Analyse de nouvelles primitives cryptographiques pour les schémas Diffie-Hellman

Jean-Gabriel Kammerer

▶ **To cite this version:**

Jean-Gabriel Kammerer. Analyse de nouvelles primitives cryptographiques pour les schémas Diffie-Hellman. Mathématiques générales [math.GM]. Université de Rennes, 2013. Français. NNT : 2013REN1S035 . tel-00872019

HAL Id: tel-00872019

https://theses.hal.science/tel-00872019

Submitted on 11 Oct 2013

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

ANNÉE 2013

THÈSE / UNIVERSITÉ DE RENNES 1
sous le sceau de l'Université Européenne de Bretagne

pour le grade de

DOCTEUR DE L'UNIVERSITÉ DE RENNES 1

Mention : Mathématiques et Applications

Ecole doctorale MATISSE

présentée par

Jean-Gabriel Kammerer

préparée à l'IRMAR, unité mixte de recherche n° 6625 du CNRS
Institut de Recherche Mathématique de Rennes (Univ. Rennes 1)
et à la Direction G^{ale} de l'Armement / Maîtrise de l'Information

---

Analyse de nouvelles primitives cryptographiques pour les schémas Diffie-Hellman

Thèse soutenue à Rennes le 23 mai 2013

devant le jury composé de :

Pierrick GAUDRY
LORIA, Nancy / rapporteur

David KOHEL
Université d'Aix-Marseille / rapporteur

Jean-Marc COUVEIGNES
Université de Bordeaux I / examinateur

Antoine JOUX
CryptoExperts et Université de Versailles Saint-Quentin-en-Yvelines / examinateur

Jean-François MESTRE
Université Paris 7 / examinateur

Guénaël RENAULT
Université Pierre et Marie Curie / examinateur

Félix ULMER
Université de Rennes 1 / examinateur

Reynald LERCIER
DGA et Université de Rennes 1 / directeur de thèse

Remerciements

Voici donc venu le moment de rédiger cette dernière page. Mes remerciements s'adressent bien sûr tout d'abord à mon directeur de thèse, Reynald Lercier. Merci de m'avoir accueilli dans l'équipe crypto du Centre d'Électronique de l'Armement (CELAr) [1], d'avoir ensuite accepté de m'encadrer pour cette thèse. Merci de m'avoir appris les méthodes de recherche que j'ai acquises durant ces années, et de m'avoir transmis cette expérience et ces connaissances tant mathématiques qu'informatiques. Enfin, merci d'avoir géré bon nombre d'aspects pratiques de la soutenance.

Merci ensuite à mes deux rapporteurs, Pierrick Gaudry et David Kohel. Merci pour votre relecture approfondie et vos remarques détaillées et constructives sur le manuscrit.

Merci également à Jean-Marc Couveignes, Antoine Joux, Jean-François Mestre, Guénaël Renault et Félix Ulmer de m'avoir fait l'honneur d'être les membres de mon jury de thèse.

Merci à mes co-auteurs, Jean-Marc Couveignes (de nouveau), Vivien Dubois, Reynald Lercier et Guénaël Renault (de nouveau). Ce fut un plaisir d'apprendre à vos côtés. Merci également pour les sujets de recherche que vous m'avez apportés. J'espère que notre collaboration ne s'arrêtera pas avec cette thèse.

Merci à tous mes collègues du laboratoire de cryptographie. Merci en particulier pour votre disponibilité à tous sujets : mathématiques, techniques, administratifs ou autres.

Merci à toute la hiérarchie du CELAr puis de DGA/MI de m'avoir donné des conditions qui m'ont permis de réaliser une thèse. Le mi-temps recherche de tout le laboratoire y est irremplaçable.

Je tiens à remercier collectivement mais individuellement l'indispensable personnel administratif (dans les secrétariats en particulier) et de soutien tant de l'IRMAR que de la DGA. Sans votre concours, les conditions de travail ne seraient pas du tout les mêmes.

1. Renommé depuis Direction Générale de l'Armement/Maîtrise de l'Information (DGA/MI).

Merci à tous ceux qui sont venus à ma soutenance, et à tous ceux qui auraient aimé être là. Je pense bien à vous.

Naturellement, merci à vous tous qui me lisez. C'est pour vous que cette thèse est écrite.

Merci à Thibaut et Warith de vous être intéressés à ma thèse, sur un sujet que vous ne maîtrisiez pas, peut-être même aride pour qui n'est pas du domaine. Merci pour votre relecture néanmoins très attentive.

Merci à tous mes amis pour leur disponibilité, leur écoute. Évidemment, merci pour nos discussions enrichissantes et les bons moments partagés.

Merci à tous ceux qui, de près ou de loin, famille ou belle-famille, m'ont encouragé et ont contribué à rendre ces années agréables.

Merci tout particulièrement à mes parents. Cette thèse n'aurait pas même existé sans la qualité de votre éducation et du soin que vous avez apporté à mon instruction.

Enfin, le dernier mais le *plus* important, merci à Solène-Florence pour toutes ces raisons et bien plus encore. Merci de m'avoir accueilli (dans ta vie), merci pour ta participation à l'organisation de ma soutenance. Merci de m'avoir fait l'honneur d'être ma femme ! Merci pour tout ce que j'apprends avec toi et les idées que tu m'apportes. J'espère que notre union ne s'arrêtera jamais. Merci pour ta disponibilité à tous sujets, merci pour ton concours à mes conditions de vie (et donc aussi à mes conditions de travail). Merci d'être venue à ma soutenance, de m'avoir relu, de t'être intéressée à la cryptologie en général et à ma thèse en particulier, préoccupations bien éloignées de l'anapath. Merci pour ta disponibilité, pour ton écoute, nos discussions. Merci également pour les bons moments que nous partageons et pour tous ceux que nous partagerons. Merci pour l'attention que tu portes à notre relation. Merci de m'avoir encouragé et d'avoir contribué à rendre ces années agréables. Bref, merci pour ton amour.

Introduction

La cryptographie, étymologiquement *écriture cachée*, a longtemps consisté en l'étude de la protection de la confidentialité des communications entre deux acteurs. Il s'agit d'éviter que la connaissance des transmissions ne permette à un adversaire qui les aurait espionnés d'en extraire le sens.

Plusieurs critères définissent un bon cryptosystème. À la fin du XIX^{e} siècle, le cryptologue néerlandais Auguste Kerckhoffs proposa plusieurs règles destinées à assurer la confidentialité d'une communication. Toujours d'actualité, on en dégage les quelques grands principes suivants. Le premier point est la sécurité : une information chiffrée ne doit pas être récupérable sans connaissance d'un secret partagé, une *clef* ; la sécurité ne repose pas sur la confidentialité des méthodes de chiffrement utilisées et la façon dont elles utilisent ce secret, et peuvent donc être publiées. Le deuxième est que pour des raisons pratiques évidentes, un message codé ne doit pas être de taille disproportionnée comparée à l'original. Enfin le système doit être simple d'utilisation.

Longtemps cantonnés à un usage diplomatique ou militaire, voire commercial, les usages de la cryptologie se sont automatisés avec l'avènement de moyens de télécommunications évolués, notamment télégraphiques. Avant tout, de nouveaux besoins se sont créés : si historiquement les communications se faisaient entre deux personnes bien identifiées, les nouveaux contextes d'utilisation sont très variés. Parallèlement, la mécanisation puis l'informatisation ont révolutionné tant les mécanismes de protection que les méthodes pour les attaquer.

Par exemple, un site internet marchand va devoir prouver qu'il est bien le commerçant légitime qu'il prétend être à un nouveau client, avant que celui-ci ne lui envoie les informations permettant le paiement de manière confidentielle. De plus, il doit être impossible que, bien que chiffrées, ces informations soient modifiées durant le transfert : le client ne veut pas qu'un montant de 20€ se transforme en prélèvement de 200€ parce que son autorisation aura été transformée, comme si on avait ajouté un zéro au montant d'un chèque.

Usuellement, on appelle Alice et Bob les deux protagonistes qui veulent communiquer de manière confidentielle. Nous appellerons Ève[2] l'adversaire qui écoute la

2. De l'anglais *eavesdrop*, espionner.

conversation et veut savoir de quoi il retourne ou simplement la perturber.

Le procédé le plus naturel, utilisé depuis des siècles, pour qu'Alice et Bob puissent s'échanger des messages en toute confidentialité est qu'ils chiffrent les messages grâce à une clef commune. Celle-ci est simplement une sorte de mot de passe secret, un dictionnaire qu'ils ont négocié antérieurement et qui leur permet aussi bien de coder le message que de le déchiffrer. La difficulté principale réside dans l'initialisation : il faut bien qu'Alice et Bob se rencontrent une première fois et s'échangent le dictionnaire en question de la main à la main, sans aucun risque d'interception. C'est seulement par la suite qu'ils pourront, de loin, s'échanger des messages chiffrés qui pourront être interceptés par Ève sans danger.

Depuis 1976, la cryptographie s'est orientée vers des systèmes à clef publique, c'est-à-dire asymétriques. Le tout premier système connu de ce type est l'échange de clef Diffie-Hellman [25], qui permet à Alice et Bob de se mettre d'accord sur un secret commun en échangeant des messages sur un canal public. Ce secret commun pourra ensuite être utilisé comme clef secrète dans un mécanisme symétrique. Ce système est une révolution : Alice et Bob n'ont plus besoin de se rencontrer ! La contrepartie est qu'il faut que les messages permettant la négociation du secret soient transmis de manière fidèle : Ève ne doit pas réussir à se faire passer pour Alice vis-à-vis de Bob.

Poussons le raisonnement plus loin encore. Pourquoi serait-il nécessaire que la clef de chiffrement soit la même que la clef de déchiffrement ? Dans cet esprit, Diffie et Hellman proposent en 1976 l'idée suivante : Alice publie une clef qui permet à Bob de chiffrer son message. Bob envoie ce dernier à Alice, qui le déchiffre grâce à une clef secrète dont elle est la seule détentrice. Ce système *à clef publique* est appelé *asymétrique* car il ne permet que l'envoi de messages à destination d'Alice. La clef de chiffrement étant publiée, tout le monde (et plus seulement Bob) peut d'ailleurs lui envoyer un message. Comme dans la négociation de secret, il est nécessaire que la clef présentée comme étant celle d'Alice le soit effectivement, c'est-à-dire qu'Ève ne peut pas proposer sa propre clef publique à Bob en lui faisant croire qu'il s'agit de celle d'Alice. Il faut donc une certification des clefs publiques.

Il est facile de faire un lien entre la négociation de secret et la cryptographie à clef publique : quand Alice et Bob veulent s'échanger une clef, ils s'envoient chacun un message, publiquement. Introduisons une asymétrie, par exemple temporelle : Alice publie son message de négociation de secret en premier, Bob répond pour établir le secret commun et envoie ses informations confidentielles. Alice n'a besoin que d'envoyer un seul message pour établir un secret commun avec Bob, ce secret dépendant en retour de la réponse de Bob. Toute personne qui aurait également reçu le message initial d'Alice pourrait à son tour répondre à Alice pour négocier un autre secret avec elle, et donc pouvoir communiquer avec elle de manière confidentielle. Finalement, le premier message d'établissement de secret partagé envoyé par Alice

peut assez facilement jouer le rôle de clef publique d'Alice : plutôt que de l'envoyer à Bob uniquement, elle peut le publier. C'est l'idée du cryptosystème ElGamal [33].

On peut imaginer aller encore plus loin. Peut-on éviter même qu'Alice doive publier une clef ? Pourquoi l'*identité* d'Alice, par exemple son nom, son numéro de sécurité sociale, ne suffirait-elle pas pour en déduire une clef de chiffrement ? C'est le principe du chiffrement basé sur l'identité [5], qui élimine le problème de la certification. En contrepartie, si Alice perd sa clef de déchiffrement, il lui sera difficile d'en obtenir une autre vu qu'elle est liée à son identité.

Tous ces cryptosystèmes asymétriques présentés ici abstraitement ont des réalisations pratiques. Les systèmes à clef publique reposent sur la notion de fonction à *trappe*. Une fonction à trappe est une fonction facilement calculable, dont l'inverse se calcule en temps raisonnable à l'unique condition de disposer d'une information supplémentaire. Dans un système à clef publique, les messages sont chiffrés à l'aide d'une clef publique et le destinataire les déchiffre grâce à ce petit surplus d'information, la clef privée, dont il est le seul détenteur.

Ces fonctions à trappe reposent toujours sur des problèmes mathématiques considérés comme difficiles. L'étude de leur complexité permet d'estimer le niveau de sécurité atteint pour un attaquant ayant une capacité de calcul donnée, et donc de dimensionner les paramètres pratiques des cryptosystèmes.

L'instanciation proposée à l'origine par Diffie et Hellman reposait sur le groupe multiplicatif d'un corps fini. La fonction qui intervient dans l'échange de clef Diffie-Hellman est généralement l'élévation à une certaine puissance. L'opération réciproque est le calcul d'un *logarithme discret*. Koblitz et Miller ont réalisé indépendamment que cette primitive peut opérer sur tout type de groupe. Devant les avancées tant théoriques que pratiques des algorithmes de calcul de logarithme discret dans les corps finis, ils proposent d'utiliser le groupe des points rationnels d'une courbe elliptique définie sur un corps fini ou plus généralement la jacobienne d'une courbe algébrique [47, 55]. Pour un même niveau de résistance au problème du logarithme discret, les courbes nécessitent un dimensionnement réduit et leur utilisation est donc plus efficace. Toutefois, ce sont des objets plus complexes et certaines opérations primitives qui étaient faciles à construire dans les corps finis deviennent alors non triviales.

L'étude des courbes elliptiques remonte à Abel et Weierstrass au XIX^{e} siècle, celle des corps finis était maîtrisée dès le début du XX^{e} siècle. Les travaux de Serre et Grothendieck lancent la géométrie algébrique moderne à partir des années 1950, qui aboutit en 1973 à la démonstration des conjectures de Weil par Deligne. Toutefois ces avancées sont majoritairement théoriques au sens où peu de méthodes effectives existaient. Mûe par les applications cryptographiques, une nouvelle discipline a donc émergé dans les années suivantes, la théorie algorithmique des nombres, avec la découverte de nombreux algorithmes permettant l'utilisation concrète des courbes

algébriques en cryptographie. Le premier problème est celui de la loi de groupe elle-même. Il a été efficacement résolu par Cantor [16] pour les jacobiennes de courbes hyperelliptiques, les courbes algébriques plus générales restant un problème parfois difficile.

Les algorithmes de la théorie des nombres en cryptographie doivent être déterministes, pour plusieurs raisons. L'intérêt est premièrement théorique : on veut maîtriser le temps de calcul, et cela passe notamment par une certitude absolue, mathématique, qu'il finira. Certains problèmes sont encore ouverts, tels que le calcul déterministe de racines de polynômes sur un corps fini, d'autres ont été résolus, comme le test de primalité déterministe AKS [2].

Deuxièmement, le temps d'exécution d'un algorithme fait fuir de l'information sur les calculs effectués, en particulier sur les secrets manipulés. Nous touchons ici l'implémentation réelle des algorithmes sur un ordinateur ou un composant. Ces idées ont été initiées dans la communauté académique par les travaux de Kocher avec les attaques mesurant la consommation de courant électrique [49]. Pour une taille de paramètres donnée, un algorithme qui effectuera toujours le même nombre d'opérations, toujours dans le même ordre indépendamment des entrées particulières ne fera pas fuir d'information sur celles-ci. Un tel algorithme est dit à *temps constant*, et il est nécessairement déterministe.

Nous nous sommes intéressés à une des primitives cryptographiques qu'il est facile de réaliser dans un corps fini, mais beaucoup moins sur une courbe algébrique. Les opérations cryptographiques asymétriques sont réalisées dans des structures mathématiques (groupes), alors que les messages sur lesquelles elles opèrent sont simplement des chaînes de caractères. Il est donc nécessaire de les transformer en éléments du groupe. Et autant il est évident d'interpréter un message comme une chaîne de bits et de l'encoder comme un élément d'un corps fini (nombre modulo p ou polynôme) pour réaliser par exemple un chiffrement asymétrique, autant il est bien moins évident d'interpréter la même chaîne de bit comme un point d'une courbe elliptique pour réaliser les mêmes opérations. On touche ici le problème de l'*encodage* de messages vers une courbe algébrique, qui occupe la première partie de ce mémoire.

Pour des raisons tant pratiques (temps constant) que théoriques (pour certains protocoles tels que le chiffrement basé sur l'identité), il faut un encodage pour lequel on maîtrise *a priori* le nombre d'antécédents de tout point encodé : il quantifie la sécurité du protocole. De plus, les contraintes de sécurité empêchent d'utiliser des encodages triviaux : reposant sur la difficulté de calculer le logarithme discret, il ne faut pas induire de relation directe entre deux messages et les logarithmes des points encodés. Il est donc hors de question de simplement élever un générateur G à la puissage t. Il nous faut en fait une *fonction de hachage* vers la courbe.

L'obstacle majeur à l'encodage d'un corps fini vers une courbe algébrique réside

dans la nécessité de trouver, de manière déterministe, sous quelles conditions certains polynômes prennent pour valeurs des résidus quadratiques.

La première avancée dans ce domaine a été proposée par Shallue et van de Woestijne [64] en 2006. Reposant sur la théorie des nombres, l'idée est de calculer trois fonctions dues à Skalba [68], qui dépendent de l'équation de la courbe. En le paramètre, au moins une de ces fonctions prend une valeur résidu quadratique. La contribution des auteurs est d'en déduire un point sur la courbe, par l'identification de la bonne fonction pour la valeur du paramètre et le calcul de la racine carrée associée de manière déterministe. Ces fonctions ont été généralisées à certaines courbes hyperelliptiques par Ulas [70]. Néanmoins, cet encodage ne s'exécute pas immédiatement en temps constant à taille de données d'entrée fixée.

Icart a amélioré ces encodages de sorte qu'ils s'exécutent en temps constant. En 2009, il a publié une nouvelle fonction d'encodage [38], plus efficace mais limitée aux courbes elliptiques. Nous avons proposé d'autres encodages pour les courbes elliptiques hessiennes et pour certaines familles, assez larges, de courbes hyperelliptiques [45]. Par rapport aux encodages proposés auparavant, leur intérêt est d'avoir un nombre d'antécédents par point encodé réduit. D'autres encodages pour les courbes hessiennes ont encore été proposés par Farashahi [29].

Toutes ces fonctions reposent sur les propriétés géométriques des courbes, en particulier sur la résolubilité des polynômes de degré 3 par radicaux. Nous les étudions en détail au chapitre 3, puis présentons la méthode systématique qui nous a permis d'en proposer de nouvelles au chapitre 4. Nous en profitons pour classifier, en fonction du corps fini de base, les différentes courbes elliptiques et hyperelliptiques pour lesquelles il existe un encodage de type géométrique, celles pour lesquelles les seules solutions connues sont celles de Shallue, van de Woestijne et Ulas, et celles pour lesquelles aucun encodage de complexité déterministe n'est connu.

Cette diversité de fonctions d'encodage pose naturellement la question de leur unification : elles semblent en effet toutes reposer sur une façon particulière de résoudre les cubiques qui interviennent dans l'équation des courbes elliptiques. Nous montrons par la suite comment les formules de Cardan-Tartaglia pour la résolution des polynômes de degré 3 et la géométrie des tangentes aux courbes elliptiques permet d'expliquer ces encodages et d'en trouver une infinité de nouveaux : nous expliquerons comment une fonction d'encodage correspond à la paramétrisation d'une courbe de genre 0 dans l'espace des tangentes. Nous aboutirons au résultat (informel) suivant, chapitre 5 :

Théorème *Soit E une courbe elliptique définie sur $\mathbb{Q}$. Il existe une infinité de pseudo-paramétrisations algébriques de E par des racines cubiques.*

Nous classifierons ensuite ces encodages. Ces travaux ont également fait l'objet d'une publication [23].

Enfin d'autres problèmes que le logarithme discret peuvent être utilisés pour réaliser des échanges de clefs ou du chiffrement asymétrique. En 2000, Ko *et al.* [46] proposent d'instancier des cryptosystèmes asymétriques sur des groupes finis *non commutatifs*. Il ne s'agit plus d'exponentiation mais d'action par conjugaison, bien plus rapides à calculer. Le problème difficile sous-jacent est alors un problème de factorisation ou de *décomposition*. Concrètement, les auteurs proposent d'utiliser des groupes de tresses. Malheureusement, ces instanciations ont fait l'objet d'attaques spécifiques [19], dont l'essence est de représenter les éléments du groupe de tresses comme des matrices de taille raisonnable sur un anneau particulier. Résoudre un problème linéaire suffit alors pour retrouver le secret partagé d'un protocole Diffie-Hellman, les groupes de tresses n'offrent donc pas une sécurité convenable.

Plutôt que d'agir par conjugaison, qui nécessite d'inverser dans le groupe, on peut simplement multiplier à gauche et à droite par deux éléments distincts. On peut alors instancier le protocole Diffie-Hellman non plus sur un groupe, mais simplement sur un semigroupe. C'est la proposition de Boucher *et al.* [10], qui instancient l'échange de clefs Diffie-Hellman sur un anneau de polynômes non commutatif. Nous nous sommes intéressés à ce cryptosystème et proposons un résultat plutôt destructif : contournant le problème difficile de décomposition, nous montrerons au chapitre 7 qu'il est possible de retrouver le secret commun d'un échange de clefs Diffie-Hellman. L'idée est que la structure très forte des polynômes non commutatifs permet de retrouver une décomposition, par calcul de PGCD et algèbre linéaire sur le corps premier de base. Ce travail a fait l'objet d'une publication [26]. Les polynômes tordus n'apportent donc pas une sécurité suffisante pour des protocoles asymétriques reposant sur le le problème Diffie-Hellman non commutatif.

L'instanciation concrète de protocoles de type Diffie-Hellman non commutatif semble donc difficile et reste un problème ouvert.

Table des matières

Index des notations

$\#E$ Cardinal d'un ensemble E, page 38

$\mathcal{C}$ Centre d'un anneau de polynômes tordus, page 101

$\mathcal{D}$ Un ensemble pour instancier le protocole Diffie-Hellman, page 20

$\mathcal{S}$ Un sous-semigroupe commutatif de $\mathcal{D}$ pour le protocole Diffie-Hellman non commutatif, page 21

$\mathcal{E}$ Une courbe elliptique, page 35

$\langle \mathcal{E}, P \rangle$ L'algèbre engendré par un ensemble $\mathcal{E}$ et un polynôme P, page 102

F Une fonction à sens unique pour le protocole Diffie-Hellman, page 20

$\mathbb{F}_q$ Un corps fini, page 41

$\bar{\mathbb{K}}$ Une clôture algébrique de $\mathbb{K}$, page 75

$\mathbb{F}_q[X;\theta]$ L'anneau des polynômes tordus en une indéterminée sur $\mathbb{F}_q$, page 99

$\mathcal{K}$ Un ensemble agissant sur $\mathcal{D}$, page 20

$\mathbb{K}$ Un corps parfait, page 29

$\mathcal{N}$ Quasi-centre d'un anneau de polynômes tordus, page 103

n Un entier tel que $q = p^n$, page 41

p La caractéristique de $\mathbb{F}_q$, page 41

$\mathcal{R}$ Anneau de polynômes tordus, $\mathbb{F}_q[X;\theta]$, page 102

Première partie

Introduction et préliminaires

Chapitre 1

Diffie-Hellman : principe et instanciations

1.1 Notions de sécurité

1.1.1 Sécurité calculatoire

La sécurité d'un système recouvre plusieurs notions, selon les modèles d'attaques choisis. Elle repose sur la notion d'opération élémentaire. Celle-ci correspond en général à un nombre borné d'opérations données sur un microprocesseur. Par exemple, un simple XOR, une opération de chiffrement (par exemple pour une recherche exhaustive), une multiplication modulaire (opération élémentaire dans un corps fini) ou bien une suite d'instructions plus complexes réalisant une addition de points sur une courbe elliptique.

La sécurité d'un cryptosystème dépend donc du nombre minimal d'opérations élémentaires à réaliser pour pouvoir effectuer une attaque avec bonne probabilité. Les attaques possibles sont variées. Il peut s'agir de :

- retrouver la clef, on parle alors de *key recovery attack* ;
- retrouver le clair associé à un chiffré, sans forcément connaître les autres clairs d'autres chiffrés ;
- être capable de distinguer un chiffré d'une chaîne de bits aléatoire avec bonne probabilité, on parle alors d'attaque par *distingueur* ; elle traduit l'idée que le système souffre de faiblesses structurelles ;
- attaque par clef corrélée, *related-key attack* ;
- attaque par collision (sur une fonction de hachage par exemple) ;
- forge (falsification) d'une signature valide sans connaître la clef de signature ;
- calcul de la clef privée à partir de la clef publique ;
- ...

Les opérations élémentaires en elles-mêmes ne sont pas un paramètre important,

Complexité (en bits)	80	128	256
Groupe générique	160	256	512
RSA/DL dans $\mathbb{F}_p^*$	1024	3072	≈ 23000

TABLE 1.1 – Paramètres de sécurité et dimensionnement

il s'agit au plus d'un cycle processeur. On peut donc facilement borner le nombre de cycles nécessaires et donc la quantité de ressources (temps de calcul et espace mémoire) nécessaires sur un microprocesseur ou un circuit électronique spécialisé et estimer ainsi la quantité de ressources nécessaire pour réaliser l'attaque. Il est pratique de considérer le logarithme en base 2 du nombre d'opérations élémentaires nécessaires. En effet, le nombre de cycles réels nécessaires pour une opération élémentaire (par exemple une addition de point sur une courbe elliptique) ne modifiera pas beaucoup ce logarithme, qui dépend ainsi vraiment du cryptosystème et non plus de son implémentation. Il permet également de comparer des systèmes asymétriques à des systèmes symétriques : il s'apparente à la complexité d'une recherche de clef par force brute sur un système symétrique. On considérait généralement dans les applications civiles que 2^{80} opérations donnaient une sécurité acceptable jusqu'à 2010, 2^{128} étant d'ores et déjà recommandé et nécessaire au-delà.

Exiger un certain niveau de sécurité d'un cryptosystème revient à en exiger un dimensionnement. Le *paramètre de sécurité* correspond ainsi à la fois aux ressources nécessaires à l'exécution de l'attaque et à sa probabilité de réussite. La complexité des attaques et leur probabilité de réussite permet alors de relier la sécurité attendue et la taille des objets utilisés dans le cryptosystème. Nous en rappelons quelques-uns dans le tableau 1.1.

1.1.2 Sécurité des implémentations et déterminisme

Le paragraphe précédent décrit la sécurité d'un cryptosystème face à un attaquant qui ne s'intéresserait qu'aux *informations* échangées par Alice et Bob. Une autre frange de la cryptologie s'intéresse au cas suivant : et si l'attaquant avait un certain accès à la machine physique qu'Alice utilise pour réaliser ses opérations cryptographiques (chiffrement, signature, etc.) ?

L'exemple le plus simple, réaliste, concerne le temps de calcul : quand Ève intercepte les messages échangés entre Alice et Bob, elle peut en plus mesurer l'heure à laquelle elle les reçoit et en déduire une information sur le temps qu'Alice et Bob ont mis pour réaliser les informations cryptographiques. Cette mesure est certes bruitée par la gigue inhérente au réseau, mais néanmoins récupérable. D'autres paramètres physiques supposent que l'attaquant a un accès plus proche encore des protagonistes. Sur une machine partagée, par exemple un serveur Web virtualisé, Ève peut mesurer

beaucoup plus finement les temps de calcul et même tenter de les gêner (pollution du cache processeur par exemple). Ou encore, Ève peut avoir accès physiquement à la machine qu'Alice utilise et mesurer la consommation de courant ou le rayonnement électromagnétique...

Ces attaques, dites *par canaux auxiliaires*, apportent une information à Ève sur le *déroulement* de l'exécution des opérations cryptologiques. La section précédente supposait qu'Ève n'interceptait que leurs *résultats*. Toute la question est alors de savoir si Ève peut utiliser utilement les informations auxiliaires obtenues et comment.

Une façon de s'assurer que le temps de calcul ne révèle pas d'information sur les secrets manipulés consiste à ce que les algorithmes cryptographiques effectuent toujours le même nombre d'opérations. Les variations de temps de calcul peuvent être liées à deux facteurs. Le premier concerne les algorithmes non déterministes : un algorithme de type Las Vegas fournit une solution toujours correcte, mais en un temps variable. Les algorithmes de type Monte-Carlo au contraire s'exécutent toujours en le même temps, mais produisent parfois des résultats faux. On les transforme donc souvent en un algorithme de type Las Vegas en les exécutant un nombre de fois variable jusqu'à obtenir une solution correcte. En s'autorisant un pourcentage d'erreur, on peut les contraindre à s'exécuter un nombre de fois fixé afin de déterminiser leur temps d'exécution, toutefois cela est peu efficace en général et non satisfaisant sur le plan théorique : bien que la probabilité en soit maîtrisée, l'algorithme peut alors ne pas retourner de résultat correct.

Une deuxième source de variabilité des temps d'exécution provient de chemins d'exécutions différents selon les *entrées*. Prenons l'exemple des tris par comparaison. Les meilleurs s'exécutent en temps quasi-linéaire. L'algorithme de tri rapide est notamment le plus efficace connu *en moyenne*, mais sa complexité dans le pire des cas est quadratique. Bien que complètement déterministe (la sélection de pivot et les diverses opérations ne se font pas aléatoirement), son temps d'exécution dépend donc de ses entrées. Mesurer son temps d'exécution révèle donc de l'information sur l'état de la liste qui lui était donnée à trier (contenait-elle des sous-listes triées ou était elle aléatoire ?), sans même la connaître. Le tri fusion s'approche d'un algorithme à temps constant, au sens où sa complexité asymptotique dans le pire des cas est égale à sa complexité dans le cas moyen et quasi-linéaire. Il effectue toujours les même comparaisons. Les variations de temps d'exécution proviennent de l'étape de fusion : suivant l'ordre relatif des éléments de deux listes à fusionner, on ne fait pas toujours le même nombre de comparaisons. Il est facile de déterminiser le temps d'exécution du tri sans modifier sa complexité, en ajoutant un symbole "infini" à la fin de chaque chaîne à fusionner. Le tri fusion s'exécute alors en temps constant déterministe, ou plus simplement temps constant, c'est-à-dire que le temps d'exécution de l'algorithme ne dépend que de la *taille* de l'entrée (longueur de la liste dans le cas du tri), pas de leur valeur (ordre initial des éléments dans la liste).

En particulier, pour une taille d'entrée donnée, le pire cas d'un algorithme à temps constant déterministe prend le même temps à être exécuté que le cas moyen.

Afin de limiter les attaques par mesure de temps d'exécution, les algorithmes de hachage vers courbes algébriques que nous étudions dans la partie II s'exécutent efficacement de façon déterministe en temps constant.

Remarque : habituellement, parler de temps d'exécution constant s'interprète en termes de complexité, temps constant signifiant un nombre d'opérations borné indépendamment de l'entrée, s'opposant donc à complexité linéaire, quadratique, exponentielle en fonction de la taille des entrées. Nous le prenons bien sûr dans l'acception décrite ci-dessus (déterminisme du temps de calcul) et étudions le cas échéant la complexité des algorithmes que nous proposerons.

1.2 Variations autour de l'échange de clefs Diffie-Hellman

1.2.1 Cadre générique

Depuis la proposition originale de Diffie et Hellman [25], beaucoup de variantes ont été proposées sur le même principe. La structure de base d'un échange de clef type Diffie-Hellman est la suivante. Soient $\mathcal{K}$ et $\mathcal{D}$ deux ensembles et soit F une fonction de $\mathcal{D} \times \mathcal{K}$ dans $\mathcal{D}$ (c'est-à-dire une action externe de $\mathcal{K}$ sur $\mathcal{D}$) telle que :

- pour tout z dans $\mathcal{D}$, $F(z, \cdot)$ est une fonction à sens unique
- l'ensemble des fonctions $F_a = F(\cdot, a)$ est commutatif pour la composition, c'est-à-dire que pour tout $(a, b) \in \mathcal{K}^2$, $F_a \circ F_b = F_b \circ F_a$.

Dans un protocole de type Diffie-Hellman, la fonction F et un élément particulier z de $\mathcal{D}$ sont des informations publiques. Lors d'un premier passage, chaque partie choisit de son côté un élément aléatoire dans l'ensemble $\mathcal{K}$ (a pour Alice et b pour Bob), chiffre z avec et envoie le résultat à l'autre partie. Alors chaque partie chiffre de nouveau l'élément reçu avec son propre élément de $\mathcal{K}$. *In fine*, tous deux détiennent

$$F_a(F_b(z)) = F_b(F_a(z)).$$

La sécurité du protocole repose sur le fait qu'étant donnés $F_a(z)$ et $F_b(z)$, il est impossible de calculer cette donnée commune (hypothèse Diffie-Hellman calculatoire). Bien sûr, cette hypothèse ne peut être vraie que si $F(\cdot, z)$ est une fonction à sens unique puisque l'on peut sinon, par exemple, retrouver a à partir de $F_a(z)$ et avoir alors autant d'information qu'Alice.

Une variante *décisionnelle* de ce problème est la suivante : étant donnés $\mathcal{K}$, $\mathcal{D}$ et F et quatre éléments u, v, z et z' dans $\mathcal{D}$, décider s'il existe a et b dans $\mathcal{K}$ tels que

$u = F_a(z),\ v = F_b(z)$ et $z' = F_a\big(F_b(z)\big)$.

1.2.2 Groupes

La proposition originelle de Diffie et Hellman était de définir F comme l'exponentiation de z par a dans un groupe multiplicatif [25]. Quand z est un élément du groupe donné, ses puissances forment un sous-groupe cyclique donc commutatif, noté $\langle z \rangle$. Le caractère sens-unique de $F(\cdot, z)$ signifie qu'il est impossible d'identifier la puissance de z correspondant à un élément quelconque de $\langle z \rangle$, c'est-à-dire qu'il est impossible de calculer le logarithme discret de base z dans $\langle z \rangle$.

Aucune autre méthode que le calcul du logarithme discret n'étant connue pour résoudre le problème Diffie-Hellman calculatoire, cette variante est de loin la plus utilisée. Elle semble trouver des instanciations satisfaisantes, *cf* section 1.3.

Plus généralement, l'échange Diffie-Hellman procède dans ce cas par l'action *transitive et libre* d'un groupe commutatif G sur un ensemble quelconque [22]. La commutativité de l'action, et donc la propriété Diffie-Hellman, découle de celle du groupe. Dans le cas original de Diffie et Hellman, $G = \mathbb{Z}/n\mathbb{Z}$ agit par exponentiation sur un groupe cyclique de cardinal n. Couveignes [22] propose un autre exemple : G peut-être le groupe des classes d'un ordre quadratique sur les courbes elliptiques à multiplication complexe (en particulier celles définies sur un corps fini $\mathbb{F}_q$), agissant sur l'ensemble (qui n'est pas un groupe) des courbes elliptiques définies sur $\mathbb{F}_q$.

1.2.3 Variantes non commutatives

Plusieurs propositions de fonctions F pour un protocole Diffie-Hellman ont été avancées sur des structures algébriques non commutatives. En général, ces schémas reposent sur un problème de factorisation (ou décomposition) particulier plutôt que sur celui du logarithme discret. De plus, ils apparaissent tous comme des variations de la construction suivante [46].

Soit $(\mathcal{D}, \diamond)$ un semigroupe non commutatif (c'est-à-dire qu'il ne possède pas nécessairement un élément neutre et que tous les éléments n'ont pas forcément un inverse). Les éléments de $\mathcal{D}$ peuvent se décomposer d'un grand nombre de façons en général. Par conséquent, on peut supposer qu'étant donnés des éléments z, z' de $\mathcal{D}$ tels que z' admette une factorisation de la forme $u \diamond z \diamond v$, il est calculatoirement difficile de retrouver de tels éléments u et v. Ainsi, on définit l'ensemble $\mathcal{K}$ comme les couples $(u, v) \in \mathcal{D}^2$ et on définit $F : \big(z, (u, v)\big) \mapsto u \diamond z \diamond v$. Lorsque le problème de décomposition mentionné ci-dessus est insoluble, alors F est à sens unique. Pour que F soit également commutative, il faut que les fonctions $F\big(\cdot, (u, v)\big)$ soient commutatives. Il suffit pour cela de choisir des éléments u, v dans un sous-semigroupe commutatif $\mathcal{S}$ de $\mathcal{D}$. Par conséquent, $\mathcal{K} = \mathcal{S} \times \mathcal{S}$. Ceci modifie en retour la propriété sens unique de F. Le problème devient alors :

Problème 1.2.1 (Problème Diffie-Hellman non commutatif) *Soit $\mathcal{S}$ un sous-semigroupe commutatif de $\mathcal{D}$. Étant donnés un élément z de $\mathcal{D}$ et un élément z' de $\mathcal{S} \diamond z \diamond \mathcal{S}$, trouver u et v dans $\mathcal{S}$ tels que $z' = u \diamond z \diamond v$.*

À ce stade, il n'est pas évident de savoir si le choix des facteurs gauche et droite dans un sous-semigroupe commutatif affaiblit le problème de décomposition. De toute façon, par construction il est difficile d'imaginer qu'un cryptosystème puisse se passer d'une telle propriété.

Parmi les variations classiques de la description ci-dessus, on peut noter l'idée de choisir u et v dans deux sous-semigroupes $\mathcal{L}$ et $\mathcal{R}$ qui sont soit tous deux commutatifs, soit commutent l'un avec l'autre (dans ce cas, un des participants au protocole Diffie-Hellman non commutatif utilise $\mathcal{L} \times \mathcal{R}$ et l'autre utilise $\mathcal{R} \times \mathcal{L}$). Un cadre plus général peut aussi être de ne plus exiger que le semigroupe commutatif $\mathcal{S}$ soit un sous-ensemble de $\mathcal{D}$: il lui suffit simplement d'agir de façon différente à gauche et à droite de $\mathcal{D}$. Ceci est d'autant plus analogue à un système générique basé sur le logarithme discret, où $\mathcal{D}$ peut être un groupe arbitraire et $\mathcal{S}$ un ensemble d'entiers modulaires.

