Définition générale des couplages
Cryptologie à base de couplage

Nadia El Mrabet

GREYC−LMNO−Université de Caen, France

Ecole « Code et Cryptographie », ENSIAS de Rabat−MAROC,
Semaine du 8 au 14 mars 2010.

Plan de la présentation

Outline

Qu'est ce qu'un couplage ?

Définition

Soit G_1, G_2 et G_3 trois sous groupes de même ordre r.

En pratique, G_1 et G_2 seront des groupes additifs et G_3 un groupe multiplicatif.

Un couplage est

une application :

$$e : G_1 \times G_2 \longrightarrow G_3$$

Qu'est ce qu'un couplage ?

Propriétés

Cette application e doit vérifier deux propriétés principales :

Qu'est ce qu'un couplage ?

Propriétés

Cette application e doit vérifier deux propriétés principales :

- **non dégénérescence en les arguments :**
  - $\forall P \in G_1 \ \{0\}, \exists Q \in G_2$ t.q. $e(P, Q) \neq 1$
  - $\forall Q \in G_2 \ \{0\} \exists P \in G_1$ t.q. $e(P, Q) \neq 1$

Qu'est ce qu'un couplage ?

Propriétés

Cette application e doit vérifier deux propriétés principales :

- **non dégénérescence en les arguments :**
  - $\forall P \in G_1 \ \{0\}, \exists Q \in G_2$ t.q. $e(P,Q) \neq 1$
  - $\forall Q \in G_2 \ \{0\} \exists P \in G_1$ t.q. $e(P,Q) \neq 1$
- **bilinéarité en les arguments :** $\forall P, P' \in G_1, \forall Q, Q' \in G_2$
- $e(P+P',Q) = e(P,Q).e(P',Q)$
- $e(P,Q+Q') = e(P,Q).e(P,Q')$

Qu'est ce qu'un couplage ?

Propriétés

Soit G_1, G_2 et G_3 trois groupes de même ordre r,
et un couplage

$$e : G_1 \times G_2 \longrightarrow G_3$$

vérifiant les propriétés de

- *non dégénérescence ;*
- *bilinéarité.*

Conséquences

$$\forall j \in \mathbb{N}, e([j]P, Q) = e(P, Q)^j = e(P, [j]Q)$$

Cryptologie à base de couplage

La propriété importante qui a impliqué l'utilisation des couplages en cryptologie est cet égalité :

$$\forall j \in \mathbb{N}, e([j]P, Q) = e(P, Q)^j = e(P, [j]Q).$$

Tout d'abord, les couplages ont été utilisés dans un but destructif : nous parlons des attaques de MOV et Frey Ruck datant respectivment de 1993 et 1994.
Ce n'est que très récemment, dans les années 2000 que les couplages ont été utilisés pour construire des protocoles cryptographiques.

Outline

Le problème du logarithme Discret

Définition

Définition du DLP

Soit $(G, +)$ un groupe, g un générateur de G et a un entier naturel. Le problème du logarithme discret consiste à retrouver l'entier a avec la donnée de g et ag, où ag représente $\underbrace{g + g + \ldots + g}_{a \text{ fois}}$.

Le signe DLP est l'abréviation courrament utilisée venant de l'anglais Discrete Logarithm Problem.
Nous allons commencer par motiver l'intérêt pour ce problème en décrivant deux méthodes de résolution suivie par un protocole cryptographique basé sur le problème du logarithme discret.

Le problème du logarithme discret

Algorithme de résolution

- L'échange de clef de Diffie Hellman peut être réaliser avec G un sous groupe d'une courbe elliptique ou d'un corps fini.
- Il existe plusieurs algorithmes pour résoudre le logarithme discret, un des algorithmes génériques le plus efficace est l'algorithme Pollard - ρ.
- Pollard - ρ s'applique tout autant sur une courbe elliptique que sur un corps fini, avec des complexités équivalentes.
- Il existe un algorithme de résolution du logarithme discret plus efficace pour les corps finis : la méthode par calcul d'index.

