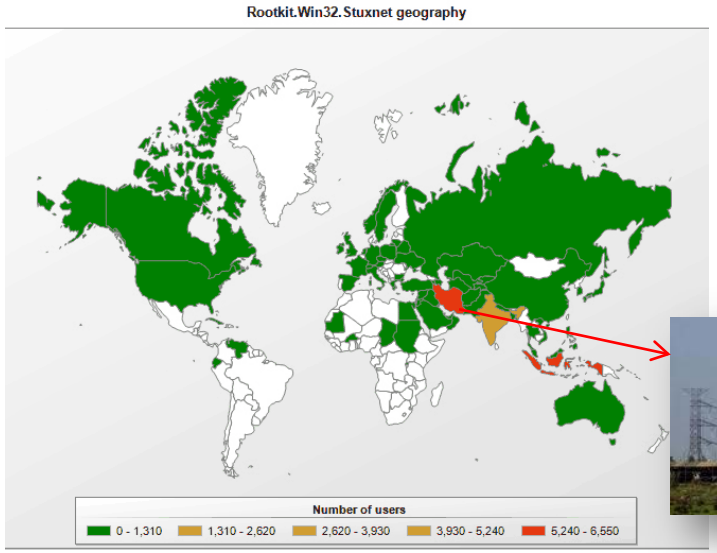
**Lilian Bossuet**
Laboratoire Hubert Curien, CNRS UMR 5516
Université Jean Monnet, Saint-Etienne, France


2 décembre 2015
Ecole Centrale de Lyon, Ecully, France

# Il était une fois *stuxnet*

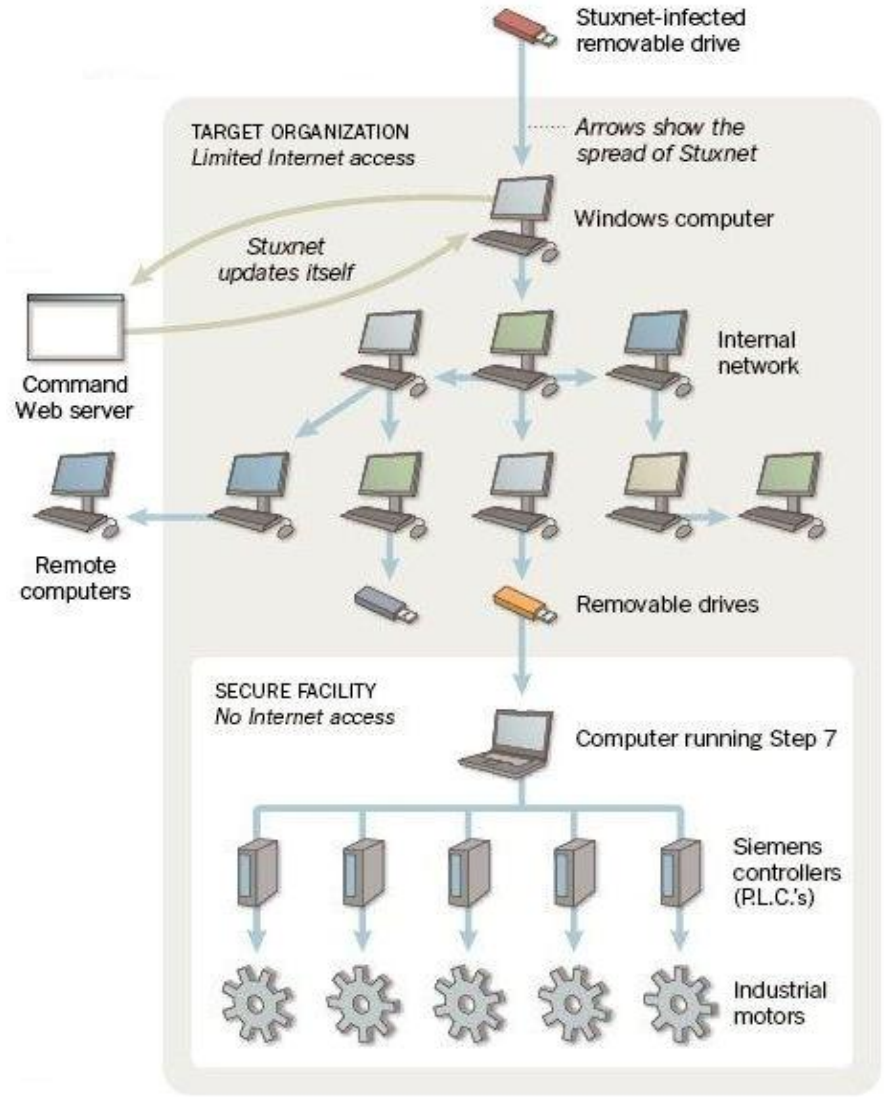
# Stuxnet

- Virus découvert en 2010 par VirusBlockAda (Biélorussie)
- Très haut niveau de développement
  - Plusieurs failles zéro-day de windows exploités
  - Plusieurs langages du C++ à l'assembleur
  - Quelle cible ?