Contrairement aux actions de groupe de la section précédente, nous n'exigeons pas que l'action du sous-semigroupe soit transitive ou libre. Ceci facilite la résolution du problème Diffie-Hellman non commutatif. Dans le cas où l'action est non libre, cela signifie que certains éléments de $\mathcal{K}$ laissent $\mathcal{D}$ invariant, et donc que l'action n'est pas à sens unique pour les stabilisateurs. Les stabilisateurs forment donc un sous-ensemble de $\mathcal{K}$ pour lequel le problème Diffie-Hellman non commutatif est trivial.

Plus intéressant est le cas d'une action non transitive : dans ce cas, pour un z' donné, il peut exister plusieurs décompositions de z' sur $\mathcal{S} \diamond z \diamond \mathcal{S}$. Il suffit pour résoudre le problème Diffie-Hellman non commutatif de trouver *une seule* de ces relations, ce qui est un problème plus facile. Nous utilisons cette propriété pour attaquer une instanciation de protocole Diffie-Hellman sur les polynômes tordus (*cf* chapitre 7).

1.2.4 Chiffrement El-Gamal

Reprenant les notations de la section 1.2.1, on peut toujours transformer un échange de clef Diffie-Hellman en un cryptosystème à clef publique : il suffit à Alice de choisir un $z \in \mathcal{D}$, un $a \in \mathcal{K}$ et de publier z et $F_a(z)$, en conservant a secret. Alors toute personne désirant envoyer un message à Alice peut choisir de son côté un élément $b \in \mathcal{K}$, envoie publiquement $F_b(z)$ à Alice et calcule $F_b\big(F_a(z)\big)$ qui est un secret partagé.

Ce secret peut alors servir à masquer un message m que Bob voudrait envoyer à Alice : par exemple, la proposition initiale de El Gamal [33] propose de réaliser l'échange dans le groupe multiplicatif d'un corps fini G. Dans ce cas, si on interprète

le message m comme un élément de G, on peut tout simplement envoyer à Alice le couple $\Big(F_b(z), m \cdot F_b\big(F_a(z)\big)\Big)$. Grâce à son élément secret a, Alice peut calculer le secret partagé à partir de $F_b(z)$ et retrouver le message m. Un exemple détaillé se trouve dans la section 1.4.1 ci-dessous.

Dans le cas où l'ensemble de base $\mathcal{D}$ n'est pas un groupe, on peut dériver une chaîne de bits aléatoire à partir du secret partagé $F_a\big(F_b(z)\big)$, par exemple grâce à une fonction de hachage, et s'en servir comme clef dans un cryptosystème symétrique.

1.3 Instanciations

1.3.1 Corps finis

Le groupe multiplicatif des corps finis est historiquement la première structure dans laquelle le problème Diffie-Hellman a semblé trouver une instanciation satisfaisante. La fonction F associée est l'exponentiation, calculer son inverse est le problème du logarithme discret dans les corps finis, longuement étudié par la communauté cryptographique par la suite.

Des algorithmes de calcul d'index (crible du corps de nombre, crible du corps de fonctions) permettent de résoudre ce problème avec complexité heuristique sous-exponentielle. De nombreux raffinements ont été proposés dans la littérature. [59] décrit l'histoire et le principe de ces algorithmes, qui dérivent d'idées dues à Kraitchik datant des années 1920, généralisant elles-mêmes des techniques de Fermat.

À niveau de difficulté du logarithme discret donné, l'existence de ces algorithmes nécessite d'augmenter considérablement la taille des corps finis. En effet, le pire cas pour le cryptanalyste, c'est-à-dire les corps les plus solides sont les corps premiers. Si $\mathbb{F}_p$ est un corps premier avec p de l'ordre de n bits, le meilleur algorithme connu résout le problème du logarithme discret avec complexité $\exp\big((c + o(1))n^{1/3}\log^{2/3}(n)\big)$. Le tableau 1.1 illustre la taille de corps nécessaire à niveau de sécurité donné.

1.3.2 Courbes elliptiques

L'idée d'utiliser les courbes algébriques définies sur un corps fini pour réaliser des cryptosystèmes asymétriques reposant sur le logarithme discret remonte à 1985. Elle est due indépendamment à Koblitz et Miller [47, 55]. Il s'agit d'utiliser le groupe des points d'une courbe elliptique et la loi bien connue dite "corde-tangente". Plus généralement, on utilise la jacobienne d'une courbe de genre g supérieur à 1, c'est-à-dire non plus des points mais des *diviseurs*, des ensembles de g points de la courbe éventuellement définis sur une extension du corps de base. Grâce aux travaux initiaux de Cantor [16], des techniques efficaces existent pour calculer la loi de groupe dans les courbes hyperelliptiques [20].

Le premier intérêt des courbes réside en le fait que les seuls algorithmes connus pour calculer le logarithme discret sont exponentiels, sauf dans des cas très particuliers. Pour une difficulté du logarithme discret donnée, il est donc possible de manipuler des objets (diviseurs sur les courbes) de taille réduite par rapport au cas des corps finis. En général, pour un groupe de cardinal $N \approx 2^n$ défini sur une courbe algébrique de genre 1 ou 2, le meilleur algorithme connu calcule le logarithme discret avec complexité $\mathcal{O}(\sqrt{N})$. Le tableau 1.1 compare les tailles de groupes nécessaires au cas des corps finis.

Enfin les courbes possèdent des propriétés mathématiques intéressantes liées à l'existence de *couplages*, c'est-à-dire qu'il est possible de calculer efficacement des morphismes de groupes entre certaines courbes ou des extensions de leurs corps finis de base. Cela peut avoir des applications cryptanalytiques (ramener le logarithme discret sur la courbe à celui sur un groupe plus facile). Cela fournit aussi de nouvelles applications cryptographiques, comme un échange de clefs Diffie-Hellman à trois protagonistes [43] ou le chiffrement basé sur l'identité [5].

1.3.3 Polynômes tordus

L'étude de cette instanciation fait l'objet d'un chapitre entier, 7. Essentiellement, nous montrerons que les systèmes Diffie-Hellman instanciés sur ces objets sont vulnérables à une attaque polynomiale : le problème de décomposition n'est en fait pas difficile.

1.3.4 Groupes de tresses

Un exemple connu de cryptosytème type Diffie-Hellman basé sur une structure de groupe non commutatif est celui des groupes de tresses [46]. Ces groupes forment une généralisation du groupe de permutation S_n : un élément du groupe de n tresses est un ensemble de transpositions d'indices consécutifs, de sorte que toute transposition σ_i correspond au croisement (ordonné) des deux tresses d'indices i et $i+1$ (on peut croiser plusieurs fois les mêmes tresses successivement dans le même sens), σ_i^{-1} correspond au croisement (ordonné) des deux tresses d'indice $i+1$ et i. Les transpositions d'indices consécutifs vérifient sinon les mêmes axiomes que dans S_n, ce qui nous donne une présentation du groupe de n tresses :

$$B_n = \langle \sigma_1, \ldots, \sigma_{n-1} | \forall i \in [\![1, n-2]\!]\ \sigma_i\sigma_{i+1}\sigma_i = \sigma_{i+1}\sigma_i\sigma_{i+1}$$

$$\text{et } \forall i \in [\![1, n-1]\!]\ \forall j \neq i \pm 1\ \sigma_i\sigma_j = \sigma_j\sigma_i \rangle$$

Il existe un morphisme surjectif (une projection) évident de B_n sur S_n, qui consiste à quotienter par la relation $\sigma_i^2 = 1$ et donc à poser $\sigma_i = \sigma_i^{-1}$.

Pour l'implémentation de protocoles Diffie-Hellman sur les groupes de tresses, plutôt que des paires d'éléments distincts dans un sous-semigroupe commutatif $\mathcal{S}$, on considère plutôt des paires de la forme $\{u, u^{-1}\}$ et on forme l'élément $u \diamond z \diamond u^{-1}$. Le problème de décomposition associé est un problème de *conjugaison*.

Un algorithme polynomial spécifique [19] résout le problème de conjugaison Diffie-Hellman dans les groupes de tresses. Toutefois il est loin d'être pratique : sur n tresses et des séquences de longueur l, la complexité est en $\mathcal{O}(n^{14,4}l^3)$.

1.4 Sécurité prouvable

1.4.1 Preuves de sécurité, modèles

Une fois la sécurité d'une primitive cryptographique raisonnablement estimée par l'étude tant théorique que pratique des algorithmes de résolution du problème difficile sous-jacent, on veut pouvoir l'utiliser dans un protocole plus élaboré. Par exemple, si le problème Diffie-Hellman est largement étudié et difficile sur certains groupes bien connus (*cf* ci-dessus 1.3), il faut encore que la sécurité du cryptosystème qui repose dessus se ramène vraiment à la complexité des algorithmes de résolution du problème Diffie-Hellman. En particulier, il ne faut pas qu'il soit possible de contourner ce problème, mieux encore il doit exister une démonstration mathématique appelée *preuve de sécurité* que la sécurité du cryptosystème est équivalente à celle du problème difficile sous-jacent.

Exemple : chiffrement El-Gamal dans un groupe cyclique $\mathcal{G}$ de cardinal q et de générateur g.

Génération des clefs Alice choisit un entier aléatoire $x \in \{1, \ldots, q\}$ et calcule $h = g^x$. Sa clef publique est l'élément h, sa clef privée est l'entier x.

Chiffrement Bob veut chiffrer le message m, considéré comme un élément de $\mathcal{G}$ pour Alice. Il choisir un élément $y \in \{1, \ldots, q\}$ et calcule $c = g^y$ et un secret partagé $s = h^y$. Il calcule $c' = m \cdot s$ et envoie $(c, c') = (g^y, m \cdot h^y)$ sur le canal public pour Alice.

Déchiffrement Alice reçoit (c, c') construit comme $(g^y, m \cdot h^y) = (g^y, m \cdot (g^x)^y)$. Utilisant sa clef secrète x, elle calcule le secret partagé h comme c^x et peut alors retrouver $m = c'/c^x$.

Si Bob utilise toujours le même aléa y, Ève a beau ne pas pouvoir calculer le secret commun $h = (g^x)^y = (g^y)^x$, elle peut retrouver de l'information sur des messages : si Bob a envoyé deux messages m_1 et m_2 chiffrés comme (c_1, c'_1) et (c_2, c'_2) (avec $c_1 = c_2$) à Alice, Ève peut retrouver le quotient $m_1/m_2 = c'_1/c'_2$.

Inversement, si Bob utilise un entier y choisi aléatoirement pour chaque message, alors il est possible de prouver que Ève ne peut pas récupérer d'information sur les

messages clairs à partir des messages chiffrés en un certain sens : dans un *modèle* où Ève fait chiffrer à Bob des messages de son choix, on peut montrer que si elle sait faire la différence entre le message qu'elle a demandé à Bob de chiffrer et un message alétoire que Bob aurait chiffré, alors elle sait résoudre le problème Diffie-Hellman décisionnel.

D'autres attaques dépendent de la manière dont les chaînes de caractères sont *encodées* en éléments m de $\mathcal{G}$ afin qu'elles puissent être chiffrées. Les constructions naïves sont généralement non sécurisées (*cf* [6]). C'est à ces encodages que nous nous sommes intéressés dans cette thèse, dans le cas des courbes algébriques.

1.4.2 Oracle aléatoire

Toute preuve de sécurité dépend bien sûr du modèle choisi. Il faut tout d'abord modéliser l'attaquant : plus il sera puissant, plus un cryptosystème prouvé sûr dans ce modèle inspirera confiance. Selon les cas, il peut s'agir d'un adversaire disposant d'une capacité de calcul illimitée (preuves de sécurité type *théorie de l'information* : aucune information ne peut être apprise par un adversaire sur les messages) ou non (notamment en cryptologie à clef publique, où la clef publique contient toute l'information nécessaire au calcul de la clef privée, la sécurité dépendant de la complexité de ce calcul), il est capable de soumettre des messages à la fois à chiffrer et à déchiffrer ou seulement à chiffrer, on quantifie sa capacité à faire des requêtes à des opérateurs tiers...

Il faut ensuite modéliser certaines primitives. Dans le cas des fonctions de hachage et en particulier vers les courbes algébriques, un modèle commode est celui de l'*oracle aléatoire* : dans ce modèle, une fonction de hachage considérée comme sûre est remplacée par une fonction aléatoire publiquement accessible. L'adversaire ne peut pas calculer lui-même cette fonction, il n'a aucune prise dessus, il peut simplement faire des requêtes à l'oracle aléatoire pour connaître les valeurs qu'il prend.

Une preuve de sécurité n'est pas tout à fait satisfaisante dans ce modèle, vu qu'elle ne signifie pas que le cryptosystème est sûr lorsqu'on remplace l'oracle aléatoire par une fonction de hachage réelle. Il est en effet possible de construire des schémas artificiels *ad-hoc* prouvés sûrs dans le modèle de l'oracle aléatoire, mais dans lesquels toute instanciation de l'oracle par une fonction de hachage réelle le rend aisément attaquable [15]. Néanmoins, une preuve de sécurité dans ce modèle indique qu'il n'y a pas de problème structurel avec la contruction proposée.

Les fonctions de hachage vers des chaînes de bits sont un domaine bien étudié de la cryptologie symétrique, et de nombreuses fonctions sont éprouvées et reconnues. Il est plutôt facile d'en déduire des fonctions de hachage vers les corps finis.

1.4.3 Indifférentiabilité

L'indifférentiabilité est la notion qui quantifie la perte de sécurité quand on remplace un oracle aléatoire par une autre construction. Essentiellement, si les distributions statistiques des sorties de l'oracle aléatoire et de la construction (qui en utilise un autre) ne sont pas distingables avec une complexité polynomiale en temps de calcul et requêtes à l'oracle ou à la construction, on dit que l'oracle et la construction sont indifférentiables.

Définition 1.4.1 (Indifférentiabilité, [53]) *Une machine de Turing C_h avec accès à un oracle aléatoire h est dite $(t_D, t_S, q_D, \varepsilon)$-indifférentiable d'un oracle aléatoire H s'il existe un simulateur S_H avec accès à H, de complexité au plus t_S tel que pour tout distingueur D de complexité t_D et faisant au plus q_D requêtes, la probabilité que D distingue s'il interagit avec C_h de s'il interagit avec S_H est inférieure à ε.*

On dit que C_h est indifférentiable de H si ε est une fonction négligeable du paramètre de sécurité si q_D, t_D et t_S sont des fonctions polynomiales en k.

Cette notion est utilisée pour construire une fonction indifférentiable d'un oracle aléatoire vers les courbes à partir d'un oracle aléatoire vers les corps finis : il s'agira de remplacer une primitive idéale (oracle aléatoire vers les courbes) par une construction basée sur des oracles aléatoires vers les corps finis et des fonctions d'encodage. L'indifférentiabilité signifie qu'il est impossible pour un adversaire disposant d'une capacité de calcul polynomiale de distinguer la distribution statistique des résultats d'appels à la construction sur des messages de son choix de celle de points aléatoires sur la courbe.

Chapitre 2

Préliminaires : courbes

Dans ce chapitre, nous revoyons quelques propriétés des courbes et la construction des courbes elliptiques en tant que groupe commutatif. Cette présentation est basée sur [20], chapitre 4.

2.1 Variétés algébriques

Soit $\mathbb{K}$ un corps parfait, $\bar{\mathbb{K}}$ une clôture algébrique de $\mathbb{K}$ et $X_0, X_1, \ldots, X_n$ $n+1$ indéterminées. On note $\mathbb{A}^n$ l'espace affine de dimension n sur $\bar{\mathbb{K}}$ (c'est la variété associée à l'idéal (0) d'après la définition ci-dessous) et $\mathbb{P}^n$ l'espace projectif de dimension n sur $\bar{\mathbb{K}}$.

2.1.1 Définitions

Définition 2.1.1 *Soit I un idéal de $\mathbb{K}[X_1, \ldots, X_n]$ (resp. engendré par des polynômes homogènes). L'ensemble V des points $x = (x_1, \ldots, x_n) \in \mathbb{A}^n$ (resp. points $x = (x_0 : \cdots : x_n)$ de l'espace projectif $\mathbb{P}^n$) tels que $\forall P \in I \ P(x) = 0$ est appelé* ensemble algébrique.

Si I est premier, on dit que V est irréductible. *On dit alors que V est une* variété *affine (resp. projective).*

On dit que V est défini sur $\mathbb{K}$.

Remarque : Avec cette définition, un idéal et son radical engendrent la même variété. Dans la suite, on peut donc ne considérer que des idéaux radicaux.

Définition 2.1.2 *Soit V une variété affine sur $\mathbb{K}$ et I l'idéal premier de $\mathbb{K}[X_1, \ldots, X_n]$ correspondant.*

*L'*anneau de coordonnées *de V, noté $\mathbb{K}[V]$, est le quotient de $\mathbb{K}[X_1, \ldots, X_n]$ par I.*

Le corps de fonctions *de V, noté $\mathbb{K}(V)$, est le corps des fractions de $\mathbb{K}[V]$.*

Cette définition n'est valable que pour une variété affine. Pour une variété projective, il nous faut définir sa déshomogénéisée.

2.1.2 Homogénéisation, déshomogénéisation

Nous rappelons ici qu'il est possible de faire un lien entre variétés affines et variétés projectives.

Soit ϕ_i : $\begin{array}{ccc} \mathbb{A}^n & \to & \mathbb{P}^n \\ (x_1, \ldots, x_n) & \mapsto & (x_1 : x_2 : \cdots : x_{i-1} : 1 : x_i : \cdots : x_n) \end{array}$.

ϕ_i est une inclusion de $\mathbb{A}^n$ dans $\mathbb{P}^n$, bijective vers sa corestriction à l'ensemble U_i des éléments $(x_0 : \cdots : x_n) \in \mathbb{P}^n$ de i-ième coordonnée non nulle. On peut donc identifier U_i et $\mathbb{A}^n$.

Déshomogénéisation

Soit V un ensemble algébrique projectif et $I(V) \in \bar{\mathbb{K}}[X_0, \ldots, X_n]$ l'idéal homogène associé. Alors $V \cap U_i$ est un ensemble algébrique affine dont l'idéal $I(V \cap U_i)$ associé est

$$\{f(X_0, \ldots, X_{i-1}, 1, X_{i+1}, \ldots, X_n) | f \in I(V)\} \subset \bar{\mathbb{K}}[X_0, \ldots, X_{i-1}, X_{i+1}, \ldots, X_n].$$

Homogénéisation

L'homogénéisation consiste à effectuer le processus inverse : soit $f \in \bar{\mathbb{K}}[X_1, \ldots, X_n]$ de degré d, et $f_i^*(X_0, \ldots, X_n) = X_i^d f(X_0/X_i, \ldots, X_{i-1}/X_i, X_{i+1}/X_i, \ldots, X_n/X_i)$. Alors f_i^* est un polynôme homogène à $n+1$ indéterminées. On dit que f_i^* est l'homogénéisation de f par rapport à X_i.

Ainsi, on peut définie la clôture projective d'une variété affine :

Définition 2.1.3 *Soit V un ensemble algébrique affine d'idéal associé $I(V)$. Considérons V comme un sous-ensemble de $\mathbb{P}^n$ par ϕ_i.*

La clôture projective *de V est l'ensemble algébrique projectif d'idéal homogène associé généré par $\{f_i^*(X_0, \ldots, X_n) | f \in I(V)\}$.*

C'est une variété projective.

Ce processus permet d'associer une unique variété projective à une variété affine.

La proposition suivante fait le lien entre homogénéisée et déshomongénéisée :

Proposition 2.1.4 ([67], proposition 2.6) *Soit V une variété projective. Alors soit $V \cap U_i$ est vide, soit V est la clôture projective de $V \cap U_i$.*

Remarque : à une variété projective non vide contenant un point P, on peut toujours associer une variété affine non vide par déshomogénéisation : il suffit de déshomogénéiser selon une coordonnée non nulle de P.

On peut donc étudier les propriétés des variétés projectives en considérant en fait leurs déshomogénéisées.

En particulier, le corps de fonctions d'une variété projective peut être défini comme celui d'une de ses déshomogénéisées non vide : deux déshomogénéisées non vides ont des corps de fonctions isomorphes (*cf.* [67]) [1].

2.1.3 Dimension

Définition 2.1.5 *Soit V une variété définie sur $\mathbb{K}$. La* dimension *de V est le degré de transcendance de $\mathbb{K}(V)$.*

Exemple : soit $P(X_1, X_2)$ un polynôme défini sur $\mathbb{F}_q$ et irréductible sur $\bar{\mathbb{F}}_q$. L'ensemble des points qui annulent P est une courbe. Le corps de fonctions de la courbe est le corps des fractions de l'anneau de coordonnées $\mathbb{F}_q[X_1, X_2]/(P)$. P lie algébriquement les deux indéterminées X_1 et X_2 et le degré de transcendance du corps de fonctions est 1.

Une courbe algébrique est une variété projective (donc irréductible) de dimension 1. Une surface est une variété de dimension 2. Dans le cas des courbes, on notera X l'élément transcendant de $\mathbb{K}(V)$. Ainsi, $\mathbb{K}(V)$ contient le corps $\mathbb{K}(X)$ des fractions rationnelles en X.

2.2 Courbes

Dans cette section, nous définissons le genre géométrique d'une courbe. Cette section est basée sur [69].

Soit $\mathcal{C}$ une courbe définie sur $\mathbb{K}$ et $\mathbb{K}(\mathcal{C})$ son corps de fonctions associé.

2.2.1 Places

On rappelle qu'un anneau de valuation d'un corps de fonctions $\mathbb{K}(\mathcal{C})$ est un anneau $\mathcal{O}$ qui vérifie les deux propriétés suivantes :

- $\mathbb{K} \subset \mathcal{O} \subset \mathbb{K}(\mathcal{C})$
- $\forall x \in \mathbb{K}(\mathcal{C})$ $x \in \mathcal{O}$ ou $x^{-1} \in \mathcal{O}$.

1. Sans passer par le processus de déshomogénéisation, on peut toutefois le définir à l'aide de fonctions rationnelles dont les numérateurs et dénominateurs sont homogènes et de même degré et en quotientant par I (*cf* [67], I.2.9).

Définition 2.2.1 *Une* place P *de* $\mathbb{K}(\mathcal{C})$ *est l'idéal maximal d'un (sous-)anneau de valuation* $\mathcal{O}_P$ *de* $\mathbb{K}(\mathcal{C})$.

Le degré *de* P *est celui de l'extension* $\mathcal{O}_P/P$ *sur* $\mathbb{K}(\mathcal{C})]$. *Il est toujours fini.*

Si le corps $\mathbb{K}$ est algébriquement clos, alors on peut interpréter les fonctions $f \in \mathbb{K}(\mathcal{C})$ comme des fonctions à valeur dans $\mathbb{K} \cup \{\infty\}$ qui s'évaluent sur la courbe $\mathcal{C}$. Grâce à la valuation de l'anneau de valuation, on peut définir la valuation $v_P(f)$ d'une fonction f en une place P. Dans le cas où $\mathbb{K}(\mathcal{C}) = \mathbb{K}(X)$ (c'est-à-dire si $\mathbb{K}(\mathcal{C})$ est de dimension 1), les places correspondent aux polynômes irréductibles de $\mathbb{K}[X]$, *cf* [69].

Cette définition cache le modèle, c'est-à-dire l'équation, qu'il serait possible de choisir pour la courbe : elle ne s'intéresse qu'à ses propriétés algébriques. En particulier, la notion d'anneau de valuation évite les problèmes qui pourraient être posés par les singularités. Ces sous-anneaux existent toujours ([69], corollaire 1.1.20).

2.2.2 Diviseurs

Définition

On peut maintenant définir un diviseur :

Définition 2.2.2 *Le groupe des diviseurs de* $\mathbb{K}(\mathcal{C})$ *est le groupe libre engendré par les places de* $\mathbb{K}(\mathcal{C})$. *On le note* $\mathrm{Div}(\mathcal{C})$.

On note ce groupe additivement : soit $A \in \mathrm{Div}(\mathcal{C})$, *on notera*

$$A = \sum_P n_P P$$

où presque tous les coefficient n_P *sont nuls.*

Le support *d'un diviseur* A *est l'ensemble des places* P *telles que* $n_P \neq 0$.

Le degré *d'un diviseur* A *est* $\deg(A) = \sum_P v_P \deg(P)$.

On définit un ordre partiel sur les diviseurs : avec des notations évidentes,

$$A \leqslant A' \Longleftrightarrow \forall P \; n_P \leqslant n'_P.$$

Une fois les places munies d'une valuation, on peut définir le diviseur associé à une fonction : si $f \in \mathbb{K}(\mathcal{C})$ est une fonction non nulle, $\mathrm{div}(f) = \sum_P v_P(f)P$. Il est naturel d'étudier l'ensemble des fonctions dont le diviseur associé est supérieur à un autre :

Définition 2.2.3 (Espace de Riemann-Roch) *Soit* $A \in \mathrm{Div}(\mathcal{C})$ *un diviseur. L'espace de Riemann-Roch associé à* A *est le* $\mathbb{K}$*-espace vectoriel des fonctions suivant :*

$$\mathcal{L}(A) = \{f \in \mathbb{K}(\mathcal{C})^* | \mathrm{Div}(f) \geqslant -A\} \cup \{0\}.$$

On note sa dimension $l(A)$.

Si $A = \sum_P n_P P$, l'espace est celui des fonctions qui ont un zéro en P d'ordre supérieur ou égal à $-n_P$ si $n_P < 0$ et ne peuvent avoir de pôles qu'en les places P telles que $n_P > 0$, d'ordre borné par n_P.

Diviseurs principaux, jacobienne

Définition 2.2.4 *Le groupe $\mathcal{P}_\mathcal{C} = \{Div(f) | f \in \mathbb{K}(\mathcal{C})\}$ des diviseurs associés aux fonctions est appelé le* groupe des diviseurs principaux *de $\mathbb{K}(\mathcal{C})$.*

On peut montrer qu'en fait toute fonction a autant de zéros que de pôles :

Théorème 2.2.5 ([69], Théorème 1.4.11) *Tout diviseur principal est de degré 0.*

$\mathcal{P}_\mathcal{C}$ est donc un sous-groupe du sous-groupe des diviseurs de degré 0. Il est alors naturel de considérer le quotient suivant :

Définition 2.2.6 (Jacobienne) *La* jacobienne *(ou* groupe de Picard*) de $\mathcal{C}$, notée $\mathrm{Pic}^0_\mathcal{C}$, est le quotient du groupe $\mathrm{Div}^0_\mathcal{C}$ des diviseurs de degré 0 par le groupe des diviseurs principaux $\mathcal{P}_\mathcal{C}$.*

Bien que $\mathcal{P}_\mathcal{C}$ et $\mathrm{Div}^0_\mathcal{C}$ soient infinis, comme $\mathbb{K}$ est un corps fini, $\mathrm{Pic}^0_\mathcal{C}$ est fini. C'est le groupe dans lequel nous voulons réaliser des opérations de cryptographie asymétrique fondées sur le problème du logarithme discret. Ce groupe a une structure de groupe *algébrique* : il s'agit également d'une variété, on peut donc représenter les éléments de $\mathrm{Pic}^0_\mathcal{C}$ par des points (affines ou projectifs) et la loi de groupe s'exprime par des formules algébriques explicites (rationnelles dans le cas affine, polynomiales en représentation projective) sur leurs coordonnées, qui fait l'objet d'un domaine de recherche en entier (cf [20]). La dimension de $\mathrm{Pic}^0_\mathcal{C}$ en tant que variété algébrique, qui mesure le nombre de coordonnées de ses points et donc l'efficacité des opérations de groupe, est donnée par le genre de la courbe que nous étudions donc ci-dessous.

Nous illustrerons cette construction de la loi de groupe dans le cas des courbes elliptiques ci-dessous, à la section 2.3.

2.2.3 Genre géométrique

La notion de genre est basée sur la proposition suivante :

Proposition 2.2.7 ([69], 1.4.14) *Il existe une constante $\gamma \in \mathbb{Z}$ telle que pour tout diviseur $A \in \mathrm{Div}(\mathcal{C})$, on ait l'inégalité suivante :*

$$\deg A - l(A) \leqslant \gamma.$$

Cela signifie qu'il ne peut pas y avoir beaucoup d'écart entre le degré d'un diviseur et la dimension de l'espace de fonctions de Riemann-Roch associé. Cet écart est mesuré par le genre géométrique :

Définition 2.2.8 *Le* genre géométrique g *de* $\mathcal{C}$ *est défini par :*

$$g = \max\{\deg A - l(A) + 1 | A \in \mathrm{Div}(\mathcal{C})\}.$$

C'est un invariant *algébrique* de la courbe $\mathcal{C}$: si elle est donnée par un modèle particulier, toutes les courbes birationnellement équivalentes à $\mathcal{C}$ seront de même genre. Il mesure en quelque sorte la complexité de la courbe.

Exemple : une droite ou une conique sont des courbes de genre 0. Une courbe elliptique (*cf* ci-dessous section 2.3) est une courbe de genre 1.

2.2.4 Genre arithmétique

Nous donnons ici une définition simple du genre arithmétique d'une *courbe* plane projective. Il se calcule à partir du degré :

Définition 2.2.9 *Soit* $\mathcal{C}$ *une courbe sur* $\mathbb{P}^2(\mathbb{K})$ *de degré* d*. Le* genre arithmétique *de* $\mathcal{C}$ *est* $(d-1)(d-2)/2$*.*

2.2.5 Lien avec les singularités

Le théorème suivant relie les deux notions de genre avec les singularités de la courbe. Il montre qu'elles coïncident pour les courbes lisses.

Théorème 2.2.10 ([32], Chapitre 8, Proposition 5) *Soit* $\mathcal{C}$ *une courbe plane de genre (géométrique)* g *sur un corps* $\mathbb{K}$ *et de degré* d*. Soit* s *le nombre de singularités de* $\mathcal{C}$*, comptées avec multiplicité.*

Alors $g = (d-1)(d-2)/2 - s$*.*

En particulier, une courbe cubique a donc au plus une singularité simple.

2.2.6 Formule de Hurwitz

Bien que nous ne nous en servions pas directement, nous ne pouvons pas, à ce point, ne pas citer la formule de Hurwitz. Quand on a affaire à une courbe lisse (*cf* la définition 2.3.1 ci-dessous), cette formule permet d'en en calculer le genre grâce à un morphisme $\mathcal{C} \longrightarrow \mathbb{P}^1(\mathbb{K})$.

Théorème 2.2.11 *Soient $\mathcal{C}$ et $\mathcal{C}'$ deux courbes lisses sur $\bar{\mathbb{K}}$ de genres g et g' respectivement. Soit $F : \mathcal{C} \longrightarrow \mathcal{C}'$ un morphisme. Alors*

$$2g - 2 = \deg(F)(2g' - 2) + \sum_{P \in \mathcal{C}} (\mathrm{mult}_P(F) - 1).$$

2.3 Courbes elliptiques

Cette section est largement inspirée de [67], chapitre III.

2.3.1 Définitions

Il nous faut d'abord définir ce qu'est un point singulier d'une variété.

Définition 2.3.1 ([67], I.1.5) *Soit V une variété, $P \in V$ un point, et $f_1, \ldots, f_m \in \bar{\mathbb{K}}[X_1, \ldots, X_n]$ un ensemble de générateurs pour l'idéal $I(V)$ associé à V.*

Alors V est non singulière *(ou* lisse*) en P si la matrice $m \times n$ des dérivées partielles $\left(\partial f_i / \partial X_j(P)\right)_{1 \leqslant i \leqslant m, 1 \leqslant j \leqslant n}$ est de rang $n - \dim(V)$.*

Si V est non singulière en tous ses points, on dit que V est non singulière (ou lisse).

Définition 2.3.2 *Une courbe elliptique $\mathcal{E}$ définie sur un corps $\mathbb{K}$ est une courbe non singulière de genre 1 possédant un point $\mathbb{K}$-rationnel O fixé.*

Remarque : Si $\mathcal{E}$ est le couple $(\mathcal{C}, O)$, et si $\mathcal{C}$ contient un autre point K-rationnel O', alors $(\mathcal{C}, O')$ et $\mathcal{E}$ sont deux courbes elliptiques dont la loi d'addition (*cf* ci-dessous) sont différentes. Elles sont isomorphes.

2.3.2 Modèles de courbes elliptiques

Nous voulons maintenant définir un *modèle* pour $\mathcal{E}$, c'est-à-dire une équation pour la définir.

Proposition 2.3.3 ([67], chapitre III proposition 3.1) *Soit $\mathcal{E}$ une courbe elliptique définie sur $\mathbb{K}$, O son point $\mathbb{K}$-rationnel particulier et $\mathbb{K}(\mathcal{E})$ son corps de fonctions.*

Il existe deux fonctions $x, y \in \mathbb{K}(\mathcal{E})$ telles que la fonction :

$$\phi : \mathcal{E} \to \mathbb{P}^2(\mathbb{K}), \phi = (x : y : 1)$$

soit un isomorphisme de $\mathcal{E}(\mathbb{K})$ sur une courbe définie par l'équation (dite de Weierstrass*) suivante :*

$$Y^2 + a_1XY + a_3 = X^3 + a_2X^2 + a_4X + a_6$$

avec $a_i \in \mathbb{K}$ *et* $\phi(O) = (0:1:0)$.

On peut donc supposer qu'une courbe elliptique est donnée par une équation de Weierstrass et le point $(0:1:0)$ qui est appelé *point à l'infini*.

Démonstration Considérons les espaces de Riemann-Roch $\mathcal{L}(nO)$ associés aux diviseurs nO pour $n \in \mathbb{N}^*$.

D'après le théorème de Riemann-Roch (*cf.* [69], théorème I.5.15), comme le genre de $\mathcal{E}$ est 1, $\dim\big(\mathcal{L}(nO)\big) = l(nO) = n$ pour tout n.

Ainsi, $\mathcal{L}(2O)$ est de dimension 2. Il contient les constantes et une fonction notée x ayant un pôle d'ordre 2 en O. $\mathcal{L}(3O)$ contient les fonctions ayant au plus un pôle d'ordre 3 en O et est de dimension 3, il contient au moins $1, x$ et une autre fonction y ayant un pôle d'ordre 3 en O, donc linéairement indépendante de x.

$\mathcal{L}(6O)$ est de dimension 6 et contient les fonctions ayant un pôle d'ordre au plus 6 en O. Il contient notamment : $1, x, y, x^2, xy, y^2, x^3$. Ces sept fonctions sont donc liées par une relation linéaire non triviale sur $\mathbb{K}$:

$$A_1 + A_2x + A_3y + A_4x^2 + A_5xy + A_6y^2 + A_7x^3 = 0.$$

Nécessairement $A_6A_7 \neq 0$. En effet, si A_6 ou A_7 était nul, alors toutes les fonctions intervenant dans la relation linéaire auraient un pôle en O d'ordres deux à deux distincts et tous les coefficients A_i seraient nuls.

L'équation s'obtient alors en posant $X = -A_6A_7x$ et $Y = A_6A_7^2y$. □

2.3.3 Propriété des équations de Weierstrass

Si la caractéristique de $\mathbb{K}$ est différente de 2 et de 3, on peut simplifier l'équation de Weierstrass $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ en l'équation réduite

$$y^2 = x^3 - 27c_4x - 54c_6. \tag{2.1}$$

Le discriminant Δ du membre de droite de cette équation est $1728\Delta = c_4^3 - c_6^2$. Il permet de connaître les singularités de la courbe associée à l'équation de Weierstrass. On définit également le j-invariant de l'équation par $j = c_4^3/\Delta$. Ces deux notions se généralisent également au cas où la caractéristique de $\mathbb{K}$ est 2 ou 3, nous renvoyons à [67] pour les calculs explicites.

Proposition 2.3.4 ([67], III.1.4) *La courbe* $\mathcal{E}$ *associée à l'équation de Weierstrass réduite* (2.1) *est non singulière si et seulement si* $\Delta \neq 0$.

Si $\Delta = 0$, *il n'existe qu'un unique point singulier.*

Deux courbes elliptiques sont isomorphes sur $\bar{\mathbb{K}}$ *si et seulement si elles ont le même* j*-invariant.*

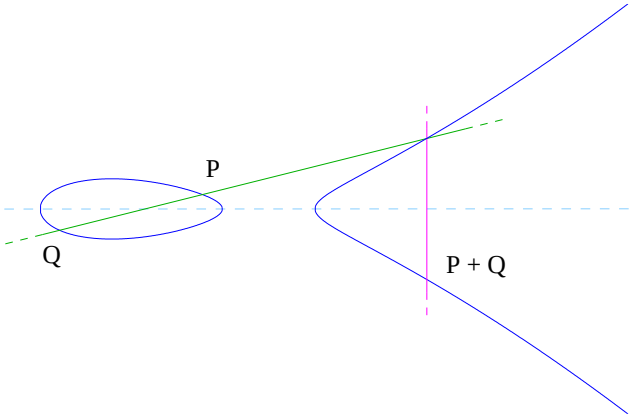

FIGURE 2.1 – Loi d'addition sur une courbe elliptique

Ainsi, d'après le théorème 2.2.10, toute cubique de Weierstrass est de genre 1 si son discriminant est non nul.

2.3.4 Loi de groupe

On peut maintenant donner une explication géométrique simple de la loi de groupe d'une courbe elliptique telle que définie à la section 2.2.2

Proposition 2.3.5 (Loi de groupe sur une courbe elliptique, [67] III.3.4) *Soit $\mathcal{E}$ une courbe de Weierstrass et O son point à l'infini.*

Pour tout diviseur D de degré 0 sur $\mathcal{E}$, il existe un unique point P sur $\mathcal{E}$ tel que $D \equiv P - O$.

La fonction σ qui à tout diviseur de degré 0 sur $\mathcal{E}$ associe le point P correspondant induit une loi de groupe sur E.

L'interprétation géométrique de cette définition plutôt algébrique est donnée à la figure 2.1 : il s'agit de la construction corde-tangente. Partant de deux points P et Q avec $Q \neq -P$, la droite passant par P et Q coupe $\mathcal{E}$ en $-(P+Q)$.

