Attaques par fautes sur les couplages

Nadia El Mrabet, Philippe Guillot

LIASD, LAGA
Université Paris 8, Université Paris 13

IHP le 19 novembre 2013

Plan de l'exposé

1. Couplage sur courbes elliptiques
   - Définition et propriétés des couplages
   - Construction et exemple de couplages
   - Calcul des couplages
   - Aspect arithmétique de la cryptographie à base de couplages

2. Attaque par injection de fautes
   - La cryptographie basée sur l'identité
   - Définition d'une attaque par injection de fautes
   - Attaque par injection de fautes contre l'algorithme de Miller
   - Attaque par fautes contre l'exponentiation finale

Qu'est ce qu'un couplage ?

Propriétés

Soient $\mathbb{G}_1$, $\mathbb{G}_2$ et $\mathbb{G}_3$ trois groupes abéliens finis, en pratique cycliques. Un couplage est une application :

$$e : (\mathbb{G}_1, +) \times (\mathbb{G}_2, +) \to (\mathbb{G}_3, \times)$$

Qu'est ce qu'un couplage ?

Propriétés

Soient $\mathbb{G}_1$, $\mathbb{G}_2$ et $\mathbb{G}_3$ trois groupes abéliens finis, en pratique cycliques. Un couplage est une application :

$$e : (\mathbb{G}_1, +) \times (\mathbb{G}_2, +) \to (\mathbb{G}_3, \times)$$

Vérifiant les propriétés :

- *Non dégénérescence :* $\forall P \in \mathbb{G}_1 \neq \{0\}, \exists Q \in \mathbb{G}_2$ t.q. $e(P, Q) \neq 1$
- *Bilinéarité par rapport aux deux variables :*
  $e(P + P', Q) = e(P, Q) \cdot e(P', Q)$ et
  $e(P, Q + Q') = e(P, Q) \cdot e(P, Q')$.

Qu'est ce qu'un couplage ?

Propriétés

Soient $\mathbb{G}_1$, $\mathbb{G}_2$ et $\mathbb{G}_3$ trois groupes abéliens finis, en pratique cycliques. Un couplage est une application :

$$e : (\mathbb{G}_1, +) \times (\mathbb{G}_2, +) \to (\mathbb{G}_3, \times)$$

Vérifiant les propriétés :

- *Non dégénérescence :* $\forall P \in \mathbb{G}_1 \neq \{0\}, \exists Q \in \mathbb{G}_2$ t.q. $e(P, Q) \neq 1$
- *Bilinéarité par rapport aux deux variables :*
  $e(P + P', Q) = e(P, Q) \cdot e(P', Q)$ et
  $e(P, Q + Q') = e(P, Q) \cdot e(P, Q')$.

Conséquences

$$\forall j \in \mathbb{Z}, e(jP, Q) = e(P, Q)^j = e(P, jQ)$$

Construction des couplages

Données

Afin de calculer un couplage, nous avons besoin de :

- Soit E une courbe elliptique sur un corps $\mathbb{K}$:
  $E(\mathbb{K}) := \{(x, y) \in \mathbb{K} \times \mathbb{K},\ y^2 = x^3 + ax + b,\ \text{avec } a, b \in \mathbb{K}\} \cup P_\infty$.

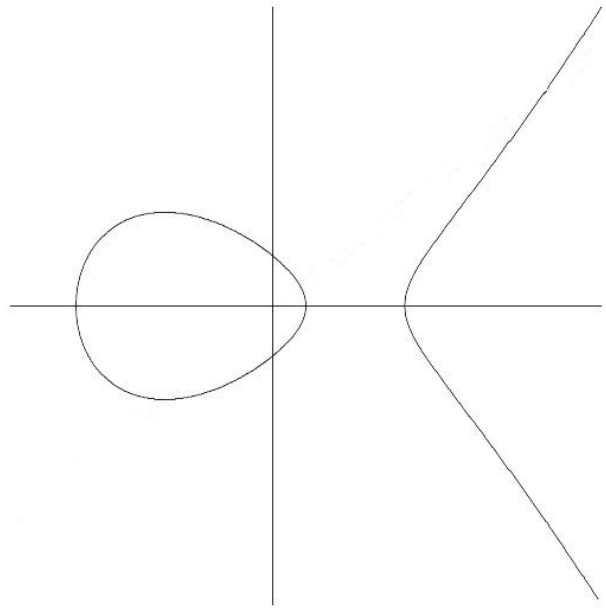


FIGURE: Courbe elliptique dans le plan réel

La courbe elliptique est munie d'une loi d'addition qui se décrit très bien graphiquement.

