



**HAL**  
open science

# État Des Lieux Attaques Passives Courbes Elliptiques

Jean-Marc Robert

► **To cite this version:**

Jean-Marc Robert. État Des Lieux Attaques Passives Courbes Elliptiques. EJCIM: École Jeunes Chercheurs en Informatique Mathématique, Apr 2013, Perpignan, France. , 2013. lirmm-00862374

**HAL Id: lirmm-00862374**

**<https://hal-lirmm.ccsd.cnrs.fr/lirmm-00862374>**

Submitted on 16 Sep 2013

**HAL** is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

# Etat Des Lieux Attaques Passives Courbes Elliptiques

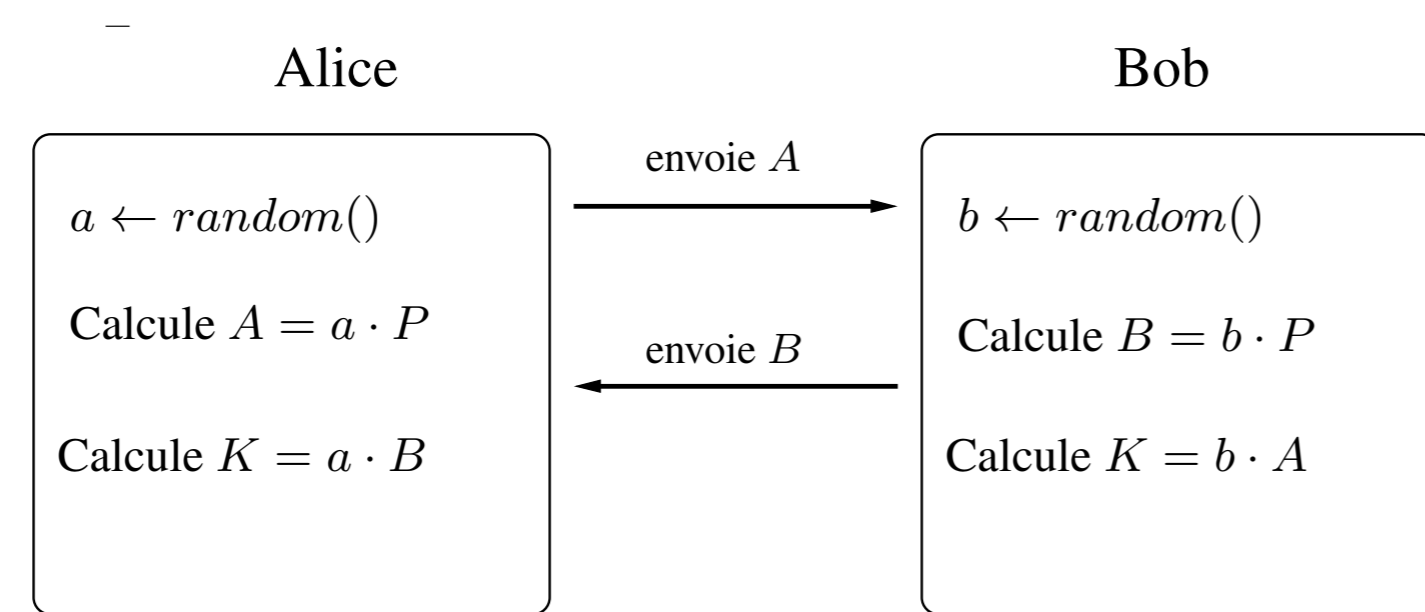
J.M. ROBERT<sup>1</sup>

<sup>1</sup>Team DALI/LIRMM, Université de Perpignan, France



## 1. ECC : Elliptic Curve Cryptography, échange de clé de Diffie-Hellmann

Alice et Bob s'accordent sur un groupe  $(G, +, \mathcal{O})$  et un point  $P$ , générateur du groupe.

