Support logiciel robuste aux attaques passives et actives pour l'arithmétique de la cryptographie asymétrique sur des (très) petits cœurs de calcul

Audrey LUCAS

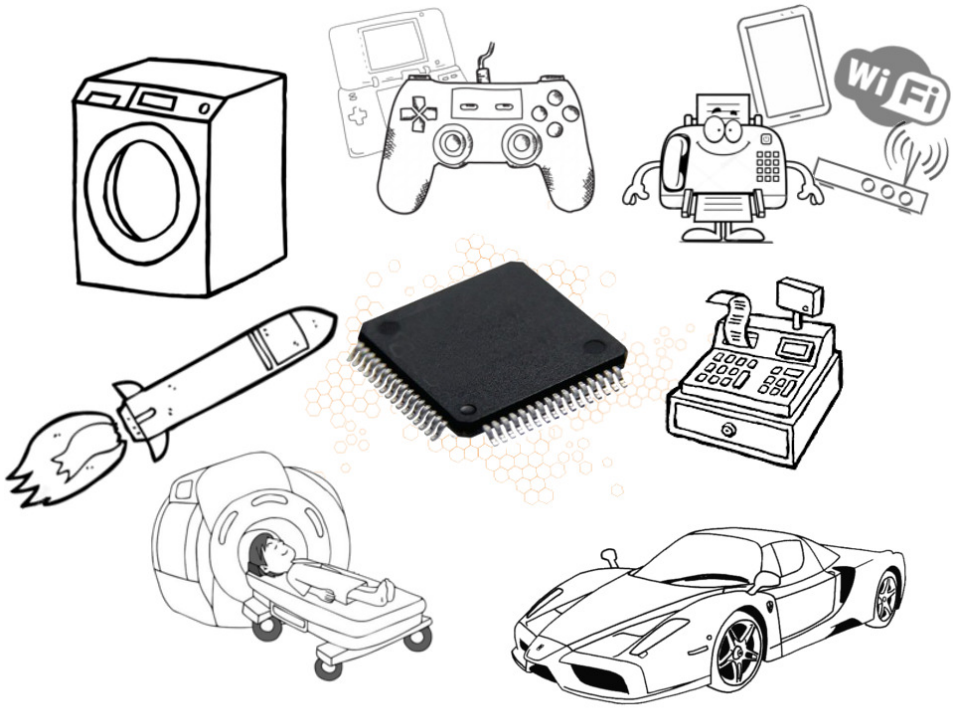
19 décembre 2019

Encadrant : Arnaud Tisserand


UMR IRISA
UNIVERSITÉ DE RENNES 1

Processeurs embarqués

Processeurs embarqués



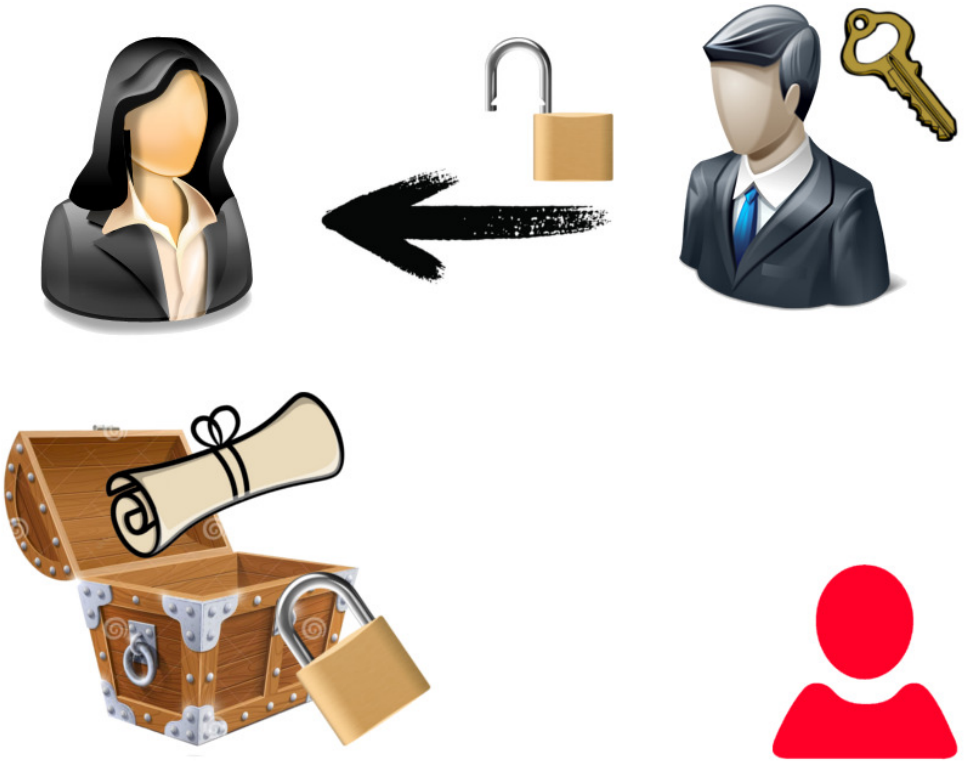
Omniprésents dans notre société

Présents dans des domaines **sensibles**

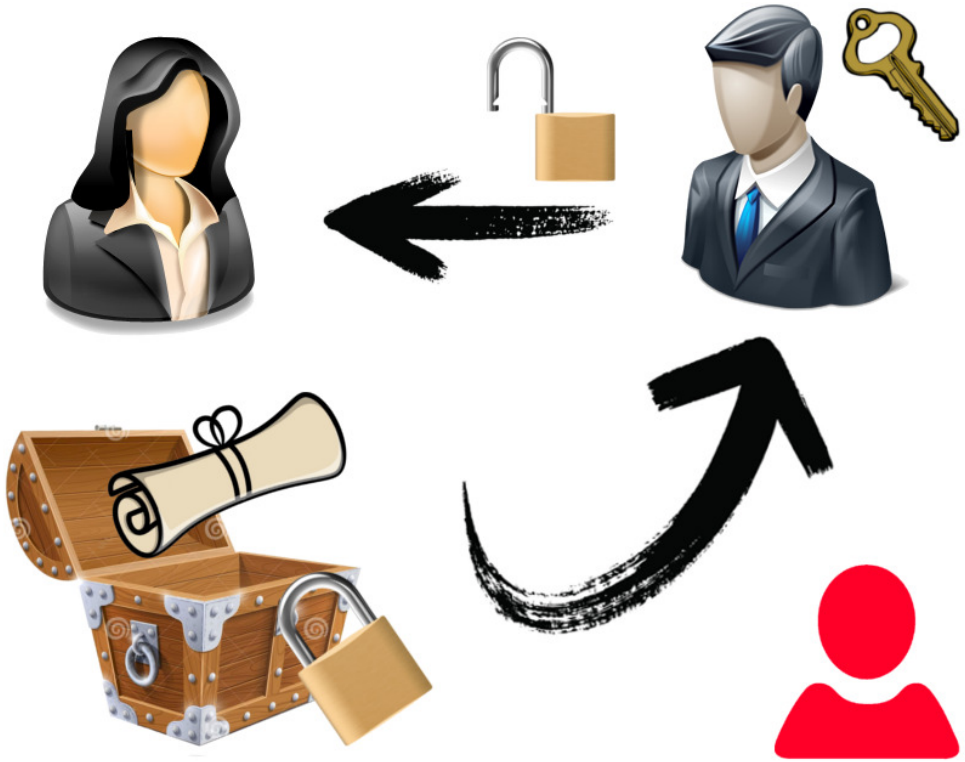
Cryptographie asymétrique

Cryptographie asymétrique

Cryptographie asymétrique

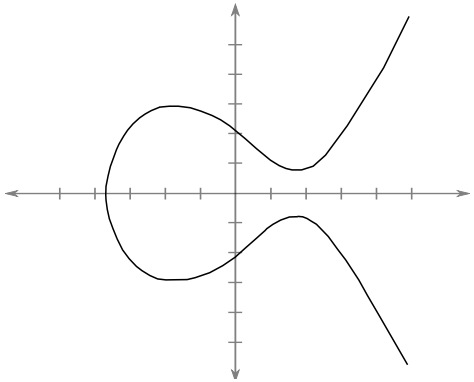


Cryptographie asymétrique

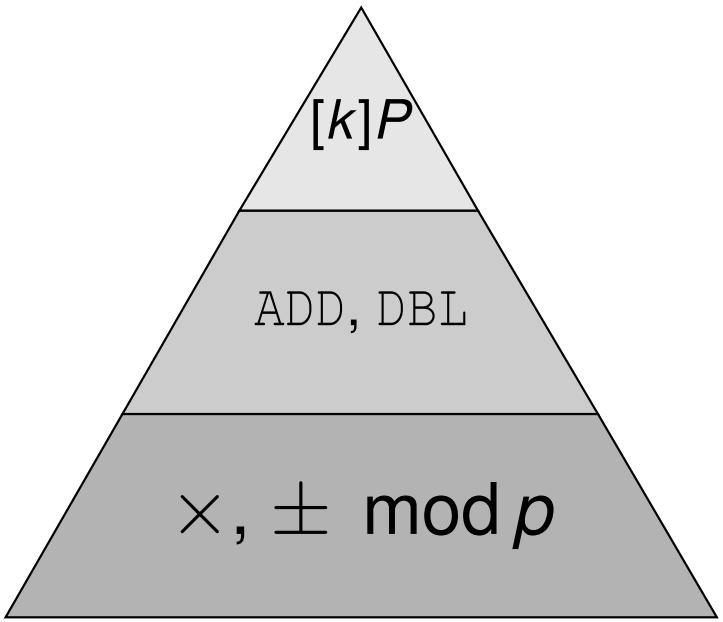


- 2 clés différentes par utilisateur : une clé publique et une clé privée
- 2 opérations : le **chiffrement** et le **déchiffrement**
- 1 secret : la clé privée !