Nous allons décrire ces deux méthodes.

Le problème du logarithme discret

Pollard - ρ

- L'algorithme Pollard - ρ calcule le logarithme discret dans n'importe quel groupe cyclique.
- C'est la méthode la plus efficace à l'heure actuelle pour résoudre un problème de logarithme discret sur une courbe elliptique,
- proposée par Pollard en 1978 pour $\mathbb{F}_p^\star$ et s'inspire du paradoxe des anniversaires.

Nous allons décrire cet algorithme.

Le problème du logarithme discret

Pollard - ρ

Soit G un groupe cyclique de cardinal r.
Choisissons une fonction $f : G \longrightarrow G$ qui servira à construire une marche pseudo aléatoire.
A partir d'un point $R_0 \in G$, nous construisons la suite :

$$\begin{cases} & R_0, \\ \forall i \in \mathbb{N}^\star R_{i+1} & = & f(R_i). \end{cases}$$

Comme G est un ensemble fini, il existe des entiers μ et τ tels que

$$R_i = R_{i+\tau}$$

pour tout $iGe\mu$.
La représentation graphique des R_i est formée d'une première suite de taille μ, suivie d'un cycle de taille τ dont le tracé fait penser à la lettre grecque ρ, d'où le nom de la méthode. Si la marche f est bien aléatoire, les valeurs de μ et τ sont en moyennes égales à $\sqrt{\pi r/8}$.

Le problème du logarithme discret

Pollard - ρ

L'efficacité de Pollard-ρ repose sur celle de la marche aléatoire.
Il existe différente méthode de construction de marche aléatoire, nous allons décrire l'algorithme de recherche de cycle de Floyd qui permet de ne pas avoir à stocker toutes les valeurs de la suite.

L'algorithme de recherche de cycle de Floyd

Le principe de cet algorithme est à calculer deux suites de points commençant à partir de R_0, mais « avançant » à des rythmes différents. Pour la première, nous appliquons une fois la fonction f, pour la seconde, deux fois.

Le problème du logarithme discret

Pollard - ρ

L'algorithme de recherche de cycles de Floyd est le suivant :

Données: $R_0 \in E$ et f une fonction aléatoire ;
Résultat: Un indice i pour lequel $R_i = R_{2i}$;
$R_1 = f(R_0)$;
$R_2 = f \circ f(R_0)$;
$i = 1$;
tant que $R_1 \neq R_2$ **faire**
    $R_1 = f(R_1)$;
    $R_2 = f \circ f(R_2)$;
    $i = i + 1$;
fin
retourner i

Algorithm 1: Recherche de cycles de Floyd

L'avantage de cet algorithme est que nous ne conservons que deux valeurs R_1 et R_2, ainsi que leurs décompositions (u_1, v_1) et (u_2, v_2) en fonction de P et Q. Dès qu'une collision nous pouvons résoudre le problème du logarithme discret.

Le problème du logarithme discret

La méthode par calcul d'index

Cette méthode est la plus efficace pour calculer le logarithme discret dans un corps fini.
Soient

- p un nombre premier,
- $\mathbb{G} \subset \mathbb{F}_p^\star$, sous-groupe multiplicatif d'ordre $r = p - 1$,
- g un générateur de G,
- et x un élément de G tel que $x = g^\alpha$, pour $\alpha \in [1, r-1]$.

La résolution du logarithme discret par la méthode de calcul d'index est la résolution la plus efficace connue à ce jour pour les corps finis. Elle est en complexité sous exponentielle, s'exprimant en fonction de l'argument q (dans notre cas, cet argument est l'ordre du groupe) par la fonction :

$$L_r(e, c) = \exp\left(c(\log r)^e(\log(\log(r)))^{1-e}\right),$$

où $e \in [0, 1]$ et $c > 0$ est une constante.