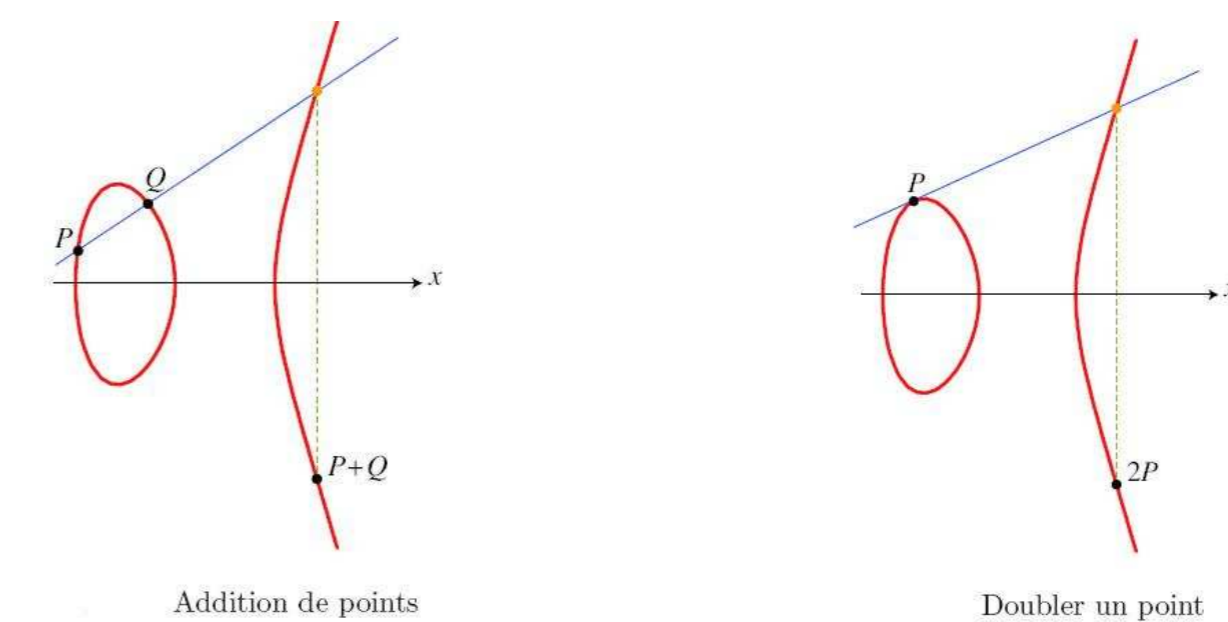


Clé secrète partagée  $K = a \cdot b \cdot P$

→ Le produit scalaire  $a \cdot P$  est la principale opération.

## 2. Le groupe choisi : l'ensemble des points d'une Courbe Elliptique sur $\mathbb{F}_{2^m}$ , muni de l'addition et d'un élément neutre

Exemples sur  $\mathbb{R}$  :



Notre courbe est sur  $\mathbb{F}_{2^m}$  (et non  $\mathbb{R}$ ) :  
 $E : Y^2 + XY = X^3 + aX^2 + b, \quad a, b \in \mathbb{F}_{2^m}$ .

- Les coordonnées des points appartiennent à  $\mathbb{F}_{2^m} = \mathbb{F}_2[x]/(f(x) \cdot \mathbb{F}_2[x])$
- Soit  $A = \sum_{i=0}^{m-1} a_i \cdot x^i$  et  $B = \sum_{i=0}^{m-1} b_i \cdot x^i, \quad a_i, b_i \in \{0, 1\}$

alors :  $A + B = \sum_{i=0}^{m-1} (a_i + b_i) \cdot x^i$ , et :  $A \times B = A \cdot B \pmod{f}$ .

## 3. Attaque SPA : Simple Power Analysis

Le produit scalaire  $k \cdot P$  est vulnérable :

**Require:**  $k = (k_{t-1}, \dots, k_1, k_0), P \in E(\mathbb{F}_q)$

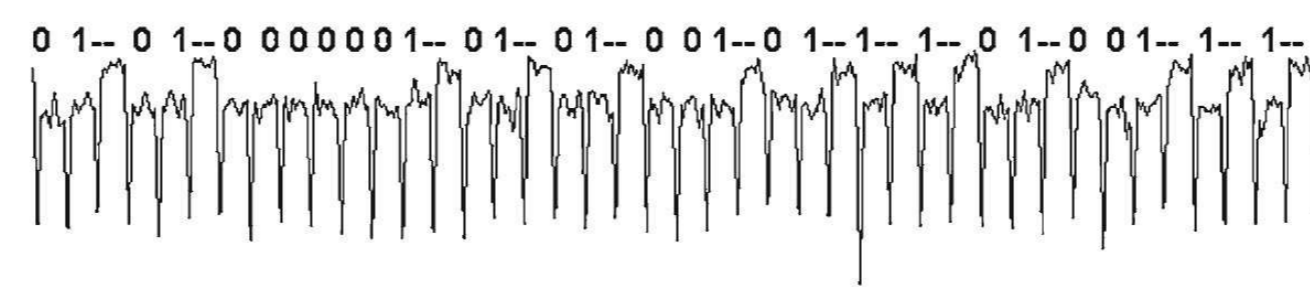
**Ensure:**  $Q = k \cdot P$

- $Q \leftarrow \mathcal{O}$
- for**  $i$  from  $t-1$  downto  $0$  **do**
- $Q \leftarrow 2 \cdot Q$
- if**  $k_i = 1$  **then**
- $Q \leftarrow Q + P$
- end if**
- end for**
- return**  $(Q)$

L-R double-and-add Elliptic Curve Scalar Multiplication (ECSM)

Cet algorithme n'est pas régulier : les opérations effectuées à chaque tour de boucle dépendent du scalaire utilisé comme exposant (on effectue l'addition de l'étape 5 uniquement si le bit de la représentation est 1).

