QUELQUES MATHÉMATIQUES DE LA CRYPTOLOGIE À CLÉS PUBLIQUES

par

Jean-Marc Couveignes

Résumé. — Cette note présente quelques développements mathématiques plus ou moins récents de la cryptologie à clés publiques.

***Abstract* (A few mathematical tools for public key cryptology)**
I present examples of mathematical objects that are of interest for public key cryptography.

Table des matières

La cryptologie à clés publiques a mobilisé depuis son invention des mathématiques plus ou moins élémentaires : arithmétique des congruences, théorie algébrique des nombres, géométrie et cohomologie des groupes algébriques, théorie des graphes, probabilités discrètes, complexité algorithmique, etc. Il n'est pas toujours facile de discerner une ligne directrice dans ces développements et c'est une des difficultés du domaine. Je me bornerai donc à présenter quelques idées et situations typiques, sans aucune prétention à l'exhaustivité.

La section 1 décrit deux protocoles classiques de la cryptographie à clés publiques dans le cadre général de l'action d'un groupe sur un ensemble fini. Le logarithme discret offre une exemple de cette situation. Les groupes utilisés sont le plus souvent des groupes de points rationnels d'un groupe algébrique commutatif sur un corps fini. Je montre dans la section 2 quel genre de propriétés on attend (ou on redoute) d'un groupe algébrique dans ce contexte. La section 3 met en jeu non plus un groupe algébrique mais une catégorie de groupes, leurs morphismes, et les graphes qui s'en déduisent.

***Classification mathématique par sujets* (2000).** — 94A60, 11Y16, 14Q05, 14Q15, 20G40, 14L10.
Mots clefs. — jacobienne, complexité algorithmique, cryptologie à clés publiques, groupe algébrique commutatif, courbe algébrique, corps fini.

L'auteur est soutenu par le fond national pour la science (ACI NIM), et par le Centre d'électronique de l'Armement (CELAR, DGA).

1. Espaces homogènes difficiles

Dans cette section nous décrivons une famille de problèmes calculatoires que nous appelons espaces homogènes difficiles (EHD). Nous montrons que cette notion offre un cadre naturel à nombre de protocoles fondamentaux de la cryptologie à clé publique, pour le chiffrement, l'identification, et l'échange de clé par exemple.

Le problème du logarithme discret (dans un groupe multiplicatif ou une courbe elliptique sur un corps fini) fournit un exemple d'EHD. Mais il existe bien d'autres EHD. Ceux que nous présentons dans la section 3 proviennent de la multiplication complexe des courbes elliptiques.

Dans le paragraphe 1.1 nous définissons les espaces homogènes difficiles. Nous expliquons au paragraphe 1.2 pourquoi le logarithme discret est un cas particulier d'espace homogène. Nous présentons dans le paragraphe 1.3 un protocole d'échange de clés de type Diffie-Hellman-Merkle dans le contexte des EHD. Nous décrivons de même dans le paragraphe 1.4 le protocole de Schnorr pour la preuve de connaissance sans apport d'information, dans le cadre général et naturel des EHD.

1.1. Définition d'un espace homogène difficile. — Soit G un groupe fini commutatif. Un espace homogène H pour G est un ensemble fini non vide H muni d'une action transitive et libre de G. Donc le cardinal de H est égal à celui de G. On note $S = \#H = \#G$. On appelle *points* les éléments de H et *vecteurs* les éléments de G. Un exemple naturel : H est un espace affine et G l'espace vectoriel sous-jacent.

Si h_1 et h_2 sont deux points, il existe un unique vecteur g tel que $g.h_1 = h_2$. On note $\overrightarrow{h_1h_2}$ ce vecteur.

Étant donné un espace homogène, on considère une série de problèmes calculatoires.

On suppose que les éléments de G et de H sont représentés par des chaînes de caractères de longueur polynomiale en $\log S$.

On doit être capable de calculer efficacement la loi de composition et l'inversion dans le groupe G et de tester l'égalité de deux éléments de ce groupe. Autrement dit, on veut que le groupe G soit calculatoire.

Problème 1 **(Opérations dans le groupe G)**. — *Étant donnés deux vecteurs g_1 et g_2, décider s'ils sont égaux, calculer l'inverse g_1^{-1} de g_1 et le produit g_1g_2.*

Il faut aussi pouvoir choisir des éléments aléatoires dans G.

Problème 2 **(Vecteur aléatoire)**. — *Choisir un vecteur g dans G avec une distribution (presque) uniforme.*

On souhaite aussi résoudre efficacement les problèmes élémentaires suivants concernant l'action de G sur H :

Problème 3 **(Action de G sur H)**. — *Étant donnés deux points $h_1, h_2 \in H$ et un vecteur $g \in G$, décider si $h_1 = h_2$, et calculer $g.h_1$.*

Notons que si l'on applique un vecteur aléatoire (avec distribution uniforme) g à un point fixe h_0, on obtient un point aléatoire (avec distribution uniforme).

On dit que l'espace homogène est calculatoire si l'on dispose d'un algorithme probabiliste polynomial en $\log S$ pour résoudre les problèmes 1, 2 et 3. Cela sous-entend que l'on considère, non pas un espace homogène, mais une famille infinie d'espaces homogènes.

Venons en maintenant à des propriétés plus subtiles.

Souvenons nous qu'il existe un unique vecteur $\overrightarrow{h_1h_2}$ qui envoie h_1 sur h_2 :

$$\overrightarrow{h_1h_2}.h_1 = h_2.$$

On peut souhaiter calculer ce vecteur.

Problème 4 **(Différence de deux points).** — *Étant donnés $h_1, h_2 \in H$ trouver $g \in G$ tel que $g.h_1 = h_2$.*

Un problème de même nature est de compléter un parallélogramme.

Problème 5 **(Complétion d'un parallélogramme).** — *Étant donnés trois points $h_1, h_2, h_3 \in H$, calculer l'unique point h_4 tel que $\overrightarrow{h_1h_2} = \overrightarrow{h_3h_4}$.*

Ce h_4 n'est autre que $\overrightarrow{h_1h_2}.h_3$. Donc le problème 5 est plus facile que le problème 4.

On s'intéresse aux espaces homogènes calculatoires pour lesquels les problèmes 4 et 5 sont difficiles. Cela signifie qu'il n'existe pas de machine de Turing probabiliste qui résolve l'un ou l'autre de ces problèmes en temps polynomial en $\log S$.

De tels espaces homogènes sont appelés espaces homogènes difficiles (EHD).

On pourrait considérer un autre problème

Problème 6 **(Vérification d'un parallélogramme).** — *Étant donnés quatre points h_1, h_2, h_3, h_4 dans H, dire si $\overrightarrow{h_1h_2} = \overrightarrow{h_3h_4}$.*

Si ce dernier problème est difficile on dit que l'espace homogène est très difficile (EHTD).

Supposons que $G = k^d$ est un espace vectoriel sur un corps fini k et $H = \mathbb{A}^d(k)$ l'espace affine associé. C'est un espace calculatoire. Les vecteurs et les points sont décrits pas leurs coordonnées et l'action de $g = (x_1, \ldots, x_d)$ sur $h = (a_1, \ldots, a_d)$ se calcule au prix de d additions dans k.

Ce n'est pas un espace homogène difficile car si $h = (a_1, \ldots, a_d)$ et $k = (b_1, \ldots, b_d)$ alors $\overrightarrow{hk} = (b_1 - a_1, \ldots, b_d - a_d)$ se calcule au prix de d soustractions dans k.

1.2. Le logarithme discret. — Un premier candidat EHD intéressant est fourni par le problème du logarithme discret.

Soit C un groupe cyclique d'ordre n et soit c un générateur de C.

Notons G le groupe des automorphismes de C. Un élément g de G envoie c sur $g(c) = c^a$ où a est un entier premier à n. L'application $g \mapsto a$ est un isomorphisme de G sur $(\mathbb{Z}/n\mathbb{Z})^*$.

Soit H l'ensemble des générateurs de C. Alors $\#H = \#G = \phi(n)$ et G agit simplement transitivement sur H.

On suppose que C est un groupe calculatoire, que son ordre n est connu, et que la factorisation de n en produit de facteurs premiers est connue elle aussi. Alors on dispose d'algorithmes polynomiaux en $S = \phi(n)$ pour calculer dans $G = (\mathbb{Z}/n\mathbb{Z})^*$. Résoudre le problème 3 revient à calculer c^a pour c un générateur de C et a un entier entre 1 et n.

Un algorithme naïf calculerait successivement c, c^2, c^3, c^4, $\ldots$, c^{a-1}, c^a, ce qui requiert $a - 1$ opérations. Ce n'est pas satisfaisant car on souhaite calculer c^a en temps $\log S$.