Le problème du logarithme discret

La méthode par calcul d'index

Soit n un entier, nous commençons par construire une base de facteurs premiers $B = \{p_1, p_2, \ldots, p_n\}$ de $\mathbb{F}_p$.
Cette base est librement choisie parmi les petits nombres premiers de $\mathbb{F}_p$, deux à deux différents.
Nous construisons alors les relations suivantes pour des éléments h tirés au hasard dans $\mathbb{F}_p$.

$$g^h \equiv \prod_i p_i^{\alpha_i} \bmod(p),$$

qui équivaut en fait à la relation :

$$h \equiv \sum_i \alpha_i \times \log_g(p_i) \bmod(r),$$

où, nous connaissons h et les α_i et nous cherchons les $\log_g(p_i)$.

Le problème du logarithme discret

La méthode par calcul d'index

Nous réitérons ce procédé jusqu'à obtenir n relations indépendantes.
Ces n relations forment un système linéaire en les valeurs $\log_g(p_i)$ pour $i = \{1, \ldots, n\}$.
La résolution de ce système nous permet d'obtenir le logarithme discret des éléments de la base B.
Pour terminer, nous cherchons aléatoirement un entier l vérifiant une dernière relation de la forme :

$$g^l x \equiv \prod_i p_i^{\alpha_i} \mod(r),$$

sachant que $x = g^\alpha$, cette relation permet de calculer α :

$$\alpha \equiv \sum_i \alpha_i \times \log_g(p_i) - l \mod(r).$$

L'algorithme que nous venons de décrire a une complexité en $L_r(1/2, c)$, sous exponentielle en les arguments.

Le problème du logarithme Discret

L'échange de clé de Diffie Hellman

Soit Alice et Bob deux personnes souhaitant construire une clef commune de chiffrement pour un protocole symétrique.
Ils se mettent d'accord sur le choix d'un groupe $(G, \oslash)$ et de g un générateur de ce groupe.

- Alice choisit un entier a et calculer $g \oslash a$,
- Bob choisit un entier b et calculer $g \oslash b$.

Ensuite,

- Alice envoie à Bob $g \oslash a$,
- Bob envoie à Alice $g \oslash b$.

Le problème du logarithme Discret

L'échange de clé de Diffie Hellman

Puis

- Alice calcule $(g \oslash b) \oslash a$,
- Bob calcule $(g \oslash a) \oslash b$.

Tous deux ont ainsi construit la même clef de chiffrement : $g \oslash ab$.
Introduisons maintenant le personnage de Eve.
Eve est une curieuse souhaitant découvrir ce qu'Alice et Bob s'échangent, pour ce faire elle doit déterminer $g \oslash ab$.
En admettant qu'elle ait écouté les échanges entre Alice et Bob, elle connait G, g, $g \oslash a$ et $g \oslash b$.
Retouver $g \oslash ab$ à l'aide de ces données est le problème de Diffie Hellman.
Clairement, résoudre le problème du logarithme discret permet de résoudre le problème de Diffie Hellamn.

Outline

Cryptanalyse à base de couplage

Définition

Rappel :

Définition

La cryptanalyse s'oppose, en quelque sorte, à la cryptographie. En effet, si déchiffrer consiste à retrouver le clair au moyen d'une clé, cryptanalyser c'est tenter de se passer de cette dernière ; et retrouver le message caché sans connaitre la clé privée de l'algorithme.

Nous avons vu qu'il existe quatre attaques générales. Ils existent plusieurs autres attaques mathématiques, liées à la structure des groupes intervenant. Nous allons voir comment la propriété de bilinéarité des couplages a permis de développer une attaque spécifique aux courbes elliptiques.

Cryptanalyse à base de couplage

Construction

Supposons que Eve se contente de retrouver la clé secrète d'Alice.
Le groupe G est un sous groupe de courbe elliptique.
Si Eve dispose de g et $ag = \underbrace{g + g + \ldots + g}_{a}$.

