10 Ans Master SCCI

Matthieu Rivain
Pomotion 2006

Grenoble
12 septembre 2011

Résumé

- Sortie du master en 2006
- Mar 06 – Aou 06 : PFE chez Axalto/Gemalto
  - Equipe Cryptographie
- Oct 06 – Jan 10 : Thèse CIFRE chez Oberthur Technologies
  - Division Card Systems, Équipe Cryptographie
  - Thèse en partenariat avec l'Université du Luxembourg
- Fev 10 – présent : chez CryptoExperts

CryptoExperts

CryptoExperts

Oberthur Technologies

Quelques chiffres:

- 6800 employés
- 65 sites dans + de 40 pays
- 14 sites de production
- 12 sites de R&D
- + de 450 ingénieurs R&D

Oberthur Technologies

4 secteurs d'activités:

- Card Systems (cartes à puce)
- Fiduciaire (billets de banque)
- Identité (documents d'identité)
- Cash Protection (équipements pour la protection des billets)

Oberthur Technologies

Produits carte à puce:

- Paiement (cartes bancaires)
- Télécommunication (cartes SIM)
- Transport (cartes de transport sans contact)
- Convergence (cartes multi-applicatives)
- Télévision à péage (cartes pour décodeur TV)

Oberthur Technologies

Équipe Cryptographie:

- une dizaine d'ingénieurs
- basée sur le site R&D de Nanterre
- missions:
  - implémentation des algos crypto pour les produits carte
  - sécurisation des produits contre les attaques cryptanalytiques par voie physique
  - veille technique et innovation
- collaboration proche avec le labo sécurité
  - 3/4 personnes
  - basé à Bordeaux
  - évaluation sécuritaire des produits

La Cryptographie dans la Carte à Puce

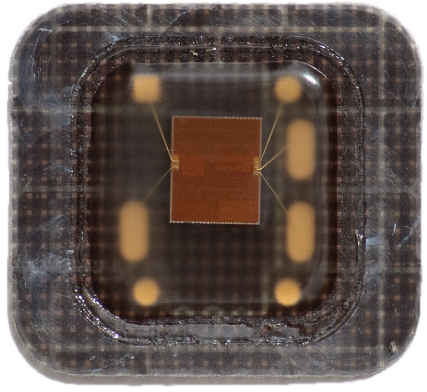
La cryptographie dans la carte à puce

Qu'est-ce qu'une carte à puce ?

CryptoExperts

La cryptographie dans la carte à puce

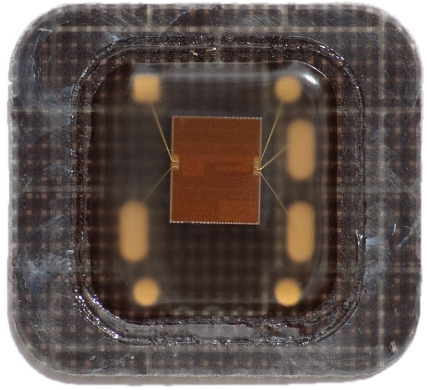
Qu'est-ce qu'une carte à puce ?