# Diffusion de stuxnet

- Clé USB
- Microsoft Window
  - Accès internet et mise à jour automatique
- Système SCADA
  - Via un portable en zone sécurisée
- WinCC Siemens des automates programmables industriels
  - Modification des paramètres des API et des mesures capteurs (masque)

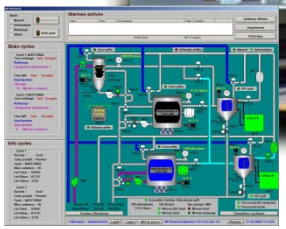


# Un monde d'objets connectés …











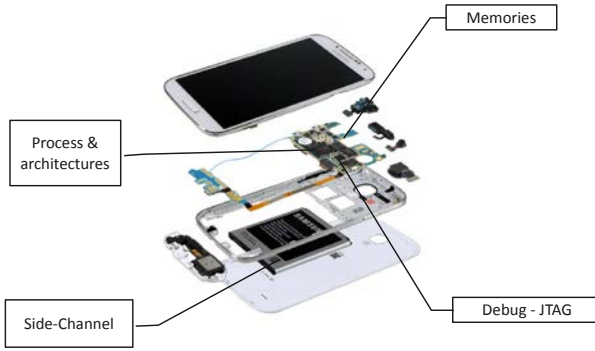


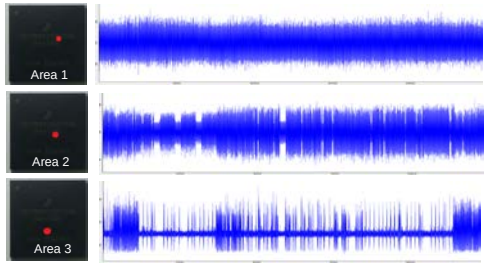

# Les besoins en sécurité matérielle

# Triptyque de la sécurité

# Besoins en sécurité matérielle

- Implantation de fonctions cryptographiques ultra-légères
  - Chiffrement symétrique et à clé publique
  - Chiffrement authentifié
  - Générateurs de nombres aléatoires dans le matériel
- Implantations sécurisées
  - Contre-mesure aux attaques en injection de fautes (*laser, EM, JTAG …)*
  - Contre-mesure aux attaques par analyse de canaux cachés (*EM, puissance, photon …)*
  - Sécurité *par conception*



# Besoins en sécurité matérielle

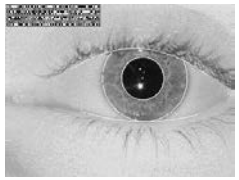
- Traçabilité et identification « biométrique » des objets
  - Empreinte digitale microélectronique du matériel
  - Certificat de confiance du matériel


- Mise à jour et mise à niveau à distance des parties matérielles des objets
  - Système de reconfiguration à distance sécurisée du matériel
  - Verrouillage / déverrouillage à distance de fonctionnalités matérielles

# Empreinte digitale microélectronique des objets

# Biométrie

- Mesure d'une caractéristique physique ou comportementale d'un individu
  - Empreintes digitales
  - Reconnaissance d'iris
  - Analyse de la voix
  - Etc.



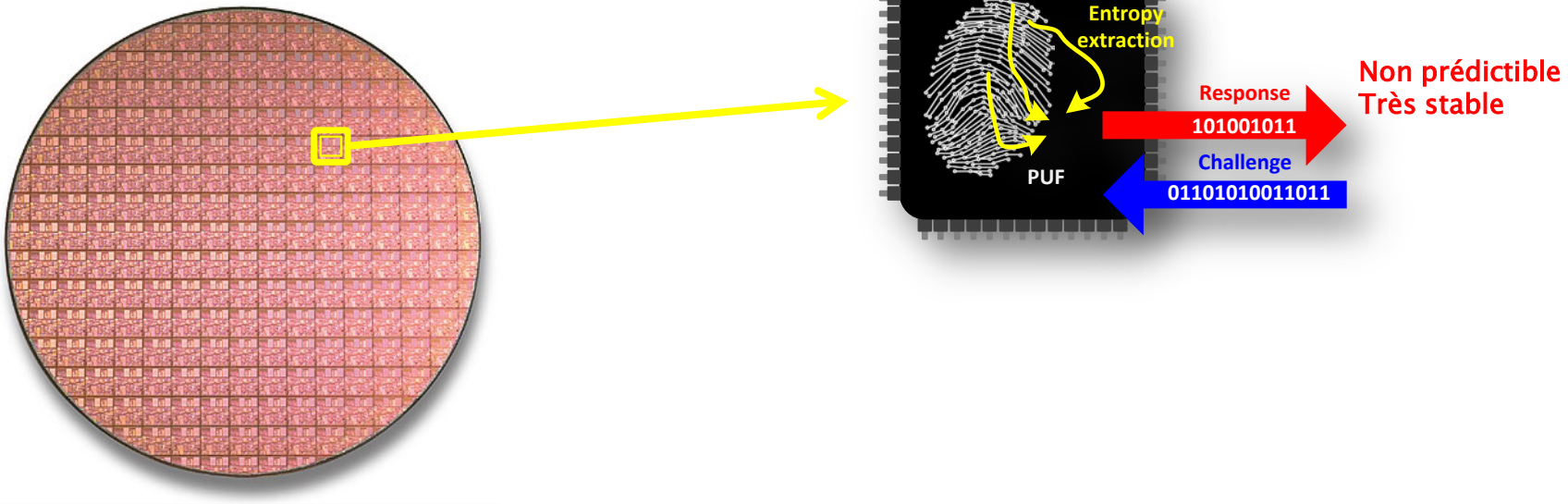
- Mesure d'une caractéristique physique ou comportementale d'un circuit intégré
  - Fingerprinting
  - Fonction physique non clonable (*Physical unclonable Function* – **PUF**)