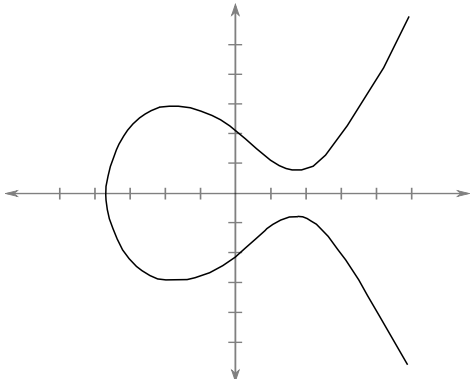
Cryptographie sur les courbes elliptiques (ECC) sur $\mathbb{F}_p$

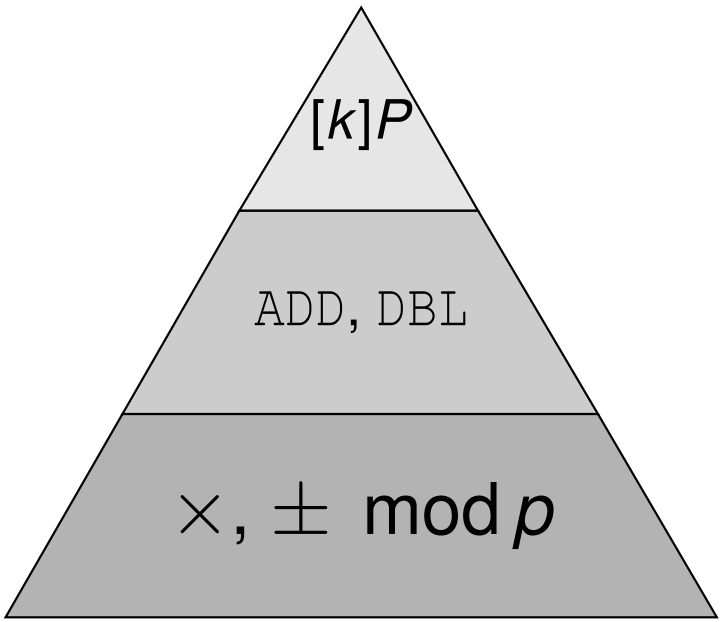


Équation de courbe
$E : y^2 = x^3 + ax + b$
avec a et b les paramètres



Cryptographie sur les courbes elliptiques (ECC) sur $\mathbb{F}_p$





Équation de courbe

$E : y^2 = x^3 + ax + b$

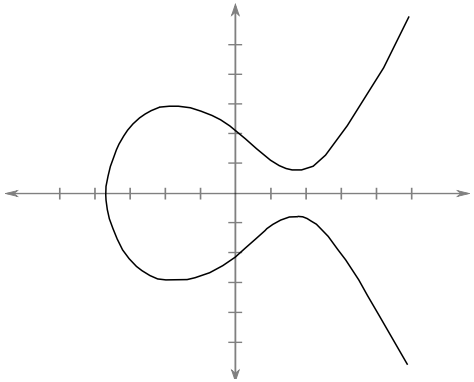
avec a et b les paramètres

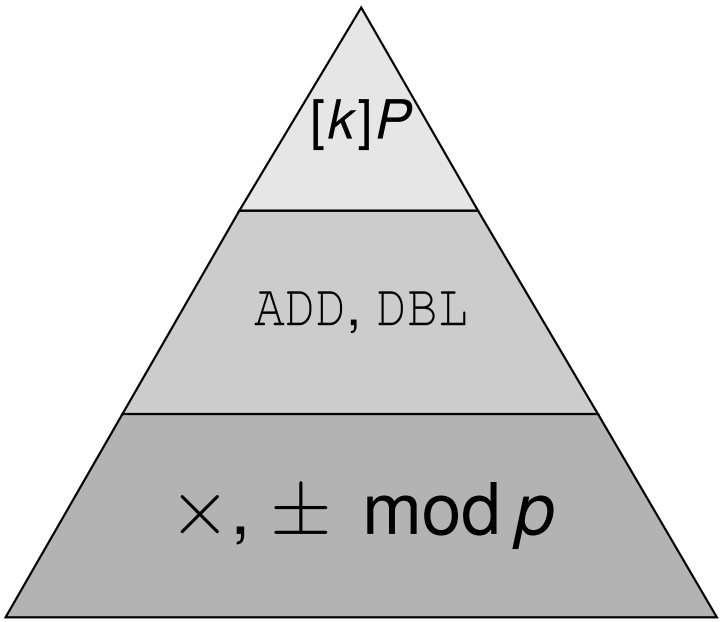
Multiplication scalaire (SM)

$$\Downarrow$$

$$[k]P = \underbrace{P + P + \ldots + P}_{k \text{ fois}}$$

Cryptographie sur les courbes elliptiques (ECC) sur $\mathbb{F}_p$





Équation de courbe

$E : y^2 = x^3 + ax + b$

avec a et b les paramètres

Multiplication scalaire (SM)

$$\Downarrow$$

$$[k]P = \underbrace{P + P + \ldots + P}_{k \text{ fois}}$$

Doublement de point : DBL

$$\neq$$

Addition de points : ADD

Exemple de SM

Doublement et addition - (DA)

Entrées : $P \in E$ et $k = (k_{m-1}, \ldots, k_0)_2 \in \mathbb{N}$

Résultat : $[k] \cdot P \in E$

$T \leftarrow O$

pour $i = m - 1$ **à** 0 **faire**

- $T \leftarrow 2 \cdot T$ DBL
- **si** $k_i = 1$ **alors**
  - $T \leftarrow T + P$ ADD

retourner T

Rappel : L'entier k peut être une **clé secrète**

Exemple de SM

Doublement et addition - (DA)

Entrées : $P \in E$ et $k = (k_{m-1}, \ldots, k_0)_2 \in \mathbb{N}$

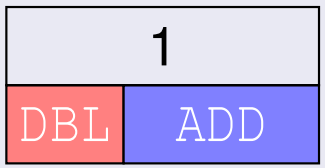
Résultat : $[k] \cdot P \in E$

$T \leftarrow O$

pour $i = m - 1$ **à** 0 **faire**

- $T \leftarrow 2 \cdot T$
- **si** $k_i = 1$ **alors**
  - $T \leftarrow T + P$

retourner T



Rappel : L'entier k peut être une **clé secrète**

Exemple de SM

Doublement et addition - (DA)

Entrées : $P \in E$ et $k = (k_{m-1}, \ldots, k_0)_2 \in \mathbb{N}$

Résultat : $[k] \cdot P \in E$

$T \leftarrow O$

pour $i = m - 1$ **à** 0 **faire**

- $T \leftarrow 2 \cdot T$ — DBL
- **si** $k_i = 1$ **alors**
  - $T \leftarrow T + P$ — ADD

retourner T

Rappel : L'entier k peut être une **clé secrète**

Exemple de SM

Doublement et addition - (DA)

Entrées : $P \in E$ et $k = (k_{m-1}, \ldots, k_0)_2 \in \mathbb{N}$

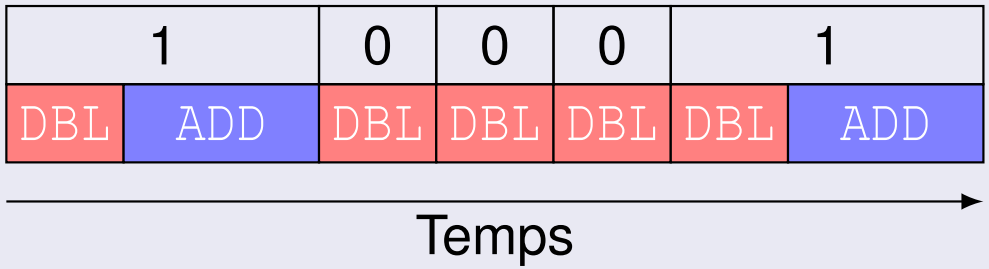
Résultat : $[k] \cdot P \in E$

$T \leftarrow O$

pour $i = m - 1$ **à** 0 **faire**

- $T \leftarrow 2 \cdot T$ — DBL
- **si** $k_i = 1$ **alors**
  - $T \leftarrow T + P$ — ADD