2.3.5 Isogénies

Entre deux courbes elliptiques, une isogénie est un morphisme de groupe non trivial qui est également un morphisme de variétés algébriques. Le théorème suivant permet de décomposer un morphisme de variétés entre deux courbes :

Théorème 2.3.6 *Soient $\mathcal{E}$, $\mathcal{E}'$ deux courbes elliptiques avec point à l'infini O et O'.*

Un morphisme de variétés non trivial $f : \mathcal{E} \longrightarrow \mathcal{E}'$ est une isogénie si et seulement si $f(O) = f(O')$.

On en déduit le corollaire suivant, qui fait le lien entre morphismes de variétés et isogénies entre deux courbes elliptiques :

Corollaire 2.3.7 *Un morphisme de variétés non trivial entre deux courbes elliptiques est la composition d'une isogénie par une translation dans le groupe des points.*

En particulier, pour les applications cryptographiques, un morphisme de variétés permet de transporter des relations entre logarithmes discrets d'une courbe à une autre.

2.3.6 Isomorphismes et tordues

Pour évaluer la difficulté du problème du logarithme discret sur les courbes elliptiques, il convient tout d'abord d'étudier les courbes isomorphes à $\mathcal{E}$ *sur* $\bar{\mathbb{K}}$. Sur un corps quelconque, celles-ci n'ont pas nécessairement de point $\mathbb{K}$-rationnel.

Définition 2.3.8 *Soit $\mathcal{E}$ une courbe projective lisse sur $\mathbb{K}$. Une* tordue *(en anglais, twist) de $\mathcal{E}$ est une courbe $\mathcal{E}'$ isomorphe à $\mathcal{E}$ sur $\bar{\mathbb{K}}$.*

Exemple : tordues quadratiques. On suppose que $\mathbb{K}$ est de caractéristique différente de 2. Soit $\mathcal{E}$ une courbe elliptique sur $\mathbb{K}$ d'équation $y^2 = x^3 + a_2x^2 + a_4x + a_6$. Étant donné $d \in \mathbb{K} \setminus \mathbb{K}^2$ non nul, la tordue quadratique de $\mathcal{E}$ est la courbe $\mathcal{E}'$ d'équation $dy^2 = x^3+a_2x^2+a_4x+a_6$, ou de façon équivalente $y^2 = x^3+da_2x^2+d^2a_4x+d^3a_6$. Les courbes $\mathcal{E}$ et $\mathcal{E}'$ ne sont pas isomorphes sur $\mathbb{K}$ mais sur l'extension $\mathbb{K}(\sqrt{d})$.

Si $\mathbb{K} = \mathbb{F}_q$ est le corps fini à q éléments, alors pour tout x il existe un y tel que (x, y) est soit sur $\mathcal{E}$ soit sur $\mathcal{E}'$. On en déduit que $\#\mathcal{E} + \#\mathcal{E}' = 2q + 2$

Dans le cas des corps finis, le théorème suivant classifie les tordues d'une courbe elliptique :

Théorème 2.3.9 *Si $\mathcal{E}$ est une courbe elliptique définie sur $\mathbb{F}_q$ où q est premier avec 6, de j-invariant différent de 0 et 1728, alors la seule tordue de $\mathcal{E}$ est sa tordue quadratique.*

Si le j-invariant de $\mathcal{E}$ est 1728, alors $\mathcal{E}$ a 4 tordues.

Si le j-invariant de $\mathcal{E}$ est nul, alors $\mathcal{E}$ a 6 tordues.

Deuxième partie

Aspects constructifs : hachage vers courbes algébriques

Les jacobiennes de courbes algébriques et au premier rang d'entre elles les courbes elliptiques sont maintenant très étudiées pour réaliser des opérations de cryptographie à clef publique. Alors qu'elles sont faciles sur les corps finis, certaines opérations sont difficiles à réaliser de manière efficace sur les courbes. Générer un élément aléatoire du groupe en est un bon exemple : dans le cas des courbes, les algorithmes classiques pour ce problème sont soit assez peu efficaces, soit ne s'exécutent pas en temps constant.

Plus précisément, un algorithme de hachage produit un haché (*digest*) à partir d'un message, c'est-à-dire une chaîne de bits de longueur donnée, unique pour chaque message (*cf* 1.1). En déduire un élément d'un corps fini est facile : sur $\mathbb{F}_p$ par exemple, il suffit de prendre la valeur numérique modulo p. Mais cela ne se généralise pas pour le groupe des points d'une courbe elliptique : on ne peut pas décider de considérer cette valeur numérique comme l'abscisse d'un point vu qu'environ la moitié seulement de ces abscisses sont celles d'un point de la courbe.

Cette opération est néanmoins nécessaire pour de nombreux protocoles cryptographiques. Les propriétés mathématiques des courbes algébriques, en particulier l'existence de couplages, en font l'outil de choix pour instancier un chiffrement basé sur l'identité, où une adresse électronique ou un numéro de téléphone servent de clef publique : il faut alors hacher (ou à tout le moins associer) l'identité en un point de la courbe. Un recensement des applications se trouve dans la thèse d'Icart [39].

Chapitre 3

Hachage vers courbes

Nous nous intéressons au hachage vers des courbes elliptiques et hyperelliptiques. Les fonctions de hachage vers courbes sont utiles pour instancier des protocoles cryptographiques de manière sûre, quand il faut considérer une chaîne de caractères comme un point sur une courbe elliptique ou la jacobienne d'une courbe hyperelliptique. Il peut par exemple s'agir de l'identité d'un utilisateur, qu'il faut transformer en sa clef publique dans un cryptosystème basé sur l'identité.

Dans ce chapitre et le suivant, nous nous plaçons dans le cadre des courbes dans le plan affine sur $\mathbb{F}_q$. Nous présenterons une approche algébrique systématique en détails dans le prochain chapitre 4.

Remarque : nous utilisons indifféremment le terme de *paramétrisation* ou d'*encodage* bien qu'à strictement parler nous ne paramétrisions pas complètement les courbes. Les fonctions proposées sont à tout le moins des paramétrisations impropres puisque leurs images n'atteignent pas toute la courbe et qu'à un point donné correspondent en général plusieurs paramètres.

3.1 Motivation

Le problème de trouver un point sur une courbes algébriques en temps polynomial par un algorithme déterministe a été posé par Koblitz [48] (Section 6.1.8 p 129) : "the main obstacle to a deterministic polynomial-time algorithm for finding a point on $\mathcal{E}$ is not the problem of taking the square root of x^3+ax+b. Rather, it is finding $x \in \mathbb{F}_q$ such that $x^3 + ax + b$ is a square. Although about 50% of the elements x have this property, no efficient deterministic way is known to find such an x except in some special cases". C'est-à-dire que le problème n'est pas tant de calculer des racines carrées que de trouver de manière déterministe un élément x de $\mathbb{F}_q$ tel que l'équation de la courbe soit satisfaite, ce qui revient à trouver x tel qu'un polynôme en x soit un carré dans $\mathbb{F}_q$. En pratique, une fois connu un résidu non quadratique

dans $\mathbb{F}_q$, on peut calculer des racines carrées en temps constant avec l'algorithme de Cipolla. Dans cette partie, nous discutons de différentes méthodes apparues depuis 2005 pour résoudre ce problème.

Au-delà de l'intérêt purement théorique de trouver simplement un point sur une courbe de manière déterministe, on peut vouloir en trouver une proportion importante, en bref trouver une paramétrisation d'une partie importante d'une courbe. Dans de nombreux protocoles cryptographiques en outre, les fonctions de hachage vers les courbes elliptiques interviennent de manière fondamentale, comme par exemple dans le chiffrement fondé sur l'identité [5] ou l'échange de clef authentifié par des mots de passe [12] [42].

En outre, plutôt que de simplement rechercher un algorithme déterministe, nous proposerons des algorithmes à temps constant pour les raisons de sécurité décrites à la section 1.1.2 ci-dessus.

Dans la suite, on considère sauf mention contraire une courbe elliptique $\mathcal{E} : y^2 = x^3 + ax + b$ sur $\mathbb{F}_q$ avec q impair, un point générateur G de $\mathcal{E}$ et une fonction de hachage $h : \{0,1\}^m \to \mathbb{F}_q$.

3.1.1 Cas des courbes de genre 0

Les seules courbes paramétrables *rationnellement*, c'est-à-dire par de simples opérations de corps sans calcul de radicaux sont les courbes de genre 0 [63, Théorème 4.11]. Elles regroupent en particulier les courbes de degré 2 (coniques) et les courbes de degré supérieur avec suffisamment de points de singularité (cf théorème 2.2.10).

Des algorithmes efficaces existent pour trouver des paramétrisations vers ces courbes, le sujet est amplement traité dans [63]. Nous utilisons simplement l'algorithme le plus connu qu'est la paramétrisation "par des droites", qui s'applique dans le cas des coniques ou des courbes de degré supérieur avec un unique point de singularité rationnel.

Cet algorithme fonctionne comme suit (voir figure 3.1) : soit $\mathcal{C}$ une courbe de genre 0 sur $\mathbb{F}_q$ (en rouge sur la figure, une cubique avec un point singulier) et P le point de singularité rationnel de $\mathcal{C}$ (confondu avec l'origine du repère de la figure) ou tout point rationnel de $\mathcal{C}$ s'il s'agit d'une conique. Toute droite passant par P (en vert sur la figure) intersecte $\mathcal{C}$ en un autre point, unique. Cela fournit une paramétrisation de $\mathcal{C}$ en associant à chaque élément t de $\mathbb{F}_q$ le point de coordonnées $(t, 1)$ (droite bleue) et la droite passant par P et ce point.

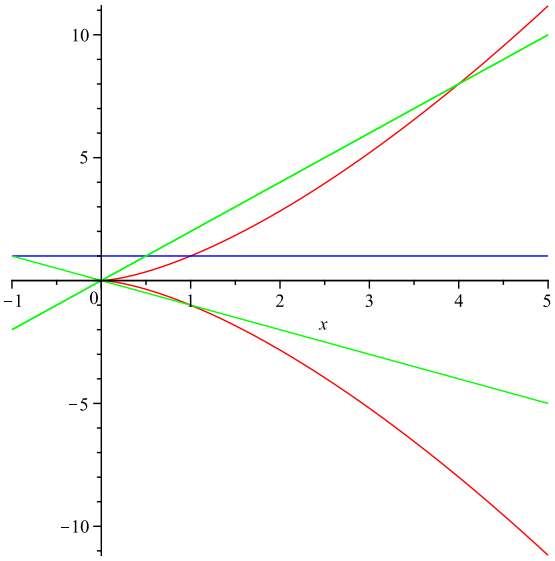

FIGURE 3.1 – Paramétrisation d'une courbe de genre 0

3.1.2 Solutions antérieures

Hachage naïf

Les courbes elliptiques disposant d'une loi de groupe, la solution la plus évidente consiste à prendre un générateur G et hacher un message m par la fonction $m \mapsto [h(m)]G$. Plusieurs problèmes se posent alors. La sécurité des protocoles cryptographiques repose sur la difficulté du calcul des logarithmes discrets, en fait de la relation entre différents logarithmes discrets dans un problème Diffie-Hellman. Ici, les relations entre les logarithmes discrets de différents hachés sont immédiatement connues, et on peut même en déduire d'autres en calculant simplement la fonction de hachage h, publique. Cela pose problème pour les protocoles dont les preuves de sécurité reposent sur l'oracle aléatoire : si h est un oracle aléatoire, cette fonction d'encodage n'est plus un oracle aléatoire vers la courbe. De plus, cela réduit à néant la sécurité des protocoles où les messages à hacher sont connus, notamment dans le cas de signatures [7] où une falsification est facile à construire. Instinctivement, cette fonction de hachage est peu satisfaisante : si on connaît un message, on connaît alors automatiquement le logarithme discret de son haché.

Try and increment

Soit $\mathcal{E}$ une courbe elliptique définie sur $\mathbb{F}_q$ et h une fonction de hachage vers $\mathbb{F}_q$. L'algorithme 3.2 calcule un point haché P sur $\mathcal{E}$.

Cet algorithme présente plusieurs inconvénients. Premièrement, d'un point de vue cryptographique, le plus important est que la sécurité de cet algorithme est

Algorithme 1: Hachage *try and increment*

Entrée : Une courbe elliptique $\mathcal{E}$ définie sur un corps fini $\mathbb{F}_q$, un message m.
Sortie : Un point $(x : y : 1)$ haché de m sur E,

$x := h(m)(\in \mathbb{F}_q)$;
repeat
  $x := x + 1$;
until $x^3 + ax + b$ *est un carré dans* $\mathbb{F}_q$ `/* x est une abscisse valide sur` $\mathcal{E}$ `*/`;
return *Un des deux points de* $\mathcal{E}$ *d'abscisse* x

FIGURE 3.2 – Hachage traditionnel

difficile à analyser : le nombre d'antécédents d'un point par ce hachage est mal connu.

Deuxièmement, l'implémentation telle que décrite ci-dessus ne s'exécute pas en temps constant. Le temps d'exécution de l'algorithme fait fuir de l'information sur la valeur hachée, ce qui est un problème si le message est un secret destiné à être chiffré par la suite. Par exemple il peut s'agir d'un mot de passe, comme dans le protocole PAKE (*Password Authenticated Key Exchange*) [60].

Troisièmement, même si en moyenne il faut deux itérations, implémenter cet algorithme en temps constant force à en faire toujours un (grand) nombre fixé k, ce qui est inefficace. Et cette solution n'est pas non plus satisfaisante : pour un corps fini fixé, les algorithmes efficaces pour vérifier si un élément est un carré ont un temps d'exécution qui dépend de la *valeur* de leurs entrées et non pas seulement de leur taille, à moins de les transformer lourdement. Enfin si on impose un nombre d'itérations maximal, l'algorithme a alors une probabilité d'échec non nulle.

3.1.3 Applications cryptographiques

Nos fonctions proposées ci-dessous répondront aux trois inconvénients de l'algorithme précédent. Tout d'abord, dans les exemples de degré 3 ci-dessous comme dans les familles de genre supérieur des sections 4.3.1 et 4.3.2, nous pourrons toujours borner le nombre d'antécédents de nos fonctions d'encodage : en effet, nous pourrons toujours calculer une relation polynomiale $P_{\underline{a}}(Y, t)$ entre la coordonnée Y d'un point de l'image et son paramètre antécédent t. Le nombre d'antécédents possible est alors borné par le degré en t de $P_{\underline{a}}(Y, t)$. La factorisation de $P_{\underline{a}}(Y, t)$ sur $\mathbb{F}_q$ en donnera le nombre précis.

Ensuite nos algorithmes, déterministes et de complexité polynomiale, s'exécuteront efficacement en temps constant : leur nombre d'opérations sur $\mathbb{F}_q$ ne dépendra pas de la valeur des messages hachés.

3.2 Encodages algébriques sur les courbes elliptiques

3.2.1 Cas supersingulier : construction de Boneh-Franklin

Pour leur schéma de cryptographie fondée sur l'identité [5], Boneh et Franklin ont introduit la paramétrisation suivante, pour les courbes elliptiques *supersingulières* c'est-à-dire de la forme $y^2 = x^3 + b$ sur $\mathbb{F}_q$ avec la condition additionnelle $q \equiv 2 \mod 3$.

Théorème 3.2.1 ([5]) *Soit $\mathbb{F}_q$ le corps fini à q éléments. Supposons q impair et $q \equiv 2 \mod 3$.*

La fonction

$$f : \begin{array}{ccc} \mathbb{F}_q & \longrightarrow & \mathcal{E} : y^2 = x^3 + b \\ t & \mapsto & \left((t^2 - b)^{1/3}, t\right) \end{array}$$

calcule un encodage déterministe bijectif de $\mathbb{F}_q$ vers $\mathcal{E}\backslash\{O\} : y^2 = x^3 + b$, avec complexité $\mathcal{O}(\log^{2+o(1)} q)$.

Cela résout le problème et il n'est même pas besoin d'utiliser la construction générique ci-dessous 3.5.1. Il est intéressant de remarquer que cette construction est quasi-bijective. L'inconvénient est que cet encodage est limité aux courbes supersingulières.

3.2.2 Première approche déterministe : encodage de Shallue et van de Woestijne

Shallue et van de Woestijne [64] ont proposé le premier algorithme déterministe qui construit des points sur une courbe elliptique, rapidement généralisé par Ulas [70] pour certaines classes de courbes hyperelliptiques. Cet encodage repose sur les deux résultats suivants :

Théorème 3.2.2 ([64]) *Soit $\mathbb{F}_q$ un corps fini.*

Il existe un algorithme déterministe à temps polynomial qui, étant donnés a_0, a_1, a_2, b quatre éléments de $\mathbb{F}_q$ tels que $a_0 a_1 a_2 = b^2$, retourne un indice $i \in \{0, 1, 2\}$ tel que a_i est un carré, et une racine de a_i.

Shallue et van de Woestijne appliquent ce résultat à une égalité dont nous donnons ici une version simplifiée par Ulas :

Théorème 3.2.3 ([70]) *Soit $\mathbb{F}_q$ un corps fini et $g(x) = x^3 + ax + b$ avec $a, b \neq 0$. Soit*

$$X_1(t,u) = u,\ X_2(t,u) = \frac{-b}{a}\left(1 + \frac{1}{t^4 g(u)^2 + t^2 g(u)}\right) \text{ et } X_3(t,u) = t^2 g(u) X_2(t,u).$$

Soit $U(t,u) = t^3 g(u)^2 g(X_2(t,u))$.
Alors $U(t,u)^2 = g\big(X_1(t,u)\big) \cdot g\big(X_2(t,u)\big) \cdot g\big(X_3(t,u)\big)$

Ces deux résultats permettent de hacher vers une courbe elliptique : à tout couple (t,u), le théorème 3.2.2 fournit un indice i tel que $g\big(X_i(t,u)\big)$ est un carré et une racine $y_{t,u}$ associée. $(X_i(t,u), y_{t,u})$ est donc un point sur la courbe elliptique d'équation $y^2 = x^3 + ax + b$.

3.2.3 Courbes elliptiques génériques

À CRYPTO 2009, Icart [38] a présenté la construction d'une fonction d'encodage pour les courbes elliptiques ordinaires quand $q \equiv 2 \mod 3$. C'est une généralisation du cas supersingulier proposé par Boneh et Franklin de la section précédente 3.2.1

Théorème 3.2.4 (Encodage d'Icart [38]) *Soit* $\mathcal{E}$ *la courbe elliptique d'équation* $y^2 = x^3 + ax + b$ *sur* $\mathbb{F}_q$. *Supposons* q *impair et* $q \equiv 2 \mod 3$.

La fonction d'encodage $e : t \mapsto (x = (v^2 - b - t^6/27)^{1/3} + t^2/3, y = tx + v)$ *avec* $v = (3a - t^4)/(6t)$ *est un encodage déterministe à temps constant de* $\mathbb{F}_q$ *vers* $\mathcal{E}$.

Pour tout point P *de* $\mathcal{E}$, $\operatorname{card} e^{-1}(P) \leqslant 4$.

3.2.4 Propriétés algébriques, complexité

Hormis l'approche de Shallue et van de Woestijne qui ne fait pas d'hypothèses sur le cardinal du corps fini de base et quelques rares autres, récapitulées ci-dessous dans le tableau 3.1 , un point crucial dans les fonctions d'encodage vers des cubiques est que la fonction $x \mapsto x^3$ doit être bijective sur $\mathbb{F}_q$. C'est le cas quand le cardinal du corps fini q est congru à 2 modulo 3. La fonction inverse est alors $x \mapsto x^e$ où $e \bmod q - 1$ est l'inverse de $3 \bmod q - 1$ et $0 \leq e < q - 1$. L'exponentiation par e se calcule alors complexité polynomiale $(\log q)^{2+o(1)}$ et de manière déterministe à temps constant quelle que soit l'entrée en utilisant des algorithmes d'exponentiation rapide.

De même, au chapitre suivant nous avons besoin de calculer des racines d'ordre supérieur pour construire des fonctions d'encodage vers certaines familles de courbes hyperelliptiques. Nous les calculons de même par exponentiation rapide et nous posons des restrictions similaires sur le cardinal du corps fini de base.

3.3 Encodage vers la jacobienne d'une courbe hyperelliptique

Soit H une courbe hyperelliptique de genre g définie sur un corps fini $\mathbb{F}_q$. Supposons que H admet un modèle imaginaire (c'est-à-dire qu'on peut définir un point

à l'infini P_∞). Nous proposerons dans les sections suivantes 4.2.2, 4.3.2 et 4.3.1 des exemples de courbes hyperelliptiques pour lesquelles il existe des fonctions déterministes e_H qui construisent des points rationnels sur H à partir d'éléments de $\mathbb{F}_q \setminus \mathcal{S}$, où $\mathcal{S}$ est un petit sous-ensemble de $\mathbb{F}_q$ qui dépend de la définition de H. Dans cette section, nous présentons deux méthodes simples pour encoder vers des *diviseurs* dans la jacobienne $\mathcal{J}_H(\mathbb{F}_q)$ de H. Ce problème a aussi été étudié par Farashahi *et al.* [30].

Chaque classe de $\mathcal{J}_H(\mathbb{F}_q)$ peut être représentée de manière unique par un diviseur réduit. Un diviseur D est dit *réduit* quand il est une somme formelle de points $\sum_{i=1}^{r} P_i - rP_\infty$ avec $r \leqslant g$, $P_i \neq -P_j$ pour $i \neq j$ et si cette somme est invariante sous l'action du groupe de Galois $\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$.

Encodage vers des diviseurs 1-friables réduits. Il existe un sous-ensemble particulier, noté $\mathcal{D}_1$, de diviseurs réduits qui sont appelés 1-friables. Ces diviseurs sont ceux qui n'ont que des points rationnels dans leur support. À partir de notre fonction d'encodage e_H, on déduit facilement une fonction vers $\mathcal{D}_1$: en premier on peut produire un ensemble de $r \leqslant g$ points (tels qu'aucun ne soit l'opposé d'un autre), ensuite on en construit un diviseur. Cette première étape peut être faite de manière déterministe en calculant g points avec e_H et en éliminant les collisions possibles après négation. Quand q est assez large, la proportion de $\mathcal{D}_1$ dans $\mathcal{J}_H(\mathbb{F}_q)$ est $\approx 1/(g!)$. De plus, comme e_H n'est pas surjectif, cette fonction n'est pas nécessairement surjective non plus. Si on veut construire des diviseurs réduits généraux il faut utiliser une autre stratégie.

Extension du corps de base et encodage. Dans la définition de l'encodage e_H, nous faisons certaines hypothèses sur le corps de base de sorte que certaines exponentiations sont bijectives et déterministiquement calculables. Si on veut encoder directement dans la jacobienne d'une courbe hyperelliptique H définie sur $\mathbb{F}_q$, on peut changer ces conditions de la façon suivante : appliquons ces conditions à l'extension $\mathbb{F}_{q^g}$ (et non plus nécessairement sur $\mathbb{F}_q$). La fonction e_H devient un encodage e'_H de $\mathbb{F}_{q^g} \setminus \mathcal{S}'$ (où l'ensemble $\mathcal{S}'$ peut être calculé de la même façon que les ensembles $\mathcal{S}$ exclus dans nos encodages) vers l'ensemble des points $\mathbb{F}_{q^g}$-rationnels de H. En utilisant cette nouvelle fonction e'_H, on peut calculer un ensemble de k points dans $H(\mathbb{F}_{q^g})$ tel que la somme de leurs degrés sur $\mathbb{F}_q$ est inférieure à g. En construisant les $\mathbb{F}_q$-conjugués de ces points et en éliminant les possibles collisions après négation, on en déduit un diviseur réduit de $\mathcal{J}_H(\mathbb{F}_q)$. Cette seconde stratégie est plus générale que la première mais elle ne suppose pas les mêmes conditions sur le corps $\mathbb{F}_q$.

Comme tous les encodages présentés dans cette thèse, ceux-ci vérifient les propriétés du théorème 3.5.1.

Caract	Courbes	G	Auteurs	Conditions	d/Dmax
$\neq 2,3$	$y^2 = x^3 + ax + b$	1	Shallue *et al.* [64]	-	1/1
			Brier *et al.* [13]	$q \equiv 3 \mod 4$	
	$y^2 = x^{2g+1} + ax + b$	g	Ulas [70]	-	2/(2g-1)
2	$y^2 + xy = x^3 + ax^2 + b$	1	Shallue *et al.* [64]		1/1
3	$y^2 + xy = x^3 + ax^2 + b$		Brier *et al.* [13]		
$\neq 2,3$	$y^2 = x^3 + ax + b$		Icart, 3.2.3	$q \equiv 2 \mod 3$	
	$x^3 + y^3 + 1 = 3dxy$		Théorème 4.2.1		
			Farashahi, [29]		
	$y^2 = (x^3 + 3\,ax + 2)^2 + 8\,bx^3$	2	Théorème 4.2.3		2/3
	$y^2/\lambda = (x^3 + 3\mu x + 2a)^2 + 4b$		Théorème 4.2.4		
	$y^2 = p_{a,b}(x), \deg p = 2g + 1$	g	Théorème 4.3.3	$< d, q - 1 >= 1$	2/(2g-1)
	$y^2 = x^{2d} + bx^d + a, g = d - 1$		Théorème 4.3.7		
	$y^2 = p(x), \deg p = 2g + 1$		Fouque *et al.* [31]	$p(x) = -p(-x)$	g/(2g-1)
2	$y^2 + y = p_{a,b}(x)$		Théorème 4.3.5	-	2/(2g-1)
	$y^2 + xy = x^3 + ax + b$	1	Icart [38]		1/1

TABLE 3.1 – Récapitulatif des fonctions d'encodage sur courbes connues

3.4 Synthèse des encodages

Nous récapitulons dans la figure 3.1 toutes les courbes elliptiques et hyperelliptiques pour lesquelles on connaît une fonction d'encodage, selon la caractéristique du corps de base. La colonne G précise le genre des courbes obtenues (génériquement) dans la famille. La dernière colonne rappelle la dimension de l'espace des courbes de la classe et la dimension totale de l'espace des courbes hyperelliptiques de ce genre.

Notons d'abord un résultat plutôt négatif dû à Zariski : il est impossible de paramétrer algébriquement, c'est-à-dire par radicaux quels qu'en soient les degrés, une courbe générique de genre supérieur ou égal à 6 [72]. C'est l'analogue de l'impossibilité de résoudre l'équation polynomiale de degré 5 par radicaux.

Toutefois, ce résultat est très général : il concerne des paramétrisations complètes de la courbe, pas les encodages (paramétrisations impropres) qui sont notre sujet bien qu'ils soient similaires dans le principe aux paramétrisations. De plus il s'agit de courbes génériques, et il est évident de trouver des paramétrisations par radicaux pour toutes les courbes hyperelliptiques (sous forme de Weierstrass si la courbe a pour équation $y^2 = p(x)$ elle se paramètre par radicaux comme $t \mapsto (t, \sqrt{p(t)})$). Enfin les courbes les plus utiles en cryptographie sont les courbes de genre 1, 2 et 3 seulement.

3.5 Fonctions de hachage

3.5.1 Construction

Une idée pour hacher vers une courbe elliptique $\mathcal{E}_{\mathbb{F}_q}$ consiste à composer une fonction de hachage classique h vers le corps fini $\mathbb{F}_q$ et une fonction d'encodage e de $\mathbb{F}_q$ vers $\mathcal{E}$. On peut ainsi espérer ramener la sécurité de la composition en tant que fonction de hachage vers la courbe aux propriétés de sécurité de h, *cf* figure 3.5.1.

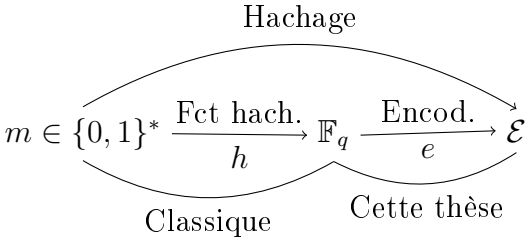

FIGURE 3.3 – Construction de fonctions de hachage vers courbes

En composant une fonction d'encodage e avec une fonction de hachage h vers le corps fini base de la courbe, on obtient une fonction qui à tout message associe un point de la courbe. Toutefois, il faut s'assurer que cette composition préserve toute les propriétés de sécurité qu'on attend d'une fonction de hachage "directe" vers la courbe.

3.5.2 Sécurité

Si nous modélisons h par un oracle aléatoire, $e \circ h$ n'est plus un oracle aléatoire sauf dans de très rares cas. En effet, il est souvent possible pour un adversaire de déterminer que les points obtenus sont tous dans l'image de e, qui n'atteint pas toute la courbe, et de déterminer au bout de quelques requêtes que cette fonction ne se comporte pas comme un oracle aléatoire vers $\mathcal{E}$.

Cet aspect a été traité par plusieurs publications [13], [30]. Il nous suffira de savoir pour l'encodage vers les courbes qu'il est possible d'utiliser cette construction $e \circ h$ de manière sûre une fois quelques propriétés de e, raisonnables, connues. Brier *et al.* ont établi le résultat suivant, qui donne des critères que doivent vérifier les fonctions d'encodage e pour qu'une primitive idéale (un oracle aléatoire vers la courbe) puisse être remplacé par cette construction, en supposant les fonctions de hachage h idéales. Cela revient essentiellement à calculer un point encodé et à le masquer par l'algorithme naïf de la section 3.1.2.

Théorème 3.5.1 ([13]) *Soit $e : \mathbb{F}_q \to \mathcal{E}$ une fonction d'encodage, h_1, h_2 deux oracles aléatoires vers $\mathbb{F}_q$ et G un point générateur de $\mathcal{E}$.*

Si il existe un entier α *tel que pour tout* $P \in \mathcal{E}$ $\operatorname{card} e^{-1}(P) \leqslant \alpha$ *et si cet ensemble* $e^{-1}(P)$ *est calculable pour tout* P*, alors la construction*

$$H : \begin{array}{ccc} \{0,1\}^* & \longrightarrow & \mathcal{E} \\ m & \mapsto & e \circ h_1(m) + [h_2(m)]G \end{array}$$

est indifférentiable d'un oracle aléatoire vers $\mathcal{E}$*.*

En toute généralité, il suffit même que α soit une fonction polynomiale en le paramètre de sécurité. Toutefois, dans tous les cas que nous aborderons, ce sera un entier bien déterminé, comme précisé ci-dessous à la section 3.1.3.

Des améliorations ont été ajoutées par la suite pour certains encodages, notamment ceux dont nous parlons ci-dessous, [30]. Une construction de même complexité théorique mais plus efficace en pratique consiste à calculer le point $e \circ h_1(m) + e \circ h_2(m)$ (ou plus généralement à effectuer une somme de $g+1$ éléments d'une jacobienne de courbe de genre g) : ceci évite l'exponentiation sur la courbe.

Le résultat de cette section est que des propriétés très raisonnables (nombre d'antécédents par élément du corps fini encodé) suffisent pour construire une fonction de hachage vers les courbes elliptiques qui possède de bonnes propriétés de sécurité.

Chapitre 4

Fonctions d'encodage : approche algébrique.

Dans ce chapitre, nous présentons de nouvelles fonctions d'encodage vers les courbes elliptiques définies sur des corps finis. Ces fonctions ont donné lieu à publication [45], conjointement avec R. Lercier et G. Renault. Contrairement aux encodages proposés par Icart [38], nous partons de polyômes résolubles par radicaux pour obtenir des modèles de courbes qui peuvent alors être paramétrées algébriquement. Cette stratégie nous a permis de découvrir des fonctions d'encodage de bas degré pour les courbes elliptiques Hessiennes et pour des courbes de genre 2. Nous présenterons également des encodages pour des familles plus restreintes de courbes hyperelliptiques de genre quelconque.

Comme nous le verrons, ces encodages ont une image suffisamment grande pour permettre leur utilisation dans des protocoles cryptographiques : les encodages que nous proposons vérifient les propriétés du théorème 3.5.1 ci-dessus, et fournissent une bonne fonction de hachage vers les courbes une fois combinés à une fonction de hachage classique.

4.1 Introduction

Reprenant les notations du chapitre précédent, soit $\mathbb{F}_q$ un corps fini de caractéristique impaire p et $H/\mathbb{F}_q : y^2 = f(x)$ avec $\deg f = d$ une courbe elliptique (si $d = 3$ ou 4) ou hyperelliptique (si $d \geqslant 5$). Nous fixerons plus tard des contraintes sur le corps fini, étant donné que pour les applications cryptographiques essentiellement seule la taille du corps compte.

Nous voyons ici le problème sous un angle légèrement différent : dans le chapitre précédent, il s'agit de trouver des fonctions d'encodage valables pour les courbes elliptiques (*id est* les courbes de genre 1). À l'inverse, étant donné un genre g fixé nous décrivons une stratégie pour trouver des courbes de genre g qui admettent une

fonction d'encodage déterministe vers un large sous-ensemble de leurs points.

Rappelons que toute courbe qui admet une paramétrisation rationnelle est une courbe de genre 0 (*cf* 3.1.1). Une fonction d'encodage pour une courbe de genre supérieur doit nécessairement être *algébrique*, c'est-à-dire qu'il sera nécessaire de calculer des radicaux. Ceci nous ramène à la paramétrisation de racines de polynômes. Ainsi, la stratégie est de partir de polynômes avec des racines qui sont facilement paramétrables et d'en déduire des courbes qui admettent un encodage déterministe.

4.1.1 Polynômes résolubles

La théorie de Galois classique fournit de larges familles de polynômes qui admettent des racines facilement paramétrables : il s'agit des polynômes résolubles par radicaux. Ils sont au cœur de notre stratégie.

Plus précisément, soit $f_{\underline{a}}(X)$ une famile de polynômes paramétrée par $\underline{a}$ (qui est un k-tuple $(a_1, a_2, \ldots, a_k)$ de paramètres) avec groupe de Galois résoluble. Nous nous intéressons non seulement à ces polynômes mais surtout en l'expression de leurs racines $\chi_{\underline{a}}$ par radicaux en fonction des paramètres.

Par exemple, $f_A(X) = X^2 + A$ en degré 2 a pour racines $\chi_A = \pm\sqrt{-A}$. Le degré 3 est plus intéressant : $f_{A,B}(X) = X^3 + A\,X + B$. Une racine de ce deuxième polynôme est calculable par les formules bien connues de Cardan-Tartaglia (voir par exemple [24], mais nous l'étudions également en détail plus loin 5.2).

4.1.2 Résolubilité et théorie des corps

Remarquons que nous pourrions utiliser les techniques classiques de la théorie des extensions de corps pour construire de nouvelles familles de polynômes résolubles par radicaux à partir de familles plus petites, comme nous l'illustrerons par les exemples des polynômes de Moivre 4.3.1 et 4.3.2.

Par exemple, considérons les polynômes de Moivre de degré d (impair) : à partir de l'extension de corps de degré 2 définie par $\theta^2 + B\theta - A^d$, puis par l'extension de Kummer de degré d définie par $\gamma^d - \theta = 0$, l'élément $X = \gamma - A/\gamma$ est défini sur un sous-corps de degré d de l'extension de degré $2d$. Le polynôme de définition de cette extension est donné par le polynôme minimal de X, qui est égal au polynôme de Moivre

$$X^d + dAX^{d-2} + 2dA^2X^{d-4} + 3dA^3X^{d-6} + \cdots + 2dA^{(d-1)/2-1}X^3 + dA^{(d-1)/2}X + B\,.$$

Une construction similaire est de considérer des extensions de Kummer d'extensions quadratiques ou de petit degré, ce qui donne $X^{2d} + AX^d + B$. À partir de ces deux familles particulières, nous proposons des encodages déterministes vers des

courbes hyperelliptiques de genre quelconque $g \geqslant 2$ dans les sections suivantes 4.3.2 et 4.3.1.

4.1.3 Paramétrisations déterministes et rationnelles

Étant donnée une famille paramétrée de polynômes résolubles $f_{\underline{t}}(X)$ et un genre g, nous substituons maintenant une fonction rationnelle $F_i(Y)$ en une indéterminée Y pour chaque paramètre a_i de $\underline{a}$.

Soit $\underline{F}(Y)$ le k-tuple de fonctions rationnelles $(F_1(Y), F_2(Y), \ldots, F_k(Y))$. L'équation $f_{\underline{F}(Y)}(X)$ définit maintenant une courbe algébrique plane C, avec les deux variables (X, Y). Le genre de C augmente avec le degré en Y de $\underline{F}(Y)$. Si on vise un genre fixé g pour C, peu de degrés sont admissibles pour les numérateurs et dénominateurs de $\underline{F}(Y)$. Comme on peut considérer les coefficients de ces paramétrisations rationnelles comme des paramètres $\underline{a} = (a_1, \ldots, a_{k'})$, ceci fournit une famille de courbes $C_{\underline{a}}$.

Parmi ces fonctions rationnelles $\underline{F}(Y)$, il reste maintenant à déterminer lesquelles donnent des racines $\chi_{\underline{F}(Y)}$ calculables en temps constant. Le cas le plus facile est quand le calcul de $\chi_{\underline{t}}$ ne fait intervenir aucune racine carrée, car alors tout choix de $\underline{F}(Y)$ convient, au prix de quelques contraintes sur le corps fini de base : on est alors sûr que toutes les opérations sont clairement définies. Ce n'est toutefois généralement pas le cas, aussi il faut relier le calcul de ces racines carrées à la paramétrisation d'une courbe algébrique auxiliaire : le problème est d'être sûr que les éléments dont nous aurons à extraire une racine carrée seront bien des résidus quadratiques dans $\mathbb{F}_q$.

4.1.4 Modèles de courbes

Dans quelques cas (typiquement, les courbes hyperelliptiques), il est intéressant d'obtenir un modèle minimal (typiquement de la forme $y^2 = g_{\underline{a}}(x)$) à partir de l'équation de $C_{\underline{a}}$ issue de la paramétrisation précédente. Pour maintenir un encodage déterministe vers le modèle minimal, il nous faut un morphisme birationnel explicite $x = \Lambda_{\underline{a}}(X, Y)$, $y = \Omega_{\underline{a}}(X, Y)$.