Construction des couplages

Données

Une construction de couplage repose sur :

- E : courbe elliptique sur un corps $\mathbb{K} \supset \mathbb{F}_p$, a et $b \in \mathbb{F}_p$:
  $E(\mathbb{K}) := \{(x, y) \in \mathbb{K} \times \mathbb{K},\ y^2 = x^3 + ax + b\} \cup \{P_\infty\}$.
- r un nombre premier divisant $\text{card}(E(\mathbb{F}_p))$,
  groupe de r-torsion : $E[r] = \{P \in E(\overline{\mathbb{F}_p}), rP = P_\infty\}$.

Construction des couplages

Données

Une construction de couplage repose sur :

- E : courbe elliptique sur un corps $\mathbb{K} \supset \mathbb{F}_p$, a et $b \in \mathbb{F}_p$:
  $E(\mathbb{K}) := \{(x, y) \in \mathbb{K} \times \mathbb{K},\ y^2 = x^3 + ax + b\} \cup \{P_\infty\}$.

- r un nombre premier divisant $\text{card}(E(\mathbb{F}_p))$,
  groupe de r-torsion : $E[r] = \{P \in E(\overline{\mathbb{F}_p}), rP = P_\infty\}$.

- Le degré de plongement relativement à r :
  - plus petit entier k tel que $r|(p^k - 1)$;
  - Degré de l'extension de $\mathbb{F}_p$ qui contient les racines r^e de l'unité.

Cryptologie à base de couplages

Cryptanalyse

Transfert du problème du logarithme discret sur une courbe elliptique en un problème de logarithme discret sur un corps fini (MOV 93 et Frey Rück 94).

$$e(\ell P, P) = e(P, P)^{\ell}$$

Cryptographie

Construction de protocoles originaux et simplification de protocoles existants :

- l'échange de clé Diffie Hellman entre trois personnes,
- schémas de signatures courtes,
- chiffrement avec l'identité.

Les couplages utilisés en cryptologie

- Le couplage de Weil,
- le couplage de Tate,
- le couplage η,
- le couplage Ate et Twisted Ate,
- les couplages optimaux,

sont les couplages les plus utilisés en cryptologie.

Construction des couplages

Le couplage de Tate

- r entier premier,
- k degré de plongement relativement à r,
- $E[r]$ groupe de r-torsion
- P et Q deux points de E, P à coordonnées dans $\mathbb{F}_p$ et Q à coordonnées dans $\mathbb{F}_{p^k}$.
- U_r groupe des racines r^{e} de l'unité, sous-groupe multiplicatif de $\mathbb{F}_{p^k}$.
- Fonction de Miller $f_{i,P}$:
  - P zéro d'ordre i,
  - iP pôle d'ordre 1,
  - P_∞ pôle d'ordre $i-1$.
- Couplage de Tate : $e(P,Q) = f_{r,P}(Q)^{\frac{p^k-1}{r}}$

Les autres couplages partagent le cœur de calcul.

L'égalité de Miller

La fonction $f_{i,P}$

Cette fonction admet le point P comme zéro d'ordre r et le point $[r]P$ comme pôle.

Formules de Victor Miller :

$$f_{i+j,P} = f_{i,P} \times f_{j,P} \times \frac{\ell_{iP,jP}}{v_{(i+j)P}}$$

- $\ell_{R,Q}$ droite passant par R et Q,
- v_R droite verticale passant par R.

$f_{r,P}(Q)$ se calcule avec une chaîne d'addition pour r :
Exemple : calcul de f_{13} :

$$f_1 \to f_2 \to f_3 \to f_6 \to f_{12} \to f_{13}$$

La sécurité des couplages

Hypothèse de sécurité

Le problème Diffie-Hellmann bilinéaire doit être difficile.
Étant donnés P, aP, bP et Q, il doit être difficile de calculer $e(P, A)^{ab}$.

Niveau de sécurité en bits	80	128	192	256
Nombre minimal de bits de r Résister au logarithme générique	160	256	384	512
Nombre minimal de bits de p^k Résister au logarithme sur corps fini	1 024	3 072	7 680	15 360

TABLE: Niveau de sécurité

Cryptologie à base de couplages

Cryptographie

les couplages ont permis la construction de protocoles originaux et la simplification de protocoles cryptographiques existants.

