École thématique ARCHI07

Architectures des systèmes matériels enfouis et méthodes de conception associées

Renforcement de la Sécurité des Cryptoprocesseurs par Codage de l'Information

Julien Francq[1♦] Jean-Baptiste Rigaud[1] Pascal Manet[2] Arnaud Tisserand[3] Jean-Claude Bajard[3]

[1]Ecole Nationale Supérieure des Mines de St-Etienne, [2]CEA-LETI

[1,2]Centre Microélectronique de Provence, Laboratoire SESAM[♣]

Avenue des Anémones - Quartier Saint-Pierre, 13541 GARDANNE

[3]LIRMM, 161 rue Ada, 34392 MONTPELLIER Cedex 05

[1]{nom @emse.fr} [2]{prénom.nom@cea.fr} [3]{prénom.nom@lirmm.fr}

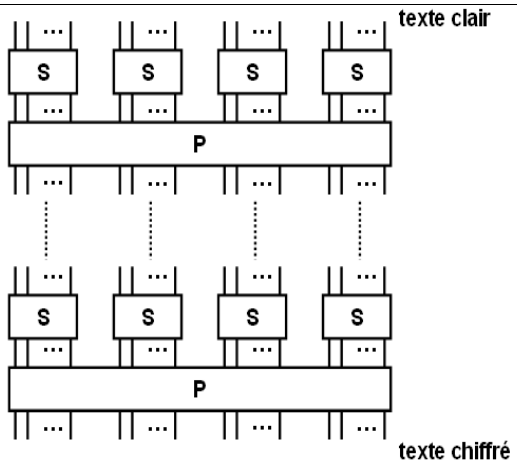
Contexte

La carte à puce, comme tout autre processeur de traitement d'informations confidentielles peut faire l'objet de manipulations frauduleuses, appelées communément attaques.

Ce type de composant embarque notamment des fonctions cryptographiques à clé publique ou privée. Les concepteurs de tels circuits doivent insérer dans ces architectures des parades aux différentes attaques répertoriées, également appelées contre-mesures. Le codage de l'information traitée par le cryptoprocesseur paraît être une contre-mesure possible pour le renforcement de la sécurité de ces systèmes.

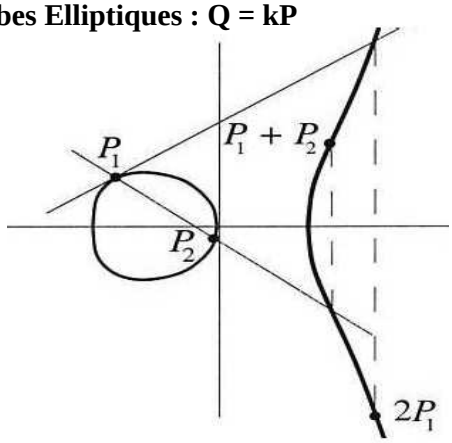
Algorithmes cryptographiques

A clé privée : DES, AES …

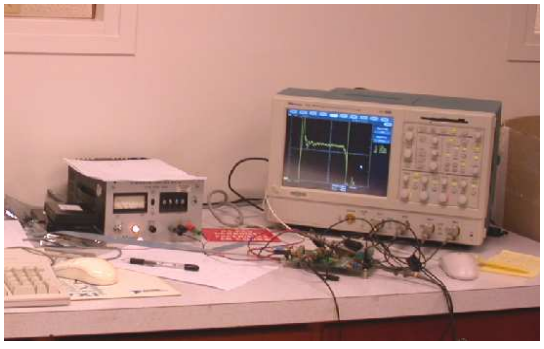


A clé publique

- **RSA : $C = P^e \bmod M$**
- **Courbes Elliptiques : $Q = kP$**



Types d'attaques



Actives	Passives
➢ Attaques DFA	➢ Temps de calcul
➢ « Safe-error »	➢ Consommation
➢ Machine d'état	➢ Champ électromagnétique

Contre-mesures

Attaques actives	Attaques passives
➢ Redondance	➢ Rendre le temps d'exécution constant
➢ Contrôle de l'intégrité des calculs intermédiaires	➢ Rendre les traces de consommation régulières

Travaux actuels

- **Implémentation d'un RSA et d'une Courbe Elliptique conformes à l'état de l'art**
- **Étude et implémentation de contre-mesures existantes et innovantes**

♦Ce travail fait l'objet d'une thèse à financement FSE (Fonds Social Européen) dans le cadre du projet BTRS (Briques Technologiques pour le Renforcement de la Sécurité).

♣Le laboratoire SESAM est une équipe mixte CEA-LETI / ENSMSE basée sur le site Georges Charpak (Gardanne, 13).