Attaque SPA



Fuite d'information par Simple Power Analysis, exponentiation rapide RSA ( $\approx$  Double-And-Add), reproduite de [2], mesure de courant instantané sur carte à puce.

- tension mesurée aux bornes d'une résistance en série avec l'alimentation de la carte ;
  - Les pics sont les multiplications (additions) ;
  - les creux sont les élévations au carré (doublements) ;
- L'attaquant peut donc reconstituer la clé secrète (l'exposant de l'exponentiation rapide) par un simple examen de la trace de consommation de courant instantanée !

Exemple de contre-mesure : Montgomery

**Require:**  $k = (k_{t-1}, \dots, k_1, k_0)$  with  $k_{t-1} = 1, P \in E(\mathbb{F}_q)$

**Ensure:**  $Q = k \cdot P$

- $Q_0 \leftarrow P, Q_1 \leftarrow 2P$
- for**  $i$  from  $t-2$  downto  $0$  **do**
- if**  $(k_i = 0)$  **then**
- $Q_1 \leftarrow Q_0 + Q_1, Q_0 \leftarrow 2 \cdot Q_0$
- else**
- $Q_0 \leftarrow Q_0 + Q_1, Q_1 \leftarrow 2 \cdot Q_1$
- end if**
- end for**
- return**  $(Q_0)$

Basic Montgomery's ladder ECSM

Cet algorithme est régulier : on effectue un addition et un doublement à chaque tour de boucle.

## 4. Attaque DPA : Differential Power Analysis

Description de l'attaque DPA

Cette attaque va contourner les principales contre-mesures précédentes. L'attaque nécessite de la part de l'adversaire :

- la mesure de la puissance consommée lors de  $m$  calculs d'ECSM  $\mathbf{T}_{1..m}[j]$  ;
- La connaissance du point de base utilisé  $P_1, P_2, \dots, P_m$  lors des  $m$  calculs.

L'attaquant procède comme suit :

- il calcule les  $4 \cdot P_i$  et sélectionne le bit  $s$  de chaque résultat ;

- il calcule la différentielle suivante ( $D(P_i, s) = \text{valeur du bit } s \text{ de } 4 \cdot P_i$ ) :

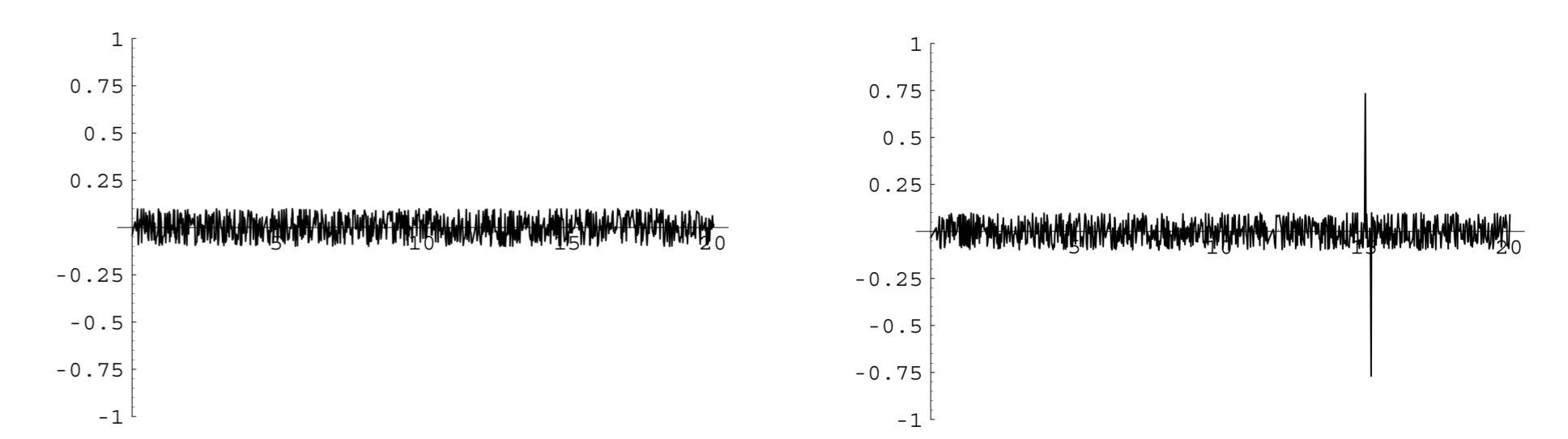
$$\Delta_D[j] = \frac{\sum_{i=1}^m D(P_i, s) \cdot \mathbf{T}_i[j]}{\sum_{i=1}^m D(P_i, s)} - \frac{\sum_{i=1}^m (1 - D(P_i, s)) \cdot \mathbf{T}_i[j]}{\sum_{i=1}^m (1 - D(P_i, s))}$$