Pour les courbes elliptiques et hyperelliptiques, la méthode usuelle consiste à travailler avec des différentielles définies par $C_{\underline{a}}$. Cette méthode est implémentée dans plusieurs logiciels de calculs algébriques, par exemple MAPLE [41] ou Magma [9].

Au final, pour un modèle minimal $y^2 = g_{\underline{a}}(x)$, nous obtenons l'encodage comme suit :

- Choisir Y comme une fonction (non rationnelle) d'un paramètre t tel que toutes les racines carrées qui apparaissent dans l'expression de $\chi_{\underline{F}(Y)}$ soient bien définies, c'est-à-dire qu'elles s'appliquent à des résidus quadratiques ;
- calculer $X = \chi_{\underline{F}(Y)}$;

– calculer $x = \Lambda_{\underline{a}}(X, Y)$ et $y = \Omega_{\underline{a}}(X, Y)$.

4.2 Polynômes de degré 3

Dans cette section, nous nous plaçons en caractéristique différente de 2 et de 3 et nous considérons des polynômes de degré 3. Après changement de variables, toute cubique peut être écrite sous la forme réduite $X^3 + 3\,A\,X + 2\,B$, dont une racine est

$$\chi_{A,B} = \sqrt[3]{-B + \sqrt{A^3 + B^2}} - \frac{A}{\sqrt[3]{-B + \sqrt{A^3 + B^2}}}.$$

Pour utiliser cette racine en s'assurant que $A^3 + B^2$ est un carré afin de paramétrer (non rationnellement) des courbes de genre non nul, nous nous restreignons tout d'abord aux corps finis $\mathbb{F}_q$ avec q impair et $q \equiv 2 \mod 3$. Le calcul des racines cubiques se fait alors par une exponentiation (déterministe) à la puissance $1/3 \mod q - 1$. Ensuite, il nous faut considérer les fonctions rationnelles A et B en Y telles que la courbe $A(Y)^3 + B(Y)^2 - Z^2$ peut être paramétrée également : une paramétrisation de Z nous assurera que le discriminant de l'équation de degré 3 est un résidu quadratique, et on obtiendra même directement une paramétrisation de sa racine carrée sans avoir à l'extraire par des algorithmes spécifiques.

Retirons de l'équation les facteurs carrés : si A est non nulle, soit $A(Y) = T(Y)$ et $B(Y) = T(Y)S(Y)$ pour une fonction rationnelle S. Le problème revient alors à celui de paramétrer la courbe

$$T(Y) + S^2(Y) = Z^2. \tag{4.1}$$

Ceci est faisable par des formules rationnelles quand elle est de genre 0 (*cf* 3.1.1), ou avec les formules d'Icart quand elle est de genre 1. Dans le cas de courbes planes irréductibles, ceci signifie que T et S doivent être de bas degré. Plutôt que de paramétrer une courbe auxiliaire, nous aurions pu choisir directement T et S telles que $T(Y) + S(Y)^2 = Z(Y)^2$ pour une fonction rationnelle Z. Avec des degrés comparables pour T et S avec ceux du reste de la section, nous n'avons obtenu que des courbes de genre 0. Il nous faudrait alors augmenter considérablement le degré de S et T pour atteindre des courbes de genre supérieur. Ces courbes auraient alors un haut degré mais un petit genre, et donc beaucoup de singularités.

Finalement, nous considérons par la suite les équations de degré 3 de la forme suivante :

$$X^3 + 3\,T(Y)\,X + 2\,S(Y)T(Y) = 0. \tag{4.2}$$

Nous aurions pu considérer également le cas $A = 0$, c'est-à-dire des polynômes de la forme $f_B = X^3 + 2B$. Nos expériences en genre 1 et 2 montrent que les courbes

ainsi obtenues sont birationnellement équivalentes aux courbes hyperelliptiques de genre quelconque construites à partir des polynômes de Moivre (section 4.3.1). Nous n'étudions pas plus avant ce cas.

4.2.1 Courbes de genre 1

Paramétrisation

Nous avons fait une étude systématique des courbes (4.2) de genre (génériquement) 1 vu comme une fonction des degrés des numérateurs et dénominateurs des fonctions rationnelles $S(Y)$ et $T(Y)$. Les résultats sont dans le tableau 4.1, où nous avons regroupé les colonnes des degrés compatibles. Typiquement, la première colonne (où S est un polynôme de degré 2 et T une constante) est un sous-cas de la seconde (où S est de degré au plus 3 et T une constante).

		Degrés										
$S(Y)$	Num.	2	3	2	0	1	0	1	0	0	0	0
	Dén.	0	0	0	1	0	0	0	1	0	1	0
$T(Y)$	Num.	0	0	1	1	1	2	2	0	0	0	0
	Dén.	0	0	0	0	0	0	0	1	2	2	3
Genre de l'équation (4.1)		1	2	1	1	0	0	0	1	1	1	2

TABLE 4.1 – Degrés de $S(Y)$ et $T(Y)$ pour les courbes planes de genre 1 produites par l'équation (4.2)

Nous sommes dans le cas où la courbe initiale (4.2) est de genre 1 et nous recherchons une nouvelle paramétrisation. Le seul cas où la courbe (4.1) est paramétrable est donc celui où elle est de genre 0, c'est-à-dire si $S(Y)$ est un polynôme de degré au plus 1 et $T(Y)$ est un polynôme de degré au plus 2. Quand $q \equiv 2 \bmod 3$, ces courbes elliptiques ont toutes un point de 3-torsion $\mathbb{F}_q$-rationnel, pour $X = 0$.

Les courbes elliptiques avec un point de 3-torsion $\mathbb{F}_q$-rationnel sont connues pour avoir des formules d'addition très efficaces quand elles sont données sous forme hessienne "généralisée" ou "tordue" [28, 4].

Partons de $S(Y) = 3\,(Y + a)/2,\ T(Y) = -\,Y/3\,$, c'est-à-dire des courbes de type

$$C_{0,a} : Y^2 + XY + aY = X^3\,,\ a \neq 0, 1/27\,. \tag{4.3}$$

Alors la conique $S^2(Y) + T(Y) = 9/4\,Y^2 + (9/2\,a - 1/3)\,Y + 9/4\,a^2 = Z^2$ peut être paramétrée "par des droites" par

$$Y = \frac{12\,t^2 - 27\,a^2}{36\,t - 4 + 54\,a}\,,\ Z = \frac{36\,t^2 + (-8 + 108\,a)\,t + 81\,a^2}{72\,t - 8 + 108\,a}\,,$$

de sorte que $X = \Delta/6 + 2Y/\Delta$, où $\Delta = \sqrt[3]{36Y\,(3\,Y + 3\,a + 2\,Z)}$.

De plus, la courbe (4.3) est birationnellement équivalente au modèle hessien

$$E_d : x^3 + y^3 + 1 = 3\,dxy,\ d \neq 1, \tag{4.4}$$

avec $a = (d^2 + d + 1)/3\,(d+2)^3$ et

$$x = \frac{3\,(d+2)^2\,(Y\,(d+2) + X)}{3\,(d+2)^2\,X + d^2 + d + 1},\ y = -\frac{d^2 + d + 1 + 3\,(d+1)\,(d+2)^2\,X + 3\,(d+2)^3\,Y}{3\,(d+2)^2\,X + d^2 + d + 1}. \tag{4.5}$$

Le seul cas restant est celui de $d = -2$, c'est-à-dire la courbe hessienne E_{-2} qui est la tordue quadratique de la courbe E_0 : toutes deux ont leur j-invariant égal à 0. Cette courbe est isomorphe à une courbe du type (4.2) avec $S = (1 - 7\,Y)/4$ et $T = -26\,(3\,Y^2 + 1)/27$. Nous pourrions utiliser cet isomorphisme pour paramétrer E_{-2}, mais il est bien plus simple d'utiliser directement la courbe $Y^2 + Y = X^3$, qu'on peut paramétrer directement par $Y = t$, $X = \sqrt[3]{t^2 + t}$. Cette courbe est isomorphe à E_{-2} en prenant $x = (X+1)/(X+Y)$, $y = (-Y + X - 1)/(X + Y)$.

Nous récapitulons ces calculs dans l'algorithme 2.

Algorithme 2: HessianEncode

Entrée : Une courbe elliptique hessienne
$E_d/\mathbb{F}_q : x^3 + y^3 + 1 = 3\,dxy,\ d \neq 1$, et $t \in \mathbb{F}_q$.
Sortie : Un point $(x_t : y_t : 1)$ de E_d.

if $d = -2$ **then** /* $t \neq 0$ */
  $Y := t$; $X := (t + t^2)^{1/3 \bmod q-1}$;
  $x_t := (X+1)/(X+Y)$; $y_t := (-Y + X - 1)/(X + Y)$;
  return $(x_t : y_t : 1)$

$a := \dfrac{d^2 + d + 1}{3\,(d+2)^3}$; /* $t \neq \dfrac{(2\,d+1)(d^2+d+7)}{18\,(d+2)^3}$ */

if $t = \pm 3a/2$ **then**
  $Y := 0$; $X := 0$;
else /* $Y \neq 0$ */
  $Y := \dfrac{12\,t^2 - 27\,a^2}{36\,t + 54\,a - 4}$; $\Delta := (36\,Y\,(2\,t + 3\,a))^{1/3 \bmod q-1}$;
  $X := \Delta/6 + 2\,Y/\Delta$;

$x_t := \dfrac{3\,(d+2)^2\,(Y\,(d+2) + X)}{3\,(d+2)^2\,X + d^2 + d + 1}$;

$y_t := -\dfrac{3\,(d+1)\,(d+2)^2\,X + 3\,(d+2)^3\,Y + d^2 + d + 1}{3\,(d+2)^2\,X + d^2 + d + 1}$;

return $(x_t : y_t : 1)$

FIGURE 4.1 – Encodage vers les courbes hessiennes

Finalement, nous avons prouvé le théorème suivant :

Théorème 4.2.1 *Soit $\mathbb{F}_q$ le corps fini à q éléments. Supposons q impair et $q \equiv 2 \mod 3$. Soit $E_d/\mathbb{F}_q$ la courbe elliptique définie par l'équation (4.4).*

Alors l'algorithme 2 calcule un encodage déterministe e_d de $\mathbb{F}_q^*$ si $d = -2$ et de $\mathbb{F}_q \setminus \left\{ \frac{(2\,d+1)\left(d^2+d+7\right)}{18\,(d+2)^3} \right\}$ sinon vers E_d, avec complexité $\mathcal{O}(\log^{2+o(1)} q)$.

Remarque : cet encodage n'est pas défini pour tout $\mathbb{F}_q$, mais on peut toujours envoyer les valeurs manquantes sur le point à l'infini de la courbe.

Nombre de courbes Une méthode pour quantifier le nombre de courbes définies par l'équation (4.4) est de calculer leur j-invariant.

On obtient ainsi

$$j_{E_d} = 27\,d^3\,\frac{(d+2)^3\,(d^2-2\,d+4)^3}{(d-1)^3\,(d^2+d+1)^3}\,. \tag{4.6}$$

Quand $q \equiv 2 \mod 3$, il y a exactement $\lfloor q/2 \rfloor$ invariants distincts. De plus, on peut montrer qu'il existe $q-1$ classes distinctes $\mathbb{F}_q$-isomorphes de courbes elliptiques hessiennes [28].

Cardinal de l'image. Il est facile de voir que $|\operatorname{Im} e_{-2}| = q-1$, simplement parce que $Y = t \neq 0$. Dans le cas général, on peut également calculer exactement $|\operatorname{Im} e_d|$ pour $d \neq 1, -2$

Théorème 4.2.2 *Soit $d \neq 1, -2$, alors $|\operatorname{Im} e_d| = (q+1)/2$ si $(d-1)/(d+2)$ est un résidu quadratique dans $\mathbb{F}_q$, et $|\operatorname{Im} e_d| = (q-1)/2$ sinon.*

Démonstration Soit $(x : y : 1)$ un point de E_d, alors il existe un unique point $(X : Y : 1)$ sur $C_{0,a}$ envoyé par l'isomorphisme (4.5) sur $(x : y : 1)$.

Vu comme un polynôme en t, l'équation $12\,t^2 - 36\,Y\,t - 54\,Y\,a - 27\,a^2 + 4\,Y$ a 0 ou 2 solutions sauf si $27\,Y^2 + (-4+54\,a)\,Y + 27\,a^2 = 0$. Ce dernier polynôme n'a pas de racine en Y si $1 - 27\,a = (d-1)^3/(d+2)^3$ est un résidu non quadratique, et il a deux racines distinctes notées Y_0 et Y_1 sinon (si $a = 1/27$, la courbe $C_{0,a}$ dégénère en une courbe de genre 0).

Récapitulons quand $(d-1)\,/\,(d+2)$ est un résidu quadratique dans $\mathbb{F}_q$:

- (1 élément) si $t \in \left\{ \frac{(2\,d+1)\left(d^2+d+7\right)}{18\,(d+2)^3} \right\}$, alors t n'est pas encodable par e_d ;
- (2 éléments) Si $t \in \{\pm \frac{d^2+d+1}{2\,(d+2)^3}\}$, alors $e_d(t) = (0 : -1 : 1)$;
- (2 éléments) Si t_i est une racine (double) de $12\,t^2 - (36\,t - 4 + 54\,a)\,Y_i - 27\,a^2$ avec $i = 0, 1$, on obtient deux points distincts $e_d(t_i) = (x_{t_i} : y_{t_i} : 1)$;
- ($q-5$ éléments) Sinon, pour tout t restant, il existe exactement un autre t' tel que $e_d(t) = e_d(t') = (x_t : y_t : 1)$.

On obtient ainsi $(q-5)/2+2+1 = (q+1)/2$ points distincts rationnels sur la courbe. Similairement si $(d-1)/(d+2)$ est un résidu non quadratique dans $\mathbb{F}_q$, on obtient $(q-1)/2$ points distincts rationnels sur E_d. □

Comparaison avec les encodages précédents. Comparé aux formules d'Icart [38], cet encodage a deux inconvénients d'impact pratique limité :

- il ne fonctionne que pour les courbes hessiennes et donc pas pour toutes les courbes ;
- le sous-ensemble de la courbe qui est paramétré est légèrement plus petit que dans le cas d'Icart : nous avons $\simeq q/2$ points contre approximativement $5/8\#E \pm \lambda\sqrt{q}$.

Toutefois il a trois avantages majeurs :

- retrouver le paramètre t à partir d'un point donné $(x : y : 1)$ est bien plus simple : il suffit de trouver les racines d'un polynôme de degré 2 au lieu du degré 4 dans le cas d'Icart ;
- le paramètre t dépend seulement de y ; on peut donc économiser la moitié de la bande passante d'un protocole en n'envoyant que y et non pas l'ensemble du point $(x : y : 1)$ sans avoir à changer de système de coordonnées : il suffit d'envoyer Y et un bit indiquant lequel des deux paramètres t solutions de l'équation de degré 2 choisir ;
- Y est calculable en n'utilisant que des opérations de corps fini simples (rationnelles) : sans avoir besoin d'exponentiation Y contient toute l'information sur le point encodé. Pour l'encodage, il est donc préférable de travailler sur le modèle $C_{0,a}$ plutôt que sur le modèle hessien [1].

4.2.2 Courbes de genre 2

Paramétrisation.

Dans la même veine que la section 4.2.1, nous avons fait une étude systématique des courbes (4.2) de genre 2 (génériquement) vues comme une fonction des degrés des numérateurs et des dénominateurs des fonctions rationnelles $S(Y)$ et $T(Y)$. Les résultats sont synthétisés dans le tableau 4.2.

Nous cherchons ici à paramétriser des courbes de genre 2 en utilisant les encodages connus pour les courbes de genre 0 et 1. Trois cas sont donc intéressants :

- si $S(Y)$ et $T(Y)$ sont tous deux des fonctions rationnelles de degré 1 ;
- si $S(Y)$ est une fonction rationnelle de degré 2 et $T(Y)$ une constante ;
- si $S(Y)$ est une constante et $T(Y)$ une fonction rationnelle de degré 2.

1. Par exemple, on pourrait imaginer qu'un appareil de puissance limitée calcule le haché y et l'envoie à un autre, spécialisé en les opérations sur les courbes et capable de calculer le x associé et réaliser les opérations de groupe.

		Degrés															
$S(Y)$	Num.	2	0	1	2	2	2	1	1	0	1	1	1	1	2	0	0	0
	Dén.	1	2	2	2	0	1	1	0	1	1	1	0	0	0	0	0	0
$T(Y)$	Num.	0	0	0	0	0	0	0	1	1	1	1	0	1	0	1	2	2
	Dén.	0	0	0	0	1	1	1	1	1	0	1	2	2	2	2	1	2
Genre de l'équation (4.2)		1	1	1	1	2	2	1	1	1	1	1	2	2	3	1	1	1

TABLE 4.2 – Degrés de $S(Y)$ et $T(Y)$ pour les courbes planes de genre 2 données par l'équation (4.2)

Nous étudions les deux premiers cas seulement : il s'avère que le troisième produit des courbes qui sont obtenues également par le second.

Si $S(Y)$ et $T(Y)$ sont des fonctions rationnelles de degré 1.

Soit $S(Y) = (\alpha Y + \beta)/(\gamma Y + \delta)$ et $T(Y) = (\varepsilon Y + \varphi)/(\mu Y + \nu)$, alors la courbe (4.2) est birationnellement équivalente aux courbes de la forme $y^2/d^2 = (x^3+3\,ax+2\,c)^2+8\,bx^3$ où

$$a = \frac{\delta\varepsilon - \gamma\varphi}{\delta\mu - \gamma\nu},\ b = \frac{(\alpha\delta - \gamma\beta)(\mu\varphi - \varepsilon\nu)}{(\delta\mu - \gamma\nu)^2}, c = \frac{\beta\varepsilon - \alpha\varphi}{\delta\mu - \gamma\nu} \quad \text{et} \quad d = (\delta\mu - \gamma\nu)\,.$$

Beaucoup de ces courbes sont isomorphes les unes aux autres, et sans perte de généralité on peu fixer $c = 1$ et $d = 1$. Finalement nous nous restreignons aux fonctions $S(Y) = -Y$, $T(Y) = (a^2Y + a)/(aY + b + 1)$, telles que, quand $4\,a^6b^3 - b^3\,(b^2 + 20\,b - 8)\,a^3 + 4\,b^3\,(b+1)^3 \neq 0$, la courbe (4.2) est birationnellement équivalente à la courbe de genre 2 qui a pour modèle de Weierstrass

$$H_{1,a,b} : y^2 = (x^3 + 3\,ax + 2)^2 + 8\,bx^3\,, \tag{4.7}$$

avec $x = X$ et $y = -4\,aY + X^3 + 3\,aX - 2$.

De plus, la courbe

$$S^2(Y) + T(Y) = Y^2 + (a^2\,Y + a)/(aY + 1 + b) = Z^2 \tag{4.8}$$

est birationnellement équivalente à la courbe elliptique dont le modèle de Weierstrass est

$$V^2 = U^3 + (-a^6 + 2\,(b+1)(2\,b-1)a^3 - (b+1)^4)\,\frac{U}{3} + \frac{1}{27}\,(2\,a^9 + 3\,(2 - 2\,b + 5\,b^2)a^6 - 6\,(2\,b-1)(b+1)^3a^3 + 2\,(b+1)^6)\,. \tag{4.9}$$

Si elle était hessienne, on pourrait utiliser la paramétrisation décrite ci-dessus. Dans tous les cas, on peut la paramétrer par la méthode d'Icart :

$$U = \frac{1}{6}\sqrt[3]{\frac{2\delta}{t^2}} + \frac{t^2}{3},\ V = \frac{1}{6}\sqrt[3]{2\delta t} + \frac{t^3}{6} + \frac{1}{6t}\left(-a^6 + 2\,(b+1)(2\,b-1)a^3 - (b+1)^4\right)$$

avec

$$\begin{aligned}\delta = -t^8 + (-12\,(b+1)(2\,b-1)a^3 + 6\,a^6 + 6\,(b+1)^4)t^4 + (12\,(2\,b - 5\,b^2 - 2)a^6 - 8\,(b+1)^6 \\ - 8\,a^9 + 24\,(2\,b-1)(b+1)^3a^3)t^2 + 3\,(a^6 - 2\,(b+1)(2\,b-1)a^3 + (b+1)^4)^2\end{aligned}$$

Revenant par le changement de variables birationnel de la courbe (4.9) à la courbe (4.8), nous obtenons Y et Z à partir de U et V (*cf.* algorithme 3 pour les formules détaillées). Soit maintenant $\Delta = \sqrt[3]{T(Y)(Z - S(Y))}$, alors $X = \Delta - T(Y)/\Delta$.

Algorithme 3: Genus2TypeAEncode

Entrée : Une courbe $H_{1,a,b}$ définie par l'équation (4.7) sur $\mathbb{F}_q$, un élément $t \in \mathbb{F}_q \setminus \mathcal{S}_1$
Sortie : Un point $(x_t : y_t : 1)$ sur $H_{1,a,b}$

$\delta := -t^8 + (-12\,(b+1)(2\,b-1)a^3 + 6\,a^6 + 6\,(b+1)^4)t^4 + (12\,(2\,b - 5\,b^2 - 2)a^6 - 8\,(b+1)^6 - 8\,a^9 + 24\,(2\,b-1)(b+1)^3a^3)t^2 + 3\,(a^6 - 2\,(b+1)(2\,b-1)a^3 + (b+1)^4)^2$;

$U := ((2\delta/t^2)^{1/3 \bmod q-1} + 2t^2)/6$;
$V := (2\delta t)^{1/3 \bmod q-1}/6 + t^3/6 + (-a^6 + 2\,(b+1)(2\,b-1)a^3 - (b+1)^4)/6t$;
$W := -3\,Ua + a((b+1)^2 + a^3)$; $Y := (3\,(b+1)U + (2\,b-1)a^3 - (b+1)^3)/W$;
$Z := 3\,V/W$;
$T := (a^2Y + a)/(aY + b + 1)$; $\Delta := (T(Z + Y))^{1/3 \bmod q-1}$;
$x_t := \Delta - T/\Delta$; $y_t := -4\,aY + X^3 + 3\,aX - 2$;
return $(x_t : y_t : 1)$

FIGURE 4.2 – Encodage sur les courbes de genre 2 (de type A).

Finalement nous obtenons le théorème suivant :

Théorème 4.2.3 *Soit $\mathbb{F}_q$ le corps fini à q éléments. Supposons q impair et $q \equiv 2 \bmod 3$. Soit $H_{1,a,b}/\mathbb{F}_q$ la courbe hyperelliptique de genre 2 définie par l'équation (4.7).*

L'algorithme 3 calcule un encodage déterministe $e_{1,a,b} : \mathbb{F}_q^* \setminus \mathcal{S}_1 \to H_{1,a,b}$, où $\mathcal{S}_1$ est un sous-ensemble de $\mathbb{F}_q$ de taille au plus 35, avec complexité $\mathcal{O}(\log^{2+o(1)} q)$.

Démonstration Les formules précédentes définissent un encodage déterministe pourvu que t, W, $aY + b + 1$ et Δ soient tous non nuls.

La condition $W = 0$ donne un polynôme en t de degré 8, il existe donc au plus 8 valeurs pour lesquelles $W = 0$. De même, la condition $aY + b + 1 = 0$ fournit au plus 8 valeurs supplémentaires pour lesquelles $W = 0$.

En outre, $\Delta = 0$ si et seulement si $T = 0$ ou $Z = -Y$. La condition $T = 0$ donne 8 valeurs supplémentaires. De même, la condition $Z + Y = 0$ donne un polynôme en t de degré 10, dans ce cas nous avons au plus 18 valeurs pour lesquelles $\Delta = 0$.

Le nombre total d'éléments de $\mathbb{F}_q$ qui ne peuvent pas être encodés est finalement au plus 35. □

Cardinal de l'image. Soit (X, Y) un point rationnel sur une courbe $C_{1,a,b,c}$, soit t un antécédent de (X, Y) par notre encodage $e_{1,a,b}$. Alors il existe une relation polynomiale entre Y et t de degré au plus 8 en t (*cf.* algorithme 3). (X, Y) a donc au plus 8 antécédents par $e_{1,a,b}$. Finalement, $|\operatorname{Im} e_{1,a,b}| \geqslant (q - 35)/8$.

Nombre de courbes. Les invariants d'Igusa [40] de ces courbes sont égaux à

$$\begin{aligned}
J_2 &= 2^6\,3\,(-9\,a^3 + 4\,b^2 + 4\,b - 9)\,,\\
J_4 &= 2^{10}\,3\,(-9\,b(4\,b-15)a^3 + 4\,b(b+1)(2\,b^2 + 2\,b - 27))\,,\\
J_6 &= 2^{14}\,(729\,a^6b^2 - 216\,b^2\left(2\,b^2 + 3\,b + 21\right)a^3 + 16\,b^2\left(4\,b^2 + 4\,b + 81\right)(b+1)^2)\,,\\
J_8 &= 2^{18}\,3\,(-6561\,a^9b^2 + 2916\,b^2\left(-7 + b^2 + 13\,b\right)a^6\\
&\quad -144\,b^2\left(4\,b^4 + 63\,b^3 + 450\,b^2 - 149\,b - 810\right)a^3\\
&\quad +64\,b^2\left(b^4 + 2\,b^3 + 154\,b^2 + 153\,b - 729\right)(b+1)^2)\,,\\
J_{10} &= 2^{28}\,3^6\,(4\,a^6b^3 - b^3\left(b^2 + 20\,b - 8\right)a^3 + 4\,b^3\,(b+1)^3)\,.
\end{aligned}$$

Le lieu géométrique de ces invariants est une surface de dimension 2 donnée par une équation homogène de degré 90, que nous ne décrivons pas plus ici. Par conséquent, l'équation (4.7) définit $\Theta(q^2)$ courbes non isomorphes sur $\mathbb{F}_q$.

Si $S(Y)$ est une fonction rationnelle de degré 2.

Soit maintenant $S(Y) = (\alpha Y^2 + \beta Y + \gamma)\ /\,(\delta Y^2 + \varepsilon Y + \varphi)$ et $T(Y) = \kappa$, la courbe (4.2) est birationnellement équivalente aux courbes de la forme $y^2/\lambda = (x^3 + 3\,\mu x + 2\,a)^2 + 4\,b$ où

$$\lambda = \varepsilon^2 - 4\,\varphi\delta\,,\ \mu = \kappa\,,\ a = \frac{\kappa}{\lambda}(\varepsilon\beta - 2\,\delta\gamma - 2\,\varphi\alpha)\ \text{ et } b = \frac{\kappa^2}{\lambda}(\beta^2 - 4\,\alpha\gamma) - a^2\,.$$

Plusieurs de ces courbes sont isomorphes les unes aux autres et, sans perte de généralité, nous pouvons fixer λ et μ comme n'importe quel résidu quadratique non nul (par exemple, $\lambda, \mu = 1$) ou n'importe quel résidu non quadratique (par exemple $\lambda, \mu = -3$ vu que $q \equiv 2 \bmod 3$).

Finalement nous obtenons :

$$S(Y) = \frac{\lambda(a-u)Y^2 - 4\,vY - 4\,(a+\,u)}{\mu(\lambda Y^2 - 4)}\ \text{ et }\ T(Y) = \mu\,,$$

où $u = \mu^3/2\,w - w/2 - a$ avec $w \in \mathbb{F}_q^*$. Alors, quand $b^3\lambda^{10}(\mu^6 + 2\,\mu^3 a^2 - 2\,b\mu^3 + a^4 + 2\,ba^2 + b^2) \neq 0$, la courbe (4.2) est birationnellement équivalente à la courbe de genre 2 dont le modèle de Weierstrass est

$$H_{2,\lambda,\mu,a,v,w} : y^2/\lambda = (x^3 + 3\,\mu x + 2\,a)^2 + 4\,b\,, \tag{4.10}$$

avec $b = v^2/\lambda - u^2$ pour $v \in \mathbb{F}_q$, $x = X$ et $y = \lambda\,(X^3/2 + 3\,\mu X/2 + a - u)\,Y - 2\,v$.

Remarque : calculer v et w connaissant b revient à construire un point $(v : w : 1)$ sur la courbe elliptique $v^2/\lambda - (\mu^3/2\,w - w/2 - a)^2 - b = 0$. Comme dans le cas précédent, on peut toujours le faire en temps déterministe avec les formules d'Icart quand on peut exhiber un changement de variables bilinéaire $\mathbb{F}_q$-rationnel entre cette courbe et le modèle de Weierstrass cubique. C'est typiquement le cas quand $\lambda = 1$, mais plus quand $\lambda = -3$.

Par ailleurs, soit $z = w/2 + r^3/2w$ et donc tel que $(u + a)^2 + r^3 = z^2$, alors

$$\begin{aligned}\mu^2(\lambda Y^2 - 4)^2(S(Y)^2 + T(Y)) = -\lambda^2(4\,ua - z^2)Y^4 - 8\,\lambda v(a - u)Y^3 \\ - 8\,\lambda(4\,\mu^3 - 3\,z^2 - 2\,b + 6\,ua + 4\,a^2)Y^2 + 32\,v(u + a)Y + 16\,z^2 = Z^2\end{aligned} \tag{4.11}$$

est birationnellement équivalent à la courbe elliptique de modèle de Weierstrass

$$\begin{aligned}V^2 = U^3 + 2^8\lambda^2(-\mu^6 + (b - 2\,a^2)\mu^3 - (a^2 + b)^2)U/3 + \\ 2^{12}\lambda^3(2\,\mu^9 + (6\,a^2 - 3\,b)\mu^6 - 3\,(a^2 + b)(b - 2\,a^2)\mu^3 + 2\,(a^2 + b)^3)/3^3\,.\end{aligned} \tag{4.12}$$

Cette dernière peut être paramétrée par la méthode d'Icart. On obtient :

$$U = \frac{1}{6}\sqrt[3]{\frac{2\delta}{t^2}} + \frac{t^2}{3}, \quad V = \frac{1}{6}\sqrt[3]{2\delta t} + \frac{t^3}{6} + 128\,(-\mu^6 + (b - 2\,a^2)\mu^3 - (b + a^2)^2)\frac{\lambda^2}{3t}$$

avec

$$\begin{aligned}\delta = -t^8 + 2^9\,3\,(\mu^6 + (-b + 2\,a^2)\mu^3 + (a^2 + b)^2)\lambda^2 t^4 + \\ 2^{14}(-2\,\mu^9 - (6\,a^2 - 3\,b)\mu^6 + 3\,(a^2 + b)(b - 2\,a^2)\mu^3 - 2\,(a^2 + b)^3)\lambda^3 t^2 + \\ 2^{16}\,3\,(\mu^{12} + (-2\,b + 4\,a^2)\mu^9 + (3\,b^2 + 6\,a^4)\mu^6 + 2\,(a^2 + b)^2(-b + 2\,a^2)\mu^3 + (a^2 + b)^4)\lambda^4\,.\end{aligned} \tag{4.13}$$

De nouveau, en revenant par le changement de variables birationnel de la courbe (4.12) à la courbe (4.11), on obtient Y et Z à partir de U et V (*cf.* algorithme 4 pour les formules précises). Soit maintenant $\Delta = \sqrt[3]{T(Y)\,(Z/\mu(\lambda Y^2 - 4) - S(Y))}$, alors $X = \Delta - T(Y)/\Delta$.

Finalement nous obtenons le théorème suivant :

Algorithme 4: Genus2TypeBEncode

Entrée : Une courbe $H_{2,\lambda,\mu,a,v,w}$ définie par l'équation (4.10) sur $\mathbb{F}_q$, un élément $t \in \mathbb{F}_q \setminus \mathcal{S}_2$.
Sortie : Un point $(x_t : y_t : 1)$ on $H_{2,\lambda,\mu,a,v,w}$

$u := -(2\,aw + w^2 - r^3)/2w$; $b := v^2/l - u^2$; $z := (w^2 + r^3)/2w$;

$$\begin{aligned}\delta \;:=\;& -t^8 + 2^9\,3\,(\,\mu^6 + (-b + 2\,a^2)\mu^3 + (a^2 + b)^2)\lambda^2 t^4 + \\ & 2^{14}(-2\,\mu^9 - (6\,a^2 - 3\,b)\mu^6 + 3\,(a^2 + b)(b - 2\,a^2)\mu^3 - 2\,(a^2 + b)^3)\lambda^3 t^2 + \\ & 2^{16}\,3\,(\,\mu^{12} + (-2\,b + 4\,a^2)\mu^9 + (3\,b^2 + 6\,a^4)\mu^6 + 2\,(a^2 + b)^2(-b + 2\,a^2)\mu^3 + (a^2 + b)^4)\lambda^4;\end{aligned}$$

$U := ((2\,\delta/t^2)^{1/3 \bmod q-1} + 2t^2)/6$;

$V := (2\delta t)^{1/3 \bmod q-1}/6 + t^3/6 + 128\,(-\mu^6 + (b - 2\,a^2)\mu^3 - (b + a^2)^2)\lambda^2/3t$;

$$\begin{aligned}W \;:=\;& -9\,U^2 - 48\,\lambda(-3\,z^2 - 2\,b + 6\,ua + 4\,a^2 + 4\,\mu^3)U + 256\,(-4\,\mu^6 + (6\,z^2 + a^2 - 12\,ua + 4\,b)\mu^3 + \\ & (b + a^2)(5\,a^2 + 6\,ua - b - 3\,z^2))\lambda^2;\end{aligned}$$

$$\begin{aligned}Y \;:=\;& (-288\,v(u + a)U - 72\,zV + 1536\,\lambda v(bu + a^3 - 2\,\mu^3 u + ab + a\mu^3 + ua^2))/W;\\ Z \;:=\;& -(-324\,zU^4 + (6912\,\lambda\mu^3 z + 1728\,\lambda z(-3\,z^2 - 2\,b + 6\,ua + 4\,a^2))U^3 - 2592\,v(u + a)U^2 V \\ & +(-27648\,\lambda^2 z(b + a^2)(2\,a^2 + 6\,ua - 4\,b - 3\,z^2) + 193536\,\lambda^2 z\mu^6 \\ & -27648\,\lambda^2 z(-5\,a^2 - 12\,ua + 6\,z^2 + 7\,b)\mu^3)U^2 \\ & +(27648\,\lambda v(-2\,u + a)\mu^3 + 27648\,\lambda v(b + a^2)(u + a))UV \\ & +(49152\,\lambda^3 z(36\,a^3 u - 18\,a^2 z^2 + 12\,a^4 + 9\,z^2 b + 30\,b^2 - 12\,a^2 b - 18\,aub)\mu^3 \\ & +49152\,\lambda^3 z(-6\,b + 18\,ua + 12\,a^2 - 9\,z^2)\mu^6 + 49152\,\lambda^3 z(b + a^2)^2(4\,a^2 + 18\,ua \\ & -14\,b - 9\,z^2) + 196608\,\lambda^3\mu^9 z)U + (-73728\,v\lambda^2(b + a^2)^2(u + a) - 73728\,v\lambda^2(4\,u - 8\,a)\mu^6 \\ & -73728\,v\lambda^2(-4\,bu + 9\,z^2 a - 7\,a^3 - 13\,ua^2 + 2\,ab)\mu^3)V - 7340032\,\lambda^4\mu^{12} z \\ & -262144\,\lambda^4 z(60\,ua - 56\,b + 85\,a^2 - 30\,z^2)\mu^9 \\ & -262144\,\lambda^4 z(b + a^2)(31\,a^4 + 72\,a^3 u - 10\,a^2 b - 36\,a^2 z^2 + 18\,aub + 13\,b^2 - 9\,z^2 b)\mu^3 \\ & -262144\,\lambda^4 z(b + a^2)^3(a^2 + 6\,ua - 5\,b - 3\,z^2) \\ & -262144\,\lambda^4 z(15\,b^2 + 87\,a^4 - 63\,a^2 z^2 + 45\,z^2 b - 90\,aub - 33\,a^2 b + 126\,a^3 u)\mu^6)/W^2;\end{aligned}$$

$S := (-u + a)Y^2\lambda - 4\,vY - 4\,a - 4\,u$; $\Delta := \sqrt[3]{(Z - S)/(\lambda Y^2 - 4)}$;
$x_t := \Delta - \mu/\Delta$; $y_t := \lambda\,(X^3/2 + 3\,\mu X/2 + a - u)\,Y - 2\,v$;
return $(x_t : y_t : 1)$

FIGURE 4.3 – Encodage sur les courbes de genre 2 (de type B).

Théorème 4.2.4 *Soit $\mathbb{F}_q$ le corps fini à q éléments. Supposons q impair et $q \equiv 2 \bmod 3$. Soit $H_{2,\lambda,\mu,a,v,w}/\mathbb{F}_q$ la courbe hyperelliptique de genre 2 definie par l'équation (4.10).*

L'algorithme 4 calcule un encodage déterministe $e_{2,\lambda,\mu,a,v,w} : \mathbb{F}_q^* \setminus \mathcal{S}_2 \to H_{2,\lambda,\mu,a,v,w}$, où $\mathcal{S}_2$ est un sous-ensemble de $\mathbb{F}_q$ de taille au plus 233, avec complexité $\mathcal{O}(\log^{2+o(1)} q)$.

Démonstration Les formules définissent un encodage déterministe pourvu que $t, W, \lambda Y^2 - 4$ et $Z - S$ soient tous non nuls.

La condition $W = 0$ revient à étudier un polynôme en U de degré 2, il existe au plus deux valeurs de U pour lesquelles $W = 0$. Chacune de ces valeurs de U fournit ensuite un polynôme en t dérivé de δ de degré 8. Ainsi, il existe au plus 16 valeurs de t à éviter pour que W soit non nul.

La condition $\lambda Y^2 - 4 = 0$ fournit de même deux valeurs pour Y. Chacune donne une relation polynomiale de degré 2 en U et de degré 1 etn V, qui peut se voir comme une courbe en t et $\tau = \sqrt[3]{2\,t\,\delta}$ de degré au plus 6. Par ailleurs, $\tau^3 = 2\,t\,\delta$ est une courbe de degré au plus 9. Le théorème de Bezout affirme qu'il existe au plus $2 \times 6 \times 9 = 108$ points d'intersection, ou de façon équivalente valeurs de t à éviter pour que $\lambda Y^2 - 4$ soit non nul.