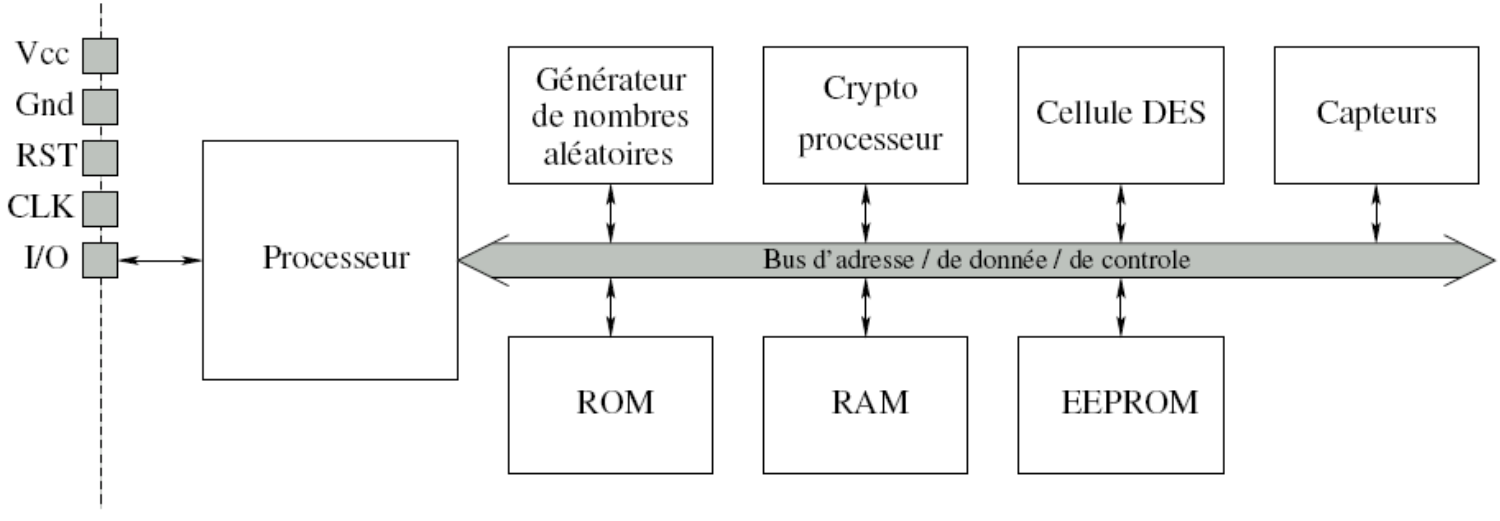


CryptoExperts

La cryptographie dans la carte à puce

Qu'est-ce qu'une carte à puce ?





La cryptographie dans la carte à puce

- Environnement contraint
  - en consommation silicium
  - en consommation électrique (applications sans contact)
  - en mémoire (RAM, NVM, ROM, ...)
  - en puissance de calcul (μP 8/16/32-bit, horloge $\sim$30 MHz)
- Divers algorithmes cryptographiques
  - DES, AES, algos symétriques propriétaires
  - SHA, HMAC, CBC-MAC
  - RSA (chiffrement & signature), DSA, ECDSA
  - échange de clé Diffie-Hellman, ECDH
- Cryptographie symétrique efficace
- Cryptographie asymétrique coûteuse
  - utilisation de crypto-processeurs
  - arithmétique modulaire