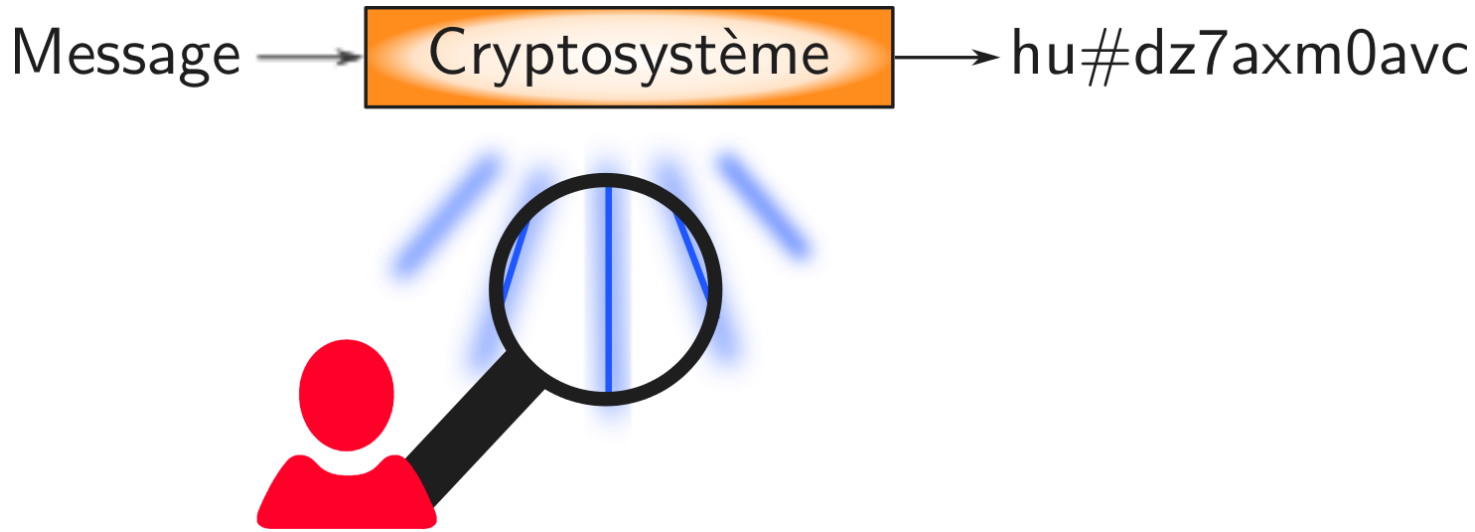
retourner T



Rappel : L'entier k peut être une **clé secrète**

Attaques par observation (SCA)

Déduction d'informations sensibles
en observant le comportement du circuit



Attaques par observation (SCA)

Déduction d'informations sensibles
en observant le comportement du circuit

Trace de consommation d'une SM

Analyse simple de consommation (SPA)

Attaques par observation (SCA)

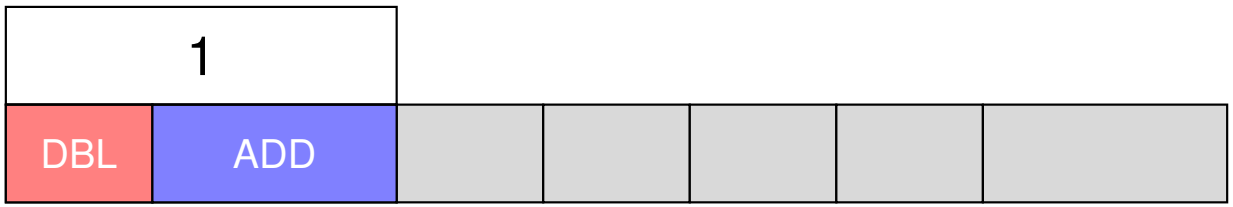
Déduction d'informations sensibles
en observant le comportement du circuit

Trace de consommation d'une SM

Analyse simple de consommation (SPA)

Attaques par observation (SCA)

Déduction d'informations sensibles
en observant le comportement du circuit

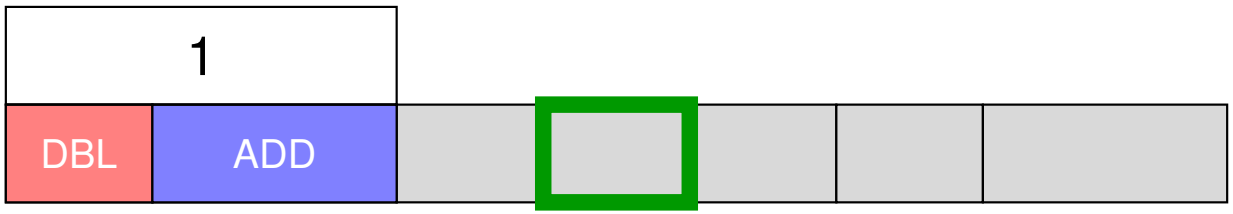


Trace de consommation d'une SM

Analyse simple de consommation (SPA)

Attaques par observation (SCA)

Déduction d'informations sensibles
en observant le comportement du circuit

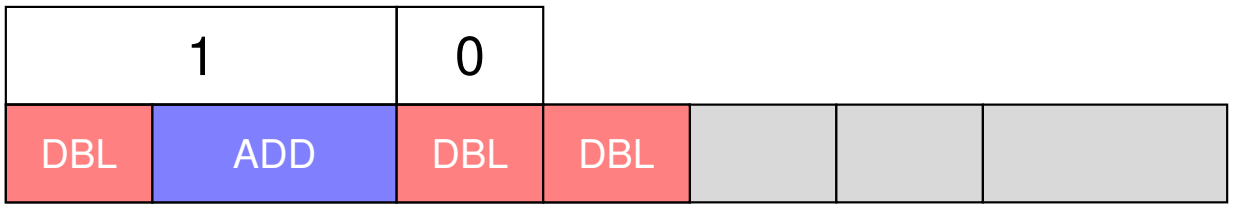


Trace de consommation d'une SM

Analyse simple de consommation (SPA)

Attaques par observation (SCA)

Déduction d'informations sensibles
en observant le comportement du circuit

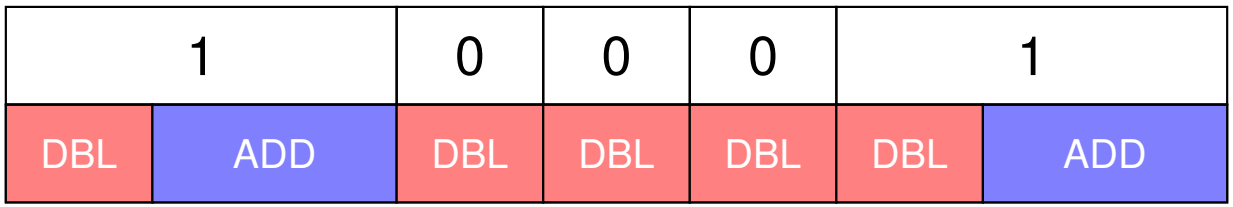


Trace de consommation d'une SM

Analyse simple de consommation (SPA)

Attaques par observation (SCA)

Déduction d'informations sensibles
en observant le comportement du circuit



Trace de consommation d'une SM

Analyse simple de consommation (SPA)

Protection SCA

Doublement et toujours addition - (DAA)

1		0		0		0		1	
DBL	ADD	DBL	ADD	DBL	ADD	DBL	ADD	DBL	ADD

Caractéristiques

- ADD est une `ADD` fictive
- La SM est régulière
- Protège contre l'attaque précédente

Protection SCA

Doublement et toujours addition - (DAA)

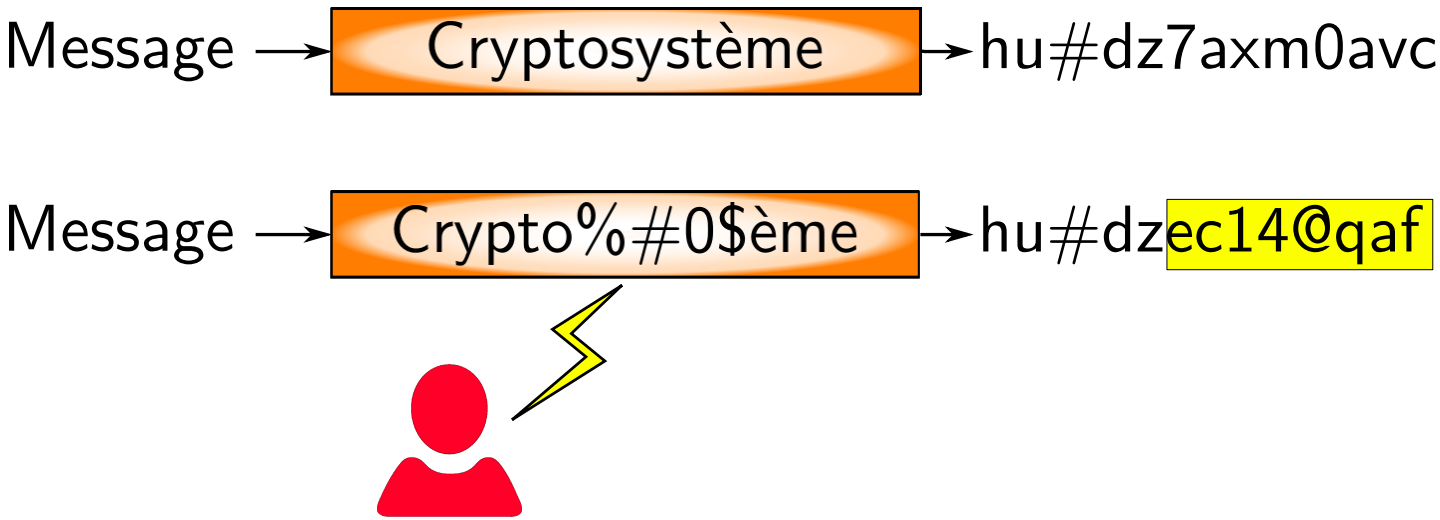
1		0		0		0		1	
DBL	ADD	DBL	ADD	DBL	ADD	DBL	ADD	DBL	ADD

Caractéristiques

- ADD est une `ADD` fictive
- La SM est régulière
- Protège contre l'attaque précédente
- MAIS ...

