Contribution à la sécurité physique des cryptosystèmes embarqués

Alexandre VENELLI

31/01/2011

Introduction

- Environnement embarqué / cartes à puce
  - Concept proposé dans les années 1970
  - Objet portable dans lequel on peut stocker des données
  - L’ajout d’un processeur (puce) dans ces objets permet d’augmenter leurs fonctionnalités et leur sécurité

- Exemples d’utilisations
  - Téléphonie mobile avec les cartes SIM
  - Cartes bancaires
  - Passeport électronique
  - Télévision à péage
  - Carte Vitale, …

Introduction

- Sécuriser ces objets → Cryptographie
  - Mélange de mathématiques appliquées et d'informatique
  - Cryptosystème = Ensemble de méthodes permettant de sécuriser des communications
  - Tout cryptosystème peut être cassé en essayant toutes les clés possibles
  - Il faut faire en sorte que cela soit impossible à calculer en un temps raisonnable
  - On peut se baser sur des problèmes mathématiques difficiles

Introduction

- Cryptographie symétrique et asymétrique
  - Symétrique : rapide mais nécessite que les parties partagent le même secret
  - Asymétrique : lent mais plus de fonctionnalités

- Exemple typique d'utilisation
  - Les parties établissent un même secret partagé grâce à la cryptographie asymétrique
  - Les données sont chiffrées par cryptographie symétrique

Introduction

- Attaques physiques sur les algorithmes cryptographiques
  - Menace pour l'embarqué
  - Mathématiquement sûr ≠ Implémentation sûre
  - Principe : l'attaquant utilise des observations / interactions, lors du fonctionnement de l'algorithme, pour en déduire le secret
  - Exemples d'observations :
    - **Consommation de courant, émissions électromagnétiques, …**

- Contre-mesures adaptées à l'embarqué
  - Différences suivant l'algorithme (symétrique / asymétrique) et le type d'attaque physique
  - Se protéger avec des ressources limitées

Résultats de la thèse

- Etude et améliorations des attaques par canaux cachés
  - Améliorer l'attaque générique utilisant l'information mutuelle

- Contre-mesures adaptées pour les méthodes cryptographiques standards
  - Pour une implémentation d'AES intéressante en hardware
  - Pour la multiplication scalaire, algorithme efficace et résistant

- Etude de la résistance des couplages
  - Attaques par canaux cachés sur une implémentation classique de couplage

Sommaire

1. Attaques par canaux cachés et information mutuelle
2. Protéger l'AES
3. Protéger la multiplication scalaire sur courbes elliptiques
4. Attaques physiques sur des cryptosystèmes à base de couplages
5. Conclusion et perspectives

Sommaire

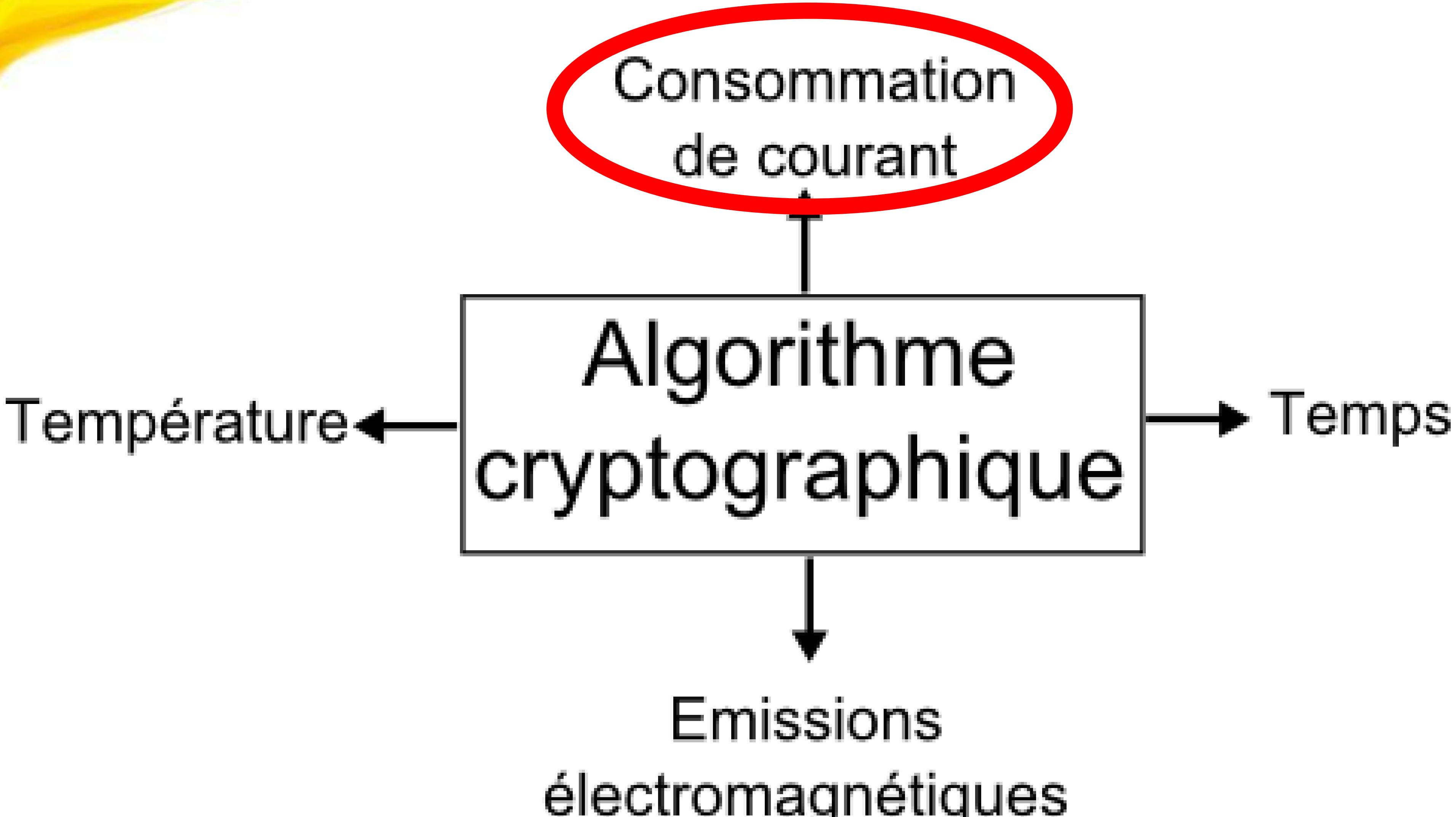
Familles d'attaques physiques

- **Attaques par analyse simple**
  L'attaquant observe un canal caché du composant lors d'un calcul cryptographique et retrouve la clé secrète