La cryptographie dans la carte à puce

Les attaques par canaux auxiliaires

CryptoExperts

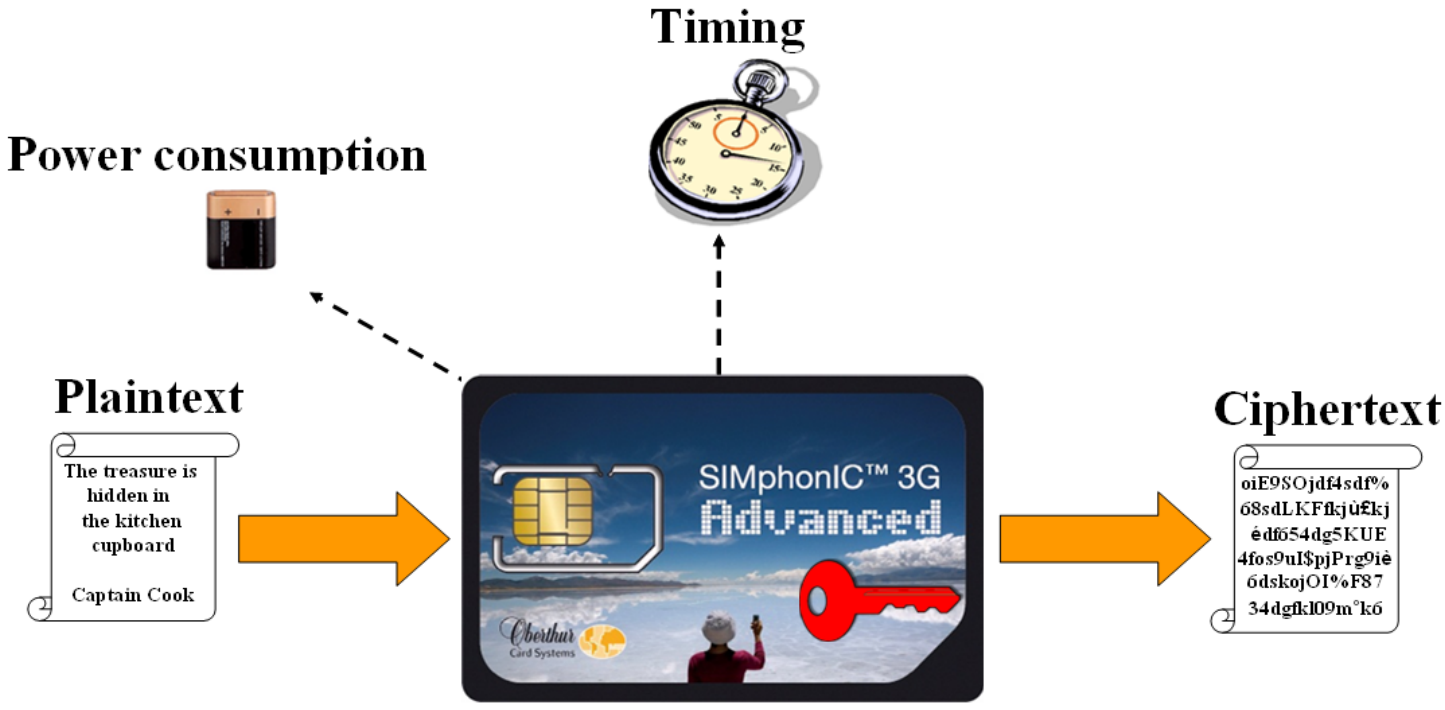
La cryptographie dans la carte à puce

Les attaques par canaux auxiliaires

CryptoExperts

La cryptographie dans la carte à puce

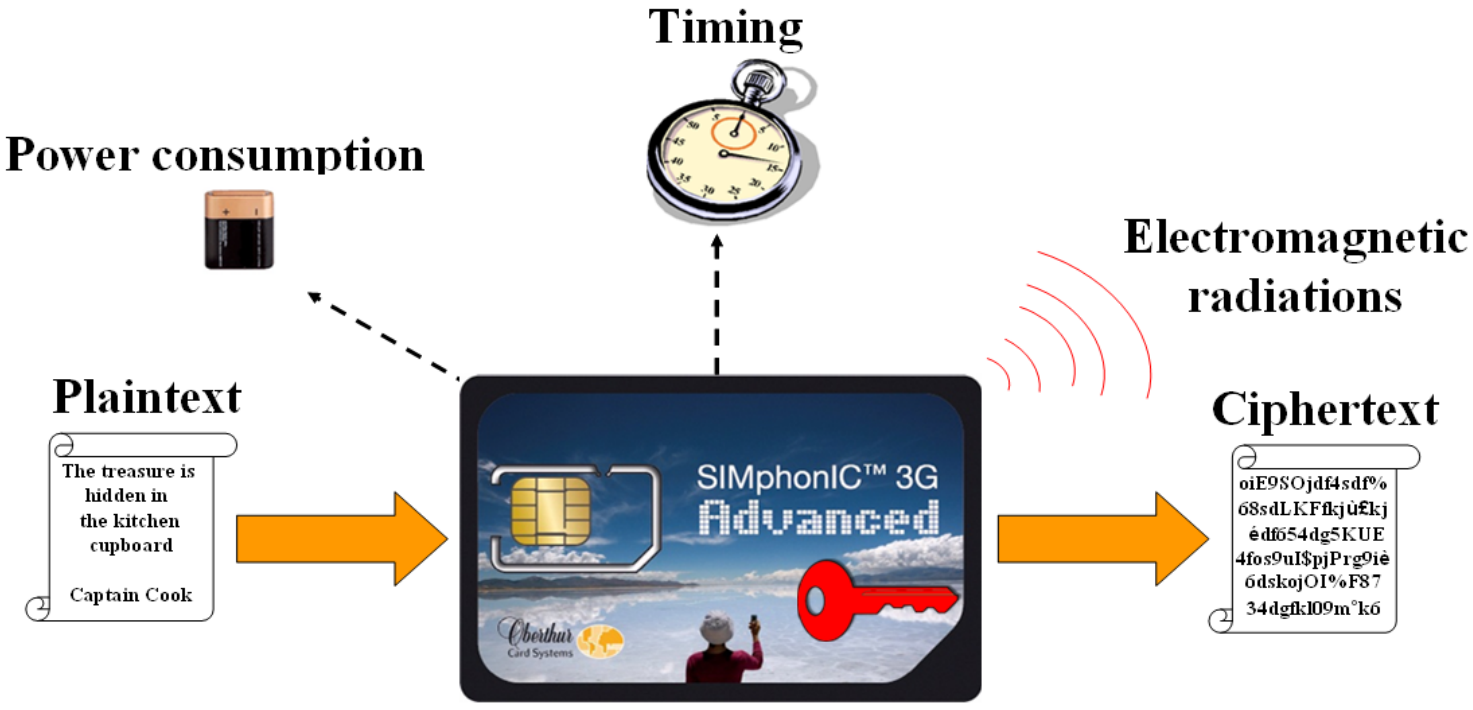