Finalement, la condition $Z = S$ peut être vue comme une courbe en t et τ de degré 12. De la même façon, $12 \times 9 = 108$ valeurs de t sont à éviter également.

Au final, le nombre total d'éléments de $\mathbb{F}_q$ qui ne peuvent pas être encodés est au plus $1 + 16 + 2 \times 108 = 233$. □

Cardinal de l'image. Soit (X, Y) un point rationnel sur $H_{2,\lambda,\mu,a,v,w}$ et t un de ses antécédents par $e_{2,\lambda,\mu,a,v,w}$. Nous avons vu dans la démonstration du théorème 4.2.4 que t et $\tau = \sqrt[3]{2\,t\,\delta}$ sont définis comme les points d'intersection de deux courbes, l'une de degré 7 paramétrée par Y et l'autre de degré 9 d'après la définition de δ. En toute généralité, pour certaines courbes et certains points, cela correspond à un nombre total d'au plus 54 valeurs de t. Ainsi, $|\operatorname{Im} e_{1,a,b}| \geqslant (q - 233)/63$.

Nombre de courbes. Les invariants d'Igusa de ces courbes sont égaux à

$$\begin{aligned}
J_2 &= -2^6\,3\,\lambda^2(9\,\mu^3 + 9\,a^2 + 10\,b)\,,\\
J_4 &= 2^9\,3\,b\lambda^4(297\,\mu^3 + 54\,a^2 + 55\,b)\,,\\
J_6 &= 2^{14}\,b^2\lambda^6(-6480\,\mu^3 + 81\,a^2 + 80\,b)\,,\\
J_8 &= -2^{16}\,3\,b^2\lambda^8(31347\,\mu^6 - 134136\,\mu^3 a^2 - 158310\,b\mu^3 + 11664\,a^4 + 23940\,ba^2 + 12275\,b^2)\,,\\
J_{10} &= -2^{24}\,3^6\,b^3\lambda^{10}(\mu^6 + 2\,\mu^3 a^2 - 2\,b\mu^3 + a^4 + 2\,ba^2 + b^2)\,.
\end{aligned}$$

Le lieu géométrique de ces invariants est une surface de dimension 2 définie par l'équation homogène de degré 30

$$11852352\,{J_2}^5{J_{10}}^2 + 196992\,{J_2}^5 J_4\,J_6\,J_{10} - 362998800\,{J_2}^3 J_4\,{J_{10}}^2 + 64\,{J_2}^6{J_6}^3 - 636672\,{J_2}^4{J_6}^2 J_{10}$$
$$- 895349625\,{J_2}^2 J_6\,{J_{10}}^2 - 64097340625\,{J_{10}}^3 - 373248\,{J_2}^4{J_4}^3 J_{10} - 4466016\,{J_2}^3{J_4}^2 J_6\,J_{10}$$
$$+2903657625\,J_2\,{J_4}^2{J_{10}}^2 - 3984\,{J_2}^4 J_4\,{J_6}^3 + 606810\,{J_2}^2 J_4\,{J_6}^2 J_{10} + 3383973750\,J_4\,J_6\,{J_{10}}^2 + 1647\,{J_2}^3{J_6}^4$$
$$+ 49583475\,J_2\,{J_6}^3 J_{10} + 11290752\,{J_2}^2{J_4}^4 J_{10} + 38072430\,J_2\,{J_4}^3 J_6\,J_{10} + 76593\,{J_2}^2{J_4}^2{J_6}^3$$
$$- 115457700\,{J_4}^2{J_6}^2 J_{10} + 20196\,J_2\,J_4\,{J_6}^4 - 530604\,{J_6}^5 - 85386312\,{J_4}^5 J_{10} - 468512\,{J_4}^3{J_6}^3\,.$$

Ceci montre que l'équation (4.10) définit $\Theta(q^2)$ courbes non isomorphes sur $\mathbb{F}_q$.

Pertinence cryptographique

Génériquement il existe $\Theta(q^3)$ courbes hyperelliptiques de genre 2 définies sur $\mathbb{F}_q$. Nos deux familles de courbes hyperelliptiques obtenues sont de cardinal $\Theta(q^2)$. C'est la même dimension, sur l'espace de modules, que l'espace des courbes hyperelliptiques dont la jacobienne est isogène à un produit de courbes elliptiques. L'intérêt des jacobiennes de courbes hyperelliptiques est justement de pouvoir avoir un sous-groupe premier plus grand que dans le cas des courbes elliptiques pour une taille de corps fini fixée ($\mathcal{O}(q^2)$ contre $\mathcal{O}(q)$) : ce cardinal est le paramètre de sécurité des cryptosystèmes à base de courbes. Il est donc important de s'assurer que nos familles ne sont pas de ce type.

Nous avons testé expérimentalement les cardinaux des jacobiennes de courbes hyperelliptiques issues de nos familles. Il s'avère qu'elles ne sont apparemment jamais de cardinal premier : il semble toujours divisible par 2 ou par 3, ce qui découle vraisemblablement de la forme particulière de leurs équations.

Hormis cet effet, il est possible de trouver des courbes de nos familles pour lesquelles le cardinal du sous-groupe restant est premier et de l'ordre de $q^2/3$. Un simple argument de cardinalité utilisant le théorème de Hasse-Weil ([20] corollaire 5.79) nous assure alors qu'il ne peut pas s'agir du groupe des points d'une courbe elliptique sur $\mathbb{F}_q$: son cardinal est trop élevé.

Exemple : sur $\mathbb{F}_{10973}$, considérons la courbe hyperelliptique d'équation $y^2 = x^6 + 6904x^4 + 1047x^3 + 10599x^2 + 4127x + 4626 = (x^3 + 3452x + 6010)^2 + 7642^2$. Elle est de type 2. Le cardinal de sa jacobienne est $117978387 = 3 \times 39326129$. Or d'après le théorème de Hasse-Weil, une courbe elliptique sur $\mathbb{F}_{10973}$ ne peut avoir qu'au plus 11078 points.

Un argument plus fort consiste à calculer le polynôme L de la courbe. Sur $\mathbb{F}_q$, la jacobienne de la courbe hyperelliptique est un produit de courbes elliptiques seulement si celui-ci se factorise. Nous avons vérifié sur des exemples que le polynôme L est irréductible. Toutefois, nos expériences en ce sens avec des logiciels de calcul

algébriques ont été plus limitées du fait du temps de calcul élevé du polynôme L.

Nous nous sommes enfin assuré que le groupe d'isomorphismes de nos courbes hyperelliptiques est génériquement $\mathbb{Z}_2$: il ne contient que l'involution hyperelliptique.

4.3 Familles de genre supérieur

4.3.1 Polynômes de Moivre

Cette famille de polynômes de degré 5 est bien connue. Elle a été proposée par De Moivre pour l'étude d'égalités trigonométriques. L'étude de ses propriétés galoisiennes a été réalisée par Borger [8]. Cette définition peut facilement se généraliser à tout degré impair.

Définition 4.3.1 (Polynômes de Moivre) *Soit $\mathbb{K}$ un corps et d un entier impair premier avec la caractéristique de $\mathbb{K}$. La famille des polynômes de Moivre $p_{a,b}(x) \in \mathbb{K}[x]$ de degré d est définie pour $a, b \in \mathbb{K}$ par*

$$p_{a,b}(x) = x^d + dax^{d-2} + 2da^2x^{d-4} + 3da^3x^{d-6} + \cdots + 2da^{(d-1)/2-1}x^3 + da^{(d-1)/2}x + b\,.$$

Exemple :

- les polynômes de Moivre de degré 5 sont $x^5 + 5ax^3 + 5a^2x + b$.
- les polynômes de Moivre de degré 13 sont $x^{13} + 13ax^{11} + 26a^2x^9 + 39a^3x^7 + 39a^4x^5 + 26a^5x^3 + 13a^6x + b$.

Borger a prouvé [8] que les polynômes de Moivre de degré 5 sont résolubles par radicaux. C'est vrai également des polynômes de Moivre de degré quelconque.

Lemme 4.3.2 (Résolution des polynômes de Moivre) *Soit $p_{a,b}$ un polynôme de Moivre de degré d, soit θ_0 et θ_1 les racines de $q_{a,b}(\theta) = \theta^2 + b\theta - a^d$, alors les racines de $p_{a,b}$ sont*

$$(\omega_k\theta_0^{1/d} + \omega_k^{d-1}\theta_1^{1/d})_{0\leqslant k<d}$$

où $(\omega_k)_{0\leqslant k<d}$ sont les racines d^e de l'unité.

Démonstration. Comme dans le cas du degré 5 (voir [8]), il faut faire le changement de variable $x = \gamma - a/\gamma$, alors γ^d est une racine du polynôme $q_{a,b}(\theta)$. □

Les polynômes de Moivre définissent également une famille de courbes hyperelliptiques de genre quelconque pour lesquelles il existe un encodage déterministe.

Théorème 4.3.3 *Soit $\mathbb{F}_q$ le corps fini à q éléments. Supposons q impair, $q \equiv 2 \bmod 3$ et d premier avec $q-1$. Soit $H_{a,b}/\mathbb{F}_q : y^2 = p_{a,b}(x)$ une courbe hyperelliptique où $p_{a,b}$ est un polynôme de Moivre défini sur $\mathbb{F}_q$ avec un discriminant non nul. .*

L'algorithme 5 calcule un encodage déterministe $e_{a,b} : \mathbb{F}_q^* \setminus \mathcal{S} \to H_{a,b}$, où $\mathcal{S}$ est un sous-ensemble de $\mathbb{F}_q$ de taille au plus 7, avec complexité $\mathcal{O}(\log^{2+o(1)} q)$.

Algorithme 5: DeMoivreEncode

Entrée : Une courbe $H : p_{a,b}(x) - y^2 = 0$ et $t \in \mathbb{F}_q^* \setminus \mathcal{S}$.
Sortie : Un point $(x_t : y_t : 1)$ sur H

if $a = 0$ **then**
  return $((t^2 - b)^{1/d \bmod q-1} : t : 1)$
$\delta := -(3a^d + b^2 + t^4)/6t - 2\,b^3/27 - a^d b/3 - t^6/27$; $A := \delta^{1/3 \bmod q-1} + t^2/3$;
$Y := tA - (3a^d + b^2 + t^4)/(6t)$;
$\alpha := 3a^d/(-3A + b)$;
$y_t := -3Y/(-3A + b)$; $x_t := \alpha^{1/d \bmod q-1} + (-a^d/\alpha)^{1/d \bmod q-1}$;
return $(x_t : y_t : 1)$

FIGURE 4.4 – Encodage sur les courbes de Moivre

Réciproquement, étant donné un point sur H nous en étudions le nombre d'antécédents par cet encodage.

Théorème 4.3.4 *Étant donné un point $(x : y : 1) \in H_{a,b}(\mathbb{F}_q)$, on peut calculer les solutions s de l'équation $e_{a,b}(s) = (x : y : 1)$ avec complexité $\mathcal{O}(\log^{2+o(1)} q)$. Elle admet au plus 8 solutions.*

Voici les démonstrations de ces deux théorèmes.

Corps finis de caractéristique impaire.

Genre de $H_{a,b}$. Comme dans la section 4.3.2, la courbe n'admet pas de singularité à l'exception du point à l'infini puisque nous imposons que le discriminant de $q_{a,b}$ soit non nul. Le genre de $H_{a,b}$ est donc $(d-1)/2$.

L'encodage. Grâce au lemme 4.3.2, paramétrer des points rationnels sur $H_{a,b}$: $p_{a,b}(x) = y^2$ revient à trouver les racines de $\theta^2 + (b - y^2)\theta - a^d$. Notons les α, α', alors $x = \alpha^{1/d} + \alpha'^{1/d}$, $\alpha\alpha' = -a^d$ et $\alpha + \alpha' = y^2 - b$, donc $\alpha^2 - a^d = \alpha y^2 - b\alpha$. Ceci est une courbe de genre 1 en les variables α, y qui est birationnellement équivalente à $Y^2 = A^3 + (-a^d - \frac{1}{3}b^2)A + \frac{2}{27}b^3 + \frac{1}{3}a^d b$, avec $\alpha = 3a^d/(-3A + b)$ et $y = -3Y/(-3A + b)$.

Cette courbe peut être paramétrer avec les formules d'Icart, ce qui donne $A = \sqrt[3]{\delta} + t^2/3$, $Y = tA - (3a^d + b^2 + t^4)/6t$ où $\delta = (-53a^d + b^2 + t^4)/6t - 2\,b^3/27 - a^d b/3 - t^6/27$. On obtient finalement l'algorithme 5.

Restrictions. Les conditions nécessaires précédentes sont également suffisantes et donnent un encodage pour tout $t \in \mathbb{F}_q$ pourvu que tous les changements de variables soient calculables.

Pour calculer A et Y en utilisant l'encodage d'Icart [38], il faut que $t \neq 0$. Alors pour calculer y et α connaissant A et Y il faut également $-3A + b \neq 0$, c'est-à-dire $\delta \neq (b/3 - t^2/3)^3$. Ceci est une équation de degré 7, au plus 7 éléments de $\mathbb{F}_q$ ne sont pas encodables.

Complexité. Notre fonction d'encodage utilise les formules d'Icart qui ont complexité $\mathcal{O}(\log^{2+o(1)} q)$ opérations dans $\mathbb{F}_q$, deux exponentiations pour calculer les racines d^{e} de l'unité et un nombre constant d'opérations dans $\mathbb{F}_q$. Au final la complexité est $\mathcal{O}(\log^{2+o(1)} q)$.

Calcul de $e_{a,b}^{-1}$. Soit $(x : y : 1)$ un point de $H_{a,b}$. Le polynôme $\beta^2 + x\beta - \sqrt[d]{(-a^d)}$ a au plus deux racines. Soit β l'une et $\alpha = \beta^5$. Soit alors $A = 1 - 3(b\alpha - 3a^d)/\alpha$ et $Y = -ya^d/\alpha$, cela revient à trouver les antécédents d'un encodage d'Icart. Il admet au plus 4 solutions par α, l'équation $e_{a,b}(t) = (x : y : 1)$ admet donc au plus 8 solutions.

Cas du genre 2. Dans ce cas, nous nous intéressons à la dimension de la famille des courbes définies par un polynôme de Moivre de degré 5, $H : y^2 = x^5 + 5ax^3 + 5a^2x + b$. Nous avons calculé leurs invariants d'Igusa,

$$J_2 = 700\,a^2\,,\ J_4 = 13750\,a^4\,,\ J_6 = -2500\,a(3\,a^5 + 32\,b^2)\,,$$
$$J_8 = -15625\,a^3(3109\,a^5 + 896\,b^2)\,,\ J_{10} = 800000\,(4\,a^5 + b^2)^2\,,$$

à partir desquels il est facile de calculer de nombreuses relations algébriques. Ceci réduit l'ensemble des courbes des q^2 attendues (il y a deux paramètres a et b) à un ensemble de cardinal $\Theta(q)$.

Corps finis de caractéristique deux.

Le cas de la caractéristique 2 est similaire. Les polynômes de Moivre sont résolubles grâce au même polynôme auxiliaire. Une famille de dimension 1 de courbes de genre 2 est donnée par $p_{a,b}(x) = y + y^2$, qui sont identiques à $p_{a,b+y+y^2}(x) = 0$. Nous en donnons le principe ci-dessous.

Algorithme 6: DeMoivreEncodeChar2

Entrée : Une courbe $H : p_{a,b}(x) - y - y^2 = 0$ sur $\mathbb{F}_q$ avec q pair et $t \in \mathbb{F}_q^* \setminus \mathcal{S}$.
Sortie : Un point $(x_t : y_t : 1)$ sur H

Mettre la courbe elliptique $E : \alpha^2 + y^2\alpha + b\alpha + a^5 = 0$ sous forme de Weierstrass $\alpha^2 + y\alpha = y^3 + \gamma y + \delta$;
Encoder t sur E grâce aux formules d'Icart et obtenir le point (α_t, y_t);
$x_t := \alpha_t^{(1/\deg p) \bmod q-1} + a/\alpha_t^{(1/\deg p) \bmod q-1}$;
return $(x_t : y_t : 1)$.

FIGURE 4.5 – Encodage sur les courbes de Moivre en caractéristique paire.

Théorème 4.3.5 *Soit $\mathbb{F}_q$ le corps fini à q éléments. Supposons q pair, $q \equiv 2 \mod 3$ et soit d impair premier avec $q - 1$. Soit $H_{a,b}/\mathbb{F}_q : y^2 + y = p_{a,b}(x)$ une courbe*

hyperelliptique, où $p_{a,b}$ est un polynôme de Moivre défini sur $\mathbb{F}_q$ de discriminant non nul.

L'algorithme 6 calcule un encodage déterministe $e_{a,b} : \mathbb{F}_q^* \setminus \mathcal{S} \to H_{a,b}$, où $\mathcal{S}$ est un sous-ensemble de $\mathbb{F}_q$ de taille au plus 12, avec complexité $\mathcal{O}(\log^{2+o(1)} q)$.

Démonstration Rappelons que $H : p_{a,b}(x) - y - y^2 = 0$. On considère l'équation auxiliaire $\theta^2 + (b - y - y^2)\theta + a^d = 0$. Soit α_0 une racine, la deuxième est $\alpha_1 = a^d/\alpha_0$. Supposons α_0 paramétrée, alors l'unique racine du polynôme de Moivre $p_{a,b-y-y^2}$ est $x = \sqrt[5]{\alpha_0} + \sqrt[5]{\alpha_1}$. Nous sommes ramenés à paramétrer y et α_0.

Remarquons que $b - y - y^2 = \alpha_0 + \alpha_1$. Ceci implique que y et α_0 sont sur la courbe de genre 1 $E : \alpha_0^2 + y^2\alpha_0 + b\alpha_0 + a^5 = 0$. On peut paramétrer cette courbe grâce aux formules d'Icart [38]. □

4.3.2 Polynômes *quasi-quadratiques*

Les courbes de la forme $y^2 = f(x^d)$ où f est une famille de polynômes résolubles quel que soit leur coefficient constant peuvent donner des courbes hyperelliptiques paramétrables. Typiquement, on peut considérer les polynômes f de degré 2, 3 ou 4 ou des familles de polynômes de degré supérieur. Ici, nous nous restreignons aux polynômes quadratiques qui donnent déjà d'autres familles de courbes hyperelliptiques non triviales.

Nous définissons les polynômes quasi-quadratiques comme suit.

Définition 4.3.6 (Polynômes quasi-quadratiques) *Soit $\mathbb{K}$ un corps et d un entier premier avec la caractéristique de $\mathbb{K}$. La famille des polynômes quasi-quadratiques $q_{a,b}(x) \in \mathbb{K}[x]$ de degré $2d$ est définie pour $a, b \in \mathbb{K}$ par $q_{a,b}(x) = x^{2d} + ax^d + b$.*

Les polynômes quasi-quadratiques définissent une famille de courbes hyperelliptiques $y^2 = q_{a,b}(x)$ qu'il est facile de paramétrer (algorithme 7). Quand d est premier avec $q - 1$ et quand $a \neq 0$, ces courbes sont isomorphes aux courbes $y^2 = q_{1,a}(x)$ par le changement de variable $x \to a^{1/d}x$. Quand $a = 0$, on est ramené à la courbe unique $y^2 = x^{2d} + b$, qu'on peut paramétrer par $t \mapsto \left(\sqrt[d]{(-b + t^2)/(2t)}, (b + t^2)/(2t)\right)$.

Algorithme 7: QuasiQuadraticEncode

Entrée : Une courbe $H_a : x^{2d} + x^d + a = y^2$, et $t \in \mathbb{F}_q \setminus \{1/2\}$.
Sortie : Un point $(x_t : y_t : 1)$ on H_a

$\alpha := (t^2 - a)/(1 - 2\,t)$;
$x_t := \alpha^{1/d}$; $y_t := (-a + t - t^2)/(1 - 2\,t)$;
return $(x_t : y_t : 1)$

FIGURE 4.6 – Encodage vers une courbe quasi-quadratique

Théorème 4.3.7 *Soit $\mathbb{F}_q$ le corps fini à q éléments. Supposons q impair, $q \neq 2, 3$ et d premier avec $q-1$. Soit $H_a/\mathbb{F}_q : y^2 = x^{2d} + x^d + a$ une courbe hyperelliptique où a est tel que le polynôme quasi-quadratique $q_{1,a}$ a un discriminant non nul sur $\mathbb{F}_q$.*

L'algorithme 7 calcule un encodage déterministe $e_a : \mathbb{F}_q^* \setminus \{1/2\} \to H_a$ avec complexité $\mathcal{O}(\log^{2+o(1)} q)$.

Genre de H_a. Soient $q_{1,a} \in \mathbb{F}_q[X]$ et $H_a : q_{1,a}(x) = y^2$, où $q_{1,a}$ est de degré $2d$. Nous avons imposé que le discriminant de $q_{1,a}$ soit non nul. Ceci implique que $q_{1,a}$ a exactement $2d$ racines distinctes. H_a est donc de genre $d-1$ pourvu que H_a n'ait pas de singularité à l'exception du point à l'infini.

Étudions les points de la courbe où les deux dérivées en x et y sont simultanément nulles. Ceci implique $y = 0$. Les seuls points singuliers sont donc les racines communes de $q_{1,a}(x)$ et son polynôme dérivé. Comme le discriminant de $q_{1,a}$ est non nul, il n'y a pas de point singulier.

Pour $d = 3$, H_a est la famille de courbes de genre 2 avec groupe d'automorphismes D_{12} [17]. Le lieu géométrique de ces courbes est une quasi-variété de dimension 1 sur l'espace des modules. De plus, quand $x \to x^d$ est inversible sur $\mathbb{F}_q$, ces courbes ont toutes exactement $q+1$ $\mathbb{F}_q$-points (mais le nombre de $\mathbb{F}_{q^2}$-points est bien mieux distribué).

Encodage. La paramétrisation est simple. Soit $H_a : x^{2d} + x^d + a = y^2$ une courbe hyperelliptique quasi-quadratique. Poser $x = \alpha^{1/d}$ ramène la paramétrisation de H_a à celle de la conique $\alpha^2 + \alpha + a - y^2 = 0$, qui donne $\alpha = (-a + t^2)/(1 - 2\,t)$ et $y = (-a + t - t^2)/(1 - 2\,t)$ pour un paramètre t. On obtient finalement l'algorithme 7.

Cardinal de l'image.

Théorème 4.3.8 *Étant donné un point rationnel $(x : y : 1)$ sur $H_a : q_{1,a}(x) = y^2$, l'équation $e_a(t) = (x : y : 1)$ a exactement une solution. Ainsi $|\operatorname{Im} e_a| = q - 1$*

Démonstration Soit $\alpha = x^d$, alors t est une solution de l'équation de degré 1 $y + \alpha = ta/(a - 2t)$. □

Chapitre 5

Hachage vers courbes elliptiques : Approche géométrique

Beaucoup de fonctions d'encodage ont été proposées pour le genre 1, par Icart, Farashahi et dans le précédent chapitre nous-mêmes. Elles utilisent toutes l'inversibilité de la fonction cube (c'est-à-dire l'existence d'une racine cubique) et la résolution de certaines équations de degré trois. Il est naturel de chercher à les unifier, à réaliser une classification "complète" des fonctions d'encodage de ce type. C'est l'objet de ce chapitre, qui a donné lieu à publication [23] en collaboration avec J-M. Couveignes.

5.1 Introduction

Trouver ces encodages est un cas particulier du problème consistant à trouver des paramétrisations des courbes par radicaux [62]. Il s'agit de paramétrisations d'une courbe elliptique $\mathcal{C}$ par des radicaux cubiques. Le terme de paramétrisation est quelque peu abusif, puisque les encodages trouvés, satisfaisant les applications cryptographiques, se contentent de paramétrer une partie seulement de $\mathcal{C}$.

Les fonctions d'encodage algébriques connues ([38, 45, 29]) vers une courbe elliptique $\mathcal{C}$ se permettent d'utiliser les opérations de corps usuelles et les racines cubiques : dans le corps fini $\mathbb{F}_q$, tout élément admet une (et une seule) racine cubique si et seulement si $q \equiv 2 \mod 3$.

Contrairement aux deux chapitres ci-dessus, nous nous plaçons cette fois dans le cadre des courbes dans le plan projectif $\mathbb{P}$ sur un corps $\mathbb{K}$. Dans ce chapitre, nous montrons comment certaines des pseudo-paramétrisations présentées aux chapitres 3 et 4, ainsi que de nombreuses autres, se déduisent de l'étude de la courbe duale de $\mathcal{C}$. Ces courbes ont été introduites par Plücker en 1830 [1].

Pour résumer, les points de $\mathcal{C}$ sont calculés comme des points d'intersection de $\mathcal{C}$ et des droites bien choisies. Si D est une droite dans le plan projectif, l'intersection $D.\mathcal{C}$ est formée de trois points, comptés avec multiplicité. Ces trois points peuvent

être calculés en résolvant une équation cubique.

Dans la section 5.2, nous rappelons comment utiliser pour ce faire les formules de Cardan-Tartaglia pour la résolution des polynômes de degré 3. Ces formules se décomposent en deux étapes : premièrement, il faut calculer une racine carrée du discriminant de l'équation. Les trois solutions se calculent en utilisant les opérations de corps et des racines cubiques. Comme les racines cubiques ne posent pas de problème dans notre contexte, la seule difficulté consiste en le calcul d'une racine carrée du discriminant. Nous choisissons donc la droite D de telle sorte que le discriminant de l'intersection $D.\mathcal{C}$ soit toujours un carré, et nous nous assurons d'avoir une formule algébrique directe pour une de ses racines carrées (le but étant qu'il en existe toujours une, de manière déterministe).

Plus précisément, nous considérons une droite D_t qui dépend d'un paramètre rationnel formel t, c'est-à-dire que les coefficients de l'équation (projective) de D_t sont des polynômes en t. Le discriminant Δ_t de l'intersection $D_t.\mathcal{C}$ est une fraction rationnelle en t. Nous cherchons à ce que ce discriminant soit un carré dans $\mathbb{K}(t)$. Nous calculons alors une fois pour toutes une racine carrée formelle δ_t de Δ_t. Pour toute valeur de t, on peut alors calculer un point sur $\mathcal{C}$ à l'aide seulement des opérations de corps dans $\mathbb{K}$ et de la racine cubique.

Nous rappelons dans la section 5.3 que les droites projectives dans $\mathbb{P}$ sont paramétrées dans le plan dual $\hat{\mathbb{P}}$. Une droite D dans $\mathbb{P}$ d'équation projective $UX+VY+WZ=0$ est représentée par le point $(U:V:W)$ dans $\hat{\mathbb{P}}$. Une famille rationnelle de droites $t \mapsto D_t$ fournit une courbe rationnelle $\mathcal{L}$ dans $\hat{\mathbb{P}}$. En effet, si l'équation projective de D_t est $U(t)X+V(t)Y+W(t)Z=0$, la fonction $t \mapsto \big(U(t):V(t):W(t)\big)$ paramètre une courbe rationnelle dans $\hat{\mathbb{P}}$. Le discriminant Δ_t est nul quand l'équation définissant $D_t.\mathcal{C}$ a une racine multiple. C'est le cas si et seulement si D_t est *tangente* à $\mathcal{C}$. Une droite projective n'est pas toujours tangente à $\mathcal{C}$. Toutefois les tangentes à $\mathcal{C}$ forment une courbe particulière dans $\hat{\mathbb{P}}$. Informellement, le sous-ensemble de $\hat{\mathbb{P}}$ qui correspond aux droites tangentes à $\mathcal{C}$ est appelée *courbe duale de* $\mathcal{C}$. C'est une courbe, notée $\hat{\mathcal{C}}$.

Ainsi, Δ_t décrit l'intersection entre $\mathcal{L}$ et la courbe duale $\hat{\mathcal{C}}$, et Δ_t est un carré si et seulement si tout point de l'intersection de $\mathcal{L}$ et $\hat{\mathcal{C}}$ est de multiplicité paire. Nous sommes donc intéressés par les courbes rationnelles $\mathcal{L}$ de $\hat{\mathbb{P}}$ qui ont une intersection paire avec la courbe duale de $\mathcal{C}$. La connexion entre ces courbes et les pseudo-paramétrisations est détaillée dans la section 5.4.

Comme la courbe duale $\hat{\mathcal{C}}$ joue un rôle si important, nous l'étudierons dans la section 5.3. Cette courbe est de genre 1 et a 9 singularités en général, qui sont toutes des points de rebroussement. Ces 9 points de rebroussement correspondent aux 9 tangentes à $\mathcal{C}$ en ses points d'inflexion, où la tangente "traverse" la courbe et "repart" dans l'autre sens. Les points réguliers de $\hat{\mathcal{C}}$ correspondent aux tangentes à $\mathcal{C}$ aux points qui ne sont pas d'inflexion. Ces neufs points de rebroussement ont une

configuration intéressante dans le plan dual, que nous étudions à la section 5.5.

Comme nous cherchons des courbes rationnelles $\mathcal{L}$ de multiplicité d'intersection avec $\hat{\mathcal{C}}$ paire, il est naturel de chercher à faire passer $\mathcal{L}$ par ces neuf points : génériquement, l'intersection avec $\hat{\mathcal{C}}$ est alors de multiplicité égale au degré de la singularité, c'est-à-dire 2. Nous pourrons montrer à la section 5.6 que les encodages de $\mathcal{C}$ présentés ci-dessus, et de nombreux autres, en dérivent.

Il sera alors naturel de se demander combien de courbes rationnelles dans $\hat{\mathbb{P}}$ sont d'intersection paire avec $\hat{\mathcal{C}}$. Nous verrons à la section 5.7 qu'il y en a une infinité, qui donnent une infinité de pseudo-paramétrisations équivalentes. Ces courbes se remontent sur le recouvrement Σ de degré 2 du plan dual ramifié sur $\hat{\mathcal{C}}$. Cela nous amènera au sujet classique des courbes rationnelles sur les surfaces $K3$.

Les résultats de cette partie sont énoncés dans le cadre des corps finis mais se généralisent sans problème à tout corps $\mathbb{K}$ de caractéristique différente de 2 et 3. Soit $\bar{\mathbb{K}}$ une clôture algébrique de $\mathbb{K}$ et $\zeta_3 \in \bar{\mathbb{K}}$ une racine cubique primitive de l'unité. Nous posons $\sqrt{-3} = 2\zeta_3 + 1$.

Le code Maple pour les calculs de ce chapitre se trouve à l'annexe A.

5.2 Résolution des équations de degré 3

Dans cette section, nous réétudions les formules de Cardan-Tartaglia pour la résolution des équations cubiques par radicaux. On peut en trouver un traitement moderne dans [27].

Il est utile de décrire ces équations sous une forme non ambiguë qui soit adaptée à notre contexte, et n'utilise pas trop de radicaux ni de racines de l'unité. Il nous faut en d'autres termes des formules génériques et régulières.

Soit $h(x) = x^3 - s_1x^2 + s_2x - s_3$ un polynôme de degré 3 séparable dans $\mathbb{K}[x]$. Soit r_0, r_1 et r_2 les trois racines de $h(x)$ dans $\bar{\mathbb{K}}$. Soit

$$\delta = \sqrt{-3}(r_1 - r_0)(r_2 - r_1)(r_0 - r_2)$$

et $\Delta = \delta^2$. Remarquons que Δ est le discriminant usuel multiplié par -3. Nous l'appelons son *discriminant réduit*. Comme c'est une fonction symétrique des racines, il s'exprime comme un polynôme en s_1, s_2 et s_3. En effet,

$$\Delta = 81s_3^2 - 54s_3s_1s_2 - 3s_1^2s_2^2 + 12s_1^3s_3 + 12s_2^3.$$

En particulier Δ appartient à $\mathbb{K}$. Soit $\mathbb{L} = \mathbb{K}(\zeta_3, \delta) \subset \bar{\mathbb{K}}$ le corps obtenu en ajoutant δ et une racine cubique primitive de l'unité à $\mathbb{K}$. Soit $\mathbb{M} = \mathbb{L}(r_1, r_2, r_0)$.

Si l'extension $\mathbb{L} \subset \mathbb{M}$ est non triviale, c'est alors nécessairement une extension cyclique cubique. En effet, r_1, r_2 et r_0 sont de degré au plus 3 sur $\mathbb{K}$ et donc sur $\mathbb{L}$. De plus $\mathbb{L}$ contient une racine cubique primitive de l'unité, l'extension $\mathbb{L} \subset \mathbb{M}$ est

donc une extension de Kummer : elle est générée par la racine cubique d'un élément de $\mathbb{L}$. Soit σ le générateur du groupe de Galois de l'extension $\mathbb{L} : \mathbb{K}$ qui envoie r_i sur r_{i+1} pour $i \in \{0, 1, 2\}$, avec la convention que les indices sont pris modulo 3. Posons

$$\rho = r_0 + \zeta_3^{-1} r_1 + \zeta_3^{-2} r_2.$$

On vérifie que $\sigma(\rho) = \zeta_3 \rho$. Posons $R = \rho^3$, alors R est invariant sous l'action de σ. R est par construction invariant sous l'action du groupe alterné sur $\{r_0, r_1, r_2\}$ et il s'exprime comme un polynôme en s_1, s_2, s_3 et δ. En effet, on trouve

$$R = \rho^3 = s_1^3 + \frac{27}{2} s_3 - \frac{9}{2} s_1 s_2 - \frac{3}{2} \delta.$$

De façon similaire, on pose

$$\rho' = r_0 + \zeta_3 r_1 + \zeta_3^2 r_2$$

et on vérifie que

$$R' = \rho'^3 = s_1^3 + \frac{27}{2} s_3 - \frac{9}{2} s_1 s_2 + \frac{3}{2} \delta.$$

Notons que $\rho\rho' = r_0^2 + r_1^2 + r_2^2 - r_0 r_1 - r_1 r_2 - r_2 r_0$ est invariant sous l'action du groupe symétrique complet et est en fait égal à $s_1^2 - 3 s_2$. Ainsi ρ et ρ' se calculent tous deux en extrayant une même racine cubique.

Finalement, les trois racines r_0, r_1, r_2 s'expriment en fonction de ρ en résolvant le système linéaire suivant :

$$\begin{cases} r_0 + r_1 + r_2 &= s_1 \\ r_0 + \zeta_3^{-1} r_1 + \zeta_3 r_2 &= \rho \\ r_0 + \zeta_3 r_1 + \zeta_3^{-1} r_2 &= \rho' \end{cases}$$

En particulier, la formule de la racine

$$r_0 = \frac{s_1 + \rho + \rho'}{3} \tag{5.1}$$

ne fait pas intervenir ζ_3.

5.3 Duale d'une cubique

5.3.1 Définitions

Dans cette section, nous revoyons les propriétés de la courbe duale d'une courbe de degré 3. Un traitement approfondi de ce sujet se trouve dans [34], [37] et [36].

Soit $E = \mathbb{K}^3$ et soit $\hat{E}$ l'espace dual de E. Soit $U = (1,0,0)$, $V = (0,1,0)$ et $W = (0,0,1)$. Alors (U,V,W) est la base canonique de E. Soit (X,Y,Z) la base duale de (U,V,W). Soit $\mathbb{P} = \mathrm{Proj}(E) = \mathrm{Proj}\,\mathbb{K}[X,Y,Z]$ le plan projectif sur $\mathbb{K}$. Soit $\hat{\mathbb{P}} = \mathrm{Proj}(\hat{E}) = \mathrm{Proj}\,\mathbb{K}[U,V,W]$ le dual du plan projectif. L'idée principale de la dualité projective est que les points de $\hat{\mathbb{P}}$ paramètrent des lignes dans $\mathbb{P}$, et réciproquement. Le point $(U : V : W)$ de $\hat{\mathbb{P}}$ correspond à la droite d'équation $UX + VY + WZ = 0$ de $\mathbb{P}$. Réciproquement le point $(X : Y : Z)$ de $\mathbb{P}$ paramètre la droite $XU + YV + ZW = 0$ dans $\hat{\mathbb{P}}$.

Définissons maintenant la courbe duale.

Définition 5.3.1 *Soit $\mathcal{C} \subset \mathbb{P}$ une courbe irréductible d'équation $F(X,Y,Z) = 0$. Soient $F_X = \frac{\partial F}{\partial X}$, $F_Y = \frac{\partial F}{\partial Y}$, $F_Z = \frac{\partial F}{\partial Z}$ les trois dérivées partielles de F. La tangente à $\mathcal{C}$ en un point régulier $P = (X_P : Y_P, Z_P)$ a pour équation*

$$F_X(X_P,Y_P,Z_P)U + F_Y(X_P,Y_P,Z_P)V + F_Z(X_P,Y_P,Z_P)W = 0.$$

Le point correspondant dans $\hat{\mathbb{P}}$ est $(F_X(X_P,Y_P,Z_P) : F_Y(X_P,Y_P,Z_P) : F_Z(X_P,Y_P,Z_P))$. La clôture de Zariski de l'ensemble de tous ces points est la courbe duale *$\hat{\mathcal{C}}$ de C. $\hat{\mathcal{C}}$ est donc la clôture de l'image des morphismes de Gauss*

$$\omega_{\mathcal{C}} : \qquad \mathcal{C}^{smo} \longrightarrow \hat{\mathbb{P}}$$

$$(X : Y : Z) \longmapsto \big(F_X(X,Y,Z), F_Y(X,Y,Z), F_Z(X,Y,Z)\big),$$

où $\mathcal{C}^{smo}$ est le lieu géométrique des points réguliers de $\mathcal{C}$.

Nous supposons que la caractéristique de $\mathbb{K}$ est impaire et que $\mathcal{C}$ n'est pas constituée uniquement de points d'inflexion ou de singularité (en particulier, $\mathcal{C}$ n'est pas une droite). Alors $\hat{\mathcal{C}}$ est une courbe irréductible.