# PUF

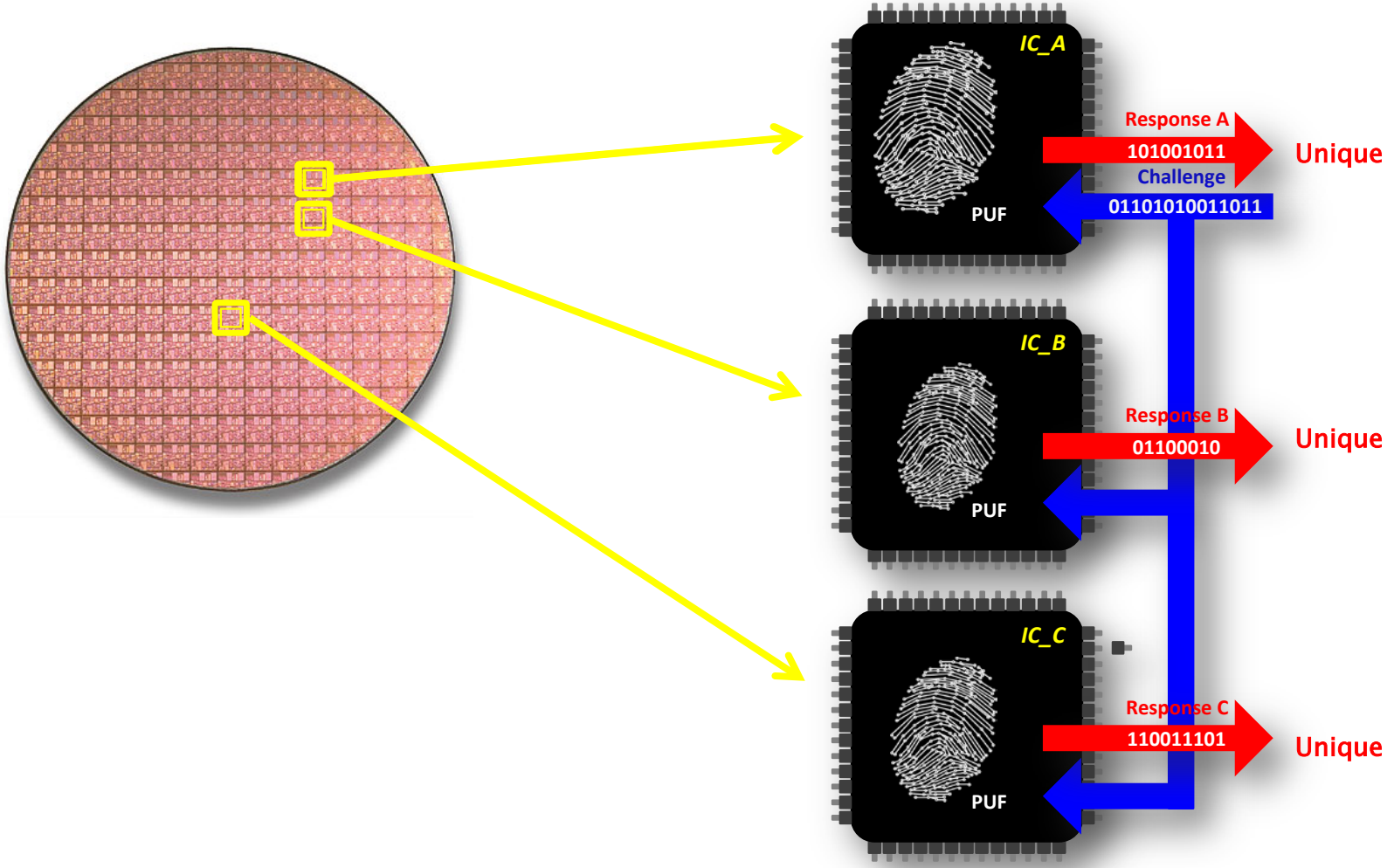
- Identification intrinsèque (*micrométrie*) d'un circuit intégré
  - Utilise un protocole challenge-réponse
  - Activation du matériel
  - Traçabilité
  - (Génération de clés cryptographiques)