Les attaques par canaux auxiliaires



CryptoExperts

La cryptographie dans la carte à puce

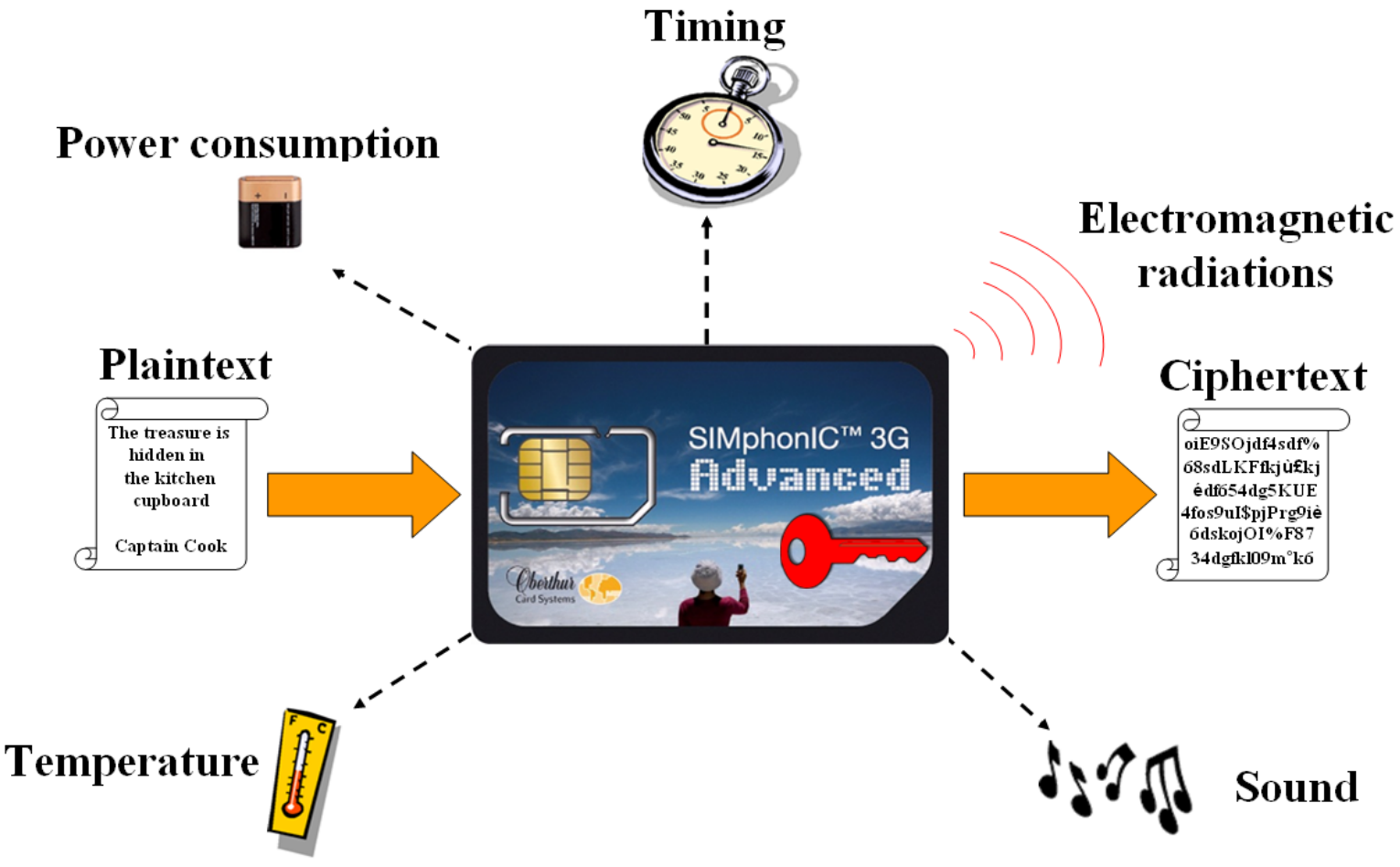
Les attaques par canaux auxiliaires



CryptoExperts

La cryptographie dans la carte à puce

Les attaques par canaux auxiliaires

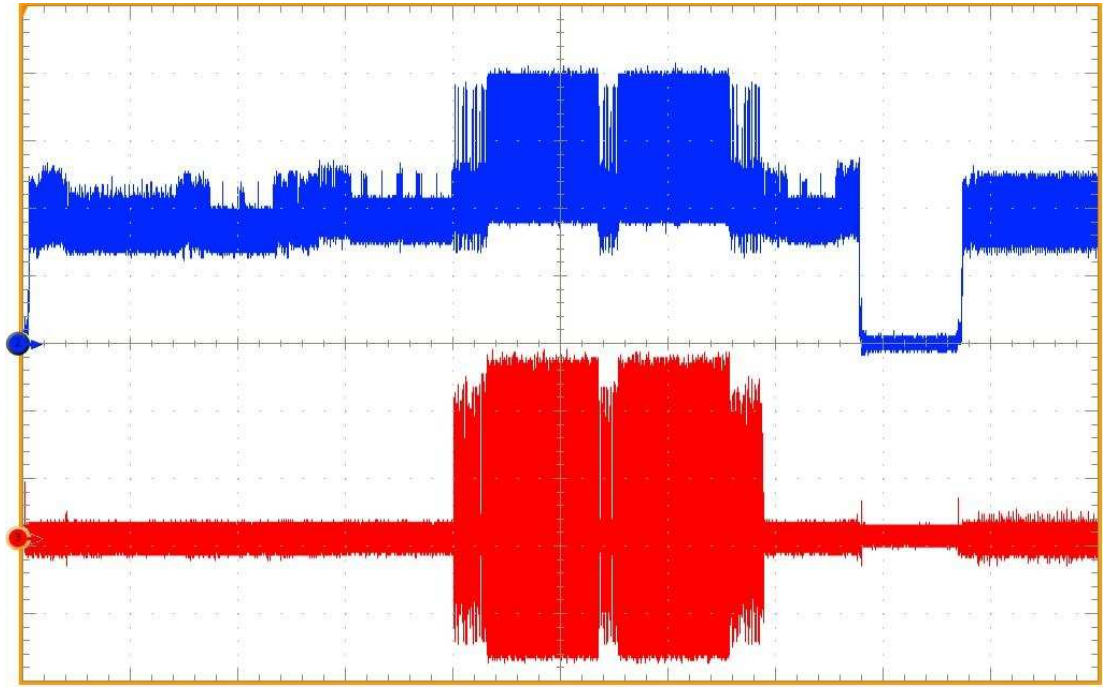