L'algorithme utilisé est connu sous le nom d'exponentiation rapide. On calcule $c_0 = c$, $c_1 = c_0^2 = c^2$, $c_2 = c_1^2 = c^4$, $c_3 = (c_2)^2 = c^8$, $\ldots$, $c_x = c^{2^x}$ où 2^x est la plus grande puissance de 2 inférieure ou égale à a. On écrit alors l'exposant a en base 2 soit $a = \sum_{1\leq k\leq x} \epsilon_k 2^k$ et on vérifie que $c^a = \prod_{1\leq k\leq x} c_k^{\epsilon_k}$. Au total le calcul de c^a n'a pas requis plus de $2\log_2 a$ opérations dans C.

En revanche, si C est un groupe quelconque, alors on ne sait pas, en général, résoudre efficacement les problèmes 4 et 5. Par exemple, le problème 4 dans ce contexte est le suivant : étant donnés deux générateurs c et d de C, trouver un entier k tel que $d = c^k$. Cet entier $k \in \mathbb{Z}/n\mathbb{Z}$ est appelé logarithme discret de d en base c et noté $\log_c(d)$.

On observe que $\log_c$ s'étend en une application $\log_c : C \to \mathbb{Z}/n\mathbb{Z}$ qui est un isomorphisme de groupe. C'est l'application réciproque de l'exponentiation de base c notée $exp_c : \mathbb{Z}/n\mathbb{Z} \to C$ et définie par $\exp_c(k) = c^k$.

Le problème du *logarithme discret* a un sens pour tout groupe cyclique et c'est un cas particulier d'espace homogène.

Nous avons là un premier exemple d'espace homogène difficile. Il n'existe pas, en effet, d'algorithme générique pour calculer les logarithmes discrets[(1)].

Une petite difficulté subsiste : il n'existe pas de groupe générique. Rien n'interdit à un algorithme d'utiliser des propriétés particulières au groupe utilisé en pratique. On ne connaît pas d'algorithme pour résoudre le logarithme discret en temps polynomial en $\log n$ dans les groupes multiplicatifs de corps finis et on suppose qu'il n'en existe pas. Cela ne prouve pas cependant qu'il n'en existe pas. Il est généralement admis cependant que les espaces homogènes correspondants sont difficiles et même très difficiles.

Ce premier exemple d'EHD est aussi un exemple (tout aussi hypothétique) de fonction asymétrique. Cela signifie que les deux fonctions $\exp_c$ et $\log_c$ sont réciproques l'une de l'autre, que $\exp_c$ se calcule en temps polynomial (grâce à l'algorithme d'exponentiation rapide) mais que $\log_c$ ne se calcule pas en temps polynomial.

On trouve dans [**14**] une introduction à la cryptologie asymétrique. Le livre [**7**] est une introduction générale aux concepts de la cryptologie moderne. Le livre [**2**] est un traité général et récent de cryptologie.

1.3. Échange de clé. — Nous présentons dans ce paragraphe un exemple de protocole cryptographique qui repose sur un EHD. Il s'agit de la transposition évidente du protocole de Diffie-Hellman-Merkle dans le contexte des EHD.

On suppose qu'Alice et Bob communiquent par un canal non sécurisé (tout le monde peut entendre ou lire l'intégralité de leurs messages). Au début du protocole ils ne partagent aucun secret. À l'issue du protocole, ils ont un secret commun, c'est-à-dire une information connue d'eux seuls. Cette information pourra leur servir de clé secrète pour des échanges ultérieurs.

Voici comment ils procèdent. Ils conviennent publiquement d'un EHD H. Dans tout ce qui suit, le mot aléatoire sous-entend que la distribution est uniforme (ou très proche de la distribution uniforme).

1. Alice choisit un point aléatoire h_0 dans H et un vecteur aléatoire g_1 dans G. Elle applique g_1 à h_0 et calcule $h_1 = g_1.h_0$. Elle envoie le couple de points (h_0, h_1) à Bob.

[(1)] Un algorithme générique est un algorithme qui n'utilise pas d'autres propriétés de C que l'existence d'une loi de groupe. Shoup a montré qu'un tel algorithme ne peut pas calculer le logarithme discret en temps $o(\sqrt{P})$ où P est le plus grand facteur premier de l'ordre n de C.

2. Bob choisit un vecteur aléatoire g_2 dans G et l'applique à h_0. Il calcule donc $h_2 = g_2.h_0$. Il envoie h_2 à Alice. La clé secrète est $K = g_2.h_1$.
3. Alice calcule la clé secrète à partir des informations dont elle dispose : elle applique g_1 à h_2. En effet $K = g_2.h_1 = g_1.h_2$.

La commutativité de G joue ici un rôle essentiel. Alice et Bob conviennent d'une origine h_0 publique. Ils choisissent chacun un vecteur et construisent ensemble un parallélogramme. Trois sommets h_0, h_1, h_2 du parallélogramme sont publics mais le quatrième K est connu d'eux seuls. Alice connaît K car elle a choisi le coté g_1 et elle a reçu de Bob le sommet h_2. Bob connaît K car il a choisi le coté g_2 et il a reçu d'Alice le sommet h_1. Un observateur étranger à cet échange voit les trois sommets h_0, h_1 et h_2 mais aucun des cotés du parallélogramme. Il doit donc compléter le parallélogramme pour violer le secret commun à Alice et Bob. Et on suppose que ce calcul est trop difficile (il n'existe pas d'algorithme polynomial en temps pour le résoudre).

1.4. Preuve de connaissance sans apport d'information. — Nous présentons dans ce paragraphe le protocole de Schnorr dans le cadre des EHD.

On suppose qu'Alice a choisi un EHD H et un point h_0, ainsi qu'un vecteur aléatoire g_A. Elle applique le vecteur g_A au point h_0 et obtient le point $h_A = g_A.h_0$.

Elle publie G, H, h_0 et h_A et garde g_A secret. Le secret d'Alice est donc le vecteur $g_A = \overrightarrow{h_0h_A}$.

Alice veut prouver à Bob qu'elle connaît ce vecteur, sans le divulguer.

1. Alice choisit un vecteur $g_r \in G$ aléatoire et calcule $g_r.h_A = h_r$. Elle envoie h_r à Bob.
2. Bob tire à pile ou face et envoie le résultat $\epsilon \in \{0, 1\}$ à Alice.
3. Si $\epsilon = 0$ alors Alice envoie $g_p = g_r$ à Bob. Sinon elle envoie $g_p = g_r g_A$.
4. Bob vérifie que $g_p.h_A$ est égal à h_r (si $\epsilon = 0$) ou $g_p.h_0 = h_r$ (si $\epsilon = 1$).

Le protocole construit un triangle h_0, h_A, h_r. Pour prouver qu'elle connaît le coté $\overrightarrow{h_0h_A}$, Alice prouve qu'elle connaît les deux autres cotés du triangle. Selon la valeur de ϵ, Bob lui demandera de dévoiler $\overrightarrow{h_0h_r}$ ou $\overrightarrow{h_Ah_r}$. Comme elle ne sait pas laquelle de ces deux questions lui sera posée, elle doit connaître la réponse au deux questions.

Si elle ne connaît pas $\overrightarrow{h_0h_A}$ elle ne peut connaître à la fois $\overrightarrow{h_0h_r}$ et $\overrightarrow{h_Ah_r}$. Donc elle est prise en défaut par la question de Bob avec une probabilité $\geq \frac{1}{2}$.

On répète le protocole un nombre suffisant de fois pour que Bob se convainque qu'Alice connaît bien $\overrightarrow{h_0h_A}$.

De son coté, Bob n'apprend aucune information sur le secret d'Alice. Car tous les vecteurs qui lui sont communiqués ont une extrémité aléatoire. Un observateur extérieur au protocole n'apprend rien lui non plus. Alice n'a donc pas besoin de révéler quoi que ce soit de son secret pour prouver à Bob qu'elle le connaît. On mesure l'avantage de cette méthode sur le classique échange de mots de passe.

Le protocole d'échange de clés a été publié par Diffie et Hellman en 1976. Le travail de Merkle sur cette question a joué un rôle important dans ce domaine. Il semble bien que ce protocole ait été découvert antérieurement par Williamson dans le cadre de son travail pour les services secrets britanniques (raison pour laquelle il ne l'a pas publié).

2. Logarithmes discrets et groupes algébriques

On cherche des groupes finis, cycliques, où le logarithme discret soit difficile. Le groupe additif d'un corps fini n'est pas un bon candidat. Supposons par exemple que $C = (\mathbb{Z}/p\mathbb{Z}, +)$ pour p premier et soient g et h deux résidus modulo p. On suppose que g engendre C. Donc g est non nul modulo p. Le logarithme discret de h en base g est l'entier k tel que $h = kg$. Donc $k = \frac{h}{g} \bmod p$ se calcule à l'aide de l'algorithme d'Euclide en temps $\leq (\log p)^{2+o(1)}$ et même plus vite si l'on a recours à des algorithmes rapides.