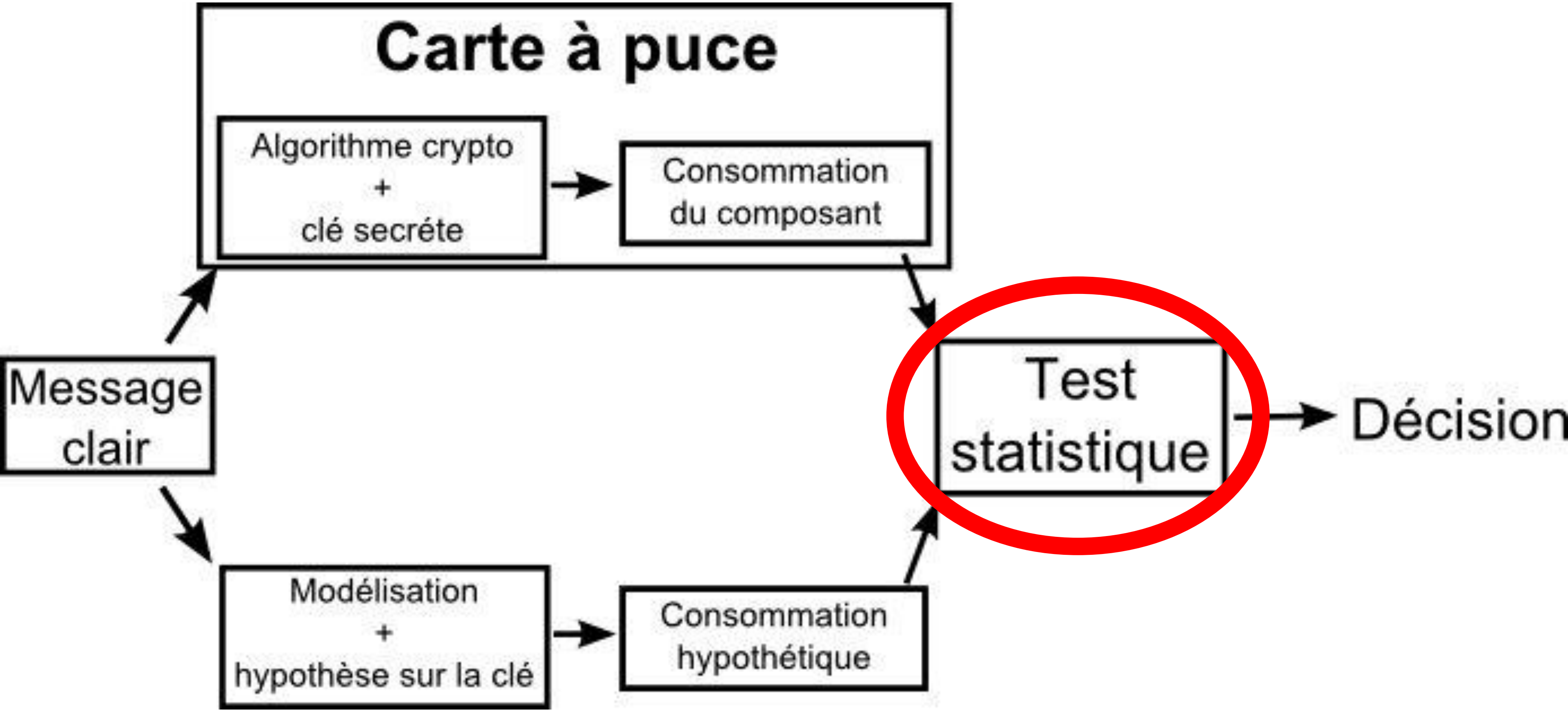
- **Attaques par analyse différentielle**
  L'attaquant observe plusieurs courbes du canal caché et retrouve le secret à l'aide d'outils statistiques

- **Attaques par injection de faute**
  L'attaquant utilise des résultats de calculs corrects, des résultats faux dus à une injection de faute et l'endroit précis où la faute a été effectuée pour retrouver le secret

Types de canaux cachés



Attaque par analyse différentielle de courant (DPA)



Historique des tests statistiques proposés

• Kocher et al. 1999	T-test simplifié (DPA)
• Brier et al. 2004	Corrélation de Pearson (CPA)
• Gierlichs et al. 2008	Information Mutuelle (MIA)
• Venelli 2010	MIA + B-spline
• Thanh-Ha Le et Berthier 2010	MIA + Cumulants

Attaque par analyse d'information mutuelle

- Information mutuelle
  - Puissante
  - Mais difficile à estimer

- Estimer l'IM → l'entropie → les densités de probabilités à partir d'un petit ensemble de données

- Deux familles de méthodes d'estimation
  - Paramétrique
  - Non-paramétrique

Estimation paramétrique et non-paramétrique

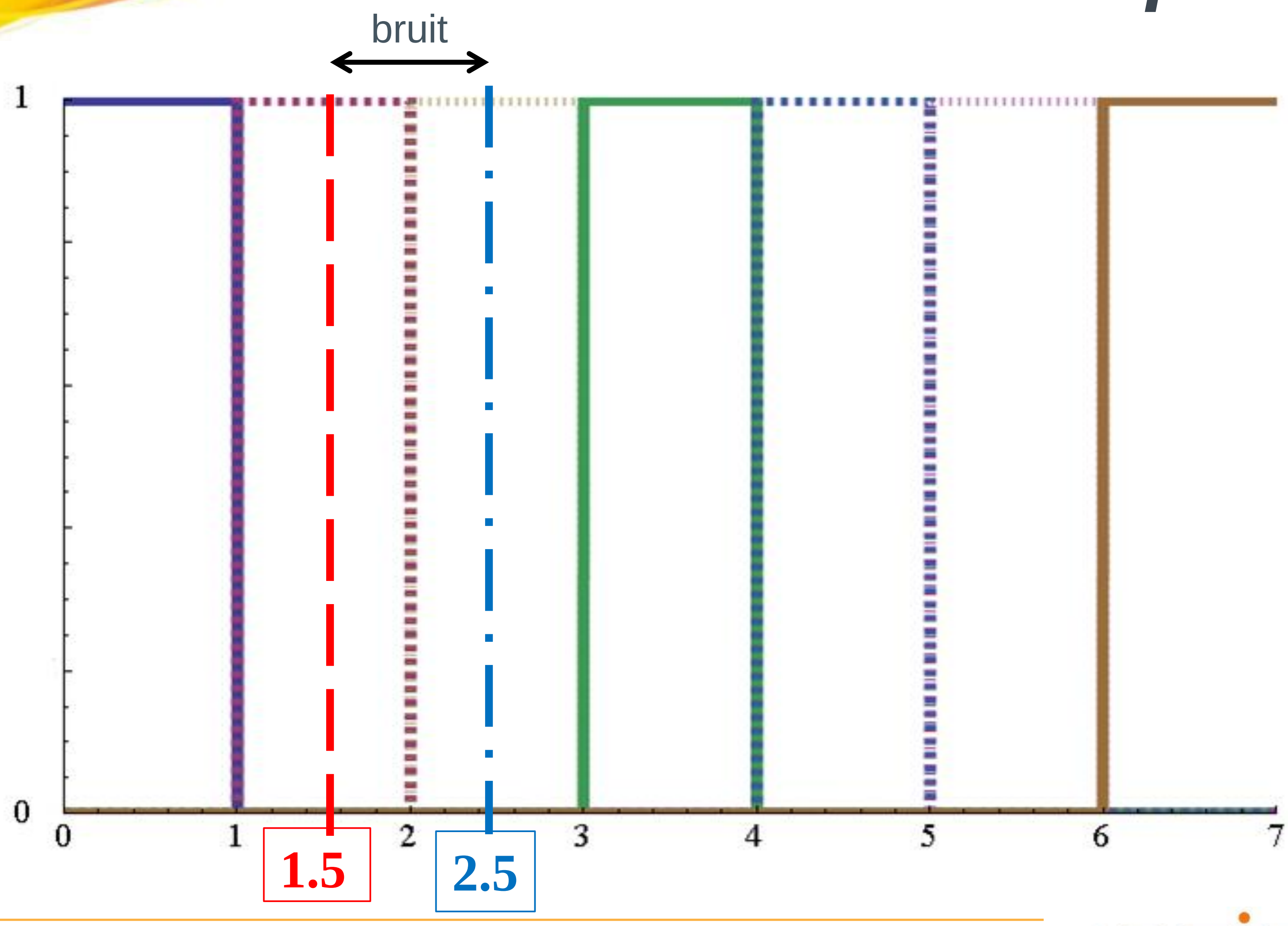
- Paramétrique
  - Hypothèse : les données proviennent d'une famille connue de distribution de probabilité (gaussienne, exponentielle, …)
  - Les paramètres sont optimisés afin que le modèle corresponde aux données