CryptoExperts

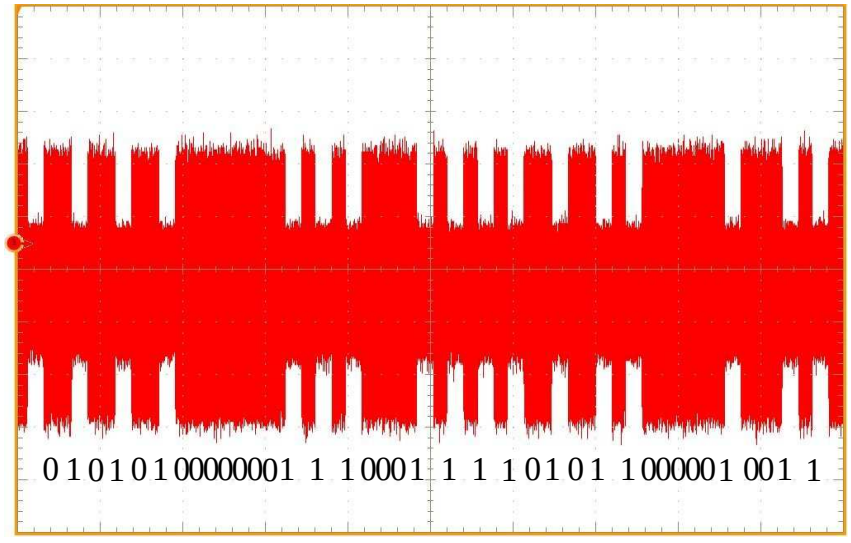
La cryptographie dans la carte à puce

Les attaques par canaux auxiliaires

- Exemple : consommation électrique et ondes électromagnétiques pendant un calcul RSA



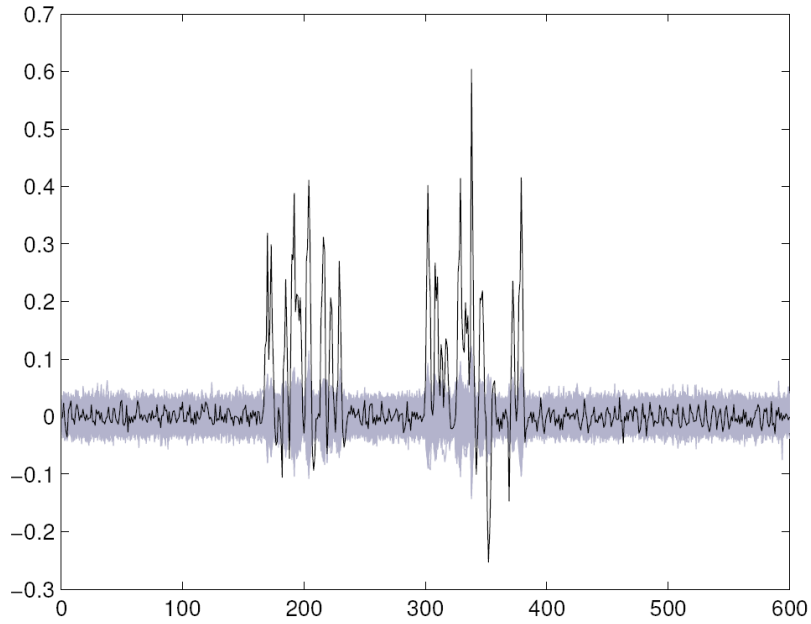
La cryptographie dans la carte à puce
L'attaque SPA (simple power analysis)



- Analyse le flot d'opérations
- Une seule mesure suffit (en général) pour retrouver la clé
- Contremesure : implémenter les algorithmes de manière *atomique*

La cryptographie dans la carte à puce
L'attaque DPA (differential power analysis)

