Algorithmes arithmétiques pour la cryptologie — 19 octobre 2015, Paris

Un algorithme quasi-polynomial

Razvan Barbulescu

CNRS et IMJ-PRG

Outline of the talk

- Corps finis de petite caractéristique

- Algorithmes classiques de log discret en petite caractéristique

- L'algorithme quasi-polynomial

Corps finis

Definition

Étant donné un nombre premier p et un polynôme irréductible $\varphi \in \mathbb{F}_p$, le corps défini par φ est l'ensemble $\mathbb{F}_p[x]/\langle\varphi\rangle$, muni des opérations

- addition: on ajoute les éléments comme les polynômes;
- multiplication: on multiplie les éléments comme polynômes et on réduit modulo φ;
- inversion: algorithme d'Euclide étendu.

On appelle p la caractéristique du corps et φ son polynôme de définition.

Example

$\varphi = x^2 + x + 1 \in \mathbb{F}_2[x]$ est irréductible car il n'a pas de racines, donc il définit un corps de 4 éléments: $0, 1, x, x + 1$. Pour calculer l'inverse d'un élément, disons $a = x$, on applique EEA à a et $b = \varphi$:

$$1 = 1 \cdot (x^2 + x + 1) + (x + 1) \cdot x$$

. Le gcd est toujours 1 car φ est irréductible. Ici $x^{-1} = x + 1$.

Le calcul des isomorphismes de corps

Propriétés

- Si φ_1 et φ_2 sont deux polynômes irréductibles de $\mathbb{F}_p[x]$ de même degré, alors on a l'isomorphisme de corps:

$$\mathbb{F}_p[x]/\langle\varphi_1\rangle \simeq \mathbb{F}_p[x]/\langle\varphi_2\rangle.$$

  Temps polynomial, changement de coordonnées.
- Pour toute paire (p, n), il existe $(1 + o(1))p^n/n$ polynômes irréductibles de degré n dans $\mathbb{F}_p[x]$.

$\boxed{\mathbb{F}_{p^n} \text{ et } \mathrm{GF}(p^n) \text{ désigne “un corps de } p^n \text{ éléments”}}$

Example

Les polynômes $\varphi_1 = x^3 + x + 1$ et $\varphi_2 = x^3 + x^2 + 1$ sont irréductibles modulo 2 (degré ≤ 3 et pas de racines). On calcule a, b, c tels que

$$\varphi_1(a + bx + cx^2) \equiv 0 \mod \varphi_2.$$

Alors, on envoie tout élément $P(x)$ du corps défini par φ_1 dans le corps défini par φ_2 comme suit

$$P(x) \mapsto P(a + bx + cx^2).$$

Ici $(a, b, c) = (1, 1, 0)$, et par exemple $x^2 + x + 1 \mapsto (x^2 + x)^2 + (x^2 + x) + 1 = x^2$.