Attaques par perturbation (FA)

Déduction d'informations sensibles
en perturbant le circuit



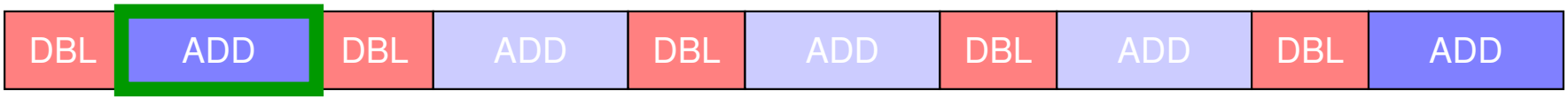
Attaques par perturbation (FA)

Déduction d'informations sensibles
en perturbant le circuit

Safe error

Attaques par perturbation (FA)

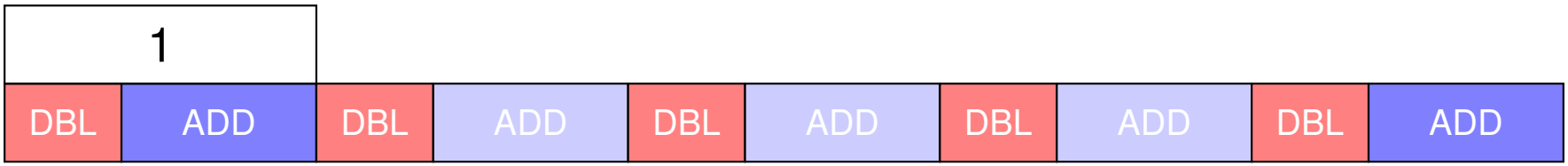
Déduction d'informations sensibles
en perturbant le circuit



Safe error

Attaques par perturbation (FA)

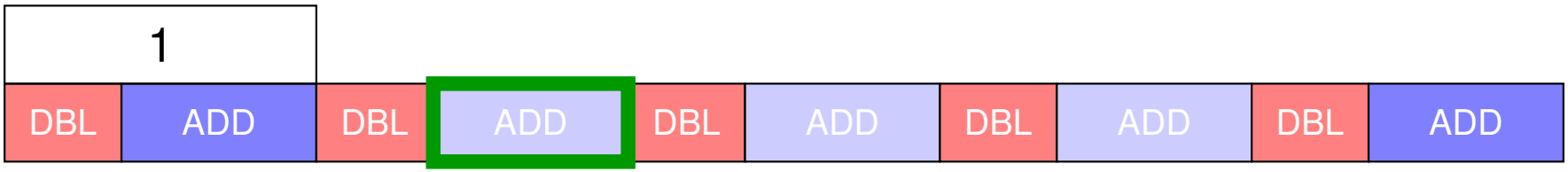
Déduction d'informations sensibles
en perturbant le circuit



Safe error

Attaques par perturbation (FA)

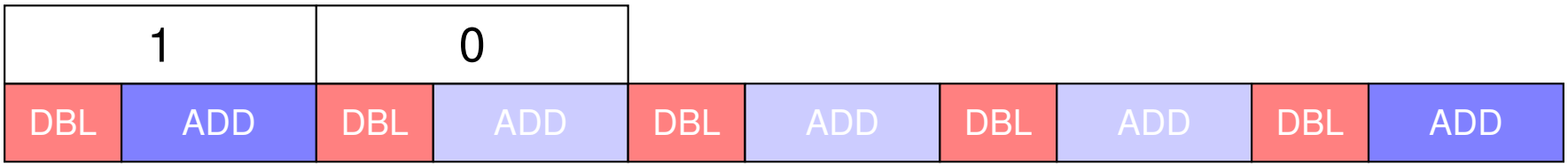
Déduction d'informations sensibles
en perturbant le circuit



Safe error

Attaques par perturbation (FA)

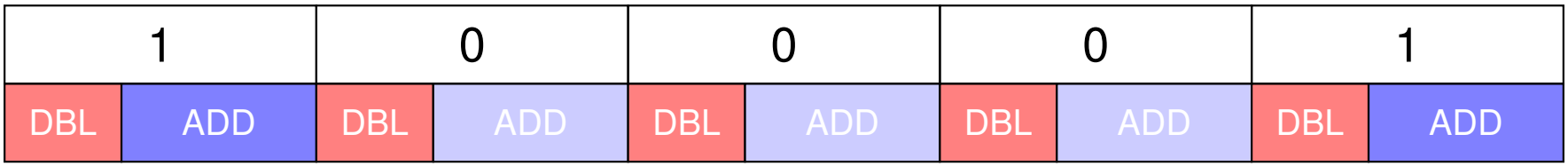
Déduction d'informations sensibles
en perturbant le circuit



Safe error

Attaques par perturbation (FA)

Déduction d'informations sensibles
en perturbant le circuit



Safe error

Problématique et contributions

Certaines protections contre un type d'attaque peuvent **rendre le système vulnérable** à l'autre type

Problématique et contributions

Certaines protections contre un type d'attaque peuvent **rendre le système vulnérable** à l'autre type

$\Downarrow$

Protéger les systèmes simultanément contre les FA et les SCA

Problématique et contributions

Certaines protections contre un type d'attaque peuvent **rendre le système vulnérable** à l'autre type

$\Downarrow$

Protéger les systèmes simultanément contre les FA et les SCA

Protections combinées

- Vérification de point (PV)
- Compteur d'itérations (IC)
- Réponse à une détection de faute

Contributions

Résistance aux SCA

$\Downarrow$

SM **régulière** $\Rightarrow$ Séquence d'opérations uniforme

Contributions

Résistance aux SCA

$\Downarrow$

SM **régulière** $\Rightarrow$ Séquence d'opérations uniforme

$\Rightarrow$ **Comportement uniforme?**

Contributions

Résistance aux SCA

$\Downarrow$

SM **régulière** $\Rightarrow$ Séquence d'opérations uniforme

$\Rightarrow$ **Comportement uniforme?**

Simulateur d'activité au niveau arithmétique

- Simulation d'une architecture matérielle
- Ordonnancement et monitoring des opérations
- Analyse des opérations
- Analyse de la SM avec différents niveaux de protection

Sommaire

Vérification de point (PV)

Principe :

- Vérifier que le point final/intermédiaire **est sur la courbe** [**?**]
- Les coordonnées du point, x et y, sont injectées dans $y^2 = x^3 + ax + b$

Vérification de point (PV)

Principe :

- Vérifier que le point final/intermédiaire **est sur la courbe** [**?**]
- Les coordonnées du point, x et y, sont injectées dans $y^2 = x^3 + ax + b$

Période de vérification :

- À la toute fin : vraiment peu coûteux mais détection tardive
- Toutes les d itérations : coût plus grand mais détection plus tôt
- **À chaque itération ($d = 1$) : coût important mais détection immédiate**

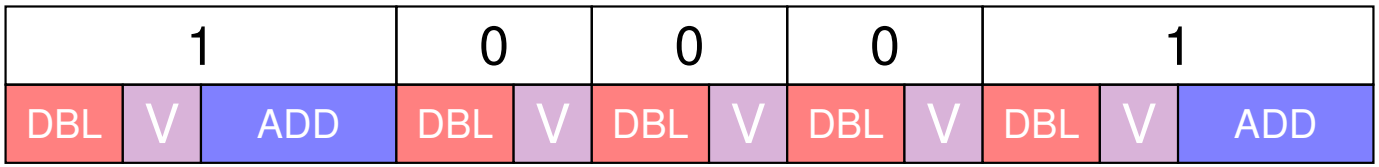
Sommaire

PV pour les courbes de Weierstrass

Objectif : **uniformiser**

la multiplication scalaire (SM)