Résoudre le problème du logarithme discret sur la courbe elliptique est difficile, si Eve se muni d'un couplage e non dégénéré sur $G \times G$, alors en calculant

$$e(g, ag) = e(g, g)^a$$

elle déplace le DLP depuis la courbe elliptique sur un corps fini.
Le problème devient trouver a connaissant $e(g, g)$ et $e(g, g)^a$.
Nous venons de décrire les attaques MOV, du nom de ses auteurs Menezes, Okamoto et Vanstone et Frey Ruck datant de 1993 et 1994.

Outline

Cryptographie à base de couplage

Apparition

La bilinéarité des couplages a permis la construction de protocoles originaux et l'amélioration des protocoles 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)

Nous allons illustrer chacun de ces protocoles.

Cryptographie à base de couplage

L'échange de Diffie Hellman à trois

Nous commençons à adapter le principe d'échange de Diffie Hellman à trois. Soit Alice, Bob et Charlie souhaitant construire une clef commune de chiffrement pour un protocole symétrique.
Ils se mettent d'accord sur le choix d'un groupe $(G, +)$ et de g un générateur de ce groupe.

- Alice calcul ag et l'envoie à Bob,
- Bob calcul bg et l'envoie à Charlie,
- Charlie calcule cg et l'envoie à Alice.

Ensuite,

- Alice calcul $a(cg)$ et l'envoie à Bob,
- Bob calcul $b(ag)$ et l'envoie à Charlie,
- Charlie calcule $c(bg)$ et l'envoie à Alice.

$\Rightarrow$ la clef commune est $(abc)g$.

Cryptographie à base de couplage

L'échange de Diffie Hellman à trois

Antoine Joux en 2001 a décrit l'échange de Diffie Hellman à trois avec un seul tour d'échange.
Ils se mettent d'accord sur le choix d'un groupe $(G, +)$, de g un générateur de ce groupe et d'un couplage.

- Alice calcul ag et l'envoie à Bob et Charlie,
- Bob calcul bg et l'envoie à Charlie et Alice,
- Charlie calcule cg et l'envoie à Alice et Bob.

Ensuite, Alice, Bob et Charlie peuvent construire la même clef de chiffrement :

- Alice calcul $e(bg, cg)^a$,
- Bob calcul $e(ag, cg)^b$,
- Charlie calcule $e(ag, bg)^c$.

$\Rightarrow$ la clef commune est $e(g, g)^{abc}$.

Cryptographie à base de couplage

La cryptographie basée sur l'identité

En 1984, Adi Shamir lança un défi à la communauté des cryptographes :

construire un protocole cryptographique basé sur l'identité.

La première réponse apportée par les cryptographes fut le protocole de Boneh et Franklin en 2001.
Ce fut l'introduction de la cryptographie basée sur l'identité.
Nous allons décrire deux exemples de protocoles basés sur l'identité :

- Construction d'une clef d'échange ;
- Le protocole de Boneh et Franklin.

Cryptographie à base de couplage

La cryptographie basée sur l'identité

Tout protocole basé sur l'identité est assujeti au patronnage d'une autorité de confiance (Trusted Authority).
Les clefs publiques sont les identités des personnes.
Les clefs privées sont construites par l'autorité de confiance et transmises aux utilisateurs.

Cryptographie à base de couplage

La cryptographie basée sur l'identité

Tout protocole basé sur l'identité est assujeti au patronnage d'une autorité de confiance (Trusted Authority).
Les clefs publiques sont les identités des personnes.
Les clefs privées sont construites par l'autorité de confiance et transmises aux utilisateurs.
Les paramètres publiques sont alors

- Les groupes G_1 et G_3 utilisés pour le calcul des couplages ;
- le couplage e ;
- une fonction de hashage $H_1 : \{0,1\}^* \longrightarrow G_1$