| ID | IC |
|---|---|
| AF30 | |
| 37B1 | |
| 8992 | |
| FE72 | |
| E90B | |
| 5129 | |
| 8C9D | |
| 253A | |

# Caractéristique d'une bonne PUF

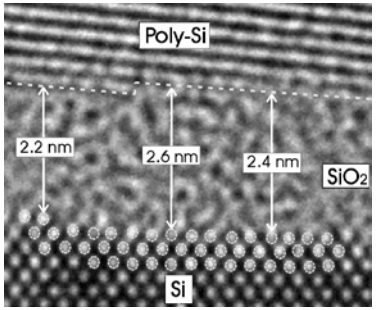


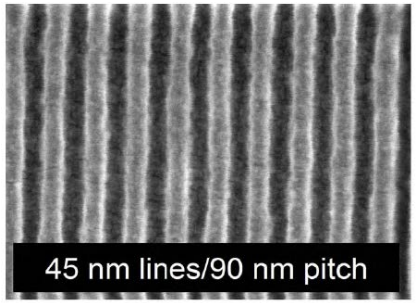
# Caractéristique d'une bonne PUF

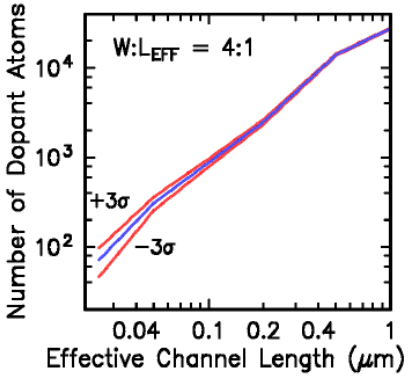


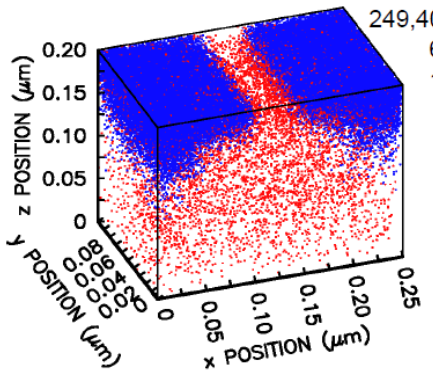
# Variabilités du procédé de fabrication CMOS

- Exemples
  - Linéarité des métallisations
  - Epaisseur d'oxyde
  - Position et densité des dopants
  - Etc.

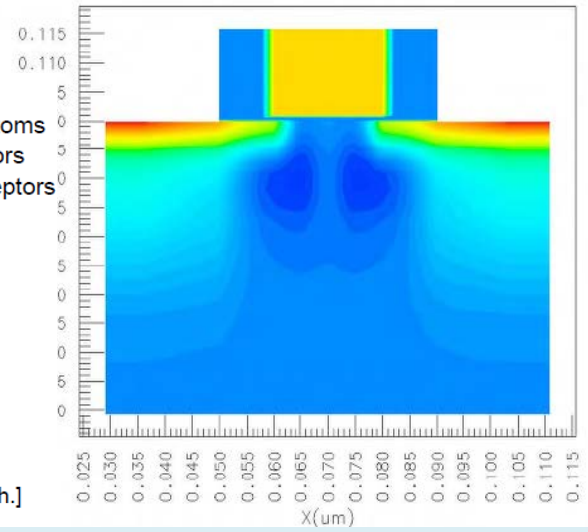


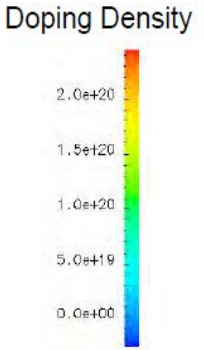



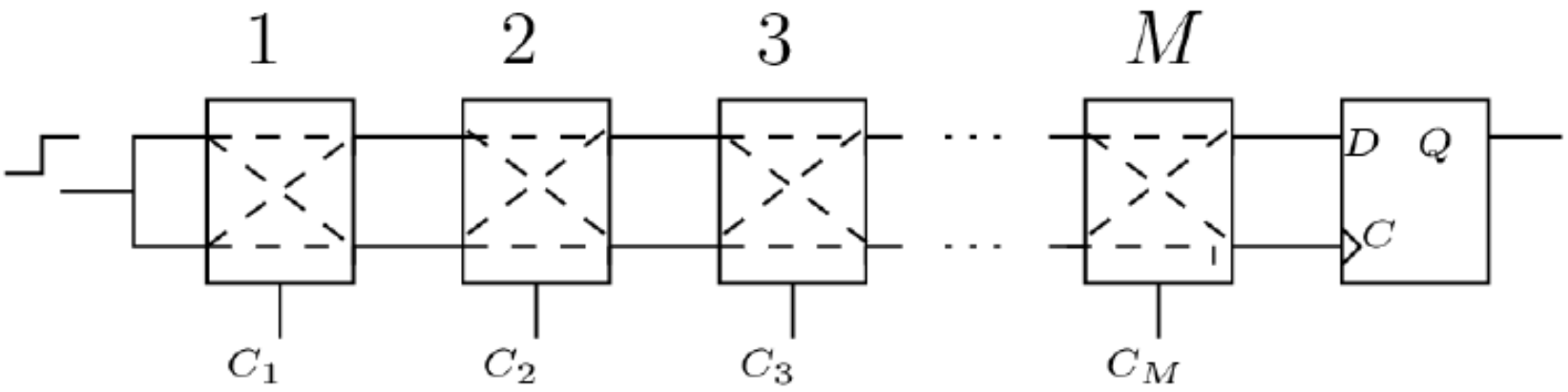

[D. J. Frank, et al., 1999 Symp. VLSI Tech.]