Le groupe le plus souvent utilisé est le groupe multiplicatif $\mathrm{G_m}(\mathbb{F}_q) = \mathbb{F}_q^*$ d'un corps fini $\mathbb{F}_q$. Les algorithmes connus les plus rapides pour calculer les logarithmes discrets dans de tels groupes ont une complexité de $\exp(\log(q)^{\frac{1}{3}+o(1)})$. Ce ne sont donc pas des algorithmes polynomiaux. La contribution de Joux et Lercier à ce volume est entièrement consacrée à cette question.

D'autres groupes algébriques sont utilisés depuis peu. Il s'agit principalement des courbes elliptiques. Mais on a aussi suggéré l'utilisation de jacobiennes de courbes de genre supérieur (surtout le genre deux). Les tores algébriques sont aussi l'objet d'études approfondies. Nous les présentons dans le paragraphe 2.1.

Les meilleurs algorithmes connus pour calculer le logarithme discret dans le groupe des points d'une courbe elliptique sur le corps à q éléments, sont des algorithmes génériques et ont donc une complexité en $\Omega(\sqrt{P})$ où P est le plus grand facteur premier de l'ordre de la courbe. On en déduit généralement que les cryptosystèmes à bases de courbes elliptiques peuvent atteindre un même niveau de sécurité que ceux basés sur les groupes multiplicatifs, avec une taille de clé (la taille de q) beaucoup plus petite (disons 200 bits au lieu de 2000 bits).

Il convient de souligner qu'il existe des instances faibles du logarithme discret, tant pour les corps finis que pour les courbes elliptiques. Plus précisément, il existe des familles infinies de groupes multiplicatifs et de courbes elliptiques pour lesquels on dispose d'algorithmes polynomiaux de calcul du logarithme discret. C'est évident pour les groupes C dont l'ordre n n'a pas de grand facteur premier. On donne des exemples moins triviaux au paragraphe 2.2.

2.1. Un aperçu de l'utilisation des tores en cryptographie. —

2.1.1. Rappels sur les groupes algébriques commutatifs. — Tout groupe algébrique affine connexe de dimension 1 sur un corps algébriquement clos est soit le groupe additif $\mathrm{G_a}$, soit le groupe multiplicatif $\mathrm{G_m}$.

Il y a deux familles importantes de groupes algébriques. Une *variété abélienne* est un groupe algébrique complet et connexe. On peut montrer qu'un tel groupe algébrique est nécessairement commutatif. Un *groupe linéaire* est un sous-groupe algébrique de GL_n pour un entier positif n.

Un théorème de Rosenlicht établit que tout homomorphisme de groupes algébriques d'une variété abélienne dans un groupe linéaire ou d'un groupe linéaire connexe dans une variété abélienne, est constant.

Remarquons qu'un groupe algébrique fini est linéaire et que toute variété abélienne admet des sous-groupes finis (de torsion). Donc l'hypothèse de connexité est nécessaire dans l'énoncé ci-dessus.

Voici un théorème de structure dû à Chevalley

Théorème 1. — *Soit G un groupe algébrique connexe. Il existe un sous-groupe algébrique normal, connexe et linéaire L de G tel que le quotient $A = G/L$ soit une* *variété abélienne. Ce L est unique et il contient tous les sous-groupes algébriques linéaires connexes de G.*

Les homomorphismes de groupes algébriques surjectifs à noyaux finis sont appelés isogénies. Pour les groupes algébriques commutatifs sur un corps fini on a un théorème de structure plus fort. Si G est un groupe algébrique connexe commutatif sur un corps fini $\mathbb{F}_q$ et si $1 \to L \to G \to A \to 1$ est la suite exacte stricte donnée par le théorème de Chevalley, alors il existe une isogénie, définie sur $\mathbb{F}_q$, de G vers le produit direct $L \times A$.

À ma connaissance, tous les groupes algébriques utilisés à ce jour en cryptographie sont, de façon plus ou moins visible, des variétés jacobiennes généralisées.

Un *tore* sur le corps K est un groupe algébrique connexe commutatif $\mathbb{T}$ de dimension d, qui devient isomorphe à $(\mathrm{G_m})^d$ après extension des scalaires de K à une extension séparable L. Un tel corps L est appelé corps de décomposition du tore $\mathbb{T}$. Donc un tore de dimension d est un tordu du groupe algébrique $(\mathrm{G_m})^d$ et ces tores sont classifiés par $H^1(K, \mathrm{Aut}_{K^s}((\mathrm{G_m})^d))$.

Observons que nous voulons tordre $(\mathrm{G_m})^d$ en tant que groupe algébrique et non seulement en tant que variété. Donc le groupe d'automorphismes $\mathrm{Aut}_{K^s}((\mathrm{G_m})^d)$ qui nous préoccupe est le groupe des automorphismes de groupe algébrique et non pas le groupe complet des automorphismes de la variété $(\mathrm{G_m})^d$.

Un automorphisme $\mathfrak{a}$ du groupe algébriques $(\mathrm{G_m})^d$ est décrit par

$$\mathfrak{a}(g_1, g_2, ..., g_d) = \mathfrak{a}((g_i)_{1 \le i \le d}) = (\prod_{1 \le j \le d} g_j^{\alpha_{i,j}})_{1 \le i \le d}.$$

Ici les $\alpha_{i,j}$ sont des entiers tels que la matrice $A = (\alpha_{i,j})$ ait un déterminant égal à ± 1.

Ainsi le groupe $\mathrm{Aut}_{K^s}((\mathrm{G_m})^d)$ est isomorphe à $\mathrm{GL}_d(\mathbb{Z})$ et l'action de Galois sur ce groupe est triviale. Donc $Z^1(K, \mathrm{Aut}_{K^s}((\mathrm{G_m})^d))$ n'est autre que $Hom(\mathrm{Gal}_K, \mathrm{Aut}_K((\mathrm{G_m})^d))$ et $H^1(K, \mathrm{Aut}_{K^s}((\mathrm{G_m})^d))$ est le quotient de ce dernier ensemble par $\mathrm{Aut}_K((\mathrm{G_m})^d)$ agissant par conjugaison.

On suppose désormais que le corps de base K est fini de caractéristique p. Le groupe de Galois absolu Gal_K est procyclique et un élément de $H^1(K, \mathrm{Aut}_{K^s}((\mathrm{G_m})^d))$ est donné par la classe de conjugaison de l'image de l'automorphisme de Frobenius F.

Pour $L \supset K$ une extension de degré d de corps finis, on identifie $(\mathrm{G_m})^d$ au produit $\Pi_{\mathrm{Gal}(L/K)}\mathrm{G_m}$ de d facteurs $\mathrm{G_m}$ indicés par les K-automorphismes de L.

On note $\mathfrak{f}_d$ l'automorphisme de $\Pi_{\mathrm{Gal}(L/K)}\mathrm{G_m}$ qui permute les composantes comme F agit sur les indices dans $\mathrm{Gal}(L/K)$:

$$\mathfrak{f}_d(g_1, g_F, g_{F^2}, ..., g_{F^{d-1}}) = (g_{F^{d-1}}, g_1, g_F, g_{F^2}, ..., g_{F^{d-2}}).$$

On note $\mathcal{G}_d$ le tordu de $\Pi_{\mathrm{Gal}(L/K)}\mathrm{G_m}$ associé au cocycle $F \mapsto \mathfrak{f}_d$. C'est la restriction de Weil de $\mathrm{G_m}$ le long de L/K. C'est un tore de dimension d, défini sur K, et qui se décompose sur L. Une de ses propriétés intéressantes est que $\mathcal{G}_d(K)$ est isomorphe, en tant que groupe, à $\mathrm{G_m}(L) = L^*$. Notons que le groupe algébrique $\mathcal{G}_d$ dépend du corps de base K et du degré d.

En effet, il existe un L-isomorphisme

$$I : (\mathrm{G_m})^d = \prod_{\mathrm{Gal}(L/K)} \mathrm{G_m} \to \mathcal{G}_d$$

tel que ${}^F I = I \circ \mathfrak{f}_d$.

Pour tout diviseur a de d posons $d = ab$. Soit M l'extension de degré a de K. Alors $K \overset{a}{\subset} M \overset{b}{\subset} L$. Le groupe de Galois $\mathrm{Gal}(L/K)$ est engendré par le Frobenius F et le groupe de Galois $\mathrm{Gal}(L/M)$ est engendré par F^a.

La restriction de L à M définit un épimorphisme de groupes $\mathrm{Gal}(L/K) \to \mathrm{Gal}(M/K)$. On en déduit l'existence d'un homomorphisme de groupes algébriques $\nu_{a,d}$ de $\mathcal{G}_d$ dans $\mathcal{G}_a$.