Logs discrets dans les corps finis

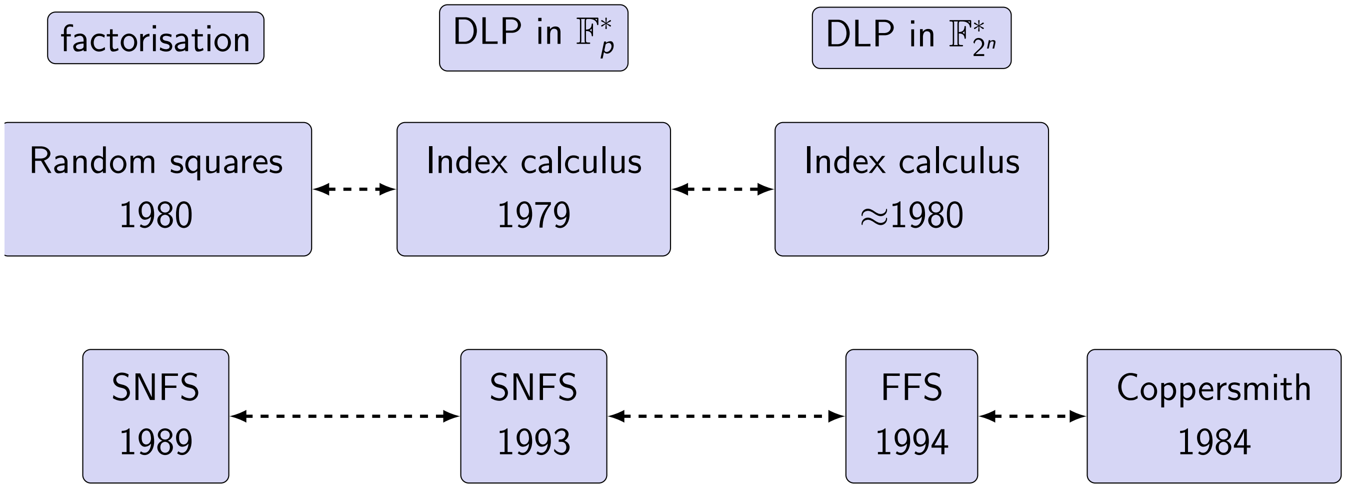
Le groupe multiplicatif

- le groupe multiplicatif $(\mathbb{F}_{p^n})^*$ est cyclique
- d'ordre $p^n - 1$, qui peut être premier, e.g. $2^{607} - 1$.
- Une proportion de $\varphi(p^n - 1)/(p^n - 1)$ des éléments sont des générateurs, étant faciles à trouver (φ=indicatrice d'Euler).
- Pour tout $a \in (\mathbb{F}_{p^n})^*$, $a^{p^n-1} = 1$.

Avantages des corps de petite caractéristique

- on peut sélectionner un polynôme de définition creux, e.g. $x^n + x + 1$ quand celui-ci est irréductible, afin d'accélérer la multiplication;
- la complexité de la multiplication des polynômes est meilleure que celle des entiers ($O(n \log n)$ et respectivement $O(n \log n 2^{O(1) \log^* n})$);
- l'arithmétique est implantée dans plusieurs bibliothèques C: NTL et gf2x;
- les processeurs Intel offrent des instructions spécifiques aux polynômes sur $\mathbb{F}_2$;
- dans le cas du matériel dédié à la crypto, par ex à l'aide de FPGA, il est plus facile d'implanter la multiplication dans $\mathbb{F}_{2^n}$ et $\mathbb{F}_{3^n}$ que dans $\mathbb{F}_p$.

Histoire



Chronologie

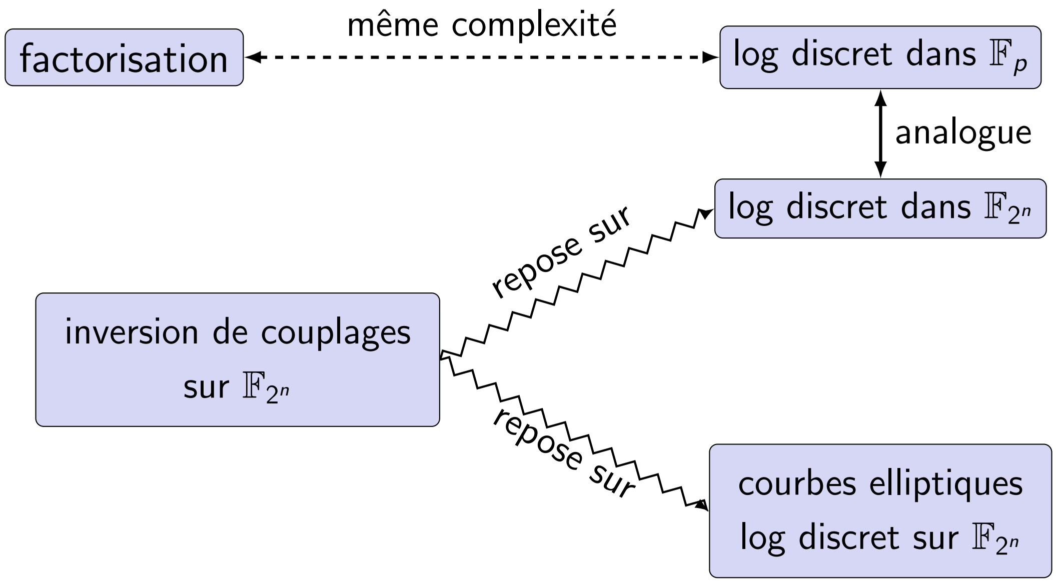
- En 1984, l'algorithme de Coppersmith a été le premier de complexité $L(1/3)$.
- En 1989 et 1993, le crible algébrique spécial(SNFS) puis crible algébrique(NFS) ont eu aussi une complexité de type $L(1/3)$.
- En 1993 et 1994 NFS a été adapté au log discret dans $\mathbb{F}_p$ et, par analogie, à $\mathbb{F}_{2^n}$ sous le nom de crible des corps de fonctions(FFS).
- En 1999, on a trouvé comment obtenir l'algorithme de Coppersmith comme cas particulier de FFS.