- Non-paramétrique
  - Hypothèse : aucune sur la distribution de probabilité de la population
  - Les paramètres sont souvent choisis de manière plus ou moins « aveugle »
  - Permet de traiter des données
    - **De « faible qualité »**
    - **À partir de petits échantillons**
    - **Dont on ne connaît que très peu sur les variables**

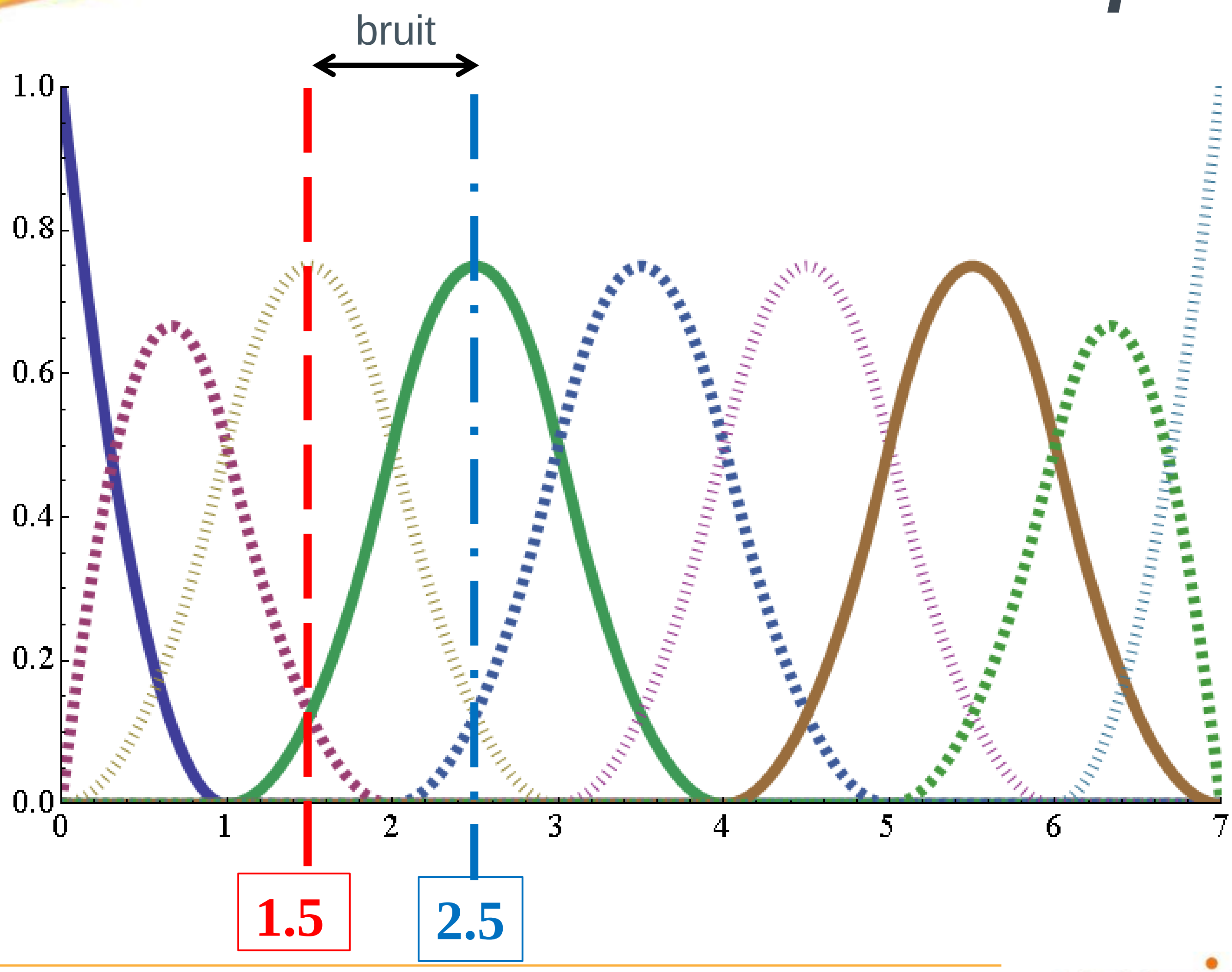
Estimation : histogrammes vs. fonctions B-splines

		
Histogrammes	Facile à calculer et à comprendre	Erreurs systématiques dues à la faible taille de l'échantillon
Fonctions B-splines	Propriété intéressante dans le cadre des attaques par canaux cachés	Estimation plus lente à calculer que les histogrammes