- L'échange de Diffie Hellman à trois (Joux 2001)
- La cryptographie basée sur l'identité (Boneh et Franklin 2001)
- Les schémas de signature courte (Boneh, Lynn, Shacham 2001)

Echange de clé à trois

	A	B	C
Secret	a	b	c
public	aP	bP	cP
calcul	$e(bP, cP)^a$	$e(aP, cP)^b$	$e(aP, bP)^c$

Les trois clés valent $e(P, P)^{abc}$.

Signature

- clé privée s
- clé publique $s \cdot P$
- signature d'un message m : $H = h(m)$ et $\sigma = sH$
- vérification : $e(H, sP) = e(H, P)^s = e(sH, P)$.

Chiffrement avec l'identité

protocoles cryptographiques asymétriques où

- la clé publique d'un utilisateur est son identité (clé publique choisie),
- la clé privée associée lui est fournie par une autorité de confiance.

Cryptographie basée sur l'identité

Echange de clé sécurisée entre Alice et Bob

Autorité de Confiance

Alice

Bob

Cryptographie basée sur l'identité

Echange de clé sécurisée entre Alice et Bob

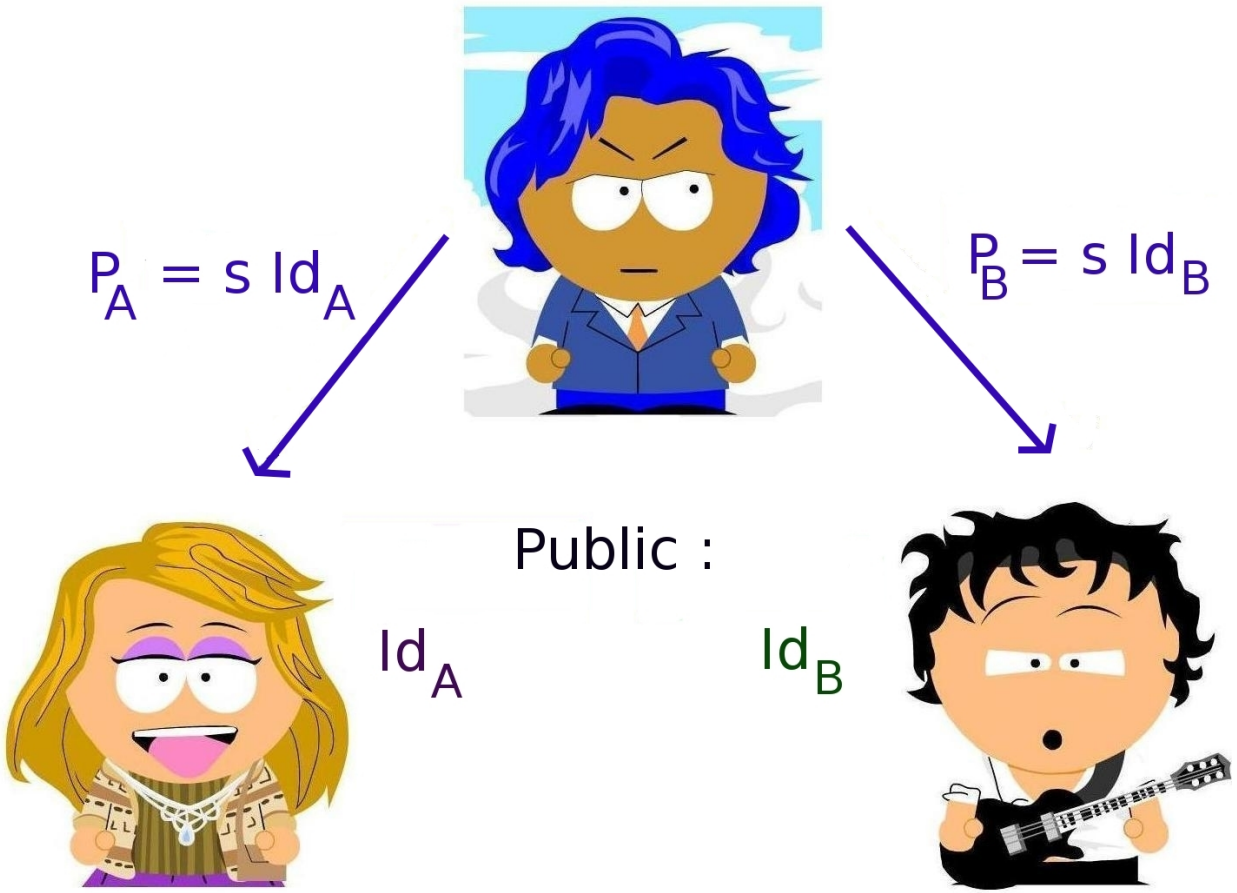
Id_A

Public :

Id_B

Cryptographie basée sur l'identité

Echange de clé sécurisée entre Alice et Bob



Cryptographie basée sur l'identité

Echange de clé sécurisée entre Alice et Bob

$$e(P_A, Id_B) = e(Id_A, Id_B)^s = e(Id_A, P_B)$$

Id_A

P_A

Id_B

P_B

Attaques par canaux cachées

Lors d'un protocole basé sur l'identité l'attaquant connait :

- l'algorithme de couplage utilisé,
- le nombre d'itérations ($N = [\log_2(r)] + 1$).