Cryptographie à base de couplage

Echange de clé sécurisée entre Alice et Bob

Autorité de Confiance

Alice

Bob

Cryptographie à base de couplage

Echange de clé sécurisée entre Alice et Bob

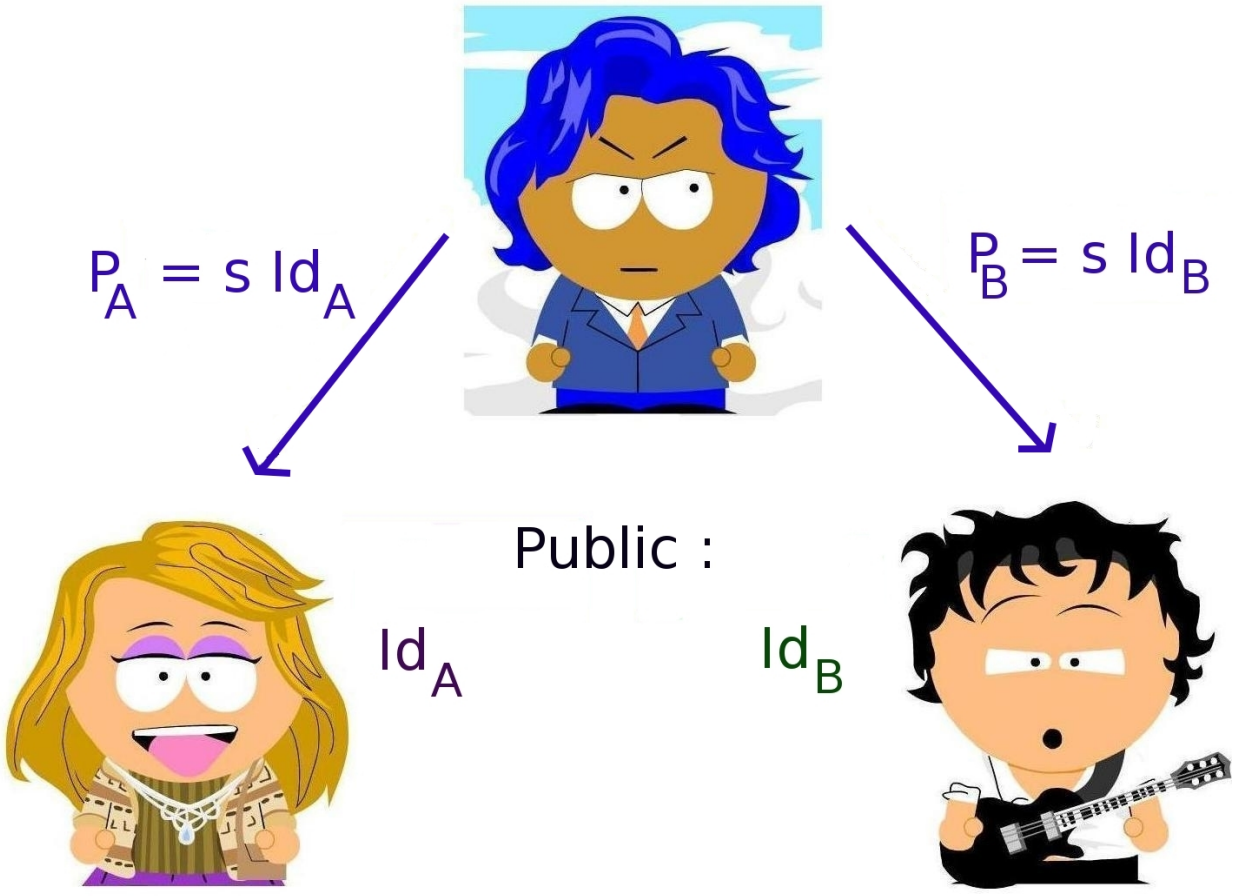
Public :

Id_A

Id_B

Cryptographie à base de couplage

Echange de clé sécurisée entre Alice et Bob



Cryptographie à base de couplage

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

Les paramètres publiques sont alors

- Les groupes G_1 et G_3 utilisés pour le calcul des couplages ;
- le couplage e ;
- une fonction de hashage $H_1 : \{0,1\}^* \rightarrow G_1$

Les paramètres secret sont les clefs privées dépendant du secret s de l'autorité de confiance.