Estimation à base de fonctions B-splines

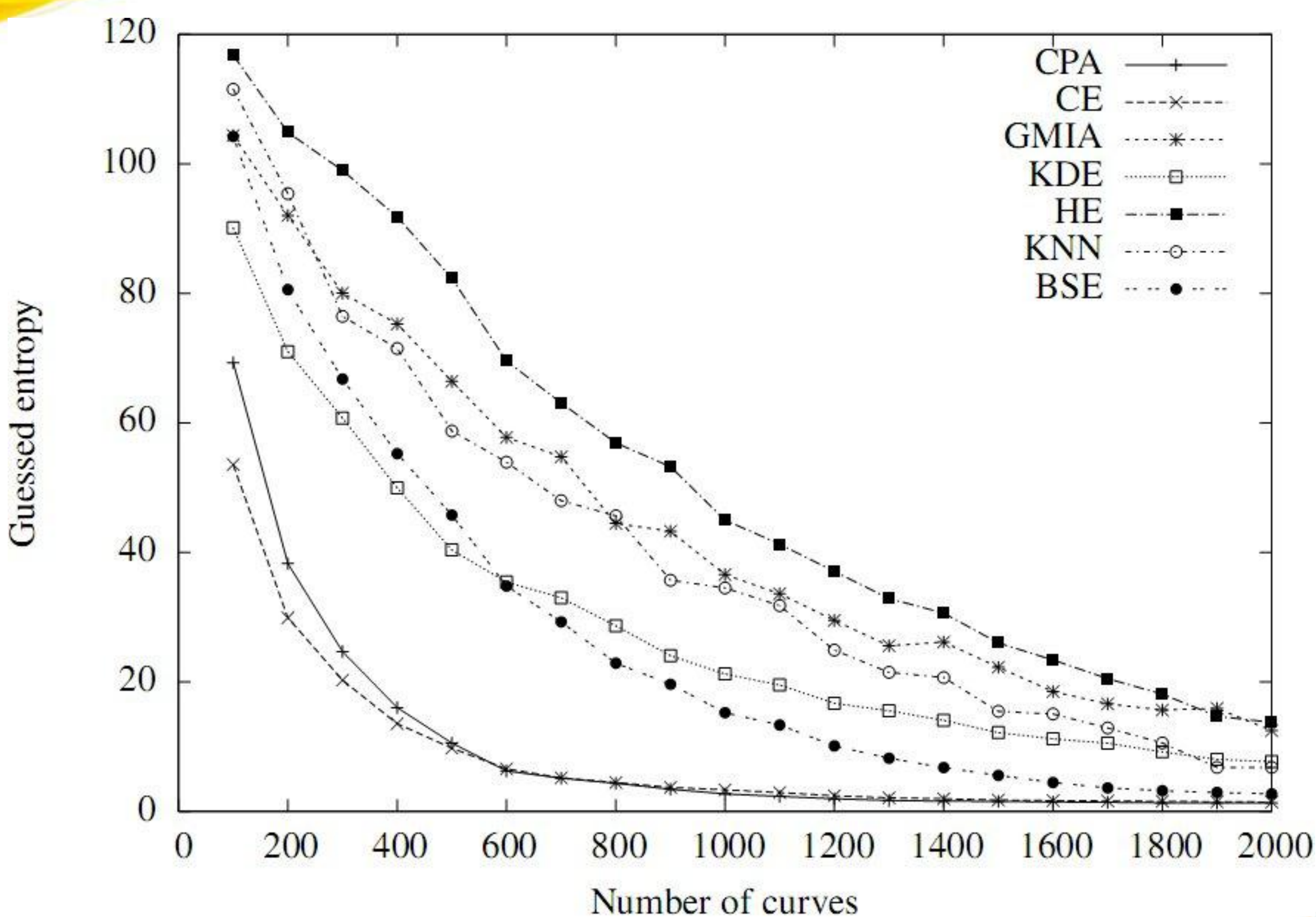


Estimation à base de fonctions B-splines



Expérimentations

Multiplication multi-précision sur AVR 8-bit



Conclusion et contributions

Partie 1

- MIA + l'estimation efficace de densité de probabilité offre de bons résultats
- L'estimation non-paramétrique a un sens dans le contexte des attaques différentielles

- *A. Venelli : Analysis of Nonparametric Estimation Methods for Mutual Information Analysis. A paraître dans ICISC 2010, 2010*
- *A. Venelli : Efficient Entropy Estimation for Mutual Information Analysis using B-splines. WISTP 2010, LNCS, 6033:17 -- 30, 2010*
- *A. Venelli : Techniques d'estimation d'entropie efficaces pour l'attaque par analyse d'information mutuelle. Soumis à la revue Technique et Science Informatiques (TSI), 2010*

Sommaire

Rappels sur AES

- Algorithme de chiffrement par blocs.
- Trois tailles de clés : 128, 192, 256 bits
- Un tour est constitué des opérations :
  - AddRoundKey
  - SubBytes
  - ShiftRows
  - MixColumns
- On travaille dans $GF(2^8)$
- SubBytes = inverse dans $GF(2^8)$ et transformation affine

- Problème : on veut masquer aléatoirement une valeur v tel que si en entrée d'inverse on a $v + r_1$ on obtienne $v^{-1} + r_2$ en sortie

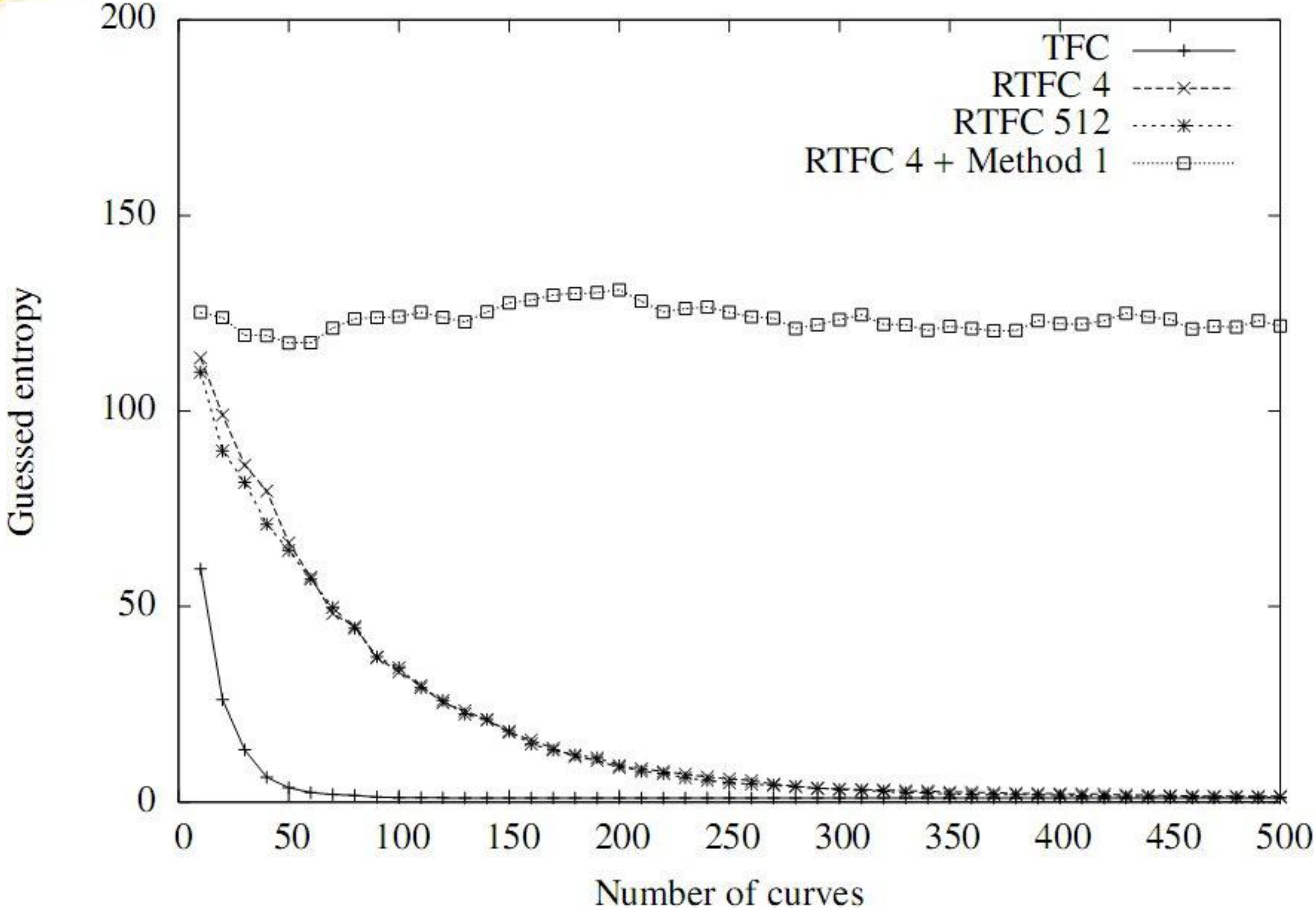
Proposition de contre-mesure DPA pour AES