- Le secret est l'un des arguments du couplage : P_A et P_B :

$$e(P_A, I_B) = e(I_A, P_B)$$

- Le secret n'influence ni le temps d'exécution ni le nombre d'itérations de l'algorithme.

Attaques par canaux cachés

- Les attaques par canaux cachés utilisent les fuites matérielles pour récupérer des secrets.
- Les attaques par injection de fautes consistent à perturber l'exécution d'un algorithme (émissions lasers).
- 2006 : Page et Vercauteren contre l'algorithme de Duursma et Lee.
- Depuis, cette attaque a été généralisée à tous les couplages construit sur le modèle du couplage de Tate.

Description de l'attaque de Page et Vercauteren [PV2006]

- la connaissance du rapport de deux résultats de l'algorithme de Duursma et Lee permet de retrouver le secret.
- Leur méthode utilise l'écriture particulière des éléments manipulés durant l'exécution de l'algorithme. La décomposition des résultats intermédiaires dans l'extension de corps $\mathbb{F}_{p^k}$ est creuse, ce qui permet aux auteurs de retrouver des informations sur le secret.

Description de l'attaque de Whelan et Scott [WS2006, WS2007]

- Whelan et Scott adaptent l'attaque de Page et Vercauteren.
- Les équations de l'algorithme de Miller n'ont pas les mêmes propriétés que celles de l'algorithme de Duursma et Lee.
- Ils perturbent la dernière itération de l'algorithme de Miller.
- Ils retrouvent le secret s'il est placé en second argument du couplage par résolution d'une équation linéaire.
- Dans le cas où le secret est le premier argument du couplage, ils ne peuvent pas résoudre l'équation non linéaire résultante.
- Leur conclusion est donc que l'algorithme de Miller n'est pas sensible à l'attaque par faute décrite par Page et Vercauteren.

Description de l'attaque contre l'algorithme de Miller [E2009]

- Hypothèse : le couplage est utilisé lors d'un protocole de cryptographie basée sur l'identité.
- Le secret est le point P, premier argument lors du calcul du couplage $e(P, Q)$.
- Le second paramètre du couplage Q est connu et maitrisé par l'attaquant.

Objectif de l'attaque par injection de fautes

L'attaque consiste à faire varier le nombre d'itérations durant l'exécution de l'algorithme de Miller, ceci afin d'obtenir les résultats de deux exécutions dont le nombre d'itérations soient consécutifs : τ et $\tau + 1$ itérations pour $\tau \in \{1, \ldots, N\}$.
Nous notons $F_{\tau,P}(Q)$ et $F_{\tau+1,P}(Q)$ les deux résultats de ces itérations.

Description de l'attaque contre l'algorithme de Miller [E2009]

Cible de l'attaque

La cible de l'attaque est le registre mémoire contenant l'entier N déterminant le nombre d'itérations exécutées par l'algorithme de Miller à l'aide d'émission laser.

Principe de l'attaque

- Il faut effectuer plusieurs exécutions de l'algorithme de Miller en modifiant aléatoirement à chaque exécution ce registre.

  en dénombrant les cycles d'horloge nous pouvons retrouver le nombre d'itérations faites.
- L'opération est réitérée jusqu'à obtenir deux nombre d'itérations consécutifs notés τ et $\tau + 1$.

Description de l'attaque contre l'algorithme de Miller [E2009]

Probabilité de réussite

Nous cherchons à tirer deux entiers consécutifs pris aléatoirement parmi N. Ce problème est similaire au paradoxe des anniversaires. Il est possible de calculer la probabilité de réussite de cet évènement. Par exemple, il suffit de 15 tirages pour obtenir deux nombres consécutifs pris parmi 256 entiers avec une probabilité supérieure à $0,5$ et de 26 pour obtenir une probabilité supérieure à $0,9$.

Résolution d'un système

Une fois le résultat de l'algorithme de Miller obtenu pour deux itérations consécutives, il est possible de construire un système admettant pour inconnues les coordonnées du point secret . L'attaque se conclut par la résolution du système.