Renaissance due aux couplages

Utilisation des corps de petite caractéristique

- Depuis 1984, la petite caractéristique paraissait beaucoup plus faible que la grande caractéristique et la factorisation, donc elle a été abandonnée.
- En 2000 Antoine Joux a proposé d'utiliser les couplages pour chiffrer, alors qu'auparavant on les utilisaient pour la cryptanalyse.
- Les couplages en caractéristique 2 et 3 sont les plus rapides et ont fait l'objet de nombreuses implantations.
- En 2013 Joux, Boneh et Franklin ont reçu le prix Gödel pour leurs travaux concernant les couplages.
- La NIST et plusieurs compagnies privées ont étudié les applications des couplages.

Les relations du log discret en petite caractéristique avec les autres problèmes



F_Q est un corps à Q éléments, Q puissance de premier.

Outline of the talk

- Corps finis de petite caractéristique
- Algorithmes classiques de log discret en petite caractéristique
- L'algorithme quasi-polynomial

Friabilité

Definition

On dit qu'un polynôme de $\mathbb{F}_q[t]$ est m-friable s'il se factorise en polynômes de degré inférieur ou égal à m.

Theorem

La probabilité qu'un polynôme de degré n soit m-friable est $1/u^{u(1+o(1))}$ où $u = \frac{n}{m}$.

Cas particuliers:

- $n = D$, $m = D/6$: probabilité constante;
- $n = D$, $m = 1$: probabilité $1/D! \approx 1/D^D$.

Collecte de relations

Le corps $\mathbb{F}_{q^k}$ est représenté par $\mathbb{F}_q[t]/\varphi$
pour un polynôme irréductible $\varphi \in \mathbb{F}_q[t]$ de degré k.

Example

Prenons $q = 3$, $k = 5$, $\varphi = t^5 + t^4 + 2t^3 + 1$, $g = t \in \mathbb{F}_{3^5}$ et $\ell = 11 \mid 3^5 - 1$. On a

$$t^5 \equiv 2(t+1)(t^3+t^2+2t+1) \mod \varphi$$

Collecte de relations

Le corps $\mathbb{F}_{q^k}$ est représenté par $\mathbb{F}_q[t]/\varphi$
pour un polynôme irréductible $\varphi \in \mathbb{F}_q[t]$ de degré k.

Example

Prenons $q = 3$, $k = 5$, $\varphi = t^5 + t^4 + 2t^3 + 1$, $g = t \in \mathbb{F}_{3^5}$ et $\ell = 11 \mid 3^5 - 1$. On a

$$\begin{aligned} t^5 &\equiv 2(t+1)(t^3+t^2+2t+1) && \mod \varphi \\ t^6 &\equiv 2(t^2+1)(t^2+t+2) && \mod \varphi \end{aligned}$$

Collecte de relations

Le corps $\mathbb{F}_{q^k}$ est représenté par $\mathbb{F}_q[t]/\varphi$
pour un polynôme irréductible $\varphi \in \mathbb{F}_q[t]$ de degré k.

Example

Prenons $q = 3$, $k = 5$, $\varphi = t^5 + t^4 + 2t^3 + 1$, $g = t \in \mathbb{F}_{3^5}$ et $\ell = 11 \mid 3^5 - 1$. On a

$$\begin{array}{lcll} t^5 & \equiv & 2(t+1)(t^3+t^2+2t+1) & \mod \varphi \\ t^6 & \equiv & 2(t^2+1)(t^2+t+2) & \mod \varphi \\ t^7 & \equiv & 2(t+2)(t+1)(t+1) & \mod \varphi \end{array}$$

Collecte de relations

Le corps $\mathbb{F}_{q^k}$ est représenté par $\mathbb{F}_q[t]/\varphi$
pour un polynôme irréductible $\varphi \in \mathbb{F}_q[t]$ de degré k.