- Inversion dans un sous-corps
  - Calcul d'inverse dans $GF(2^4) \rightarrow$ plus rapide
  - Inverse de la norme d'un élément de $GF(2^4) \times GF(2^4)$

- 1) Choisir au hasard la représentation du corps pour calculer l'inverse
  - Utilisation de différents polynômes, différents éléments primitifs
  - La norme d'un élément ne prend, au maximum, que 4 valeurs distinctes

- 2) Augmenter le nombre de représentations de la norme
  - Relation entre la norme d'un élément dans $GF(2^4)$ et son ordre dans $GF(2^8)$
  - Modification de l'ordre pour un faible sûrcout mémoire/complexité

Expérimentations



Conclusion et contributions

Partie 2

- Contre-mesure pour un AES adapté au hardware
- Accompagnée d'un masquage booléen, on améliore la résistance aux attaques différentielles de premier ordre

- *A. Bonnecaze, P. Liardet et A. Venelli : AES Side-Channel Countermeasure using Random Tower Fields Constructions. Soumis au journal DCC Janvier 2011.*

Sommaire

1. Attaques par canaux cachés et information mutuelle
2. Protéger l'AES
3. Protéger la multiplication scalaire sur courbes elliptiques
4. Attaques physiques sur des cryptosystèmes à base de couplages
5. Conclusion et perspectives

Courbes elliptiques

- Courbes elliptiques sous forme de Weierstrass simplifiée comme spécifié dans les normes internationales (FIPS, ANSI, SEC, …)
  - Sur $GF(p)$, cardinal du groupe de point premier
  - Sur $GF(2^n)$, cofacteur égal à 2 ou 4

- Courbe elliptique définie sur un corps de grande caractéristique :
  $E: y^2 = x^3 + ax + b, avec\ a, b \in GF(p), 4a^3 + 27b^2 \neq 0, p > 3$

- Soit $P_1 = (x_1, y_1), P_2 = (x_2, y_2), P_3 = (x_3, y_3) \in E$
- Doublement de point (ECDBL) : $P_3 = 2P_1$
- Addition de points (ECADD) : $P_3 = P_1 + P_2\ (P_1 \neq P_2)$

Addition « simplifiée »

- Aussi appelée addition co-Z
- Soit $P_1 = (X_1, Y_1, \boxed{Z}), P_2 = (X_2, Y_2, \boxed{Z}) \in E$

$$\boxed{ZADDU(P_1, P_2) \rightarrow \left(\widetilde{P_1}, P_1 + P_2\right) \text{ avec } Z_{\tilde{P}_1} = Z_{P_1+P_2}}$$

- Sur $GF(p)$, coordonnées projectives jacobiennes :
  - ZADDU = 5M+2S (Méloni 2007)
- Sur $GF(2^n)$, coordonnées projectives jacobiennes :
  - ZADDU = 7M+2S (Venelli et Dassance 2010)
- Ne peut pas être utilisé tel quel dans un algorithme de multiplication scalaire

Familles d'attaques par canaux cachés

- **Attaques par analyse simple**
  L'attaquant observe un canal caché du composant lors d'un calcul cryptographique et retrouve la clé secrète

- **Attaques par analyse différentielle**
  L'attaquant observe plusieurs courbes du canal caché et retrouve le secret à l'aide d'outils statistiques

- **Attaques par injection de faute**
  L'attaquant utilise des résultats de calculs corrects, des résultats faux dus à une injection de faute et l'endroit précis où la faute a été effectuée pour retrouver le secret

SPA sur ECC

Algorithme 2: *Left-to-right* doublement-et-addition

Entrées : $P \in E$ et $k = (k_{n-1} \dots k_1 k_0)_2$
Sorties : $[k]P \in E$

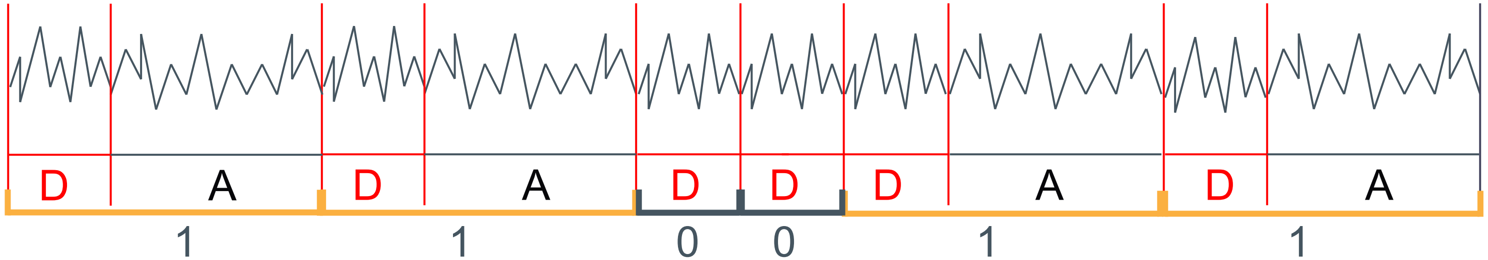
```
P_0 ← O
P_1 ← P
pour i ← n − 1 a 0 faire
    P_0 ← [2]P_0            ECDBL
    si k_i = 1 alors         ECADD
        P_0 ← P_0 + P_1
retourner P_0
```