# Exemples d'architectures de PUF

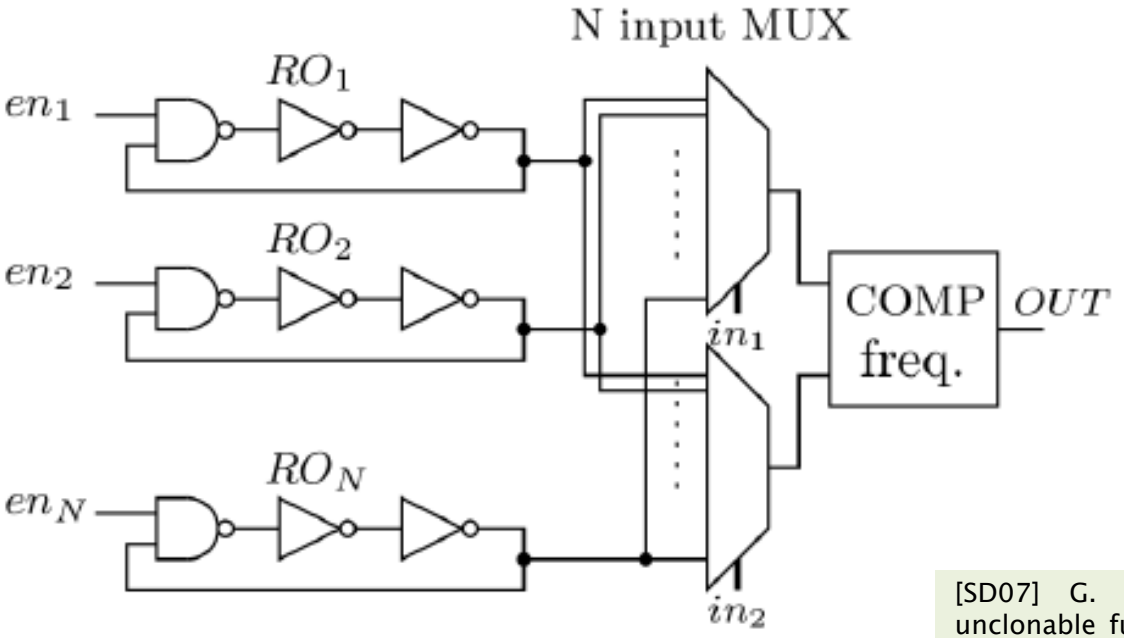
- 1 – Le PUF à arbitre [GLC+04]
  - Un événement parcourt deux lignes théoriquement identiques




[GLC+04] B. Gassend, D. Lim, D. Clarke, M. Van Dijk, S. Devadas. Identification and authentication of integrated circuits. Concurrency and Computation: Practice & Experience, 16(11):1077–1098, 2004.

# Exemples d'architectures de PUF

- 2 – Le PUF à N oscillateurs en anneaux [SD07]
  - Comparaison deux à deux des fréquences des oscillateurs théoriquement identiques

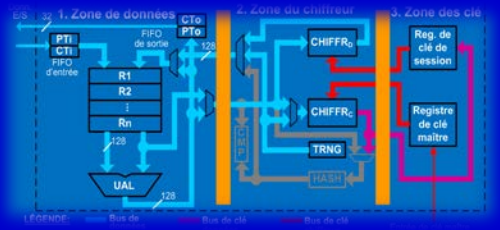



[SD07] G. Edward Suh, S. Devadas. Physical unclonable functions for device authentication and secret key generation. In DAC, pp. 9–14, 2007.

# Enjeux

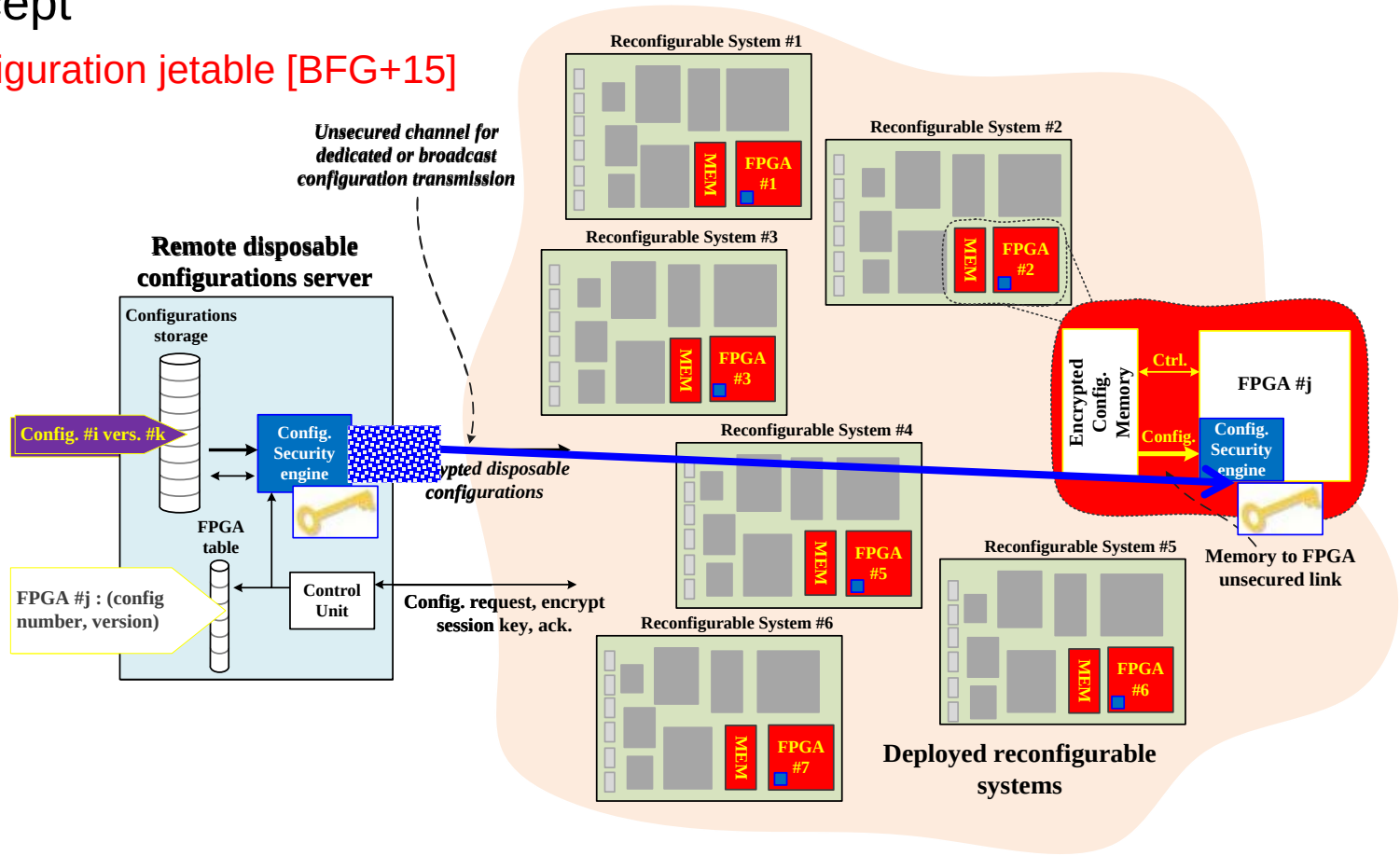
- Aujourd'hui la caractérisation des PUF ce fait de façon statistique avec un échantillon de quelques dizaines de circuits
  - C'est insuffisant pour une certification standardisée
- Besoin de développer des modèles
  - Modèles stochastiques des variations du process CMOS
  - Modèles physiques du PUF
- Analyse de la sécurité
  - Vis-à-vis des attaques par analyse (principalement EM et optique)
  - Vis-à-vis des attaques par modélisation incrémentale
- Conception bas coûts