Exemple de rapport

Le système est :

$$\begin{aligned} Y_j Z_j^3 &= \lambda_2 \\ Z_j^2(X_j^2 - Z_j^4) &= \lambda_1 \\ 3X_j(X_j^2 - Z_j^4) + 2Y_j^2 &= \lambda_0. \end{aligned}$$

où nous connaissons les valeurs de λ_0, λ_1 et λ_2 dans $\mathbb{F}_p$, et le secret est $[j]P = (X_j, Y_j, Z_j)$.

Exemple de rapport

Le système est :

$$\begin{aligned} Y_j Z_j^3 &= \lambda_2 \\ Z_j^2(X_j^2 - Z_j^4) &= \lambda_1 \\ 3X_j(X_j^2 - Z_j^4) + 2Y_j^2 &= \lambda_0. \end{aligned}$$

où nous connaissons les valeurs de λ_0, λ_1 et λ_2 dans $\mathbb{F}_p$, et le secret est $[j]P = (X_j, Y_j, Z_j)$.

La résolution de ce système nous permet d'exprimer les inconnues X_j et Y_j en fonction de Z_j.
Cela nous permet de construire une équation de degré 12 admettant Z_j comme solution.

Exemple de rapport

Le système est :

$$\begin{aligned} Y_j Z_j^3 &= \lambda_2 \\ Z_j^2(X_j^2 - Z_j^4) &= \lambda_1 \\ 3X_j(X_j^2 - Z_j^4) + 2Y_j^2 &= \lambda_0. \end{aligned}$$

où nous connaissons les valeurs de λ_0, λ_1 et λ_2 dans $\mathbb{F}_p$, et le secret est $[j]P = (X_j, Y_j, Z_j)$.

La résolution de ce système nous permet d'exprimer les inconnues X_j et Y_j en fonction de Z_j.
Cela nous permet de construire une équation de degré 12 admettant Z_j comme solution.

$$(\lambda_0^2 - 9\lambda_1^2)Z^{12} - (4\lambda_0\lambda_2^2 + 9\lambda_1^3)Z^6 + 4\lambda_1^4 \equiv 0 \mod p$$

Attaque contre l'exponentiation finale

- Le couplage Tate et ses variantes sont composés de l'algorithme de Miller suivi d'une exponentiation finale.
- Dans [WS2007], les auteurs considèrent l'exponentiation finale comme une contre mesure suffisante pour protéger le couplage de Tate et ses variantes.
- Récemment, dans [LFG2013], les auteurs parviennent à retrouver le résultat de l'algorithme de Miller en provoquant trois fautes lors du calcul de l'exponentiation finale.

Description de l'attaque contre l'exponentiation finale

- L'attaque utilise la décomposition de l'exposant en $\frac{p^{2d}-1}{r} = (p^d - 1)\frac{p^d+1}{r}$.
- Chaque résultat intermédiaire de l'exponentiation appartient a un sous groupe connu des racines de l'unité.
- L'attaque consiste à injecter une erreur Δ maitrisée par l'attaquant pour faire sortir les résultats intermédiaires du groupe des racines de l'unité.

Conclusion

Attaquer l'intégralité du couplage Tate (ou équivalent)

- Pour l'instant, deux attaques indépendantes :
  - modifier le nombre d'itérations pour retrouver le secret de l'algorithme de Miller
  - injecter deux fautes au résultat de l'algorithme de Miller pour inverser l'exponentiation.

$\Rightarrow$ Essayer de combiner les deux ?

Bibliographie

[PV2006] Page and Vercauteren, *Fault and Side Channel Attacks on Pairing based Cryptography*, IEEE Transactions on Computer, 2006.

[WS2006] Whelan and Scott, *Side Channel Analysis of Practical Pairing Implementation : Which Path is More Secure ?*, VietCrypt2006.

[WS2007] Whelan and Scott, *The Importance of the Final exponentiation in Pairings when considering Fault Attacks*, Pairing 2007.

[E2009] El Mrabet, *What about the Vulnerability of the Miller algorithm considering Fault attacks*, ISA 2009.

[EPV] El Mrabet, Page and Vercauteren, *Fault Attacks on Pairing Based Cryptography : A State of the Art*, in Fault Analysis in Cryptography, Eds M. Joye and M. Tunstall, Springer 2012.

[LFG] Lasherme, Fournier and Goubin, *Inverting the final exponentiation of the Tate pairings on ordinary elliptic curves using faults*, CHES 2013.