$\Rightarrow$ **PV est ajoutée** à DBL



Les séquences d'opérations de ADD et de DBL V doivent être **indistinguables**

Nouvelle PV - Coordonnées projectives

Nouvelle vérification

Coût de ADD : $11M+6S+18A$

- **Multiplication** de V par Y et **inclusion** de V dans DBL
  $\Rightarrow$ Coût de : $13M+9S+19A+1\times b$
- **Factorisation** des calculs
  $\Rightarrow$ Coût : $11M+6S+18A+1\times b$
- Ajout de $1\times b$ à ADD (sans être une opération fictive)

Les coûts de ADD et DBL V sont égaux

Avoir le même coût n'est **pas suffisant**

ADD et DBL V doivent avoir

des **séquences d'opérations uniformes**

- **ré-ordonnancement** des séquences d'opérations

  $\Rightarrow$ ADD et DBL V ont alors la **même séquence d'opérations**

  $\Rightarrow$ SM **uniforme**

Ce qui est obtenu :

Une SM **régulière protégée des FA** visant les coordonnées des points et les paramètres de la courbe

Sommaire

PV pour les courbes de Montgomery

Coordonnées XZ

- Couramment utilisées car peu coûteuses
- $P = (x, z) \Rightarrow$ pas de coordonnée y

PV classique

La PV classique **ne permet pas** de vérifier directement l'équation de courbe :

$\rightarrow$ Vérification que $x^3 + ax^2 + x$ est un carré

$\rightarrow$ Avec le symbole de Legendre : $(x^3 + ax^2 + x)^{\frac{p-1}{2}}$
où la taille de $p \geq 256$ bits

$\Rightarrow$ **Trop coûteux !!**

L'échelle de Montgomery

Algorithme 1 : Échelle de Montgomery

Entrées : P et $k = (k_{m-1}, \ldots, k_0)_2$

Résultat : $[k] \cdot P$

1 $T_1 \leftarrow O, \quad T_2 \leftarrow P$

2 **pour** $i = m - 1$ **à** 0 **faire**

3 $\quad T_1, T_2 \leftarrow \text{cswap}(T_1, T_2, k_{i-1} \oplus k_i)$ // cswap interverti T_1 et T_2 si $k_{i-1} \oplus k_i = 1$

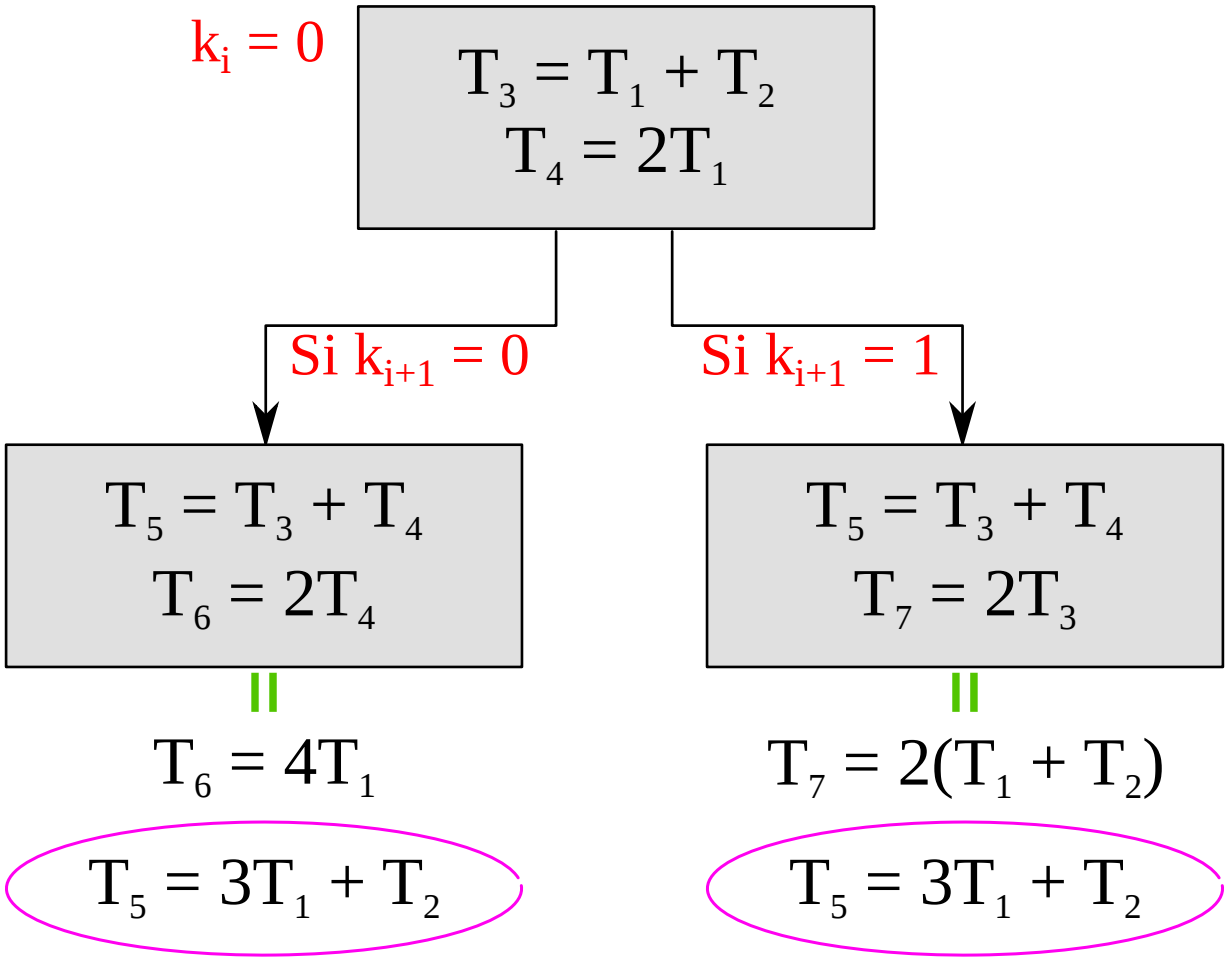
4 $\quad T_1 \leftarrow T_1 + T_2$

5 $\quad T_2 \leftarrow 2 \cdot T_2$

6 **retourner** T_1

- $T_2 - T_1 = P$ à chaque itération
- **Régulier** et naturellement **résistant** aux *safe-error*

Étape de l'échelle de Montgomery



Nouvelle PV

Constatations

Utilisation des égalités :

$$\begin{cases} T_5 + P &= 3T_1 + T_2 + T_2 - T_1 &= T_7 \\ T_5 - P &= 3T_1 + T_2 - T_2 + T_1 &= T_6 \end{cases}$$

Si perturbation $\Rightarrow$ alors pas d'égalité

- Calcul de $T_3, T_4, T_5, T_6, T_7, T_5 \pm P$
- Coût $\times 3 \Rightarrow$ **trop coûteux !**

$\Rightarrow$ Modification de l'échelle de Montgomery

- Traite 2 bits en une itération $\Rightarrow$ réduction du surcoût

Nouvelle étape de l'échelle de Montgomery

Entrées : T_1, T_2, $xor \leftarrow k_i \oplus k_{i+1}$

1 $T_3 \leftarrow 2T_1$

2 $T_4 \leftarrow T_1 + T_2$

3 $T_5 \leftarrow 2T_4$ /*nouveau T_1, si xor = 1*/

4 $T_6 \leftarrow T_3 + T_4$ /*nouveau T_2*/

5 $T_7 \leftarrow 2T_3$ /*nouveau T_1, si xor = 0*/

6 $T_8 \leftarrow T6 + P$ /*utilise la coordonnée x du nouveau T_1*/

7 **si** $xor = 1$ **alors**

8 $\quad T_8 = T_7$

9 **sinon**

10 $\quad T_8 = T_5$

Nouvelle étape de l'échelle de Montgomery

Entrées : T_1, T_2, $xor \leftarrow k_i \oplus k_{i+1}$

1 $T_3 \leftarrow 2T_1$
2 $T_4 \leftarrow T_1 + T_2$
3 $T_5 \leftarrow 2T_4$ /*nouveau T_1, si xor = 1*/
4 $T_6 \leftarrow T_3 + T_4$ /*nouveau T_2*/
5 $T_7 \leftarrow 2T_3$ /*nouveau T_1, si xor = 0*/
6 $T_8 \leftarrow T6 + P$ /*utilise la coordonnée x du nouveau T_1*/
7 **si** $xor = 1$ **alors**
8 $T_8 = T_7$
9 **sinon**
10 $T_8 = T_5$

Ce qui est obtenu :

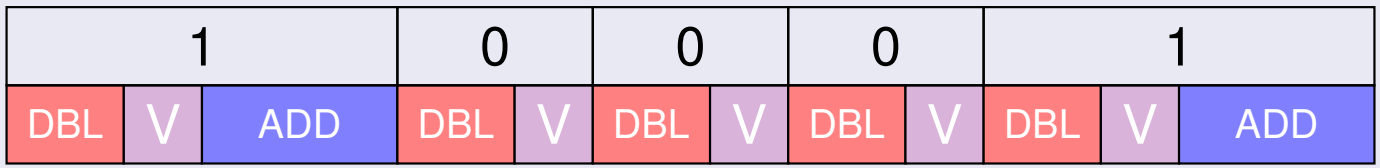
SM régulière et protégée de certaines FA