# Reconfiguration matérielle à distance et sécurisée des objets



# Reconfiguration à distance sécurisée par conception

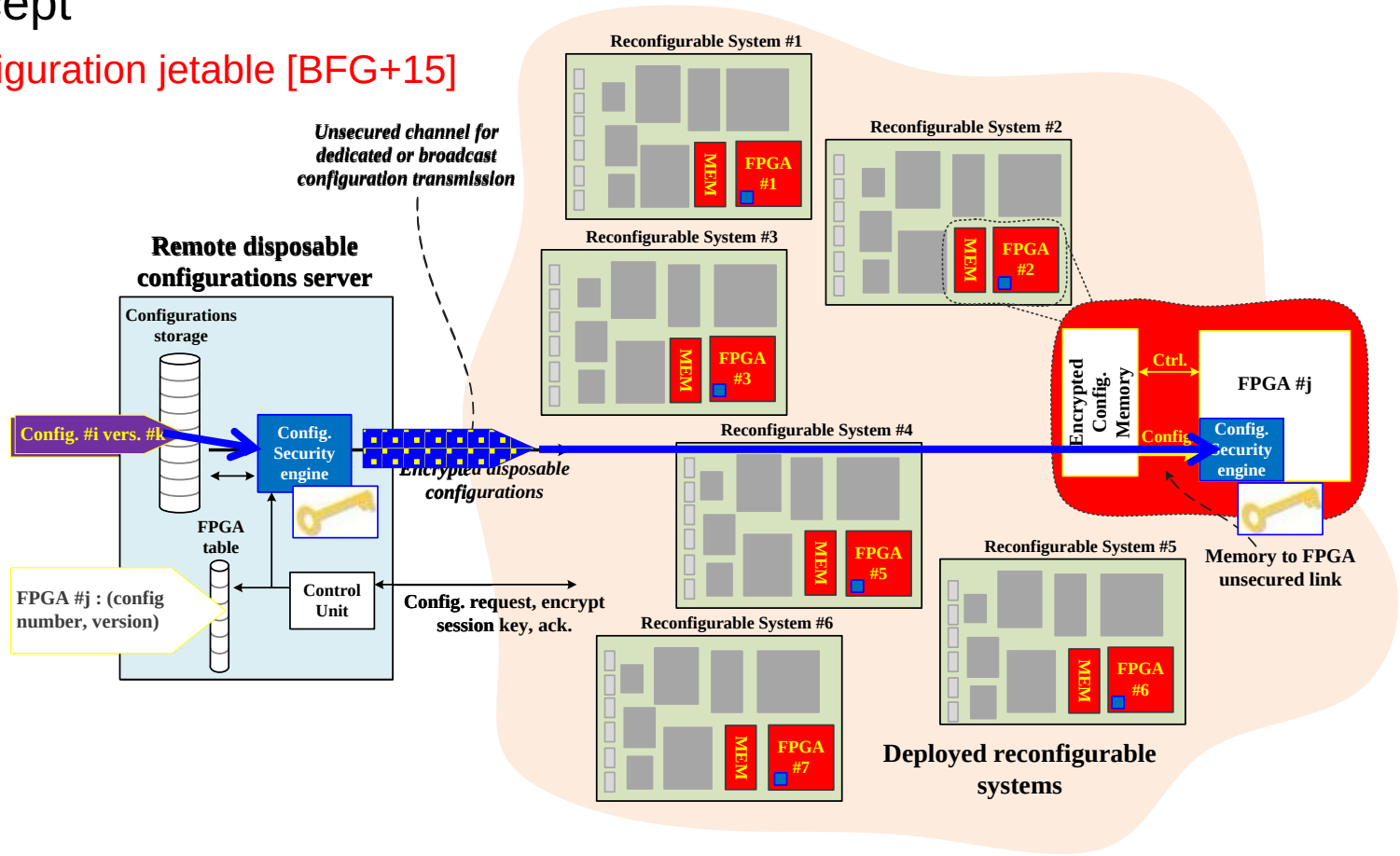
- Le concept
  - la configuration jetable [BFG+15]