Example

Prenons $q = 3$, $k = 5$, $\varphi = t^5 + t^4 + 2t^3 + 1$, $g = t \in \mathbb{F}_{3^5}$ et $\ell = 11 \mid 3^5 - 1$. On a

$$\begin{aligned}
t^5 &\equiv 2(t+1)(t^3+t^2+2t+1) &\mod \varphi\\
t^6 &\equiv 2(t^2+1)(t^2+t+2) &\mod \varphi\\
t^7 &\equiv 2(t+2)(t+1)(t+1) &\mod \varphi
\end{aligned}$$

La dernière relation donne:

$$7\log_g t \equiv \log_g 2 + 1\log_g(t+2) + 2\log_g(t+1) \mod 11$$

Collecte de relations

Le corps $\mathbb{F}_{q^k}$ est représenté par $\mathbb{F}_q[t]/\varphi$
pour un polynôme irréductible $\varphi \in \mathbb{F}_q[t]$ de degré k.

Example

Prenons $q = 3$, $k = 5$, $\varphi = t^5 + t^4 + 2t^3 + 1$, $g = t \in \mathbb{F}_{3^5}$ et $\ell = 11 \mid 3^5 - 1$. On a

$$\begin{aligned} t^5 &\equiv 2(t+1)(t^3+t^2+2t+1) && \bmod \varphi \\ t^6 &\equiv 2(t^2+1)(t^2+t+2) && \bmod \varphi \\ t^7 &\equiv 2(t+2)(t+1)(t+1) && \bmod \varphi \end{aligned}$$

La dernière relation donne:

$$7 \log_g t \equiv \cancel{\log_g 2} + 1 \log_g(t+2) + 2 \log_g(t+1) \quad \bmod 11$$

Proposition

Si $a \in \mathbb{F}_q^*$ et ℓ est un facteur de $q^k - 1$ relativement premier avec $(q-1)$, alors $\log a \equiv 0 \mod \ell$.

Collecte de relations

Le corps $\mathbb{F}_{q^k}$ est représenté par $\mathbb{F}_q[t]/\varphi$
pour un polynôme irréductible $\varphi \in \mathbb{F}_q[t]$ de degré k.

Example

Prenons $q = 3$, $k = 5$, $\varphi = t^5 + t^4 + 2t^3 + 1$, $g = t \in \mathbb{F}_{3^5}$ et $\ell = 11 \mid 3^5 - 1$. On a

$$\begin{aligned} t^5 &\equiv 2(t+1)(t^3+t^2+2t+1) && \mod \varphi \\ t^6 &\equiv 2(t^2+1)(t^2+t+2) && \mod \varphi \\ \\ t^8 &\equiv \dots \end{aligned}$$

La dernière relation donne:

$$\begin{aligned} 7\log_g t &\equiv 1\log_g(t+2) + 2\log_g(t+1) && \mod 11 \\ 8\log_g(t+1) &\equiv 1\log_g(t+2) && \mod 11 \\ 9\log_g(t+2) &\equiv 2\log_g t && \mod 11 \end{aligned}$$

On trouve $\log_g(t+1) \equiv 158 \mod 11$ et $\log_g(t+2) \equiv 54 \mod 11$.

Descente

Example (suite)

On se propose de calculer $\log_g P$ pour un polynôme arbitraire, disons $P = t^4 + t + 2$. On a

$$\begin{aligned} P^2 &\equiv t^4 + t^3 + 2t^2 + 2t + 2 && \bmod \varphi \\ P^3 &\equiv 2(t+1)(t+2)(t^2+1) && \bmod \varphi \\ P^4 &\equiv (t+1)(t+2)t^2 && \bmod \varphi. \end{aligned}$$

Descente

Example (suite)

On se propose de calculer $\log_g P$ pour un polynôme arbitraire, disons $P = t^4 + t + 2$. On a

$$\begin{aligned} P^{2} &\equiv t^4 + t^3 + 2t^2 + 2t + 2 && \mod \varphi \\ P^{3} &\equiv 2(t+1)(t+2)(t^2+1) && \mod \varphi \\ P^{4} &\equiv (t+1)(t+2)t^2 && \mod \varphi. \end{aligned}$$

En prenant le log discret on trouve

$$4 \log_g P = 1 \log_g(t+1) + 1 \log_g(t+2) + 2 \log_g t.$$

Donc $\log_g P = 114$.

Le log discret des constantes

Ici ℓ est un facteur premier de l'ordre du groupe, $q^k - 1$, supérieur à $q - 1$.