Sommaire

Protection du scalaire

La PV **ne détecte pas** les fautes faites sur le **scalaire**

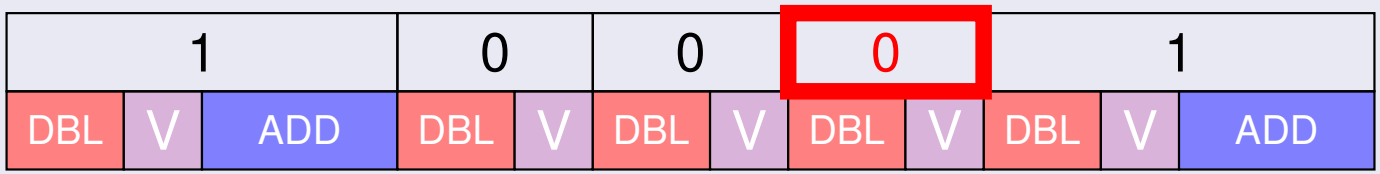
Exemple



Protection du scalaire

La PV **ne détecte pas** les fautes faites sur le **scalaire**

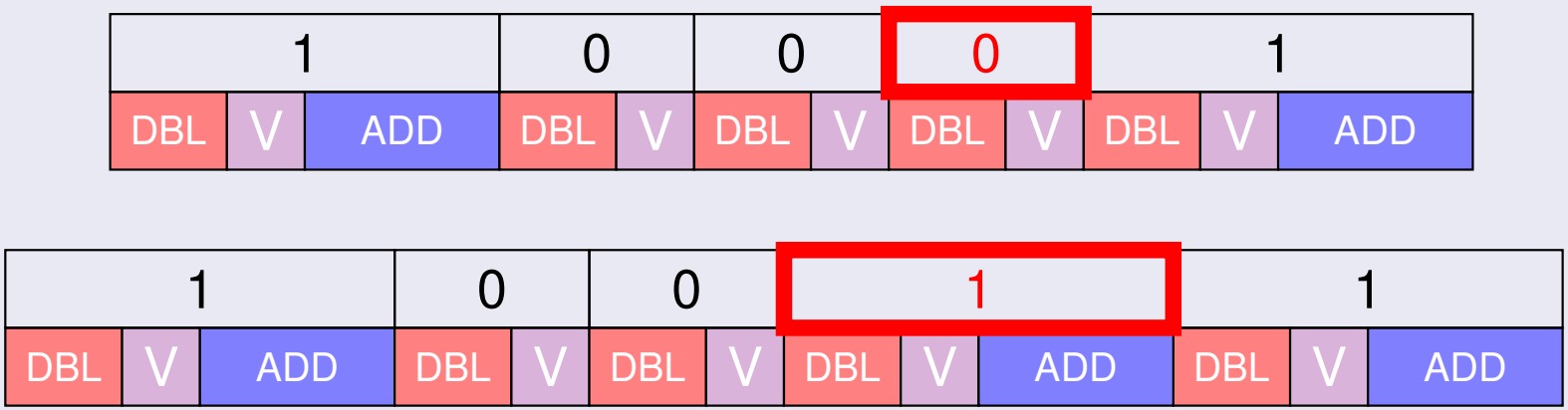
Exemple



Protection du scalaire

La PV **ne détecte pas** les fautes faites sur le **scalaire**

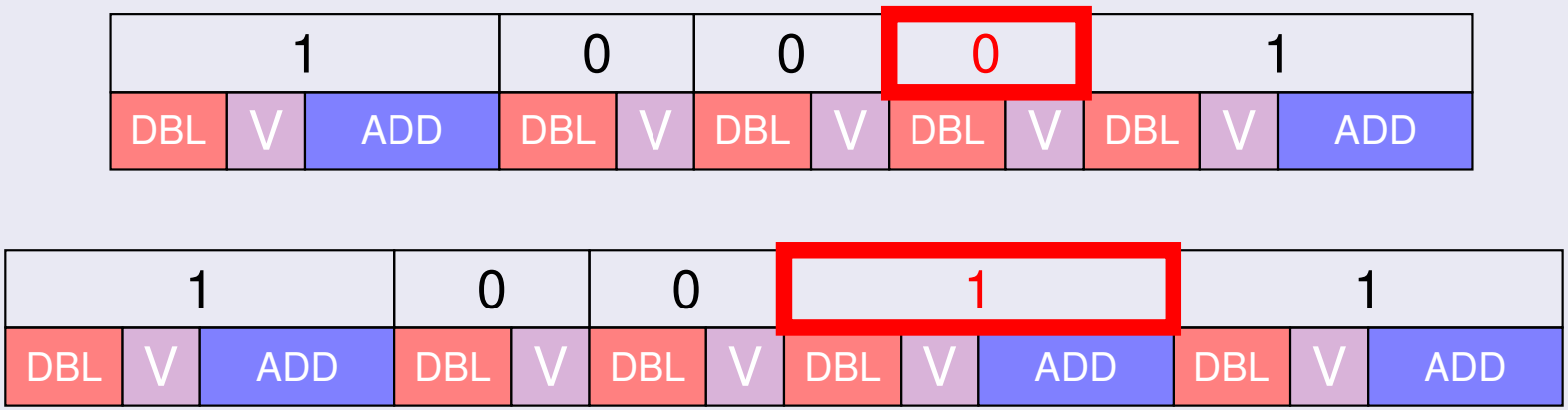
Exemple



Protection du scalaire

La PV **ne détecte pas** les fautes faites sur le **scalaire**

Exemple



- L'attaque n'est pas détectée : tous les points intermédiaires sont sur la courbe, mais le point final ne correspond pas au résultat attendu
- Protection proposée : ***Compteur d'itération***

Compteur d'itération (IC)

But : Vérifier que la multiplication scalaire (SM) correspond à la clé attendue

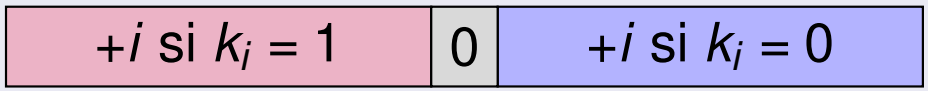
Principe :

Compter le **nombre de** ADD associées à un **poids**

- Une valeur de référence *ref*
- Le poids est l'**indice de l'itération** *i*

Division du registre en 2 parties :

- Partie de gauche : le compteur *IC*
- Partie de droite : du bruit



À la fin : comparaison entre *IC* et *ref*

Compteur d'itération (IC)

Variante - Compteur d'itération avec cswap (ICC)

- Fonction cswap de l'échelle de Montgomery
- Si $k_i \neq k_{i+1}$, cswap intervertit les coordonnées des points

Compteur d'itération (IC)

Variante - Compteur d'itération avec cswap (ICC)

- Fonction cswap de l'échelle de Montgomery
- Si $k_i \neq k_{i+1}$, cswap intervertit les coordonnées des points

Ce qui est obtenu :

- Détection des FA du type **bit flip** sur le **scalaire**
- SM reste **uniforme**
- Très faible surcoût
- Ne protège pas des FA du type **collage**

Sommaire

Expérimentations

Cible d'implantation

- Cortex-M0, 32 bits
- Bibliothèque μNaCl

Expérimentations

Cible d'implantation

- Cortex-M0, 32 bits
- Bibliothèque μNaCl

Protections implantées

- PV au début et à la toute fin
- PV toutes les d itérations (incluant $d = 1$)
- `IC` et `ICC`
- Clé aléatoire après détection
- `DBL` et toujours `ADD` (DAA)

Expérimentations

Cible d'implantation

- Cortex-M0, 32 bits
- Bibliothèque μNaCl

Protections implantées

- PV au début et à la toute fin
- PV toutes les d itérations (incluant $d = 1$)
- `IC` et `ICC`
- Clé aléatoire après détection
- `DBL` et toujours `ADD` (DAA)