Consommation de courant des opérations ECC

- ECDBL

- ECADD

Ex : $51P = (110011)_2 P$



Contre-mesures SPA

- Rendre ECADD et ECDBL indistinguables
  - Formules unifiées pour les courbes sous forme de Weierstrass simplifiée : très coûteuses
  - Utiliser des familles de courbes spécifiques (Jacobi, Hesse, Edwards, Huff) : pas utilisable pour les courbes définies sur $GF(p)$

- Utiliser un algorithme de multiplication scalaire régulier
  - Doublement-et-toujours-addition (Coron 1999)
  - Doublement-et-addition atomique (Chevallier-Mames et al. 2004)
  - Chaînes d'addition Euclidiennes (Méloni 2007)
  - Echelle de Montgomery (Montgomery 1987, Brier et Joye 2002)
  - Doublement-et-addition de Joye (Joye 2007)

Doublement-et-toujours-addition

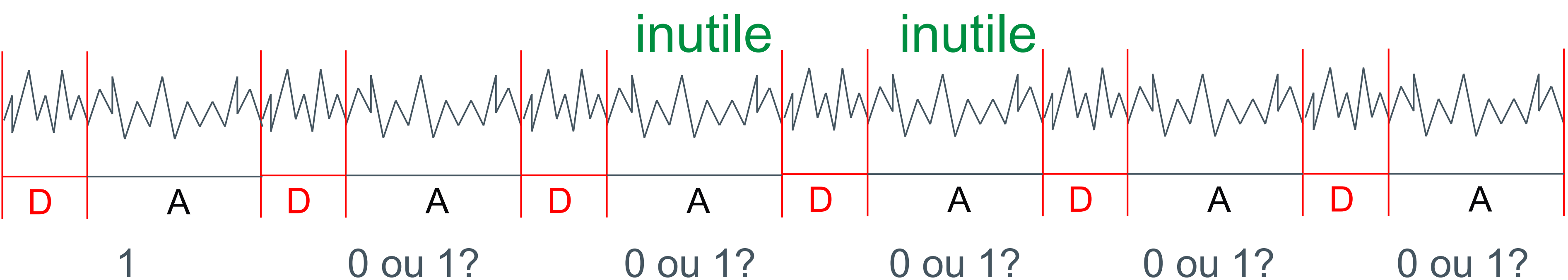
Algorithme 7: Doublement-et-toujours-addition

Entrées : $P \in E$ et $k = (k_{n-1} \dots k_1 k_0)_2$
Sorties : $[k]P \in E$

$P_0 \leftarrow \mathcal{O}$
$P_1 \leftarrow P$
pour $i \leftarrow n-1$ **a** 0 **faire**
  $\boxed{P_0 \leftarrow [2]P_0}$ ECDBL
  $\boxed{P_1 \leftarrow P_0 + P}$ ECADD
  $P_0 \leftarrow P_{k_i}$
retourner P_0

Ex :

$$51P = (110011)_2 P$$



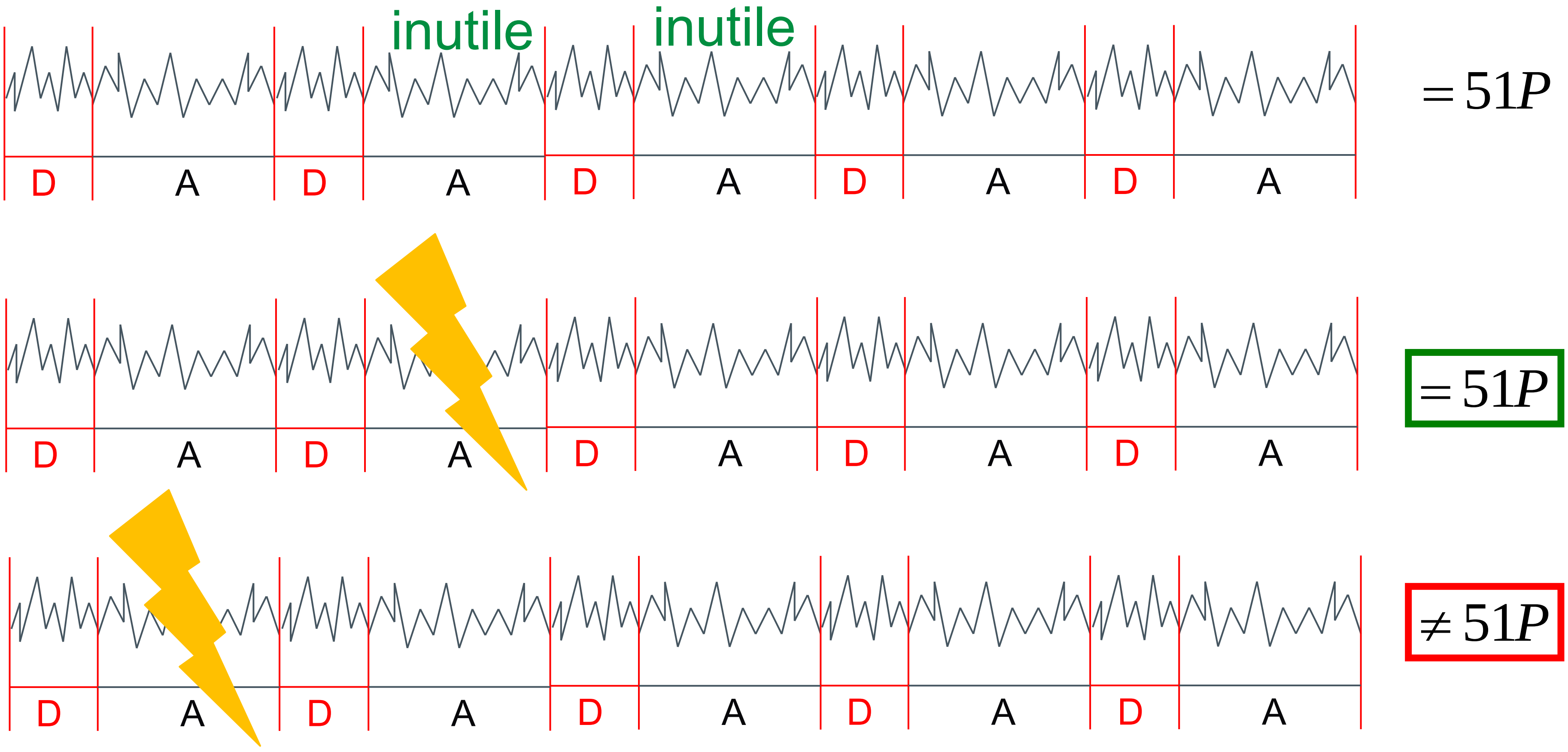
Familles d’attaques par canaux cachés

- **Attaques par analyse simple de courant (SPA)**
  L’attaquant observe la consommation de courant du composant lors d’un calcul cryptographique et retrouve la clé secrète