En effet, on a un morphisme

$$\mathcal{N}_{a,d} : (\mathrm{G_m})^d = \prod_{\mathrm{Gal}(L/K)} \mathrm{G_m} \to (\mathrm{G_m})^a = \prod_{\mathrm{Gal}(M/K)} \mathrm{G_m}$$

défini par

$$\begin{aligned}\mathcal{N}_{a,d}(g_1, g_F, g_{F^2}, ..., g_{F^{d-1}}) \quad &= \quad (g_1 g_{F^a} g_{F^{2a}} ... g_{F^{(b-1)a}}, g_F g_{F^{a+1}} g_{F^{2a+1}} ... g_{F^{(b-1)a+1}}, \\ g_{F^2} g_{F^{a+2}} g_{F^{2a+2}} ... g_{F^{(b-1)a+2}}, \quad &\ldots \quad , g_{F^{a-1}} g_{F^{a+a-1}} g_{F^{2a+a-1}} ... g_{F^{(b-1)a+a-1}})\end{aligned}$$

et tel que $\mathcal{N}_{a,d} \circ \mathfrak{f}_d = \mathfrak{f}_a \circ \mathcal{N}_{a,d}$.

On note $\mathcal{T}_d$ l'intersection des noyaux des morphismes $\nu_{a,d}$ pour tous les diviseurs stricts a de d. C'est un tore de dimension $\phi(d)$ tel que $\mathcal{T}_d(K) \subset \mathcal{G}_d(K) = \mathrm{G_m}(L) = L^*$ est le sous groupe des points qui ont norme égale à 1 dans toute sous-extension de L/K. Ce sous groupe a pour cardinalité $\Phi_d(q)$ où $\Phi_d(X)$ est le d-ième polynôme cyclotomique et q la cardinalité de K.

2.1.2. Le tore de Lucas. — Soit encore K un corps fini de caractéristique impaire p. Soit $D \in K^*$ un scalaire qui n'est pas un carré dans K. Soit $L = K(\sqrt{D})$. Soit $\mathbb{A}^2/K$ le plan affine et $\mathcal{U}$ l'ouvert défini par l'inégalité $x^2 - Dy^2 \neq 0$. On construit un L-isomorphisme de $\mathcal{U} \otimes_K L$ dans $(G_m)^2$ en envoyant (x, y) sur $(x + y\sqrt{D}, x - y\sqrt{D})$. L'isomorphisme inverse est $I : (G_m)^2 \to \mathcal{U} \otimes_K L$ défini par $I(z_1, z_2) = (x, y) = (\frac{z_1+z_2}{2}, \frac{z_1-z_2}{2\sqrt{D}})$.

On vérifie que $I^{-1\sigma}I$ est l'identité si σ fixe $\sqrt{D}$ et l'application d'inversion sinon. Cela prouve que $\mathcal{U}$ est K-isomorphe à $\mathcal{G}_2$.

Le sous groupe $\mathcal{T}_2 \subset \mathcal{G}_2$ est défini par la condition supplémentaire que $z_1 z_2 = 1$ ou de façon équivalente $x^2 - Dy^2 = 1$.

Donc $\mathcal{T}_2$ est le fermé de $\mathbb{A}^2$ défini par l'équation $x^2 - Dy^2 = 1$. Le tore $\mathcal{T}_2$ est appelé tore de Lucas.

La loi de groupe sur $\mathcal{G}_2$ et $\mathcal{T}_2$ est donnée par les applications de multiplication et d'inversion :

$$\begin{aligned}\mu : \qquad \mathcal{G}_2 \times \mathcal{G}_2 &\longrightarrow \mathcal{G}_2 \\ ((x_1, y_1), (x_2, y_2)) &\longmapsto (x_1 x_2 + D y_1 y_2, y_1 x_2 + x_1 y_2)\end{aligned}$$

et

$$\begin{aligned}i : \qquad \mathcal{G}_2 &\longrightarrow \mathcal{G}_2 \\ (x, y) &\longmapsto (x, -y)\end{aligned}$$

Le groupe $\mathcal{T}_2(K)$ des points K-rationnels du tore de Lucas est parfois préféré au groupe $\mathrm{G_m}(K)$ parce que le logarithme discret y est supposé un peu plus difficile. Notons que les points de $\mathrm{G_m}(K)$ sont représentés par une seule coordonnée affine alors que les points de $\mathcal{T}_2(K)$ sont représentés ici par leurs deux coordonnées x et y. On a donc une représentation deux fois plus longue pour $\mathcal{T}_2(K)$ alors que les deux groupes sont de tailles comparables. C'est un inconvénient sérieux.

Une première parade, qui est assez générique, consiste à noter que l'exponentiation par un entier k dans le groupe algébrique $\mathcal{T}_2$ est donnée par $[k] : \mathcal{T}_2 \to \mathcal{T}_2$ avec

$$[k](x,y) = (\sum_{0\le 2l\le k} (x^2-1)^l x^{k-2l} \begin{pmatrix} k \\ 2l \end{pmatrix}, y \sum_{0\le 2l+1\le k} (x^2-1)^l x^{k-2l} \begin{pmatrix} k \\ 2l+1 \end{pmatrix}).$$

En particulier, la coordonnée x de $[k]P$ ne dépend que de la coordonnée x de P. Ceci simplement par ce que $[k]$ commute à l'inversion i.

Il est donc naturel de considérer la variété quotient $\mathcal{X}_2 = \mathcal{T}_2/\{1, i\}$. Celle-ci n'est autre que la droite affine avec x pour coordonnée.

Ce quotient n'est plus un groupe algébrique mais il conserve une action du monoide multiplicatif des entiers positifs $(\mathbb{Z}_{>0}, \times)$, donnée par les applications $[k]$ d'exponentiation.

Cela suffit pour faire de la cryptographie à base de logarithme discret pourvu que l'on se contente de l'exponentiation et que l'on renonce à la multiplication.

Cette variété $\mathcal{X}_2$ présente l'avantage d'être rationnelle : les points sont décrits par une seule coordonnée. On peut ainsi représenter des problèmes de logarithme discret dans le sous-groupe de cardinal $q+1$ de L^* avec seulement $\log_2(q)$ bits (ceux qui suffisent à décrire la coordonnée x).

C'est l'idée à l'origine du système LUC de [**21**].

Il est de la première importance pour cette méthode que la variété $\mathcal{X}_2$ soit *rationnelle*.

Notons que le même procédé est utilisé pour les courbes elliptiques car le quotient d'une courbe elliptique par son involution est rationnel lui aussi.

Mais il y a mieux. Rubin et Silverberg rappellent dans [**11, 12**] que le tore $\mathcal{T}_2$ lui-même est rationnel comme K-variété.

En effet, l'équation $x^2 - Dy^2 = 1$ est rendue homogène en posant $x^2 - Dy^2 = t^2$ qui est aussi $x^2 - t^2 = Dy^2$ ou encore $(x-t)(x+t) = Dy^2$. On pose $u = \frac{x-t}{y}$ et il vient une paramétrisation $\frac{x}{y} = \frac{u+\frac{D}{u}}{2}$ et $\frac{t}{y} = \frac{-u+\frac{D}{u}}{2}$ donc une paramétrisation de $x^2 - Dy^2 = t^2$ par

$$\begin{aligned} x &= u^2 + D \\ t &= -u^2 + D \\ y &= 2u \end{aligned}$$

ce qui en coordonnées affines donne $x = \frac{D+u^2}{D-u^2}$ et $y = \frac{2u}{D-u^2}$.

Ce qui se produit ici est que G_m est une sous variété de $\mathbb{P}^1$. Bien qu'il existe un tordu non-trivial du groupe G_m, le 1-cocycle associé s'annule dans $H^1(K, \mathrm{Aut}_{K^s}(\mathbb{P}^1))$.

Une conséquence intéressante est qu'un élément de $\mathcal{T}_2$ peut être représenté par une seule coordonnée u et que la loi de groupe peut s'exprimer en terme de cette unique coordonnée.

En effet, soit P_1 de u-coordonnée u_1 et P_2 de u-coordonnée u_2, un calcul sans mystère donne la u-coordonnée de P_3 que l'on note u_3 :

$$u_3 = \frac{D(u_1 + u_2)}{u_1 u_2 + D}.$$

L'élément identité de $\mathcal{G}_2$ a une u-coordonnée égale à 0 et l'application d'inversion change u en $-u$.

Le point de coordonnées $x = -1$ et $y = 0$ correspond à $u = \infty$.

Si u parcourt $K \cup \{\infty\}$ il représente les $q + 1$ points de $\mathcal{T}_2(K)$.