La dualité est une notion réciproque ([37, Théorème 5.91]) :

Théorème 5.3.2 (Bidualité) *La duale de $\hat{\mathcal{C}}$ est $\mathcal{C}$.*

Ainsi la dualité est une notion très utile : les propriétés de $\mathcal{C}$ se traduisent en des propriétés sur $\hat{\mathcal{C}}$ et réciproquement. En particulier, le morphisme de Gauss $\omega_{\mathcal{C}}$ est un morphisme birationnel de $\mathcal{C}$ sur $\hat{\mathcal{C}}$. Il envoie les points d'inflexion de $\mathcal{C}$ sur les points de rebroussement de $\hat{\mathcal{C}}$.

Exemple : l'exemple de dualité non trivial le plus simple consiste en les coniques, c'est-à-dire les courbes planes projectives de degré 2. La duale d'une conique est une conique.

5.3.2 Propriétés

Propriété 5.3.3 *Supposons que $\mathcal{C}$ est une cubique non singulière. Alors $\hat{\mathcal{C}}$ est de degré 6, et a exactement 9 singularités comptées avec multiplicité.*

Démonstration Comme $\mathcal{C}$ est non singulière, elle n'a pas de point de singularité. Le théorème 2.2.10 permet de déduire que $\mathcal{C}$ est de genre (géométrique) 1 donc, les morphismes de Gauss étant birationnels, $\hat{\mathcal{C}}$ est de genre (géométrique) 1.

Par ailleurs, comme $\mathcal{C}$ n'a pas de points de singularité, $\hat{\mathcal{C}}$ est de degré 6 d'après la première formule de Plücker ([1] p 63).

$\hat{\mathcal{C}}$ est par ailleurs de genre arithmétique (lié au degré) $10 = (6-1)(6-2)/2$. Ceci prouve qu'elle possède au plus 9 points de singularité d'après le théorème 2.2.10. □

Exemple : Si $\mathcal{C}$ est la courbe hessienne d'équation $F(X,Y,Z) = 0$ où

$$F(X,Y,Z) = X^3 + Y^3 + Z^3 - 3aXYZ, \tag{5.2}$$

alors sa courbe duale a pour équation $G(U,V,W) = 0$ où

$$\begin{aligned} G(U,V,W) = U^6 + V^6 + W^6 - 6a^2(U^4VW + UV^4W + UVW^4) \\ +(4a^3 - 2)(U^3V^3 + U^3W^3 + V^3W^3) + (12a - 3a^4)U^2V^2W^2. \end{aligned} \tag{5.3}$$

5.3.3 Calcul

On peut calculer l'équation de $\hat{\mathcal{C}}$ en éliminant X, Y et Z du système suivant :

$$\begin{cases} U &= F_X(X,Y,Z) \\ V &= F_Y(X,Y,Z) \\ W &= F_Z(X,Y,Z) \\ 0 &= F(X,Y,Z) \end{cases}$$

Chacune des trois premières équations est de degré 2 et la dernière de degré 3. On peut calculer l'équation de la duale grâce aux premières lignes de code de la section A.1, qui résout le système avec un algorithme de calcul de base de Gröbner.

Le lieu géométrique affine réel de deux courbes $\mathcal{C}$ et $\hat{\mathcal{C}}$ est représenté dans la figure 5.1, dans le cas où $a = 0$.

L'équation de la courbe duale intervient naturellement quand on étudie l'intersection de la cubique $\mathcal{C}$ avec une droite projective D. En effet, une telle droite $D \subset \mathbb{P}$ coupe $\mathcal{C}$ en exactement trois points à moins que D soit tangente à $\mathcal{C}$ (auquel cas on a un point de multiplicité 1, simple, et un point double) ou même que D soit tangente à $\mathcal{C}$ en un point d'inflexion (auquel cas l'intersection est réduite à un unique point

FIGURE 5.1 – $\mathcal{C} : X^3 + Y^3 + Z^3 = 0$ (à gauche) ; $\hat{\mathcal{C}} : U^6 + V^6 + W^6 - 2U^3V^3 - 2V^3W^3 - 2U^3W^3 = 0$

triple). Supposons que D est la droite d'équation

$$UX + VY + WZ = 0. \tag{5.4}$$

L'intersection $D.\mathcal{C}$ est décrite par le système homogène constitué de l'équation (5.4) et de l'équation de la cubique $\mathcal{C}$. L'équation de la droite (5.4) peut servir à éliminer l'une des trois variables X, Y, Z de l'équation de $\mathcal{C}$. On obtient ainsi une forme binaire cubique homogène en les deux variables restantes, dont le discriminant réduit $\Delta(U, V, W)$ est l'équation de la courbe duale $\hat{\mathcal{C}}$ (en fait, son carré). En effet, le discriminant s'annule exactement là où l'intersection $D.\mathcal{C}$ a multiplicité strictement supérieure à 1, c'est-à-dire (vu que $\mathcal{C}$ est non singulière) quand D est tangente à $\mathcal{C}$. Or d'après le théorème de Bezout ([32], section 5.3), la multiplicité d'intersection d'une droite avec $\mathcal{C}$ est au plus 3. $\mathcal{C}$ a donc multiplicité d'intersection 3 avec D uniquement quand D est tangente à $\mathcal{C}$ en ses points d'inflexions. En ces points (au nombre de 9), la racine de la forme binaire cubique homogène décrivant l'intersection $D.\mathcal{C}$ est triple et son discriminant est donc nul avec multiplicité au moins 2, ce qui signifie que $\hat{\mathcal{C}}$ y est singulière. Ainsi on a démontré la propriété suivante :

Propriété 5.3.4 *À chacun des neuf points d'inflexion de $\mathcal{C}$ correspond un point de singularité de $\hat{\mathcal{C}}$.*

Ces points de singularités ne peuvent pas être des points doubles : un point double de $\hat{\mathcal{C}}$ signifierait qu'il existe une tangente D à $\mathcal{C}$ qui lui est tangente en deux points distincts. $D.\mathcal{C}$ serait donc de degré 4, ce qui n'est pas possible d'après le théorème de Bezout.

Ainsi, on a démontré la propriété suivante :

Propriété 5.3.5 *À chacun des neuf points d'inflexion de $\mathcal{C}$ correspond un point de rebroussement de première espèce de $\hat{\mathcal{C}}$.*

$\hat{\mathcal{C}}$ n'a pas d'autre points de singularité que ces neuf points.

5.4 Pseudo-paramétrisations

5.4.1 Définition

Définition 5.4.1 *Soit $\mathcal{C}$ une courbe irréductible plane projective sur le corps $\mathbb{K}$. Une* paramétrisation *de $\mathcal{C}$ est une fonction non constante de $\mathbb{P}^1$ sur $\mathcal{C}$.*

Concrètement, à tout paramètre t on associe un point $P = \big(X(t) : Y(t) : Z(t)\big)$ sur $\mathcal{C}$, les trois coordonnées étant des polynômes dans $\mathbb{K}[t]$.

Il est bien connu (*cf* section 3.1.1) qu'une condition nécessaire pour qu'une telle paramétrisation existe est que $\mathcal{C}$ soit de genre (géométrique) 0. En particulier ce n'est jamais possible pour une courbe elliptique. On peut relâcher la condition que les coordonnées $X(t), Y(t)$ et $Z(t)$ soient des polynômes en t et les autoriser à être des fonctions algébriques plus générales. Typiquement, on pourrait exiger que $X(t), Y(t)$ et $Z(t)$ appartiennent à une extension radicale de $\mathbb{K}(t)$. En d'autres termes, il s'agirait alors de fonctions rationnelles en t et $\sqrt[e]{R(t)}$ pour un entier positif e et une fonction rationnelle $R(t) \in \mathbb{K}(t)$.

5.4.2 Pseudo-paramétrisation des cubiques

Comme précisé dans l'introduction de ce chapitre, nous allons nous intéresser au cas où $\mathcal{C}$ est une cubique lisse, $\mathbb{K}$ un corps de caractéristique différente de 2 et de 3 et $e = 3$. Nous voulons paramétrer des cubiques planes par radicaux. Une telle paramétrisation sera appelée *pseudo-paramétrisation* pour éviter toute confusion avec une paramétrisation rationnelle, qui ne peut pas exister pour une courbe de genre 1.

Nous supposerons que l'ensemble des points $\mathbb{K}$-rationnels de $\mathcal{C}$ est non vide. Ce n'est pas une restriction quand $\mathbb{K}$ est un corps fini, et n'en est jamais une pour les courbes elliptiques (cf la définition 2.3.2). Nous supposerons en outre que $\mathcal{C}$ a un point d'inflexion $\mathbb{K}$-rationnel. Ce n'est pas non plus une restriction : toute cubique avec un point rationnel est $\mathbb{K}$-isomorphe à une cubique plane avec un point d'inflexion rationnel (on peut prendre le point à l'infini dans un modèle de Weierstrass, cf section 2.3.2).

Nous avons esquissé dans l'introduction de ce chapitre comment nous pouvons trouver des pseudo-paramétrisations. Nous considérons une droite

$$D_t : U(t)X + V(t)Y + W(t)Z = 0$$

dans $\mathbb{P}$, qui dépend d'un paramètre rationnel t. Comme toute droite de $\mathbb{P}$ correspond à un point dans le plan dual $\hat{\mathbb{P}}$, on peut associer à la famille D_t une courbe rationnelle

$\mathcal{L} \subset \hat{\mathbb{P}}$ qui est l'image de l'application

$$\mu : t \mapsto \big(U(t) : V(t) : W(t)\big). \tag{5.5}$$

Nous avons vu dans la section 5.3 que l'intersection $D_t.\mathcal{C}$ est décrite par une forme cubique dont le discriminant réduit $\Delta(t)$ est, à un facteur carré près, égal à $G\big(U(t), V(t), W(t)\big)$ où $G(U, V, W) = 0$ est l'équation projective de la duale $\hat{\mathcal{C}}$. Nous recherchons donc des polynômes $U(t)$, $V(t)$ et $W(t)$ tels que $G(U(t), V(t), W(t))$ est un carré dans $k(t)$.

Une interprétation géométrique de cette condition est que la courbe rationnelle $\mathcal{L}$ coupe la duale $\hat{\mathcal{C}}$ avec multiplicité toujours paire. Plus précisément, l'image réciproque de $\hat{\mathcal{C}}$ par μ doit être un diviseur sur $\mathbb{P}^1$ de multiplicités toutes paires, c'est-à-dire que tous les paramètres t_i qui interviennent dans l'intersection de $\mathcal{L}$ et $\hat{\mathcal{C}}$ soient de multiplicité paire. Nous recherchons donc une courbe rationnelle $\mathcal{L} \subset \hat{\mathbb{P}}$ et une fonction rationnelle $\mu : \mathbb{P}^1 \to \mathcal{L}$ qui possèdent cette propriété.

5.4.3 Réciproque : exhaustivité des paramétrisations obtenues

On peut se demander si on obtient ainsi toutes les pseudo-paramétrisations par radicaux d'ordre $e = 3$. C'est en effet le cas : toute pseudo-paramétrisation est en fait la paramétrisation d'une famille de droites et de son intersection avec $\mathcal{C}$.

Théorème 5.4.2 *Soit $\mathcal{C}$ une cubique définie sur $\mathbb{K}$ avec un point rationnel et $t \mapsto P_t$ une pseudo-paramétrisation de $\mathcal{C}$.*

Alors il existe une famille de droites $t \mapsto D_t$ telle que pour tout t, $P_t = D_t.\mathcal{C}$.

Démonstration Une pseudo-paramétrisation (par radicaux d'indice 3) $t \mapsto P_t$ est une application surjective d'un recouvrement cyclique de degré $e = 3$ de $\mathbb{P}^1$ sur $\mathcal{C}$. Ainsi P_t a deux points conjugués P'_t et P''_t. Comme $\mathcal{C}$ a un point d'inflexion rationnel O, nous avons une loi de groupe (*cf* ci-dessus 2.3.4), notée $\oplus$. On considère la somme $Q_t = P_t \oplus P'_t \oplus P''_t$. C'est un point de $\mathcal{C}$ si on la considère définie sur $\mathbb{K}(t)$, ou de façon équivalente une fonction rationnelle $t \mapsto Q_t$. Nous avons vu qu'une telle fonction doit être constante puisque $\mathcal{C}$ est de genre 1. Donc $P_t \oplus P'_t \oplus P''_t$ est un point constant $A \in \mathcal{C}_{\mathbb{K}}$. Si A est l'origine (le point à l'infini) O, alors pour toute valeur du paramètre t les trois points P_t, P'_t et P''_t sont colinéaires. Ils sont donc sur une même droite D_t d'équation $U(t)X + V(t)Y + W(t)Z = 0$ où $U(t)$, $V(t)$, $W(t)$ sont des polynômes de $\mathbb{K}[t]$. La pseudo-paramétrisation $t \mapsto P_t$ est donc du type étudié ci-dessus.

Si A n'est pas O, on peut chercher un point $B \in \mathcal{C}(\mathbb{K})$ tel que $B \oplus B \oplus B = A$. Un tel point existe toujours si $\mathbb{K}$ est un corps fini et $\operatorname{card}\mathcal{C}(\mathbb{K})$ n'est pas divisible par 3. Alors on pose $R_t = P_t \ominus B$ et vérifie que $R_t \oplus R'_t \oplus R''_t = O$ La pseudo-paramétrisation

$t \mapsto P_t$ est donc du même type que celle étudiée ci-dessus, à une translation par un facteur constant près : dans le cas général, on pose $R_t = P_t \oplus P_t \oplus P_t \ominus A$ et on vérifie que $R_t + R'_t + R''_t = O$. Alors $t \mapsto P_t$ convient, à une translation et une isogénie de multiplication par 3 (rationnelle) près. □

5.4.4 Pseudo-paramétrisations équivalentes

Définition 5.4.3 *On dit que deux pseudo-paramétrisations $t \mapsto P_t$ et $t \mapsto Q_t$ sont* équivalentes *s'il existe une fraction birationnelle $\phi(t)$ telle que $Q_t = P_{\phi(t)}$.*

On peut se demander si deux familles de droites projectives $t \mapsto D_t$ et $t \mapsto E_t$ peuvent donner deux pseudo-paramétrisations équivalentes $t \mapsto P_t$ et $t \mapsto Q_t$. Le théorème suivant montre qu'alors les deux familles de droites sont identiques.

Théorème 5.4.4 *Soient $t \mapsto D_t$ et $t \mapsto E_t$ deux familles de droites projectives telles que les deux pseudo-paramétrisations associées $t \mapsto P_t$ et $t \mapsto Q_t$ sont équivalentes.*

Alors il existe une fonction birationnelle $\phi \in \mathbb{K}(t)$ telle que $\forall t \quad D_{\phi(t)} = E_t$.

En particulier, les deux courbes rationnelles associées aux familles (D_t) et (E_t) dans le plan dual sont identiques.

Démonstration Dans ce cas, $P_{\phi(t)} = Q_t$ est le point d'intersection de $D_{\phi(t)}$ et E_t. Si ces deux droites sont distinctes, alors leur intersection consiste en un unique point $P_{\phi(t)} = Q_t$ défini sur $\mathbb{K}(t)$. Comme tout point $\mathbb{K}(t)$-rationnel de $\mathcal{C}$ est constant, on en déduit que P_t et Q_t sont constants, ce qui est une contradiction.

Donc $D_{\phi(t)} = E_t$ et les deux familles sont identiques à un changement de variable birationnel près. □

La conclusion de cette section est que trouver une pseudo-paramétrisation revient à trouver une courbe rationnelle $\mathcal{L}$ dans le plan dual $\hat{\mathbb{P}}$, et une paramétrisation $\mu : \mathbb{P}^1 \to \mathcal{L}$ telle que l'image réciproque de $\hat{\mathcal{C}}$ par μ a multiplicité paire dans $\mathbb{P}^1$.

Pour trouver des pseudo-paramétrisations, il est naturel d'étudier d'abord les courbes rationnelles qui passent par plusieurs points de rebroussement de $\hat{\mathcal{C}}$, puisque la multiplicité de l'intersection à un point singulier est supérieure (et, espérons, égale) à 2. Cela fait l'objet de la section suivante.

5.5 Géométrie des points d'inflexion

Plutôt que de partir des pseudo-paramétrisations décrites dans les chapitres précédents et de retrouver la famille de droites associées grâce au théorème 5.4.2 dont la démonstration est constructive, nous allons montrer qu'elles se déduisent naturellement des propriétés géométriques des points d'inflexion des cubiques.

Soit $\mathcal{C} \subset \mathbb{P}$ une cubique projective plane lisse. Les neuf points d'inflexion de $\mathcal{C}$ définissent une configuration dans le plan $\mathbb{P}$. De façon plus intéressante, les neuf tangentes en ces points correspondent à neuf points dans le plan dual $\hat{\mathbb{P}}$. C'est cette dernière configuration que nous étudions dans cette section.

Suite à la section précédente, nous sommes spécialement intéressés par les courbes *rationnelles* de bas degré qui passent par plusieurs de ces neuf points de rebroussement de $\hat{\mathcal{C}}$. Rappelons qu'une courbe *rationnelle* est une courbe de genre géométrique 0 et qui possède un point rationnel. Ceci est équivalent à l'existence d'une paramétrisation rationnelle (*cf* section 3.1.1).

Nous allons d'abord supposer que $\mathcal{C}$ est la cubique plane hessienne donnée par l'équation (5.2). En effet, toute cubique plane lisse peut être envoyée sur une telle cubique hessienne par une transformation linéaire projective, en remplaçant le cas échéant $\mathbb{K}$ par une extension finie. Le j-invariant de $\mathcal{C}$ est

$$j(a) = \frac{27a^3(a+2)^3(a^2-2a+4)^3}{(a-1)^3(a^2+a+1)^3}.$$

Considérons le morphisme de Gauss associé à $\mathcal{C}$:

$$\omega_{\mathcal{C}} : (X : Y : Z) \mapsto (X^2 - aYZ : Y^2 - aXZ : Z^2 - aXY).$$

Les images des neuf points d'inflexion de $\mathcal{C}$ par $\omega_{\mathcal{C}}$ sont les trois points de l'orbite de $(a : 1 : 1)$ sous l'action de $\mathcal{S}_3$ et les six points de l'orbite de $(\zeta_3^2 : \zeta_3 : a)$ sous l'action de $\mathcal{S}_3$. La figure 5.2 liste ces points d'inflexion et leurs images par $\omega_{\mathcal{C}}$. Nous posons $O = A_0 = (0 : -1 : 1)$ et $\hat{O} = B_0 = (a : 1 : 1)$.

Point d'inflexion de $\mathcal{C}$	Point de rebroussement de $\hat{\mathcal{C}}$
$A_0 = (0 : -1 : 1)$	$B_0 = (a : 1 : 1)$
$A_1 = (-1 : 1 : 0)$	$B_1 = (1 : 1 : a)$
$A_2 = (1 : 0 : -1)$	$B_2 = (1 : a : 1)$
$A_3 = (-1 : \zeta_3 : 0)$	$B_3 = (\zeta_3^2 : \zeta_3 : a)$
$A_4 = (\zeta_3 : 0 : -1)$	$B_4 = (\zeta_3 : a : \zeta_3^2)$
$A_5 = (0 : -1 : \zeta_3)$	$B_5 = (a : \zeta_3^2 : \zeta_3)$
$A_6 = (\zeta_3 : -1 : 0)$	$B_6 = (\zeta_3 : \zeta_3^2 : a)$
$A_7 = (-1 : 0 : \zeta_3)$	$B_7 = (\zeta_3^2 : a : \zeta_3)$
$A_8 = (0 : \zeta_3 : -1)$	$B_8 = (a : \zeta_3 : \zeta_3^2)$

FIGURE 5.2 – Points d'inflexion de $\mathcal{C}$ et points de rebroussement correspondants sur sa duale.

Ces neuf points dans le plan dual forment une configuration intéressante, qui dépend du paramètre a.

5.5.1 Position vis-à-vis des droites

On peut tout d'abord vérifier, par exemple par recherche exhaustive, qu'il n'existe pas trois points colinéaires parmi ces neufs points de rebroussement dans le plan dual, à moins que le j-invariant de $\mathcal{C}$ soit nul. C'est également démontré par la proposition 1 de [14]. Les neuf points du plan dual qui correspondent aux neuf tangentes aux points d'inflexion de $\mathcal{C}$ sont en position générique vis-à-vis des droites.

On en déduit le lemme suivant par dualité :

Lemme 5.5.1 *Une cubique plane lisse projective définie sur un corps $\mathbb{K}$ de caractéristique première avec 6 n'a pas trois tangentes aux points d'inflexion concourantes, à moins que son j-invariant soit nul.*

5.5.2 Position vis-à-vis des coniques

On considère maintenant la configuration des neuf tangentes aux points d'inflexion du point de vue de faisceaux de coniques, c'est-à-dire que nous cherchons la courbe rationnelle $\mathcal{L}$ sous la forme d'une conique. Rappelons que 6 points, en position générique, ne sont pas sur une même conique. Définissons donc un peu de vocabulaire :

Définition 5.5.2 *Six points deux à deux distincts qui appartiennent à une même conique sont dits* coniques.

Six droites deux à deux distinctes qui sont toutes tangentes à une même conique sont dites coniques.

Le résultat suivant affirme que 6 tangentes aux points d'inflexion sont coconiques.

Lemme 5.5.3 *Soit $\mathcal{C}$ une courbe cubique plane lisse projective sur un corps $\mathbb{K}$ de caractéristique première avec 6. Supposons que le j-invariant de $\mathcal{C}$ est non nul.*

Retirons 3 points d'inflexion colinéaires. Alors les six tangentes aux points d'inflexion restants sont coconiques.

Il existe douze configurations de telles tangentes à six points d'inflexion.

Remarque : nous affirmons que les six *tangentes* sont coconiques, pas les six *points*. De manière équivalente, nous affirmons que les six points qui correspondent aux six tangentes dans le plan dual sont coconiques.

Démonstration Notons tout d'abord que la conique d'équation $UW - aV^2 = 0$ coupe $\hat{\mathcal{C}}$ en les points de coordonnées $(a : 1 : 1)$, $(1 : 1 : a)$, $(\zeta_3^2 : \zeta_3 : a)$, $(a : \zeta_3^2 : \zeta_3)$, $(\zeta_3 : \zeta_3^2 : a)$ et $(a : \zeta_3 : \zeta_3^2)$. Les trois points d'inflexion restant dans $\mathbb{P}$ sont $(1 : 0 : -1)$, $(\zeta_3 : 0 : -1)$ et $(1 : 0 : \zeta_3)$ et ils sont sur la droite d'équation $Y = 0$. L'action de $\mathcal{S}_3$ sur U, V et W produit deux coniques similaires.

La conique d'équation $U^2 + V^2 + W^2 + (a+1)(UV + UW + VW) = 0$ coupe $\hat{C}$ en les six points de l'orbite de $(\zeta_3^2 : \zeta_3 : a)$ sous l'action de $\mathcal{S}_3$. Les trois points d'inflexion restants dans $\mathbb{P}$ sont $(0 : -1 : 1)$, $(-1 : 1 : 0)$ et $(1 : 0 : -1)$. Ils sont sur la droite d'équation $X + Y + Z = 0$.

La conique d'équation $U^2 + \zeta_3 V^2 + \zeta_3^2 W^2 + (a+1)(\zeta_3^2 UV + \zeta_3 UW + VW) = 0$ coupe $\hat{C}$ en les trois points de l'orbite de $(a : 1 : 1)$ sous l'action de $\mathcal{S}_3$, et aussi en les trois points de l'orbite de $(\zeta_3^2 : \zeta_3 : a)$ sous l'action de $\mathcal{S}_3$. Les trois points d'inflexion restants dans $\mathbb{P}$ sont $(0 : \zeta_3 : -1)$, $(\zeta_3 : -1 : 0)$ et $(-1 : 0 : \zeta_3)$. Ils sont sur la droite d'équation $X + \zeta_3 Y + \zeta_3^2 Z = 0$. L'action de $\mathcal{S}_3$ produit encore une conique supplémentaire.

La conique d'équation $\zeta_3 U^2 + V^2 + \zeta_3 W^2 + (a + \zeta_3^2)(UV + \zeta_3^2 UW + VW) = 0$ coupe $\hat{C}$ en $(a : 1 : 1)$, $(1 : 1 : a)$, $(\zeta_3 : a : \zeta_3^2)$, $(a : \zeta_3^2 : \zeta_3)$, $(\zeta_3 : \zeta_3^2, a)$, $(\zeta_3^2 : a : \zeta_3)$. Les trois points d'inflexion restants dans $\mathbb{P}$ sont $(1 : 0 : -1)$, $(-1 : \zeta_3 : 0)$ et $(0 : \zeta_3 : -1)$. Ils sont sur la droite d'équation $\zeta_3 X + Y + \zeta_3 Z = 0$. L'action de $\mathcal{S}_3$ produit encore cinq coniques supplémentaires.

On obtient finalement douze coniques qui coupent la courbe duale $\mathcal{C}$ en six des neufs points de rebroussement. Chacune de ces coniques est associée à l'un des douze triplets de points d'inflexion colinéaires. □

Les quatre premières de ces douze coniques sont spécialement intéressantes pour la rationnalité parce que leurs équations ne font pas intervenir la racine cubique de l'unité ζ_3. Nous notons que trois de ces quatre coniques sont clairement rationnelles sur $\mathbb{K}(a)$ puisqu'elles ont un point $\mathbb{K}(a)$-rationnel évident. La dernière est rationnelle parce que son quotient par l'automorphisme d'ordre 3 évident est $\mathbb{P}^1$ sur $\mathbb{K}(a)$.

5.5.3 Position par rapport aux cubiques

Nous étudions maintenant un faisceau de cubiques qui passerait par les neufs points de $\hat{\mathbb{P}}$ associés aux neuf tangentes en les points d'inflexion de $\mathcal{C}$. Il est de dimension projective 0 en général, c'est-à-dire que les coefficients de l'équation de ces cubiques sont contraints, déterminés par le fait que la cubique passe par ces neuf points.

La cubique d'équation

$$a(U^3 + V^3 + W^3) = (a^3 + 2)UVW$$

passe par ces neuf points dans le plan dual. Toutefois, elle est en général non singulière, et est donc de genre 1. Elle n'est en particulier pas rationnelle et ne nous intéresse donc pas.

5.5.4 Position vis-à-vis des quartiques

Nous considérons maintenant les courbes de degré 4 dans le plan dual. La dimension projective de l'espace de quartiques est 14. On peut donc forcer une quartique à rencontrer les 9 points qui nous intéressent, et il reste 5 degrés de liberté. Comme nous sommes intéressés par des courbes rationnelles, nous utilisons ces degrés de liberté pour créer une grosse singularité en $\hat{O} = B_0 = (a : 1 : 1)$. En effet, deux degrés de liberté suffisent à annuler la partie de degré 1 de l'expansion de Taylor en $\hat{O}$. Trois degrés supplémentaires suffisent à annuler la partie de degré 2.

On trouve ainsi une quartique rationnelle Q dans $\hat{\mathbb{P}}$ qui passe par les neuf points de rebroussement de $\hat{\mathcal{C}}$ et qui a multiplicité d'intersection au moins 2 en chacun (puisque ce sont des points de rebroussement) et au moins 6 en celui $\hat{O}$.

L'équation de cette quartique rationnelle Q est

$$\begin{aligned}\mathcal{L} : U^4 + a(V^4 + W^4) - 2a(U^3V + U^3W + V^3W + VW^3) - (a^3+1)U(V^3+W^3) \\ +3a^2U^2(V^2+W^2) + (a^4+2a)V^2W^2 + (1-a^3)UVW(V+W) = 0.\end{aligned}$$

Cette quartique est irréductible si et seulement si le j-invariant de $\mathcal{C}$ est non nul, ce que nous supposons. En calculant son intersection avec les droites passant par $\hat{O}$ (comme décrit à la section 3.1.1), nous trouvons la paramétrisation suivante :

$$\begin{aligned} U(t) &= a^2t^4 - 2at^3 + (a^3+2)t^2 - 2a^2t + a, \\ V(t) &= a^4t^4 + (1-3a^3)t^3 + 3a^2t^2 - 2at + 1, \\ W(t) &= at^4 - (a^3+1)t^3 + 3a^2t^2 - 2at + 1. \end{aligned}$$

En substituant U, V et W par $U(t)$, $V(t)$ et $W(t)$ dans l'équation de $\hat{C}$, on trouve le polynôme de degré 24

$$t^6(t+1)^2(t^2-t+1)^2(at-2)^2((a+1)t-1)^2((a^2-a+1)t^2+(1-2a)t+1)^2(a^2t^2+1-at)^2.$$

On vérifie que Q a deux branches en $\hat{O}$. Une branche correspond à $t = 0$, et elle a multiplicité d'intersection 6 avec $\hat{\mathcal{C}}$. L'autre branche correspond à $t = 2/a$, avec multiplicité d'intersection 2 avec $\hat{\mathcal{C}}$. Ceci est illustré par la figure 5.3 où le lieu réel de $\hat{\mathcal{C}}$ est en noir et celui de Q en rouge. La multiplicité d'intersection totale de $Q.\hat{\mathcal{C}}$ en $\hat{O}$ est donc 8. L'intersection $Q.\hat{\mathcal{C}}$ se fait donc uniquement aux points de rebroussement de $\hat{\mathcal{C}}$: l'un avec multiplicité 8, les huit autres avec multiplicité 2.

On a en fait démontré le lemme suivant :

Lemme 5.5.4 *Soit $\mathcal{C}$ une courbe plane lisse projective définie sur un corps $\mathbb{K}$ de caractéristique première avec 6. Supposons que le j-invariant de $\mathcal{C}$ est non nul. Soit $\hat{\mathcal{C}}$ la duale de $\mathcal{C}$ et $\hat{O}$ un des neuf points de rebroussement de $\hat{\mathcal{C}}$.*

Il existe une quartique rationnelle Q dans le plan dual $\hat{\mathbb{P}}$ et une paramétrisation $\mu : \mathbb{P}^1 \to Q$ telle que l'image réciproque de $\hat{\mathcal{C}}$ par μ a multiplicité 6 et 2 au-dessus de $\hat{O}$, et 2 au-dessus des huit autres points de rebroussement.

Remarque : la définition de la quartique Q utilise un point d'inflexion d'une part, et les huit autres d'autre part. On peut donc définir cette quartique pour toute cubique qui a un point d'inflexion rationnel, c'est-à-dire pour toute courbe elliptique. Ce cas est différent de celui des coniques, où il fallait distinguer un *triplet* de points d'inflexion colinéaires qui ne pouvait pas toujours être défini sur le corps de base (uniquement si la courbe est hessienne sur le corps de base).

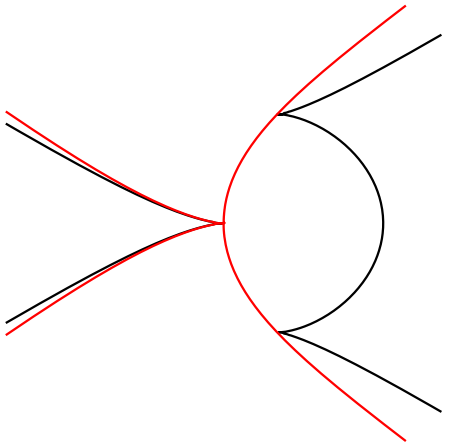

FIGURE 5.3 – Partie réelle de l'intersection de $\hat{C}$ et Q.

On peut donc prendre pour $\mathcal{C}$ la courbe elliptique d'équation de Weierstrass

$$F(X, Y, Z) = Y^2Z - X^3 - aXZ^2 - bZ^3. \tag{5.6}$$

Nous supposons $a \neq 0$, de sorte que le j-invariant est non nul également. L'image du point à l'infini $O = (0 : 1 : 0)$ par le morphisme de Gauss est $\hat{O} = (0 : 0 : 1)$, et la quartique $\hat{Q}$ donnée par le lemme 5.5.4 a pour équation

$$U^4 - 3V^4 + 6UV^2W = 0,$$

et paramétrisation

$$\begin{aligned} U(t) &= 6t^2, \\ V(t) &= 6t^3, \\ W(t) &= 3at^4 - 1. \end{aligned} \tag{5.7}$$

5.6 Intersection d'une cubique par des droites

Dans cette section, nous repassons du plan dual $\hat{\mathbb{P}}$ au plan projectif initial $\mathbb{P}^2(\mathbb{K})$. Nous supposons que la fonction $a \mapsto a^3$ est surjective. C'est le cas si $\mathbb{K}$ est le corps des nombres réels par exemple. C'est aussi le cas si $\mathbb{K}$ est le corps fini à q éléments $\mathbb{F}_q$ si q est congru à 2 modulo 3. Pour tout élément a de $\mathbb{K}$, on choisit une fois pour toute une racine cubique $\sqrt[3]{a}$ de a. De ce fait nous définissons une fonction $\sqrt[3]{\ } : \mathbb{K} \to \mathbb{K}$. Nous allons utiliser la méthode de la section 5.4 et les courbes rationnelles de la section 5.5 précédentes pour exhiber plusieurs pseudo-paramétrisations d'une cubique plane $\mathcal{C}$.

Par ordre croissant de complexité, nous commencerons par étudier les coniques, puis les quartiques, puis les droites.

5.6.1 Intersection de la courbe duale et d'une conique

On peut tout d'abord prendre pour $\mathcal{L}$ l'une des douze coniques du lemme 5.5.3. Nous supposons donc que $\mathcal{C}$ est la cubique hessienne de l'équation (5.2) pour a tel que $a^3 \neq -1$. Quatre coniques parmi les douze du lemme 5.5.3 sont rationnelles sur $\mathbb{K}(a)$. L'intersection $D.\hat{\mathcal{C}}$ est de degré 12 et contient six des neuf points de rebroussement de $\hat{\mathcal{C}}$, l'intersection en chacun étant de multiplicité 2. Choisissons par exemple $\mathcal{L}$ comme la conique d'équation $UW - aV^2 = 0$, dont une paramétrisation est donnée par $U(t) = 1, V(t) = -t$ et $W(t) = at^2$. La droite D_t correspondante a pour équation

$$X - tY + at^2 Z = 0.$$

Nous substituons X par $tY - at^2 Z$ dans l'équation hessienne (5.2) et trouvons la forme binaire de degré 3 suivante en Y et Z

$$(t^3+1)Y^3 - 3at(t^3+1)Y^2 Z + 3a^2t^2(t^3+1)YZ^2 + (1-a^3t^6)Z^3$$

qui décrit l'intersection $D_t.\mathcal{C}$. En divisant par $(t^3+1)Z^3$, nous obtenons un polynôme cubique en $y = Y/Z$ dont le discriminant réduit est

$$\Delta(t) = \left(\frac{9(1+a^3t^3)}{1+t^3}\right)^2.$$

Nous reprenons les formules et les notations de la section 5.2. Nous obtenons

$$\begin{aligned} s_1 &= 3at, \\ s_2 &= 3a^2t^2, \\ s_3 &= \frac{a^3t^6-1}{t^3+1}, \\ \delta &= \frac{9(1+a^3t^3)}{1+t^3}, \\ R &= -27\frac{a^3t^3+1}{t^3+1}, \\ R' &= 0. \end{aligned}$$

Nous trouvons ainsi les solutions

$$y = at - \sqrt[3]{\frac{a^3t^3+1}{t^3+1}},$$

dont nous déduisons

$$x = X/Z = ty - at^2 = -t\sqrt[3]{\frac{a^3t^3+1}{t^3+1}},$$

C'est la pseudo-paramétrisation découverte par Farashahi [29].

5.6.2 Intersection de la courbe duale et d'une quartique

Choisissons maintenant pour $\mathcal{L}$ la quartique Q du lemme 5.5.4. Toutes les multiplicités de l'intersection $Q.\hat{\mathcal{C}}$ sont paires. Nous nous attendons donc à ce que le discriminant réduit soit un carré. Cette fois-ci, on peut aussi bien prendre pour modèle de $\mathcal{C}$ la cubique de Weierstrass de l'équation (5.6). La paramétrisation de Q donnée par l'équation (5.7) fournit une famille de droites $(D_t)_t$, dépendant du seul paramètre t. L'équation de D_t est

$$6t^2X + 6t^3Y + (3at^4 - 1)Z = 0.$$

Nous divisons par Z, posons $x = X/Z$, $y = Y/Z$ et substituons y par $1/(6t^3) - at/2 - x/t$ dans l'équation de Weierstrass (5.6). On trouve l'équation cubique $x^3 - s_1x^2 + s_2x - s_3$ en $x = X/Z$, où

$$\begin{aligned} s_1 &= 1/t^2, \\ s_2 &= 1/(3t^4), \\ s_3 &= (1/t^6 - 6a/t^2 - 36b + 9a^2t^2)/36. \end{aligned}$$

Reprenant de nouveau les formules et notations de la section 5.2, on obtient

$$\begin{aligned} \delta &= (-1/t^6 - 108b - 18a/t^2 + 27a^2t^2)/12, \\ R &= 0, \\ R' &= (-1/t^6 - 108b - 18a/t^2 + 27a^2t^2)/4. \end{aligned}$$

Finalement nous trouvons la solution

$$x = X/Z = \frac{1}{3t^2} + \sqrt[3]{\frac{a^2t^2}{4} - \frac{1}{108t^6} - b - \frac{a}{6t^2}}$$

et

$$y = Y/Z = \frac{1}{6t^3} - at/2 - x/t.$$

C'est la pseudo-paramétrisation découverte par Icart [38], rappelée ci-dessus 3.2.3, au changement de variable $t \mapsto -1/t$ près.

5.6.3 Intersection de la courbe duale avec une droite

Choisissons enfin pour $\mathcal{L}$ une droite qui passe par deux points de rebroussement de $\hat{\mathcal{C}}$. Nous supposons donc que $\mathcal{C}$ est la cubique hessienne définie par l'équation (5.2) avec $a^3 \neq 1$. Supposons que $\mathcal{L}$ est l'unique droite qui passe par les deux points de rebroussement $B_0 = (a : 1 : 1)$ et $B_2 = (1 : a : 1)$ de $\hat{\mathcal{C}}$. L'intersection $L.\hat{C}$ est de degré 6. Comme $(a : 1 : 1)$ et $(1 : a : 1)$ ont tous deux multiplicité d'intersection ≥ 2, il reste au plus deux points d'intersection. Une illustration de cette situation dans le plan réel projectif est donnée à la figure 5.4.