[BFG+15] L. Bossuet, V. Fischer, L. Gaspar, L. Torres, G. Gogniat. *Disposable Configuration of Remotely Reconfigurable Systems.* Microprocessors and Microsystems, Embedded Hardware Design, Elsevier, Vol. 39, No. 6, pp. 382–392, August 2015

# Reconfiguration à distance sécurisée par conception

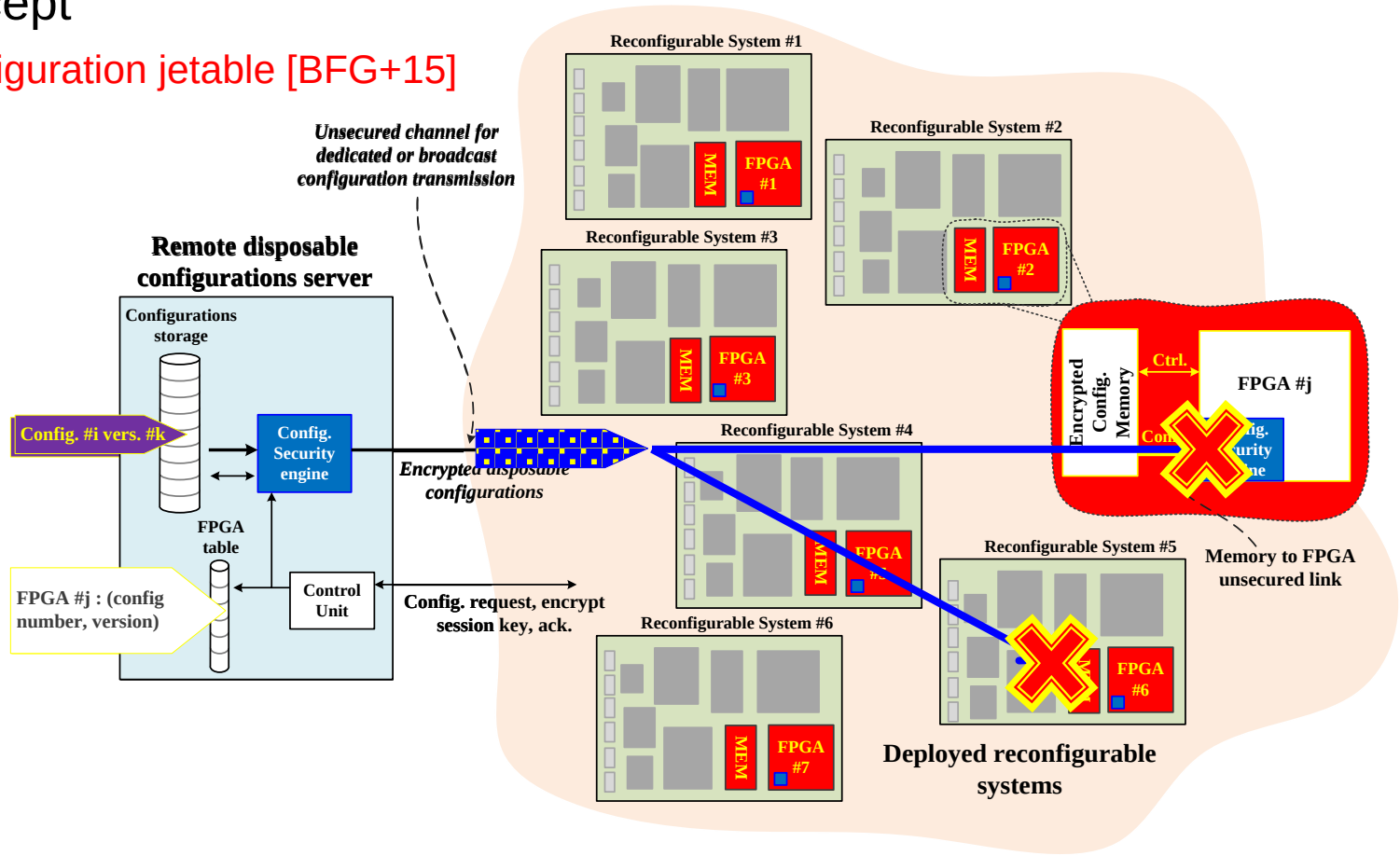
- Le concept
  - la configuration jetable [BFG+15]




[BFG+15] L. Bossuet, V. Fischer, L. Gaspar, L. Torres, G. Gogniat. *Disposable Configuration of Remotely Reconfigurable Systems.* Microprocessors and Microsystems, Embedded Hardware Design, Elsevier, Vol. 39, No. 6, pp. 382–392, August 2015