Silverberg (qui s'appelle Alice) et Rubin (qui ne s'appelle pas Bob) montrent que le cryptosystème XTR [**8**] utilise une variété de type $\mathcal{X}$ tout comme LUC. La question qui se pose alors est de déterminer dans quels cas cette variété quotient d'un tore est rationnelle. Et si elle l'est, de donner une paramétrisation explicite. La même question se pose pour les tores $\mathcal{T}_d$ eux mêmes et elle est assez ouverte. Le tore $\mathcal{T}_d$ et son quotient $\mathcal{X}_d$ sont de dimension $\phi(d)$. Pour $d = 2 \times 3 \times 5$ on a $\phi(d) = 8$ et on cherche des paramétrisations ...

Le tore de Lucas est utilisé (au moins implicitement) depuis longtemps. Il est le ressort de la méthode appelée "$p+1$" pour factoriser des entiers naturels en produit de facteurs premiers.

D'une manière générale, factoriser un nombre entier N revient à calculer le nombre de points $\mathbb{Z}/\mathbb{N}\mathbb{Z}$ rationnels d'un groupe algébrique G bien choisi. C'est évident si on choisit $\mathrm{G} = \mathrm{G_m}$ mais il peut être plus habile de choisir $\mathrm{G} = \mathcal{T}_2$ le tore de Lucas ou encore $\mathrm{G} = A$ une variété abélienne.

Dans le même ordre d'idée, on prouve qu'un nombre P est premier en prouvant que $\mathrm{G}(\mathbb{Z}/P\mathbb{Z})$ a le cardinal attendu où G est un groupe algébrique bien choisi. Si $\mathrm{G} = \mathrm{G_m}$ on attend $P - 1$, si $\mathrm{G} = \mathcal{T}_2$ on attend $P + 1$, et si G est une variété abélienne à multiplication complexe, on sait aussi à quoi s'attendre, grâce à la théorie de Shimura.

La variété (pas si grande) des groupes algébriques commutatifs a donc été explorée largement par de nombreux auteurs intéressés à l'une ou l'autre de ces questions : factorisation, primalité, logarithme discret protocoles cryptographiques.

On trouve dans [**5**] un état de ces méthodes et dans [**19**] une introduction aux groupes algébriques.

2.2. Des exemples d'instances faibles du logarithme discret. — Le problème du logarithme discret n'est pas toujours difficile. On a vu qu'il est facile dans le groupe additif d'un corps fini. Il est facile aussi dans un groupe $C = \prod_i C_i$ produit direct de petits groupes. Dans ce cas, il se décompose en autant de problèmes de logarithmes discrets dans les facteurs C_i. On évite donc les groupes $\mathrm{G_m}(\mathbb{F}_q)$ si $q - 1$ est friable (produit de petits facteurs premiers).

Dans ce paragraphe nous montrons un autre exemple d'instance faible du logarithme discret. La cause, ici, est analytique : on réduit le logarithme discret à un logarithme p-adique.

L'alinéa 2.2.2 présente la méthode de Riesel pour calculer le logarithme discret dans le groupe multiplicatif $\mathrm{G_m}(\mathbb{Z}/p^k\mathbb{Z})$. L'alinéa 2.2.5 expose l'extension de cette méthode au cas des courbes elliptiques de trace 1, d'après les travaux de Smart, Araki, Satoh, Semaev.

2.2.1. Rappels sur les logarithmes p-adiques. — Un élément de l'anneau $\mathbb{Z}_p$ des entiers p-adiques est noté

$$z = z_0 + z_1 p + z_2 p^2 + ... + z_{k-1} p^{k-1} + O(p^k)$$

où les z_i sont des entiers tels que $0 \leq z_i < p$ et k est la précision absolue requise.

On note v_p la valuation p-adique sur $\mathbb{Q}_p$. On sait que $\mathbb{Q}_p^* =< p > \times \mathbb{Z}_p^*$. On note $\mathbb{U} = \mathbb{Z}_p^*$ et pour tout entier $n \geq 1$ soit $\mathbb{U}_n = 1 + p^n \mathbb{Z}_p$. La réduction modulo p donne une suite exacte

$$1 \to \mathbb{U}_1 \to \mathbb{Z}_p^* \to \mathbb{F}_p^* \to 1. \tag{1}$$

Le lemme de Hensel montre que $\mathbb{U}$ contient le groupe $\mathbb{V}$ des racines $(p-1)$-ièmes de l'unité. Donc la suite exacte ci-dessus se décompose et on a $\mathbb{U} = \mathbb{V} \times \mathbb{U}_1$.

Reste à décrire $\mathbb{U}_1$. Si $p \geq 3$ on construit un homomorphisme de groupes topologiques entre $(\mathbb{U}_1, \times)$ et $(p\mathbb{Z}_p, +)$.

Si $p = 2$ alors $\mathbb{U}_1 =< -1 > \times \mathbb{U}_2$ et on construit un homomorphisme de groupes topologiques entre $(\mathbb{U}_2, \times)$ et $(4\mathbb{Z}_p, +)$.

Dans les deux cas, l'isomorphisme est donné par la série logarithme

$$\mathrm{Log}(z) = -\sum_{n=1}^{\infty} \frac{(-1)^n}{n} (z-1)^n.$$

L'application inverse est l'exponentielle

$$\exp(z) = \sum_{n=0}^{\infty} \frac{z^n}{n!}.$$

La série $\mathrm{Log}(z)$ converge sur $\mathbb{U}_1$ ($\mathbb{U}_2$ si $p = 2$) et la série $\exp(z)$ converge sur $p\mathbb{Z}_p$ ($4\mathbb{Z}_2$ si $p = 2$). Donc la structure de $\mathbb{Q}_p^*$ est

$$\mathbb{Z} \times \mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}_p$$

pour p impair et

$$\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}_2$$

pour $p = 2$.

2.2.2. Calcul de logarithmes discrets dans $(\mathbb{Z}/p^k\mathbb{Z})^*$. — Nous supposons dans la suite que p est un entier premier impair.

Soit $k \geq 2$ un entier et b_k un générateur de $(\mathbb{Z}/p^k\mathbb{Z})^*$. Soit c_k un autre élément de $(\mathbb{Z}/p^k\mathbb{Z})^*$. On veut calculer le logarithme discret $\ell_k = \log_{b_k} c_k$. On voit $(\mathbb{Z}/p^k\mathbb{Z})^*$ comme le quotient de $\mathbb{Z}_p^*$ par $\mathbb{U}_k$ et on fixe un relèvement b de b_k dans $\mathbb{Z}_p^*$ et un relèvement c de c_k dans $\mathbb{Z}_p^*$.

Soient c_1 et b_1 les images de c et b dans $(\mathbb{Z}/p\mathbb{Z})^* = \mathbb{Z}_p^*/\mathbb{U}_1$ et supposons que le logarithme $\ell_1 = \log_{b_1} c_1 \in \mathbb{Z}/(p-1)\mathbb{Z}$ est connu. On identifie la classe de congruence ℓ_1 modulo $p-1$ à son représentant dans l'intervalle $[0, p-1[$.

Cet entier peut être calculé par recherche exhaustive au prix de $O(p)$ opérations dans $\mathbb{Z}/p\mathbb{Z}$.

On pose $C = cb^{-\ell_1}$ et on vérifie que $C \in \mathbb{U}_1$. Soit $B = b^{p-1} \in \mathbb{U}_1 - \mathbb{U}_2$.

On calcule à l'aide du développement en série convergente

$$L = \frac{\mathrm{Log}\, C}{\mathrm{Log}\, B} \pmod{p^{k-1}}$$

donc $C = B^L \pmod{p^k}$ et $c = b^{\ell_1} b^{(p-1)L} \pmod{p^k}$ ce qui nous donne le logarithme discret cherché

$$\log_{b_k} c_k = \ell_1 + (p-1)L \pmod{p^{k-1}(p-1)}.$$

Ainsi, le calcul du logarithme discret dans $\mathbb{Z}/p^k\mathbb{Z}$ se réduit au calcul d'un logarithme discret dans $\mathbb{Z}/p\mathbb{Z}$. Pour p fixé et k tendant vers l'infini, on obtient un exemple de grand groupe multiplicatif où le logarithme discret se calcule en temps polynomial en le logarithme de la taille $S = (p-1)p^{k-1}$ du groupe.

2.2.3. Un exemple. — Soit $p = 3$ et $k = 10$. On choisit

$$b = 59045 = 2 + 3 + 2.3^2 + 2.3^3 + 2.3^4 + 2.3^5 + 2.3^6 + 2.3^7 + 2.3^8 + 2.3^9 + O(3^{10})$$

un générateur de $\mathbb{Z}/3^{10}\mathbb{Z}$.

Posons $B = b^2 = 1 + 2.3 + 3^2 + O(3^{10})$. C'est un générateur de $\mathbb{U}_1$.

Soit

$$c = 24731 = 2 + 2.3 + 2.3^2 + 2.3^4 + 2.3^5 + 2.3^7 + 3^9 + O(3^{10}).$$

On veut calculer $\log_{b_{10}} c_{10}$.