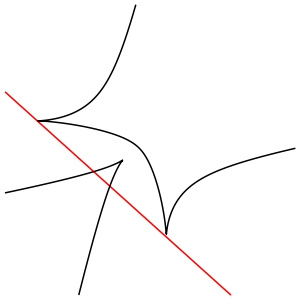

FIGURE 5.4 – L'intersection $\hat{\mathcal{C}}$ et $\mathcal{L}$

Toutes les multiplicités de l'intersection $\mathcal{L}.\hat{\mathcal{C}}$ ne sont pas paires, mais seules deux multiplicités sont impaires, et égales à 1. Nous nous attendons donc à ce que $\Delta(t)$ soit un carré multiplié par un polynôme de degré 2 en t. Les points de $\mathcal{L} \subset \hat{\mathbb{P}}$ représentent un faisceau de droites dans $\mathbb{P}$ généré par les tangentes à $\mathcal{C}$ en $(0 : -1 : 1)$ et $(1 : 0 : -1)$. La première tangente a pour équation $aX + Y + Z = 0$. La deuxième a pour équation $X + aY + Z = 0$. Soit donc t un paramètre formel et considérons la

droite D_t d'équation $(at+1)X+(t+a)Y+(t+1)Z=0$. La tangente en $(0:-1:1)$ correspond à la valeur $t=\infty$. La tangente en $(1:0:-1)$ correspond à $t=0$. La droite D_t passe par le point fixé $(1:1:-a-1)$ et le point variable $(1,-t,t-1)$. Une description paramétrique de D_t est donc donnée par

$$i \mapsto (i+1 : i-t : t-1-(a+1)i).$$

Remplaçons X par $i+1$, Y par $i-t$ et Z par $t-1-(a+1)i$ dans l'équation (5.2) et divisions par le coefficient dominant. L'intersection $D_t.\mathcal{C}$ est définie par le polynôme de degré 3

$$h(i) = i^3 + \frac{3t(a+2)i}{a^2+a+1} + \frac{3t(1-t)}{a^2+a+1}. \tag{5.8}$$

Son discriminant réduit est

$$\Delta(t) = 81t^2 \frac{9(a^2+a+1)t^2 + 2(2a+1)(a^2+a+7)t + 9(a^2+a+1)}{(a^2+a+1)^3}. \tag{5.9}$$

Ce n'est pas un carré dans $k(a)(t)$. Toutefois il a seulement deux racines de multiplicité impaires (et égales à 1). Nous pouvons donc substituer à t une fonction rationnelle bien choisie, de sorte que Δ soit transformé en un carré. Cela revient à chercher une paramétrisation de la conique plane projective d'équation

$$(a^2+a+1)S^2 = 9(a^2+a+1)T^2 + 2(2a+1)(a^2+a+7)TK + 9(a^2+a+1)K^2. \tag{5.10}$$

Nous utilisons ici encore la méthode de la section 3.1.1. Cette conique a deux points $\mathbb{K}$-rationnels, à savoir $(3:1:0)$ et $(3:0:1)$. La droite qui passe par ces deux points a pour équation

$$-S+3T+3K=0.$$

La tangente en $(3:0:1)$ a pour équation

$$3(a^2+a+1)S - (2a+1)(a^2+a+7)T - 9(a^2+a+1)K = 0.$$

La droite générique dans le faisceau linéaire généré par ces deux droites a pour équation

$$(3(a^2+a+1)-j)S + (3j-(2a+1)(a^2+a+7)j)T + (3j-9(a^2+a+1)j)K = 0 \tag{5.11}$$

où j est un paramètre formel.

L'intersection de la conique d'équation (5.10) avec la droite d'équation (5.11) donne alors la paramétrisation

$$\begin{cases} S(j) &= 3j^2 - 2(a+2)^3 j + 3(a+2)^3(a^2+a+1), \\ T(j) &= j(j - 3(a^2+a+1)), \\ K(j) &= (a^2+a+1)((a+2)^3 - 3j). \end{cases}$$

Nous remplaçons maintenant t par $T(j)/K(j)$ dans l'équation (5.8) et trouvons un polynôme de degré trois avec coefficients dans le corps $k(a)(j)$. Si nous substituons $T(j)/K(j)$ à t dans l'équation (5.9), nous obtenons enfin un carré, de sorte que $\Delta = \delta^2(j)$ avec

$$\delta(j) = \frac{9j(3j^2 - 2(a+2)^3 j + 3(a^2+a+1)(a+2)^3)(3(a^2+a+1) - j)}{((a+2)^3 - 3j)^2(a^2+a+1)^3}.$$

Nous reprenons les formules et les notations de la section 5.2. Le polynôme h de l'équation (5.8) a pour coefficients coefficients 1, $-s_1$, s_2 et $-s_3$ avec

$$\begin{aligned} s_1 &= 0, \\ s_2 &= -\frac{3j(a+2)(3(a^2+a+1) - j)}{(a^2+a+1)^2((a+2)^3 - 3j)}, \\ s_3 &= \frac{3j(3(a^2+a+1) - j)((a^2+a+1)(a+2)^3 - j^2)}{(a^2+a+1)^3((a+2)^3 - 3j)^2}. \end{aligned}$$

Nous en déduisons la pseudo-paramétrisation de la cubique $\mathcal{C}$ suivante :

$$\begin{aligned} R(j) &= \frac{27j^2(3(a^2+a+1) - j)}{((a+2)^3 - 3j)(a^2+a+1)^3} \\ \rho(j) &= \sqrt[3]{R(j)} \\ \rho'(j) &= \frac{9j(a+2)(3(a^2+a+1) - j)}{(a^2+a+1)^2((a+2)^3 - 3j)\rho(j)} \\ i(j) &= \frac{\rho(j) + \rho'(j)}{3} \\ t(j) &= \frac{j(3(a^2+a+1) - j)}{(a^2+a+1)((a+2)^3 - 3j)} \\ P(j) &= (i(j) + 1 : i(j) - t(j) : t(j) - 1 - (a+1)i(j)). \end{aligned}$$

où $P(j)$ est le point de $\mathcal{C}$ associé au paramètre j.

Cette situation est illustrée par la figure 5.5 dans le cas $a = 2$. Le segment rouge correspond au cas où le paramètre j prend des valeurs dans l'intervalle $[-4, -0.3]$. Les calculs de la section 4.2.1 ont une situation géométrique similaire.

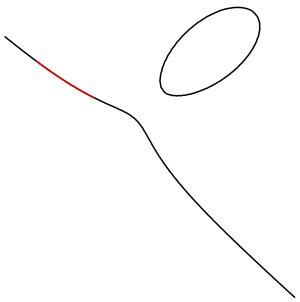

FIGURE 5.5 – Une pseudo-paramétrisation

5.7 Classification des pseudo-paramétrisations

Nous avons vu plusieurs pseudo-paramétrisations différentes d'une cubique plane, chacune associée à une courbe rationnelle dans $\hat{\mathbb{P}}$ de multiplicité d'intersection paire avec la courbe duale $\hat{\mathcal{C}}$ de l'équation (5.3). Nous nous demandons dans cette section s'il existe d'autres courbes rationnelles similaires, qui fourniraient encore d'autres pseudo-paramétrisations. Nous désirons également mettre un peu de structure sur l'ensemble de ces courbes.

Nous avons construit des solutions (u, v, h) à l'équation suivante, définie sur $\mathbb{K}(t)$:

$$h^2 = G(u, v, 1) \tag{5.12}$$

où G est l'équation de la courbe duale (*cf* équation (5.3)), $u = U(t)/W(t)$, $v = V(t)/W(t)$ et $h = \delta(t)/W^3(t)$

Nous appelons $\mathcal{S}$ le modèle minimal de la surface définie par l'équation (5.12). Nous verrons que c'est une surface $K3$. Chercher des pseudo-paramétrisations revient à chercher des courbes rationnelles dessus. Les courbes sur $\mathcal{S}$ sont des *diviseurs* de $\mathcal{S}$. Ceux-ci sont classifiés, à équivalence algébrique (linéaire) près, par le *groupe de Néron-Severi* $\mathrm{NS}(\mathcal{S})$ de $\mathcal{S}$.

Plus formellement, toute courbe rationnelle $\mathcal{L}$ qui a une intersection paire avec $\hat{\mathcal{C}}$ se relève en une courbe rationnelle sur le revêtement de degré deux Σ de $\hat{\mathbb{P}}$ le long de $\hat{\mathcal{C}}$. Pour définir Σ, nous considérons le corps de fonctions $\mathbb{K}(a)/(U/W, V/W)$ de $\hat{\mathbb{P}}$ sur $\mathbb{K}(a)$. On peut en définir une extension quadratique en ajoutant une racine carrée γ de $G(U, V, W)/W^6$ où $G(U, V, W)$ est l'équation de $\hat{\mathcal{C}}$. La clôture normale de $\hat{\mathbb{P}}$ $\mathbb{K}(a)(U/W, V/W, \gamma)$ est Σ. Elle a neuf singularités, une au-dessus de chacun des neuf points de rebroussement de $\hat{\mathcal{C}}$. Afin d'obtenir un modèle lisse pour Σ, nous éclatons tout d'abord $\hat{\mathcal{C}}$ en chacun des points de rebroussement de $\hat{\mathcal{C}}$. Nous appelons Π la surface ainsi obtenue. L'image réciproque de $\hat{\mathcal{C}}$ par $\Pi \to \hat{\mathbb{P}}$ consiste en une courbe lisse de genre 1 et 9 courbes rationnelles qui lui sont tangentes. Soit $\mathcal{S}$ la clôture normale de Π dans $\mathbb{K}(a)/(U/W, V/W, \gamma)$. C'est une surface lisse, le modèle minimal de Σ.

Soit σ_1 l'automorphisme de $\hat{\mathbb{P}}$ qui envoie $(U : V : W)$ sur $(V : W : U)$. Soit σ_2 l'automorphisme de $\hat{\mathbb{P}}$ qui envoie $(U : V : W)$ sur $(U : \zeta_3 V : \zeta_3^2 W)$. Soit σ_3 l'automorphisme de $\hat{\mathbb{P}}$ qui envoie $(U : V : W)$ sur $(V : U : W)$. Nous étendons ces trois automorphismes à $\mathbb{K}(a)/(U/W, V/W, \gamma)$ en envoyant γ sur lui-même. Les automorphismes obtenus sont de même appelés σ_1, σ_2 et σ_3. Ils induisent des automorphismes sur Π, Σ et $\mathcal{S}$ appelés également σ_1, σ_2 et σ_3.

Soit σ_4 l'unique automorphisme non trivial de l'extension $\mathbb{K}(a)/(U/V, V/W, \gamma) : \mathbb{K}(a)/(U/W, V/W)$. Il induit des automorphismes de Σ et $\mathcal{S}$ notés également σ_4.

L'action de σ_1, σ_2 et σ_3 sur les points de rebroussement B_i (*cf* figure 5.2) est donnée par les permutations des indices suivantes :

$$\begin{aligned} \sigma_1 &= (0,1,2)(3,4,5)(6,7,8), \\ \sigma_2 &= (0,5,8)(1,3,6)(2,4,7), \\ \sigma_3 &= (0,2)(1)(3,6)(4,8)(5,7). \end{aligned}$$

Le groupe engendré par σ_1 et σ_2 est d'ordre neuf. Il agit transitivement sur les neufs points de rebroussement, et sur les neuf courbes rationnelles correspondantes sur l'éclatement Π. Nous choisissons l'une des deux courbes rationnelles sur $\mathcal{S}$ au-dessus de B_0 et l'appelons E_0. Pour $1 \leq i \leq 9$, nous appelons E_i l'image de E_0 par l'unique automorphisme engendré par $\langle \sigma_1, \sigma_2 \rangle$ qui envoie B_0 sur B_i. Soit F_i l'image de E_i par σ_4. On obtient ainsi dix-huit courbes rationelles sur $\mathcal{S}$. Soit H l'image réciproque d'une droite de $\hat{\mathbb{P}}$ par $\mathcal{S} \longrightarrow \hat{\mathbb{P}}$. Le réseau engendré par les E_i, F_i et H dans le groupe de Néron-Severi est de rang 19 et de discriminant 2.3^9. Les index d'intersection sont

$$\begin{aligned} E_i.F_i &= 1, \\ E_i^2 &= -2, \\ F_i^2 &= -2, \\ E_i.E_j &= 0 \text{ for } i \neq j, \\ E_i.F_j &= 0 \text{ for } i \neq j, \\ E_i.H &= 0, \\ F_i.H &= 0, \\ H^2 &= 2. \end{aligned}$$

Soit D une droite générique dans $\hat{\mathbb{P}}$ passant par B_0. L'intersection $D.\hat{\mathcal{C}}$ est $2B_0$ plus un diviseur effectif de degré 4, c'est-à-dire que c'est le point B_0 avec multiplicité 2 et quatre autres points. L'image réciproque de D dans $\mathcal{S}$ est donc l'union de E_0, F_0 et une courbe de genre 1 avec au moins deux points rationnels : les points d'intersection avec E_0 et F_0. L'image réciproque par $\mathcal{S} \to \hat{\mathbb{P}}$ du faisceau de droites

qui passent par B_0 définit donc une fibration elliptique $f : \mathcal{S} \to \mathbb{P}^1$ de $\mathcal{S}$, avec deux sections E_0 et F_0, donc $\mathcal{S}$ est une surface $K3$ elliptique. Le lemme suivant [50, 2.3] est utile quand on cherche des courbes rationnelles sur une surface $K3$.

Lemme 5.7.1 *Soit D une classe d'auto-intersection -2 dans le groupe de Néron-Severi d'une surface $K3$. Alors D ou $-D$ contient un diviseur effectif. Si ce diviseur est irréductible, c'est une courbe rationnelle lisse.*

On peut aussi chercher des courbes rationnelles singulières avec auto-intersection positive. Il est même possible de compter les courbes rationnelles dans ces classes [3, 51, 71]. Puisqu'il y en a beaucoup, il est improbable qu'elles soient définies sur le corps de base. En effet, toutes les courbes rationnelles de la section 5.5 se remontent en des courbes rationnelles lisses sur $\mathcal{S}$ d'auto-intersection -2.

Exemple : la conique dans $\hat{\mathbb{P}}$ qui passe par B_0, B_1, B_2, B_3, B_4, B_5 se remonte en une courbe rationnelle I_{012345} sur $\mathcal{S}$. On a $H.I_{012345} = 2$, $E_0.I_{012345} = E_1.I_{012345} = E_2.I_{012345} = 1$ et $F_3.I_{012345} = F_4.I_{012345} = F_5.I_{012345} = 1$; et I_{012345} a intersection zéro avec les autres E_i et F_i. On en déduit l'identité suivante dans le groupe de Néron-Severi :

$$3I_{0,1,2,3,4,5} = 3H - 2(E_0 + E_1 + E_2) - (F_1 + F_2 + F_3) - (E_3 + E_4 + E_5) - 2(F_3 + F_4 + F_5),$$

et donc $I_{0,1,2,3,4,5}$ a pour auto-intersection -2. De même, avec des notations évidentes :

$$3I_{0,1,3,4,7,8} = 3H - 2(E_0 + E_3 + E_7) - (F_0 + F_3 + F_7) - (E_1 + E_4 + E_8) - 2(F_1 + F_4 + F_8),$$

et

$$3I_{0,1,3,5,6,8} = 3H - 2(E_0 + E_5 + E_8) - (F_0 + F_5 + F_8) - (E_1 + E_3 + E_6) - 2(F_1 + F_3 + F_6).$$

L'action de $\langle \sigma_1, \sigma_2, \sigma_3, \sigma_4 \rangle$ produit 24 courbes rationnelles similaires sur S avec auto-intersection -2. C'est la contribution des coniques du lemme 5.5.3.

Exemple : Considérons maintenant la quartique donnée par le lemme 5.5.4. Elle se remonte en une courbe rationnelle J_0 sur $\mathcal{S}$, telle que $J_0.H = 4$, $J_0.E_0 = 2$, $J_0.F_0 = 1$, $J_0.E_i = 1$, $J_0.F_i = 0$ pour $1 \leq i \leq 8$. On obtient l'identité suivante dans le groupe de Néron-Severi :

$$3J_0 = 6H - 5E_0 - 4F_0 - \sum_{1 \leq i \leq 8} (2E_i + F_i).$$

L'action de $\langle \sigma_1, \sigma_2, \sigma_4 \rangle$ produit 18 courbes rationnelles similaires d'auto-intersection

-2. Le réseau engendré par H, les neuf E_i, les neuf F_i, et les $24+18$ classes des quartiques et des coniques a dimension 19 et discriminant 54. C'est le groupe de Néron-Severi complet de $\mathcal{S}$ si k est de caractéristique zéro et quand a est transcendant. Cette structure du groupe de Néron-Severi permet maintenant de prouver qu'il existe une infinité de courbes rationnelles sur $\mathcal{S}$, qui donnent lieu à une infinité de pseudo-paramétrisations de la cubique initiale $\mathcal{C}$.

Considérons une fibration elliptique de $\mathcal{S}$, par exemple la fibration $f : \mathcal{S} \to \mathbb{P}^1$ décrite ci-dessus. Nous choisissons la section E_0 pour origine. La fibre générique de f est une courbe elliptique sur le corps de fonctions $k(t)$ de $\mathbb{P}^1$. Les fibres de f s'envoient sur des droites qui passent par B_0 dans $\hat{\mathbb{P}}$. Les huit fibres singulières de f s'envoient sur les droites B_0B_i pour $1 \leq i \leq 8$. Chacune d'entre elles a pour type de Kodaira I_3, les trois composantes irréductibles étant E_i, F_i, et une troisième courbe rationnelle G_i qui coupe E_0 et F_0. Soit $T \subset \mathrm{NS}(\mathcal{S})$ le groupe généré par la section zéro E_0 et les composants de la fibre E_i, F_i, G_i pour $1 \leq i \leq 8$. Le groupe de Mordell-Weil de la fibre générique est isomorphe au quotient $\mathrm{NS}(\mathcal{S})/T$, [61, Théorème 6.3]. Puisque $E_i + F_i + G_i = H - E_0 - F_0$ ne dépend pas de i pour $1 \leq i \leq 8$, le rang de T est 18 et celui de $\mathrm{NS}(\mathcal{S})$ est 1. Nous avons donc une infinité de sections de f. Les images de ces sections sont toutes des courbes rationnelles d'auto-intersection -2. La figure 5.6 présente la représentation d'une de ces courbes rationnelles (ou plutôt son image dans $\hat{\mathbb{P}}$). Dans le cas où $\mathcal{C}$ est la cubique de Weierstrass de l'équation (5.6), une paramétrisation de cette courbe rationnelle est

$$\begin{aligned} U(t) &= 4at^6 + 4t^2/27, \\ V(t) &= t(4at^6 + 4t^2/27), \\ W(t) &= a^2t^8 + 2at^4/27 + 4bt^6 + 1/81. \end{aligned} \tag{5.13}$$

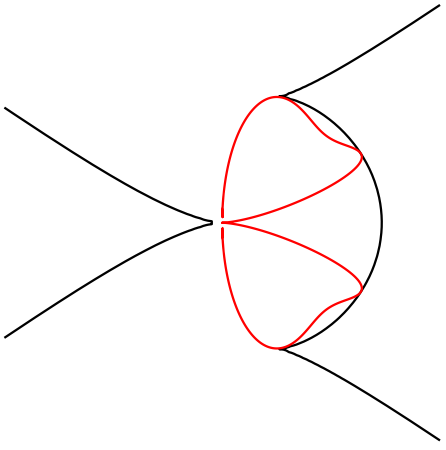

FIGURE 5.6 – Une autre courbe rationnelle d'intersection paire avec $\hat{\mathcal{C}}$.

Troisième partie

Cryptanalyse

Chapitre 6

Préliminaires : polynômes tordus

Dans ce chapitre, nous revoyons la théorie des polynômes tordus sur les corps finis. Ceux-ci semblent propres à l'instanciation de schémas cryptographiques asymétriques non commutatifs tels que ceux présentés à la section 1.2.1. Comme pour les polynômes classiques, on peut former par réduction modulaire des anneaux quotients non commutatifs qui pourraient servir le même but.

Ces objets ont été initialement introduits par Ore [56] pour traiter des opérateurs linéaires en analyse. Une théorie exhaustive a été réalisée par McDonald [54]. Nous en présentons ici les principaux résultats, dans le cadre des corps finis.

6.1 Polynômes tordus

6.1.1 Définition, euclidianité

Soit $\mathbb{F}_q$ un corps fini, avec $q = p^n$ et p premier et θ un automorphisme de corps de $\mathbb{F}_q$.

Définition 6.1.1 *L'anneau non commutatif $\mathbb{F}_q[X;\theta]$ des polynômes tordus en l'indéterminée X est l'ensemble des polynômes formels $a_kX^k + \cdots + a_1X + a_0$ muni de l'addition classique et du produit $\star$ défini récursivement par la distributivité sur l'addition et $X \star a = \theta(a)X$.*

On le note $\mathcal{R}$.

Exemple : si $P = \sum_{i=0}^{k} a_iX^i$ et $Q = \sum_{j=0}^{k'} b_jX^j$, alors $P \star Q = \sum_{l=0}^{k+k'} \sum_{i+j=l} a_i\theta^i(b_j)X^l$

Remarque : Dans le cas où $\mathbb{F}_q$ est de degré 1 (c'est-à-dire si $n = 1$), θ est réduit à l'identité et on retrouve les polynômes classiques.

Propriété 6.1.2 *L'anneau $\mathbb{F}_q[X;\theta]$ est euclidien à gauche et à droite.*

C'est-à-dire que pour tout $(f, g) \in \mathbb{F}_q[X;\theta]$ *il existe un unique couple* $(Q_g, R_g) \in \mathbb{F}_q[X;\theta]$ *et un unique couple* $(Q_d, R_d) \in \mathbb{F}_q[X;\theta]$ *tels que*

$$f = g \star Q_g + R_g = Q_d \star g + R_d \text{ avec } \deg R_g < \deg f \text{ et } \deg R_d < \deg f$$

Les algorithmes de divisions euclidiennes à gauche et à droite de polynômes tordus sont similaires aux algorithmes des polynômes classiques, en faisant attention à l'isomorphisme θ.

Exemple : soient deux monômes $f = a_k X^k$ et $g = b_d X^r$ avec $k > r$. Alors

$$f = g \star Q_g = Q_d \star g \text{ avec } Q_g = \theta^{-r}\left(\frac{a_k}{b_d}\right) X^{k-r} \text{ et } Q_d = \frac{a_k}{\theta^{k-r}(b_d)} X^{k-r}$$

Une fois la division de monômes ainsi définie, on peut construire itérativement la division euclidienne à gauche ou à droite de deux polynômes tordus de la même façon que pour les polynômes classiques.

Muni d'une division euclidienne à gauche et d'une division euclidienne à droite, il est possible de définir les plus grands diviseurs communs à gauche et à droite, dénotés respectivement GCLD et GCRD.

Ainsi muni de divisions euclidiennes à gauche et à droite, l'anneau des polynômes tordus est *principal à gauche et à droite*, c'est-à-dire que tout idéal à gauche (resp. à droite) est engendré par un seul polynôme.

À l'instar des anneaux de polynômes commutatifs, tout polynôme tordu f peut se factoriser en un produit de polynômes irréductibles $f = f_1 \cdots f_k$. Cette factorisation n'est pas nécessairement unique. Toutefois, les degrés des facteurs irréductibles sont toujours identiques, à permutation près.

Théorème 6.1.3 (Ore, [56]) *Si* $f \in \mathbb{F}_q[X;\theta]$ *se factorise complètement en*

$$f = f_1 \cdots f_k = g_1 \cdots g_{k'}$$

où les f_i, g_i *sont irréductibles dans* $\mathbb{F}_q[X;\theta]$*, alors* $k = k'$ *et il existe une permutation* φ *de* $[\![1, \ldots, k]\!]$ *telle que* $\forall 1 \leqslant i \leqslant k \quad \deg f_i = \deg g_{\varphi(i)}$.

Il est possible de calculer une décomposition en facteurs irréductibles en temps polynomial grâce à un algorithme dû à Giesbrecht [35]. Le théorème précédent laisse néanmoins penser que le nombre de factorisations distinctes d'un polynôme tordu peut atteindre une valeur exponentielle en le nombre de ses facteurs de degrés distincts.

6.1.2 Commutativité

Dans le but de définir un cryptosystème de type Diffie-Hellman, nous devons étudier les propriétés de commutativité des anneaux de polynômes tordus.

Soit $m = \text{ord}\theta$ et $\mathbb{F}_{q'} = \mathbb{F}_{p^{n/m}}$ le sous-corps des éléments laissés invariants par θ.

Centre

Nous nous intéresserons à des sous-ensembles commutatifs parmi les polynômes tordus. Il est donc naturel de commencer par étudier les polynômes f qui commutent avec tous les polynômes de $\mathbb{F}_q[X;\theta]$, c'est-à-dire le centre de $\mathcal{R}$.

Proposition 6.1.4 ([54], p 24-25) *Le centre $\mathcal{C}$ de l'anneau $\mathbb{F}_q[X;\theta]$ est le sous-anneau $\mathbb{F}_{q'}[X^m]$ des polynômes en X^m à coefficients sur le sous-corps laissé invariant par θ.*

Démonstration $\mathcal{C}$ est un sous-anneau de $\mathbb{F}_q[X;\theta]$. Par induction, il suffit de vérifier les propriété de commutativité pour les monômes.

X^k commute avec tous les monômes, si et seulement si il commute avec les monômes de degré 0. $X^k \star a = \theta^k(a) \star X^k$ donc X^k commute avec tous les monômes de degré 0 si et seulement si $k = \text{ord}\theta$.

Un monôme a de degré 0 commute avec tous les monômes si et seulement si il commute avec X. Or $X \star a = \theta(a) \star X$ donc a commute avec X si et seulement si a est laissé invariant par θ. □

Exemple : Si θ est l'identité, on retrouve les polynômes classiques.

Exemple : Sur $\mathbb{F}_9$, si $\theta : a \mapsto a^3$ est le Frobenius, alors le centre est $\mathbb{F}_3[X^2]$.

Centralisateur d'un polynôme donné

Proposition 6.1.5 *Soit $P \in \mathbb{F}_q[X;\theta]$ fixé. Soit s le PGCD des exposants des monômes (non nuls) de P, $\mathbb{L}$ le sous-corps de $\mathbb{F}_q$ laissé invariant par $\langle\theta^s\rangle$ et r tel que $\langle\theta^r\rangle$ laisse invariant les coefficients de P. Alors le centralisateur $\mathcal{C}_P$ de P contient l'anneau $\mathbb{L}[X^r,\theta]$.*

En particulier, si $P \in \mathbb{F}_{q'}[X]$, alors $\mathcal{C}_P \supseteq \mathbb{F}_{q'}[X]$.

Démonstration Soit $a \in \mathbb{L}$. La construction de $\mathbb{L}$ assure que pour tout monôme non nul $p_k X^k$ de P, on ait $\theta^k(a) = a$ et donc $ap_k \star X^k = p_k \star X^k \star a$.

De même, tout monôme en X^r commute avec les coefficients non nuls des termes de P par construction. □

Pour P donné et un degré r fixé, on peut calculer l'ensemble des polynômes Q de degré inférieur ou égal à r tels que $P \star Q = Q \star P$, par algèbre linéaire sur leurs coefficients : l'automorphisme θ est en effet une puissance du Frobenius.

Dans les deux cas, nous avons lancé des expériences sur les tailles de polynômes qui nous intéressaient pour le cryptosystème visé comme expliqué dans [26]. Ces inclusions semblent en fait être des égalités :

Heuristique 6.1.6 *Le centralisateur $\mathcal{C}_P$ d'un polynôme tordu non central $P \in \mathbb{F}_q[X;\theta]\backslash\mathcal{C}$ est égal à $\mathbb{F}_{q'}[X]$ si $P \in \mathbb{F}_{q'}[X]$ ou à l'idéal engendré par P et le centre $\langle \mathcal{C}, P\rangle$ sinon. On le note $\mathcal{C}[P]$.*

Exemple : dans [10], les auteurs génèrent deux sous-ensembles commutatifs distincts d'environ 90 polynômes chacun $\mathcal{S}_0$ et $\mathcal{S}_1$ de $\mathbb{F}_4[X;\theta]$ par *essai/erreur* :

- choix d'un polynôme aléatoire P initial pour chaque ensemble
- tirage aléatoire de polynômes Q_i en ne conservant que ceux qui commutent avec P.

En notant $\mathbb{F}_4 = \{0, 1, \alpha, \alpha^2\}$, nous avons trouvé en particulier que $\mathcal{S}_0 \subseteq \mathcal{C}_{X^5+X^3+\alpha}$ et $\mathcal{S}_1 \subseteq \mathcal{C}_{X^3+X+\alpha}$.

6.2 Polynômes tordus modulaires

Dans cette section, nous voulons, par analogie avec les polynômes, construire des anneaux de polynômes tordus quotients. Ils constituent un exemple d'anneaux non commutatifs finis. McDonald a étudié une condition nécessaire sur les générateurs des idéaux bilatères dans $\mathbb{F}_q[X;\theta]$ ([54], théorème II.12) ; nous donnons ici une condition nécessaire et suffisante sur ces générateurs, et étudions plus particulièrement les anneaux quotients.

Le résultat le plus important de cette section concerne la caractérisation du quasi-centre, c'est-à-dire des générateurs des idéaux bilatères de $\mathbb{F}_q[X;\theta]$. Ces polynômes peuvent servir de modulo.

Soit $\mathcal{R}$ un anneau de polynômes tordus $\mathbb{F}_q[X;\theta]$ et soit N un élément arbitraire de $\mathcal{R}$. Soit $\mathcal{R} \star N$ l'idéal des multiples à gauche de N. Le théorème suivant, sur les quotients à droite par un idéal à gauche, est standard (et valable pour un anneau quelconque, non nécessairement euclidien).

Théorème 6.2.1 *La relation de congruence à gauche modulo $\mathcal{R}\star N$ est une relation d'équivalence sur $\mathcal{R}$. Les classes associées sont appelées classes à gauche modulo N.*

Cette relation est compatible avec l'addition des polynômes tordus.

Remarque : La propriété d'équivalence découle immédiatement de l'unicité de la division euclidienne à droite par N, de la même façon que pour les polynômes classiques.

De façon similaire on peut définir les classes à droite modulo $N \star \mathcal{R}$. La réduction modulo $\mathcal{R} \star N$ (resp. $N \star \mathcal{R}$) se calcule en utilisant la division euclidienne à droite (resp. à gauche).

Enfin chaque classe à gauche modulo N a un unique représentant, *canonique*, de degré strictement inférieur à N : c'est le reste dans la division euclidienne à droite par N.

6.2.1 Quasi-centre

Étant donné que $\mathbb{F}_q[X;\theta]$ n'est pas commutatif, ces relations d'équivalence ne sont pas compatibles avec la loi de multiplication dans le cas général. Toutefois, les classes à gauche peuvent être multipliées entre elles pourvu que N commute avec les polynômes tordus dans un certain sens.

Définition

En effet, soient $U + \Lambda \star N$ et $V + \Lambda' \star N$ deux représentants arbitraires de deux classes (à gauche) modulo $\mathcal{R} \star N$. Alors leur produit

$$(U + \Lambda \star N) \star (V + \Lambda' \star N) = U \star V + \Lambda \star N \star V + (U \star \Lambda' + \Lambda \star N \star \Lambda') \star N$$

n'est pas égal à $U \star V$ modulo $\mathcal{R} \star N$ à moins que $\Lambda \star N \star V$ soit divisible par N. Comme Λ peut-être choisi de manière arbitraire, cela signifie que $N \star V$ est divisible à droite par N, ou encore qu'il existe $W \in \mathcal{R}$ tel que $N \star V = W \star N$.

Ceci motive la définition suivante :

Définition 6.2.2 *Soit $N \in \mathcal{R}$. On dit que N* quasi-commute *à gauche avec $V \in \mathcal{R}$ si $N \star V$ est divisible à droite par N, c'est-à-dire s'il existe $W \in \mathcal{R}$ tel que $N \star V = W \star N$.*

On dit alors que V et W sont duaux l'un de l'autre. Ils ont le même degré.

Nous appelons quasi-centre *de $\mathcal{R}$, noté $\mathcal{N}$, l'ensemble des polynômes N qui quasi-commutent avec tous les éléments de $\mathcal{R}$. On dit que N quasi-commute. En d'autres termes, $\mathcal{N}$ est l'ensemble des générateurs des idéaux bilatères de $\mathcal{R}$.*

Exemple : sur $\mathbb{F}_4 = \{0, 1, \alpha, \alpha^2 = \alpha + 1\}$, soient $V = \alpha + X^3 + X^5$ et $N = \alpha X + \alpha X^5$, alors

$$N \star V = X + \alpha X^4 + X^5 + \alpha X^6 + \alpha X^8 + \alpha X^{10} = W \star N$$

$$\text{avec } W = \alpha^2 + \alpha^2 X^3 + \alpha^2 X^5$$

Proposition 6.2.3 *Soit $N \in \mathcal{R}$. L'ensemble des éléments qui quasi-commutent à gauche avec N est un sous-anneau de $\mathcal{R}$.*

Démonstration Soit $I = N \star \mathcal{R}$ l'idéal à droite engendré par N. L'ensemble des éléments qui quasi-commutent à gauche avec N est par définition le stabilisateur à gauche de I, $\mathrm{End}_g(I) = \{f \in \mathcal{R} | f \star I \subseteq I\}$. C'est un anneau d'endormorphismes du $\mathcal{R}$-module I. □

Exemple : reprenant V et N de l'exemple précédent, si $V' = \alpha^2 1 + X + \alpha^2 X^2 + \alpha X^4 + \alpha^2 X^5$ et $W' = \alpha 1 + \alpha^2 X + \alpha X^2 + \alpha^2 X^4 + X^5$ alors N quasi-commute avec V' :

$$N \star V' = \alpha^2 X + \alpha X^2 + \alpha^2 X^3 + \alpha X^5 + X^6 + \alpha^2 X^7 + X^9 + \alpha^2 X^{10} = W' \star N$$

et N quasi-commute avec $(V + V')$:

$$\begin{aligned} &N \star (V + V') = N \star (1 + X + \alpha^2 X^2 + X^3 + \alpha X^4 + \alpha X^5) \\ &= \alpha X + \alpha X^2 + \alpha^2 X^3 + \alpha X^4 + \alpha^2 X^5 + \alpha^2 X^6 + \alpha^2 X^7 + \alpha X^8 + X^9 + X^{10} \\ &= (1 + \alpha^2 X + \alpha X^2 + \alpha^2 X^3 + \alpha^2 X^4 + \alpha X^5) \star N = (W + W') \star N \end{aligned}$$

et avec $(V \star V')$:

$$\begin{aligned} N \star (V \star V') &= N \star (1 + \alpha X + X^2 + \alpha X^3 + \alpha X^4 + X^5 + X^6 + X^7 + \alpha X^8 \\ &\quad + \alpha^2 X^9 + \alpha X^{10}) \\ &= \alpha X + X^2 + \alpha X^3 + X^4 + \alpha^2 X^5 + \alpha^2 X^6 + \alpha^2 X^8 + X^{10} + \alpha^2 X^{11} \\ &\quad + \alpha X^{12} + X^{13} + \alpha^2 X^{14} + X^{15} \\ &= (1 + \alpha X + X^2 + \alpha X^3 + \alpha^2 X^4 + \alpha^2 X^5 + X^6 + \alpha^2 X^7 + \alpha^2 X^8 \\ &\quad + X^9 + \alpha^2 X^{10}) \star N \\ &= (W \star W') \star N \end{aligned}$$

Caractérisation de $\mathcal{N}$

$(\mathcal{N}, \star)$ est un monoïde. L'application qui à tout $N \in \mathcal{N}$ associe l'idéal bilatère (N) est un morphisme de monoïdes. Son noyau est le sous-groupe $\mathcal{R}^*$ des unités de $\mathcal{R}$, c'est-à-dire $\mathbb{F}_q^*$.

Soit N un élément du quasi-centre. Nous voulons que l'ensemble des classes à gauche (ou à droite) soit lui-même un anneau (non commutatif). Il faut pour cela que N quasi-commute avec tout $\mathcal{R}$.

D'après la propriété 6.2.3, N quasi-commute avec tous les éléments de $\mathcal{R}$ si et seulement si N quasi-commute avec X et avec toutes les constantes. Ceci nous donne une caractérisation des éléments de $\mathcal{N}$.

Théorème 6.2.4 *Le quasi-centre $\mathcal{N}$ de $\mathcal{R}$ est l'ensemble des polynômes de la forme $a \star C \star X^k$ avec $a \in \mathcal{R}^* = \mathbb{F}_q^*$ et $C \in \mathcal{C}$.*

Exemple : dans le cas des polynômes tordus définis sur $\mathbb{C} : \mathbb{R}$ pour l'automorphisme de conjugaison, le quasi-centre est constitué des polynômes dont les monômes non nuls sont de degré soit tous impairs, soit tous pairs, et dont les coefficients ont le même argument.

Démonstration Soit $a \in \mathbb{F}_q \backslash \mathbb{F}_{q'}$ une constante qui quasi-commute avec N. Pour des raisons de degré, son élément dual b (tel que $N \star a = b \star N$) est également une constante.

Écrivant $N = \sum_i n_i X^i$, alors

$$N \star a = \sum_i n_i \theta^i(a) X^i = b \star N = \sum_i n_i b X^i,$$

ce qui implique que pour tout i tel que n_i est non nul, $\theta^i(a) = b$. Les puissances de θ apparaissent toutes avec le même degré. Il existe donc k tel que tous les termes non nuls soient de degré $i \equiv k \mod m$ (où $m = \mathrm{ord}(\theta)$). Les monômes de N ont donc une forme particulière : il existe un coefficient b tel qu'ils soient tous de la forme bX^k fois un monôme du centre.

