TP14 : Logarithme discret et couplages

Résumé du TP

Bertrand Meyer

15 juin 2020

Le contexte cryptographique

Hypothèse de sécurité

La sécurité 💪 de nombreux protocoles cryptographiques est gagée sur la difficulté du logarithme discret, i.e. trouver $k \in \mathbb{Z}$ tel que

$$g = b^k, \text{ pour } g, b \text{ donnés dans un groupe abélien } (G, \cdot).$$

Exemple

- Diffie-Hellman
- Elgamal
- Protocole à 3 passes de Shamir ou de Massey-Omura

État de l'art

- Dans un groupe générique G, la complexité est en $O(\sqrt{|G|})$.
  $\rightarrow$ Baby-step, giant step 👶🗿 de Shanks

État de l'art

- Dans un groupe générique G, la complexité est en $O(\sqrt{|G|})$.
  $\rightarrow$ Baby-step, giant step 👶🗿 de Shanks
- Si la factorisation de $|G|$ est connue, on peut réduire le problème à des sous-groupes d'ordre p où p diviseur premier de $|G|$ (lemme chinois et relèvement p-adique).
  $\rightarrow$ méthode de Pohlig-Hellman

État de l'art

- Dans un groupe générique G, la complexité est en $O(\sqrt{|G|})$.
  $\rightarrow$ Baby-step, giant step 👶🗿 de Shanks
- Si la factorisation de $|G|$ est connue, on peut réduire le problème à des sous-groupes d'ordre p où p diviseur premier de $|G|$ (lemme chinois et relèvement p-adique).
  $\rightarrow$ méthode de Pohlig-Hellman
- Si $G = \mathbb{F}_q^\times$, la complexité est dans certains cas en $(\log q)^{O(\log \log q)}$ (quasipolynomiale)
  $\rightarrow$ Barbulescu, Gaudry, Joux & Thomé (2013)

On préfère désormais les courbes elliptiques de taille proche d'un premier pour les usages cryptographiques.

Quelques techniques

Pas de bébé, pas de géant

Supposons que $|G| < s^2$ et $g = b^k$ ($b, g \in G$ connus, $k \in \mathbb{Z}$ inconnu).

Ecrivons $k = \log_b g = is + j$ avec $i, j < s$. Alors

$$b^k = b^{is+j} = g \Leftrightarrow gb^{-j} = (b^s)^i.$$

On énumère dans une table de hachage 🗃️

ℓ	pas de bébé : $gb^{-\ell}$ 👶	pas de géant : $(b^s)^\ell$ 🗿
0	$*$	$*$
1	$*$	$*$
$\vdots$	$\vdots$	$\vdots$
$s-1$	$*$	$*$

et on cherche une collision.

Complexité $O(\sqrt{|G|})$

ρ de Pollard

On cherche k tel que $b^k = g$.
On simule une « marche aléatoire » dans $b^\alpha g^\beta$ avec une suite définie par récurrence $(w_n)_{n\in\mathbb{N}}$. Forme de la suite en ρ 🐍.

$$w_{n+1} = \begin{cases} g \cdot w_n & \text{si } \mathbf{hash}(w_n)\%3 = 0 & (\beta \leftarrow \beta + 1) \\ w_n^2 & \text{si } \mathbf{hash}(w_n)\%3 = 1 & (\alpha \leftarrow 2\alpha, \beta \leftarrow 2\beta) \\ b \cdot w_n & \text{si } \mathbf{hash}(w_n)\%3 = 2 & (\alpha \leftarrow \alpha + 1) \end{cases}$$

En cas de collision (algorithme du lièvre 🐇 et de la tortue 🐢)

$$w_i = w_j \Leftrightarrow b^{\alpha_i} g^{\beta_i} = b^{\alpha_j} g^{\beta_j} \Leftrightarrow k = \log_b g = \frac{\alpha_i - \alpha_j}{\beta_j - \beta_i}$$

Paradoxe des anniversaires : complexité en $O(\sqrt{|G|})$.

Calcul d'indice (version simplifiée)

On fixe une base de friabilité $\{p_1, p_2, \ldots, p_k\}$.

On génère des relations (en tirant des α)

$$\{b^\alpha = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}\}.$$

Calcul d'indice (version simplifiée)

On fixe une base de friabilité $\{p_1, p_2, \ldots, p_k\}$.

On génère des relations (en tirant des α)

$$\{b^\alpha = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}\}.$$

On résout le système

$$\{\alpha = e_1 \log_b p_1 + e_2 \log_b p_2 + \cdots e_k \log_b p_k.$$

pour déterminer $\log_b p_1$, ..., $\log_b p_k$.