- La clé privée de Alice est $P_A = [s]Q_A$ où $Q_A = H_1(Id_A) \in G_1$.
- La clé privée de Bob est $P_B = [s]Q_B$ où $Q_A = H_1(Id_A) \in G_1$.

La sécurité des protocoles basés sur l'identité repose

- sur la non collision possible d'identités ;
- sur la difficulté de résoudre le problème DH.

Cryptographie à base de couplage

Le protocole de Boneh et Franklin

Les paramètres sont :

- G_1, G_3 les groupes pour le couplage (publiques),
- e le couplage (publique),
- P un générateur de G_1 (publique),
- s le secret de l'autorité de confiance,
- $Q_0 = sP$ la clef privée du protocole (publique ! !)
- deux fonctions de hash : $H_1 : \{0,1\}^* \longrightarrow G_1$ et $H_2 : G_3 \longrightarrow \{0,1\}^n$.

Etape de chiffrement du message clair M

Alice veut envoyer un message à Bob :

- elle choisit un entier a au hasard,
- elle récupère la clef publique de Bob : I_B,
- elle calcule le couplage $e(I_B, Q_0)^a$,
- elle envoie à Bob : $\langle aP, M \otimes H_2\left(e(I_B, Q_0)\right)\rangle$.

Etape de déchiffrement du message chiffré $\langle U, V \rangle$.

Bob suit les étapes suivantes :

- il contacte l'autorité de confiance pour récupérer sa clef privée $P_B = sI_B$,
- il déchiffre le message en calculant $V \otimes H_2\left(e(P_B, U)\right)$.

Pourquoi est ce que ça marche ?

Encore et toujours la bilinéarité des couplages. En effet :

$$e(P_B, U) = e(sI_B, aP) = e(I_B, P)^{as} = e(I_B, sP)^a.$$

Cryptographie à base de couplage

Les schémas de signatures courtes

Pour assurer l'intégrité et l'authentification des messages chiffrés, des schémas de signatures ont été mis en place.
Boneh, Lynn, et Shacham en ont proposé en 2001 un protocole de signature courte à base de couplage dont les signatures sont assez courtes.
Ex : une signature de taille 170 bits, pour une sécurité équivalente à une signature DSA de 320 bits.
Les paramètres sont :

- G_1, G_3 les groupes pour le couplage (publiques),
- e le couplage (publique),
- P un générateur de G_1 (publique)
- deux fonctions de hash : $H_1 : \{0,1\}^* \rightarrow G_1$ et $H_2 : G_3 \rightarrow \{0,1\}^n$.

Pour signer son message, Alice

- choisit a qu'elle garde secret,
- calcule sa clef publique aP
- calcule $h = H_1(M) \in G_1$,
- envoie à Bob le couple (M, ah).

Pour vérifier la signature Bob

- vérifie que $e(H_1(M), aP) = e(ah, P)$.

Cryptographie à base de couplage

Les schémas de signatures courtes

- Il existe d'autres schémas de signature,
- des signatures de groupes,
- et toute une floppée de protocoles à base de couplages
- pour un survey : Pairing-Based Cryptographic Protocols : A Survey de Ratna Dutta, Rana Barua and Palash Sarkar

Suite des festivités

Les couplages dans tout leur état

Dans la suite, nous allons commencer à entrer dans le vif du sujet

- Définition mathématiques des couplages
- Exemple et calcul de couplages
- Optimisation des couplages Mathématiques et Arithmétique
- Attaques par canaux cachés : SPA, attaque par faute, DPA
- Application au couplage
- Perspective de la recherche à base de couplage.