Deux types de courbe

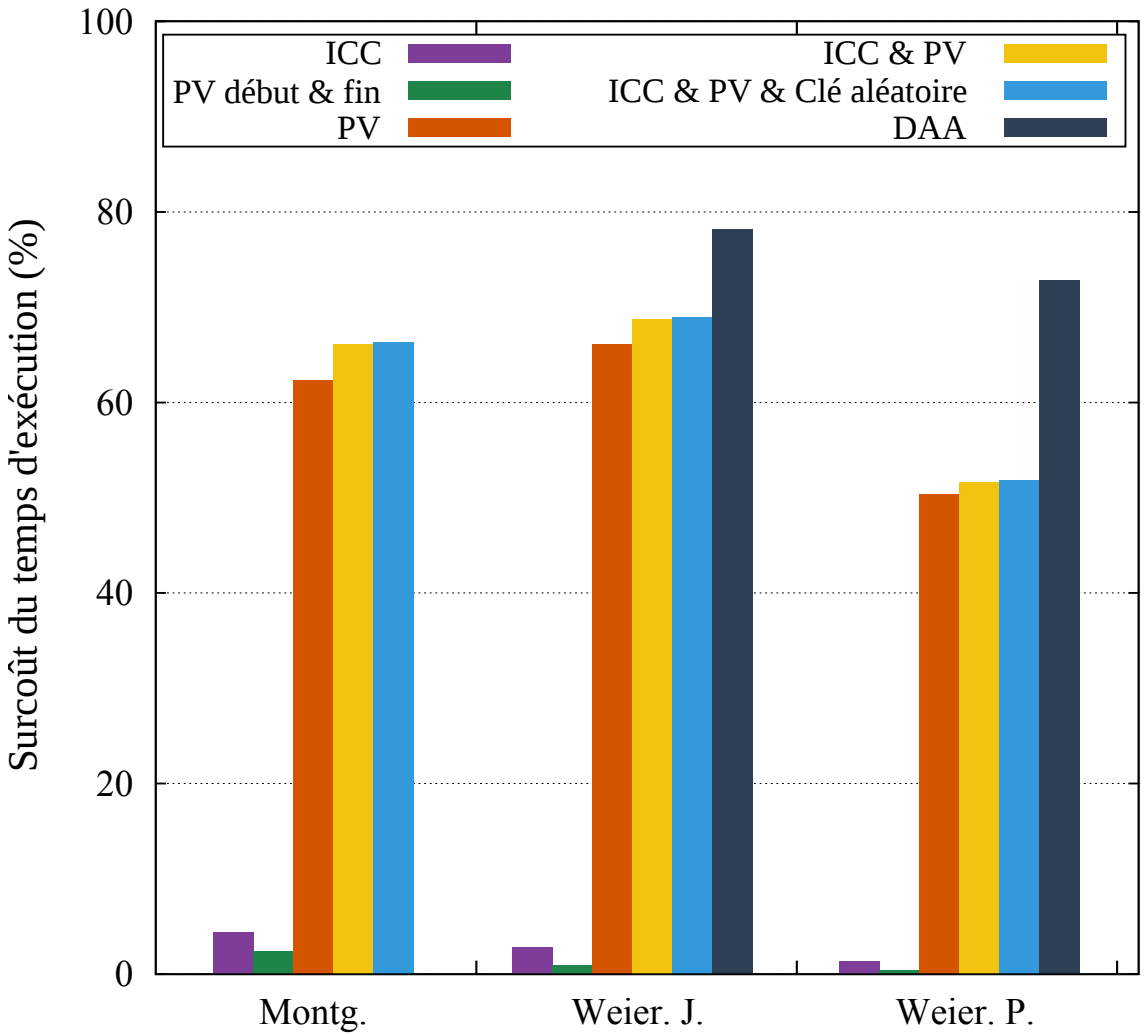
Montgomery:

- Coordonnées XZ
- Courbe Bernstein

Weierstrass:

- Coordonnées projectives (P.) et jacobiennes (J.)
- Courbe aléatoire sur $\mathbb{F}_p$ avec $p = 2^{255} - 19$

Résultats d'expérimentation

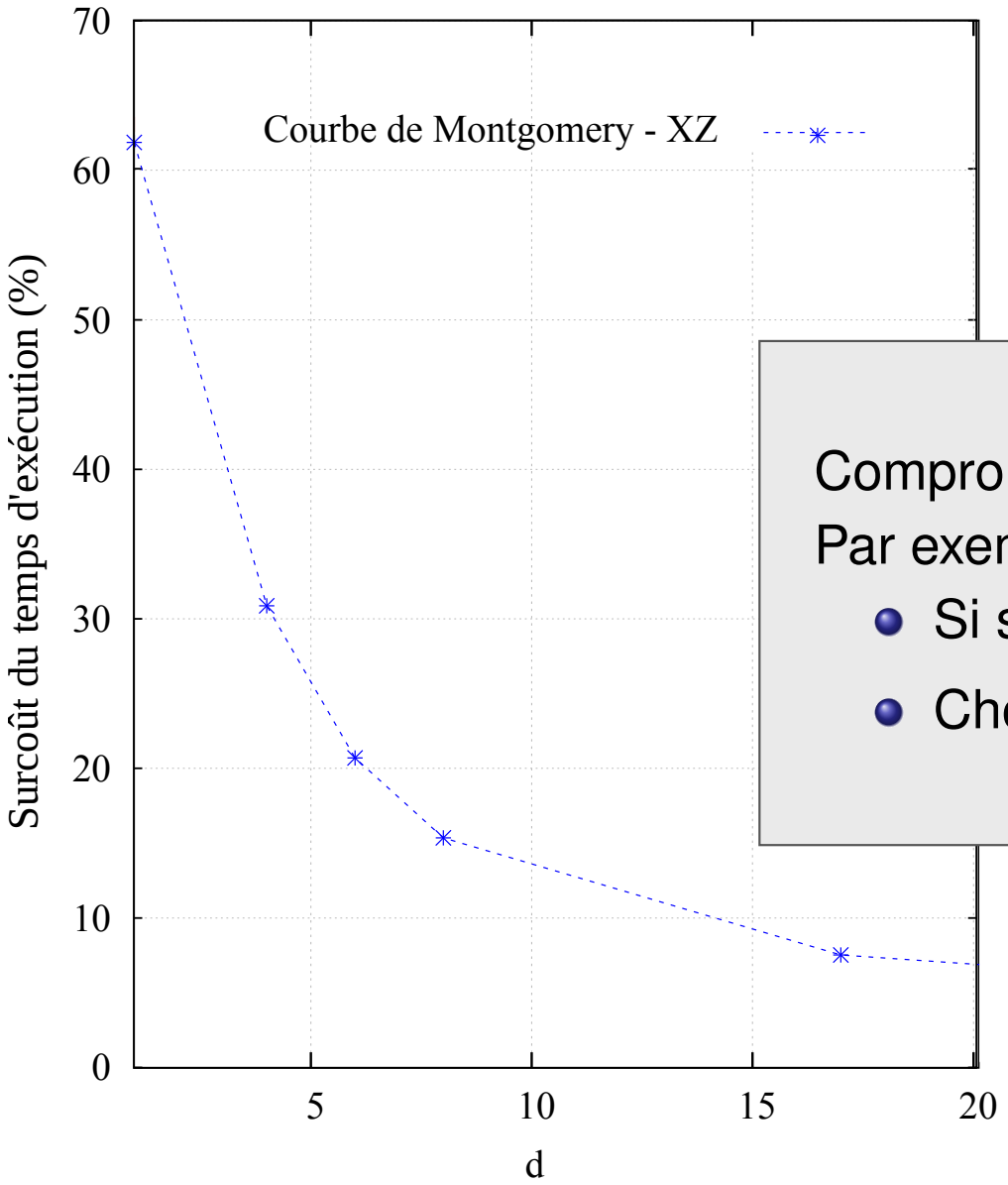


Surcoût de ICC faible

PV dans le pire des cas

- Weierstrass : meilleur que DAA
- Montgomery : meilleur que redondance classique

Compromis pour les courbes de Montgomery



Compromis entre performance et sécurité

Par exemple :

- Si surcoût autorisé : 10%
- Choisir $d \geq 15$

Ce qui est obtenu

Implantation

- Sur un Cortex M0 avec μNaCl
- Pour les courbes de Weierstrass et de Montgomery
- Pour plusieurs niveaux de protections

Ce qui est obtenu

Implantation

- Sur un Cortex M0 avec μNaCl
- Pour les courbes de Weierstrass et de Montgomery
- Pour plusieurs niveaux de protections

Protection des points et paramètres de la courbe

- Meilleur que l'état de l'art
- Contre des **FA** et des **SCA**
- Compromis possibles pour les courbes de Montgomery

Ce qui est obtenu

Implantation

- Sur un Cortex M0 avec μNaCl
- Pour les courbes de Weierstrass et de Montgomery
- Pour plusieurs niveaux de protections

Protection des points et paramètres de la courbe

- Meilleur que l'état de l'art
- Contre des **FA** et des **SCA**
- Compromis possibles pour les courbes de Montgomery

Protection du scalaire

- Contre des **FA**
- Faible coût

Sommaire

Préliminaires

Modélisation d'une architecture de petits processeurs

- Mots de `w` bits : `w`= 32
- Unités arithmétiques : 1 additionneur (`wadd`), 1 multiplieur (`wmul`)
- Opérations de corps **modulo** p (avec p générique ou $p = 2^{255} - 19$)

Le simulateur peut modéliser d'autres architectures par la modification :

- de `w`, du nombre de `wadd`, du nombre de `wmul`, de p

Préliminaires

Modélisation d'une architecture de petits processeurs

- Mots de `w` bits : `w`= 32
- Unités arithmétiques : 1 additionneur (`wadd`), 1 multiplieur (`wmul`)
- Opérations de corps **modulo** p (avec p générique ou $p = 2^{255} - 19$)

Le simulateur peut modéliser d'autres architectures par la modification :