Calcul d'indice (version simplifiée)

On fixe une base de friabilité $\{p_1, p_2, \dots, p_k\}$.
On génère des relations (en tirant des α)

$$\{b^\alpha = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}\}.$$

On résout le système

$$\{\alpha = e_1 \log_b p_1 + e_2 \log_b p_2 + \cdots e_k \log_b p_k.$$

pour déterminer $\log_b p_1$, ..., $\log_b p_k$.
On cherche β tel que $b^\beta g$ est friable

$$b^\beta g = p_1^{f_1} p_2^{f_2} \cdots p_k^{f_k}$$

$$\log_b g = -\beta + f_1 \log_b p_1 + \cdots + f_k \log_b p_k$$

Brutal en apparence, complexité ok selon mise en œuvre de l'idée.

Couplages

Définition des couplages

Définition

Un couplage (en anglais *pairing*) 👫 sur une courbe elliptique $\mathcal{E}$ est une application

$$e : \underbrace{\mathcal{E}[r]}_{r-\text{torsion}} \times \mathcal{E}[r] \to \underbrace{\mu_r}_{\text{racines } r^{\text{ièmes}} \text{ de l'unité}}$$

telle que

- $\forall P, P', Q \in \mathcal{E}, \quad e(P + P', Q) = e(P, Q)e(P', Q)$
- $\forall P, Q, Q' \in \mathcal{E}, \quad e(P, Q + Q') = e(P, Q)e(P, Q')$
- $\forall P \in \mathcal{E} \setminus 0_{\mathcal{E}}, \exists Q \in \mathcal{E} , \quad e(P, Q) \neq 1$
- $\forall Q \in \mathcal{E} \setminus 0_{\mathcal{E}}, \exists P \in \mathcal{E} , \quad e(P, Q) \neq 1$

Dans la pratique

Remarque : si t t.q. $r|q^t - 1$, alors $\mu_r \subseteq \mathbb{F}_{q^t}$ et $\mu_r \simeq \mathbb{F}_{q^t}/(\mathbb{F}_{q^t})^r$.

Exemple

Deux couplages sont employés pour les courbes elliptiques

- Le couplage de Tate
- Le couplage de Weil

Applications en cryptographie

- Attaque de Menezes, Okamoto et Vanstone sur le log discret
- Diffie-Hellman triparti (Joux 2000)
- Chiffrement fondé sur l'identité (Boneh-Franklin 2004)
- Signatures courtes (Boneh-Lynn-Shacham 2004)

Attaque de M.O.V. sur le logarithme discret

Soient $B, G \in \mathcal{E}$ et $k \in \mathbb{Z}$ tels que $G = k \cdot B$. On note r l'ordre de B.

But :
Trouver k à partir de B et G.

Idée :
Pour tout $S \in \mathcal{E}$,

$$e(G,S) = e(kB,S) = e(B,S)^k$$

Conditions de fonctionnement :
Travailler dans $\mathbb{F}_{q^t}$ avec $r|q^t - 1$ pour assurer l'existence de racines r-ièmes de l'unité où r est l'ordre B.

$\rightarrow$ l'attaque n'est viable que si t est petit.

Fonctions de Miller et couplage de Tate

Pour $S \in \mathcal{E}[r]$ (point de r-torsion), on appelle fonction de Miller la fonction $f_{r,S}$ (unique à constante près) telle que

$$\mathrm{div}(f_{r,S}) = r \cdot (S) - r \cdot (0_{\mathcal{E}}).$$

Pour $T \in \mathcal{E}[r]$, on pose (le choix de Q n'a pas d'importance)

$$\hat{D}_T = (T + Q) - (Q)$$

Définition (Couplage de Tate)

$$\langle S, T \rangle_r = f_S(\hat{D}_T) = \frac{f_S(T+Q)}{f_S(Q)} \quad \mathbf{mod} \text{ puissances } r\text{-ième}$$

Couplage de Weil

On définit de également un second couplage, dit couplage de Weil.

Théorème (Couplage de Weil)
Le couplage de Weil se calcule par la formule

$$e_r(S,T) = \frac{\langle S,T\rangle_r}{\langle T,S\rangle_r} \mod \textit{puissances } r\textit{-ième}$$

Evaluer une fonction de Miller

On note $f_{m,S}$ la fonction (unique à constante près) telle que

$$\mathrm{div}(f_{m,S}) = m(S) - (m \cdot S) - (m-1)(0_{\mathcal{E}}).$$

On note ℓ_{P_1,P_2} une équation de la droite passant par P_1 et P_2 et h_{P_1,P_2} la fraction $h_{P_1,P_2} = \frac{\ell_{P_1,P_2}}{\ell_{P_1+P_2,-P_1-P_2}}$

On a (par observation des diviseurs)

$$f_{m+1,S} = f_{m,S} \cdot h_{mS,S}$$

$$f_{2m,S} = f_{m,S}^2 \cdot h_{mS,mS}$$

On en déduit un algorithme qui calcule $f_{r,S}(P)$ en remontant la décomposition binaire de r.