Éléments de $\mathbb{F}_q$

Éléments de $\mathbb{F}_q \subset \mathbb{F}_{q^k}$ sont représenté dans $\mathbb{F}_q[t]/\langle\varphi\rangle$ comme constantes a. Ils vérifient $a^{q-1} = 1$, donc on a

$$\log_g(a^{q-1}) \equiv \log_g(1) \equiv 0 \mod \ell.$$

Alors,

$$(q-1)\log_g a \equiv 0 \mod \ell.$$

Puisque ℓ est premier et supérieur à $q - 1$,

$$\log_g a \equiv 0 \mod \ell.$$

Outline of the talk

- Corps finis de petite caractéristique
- Algorithmes classiques de log discret en petite caractéristique
- L'algorithme quasi-polynomial

Résultat principal

Théorème (sous heuristiques)

Soit K un corps fini $\mathbb{F}_{q^k}$. On résout le problème du logarithme discret dans K en temps heuristique

$$\max(q,k)^{O(\log k)}.$$

Cas particuliers:

- $K = \mathbb{F}_{2^n}$, pour n premier. Complexité: $n^{O(\log n)}$. Considérablement plus faible que $L_{2^n}(1/4 + o(1)) \approx 2^{\sqrt[4]{n}}$ (état d'art: Joux 2013).
- $K = \mathbb{F}_{q^k}$, avec $q = k^{O(1)}$. Complexité : $\log Q^{O(\log\log Q)}$, où $Q = \#K$. Rappel: cela s'écrit $L_Q(o(1))$.
- $K = \mathbb{F}_{q^k}$, avec $q \approx L_{q^k}(\alpha)$. Complexité est $L_{q^k}(\alpha + o(1))$, c-à-d mieux que l'algorithme de Joux-Lercier et FFS quand $\alpha < 1/3$.

Un nouveau modèle pour $\mathbb{F}_{q^{2k}}$

On commence par un cas particulier

On suppose d'abord que $k \approx q$ et $k \leq q + 2$.

Choix de φ (même que dans l'algorithme de Joux)

Tirer au hasard $h_0, h_1 \in \mathbb{F}_{q^2}[t]$ avec $\deg h_0, \deg h_1 \leq 2$ jusqu'à ce que $T(t) := h_1(t)t^q - h_0(t)$ a un facteur irréductible φ de degré k.

Heuristique

L'existence de h_0 et h_1 est heuristique, mais il est trouvé en pratique après $O(k)$ essais.

Propriétés de φ

- $h_1(t)t^q \equiv h_0(t) \mod \varphi$;
- $P(t^q) \equiv P\left(\frac{h_0}{h_1}\right) \mod \varphi$;
- $P^q \equiv \tilde{P}(t^q) \equiv \tilde{P}\left(\frac{h_0}{h_1}\right) \mod \varphi$,
  où le signe tilde désigne la conjugaison dans $\mathbb{F}_{q^2}$.

Une identité célèbre

Rappelons l'identité

$$x^q - x = \prod_{\alpha \in \mathbb{F}_q} (x - \alpha).$$

Cela donne $x^q y - x y^q = \prod_{(\alpha:\beta) \in \mathbb{P}^1(\mathbb{F}_q)} (\beta x - \alpha y)$.

Une identité célèbre

Rappelons l'identité

$$x^q - x = \prod_{\alpha \in \mathbb{F}_q} (x - \alpha).$$

Cela donne $x^q y - x y^q = \prod_{(\alpha:\beta) \in \mathbb{P}^1(\mathbb{F}_q)} (\beta x - \alpha y)$.

Une machine à produire des relations

- $x = t$ et $y = 1$: $h_0/h_1 - t \equiv t^q - t \equiv \prod_{\alpha \in \mathbb{F}_q} (t - \alpha)$.
  Si le numérateur du membre de gauche est friable, on obtient des relations entre les polynômes linéaires.
- $x = t + a$, $a \in \mathbb{F}_q$, et $y = 1$: même relation.
- $x = t + a$, $a \in \mathbb{F}_{q^2}$, et $y = 1$: nouvelles relations. L'algorithme de Joux utilise déjà cette idée.
- Soit P un polynôme pour lequel on cherche le log discret.

Une identité célèbre

Rappelons l'identité

$$x^q - x = \prod_{\alpha \in \mathbb{F}_q} (x - \alpha).$$

Cela donne $x^q y - x y^q = \prod_{(\alpha:\beta) \in \mathbb{P}^1(\mathbb{F}_q)} (\beta x - \alpha y)$.