- **Attaques par analyse différentielle de courant (DPA)**
  L’attaquant observe plusieurs courbes de consommation et retrouve le secret à l’aide d’outils statistiques

- **Attaques par injection de faute (FA)**
  L’attaquant utilise des résultats de calculs corrects, des résultats faux dus à une injection de faute et l’endroit précis où la faute a été effectuée pour retrouver le secret

Résistant aux SPA mais pas aux FA



Contre-mesures FA

- Vérifier que le point, résultat de la multiplication, est *valide* :
  - P n'est pas le point à l'infini
  - Les coordonnées de P sont bien des éléments du corps de base
  - P satisfait à l'équation de la courbe
  - Vérifier $nP = \infty$ avec n le cardinal du sous-groupe premier utilisé

- Faire en sorte que tous les résultats intermédiaires soient utilisés pour le calcul du résultat final
  - faute injectée → résultat faux <u>dans tous les cas</u>
  - dépend de l'algorithme choisi

Echelle de Montgomery

Algorithme

Algorithme 9: Échelle de Montgomery

Entrées : $P \in E$ et $k = (k_{n-1} \ldots k_1 k_0)_2$

Sorties : $[k]P \in E$

$P_0 \leftarrow \mathcal{O}$

$P_1 \leftarrow P$

pour $i \leftarrow n - 1$ **a** 0 **faire**

- $P_{\bar{k_i}} \leftarrow P_{\bar{k_i}} + P_{k_i}$
- $P_{k_i} \leftarrow [2]P_{k_i}$

retourner P_0

Echelle de Montgomery

Principe

Tour i

[k]P

[k+1]P

ECDBL

x2

ECADD

+

Tour i+1

[2k]P

[2k+1]P

bit = 0

[2k+2]P

Proposition

(Venelli et Dassance, Geocrypt 2009)

- Combiner l'échelle de Montgomery avec l'addition co-Z (ZADDU) pour obtenir un algorithme résistant et efficace

- Problème :
  - L'échelle de Montgomery effectue un ECDBL à chaque tour
  - Le tour suivant, si on utilise ZADDU, il faut que les coordonnées Z des deux points soient égales
  - Modifier la sortie de ECDBL en conséquence est beaucoup trop coûteux

- Solution : supprimer ECDBL, n'utiliser que des additions

Echelle de Montgomery modifiée

Algorithme

Algorithme 11: Échelle de Montgomery avec additions

Entrées : $P \in E$ et $k = (k_{n-1} \dots k_1 k_0)_2$

Sorties : $[k]P \in E$

$P_0 \leftarrow \mathcal{O}$

$P_1 \leftarrow P$

pour $i \leftarrow n-1$ **a** 0 **faire**

  $P_0 \leftarrow P_0 + P_1$

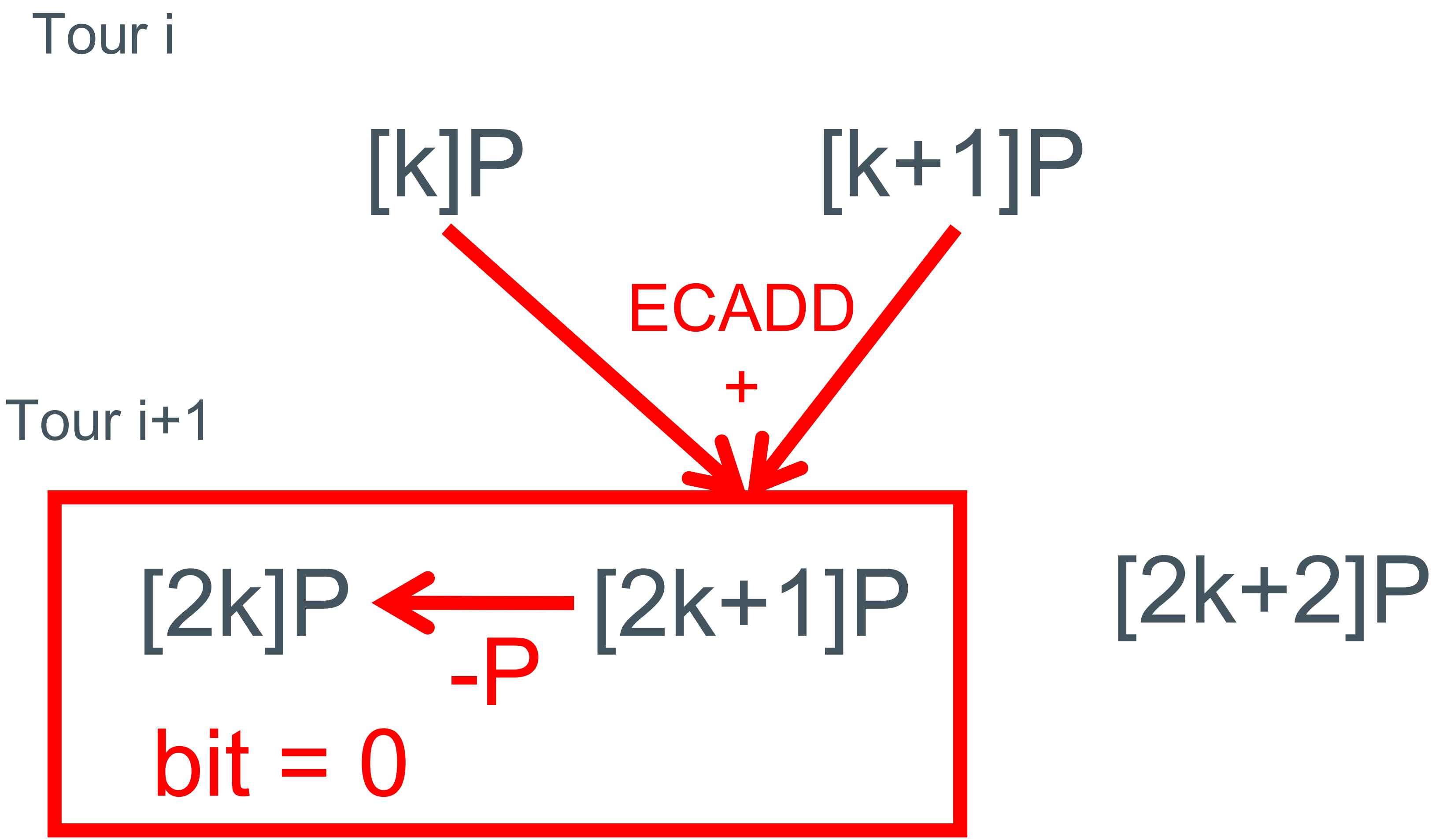
  $P_1 \leftarrow P_0 + (-1)^{\bar{k}_i} P$