- Cible les données manipulées
- Traitement statistique sur plusieurs mesures



CryptoExperts

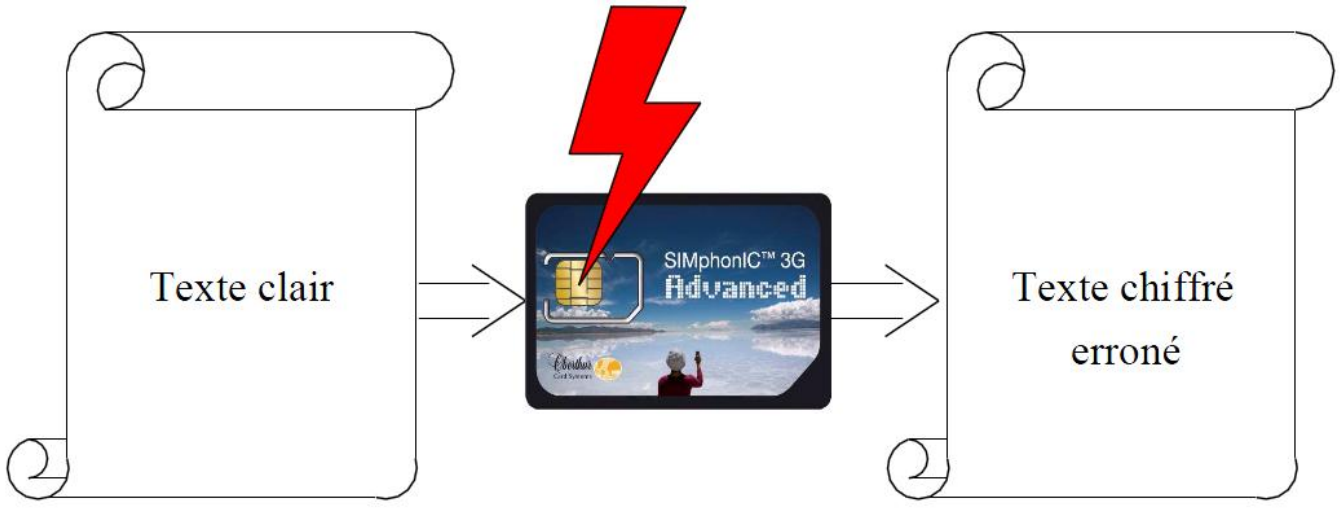
La cryptographie dans la carte à puce

Les attaques par injection de fautes

CryptoExperts

La cryptographie dans la carte à puce

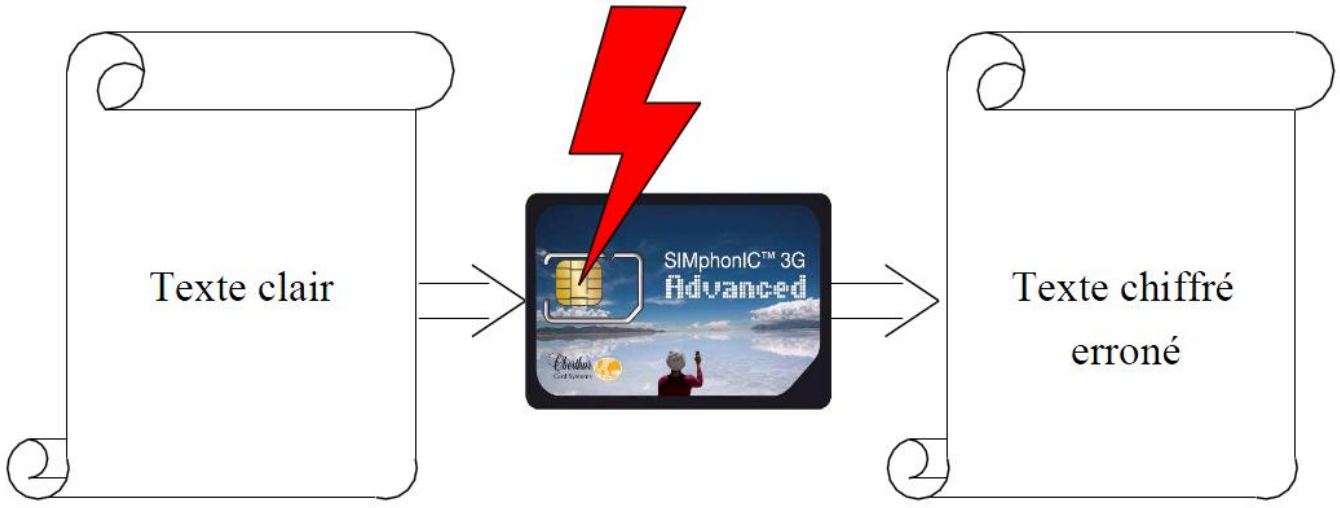
Les attaques par injection de fautes



- Exploitation des résultats erronés pour en déduire la clé secrète

La cryptographie dans la carte à puce

Les attaques par injection de fautes



- Exploitation des résultats erronés pour en déduire la clé secrète
- Techniques d'injection de fautes :
  - *glitch* d'alimentation ou d'horloge
  - injection lumineuse (*e.g.* flash, laser)

Thèse CIFRE chez Obertur

CryptoExperts

Thèse CIFRE chez Obertur

- 50 % recherche, 50% développement
- Travaux de recherche:
  - formalisation & analyse des attaques de type DPA
  - contremesures par masquage pour le chiffrement par bloc
  - attaques par fautes & contremesures (DES, RSA)
- En charge d'un projet financé SecureAlgorithm (avec l'ENST, Nagra, Paris 8, Thales et l'UVSQ)
- Développement:
  - divers algorithmes (DES, AES, SHA, MAC, Diffie-Hellman, ...)
  - sur divers composants 8/16/32-bit
  - en assembleur et en C
  - avec contremesures
- Formation interne d'introduction à la cryptographie

Thèse CIFRE chez Obertur

- La thèse CIFRE, c'est bien !
- Un pied dans le monde industriel, un pied dans le monde académique
- Recherche motivée et appliquée à des problématiques industriels

CryptoExperts

CRYPTOEXPERTS

CryptoExperts

- SAS crée en 2009 par les experts crypto de Gemalto
  - P. Paillier, A. Gouget, C. Clavier, L. Goubin
- Aujourd'hui 4 salariés