Une machine à produire des relations

- $x = t$ et $y = 1$: $h_0/h_1 - t \equiv t^q - t \equiv \prod_{\alpha \in \mathbb{F}_q} (t - \alpha)$.
  Si le numérateur du membre de gauche est friable, on obtient des relations entre les polynômes linéaires.
- $x = t + a$, $a \in \mathbb{F}_q$, et $y = 1$: même relation.
- $x = t + a$, $a \in \mathbb{F}_{q^2}$, et $y = 1$: nouvelles relations. L'algorithme de Joux utilise déjà cette idée.
- Soit P un polynôme pour lequel on cherche le log discret.
  $x = aP + b$ et $y = cP + d$, $a, b, c, d \in \mathbb{F}_{q^2}$: montrons que le côté gauche est congruent à un polynôme de petit degré, tandis que le membre droit est friable dans un nouveau sens.

Le membre droit est “friable”

$$
\begin{aligned}
(aP+b)^q(cP+d)-(aP+b)(cP+d)^q &= \prod_{(\alpha,\beta)\in\mathbb{P}^1(\mathbb{F}_q)} \beta(aP+b)-\alpha(cP+d)\\
&= \prod_{(\alpha,\beta)\in\mathbb{P}^1(\mathbb{F}_q)} (-c\alpha+a\beta)P-(d\alpha-b\beta)\\
&= \lambda \prod_{(\alpha,\beta)\in\mathbb{P}^1(\mathbb{F}_q)} \left(P-\frac{d\alpha-b\beta}{a\beta-c\alpha}\right),
\end{aligned}
$$

Dans chaque relation apparaissent $q+1$ sur q^2+1 éléments de $\{1\}\bigcup\{P+\gamma:\gamma\in\mathbb{F}_{q^2}\}$.

Le membre de gauche est petit

Pour $m \in \mathrm{GL}_2(\mathbb{F}_{q^2})$, on note $\mathcal{L}_m$ le reste

$$\mathcal{L}_m := h_1^{\deg P}\left((aP+b)^q(cP+d) - (aP+b)(cP+d)^q\right) \mod \varphi(t).$$

Le membre de gauche est petit

Pour $m \in \mathrm{GL}_2(\mathbb{F}_{q^2})$, on note $\mathcal{L}_m$ le reste

$$\mathcal{L}_m := h_1^{\deg P}\left((aP+b)^q(cP+d)-(aP+b)(cP+d)^q\right) \mod \varphi(t).$$

On a $\deg \mathcal{L}_m \leq 3 \deg P$. En effet, on a

$$\begin{aligned}\mathcal{L}_m &= h_1^{\deg P}(\tilde{a}\tilde{P}(t^q)+\tilde{b})(cP+d)-(aP(t)+b)(\tilde{c}\tilde{P}(t^q)+\tilde{d}) \\ &= h_1^{\deg P}\left(\tilde{a}\tilde{P}\left(\frac{h_0}{h_1}\right)+\tilde{b}\right)(cP+d)-(aP+b)\left(\tilde{c}\tilde{P}\left(\frac{h_0}{h_1}\right)+\tilde{d}\right).\end{aligned}$$

Pour une proportion constante de matrices m, $\mathcal{L}_m$ est $(\deg P)/2$-friable.

Procédure pour "casser" un polynôme P

Chaque matrice m de l'ensemble quotient $\mathcal{P}_q := \mathrm{PGL}_2(\mathbb{F}_{q^2})/\mathrm{PGL}_2(\mathbb{F}_q)$ tel que $\mathcal{L}_m$ est $(\deg P)/2$-friable produit une équation différente

$$\prod_i P_{i,m}^{e_{i,m}} = \lambda \prod_{\gamma \in \mathbb{P}^1(\mathbb{F}_{q^2})} (P+\gamma)^{v_m(\gamma)},$$

où

- $\deg P_i \leq (\deg P)/2$;
- $v_m(\gamma)$ sont les exposants;
- λ sont des constantes dans $\mathbb{F}_{q^2}$.