retourner P_1

inside SECURE

Echelle de Montgomery modifiée

Principe



Proposition d'algorithme 1

Algorithme 12: Échelle de Montgomery avec ZADDC

Entrées : $P \in E$ et $k = (k_{n-1} \dots k_1 k_0)_2$

Sorties : $[k]P \in E$

$P_0 \leftarrow [2]P$

$P_1 \leftarrow P$

// On suppose $Z_{P_0} = Z_{P_1}$

pour $i \leftarrow n-2$ **a** 0 **faire**

- $(Q_0, Q_1, Q_2) \leftarrow \mathtt{ZADDC}(P_{k_i}, P_{\bar{k}_i})$
- $P_{\bar{k}_i} \leftarrow Q_1$ /* $P_{\bar{k}_i} \leftarrow (P_0 + P_1)$ */
- $P_{k_i} \leftarrow Q_2$ /* $P_{k_i} \leftarrow (P_{k_i} - P_{\bar{k}_i}) = \pm P$ */
- $(Q_0, Q_1, Q_2) \leftarrow \mathtt{ZADDC}(P_{\bar{k}_i}, P_{k_i})$
- $P_{k_i} \leftarrow Q_0$ /* $P_{k_i} \leftarrow \tilde{P}_{\bar{k}_i}$ */
- $P_{\bar{k}_i} \leftarrow Q_1$ /* $P_{\bar{k}_i} \leftarrow P_0 + P_1$ */

retourner P_1

Un travail équivalent à cette proposition a été publié par Goundar et al. dans CHES 2010 sur $GF(p)$

Proposition d'algorithme 2

- Uniquement sur un corps de grande caractéristique
- On peut **ne pas** calculer la coordonnée Z tout au long de l'algorithme
- La coordonnée Z du point final est recalculée lors du dernier tour de l'algorithme pour un coût de 5M+1I
- Les complexités des algorithmes ZADDU et ZADDC deviennent :
  - ZADDUwoZ = 4M+2S
  - ZADDCwoZ = 5M+3S

Comparaison de performances

$GF(2^n)$

Algorithmes	Complexités
ML Basique	16M+9S ≈ 25M
ML X-only	6M+5S ≈ 11M
D&A + Edwards	27M+3S ≈ 30M
D&A + Huff	22,5M+4,5S ≈ 27M
ML + ZADDC + ZADDU (Prop. 1)	**18M+4S ≈ 22M**

$GF(p)$

Algorithmes	Complexités
ML Basique	12M+13S ≈ 25M
ML X-only	9M+7S≈ 16M
ML + ZADDU + ZADDC (Prop. 1)	**11M+5S ≈ 16M**
ML + ZADDUwoZ + ZADDCwoZ (Prop. 2)	**9M+5S ≈ 14M**

Conclusion et contributions

Partie 3

- Sur $GF(p)$, Proposition 2 est l'algorithme le plus efficace en considérant ce niveau de sécurité et pour toute courbe elliptique
- Sur $GF(2^n)$, Proposition 1 alternative à ML X-Only brevetée

- *A. Venelli et F. Dassance : Fast Scalar Multiplication for Elliptic Curve Cryptosystems over Prime Fields. Brevet (20100040225), 2010*
- *A. Venelli et F. Dassance : Faster Side-Channel Resistant Elliptic Curve Scalar Multiplication. Arithmetic, Geometry, Cryptography and Coding Theory 2009, Contemporary Mathematics, 521:29--40, 2010*
- *A. Venelli et F. Dassance : Side-Channel Resistant Scalar Multiplication Algorithms over Finite Fields. In 5th Conf. on Network Architectures and Information Systems Security, 2010*

Sommaire

1. Attaques par canaux cachés et information mutuelle

2. Protéger l'AES

3. Protéger la multiplication scalaire sur courbes elliptiques

4. Attaques physiques sur des cryptosystèmes à base de couplages

5. Conclusion et perspectives

Couplages

- Définition d'un couplage
  - $e: G_1 \times G_2 \rightarrow G_T$
  - Propriété principale : $e(aP, bQ) = e(bP, aQ) = e(P, Q)^{ab}$

- Les couplages en cryptographie
  - Attaques ECC → MOV et FR
  - Protocoles cryptographiques → IBE, BLS, …

- Couplages sur cartes à puces
  - Récent (2005 - …)
  - Réaliste pour certains niveaux de sécurité, certains types de couplages

Calculer un couplage

Algorithme de Miller classique pour $e(P,Q)$

$$T \leftarrow P\ ,\ f \leftarrow 1$$

pour $i \leftarrow \lfloor \log(r) \rfloor - 1$ jusqu'à 0 faire:

$$f = f^2 . l_{T,T}(Q) / v_{2T}(Q)$$

$$T = 2T$$

si $r_i = 1$ alors:

$$f = f . l_{T,P}(Q) / v_{T+P}(Q)$$

$$T = T + P$$

finsi

finpour

$$f \leftarrow f^{(p^k - 1)/r}$$

Exponentiation finale

retourner f

Attaque DPA sur une implémentation classique

- Point P en coordonnées projectives, Q en affine
- Attaque lors du calcul de $l_{T,T}(Q)$ sur une multiplication dans un corps fini
- Si Q est secret
  - On retrouve facilement x_Q lors du calcul de $Z_P^2 x_q$ → on en déduit y_Q
- Si P est secret
  - Résultat Whelan et Scott 2006 : si P est secret, l'algorithme est résistant
  - On retrouve d'abord Z_P, puis on retrouve Y_P → on en déduit X_P
  - Réalisation et confirmation de l'attaque sur composant

Conclusion et contributions

Partie 4

- Mise en évidence d'une attaque différentielle même lorsque le secret est le point P
  - Travail en collaboration avec Nadia El Mrabet et Victor Lomné

- Développement d'une mini librairie crypto C et assembleur AVR 8-bit pour la réalisation de l'attaque

- *A. Venelli : Yet Another Crypto Library (YACL), 2010. http://code.google.com/p/yacl/*

Sommaire

1. Attaques par canaux cachés et information mutuelle
2. Protéger l'AES
3. Protéger la multiplication scalaire sur courbes elliptiques
4. Attaques physiques sur des cryptosystèmes à base de couplages
5. Conclusion et perspectives

Conclusion et perspectives

- Attaques physiques d'ordre supérieur
- Attaques physiques combinées
- Etudier l'arithmétique de base
- Etudier au niveau hardware
- Améliorer la multiplication scalaire sur courbes elliptiques définies sur $GF(2^n)$
- Implémenter des couplages sur carte à puce sans hardware particulièrement dédié
- Approfondir les attaques physiques sur couplages

Merci de votre attention