  - P. Paillier, C. Delerablée, T. Baignères, M. Rivain
  - tous docteurs en cryptographie
  - différents domaines d'expertise
- Trois types d'activité:
  - prestations de R&D externalisées et consulting
  - recherche financée (JEI, CIR, projets financés)
  - innovation (projets internes)

CryptoExperts

CryptoExperts

Nos prestations de R&D externalisées:

- conception d'algorithmes et protocoles crypto sur mesure
- développements de prototypes
- audit d'algorithmes/protocoles et preuves de sécurité
- accompagnement technique en normalisation
- développement de librairies crypto embarquées sécurisées
- audit et conseil en sécurité des implémentations
- aide à la conception de crypto-processeurs hardware

CryptoExperts

Nos clients:

- Gemalto (contrat cadre)
- La Française des Jeux (sécurité des jeux)
- INVIA (libs crypto & design hardware)
- INRIA (databases sécurisées)
- Xiring (lecteurs de cartes ID/santé)
- Comexposium (site web salon Cartes)
- Tranef (sécurité prouvée contre les attaques physiques)

CryptoExperts

Nos projets de recherche financés:

- Projet ANR BEST (pay-TV anti-piratage)
- Projet ANR ECLIPSES (module hardware embarquée pour la crypto à base de courbes elliptiques et pairings)
- Projet FUI Tisphanie (sécurité des téléphones mobiles)
- Projet FP7 IP ABC4Trust (privacy-preserving attribute-based credentials)

Projet de R&D interne:

- STONE (chiffrement broadcast, 3 brevets déposés)

CryptoExperts

Mes activités chez CryptoExperts:

- En charge du projet ECLIPSES
- Développement de librairies crypto sécurisées
- Participation aux projets de recherche
- Veille technique et publications

CryptoExperts