Puisque $c = b \pmod 3$ on a $\ell_1 = 1$ et on pose

$$C = c/b = 1 + 2.3 + 3^3 + 2.3^4 + 3^6 + 2.3^7 + 2.3^8 + 3^9 + O(3^{10}).$$

On calcule $L = \mathrm{Log}(C)/\mathrm{Log}(B)$ grâce au développement en série du logarithme

$$L = 1 + 3 + 2.3^2 + 2.3^3 + 3^5 + 3^7 + O(3^9)$$

Donc $L = 2506 \pmod{3^9}$ et $\ell_{10} = 1 + 2 \times 2506 = 5013$.

Dans l'article original [**10**]de Riesel, le logarithme p-adique est remplacé par le quotient de Fermat.

2.2.4. Courbes elliptiques sur un corps local. — On suppose encore que p est premier impair. Soit $\mathcal{E}$ une courbe elliptique d'équation affine

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

avec a_1, a_2, a_3, a_4, a_6 dans $\mathbb{Z}_p$.

On suppose que $\mathcal{E}$ a bonne réduction : le discriminant Δ est une unité. On note $\tilde{\mathcal{E}}$ la réduction de $\mathcal{E}$ modulo p.

La réduction modulo p définit un épimorphisme de groupes $\rho : \mathcal{E}(\mathbb{Q}_p) \to \tilde{\mathcal{E}}(\mathbb{F}_p)$ de $\mathcal{E}(\mathbb{Q}_p)$ vers $\tilde{\mathcal{E}}(\mathbb{F}_p)$. Le noyau de ρ est formé des points proches p-adiquement de l'origine. On note $z = -x/y$ le paramètre local en l'origine et pour tout k positif on note $\mathcal{E}_k(\mathbb{Q}_p)$ l'ensemble des points $P \in \mathcal{E}(\mathbb{Q}_p)$ tels que $v_p(z_P) \geq k$. On a la suite exacte

$$0 \to \mathcal{E}_1(\mathbb{Q}_p) \to \mathcal{E}(\mathbb{Q}_p) \xrightarrow{\rho} \tilde{\mathcal{E}}(\mathbb{F}_p) \to 0. \tag{2}$$

qui est très proche de la suite 1.

On étudie donc la structure de groupe de $\mathcal{E}_1(\mathbb{Q}_p)$. La loi de groupe sur $\mathcal{E}_1(\mathbb{Q}_p)$ est exprimée en terme du paramètre z. En effet $z(P+Q)$ est une série formelle en $z(P)$ et $z(Q)$. Cette série formelle n'est autre que le groupe formel associé à $\mathcal{E}$, c'est-à-dire le développement de Taylor à l'origine de la loi d'addition. Les coefficients de ce développement sont des polynômes en les coefficients de l'équation de $\mathcal{E}$:

$$z(P+Q) = z(P) + z(Q) - a_1 z(P)z(Q) - a_2(z(P)^2 z(Q) + z(Q)^2 z(P)) + \cdots$$

Le paramètre local z induit une bijection de $\mathcal{E}_1(\mathbb{Q}_p)$ sur $p\mathbb{Z}_p$. La série $F(z_1, z_2)$ converge sur $p\mathbb{Z}_p \times p\mathbb{Z}_p$ et pour tout P et Q dans $\mathcal{E}_1(\mathbb{Q}_p)$ on a $z(P+Q) = F(z(P), z(Q))$. On pose $z_1 \oplus_{\mathcal{F}} z_2 = F(z_1, z_2)$ pour z_1 et z_2 dans $p\mathbb{Z}_p$. Cela fait de z un homomorphisme de groupes topologiques de $(\mathcal{E}_1, +)$ vers $(p\mathbb{Z}_p, \oplus_{\mathcal{F}})$.

Il existe un *logarithme formel* associé au groupe formel F et noté $\mathrm{Log}_{\mathcal{F}}(z)$. Il est caractérisé par l'identité

$$\mathrm{Log}_{\mathcal{F}}(F(z_1, z_2)) = \mathrm{Log}_{\mathcal{F}}(z_1) + \mathrm{Log}_{\mathcal{F}}(z_2).$$

La série réciproque de $\mathrm{Log}_{\mathcal{F}}(z)$ est notée $\exp_{\mathcal{F}}(z)$.

Un simple calcul montre que $\mathrm{Log}_{\mathcal{F}}(z) = \sum_{n=1}^{\infty} \frac{b_n}{n} z^n$ et $\exp_{\mathcal{F}}(z) = \sum_{n=1}^{\infty} \frac{c_n}{n!} z^n$ où les b_n et c_n sont dans $\mathbb{Z}_p$, et $b_1 = c_1 = 1$. On en déduit que $\mathrm{Log}_{\mathcal{F}}(z)$ converge pour $v_p(z) > 0$ et $\exp_{\mathcal{F}}(z)$ pour $v_p(z) > 1/(p-1)$.

En considérant l'isomorphisme composé

$$\mathcal{E}_1(\mathbb{Q}_p) \xrightarrow{z} (p\mathbb{Z}_p, \oplus_{\mathcal{F}}) \xrightarrow{\mathrm{Log}_{\mathcal{F}}} (p\mathbb{Z}_p, +)$$

on prouve que $\mathcal{E}_1(\mathbb{Q}_p)$ est sans torsion et que la réduction modulo p est injective sur le sous-groupe de torsion de $\mathcal{E}(\mathbb{Q}_p)$. On note $\tilde{o} = \#\tilde{\mathcal{E}}(\mathbb{F}_p)$. Si $\tilde{o}$ est premier à p alors $\tilde{\mathcal{E}}(\mathbb{F}_p)$ se relève en un groupe de torsion dans $\mathcal{E}(\mathbb{Q}_p)$ et la réduction modulo p induit une bijection entre les torsions de $\mathcal{E}(\mathbb{Q}_p)$ et $\tilde{\mathcal{E}}(\mathbb{F}_p)$. Donc

$$\mathcal{E}(\mathbb{Q}_p) \sim \mathcal{E}_1(\mathbb{Q}_p) \times \tilde{\mathcal{E}}(\mathbb{F}_p) \sim \mathbb{Z}_p \times \tilde{\mathcal{E}}(\mathbb{F}_p).$$

Supposons maintenant que $\tilde{o} = \mathcal{E}(\mathbb{F}_p) = p$. C'est un cas très particulier car la trace de l'endomorphisme de Frobenius de $\mathcal{E}$ vaut 1. Alors $\mathcal{E}(\mathbb{Q}_p)$ est coincé dans la suite exacte

$$0 \to \mathbb{Z}_p \to \mathcal{E}(\mathbb{Q}_p) \to \mathbb{Z}/p\mathbb{Z} \to 0.$$

Donc il est isomorphe à $\mathbb{Z}_p$ (cas I) ou a $\mathbb{Z}_p \times \mathbb{Z}/p\mathbb{Z}$ (cas II).

Supposons que l'on se trouve dans le cas I. Donc $\mathcal{E}(\mathbb{Q}_p)$ est sans torsion et il existe une bijection entre $\tilde{\mathcal{E}}(\mathbb{F}_p)$ et $\mathcal{E}_1/\mathcal{E}_2$. Soit en effet $\tilde{P}$ un point dans $\tilde{\mathcal{E}}(\mathbb{F}_p)$ et soit $P \in \mathcal{E}(\mathbb{Q}_p)$ un relèvement $\tilde{P}$. Le point $[p]P$ est dans $\mathcal{E}_1(\mathbb{Q}_p)$ car $\widetilde{[p]P} = [p]\tilde{P} = 0$. En outre, si nous choisissons un autre relèvement P' de $\tilde{P}$, alors $[p]P - [p]P' = [p](P - P') \in \mathcal{E}_2$. On a donc une application

$$\Pi : \tilde{\mathcal{E}}(\mathbb{F}_p) \to \mathcal{E}_1/\mathcal{E}_2.$$

Elle est injective. En effet, soit $P \in \mathcal{E}(\mathbb{Q}_p)$ tel que $[p]P \in \mathcal{E}_2$. La multiplication par p définit une bijection entre $\mathcal{E}_1$ et $\mathcal{E}_2$. Il y a un $R \in \mathcal{E}_1$ tel que $[p]R = p[P]$. Donc $[p](R - P) = 0$ et puisque on est dans le cas I on a $P = R \in \mathcal{E}_1$ et $\tilde{P} = 0$.

2.2.5. La méthode de Smart-Araki-Satoh-Semaev. — Pour calculer le logarithme discret dans une courbe elliptique de trace 1, ils utilisent la bijection Π de l'alinéa précédent et transforment un problème de logarithme discret dans $\tilde{\mathcal{E}}(\mathbb{F}_p)$ en un problème de logarithme dans $\mathcal{E}_1(\mathbb{Q}_p)$. Ce dernier logarithme est un logarithme elliptique et se calcule efficacement en raison de ses propriétés analytiques.