En prenant les logs discrets on trouve

$$\sum_i e_{i,m} \log P_{i,m} \equiv \sum_\gamma v_m(\gamma) \log(P+\gamma) \mod \ell.$$

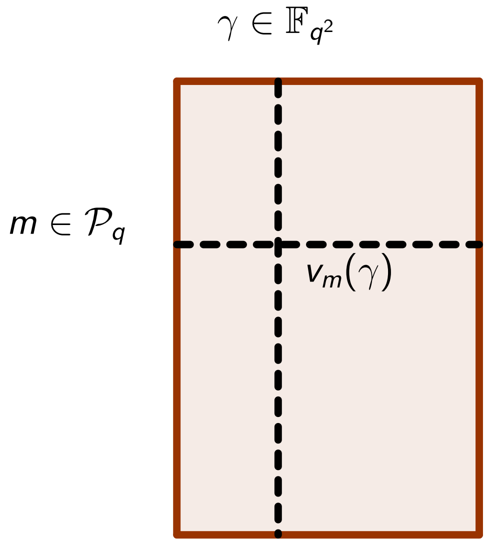
Heuristique

On dispose d'un nombre suffisant d'équations pour les combiner et obtenir

$$\sum_{i,m} e'_{i,m} \log P_{i,m} \equiv \log P \mod \ell.$$

L'étape d'algèbre linéaire pour P

Puisque $\#\mathrm{PGL}_2(\mathbb{F}_{q^i}) = q^{3i} - q^i$, $\#\mathcal{P}_q = q^3 + q$. Une fraction constante d'éléments produisent des équations linéaires entre les log discrets, donc la matrice ci-dessous a plus de lignes que de colonnes.



Due à l'heuristique on peut combiner ses lignes pour obtenir

$$(1, 0, \ldots, 0).$$

Brique de base de l'algorithme quasi-polynomial

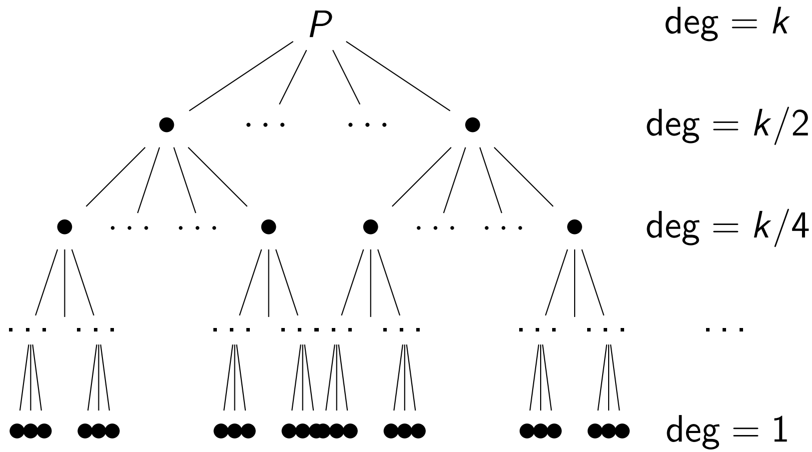
On vient de prouver:

Proposition (sous heuristiques)

Il existe un algorithme de complexité polynomiale en q et k, qui résout les deux tâches suivantes.

1. Étant donné un élément de $\mathbb{F}_{q^{2k}}$ représenté par un polynôme $P \in \mathbb{F}_{q^2}[t]$ avec $2 \leq \deg P \leq k-1$, l'algorithme renvoie une expression de $\log P$ comme combinaison linéaire d'au plus $O(kq^2)$ logarithmes $\log P_i$ avec $\deg P_i \leq \lceil \frac{1}{2} \deg P \rceil$ et de $\log h_1$.
2. L'algorithme renvoie le logarithme de h_1 et ceux de tous les éléments de $\mathbb{F}_{q^{2k}}$ de la forme $t + a$, pour a dans $\mathbb{F}_{q^2}$.

Complexité



Propriétés de l'arbre de descente

- hauteur$=\log k$ car on divise par deux le degré à chaque niveau;
- arité$=O(q^2k)$ car les enfants sont les facteurs irréductibles de s q^2 membres droits;
- nombre de nœuds$=q^{O(\log k)}$ car $k \leq q+2$.

Conclusion

- Le calcul de logarithmes discrets dans les corps de petite caractéristique a été introduit en cryptologie car l'arithmétique est plus rapide;
- abandonné en 1984 après la publication de l'algorithme de Coppersmith
- réintroduit en 2000 grâce à Antoine Joux
- asymptotiquement faible après l'algorithme quasi-polynomial.
- Les couplages de petite caractéristique sont cassés pour les tailles de clé proposées dans les articles de recherche.