# Reconfiguration à distance sécurisée par conception

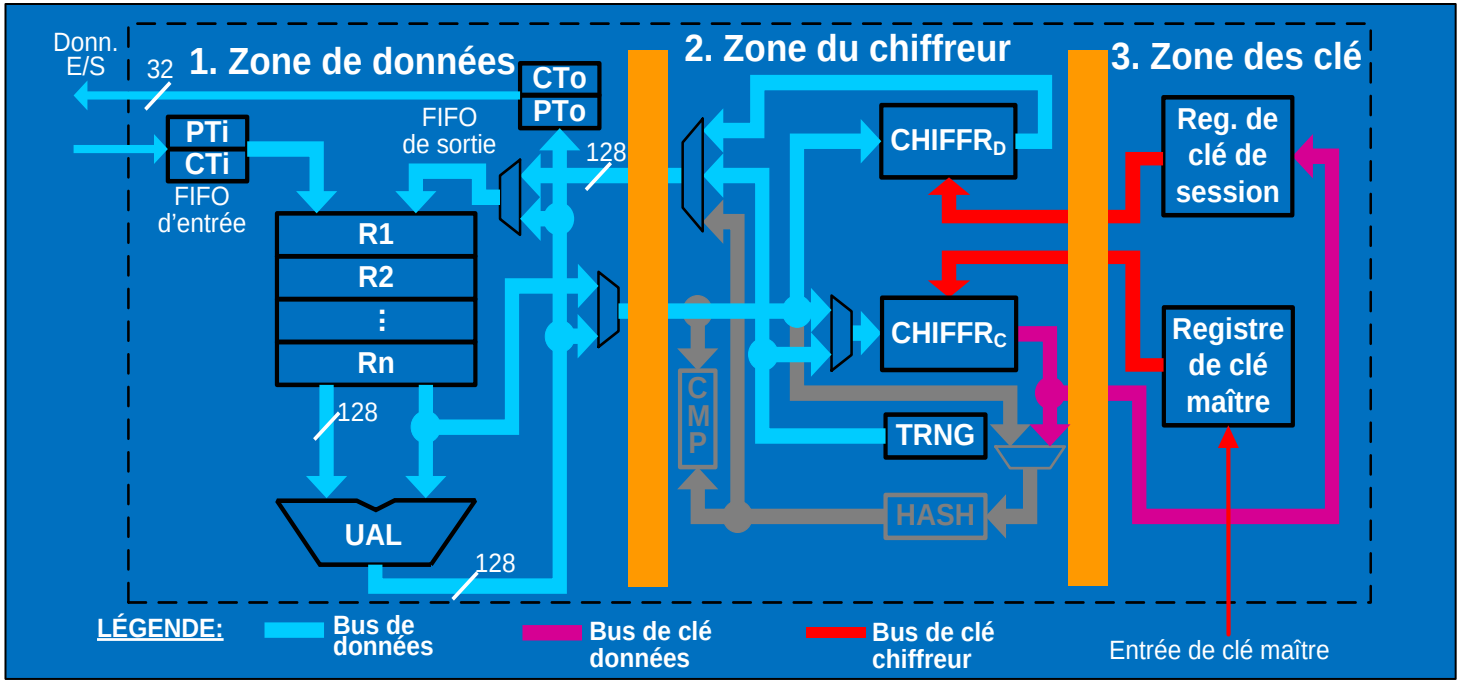
- Le concept
  - la configuration jetable [BFG+15]




[BFG+15] L. Bossuet, V. Fischer, L. Gaspar, L. Torres, G. Gogniat. *Disposable Configuration of Remotely Reconfigurable Systems.* Microprocessors and Microsystems, Embedded Hardware Design, Elsevier, Vol. 39, No. 6, pp. 382–392, August 2015

# Un cryptoprocesseur résistant aux attaques logicielles

- HCrypt est le résultat de l'ANR SecReSoC [GFB+10]
- Cloisonnement matérielle : séparation en trois zones




[GFB+10] L. Gaspar, V. Fischer, F. Bernard, L. Bossuet, P. Cotret. *HCrypt: A Novel Reconfigurable Crypto-processor with Secured Key Management*. In International Conference on ReConFigurable Computing and FPGAs, pp. 280-285, Cancun, Mexico, December 13-15 2010.

# Enjeux

- Proposer des solutions sécurisées très (ultra) bas coût
  - En surface / en consommation de puissance
  - Peu de contraintes de délais
- Etendre à la mise à niveaux par activation à distance de fonctionnalités
  - Matériel (IP) évolutif …
  - License d'utilisation du matériel
- Vers un nouveau business …
  - De la vente de matériel à le vente de configuration du matériel (mise à jour / mise à niveau)

# Conclusion

# Conclusion

- Pour le déploiement des objets connectés
  - La sécurité est plus qu'une contrainte de conception, c'est une propriété à développer
  - La sécurité est à prendre en compte dès les premières phases de conception et doit s'appuyer sur des méthodes et des moyens standardisés
- Le défi est principalement matériel
  - Nombreuses solutions pour le logiciel (maturité)
  - Problématique sécurité vs. coûts (surface, performance, €, …)
- Les ingénieurs sont-ils bien formés ???

# Ces travaux font partie du projet SALWARE

French ANR Project

“Le projet jeune chercheur **SALWARE** est financé par l’agence nationale de la recherche (ref. ANR-13-JS03-0003), il est co-financé par la fondation de recherche pour l’aéronautique et l’espace”

contacts:
lilian.bossuet@univ-st-etienne.fr
Site internet du projet : http://www.univ-st-etienne.fr/salware/

# 28ème entretiens Jacques Cartier
# Colloque “Objets Connectés”

# La sécurité des objets connectés
## *les défis matériels*

**Lilian Bossuet**
Laboratoire Hubert Curien, CNRS UMR 5516
Université Jean Monnet, Saint-Etienne, France


2 décembre 2015
Ecole Centrale de Lyon, Ecully, France