Il reste à s'assurer que l'on se trouve dans le cas I de l'alinéa précédent. En fait Voloch a noté que le cas II corresponds au cas où $\mathcal{E}$ est le relèvement canonique de

$\tilde{\mathcal{E}}$ modulo p^2. Comme ce relèvement canonique est unique, il n'est pas très difficile à éviter…

D'un point de vue pratique, le développement du logarithme elliptique est obtenu en intégrant la forme différentielle canonique ω.

On développe x, y et ω en $z = -x/y$ et on calcule

$$\begin{aligned} x &= z^{-2} - a_1 z^{-1} - a_2 .... \\ y &= -x/z \\ \omega &= \frac{dy}{3x^2 + 2a_2 x + a_4 - a_1 y} = (1 + a_1 z + (a_1^2 + a_2)z^2 + ...)dz \\ \mathrm{Log}_{\mathcal{F}} &= \int \omega = z + \frac{a_1}{2} z^2 + \frac{a_1^2 + a_2}{3} + ... \end{aligned}$$

Finissons par un exemple. Soit $p = 655387895585476301924777$ et $\tilde{\mathcal{E}}$ la courbe d'équation

$$\tilde{E} : y^2 + xy = x^3 + 114287067913850793676921x + 349073807889941681395769$$

sur $\mathbb{F}_p$.

Soit $\tilde{P} = (170219448, 146437358154002252722 19)$ un point dans $\tilde{\mathcal{E}}(\mathbb{F}_p)$. On vérifie que $[p]\tilde{P} = 0$.

Soit $\tilde{Q} = (714342439934502571150 04, 316317604915944437378529)$ un autre point de $\tilde{\mathcal{E}}(\mathbb{F}_p)$.

On choisit un relevé $\mathcal{E}$ de $\tilde{\mathcal{E}}$ sur $\mathbb{Q}_p$. Par exemple on choisit $\mathcal{E}$ d'équation

$$E : y^2 + xy = x^3 + 114287067913850793676921x + 349073807889941681395769$$

sur $\mathbb{Q}_p$.

On cherche un $P = (x_P, y_P)$ dans $\mathcal{E}(\mathbb{Q}_p)$ au dessus de $\tilde{P}$. On fixe $x_P = 170219448$ par exemple et on résout dans $\mathbb{Q}_p$ l'équation en y

$$y^2 + x_P y = x_P^3 + 114287067913850793676921 x_P + 349073807889941681395769.$$

On choisit la racine congrue à
146437358154002252722 19 modulo p.
Donc

$$y_P = 146437358154002252722 19 + 241062303587335366096866.p + O(p^2).$$

Alors

$$\begin{aligned} \Pi(\tilde{P}) &= [p]P \\ &= (246304660834813598643589.p^{-2} + O(p^{-1}), 213491610344127745612815.p^{-3} + O(p^{-2})). \end{aligned}$$

Et

$$\mathrm{Log}_{\mathcal{F}}([p]P) = z_P + O(z_P^2) = -\frac{246304660834813598643589}{213491610344127745612815} p + O(p^2).$$

De même

$$\mathrm{Log}_{\mathcal{F}}([p]Q) = 169836480309236709243708.p + O(p^2).$$

Le quotient est $\log_P(Q) = 123456789 \pmod p$.

On voit que les courbes elliptiques qui ont p points rationnels sur $\mathbb{F}_p$ sont des instances faibles pour le logarithme discret. Cette observation a été faite par Araki et Satoh [**1**], Smart [**20**], Semaev [**18**] indépendemment. Ruck [**13**] et Voloch ont unifié et généralisé ces travaux dans le langage naturel de la cohomologie galoisienne.

3. Isogénies et cryptographie

Dans cette section, je décris un EHD qui n'est pas un problème de logarithme discret. Lorsque j'ai présenté cet exemple en 1997 au séminaire de cryptographie de l'ENS, il s'agissait d'une curiosité (voir [**6**]). Mais les progrès réalisés dans le calcul explicite des isogénies et les travaux menés par Charles, Lauter, Jao et Venkatesan depuis lors, montrent qu'il n'est pas irréaliste de fonder la sécurité d'un cryptosystème sur la difficulté de trouver un morphisme entre deux objets.

Le paragraphe 3.1 décrit l'action du groupe des classes d'un ordre quadratique sur les courbes elliptiques à multiplication complexe par cet ordre, d'un point de vue algorithmique. Cette situation produit un candidat EHD.

Le paragraphe 3.2 rappelle quelques propriétés des graphes d'isogénies entre courbes elliptiques et donne une idée de leur intérêt cryptographique.

3.1. L'espace homogène des courbes ordinaires à multiplication par un ordre quadratique. — Soit $\mathbb{F}_q$ un corps de cardinal $q = p^d$ et E une courbe elliptique sur $\mathbb{F}_q$, supposée ordinaire. L'anneau des endomorphismes de E est isomorphe à un ordre quadratique $\mathcal{O}$. On fixe un tel isomorphisme $\iota : \mathrm{End}(E) \to \mathcal{O}$. On note t la trace de l'endomorphisme de Frobenius Φ. Donc $\#E(\mathbb{F}_q) = q + 1 - t$.

On pose $\Delta = t^2 - 4q$ et on suppose que Δ est sans facteur carré. Donc $\mathcal{O} = \mathbb{Z}[\Phi]$ est maximal.

Si $\mathfrak{a}$ est un idéal de $\mathcal{O}$ premier à p, on note $\mathrm{Ker}\,\mathfrak{a} \subset E$ l'intersection des noyaux des isogénies de E appartenant à $\iota^{-1}(\mathfrak{a})$.

Soit F le quotient de E par $\mathrm{Ker}\,\mathfrak{a}$ et $I_{\mathfrak{a}} : E \to F$ l'isogénie quotient. Soit $\kappa : \mathrm{End}(F) \to \mathcal{O}$ l'isomorphisme défini par $\kappa(\alpha) = \iota(I_{\mathfrak{a}}^{-1}\alpha I_{\mathfrak{a}})$.

On note $[\mathfrak{a}]$ la classe de $\mathfrak{a}$ dans $\mathrm{Pic}(\mathcal{O})$ et on pose $[\mathfrak{a}].(E,\iota) = (F,\kappa)$. On définit ainsi une action du groupe des classes $G = \mathrm{Pic}(\mathcal{O})$ de $\mathcal{O}$ sur l'ensemble des classes d'isomorphismes de couples (E,ι) formés d'une courbe elliptique sur $\mathbb{F}_q$ et d'un isomorphisme de $\mathrm{End}(E)$ vers $\mathcal{O}$.

Cette action admet deux orbites, permutées par la conjugaison complexe. Soit H l'une des deux orbites. L'action de G sur H est simplement transitive. Le cardinal $S = \#G = \#H$ est le nombre de classes de $\mathcal{O}$. On a $S = \Delta^{\frac{1}{2}+o(1)}$.

Il est facile de vérifier qu'une courbe elliptique E a un anneau d'endomorphismes isomorphe à $\mathcal{O}$. Il suffit de vérifier que $\#E = p + 1 - t$ à l'aide de la méthode de Schoof [**16**] ou plus vite encore si on dispose d'une factorisation de $p+1-t$ et si ce dernier entier est sans facteur carré.

Si $\ell \neq p$ est un entier premier impair décomposé dans $\mathcal{O}$, le polynôme $f(X) = X^2 - tX + q$ a deux racines distinctes λ et μ modulo ℓ et on a $\ell = \mathfrak{l}\bar{\mathfrak{l}}$ avec $\mathfrak{l} = (\ell, \Phi - \lambda)$ et $\bar{\mathfrak{l}} = (\ell, \Phi - \mu)$.

Le noyau $\mathrm{Ker}\,\mathfrak{l}$ est un sous-groupe de $E[\ell]$. Il correspond à un facteur de degré $\frac{\ell-1}{2}$ du polynôme de ℓ-division. Ce facteur se calcule en temps polynômial en $\log q$

et ℓ par divers moyens (soit brutalement, soit en suivant les idées de Schoof, Atkin, Elkies et quelques autres [**17**]).

Le quotient de E par $\operatorname{Ker}\mathfrak{l}$ se calcule en temps polynômial en ℓ et $\log q$ à l'aide des formules de Vélu ou, plus efficacement encore, en utilisant des méthodes plus récentes proposées par Elkies, Schoof, Lercier, moi-même, Morain, Salvy, Schost, etc. On peut consulter [**3**] qui est un texte récent sur le sujet. Notons que le calcul d'isogénies se décompose en deux étapes : trouver d'abord le noyau, puis quotienter la courbe, ou bien au contraire, trouver d'abord la courbe quotient (à l'aide d'équations modulaires) puis en déduire le noyau.