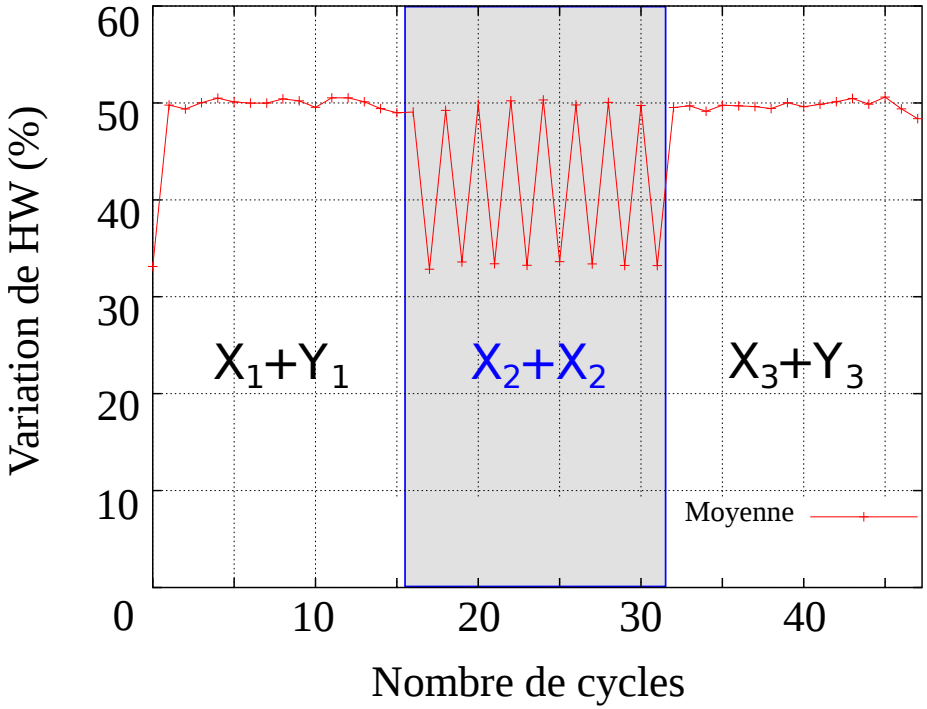
- de `w`, du nombre de `wadd`, du nombre de `wmul`, de p

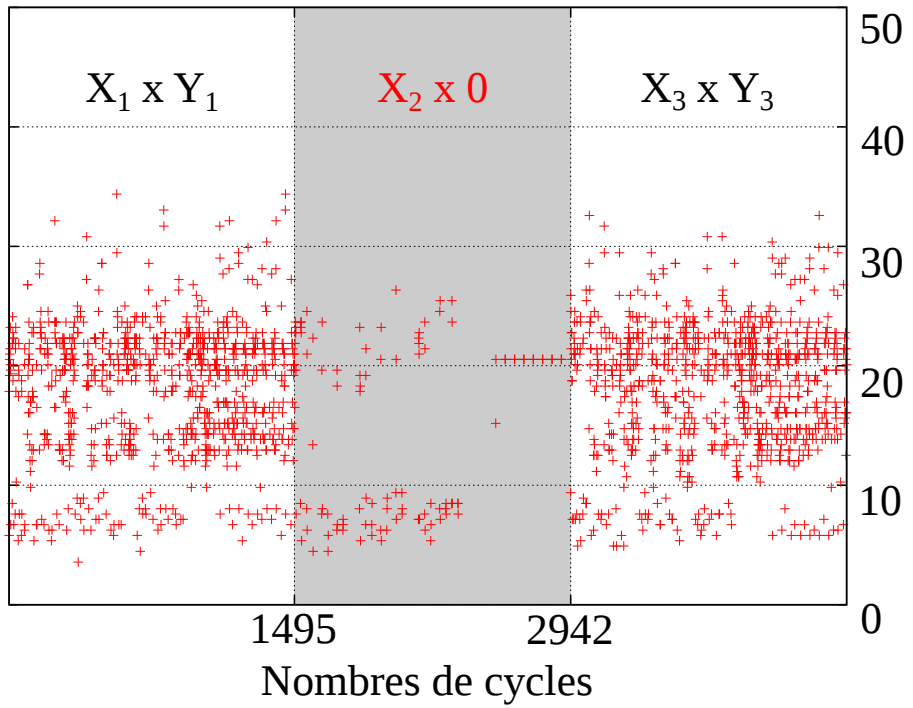
Étapes du simulateur

1. **Ordonnancement** des opérations pour approcher le comportement d'un circuit
2. **Monitoring** des opérations $\rightarrow$ Traces d'opérations de corps
3. Fusion des traces d'opérations de corps $\rightarrow$ **Trace globale pour la SM**

Sommaire

Traces d'opérations de corps avec le simulateur





Les opérandes des opérations de corps ont un impact sur l'activité

Attaques SPA et DPA avec le simulateur

Cibles des attaques

- Courbes et coordonnées :
  - Weierstrass
    - coordonnées jacobiennes
    - coordonnées projectives
- Algorithmes :
  - Doublement et addition (non protégée)
  - Doublement et toujours addition (DAA)
  - PV sans uniformisation
  - PV avec uniformisation et `ICC`

Résultats - Weierstrass en coordonnées jacobiennes

Taux de réussite SPA

Non protégée	DAA	PV
71.48%	49.2%	35.8%

SM uniformisée avec PV et IC : comportement plus uniforme que DAA

Résultats - Weierstrass en coordonnées jacobiennes

Taux de réussite SPA

Non protégée	DAA	PV
71.48%	49.2%	35.8%

SM uniformisée avec PV et IC : comportement plus uniforme que DAA

Taux de réussite DPA

Nombre de traces	Non protégée	PV basique	PV et IC
300	57%	50%	40%
400	70%	53%	43%

PV et IC améliore la sécurité vis-à-vis des DPA

Ce qui est obtenu

- Développement d'un **simulateur d'activité** au niveau arithmétique
  - **Modélisation** des unités arithmétiques
  - **Ordonnancement** et **monitoring** des opérations
  - Génération de **traces d'activité**

Ce qui est obtenu

- Développement d'un **simulateur d'activité** au niveau arithmétique
  - **Modélisation** des unités arithmétiques
  - **Ordonnancement** et **monitoring** des opérations
  - Génération de **traces d'activité**
- Étude de l'**impact des opérandes** dans les opérations de corps
  - Pour l'addition et la multiplication

Ce qui est obtenu

- Développement d'un **simulateur d'activité** au niveau arithmétique
  - **Modélisation** des unités arithmétiques
  - **Ordonnancement** et **monitoring** des opérations
  - Génération de **traces d'activité**
- Étude de l'**impact des opérandes** dans les opérations de corps
  - Pour l'addition et la multiplication
- Simulation d'attaques **DPA et SPA** sur différents niveaux de protection
  - Non protégée
  - Doublement et toujours addition
  - PV sans uniformisation de la SM
  - SM uniformisée avec PV et IC

Sommaire

Conclusion

Protections combinées

- SM **régulière**
  - **protégée contre les FA** sur les **points** et **paramètres** de la courbe
  - protégée contre les fautes bit flip sur le **scalaire**
- Meilleur que l'état de l'art

Implantation sur un Cortex M0 avec μNaCl pour les courbes de Weierstrass et de Montgomery

Conclusion

Protections combinées

- SM **régulière**
  - **protégée contre les FA** sur les **points** et **paramètres** de la courbe
  - protégée contre les fautes bit flip sur le **scalaire**
- Meilleur que l'état de l'art

Implantation sur un Cortex M0 avec μNaCl pour les courbes de Weierstrass et de Montgomery

Simulateur d'activité au niveau arithmétique

- Développement d'un **simulateur d'activité** au niveau arithmétique
- Étude de l'**impact des opérandes** dans les opérations de corps
- Attaques **DPA et SPA** sur différents niveaux de protection

Quelques perspectives

Protections combinées

- Éprouver les protections sur un banc d'attaque
- Étendre PV à d'autres courbes, coordonnées, algorithmes de SM
  - p. ex. algorithme *w*-NAF
- Coupler avec des contre-mesures ajoutant de l'aléa
  - meilleur résistance aux DPA

Quelques perspectives

Protections combinées

- Éprouver les protections sur un banc d'attaque
- Étendre PV à d'autres courbes, coordonnées, algorithmes de SM
  - p. ex. algorithme *w*-NAF
- Coupler avec des contre-mesures ajoutant de l'aléa
  - meilleur résistance aux DPA

Simulateur d'activité au niveau arithmétique

- Analyser d'autres types de courbes et coordonnées
  - p. ex. courbes d'Edwards
- Ajouter une interface graphique
- Utilisation pour faciliter/optimiser des attaques ou protections

Publications

2017 *ECC Protections against both Observation and Pertubation Attacks*
Audrey Lucas, Arnaud Tisserand
CryptArchi - International Workshops on Cryptographic architectures embedded in logic devices, Slovakia

2018 *Microcontroller Implementation of Simultaneous Protections Against Observation and Perturbation Attacks for ECC*
Audrey Lucas, Arnaud Tisserand
SECRYPT - International Conference on Security and Cryptography, Portugal

2018 *A Simulator for Evaluating the Leakage in Arithmetic Circuits*
Audrey Lucas
CryptArchi - International Workshop on Cryptographic architectures embedded in logic devices, France

Merci de votre attention