$$\approx 2 \cdot \left( \frac{\sum_{i=1}^m D(P_i, s) \cdot \mathbf{T}_i[j]}{\sum_{i=1}^m D(P_i, s)} - \frac{\sum_{i=1}^m \mathbf{T}_i[j]}{m} \right)$$

↔ L'attaquant joue aux devinettes :

- si  $4 \cdot P$  n'est pas calculé,  $\Delta_D[j] = 0$  au bruit près ;
- si  $4 \cdot P$  est calculé,  $\Delta_D[j]$  va présenter un pic à l'instant où le calcul traite le bit  $s$ .

En pratique, avec environ mille traces de consommation de puissance (carte à puce, tiré de Coron dans [1]) :



↔ À gauche : pari perdu,  $4 \cdot P$  n'est pas calculé ;  
 ↔ à droite : c'est gagné !

## 5. Efficacité de l'attaque DPA :

tour $i$ :				$i = l-2$	$i = l-3$
$k_{i-1} = 1$	$k_{i-2}$	$k_{i-3}$	...	$Q$	$Q$
1	0	0	...	$2P$	$4P$
1	0	1	...	$2P$	$4P + P = 5P$
1	1	0	...	$3P$	$6P$
1	1	1	...	$3P$	$6 \cdot P + P = 7P$

Premiers tours de boucle de l'algorithme L-R Double-and-Add pour l'ECSM :

↔  $4 \cdot P$  n'est calculé que pour  $k_{l-2} = 0$ .

tour $i$ :				$i = l-2$	$i = l-3$
$k_{l-1} = 1$	$k_{l-2}$	$k_{l-3}$	...	$Q_0$	$Q_1$
1	0	0	...	$2P$	$3P$
1	0	1	...	$2P$	$3P$
1	1	0	...	$3P$	$4P$
1	1	1	...	$3P$	$4P$

Premiers tours de boucle de l'algorithme échelle binaire de Montgomery pour l'ECSM :

↔  $5 \cdot P$  n'est calculé que pour  $k_{l-2} = 0$ .

## 6. Conclusion

- Contres-mesures classiques : randomization proposées par Coron dans [1]

1. Randomization of the private exponent : une courbe elliptique sur  $\mathbb{F}_{2^m}$  ou  $\mathbb{F}_q$  comporte un nombre fini de points, que l'on note  $\#\mathcal{E}$ , dont l'ordre divise  $\#\mathcal{E}$ .

$$Q = d \cdot P = (d + k \cdot \#\mathcal{E}) \cdot P, \forall k \in \mathbb{Z} \text{ (On a en effet : } \#\mathcal{E} \cdot P = \mathcal{O} \text{),}$$

2. Blinding the point  $P$  : ajouter un point aléatoire  $R$  au point de base  $P$  dont on connaît le multiple à l'avance  $S = d \cdot R$ .

↔ point utilisé dans l'opération  $P' = P + R$

↔ Variante :  $R \leftarrow (-1)^{b_2} R, \quad S \leftarrow (-1)^{b_2} S, \quad (b \text{ un bit aléatoire}).$

3. Randomized projective coordinates : pour un point en coordonnées affines  $(x, y)$ , on a une infinité de points  $(X, Y, Z)$  correspondants tels que  $(x = X/Z, y = Y/Z^2)$  en  $\mathcal{L}D$  projective.

- Travail en cours

- ▶ nouveaux algorithmes : Montgomery avec Halving et représentation signée du scalaire ;
- ▶ en prévision : implémentation sur FPGA (développement d'un cryptoprocresseur ECC).

## Références

[1] Jean-Sébastien Coron. Resistance against differential power analysis for elliptic curve cryptosystems. In CHES, pages 292–302, 1999.

[2] Paul C. Kocher, Joshua Jaffe, Benjamin Jun, and Pankaj Rohatgi. Introduction to differential power analysis. J. Cryptographic Engineering, 1(1):5–27, 2011.