Un nombre premier sur deux se décompose dans $\mathcal{O}$. Si cette proportion est respectée pour les petits nombres premiers, en admettant l'hypothèse de Riemann généralisée, on dispose d'un ensemble d'éléments de G dont l'action sur H se calcule en temps polynômial en $\log q$ et qui engendrent G.

Une combinaison de ces éléments à coefficients entiers aléatoires et assez grands produit un élément aléatoire de G avec distribution assez proche de la distribution uniforme (sur la composante connexe du point de départ).

Il est raisonnable de penser qu'il n'existe pas d'algorithme rapide pour calculer l'unique classe de $\operatorname{Pic}(\mathcal{O})$ qui envoie une courbe E sur une courbe F. On a donc un candidat EHD sérieux qui ne provient pas du logarithme discret.

On ne connaît pas d'algorithme pour calculer S le nombre de classes de $\mathcal{O}$ en temps polynômial en $\log \Delta$. Mais connaître le cardinal exact d'un EHD n'est pas indispensable aux protocoles que nous avons présentés.

Pour construire un EHD tel que décrit dans le paragraphe précédent, on choisit d'abord un corps fini $\mathbb{F}_q$. On choisit une courbe elliptique au hasard et on calcule la trace t de l'endomorphisme de Frobenius avec la méthode de Schoof. On vérifie que $\Delta = t^2 - 4q$ est sans facteur carré et se factorise aisément (sinon on recommence).

On collectionne alors les petits nombres premiers ℓ qui se décomposent dans $\mathbb{Z}[\Phi]$.

3.2. Graphes d'isogénies. — Dans la situation du paragraphe précédent, on fixe un réel positif δ et on pose $B = (\log q)^{2+\delta}$. Soit $\mathcal{G}$ le graphe dont les sommets sont les éléments de H et dont les cotés sont les paires $\{(E,\iota),(F,\kappa)\}$ d'éléments de H telles qu'il existe un idéal premier $\mathfrak{a}$ de $\mathcal{O}$, de degré d'inertie 1, de norme $\leq B$ et tel que $[\mathfrak{a}].E = F$. C'est un graphe de Cayley. Il est k-régulier où k est le nombre d'idéaux premier de degré d'inertie 1 et de norme $\leq B$ dans $\mathcal{O}$. On note $M = [m_{e,f}]_{e,f\in H}$ sa matrice d'adjacence. Donc $m_{e,f} = 1$ si $\{e,f\}$ est un coté du graphe, et $m_{e,f} = 0$ sinon.

Le matrice $\frac{1}{k}M$ est une matrice de Markov, correspondant à une marche aléatoire dans le graphe : si l'on se trouve au sommet e du graphe, on choisit un des k cotés issus de e avec probabilité uniforme et on avance le long de ce sommet.

La distribution uniforme de probabilités sur l'ensemble H des sommets est un vecteur propre de M et sa valeur propre est k.

Toutes les valeurs propres de M sont réelles et de valeur absolue $\leq k$. On peut consulter le petit livre [**15**] de Sarnak sur les graphes et les formes modulaires pour toutes ces questions.

Les valeurs propres non-triviales (celles dont la valeur absolue est $< k$) ralentissent la convergence du processus de Markov vers la distribution uniforme. Si elles sont petites, alors cette convergence est rapide.

Jao, Miller et Venkatesan montrent que pour le graphe ci-dessus, sous reserve que l'hypothèse de Riemann généralisée soit correcte, le graphe est connexe et les valeurs propres non-triviales ont une valeur absolue $O(k^\beta)$ pour tout $\beta > \frac{1}{2} + \frac{1}{\delta+2}$. Comme δ est positif, ces valeurs propres sont nettement séparées de la valeur propre associée à la distribution uniforme. Donc le processus markovien converge vite.

On dit que la famille des graphes ainsi construits est une famille de graphes d'expansion.

Classiquement, on construit plutôt des graphes d'isogénies à l'aide de courbes supersingulières, comme dans [**9**]. En effet, les matrices d'adjacences, appelées matrices de Brandt, expriment l'action d'opérateurs de Hecke sur des espaces de formes modulaires. Leurs valeurs propres sont majorées à l'aide de la conjecture de Ramanujan. Ces graphes réguliers, appelés graphes de Pizer, sont encore meilleurs que les précédents, car leurs valeurs propres non-triviales sont en valeur absolue $\leq 2\sqrt{k-1}$. On dit que ce sont des graphes de Ramanujan.

Outre leurs remarquables propriétés spectrales, les graphes d'isogénies présentent un grand intérêt calculatoire. Ce sont de grands graphes dans lesquels on peut circuler facilement (cela revient à calculer des isogénies de petit degré). Mais il est difficile de trouver un chemin entre deux sommets donnés, comme nous l'avons vus dans le paragraphe 3.1. Charles, Goren et Lauter proposent dans [**4**] d'utiliser cette propriété pour construire des fonctions de hachage cryptographique. Le principe est le suivant : on appelle $\mathcal{C}$ l'ensemble des entiers premiers $\leq B$ qui se décomposent dans $\mathcal{O}$ et on forme un ensemble $\mathcal{B}$ en choisissant pour tout ℓ dans $\mathcal{C}$ un idéal au dessus de ℓ. On choisit une origine parmi les sommets du graphe et on fixe une bijection entre les lettres de l'alphabet et les idéaux dans $\mathcal{B}$, de sorte qu'à tout mot de longueur quelconque on peut associer un chemin dans le graphe. Le sommet où l'on aboutit à l'issue de ce cheminement est la valeur de la fonction de hachage. Trouver deux mots qui se hachent sur le même sommet revient à trouver un cycle non-trivial dans le graphe.

Références

[1] K. Araki & T. Satoh – « Fermat quotients and the polynomial time discrete logarithm algorithm for anomalous elliptic curves », *Comment. Math. Univ. St. Paul.* **47** (1998), p. 81–92.

[2] P. Barthélemy, R. Rolland & P. Véron – *Cryptographie, principes et mises en œuvre*, Lavoisier, 2005.

[3] A. Bostan, F. Morain, B. Salvy & E. Schost – « Fast algorithms for computing isogenies between elliptic curves », *prépublication* (2007).

[4] D. Charles, E. Goren & K. Lauter – « Cryptographic hash functions from expander graphs », *Journal of Cryptology, à paraître* (2006).

[5] H. Cohen – *A course in computational algebraic number theory*, GTM, vol. 138, Springer, 1993.

[6] J.-M. Couveignes – « Hard homogeneous spaces », *Cryptology ePrint Archive, eprint.iacr.org/2006/291.ps* (2006).

[7] O. Goldreich – *Modern cryptography, probabilistic proofs and pseudo-randomness*, Algorithms and Combinatorics, vol. 17, Springer, 1999.

[8] A. K. Lenstra & E. Verheul – « The XTR public key system », *LNCS* **1880** (2000), p. 1–19.

[9] A. Pizer – « Ramanujan graphs and Hecke operators », *Bulletin of the AMS* **23** (1990), no. 1.

[10] H. Riesel – « Some soluble cases of the discrete logarithm problem », *BIT* **28** (1988), p. 839–851.

[11] K. Rubin & A. Silverberg – « Torus-based cryptography », *LNCS* (2003), no. 2729, p. 349–365.

[12] ———, « Using primitive subgroups to do more with fewer bits », *LNCS* (2004), no. 3076, p. 18–41.

[13] H.-G. Ruck – « On the discrete logarithm in the divisor class group of curves », *Math. Comp.* **68** (1999), p. 805–806.

[14] A. Salomaa – *Public-key cryptography*, Springer, 1996.

[15] P. Sarnak – *Some applications of modular forms*, Cambridge Tracts in Mathematics, vol. 99, Cambridge, 1990, — **N° 160**.

[16] R. Schoof – « Elliptic curves over finite fields and the computation of square roots modulo p », *Math. Comp.* **44** (1985), p. 183–211.

[17] ———, « Counting points on elliptic curves over finite fields », *Journal de Théorie des Nombres de Bordeaux* **7** (1995), p. 219–254.

[18] I. Semaev – « Evaluation of discrete logarithms in a group of p-torsion of an elliptic curve in characteristic p », *Math. Comp.* **67** (1998), p. 353–356.

[19] J.-P. Serre – *Groupes algébriques et corps de classes*, deuxième éd., Hermann, 1959.

[20] N. Smart – « The discrete logarithm problem on elliptic curves of trace one », *Journal of Cryptology* **12** (1997), no. 3, p. 193–196.

[21] P. Smith & C. Skinner – « A public-key cryptosystem and a digital signature system based on the Lucas functions analogue to discrete logarithm », *LNCS* (1995), no. 917, p. 357–364.

Jean-Marc Couveignes, Institut de mathématiques de Toulouse, Université de Toulouse et CNRS
E-mail : couveig@univ-tlse2.fr • *Url :* http://www.picard.ups-tlse.fr/~couveig