Une propriété de ce coefficient se déduit de la quasi-commutation avec X. Pour les mêmes raisons de degré, il existe deux constantes a et c dans $\mathbb{F}_q$ telles que

$$N \star X = \sum_i n_i X^{i+1} = (aX + c) \star N = \sum_i (a\theta(n_i) + c n_{i+1}) X^{i+1} + c n_0.$$

Soit j le plus petit des degrés i tels que $n_i \neq 0$. Alors $c \cdot n_j = 0$ implique que $c = 0$ (c'est-à-dire que le produit des polynômes tordus préserve la valuation), et que pour tout i tel que $n_i \neq 0$, $a = n_i / \theta(n_i)$.

Réciproquement, il est facile de vérifier que ces polynômes sont dans le quasi-centre.

Finalement nous avons démontré que le quasi-centre est l'ensemble des polynômes tordus $N = \sum_{i=0}^{j} n_i X^i$ tels que :

- Monômes : il existe k tel que pour tout i tel que $n_i \neq 0$, $i \mod \mathrm{ord}\theta = k$
- Coefficients : il existe une constante $a \in \mathbb{F}_q$ telle que $\forall i \ \theta(n_i)/n_i = a$.

□

Les polynômes du quasi-centre sont les seuls bons candidats pour définir un anneau de polynômes tordus modulaires. $\mathcal{N}$ est l'ensemble des générateurs des idéaux bilatères, une propriété particulière de la quasi-commutativité est l'égalité des classes à gauche et à droite :

Propriété 6.2.5 *Soit N un polynôme du quasi-centre de $\mathcal{R}$. Alors les idéaux à gauche et à droite engendrés par N sont identiques.*

Les classes modulo ces ensembles sont appelées simplement classes modulo N. Ces classes forment un anneau, que l'on note $\mathcal{R}/(N)$.

Démonstration C'est le théorème fondamental de la construction d'anneaux quotients. □

Exemple : Continuant les exemples précédents sur $\mathbb{F}_4$, soit $N = \alpha X + \alpha X^5$. N est dans le quasi-centre. Soit $U = 1 + X + \alpha X^2 + \alpha^2 X^3 + \alpha X^4 + \alpha^2 X^6 + X^7 + X^8 + \alpha X^9 + \alpha X^{10}$. Alors avec des notations évidentes,

$$U \mod \star N = 1 + \alpha^2 X + \alpha^2 X^2 + \alpha X^3 + \alpha^2 X^4 = U \mod N\star$$

Dans la suite, on note $\circ$ la loi de multiplication dans $\mathcal{R}/(N)$.

6.2.2 Décomposition dans $\mathcal{R}/(N)$

Pour les problèmes de type Diffie-Hellman qui nous préoccuperont, il est intéressant d'étudier comment les éléments de $\mathcal{R}/(N)$ peuvent être décomposés en produit de facteurs. Toutefois, factoriser dans $\mathcal{R}/(N)$ n'a pas grand sens, vu que toute unité modulo N est facteur de tout élément de $\mathcal{R}/(N)$. Nous nous intéresserons donc aux diviseurs de zéro : il est en effet immédiat que $\mathcal{R}/(N)$ n'est pas intègre, puisque pour toute factorisation non triviale $U \star V$ de N, on a $U \star V = 0 \mod N$ alors que ni U ni V ne sont divisibles par N.

Par définition, une classe $\bar{U}$ est un facteur gauche d'une classe $\bar{P}$ si $\bar{P}$ est dans l'espace image de l'application suivante :

$$\begin{array}{rccc} \mu(\bar{U}) & : & \mathcal{R}_N & \longrightarrow & \mathcal{R}_N \\ & & \bar{V} & \longmapsto & \bar{U} \circ \bar{V}. \end{array}$$

Rappelons que le produit $\bar{U} \circ \bar{V}$ est égal à $U \star V \mod N$. On peut remarquer que l'ensemble $U\star + N\star$ est indépendant du représentant particulier U de $\bar{U}$. Le pgcd à gauche G de U et N est donc indépendant du représentant U de $\bar{U}$. Donc, de l'égalité $U\star + N\star = G\star$ on obtient que les multiples à droite de U et G sont identiques modulo N. Par conséquent, l'image de $\mu(\bar{U})$ est l'ensemble $\bar{G}\circ$. Finalement :

Proposition 6.2.6 *L'ensemble des facteurs à gauche d'une classe $\bar{P}$ est l'ensemble des classes $\bar{U}$ dont le pgcd à gauche avec N est un facteur gauche du représentant canonique $\hat{P}$ de $\bar{P}$.*

Exemple : Sur $\mathbb{F}_4$, soit $P = \alpha + \alpha^2 X + \alpha^2 X^2 + \alpha X^3 + \alpha^2 X^4 + \alpha^2 X^5$ et $N = \alpha X + \alpha X^5$, alors $GCLD(P, N) = G = \alpha + \alpha^2 X + \alpha^2 X^2$. Le polynôme $D = 1 + \alpha^2 X$ est un diviseur à gauche de G, et sa classe $\bar{D}$ modulo N est un facteur gauche de la classe $\bar{P}$ de P.

6.2.3 Unités

En particulier, les classes qui sont premières à gauche avec N sont les facteurs gauches de toute classe : elles forment le sous-groupe des unités de l'anneau quotient $\mathcal{R}/(N)$. Elles sont donc également premières à droite.

Proposition 6.2.7 *Soit N un élément du quasi-centre. Alors U est premier à gauche avec N si et seulement si U est premier à droite avec N.*

Démonstration U est premier à gauche avec N, donc $\bar{U}$ est inversible dans $\mathcal{R}/(N)$. □

6.3 Opérateurs linéaires sur corps finis

6.3.1 Introduction

Nous explicitons ici une connexion bien connue entre les matrices sur corps finis et les polynômes tordus modulaires (*cf* [21]). Les matrices carrées sur un corps fini forment un autre exemple, classique, d'algèbre non commutative, qui pourrait être intéressant pour instancier un protocole Diffie-Hellman.

Soit $\mathbb{F}_p$ un corps fini arbitraire et $\mathbb{F}_q = \mathbb{F}_{p^m}$ son extension de degré m. $\mathbb{F}_q$ est un espace vectoriel de dimension m sur $\mathbb{F}_p$, et que l'anneau des opérateurs $\mathbb{F}_p$-linéaires sur $\mathbb{F}_q$ est isomorphes aux matrices $m \times m$ à coefficients dans $\mathbb{F}_p$. Nous notons cet anneau $L_p(\mathbb{F}_q)$.

$\mathcal{R}/(X^m - 1)$ est une $\mathbb{F}_q$-algèbre cyclique. L'extension $\mathbb{F}_q$ sur $\mathbb{F}_p$ est cyclique, donc cette algèbre est simple sur $\mathbb{F}_p$. D'après le théorème de Wedderburn, toute algèbre simple est une algèbre d'endomorphismes. Explicitement, $\mathcal{R}/(X^m - 1)$ est isomorphe à l'anneau des endomorphismes du $\mathbb{F}_p$-espace vectoriel $\mathbb{F}_q$. Cet anneau est isomorphe à $L_p(\mathbb{F}_q)$ par un choix de base de $\mathbb{F}_q$ sur $\mathbb{F}_p$. Nous détaillons ci-dessous cet isomorphisme.

6.3.2 Interprétation en termes de polynômes tordus

Endomorphismes linéaires et puissances du Frobenius

Proposition 6.3.1 *Soit θ l'endomorphisme de Frobenius de $\mathbb{F}_q$ ($\theta : \begin{array}{ccc} \mathbb{F}_q & \longrightarrow & \mathbb{F}_q \\ t & \mapsto & t^p \end{array}$).*

Les combinaisons linéaires des puissances de θ à coefficients dans $\mathbb{F}_q$ sont des endomorphismes $\mathbb{F}_p$-linéaires de $\mathbb{F}_q$.

On en déduit une représentation des endomorphismes $\mathbb{F}_p$-linéaires de $\mathbb{F}_q$:

Proposition 6.3.2 *L'application suivante :* $\begin{array}{ccc} (\mathbb{F}_q)^m & \longrightarrow & L_p(\mathbb{F}_q) \\ (c_i) & \mapsto & \sum_{i=0}^{m-1} c_i\theta^i \end{array}$ *est bijective.*

Démonstration Cette application est clairement injective. Pour des raisons de cardinalité, elle est également bijective. □

Identification avec les polynômes tordus

Venant de revoir que les endomorphismes $\mathbb{F}_p$-linéaires de $\mathbb{F}_q$ sont simplement les combinaisons $\mathbb{F}_q$-linéaires des puissances du Frobenius, il reste à interpréter ces combinaisons en termes de polynômes tordus modulaires.

Proposition 6.3.3 *L'anneau $(L_p(\mathbb{F}_q), +, \circ)$ est isomorphe à $(\mathbb{F}_q[X;\theta], +, \star)/(X^m - 1)$.*

Démonstration Les applications $\sum_{i=0}^{m-1} c_i\theta^i$ peuvent être clairement identifiées avec les polynômes tordus $\sum_{i=0}^{m-1} c_iX^i$.

En faisant le lien entre les deux structures d'anneau, on obtient la loi d'addition $+$ usuelle mais la multiplication suit les deux identités $X \circ a = \theta(a)X$ et $X^m - 1$ (où m est l'ordre du Frobenius. □

Chapitre 7

Cryptanalyse d'un cryptosystème asymétrique basé sur les polynômes tordus

Dans ce chapitre, nous décrivons la cryptanalyse que nous avons proposée dans [26], conjointement avec V. Dubois, sur le cryptosystème asymétrique proposé par Boucher *et al* [10].

Nous présentons tout d'abord quelques réflexions autour du problème Diffie-Hellman tel que défini ci-dessus au paragraphe 1.2.1. Ensuite nous déroulons l'attaque dans le cas précis des polynômes tordus, puis des polynômes tordus modulaires.

Nous reprenons les notations de la section 1.2 : Alice et Bob se sont publiquement accordés sur un semigroupe non commutatif $(\mathcal{D}, \diamond)$, un sous-semigroupe commutatif $\mathcal{S}$ qui sert à l'instanciation du cryptosystème, z est un élément de $\mathcal{D}$. Alice a construit un élément z' de $\mathcal{S} \diamond z \diamond \mathcal{S}$. Nous spécialiserons par la suite au cas des polynômes tordus $\mathbb{F}_q[X;\theta]$.

7.1 Stratégie d'attaque

7.1.1 Préliminaire : cas inversible

Supposons tout d'abord que $\mathcal{S}$ est un groupe, c'est-à-dire que tous ses éléments sont inversibles. Dans ce cas, une paire $[u, v] \in \mathcal{S} \times \mathcal{S}$ est une solution au problème de décomposition Diffie-Hellman pour z et z' si et seulement si $z' = u \diamond z \diamond v$, soit encore $u' \diamond z' = z \diamond v$ avec $u' = u^{-1}$.

Notons les variables connues de l'attaquant en gras. Quand $\mathcal{S}$ est un groupe, l'équation de type quadratique $\boldsymbol{z'} = u \diamond \boldsymbol{z} \diamond v$ d'inconnues (u, v) peut être directement transformée en une équation de type linéaire $u' \diamond \boldsymbol{z'} = \boldsymbol{z} \diamond v$ d'inconnues $(u' = u^{-1}, v)$.

Exemple des groupes de tresses

C'est le cas par exemple dans les groupes de tresses [46], où on a en outre $u' = v$ (problème de conjugaison plutôt que problème de décomposition). Des attaques partielles sur le problème général de conjugaison dans les groupes de tresses étaient connues (voir [52]), toutefois elles restaient de complexité exponentielle. Il s'est avéré qu'il existait un algorithme pour le résoudre, spécifique aux groupes de tresses, mais de complexité polynomiale (voir [19]). Cette attaque utilise le fait qu'il est possible de représenter les éléments de groupes de tresses par des matrices sur un anneau (plutôt complexe). Ces matrices sont de taille polynomiale en la taille des éléments considérés du groupe de tresses. Pour tout élément $\boldsymbol{z}$ du groupe de tresses, notons $\boldsymbol{Z}$ la matrice associée. Alors le problème de conjugaison du protocole de type Diffie-Hellman revient à trouver U dans la représentation matricielle de l'ensemble commutatif $\mathcal{S}$ tel que $\boldsymbol{Z'} = U\boldsymbol{Z}U^{-1}$ où $\boldsymbol{Z}$ et $\boldsymbol{Z'}$ sont des matrices publiques telles qu'au moins une solution U existe.

Les solutions candidates peuvent être calculées en résolvant le problème algébrique linéaire suivant : trouver une matrice U telle que $\boldsymbol{Z'}U - U\boldsymbol{Z} = 0$ et $S_iU - US_i = 0$ pour tous les générateurs S_i de $\mathcal{S}$. Ce système a en général plusieurs solutions qui ne sont pas des matrices représentatives d'éléments du groupe de tresses. Quand il est impossible de les filtrer, cela ne résout pas le problème de conjugaison. Toutefois, les auteurs de l'attaque ont noté que toute solution inversible de ce problème linéaire (une solution aléatoire est heuristiquement inversible avec forte probabilité) commute avec les éléments de $\mathcal{S}$, donc est suffisante pour calculer le secret partagé du protocole Diffie-Hellman.

Autres exemples

La même approche peut être aussi utilisée pour trouver un changement de variables linéaire inversible qui permette de relier deux ensembles d'équations quadratiques multivariées définies sur un corps, qui est une instance particulière du problème d'"isomorphisme de polynômes" [57]. En effet, des polynômes quadratiques multivariés peuvent être représentés par des matrices triangulaires supérieures (avec le même nombre de coefficients non nuls), et quand un changement de coordonnées linéaire U envoie un polynôme quadratique $\boldsymbol{p}$ sur un polynôme $\boldsymbol{p'}$, cela se traduit par l'identité matricielle $\boldsymbol{P'} = U^t\boldsymbol{P}U$ (où t signifie la transposition). Comme U est inversible, on peut attaquer ce problème en résolvant l'équation linéaire $V\boldsymbol{P'} - \boldsymbol{P}U = 0$ d'inconnue $(V = (U^t)^{-1}, U)$. Il suffit alors heuristiquement d'environ 3 paires indépendantes $(\boldsymbol{p}, \boldsymbol{p'})$ construites avec le même U pour résoudre directement le système, c'est-à-dire trouver un espace de solutions de dimension 1. Il est également possible d'attaquer le cas du degré supérieur en utilisant l'identité entre des parties homogènes de degré 2. Une attaque moins immédiate a aussi été développée dans [58].

Une attaque similaire a été développée indépendamment dans [11].

7.1.2 Position de l'attaque

Nous considérons maintenant le cas où les éléments de $\mathcal{S}$ ne sont pas inversibles, mais où attaquer le problème Diffie-Hellman revient à résoudre une équation de type centralisateur (de type linéaire). Pour cela, la structure minimale de $\mathcal{D}$ dont nous avons besoin est qu'il soit un anneau intègre, avec une notion calculable de plus grand diviseur commun à gauche (ou à droite) et une notion de division à gauche (ou à droite) exacte. Il faut également que $\mathcal{S}$ soit un sous-semigroupe commutatif. Ici, intègre signifie qu'il n'y a pas de diviseurs de zéro : $u \diamond v = 0 \Rightarrow u$ ou $v = 0$. Notons qu'il n'est pas nécessaire qu'il soit euclidien.

Avant de décrire l'attaque, rappelons la hiérarchie de problèmes sur laquelle le protocole repose. Le problème Diffie-Hellman est : étant donnés $\boldsymbol{z}_A = u_A \diamond \boldsymbol{z} \diamond v_A$ et $\boldsymbol{z}_B = u_B \diamond \boldsymbol{z} \diamond v_B$, calculer

$$z_{AB} = u_A \diamond \boldsymbol{z}_B \diamond v_A = u_B \diamond \boldsymbol{z}_A \diamond v_B.$$

Une condition suffisante pour attaquer le problème Diffie-Hellman est de résoudre le problème de décomposition qui se manifeste dans les protocoles Diffie-Hellman : étant donnés $\boldsymbol{z} \in \mathcal{D}$ et $\boldsymbol{z}' \in \mathcal{S} \diamond \boldsymbol{z} \diamond \mathcal{S}$, calculer $(u, v) \in \mathcal{S}$ tel que $\boldsymbol{z}' = u \diamond \boldsymbol{z} \diamond v$. Toutefois, il a été noté dans [19, 66] qu'il suffit de casser la variante réduite suivante de ce problème pour résoudre le problème Diffie-Hellman : étant donnés $\boldsymbol{z} \in \mathcal{D}$ et $\boldsymbol{z}' \in \mathcal{S} \diamond \boldsymbol{z} \diamond \mathcal{S}$, calculer u, v *qui commutent avec les éléments de* $\mathcal{S}$ tels que $\boldsymbol{z}' = u \diamond \boldsymbol{z} \diamond v$.

En effet, si un attaquant peut trouver u'_A et v'_A qui commutent avec $\mathcal{S}$ et tels que $\boldsymbol{z}_A = u'_A \diamond \boldsymbol{z} \diamond v'_A$, il peut alors calculer

$$u'_A \diamond \boldsymbol{z}_B \diamond v'_A = u_B \diamond u'_A \diamond \boldsymbol{z} \diamond v'_A \diamond v_B = u_B \diamond \boldsymbol{z}_A \diamond v_B = z_{AB}.$$

Ainsi, avec des notations évidentes, la hiérarchie des problèmes est

$$\text{DH} \quad \leq \quad \text{DH-Décomposition relâchée} \quad \leq \quad \text{DH-Décomposition}.$$

On a donc toujours intérêt à choisir $\mathcal{S}$ maximal.

7.1.3 Attaque

Supposons que $\mathcal{D}$ est un anneau intègre tel que le plus grand diviseur commun à gauche (ou à droite) existe toujours et peut être calculé efficacement, ainsi qu'une division exacte à droite (ou à gauche). L'attaque découle de l'observation suivante : les éléments de l'ensemble $\mathcal{S} \diamond \boldsymbol{z} \diamond \mathcal{S}$ sont transformés d'une manière particulière

quand on les multiplie à gauche (ou à droite) par ceux de $\mathcal{S}$. Cette propriété est utilisée au cœur du protocole Diffie-Hellman.

Toutefois, cette propriété peut être utilisée pour attaquer le cryptosystème. Soit $\boldsymbol{\lambda}$ un élément arbitraire de $\mathcal{S}$. Alors

$$\boldsymbol{\lambda} \diamond (u \diamond \boldsymbol{z} \diamond v) = u \diamond \boldsymbol{\lambda} \diamond \boldsymbol{z} \diamond v.$$

Ainsi, on obtient un autre élément de $\mathcal{S} \diamond \boldsymbol{z} \diamond \mathcal{S}$ qui admet également u comme diviseur à gauche. Par conséquent, en prenant le plus grand diviseur commun à gauche de $\boldsymbol{z}' = u \diamond \boldsymbol{z} \diamond v$ et $\boldsymbol{\lambda} \diamond \boldsymbol{z}'$, on obtient un multiple (non nul) de u. On peut faire la même chose avec tous les éléments $\boldsymbol{\lambda}$ de $\mathcal{S}$. Soit $\boldsymbol{\lambda}_1, \ldots, \boldsymbol{\lambda}_s$ un ensemble de générateurs de $\mathcal{S}$. Pour des raisons d'efficacité (par exemple, il peut être nécessaire de transmettre $\mathcal{S}$, c'est-à-dire son système de générateur, sur un canal public afin que les deux protagonistes disposent du même ensemble lors de l'échange), cet ensemble doit être de taille pratique, que nous ne considérons pas plus ici. Soit $\boldsymbol{g}$ le pgcd à gauche de $\{\boldsymbol{z}', \boldsymbol{\lambda}_1 \diamond \boldsymbol{z}', \ldots, \boldsymbol{\lambda}_s \diamond \boldsymbol{z}'\}$, obtenu de manière itérative par des pgcd à gauche entre deux éléments successifs. Étant donné que $\boldsymbol{z}$ ne commute pas avec $\mathcal{S}$, $\boldsymbol{g}$ pourrait être u lui-même. Il est possible qu'on ait un moyen de distinguer u et ses multiples non triviaux (par exemple des considérations de degré). Dans ce cas, ou si $\boldsymbol{g}$ est vraiment égal à u, on utilise la division exacte à gauche et on peut récupérer v, et le problème de décomposition est résolu.

Sinon, soit a un élément tel que $\boldsymbol{g} = u \diamond a$. En utilisant l'algorithme de division exacte, on obtient $\boldsymbol{m}$ et $\boldsymbol{m}_i$, $i = 1, \ldots, s$ tels que :

$$\begin{cases} \boldsymbol{z}' &= \boldsymbol{g} \diamond \boldsymbol{m} \\ \boldsymbol{\lambda}_i \diamond \boldsymbol{z}' &= \boldsymbol{g} \diamond \boldsymbol{m}_i. \end{cases} \tag{7.1}$$

Comme $\mathcal{D}$ ne possède pas de diviseurs de zéro, ce système se réécrit en

$$\begin{cases} \boldsymbol{z} \diamond v - a \diamond \boldsymbol{m} &= 0 \\ \boldsymbol{\lambda}_i \diamond \boldsymbol{z} \diamond v - a \diamond \boldsymbol{m}_i &= 0. \end{cases} \tag{7.2}$$

On obtient par conséquent un ensemble d'équation de type linéaire en les inconnues (v, a). De plus, comme les solutions v qui nous intéressent commutent avec $\mathcal{S}$, on obtient également les équations de type linéaire $\boldsymbol{\lambda}_i \diamond v - v \diamond \boldsymbol{\lambda}_i$ pour tout $i = 1, \ldots, s$.

Toutefois, les solutions de ces équations linéaires ne sont pas nécessairement toutes solutions du problème de décomposition initial. En effet, en passant du système initial (7.1) au système linéaire (7.2), on perd l'information que $\boldsymbol{z} \diamond v$ est un diviseur à droite de $\boldsymbol{z}'$. Par exemple, toute combinaison linéaire de ces solutions est solution des équations linéaires sans forcément être solution de la condition de

divisibilité.

Définissons les *solutions diviseurs* comme étant les solutions linéaires (v, a) telles que $\boldsymbol{z} \diamond v$ est un diviseur à droite de $\boldsymbol{z}'$. Montrons tout d'abord que toute solution diviseur est suffisante pour résoudre le problème de décomposition relâchée. Supposons en effet que le système de type linéaire peut être résolu, et soit (v', a') une solution diviseur arbitraire. En utilisant l'algorithme de division exacte, on peut calculer u' tel que $\boldsymbol{z}' = u' \diamond \boldsymbol{z} \diamond v'$. En utilisant le fait que $\boldsymbol{z} \diamond v' = a' \diamond \boldsymbol{m}$, on trouve que $\boldsymbol{z}' = u' \diamond a' \diamond \boldsymbol{m}$, et donc on en déduit aussi que $\boldsymbol{g} = u' \diamond a'$. De plus, u' commute avec tous les générateurs de $\mathcal{S}$: comme $\boldsymbol{\lambda}_i \diamond \boldsymbol{z} \diamond v' = a' \diamond \boldsymbol{m}_i$, on obtient :

$$u' \diamond \boldsymbol{\lambda}_i \diamond \boldsymbol{z} \diamond v' = \boldsymbol{g} \diamond \boldsymbol{m}_i = \boldsymbol{\lambda}_i \diamond \boldsymbol{z}' = \boldsymbol{\lambda}_i \diamond u' \diamond \boldsymbol{z} \diamond v',$$

et donc $u' \diamond \boldsymbol{\lambda}_i = \boldsymbol{\lambda}_i \diamond u'$. Par conséquent, (u', v') est un couple d'élements qui commutent avec $\mathcal{S}$ et vérifient $\boldsymbol{z}' = u' \diamond \boldsymbol{z} \diamond v'$. Ainsi, le problème de décomposition relâchée est cassé.

La seule étape non démontrée de notre attaque est celle qui consiste à trouver une solution diviseur parmi l'espace vectoriel des solutions. Outre l'expérimentation, nous pouvons toutefois en donner une justification heuristique. Il nous faut d'abord comprendre la structure de l'espace vectoriel des solutions.

Proposition 7.1.1 *Soit $\tilde{\mathcal{C}}(\boldsymbol{z})$ l'ensemble des couples (c, c') tels que $\boldsymbol{z} \diamond c = c' \diamond \boldsymbol{z}$. Pour toute solution (v, a) de l'équation de type linéaire $\boldsymbol{z} \diamond v - a \diamond \boldsymbol{m} = 0$ et tout $(c, c') \in \tilde{\mathcal{C}}(\boldsymbol{z})$, le couple $(c \diamond v, c' \diamond a)$ est aussi une solution linéaire.*

Corollaire 7.1.2 *L'ensemble des solutions de l'équation $\boldsymbol{z} \diamond v - a \diamond \boldsymbol{m} = 0$ est clos par la multiplication à gauche membre à membre par $\tilde{\mathcal{C}}(\boldsymbol{z})$.*

Il est également clos pour la loi d'addition.

Cette propriété se généralise aux solutions (v, a) du système linéaire complet avec la multiplication à gauche par $\mathcal{A} = \tilde{\mathcal{C}}(\boldsymbol{z}) \cap \big(\cap_i \tilde{\mathcal{C}}(\boldsymbol{\lambda}_i \diamond \boldsymbol{z})\big) \cap (\mathcal{R}, \mathcal{C}_{\mathcal{S}})$, où $\mathcal{C}_{\mathcal{S}}$ est l'anneau des éléments qui commutent avec $\mathcal{S}$. On vérifie facilement que $\mathcal{A} = \tilde{\mathcal{C}}(\boldsymbol{z}) \cap (\mathcal{C}_{\mathcal{S}}, \mathcal{C}_{\mathcal{S}})$. Remarquons que $\mathcal{A}$ est un sous-anneau de $\mathcal{D} \times \mathcal{D}$.

L'additivité et la multiplication à gauche par $\mathcal{A}$ sont des dégénérescences qui sont indépendantes de la solution spécifique, c'est-à-dire les éléments précis u et v de $\mathcal{S}$ choisis initialement par Alice pour construire $\boldsymbol{z}'$. Ces dégénérescences mises à part, nous nous attendons à ce que le système d'équations soit caractéristique de cette solution particulière. Ainsi :

Heuristique 7.1.3 *Les solutions du système linéaire sont générées par un générateur unique, par addition et multiplication à gauche par $\mathcal{A}$.*

En d'autres termes, l'espace des solutions du système linéaire est un module à gauche libre de rang 1 sur $\mathcal{A}$.

Nous voulons maintenant un algorithme pour calculer explicitement une solution qui résolve le problème Diffie-Hellman initial. Soit (v_g, a_g) ce générateur. Comme $\mathcal{A}$ est un anneau, l'espace vectoriel des solutions est simplement $\mathcal{A} \diamond (v_g, a_g)$. En particulier, pour la solution spécifique construite initialement par Alice $(\hat{v}, \hat{a})$ il existe $(\hat{c}, \hat{c}') \in \mathcal{A}^2$ tel que $(\hat{v}, \hat{a}) = (\hat{c}, \hat{c}') \diamond (v_g, a_g)$. Ceci signifie que (v_g, a_g) est simplement $(\hat{v}, \hat{a})$ une fois purgé de ses facteurs dans $\mathcal{A}$. Ceci montre que (v_g, a_g), comme $(\hat{v}, \hat{a})$, est une solution diviseur. Les autres solutions sont générées par des facteurs (c, c') en lien avec les facteurs gauche c de v ou droits c' de u. Finalement, remarquons que (v_g, a_g) est un facteur commun à droite de toutes les solutions linéaires. Comme il est également solution, c'est tout simplement le plus grand diviseur commun à droite de toutes les solutions linéaires non nulles.

7.1.4 Interprétation en termes d'idéaux

Nous cherchons à comprendre la structure de l'espace des solutions de la première équation du système (7.2).

Définissons la notation suivante : si $(x, y) \in \mathcal{D}^2$, on pose$\mathcal{M}(x, y) = \{(v, a) | x \diamond v = a \diamond y\}$. Alors $\tilde{\mathcal{C}}(z) = \mathcal{M}(z, z)$. La proposition 7.1.1 et le corollaire 7.1.2 signifient que $\mathcal{M}(z, w)$ est un bimodule à gauche pour $\tilde{\mathcal{C}}(z)$ et à droite pour $\tilde{\mathcal{C}}(w)$ et que $\tilde{\mathcal{C}}(z)$ est un anneau (d'endomorphismes de $\mathcal{M}(z, m)$).

Nous cherchons à interpréter $\mathcal{M}(z, m)$. Considérons le module des morphismes à droite

$$\mathrm{Hom}_d(\mathcal{D} \diamond z, \mathcal{D} \diamond m) = \{v \in \mathcal{D} | \mathcal{D} \diamond z \diamond v \subseteq \mathcal{D} \diamond m\}.$$

En effet, si $\mathcal{D} \diamond z \diamond v \subseteq \mathcal{D} \diamond m$, en particulier $z \diamond v \in \mathcal{D} \diamond m$. Comme $\mathcal{D}$ est intègre, il existe donc (exactement) un $a \in \mathcal{D}$ tel que $z \diamond v = a \diamond m$. On définit de même :

$$\mathrm{Hom}_g(m \diamond \mathcal{D}, z \diamond \mathcal{D}) = \{a \in \mathcal{D} | a \diamond m \diamond \mathcal{D} \subseteq z \diamond \mathcal{D}\}.$$

a est uniquement déterminé par v et réciproquement v est uniquement déterminé par a. On a donc un isomorphisme

$$i : \mathrm{Hom}_g(m \diamond \mathcal{D}, z \diamond \mathcal{D}) \longrightarrow \mathrm{Hom}_d(\mathcal{D} \diamond z, \mathcal{D} \diamond m)$$

$\mathcal{M}(z, w)$ correspond donc aux couples d'éléments (v, a) de $\mathrm{Hom}_d(\mathcal{D} \diamond z, \mathcal{D} \diamond w) \times \mathrm{Hom}_g(m \diamond \mathcal{D}, z \diamond \mathcal{D})$ tel que v est envoyé sur a par l'isomorphisme précédent. C'est-à-dire que l'application $(v, a) \mapsto \big(v, i(a)\big)$ envoie $\mathcal{M}(z, w)$ sur la diagonale de l'ensemble $\mathrm{Hom}_d(\mathcal{D} \diamond z, \mathcal{D} \diamond w)^2$.

7.2 Application : cryptosystèmes de polynômes tordus

Des cryptosystèmes de type Diffie-Hellman ou El-Gamal ont été proposés à PQ-Crypto 2010 [10]. Le protocole Diffie-Hellman suit exactement la construction générique présentée au chapitre 1.2. Dans cette section, nous revoyons la construction du cryptosystème dans le cas particulier des polynômes tordus et nous déroulons l'attaque dans ce cas particulier. Comme le chiffrement El-Gamal repose sur le problème Diffie-Hellman 1.2.1, nous ne considérons que le protocole Diffie-Hellman.

7.2.1 Sécurité et dimensionnement

Comme précisé au chapitre 6, l'anneau des polynômes tordus est un anneau non commutatif, euclidien à gauche et à droite. C'est-à-dire qu'il existe un algorithme de division euclidienne et qu'on peut calculer des pgcd à gauche et à droite.

Comme précisé plus haut dans le cadre générique, comme le produit $\star$ n'est pas commutatif, un polynôme tordu admet beaucoup de factorisations au lieu d'une unique. On s'attend à ce que le cardinal de l'ensemble des factorisations soit exponentiel en le degré du polynôme. Ceci donne l'idée du dimensionnement de la sécurité du cryptosystème par ses concepteurs : bien qu'il soit peu complexe de faire des calculs sur les polynômes tordus, il devrait être difficile de retrouver la décomposition précise des éléments échangés par les protagonistes parmi leurs nombreuses factorisations possibles.

Nous rappelons ici la spécification proposée par [10]. Toutefois, l'attaque est indépendante de la méthode de génération des clefs.

Une approche type "force brute" est proposée pour construire l'ensemble commutatif $\mathcal{S}$, comme rappelé ci-dessus 6.1.2. On construit itérativement un ensemble de générateurs $G_0, \ldots, G_s$ de petit degré δ. À chaque étape, un polynôme de degré δ est choisi aléatoirement et on teste sa commutativité avec l'ensemble des générateurs courant. S'il commute, on l'ajoute à cet ensemble, sinon on recommence. L'ensemble $\mathcal{S}$ est l'algèbre commutative engendrée par ces générateurs.

Soit d le paramètre de sécurité du protocole. On génère un polynôme public $\boldsymbol{Z}$. Lors de l'exécution du protocole Diffie-Hellman, chaque participant choisit deux éléments U et V de degré d dans $\mathcal{S}$, par combinaison des générateurs de $\mathcal{S}$. Plus précisément, U et V sont des produits de sommes de produits des générateurs de $\mathcal{S}$.

Toutes les étapes du protocole reviennent à des opérations d'anneau sur les polynômes tordus et sont donc de complexité pratique. [10] reste vague sur la génération de $\mathcal{S}$. L'instanciation proposée est basée sur les polynômes tordus sur $\mathbb{F}_4$, les générateurs de $\mathcal{S}$ sont de degré 8 ou 9 et le protocole utilise des polynômes tordus de degré $d = 600$. Pour ces paramètres, les auteurs proposent deux exemples d'ensembles $\mathcal{S}$

en fournissant des ensembles de générateurs de plus de 90 polynômes.

Comme étudié ci-dessus 6.1.2, nous avons réduit ces ensembles de générateurs au centre et à deux polynômes de degré 5.

Exemple : Pour clarifier l'exemple, les degrés sont volontairement fortement réduits.

Sur $\mathbb{F}_4 = \{0, 1, \alpha, \alpha^2 = \alpha + 1\}$, soient $\boldsymbol{P_0} = \alpha + X^3$ et

$$\boldsymbol{Z} = X^2 + \alpha^2 X^6 + \alpha^2 X^8 + \alpha X^9 + \alpha X^{10} + \alpha^2 X^{11} + \alpha^2 X^{12} + \alpha^2 X^{13} + \alpha^2 X^{14} + X^{15}.$$

Alice génère deux éléments de $\mathcal{S}$ aléatoires

$$U_A = \alpha + \alpha^2 X^2 + X^3 + \alpha^2 X^4 + X^5 + X^6 + X^7 + \alpha X^8 + X^{11} + X^{12}$$

$$\text{et } V_A = \alpha + \alpha X^2 + X^3 + \alpha^2 X^4 + X^5 + X^6 + X^7 + X^8 + X^{10}$$

et envoie à Bob le polynôme

$$\begin{aligned} \boldsymbol{Z'} = U_A \star \boldsymbol{Z} \star V_A \;=\; & \alpha^2 X^2 + \alpha X^4 + X^5 + \alpha^2 X^6 + X^7 + X^8 + \alpha X^9 + X^{10} + \alpha^2 X^{12} \\ & + X^{13} + \alpha X^{14} + \alpha^2 X^{15} + \alpha X^{18} + X^{19} + \alpha X^{20} + \alpha^2 X^{21} \\ & + \alpha^2 X^{23} + X^{24} + X^{25} + \alpha^2 X^{26} + X^{27} + X^{29} + \alpha X^{30} + \alpha^2 X^{32} \\ & + X^{33} + \alpha X^{34} + \alpha X^{36} + X^{37}. \end{aligned}$$

7.2.2 Déroulement de l'attaque

Soit $\boldsymbol{Z'} = U \star \boldsymbol{Z} \star V$ les données transmises par l'un des participants du protocole. Notre première étape est de calculer le pgcd à gauche de $\boldsymbol{Z'}$ et $\boldsymbol{\Lambda}_i \star \boldsymbol{Z'}$ pour tous les générateurs $\boldsymbol{\Lambda_i}$ de $\mathcal{S}$. Suite à notre remarque précédemment sur le fait que ces générateurs sont en fait issus d'un même polynôme générateur $\boldsymbol{P_0}$, il suffit de prendre le pgcd de $\boldsymbol{Z'}$ et $\boldsymbol{P_0} \star \boldsymbol{Z'}$. On obtient un polynôme $\boldsymbol{G}$ qui est multiple à droite de U : il existe un polynôme A tel que $\boldsymbol{G} = U \star A$. On calcule également $\boldsymbol{M}, \boldsymbol{M}_0$ tels que

$$\begin{cases} \boldsymbol{Z'} &= \boldsymbol{G} \star \boldsymbol{M} \\ \boldsymbol{P_0} \star \boldsymbol{Z'} &= \boldsymbol{G} \star \boldsymbol{M}_0. \end{cases}$$

Et comme l'anneau des polynômes tordus sur un corps fini est intègre, on déduit :

$$\begin{cases} \boldsymbol{Z} \star V &= A \star \boldsymbol{M} \\ \boldsymbol{P_0} \star \boldsymbol{Z} \star V &= A \star \boldsymbol{M}_0. \end{cases}$$

De plus, $\boldsymbol{P_0} \star V = V \star \boldsymbol{P_0}$ puisque V commute avec $\mathcal{S}$. Ces trois équations ne sont

pas linéaires sur $\mathbb{F}_q$ comme elles le seraient avec le produit des polynômes classiques, mais elles le sont tout de même sur le corps invariant par θ $\mathbb{F}_p$. En développant ces équations sur $\mathbb{F}_p$ et en bornant l'espace de recherche grâce au degré attendu de la solution spécifique (V, A), on peut résoudre le système par algèbre linéaire.

Cette phase fournit ainsi un sous-espace borné par le degré de l'espace complet des solutions du système linéaire. D'après la section 7.1.3, l'ensemble complet des solutions est clos par multiplication à gauche par $\mathcal{A} = \tilde{\mathcal{C}}(\boldsymbol{Z}) \cap (\mathcal{C}_{\mathcal{S}}, \mathcal{C}_{\mathcal{S}})$. Si l'espace des solutions complet est monogène pour la linéarité et la multiplication à gauche par $\mathcal{A}$, alors ce générateur est la solution (V, A) de plus bas degré. On peut alors la calculer comme le pgcd à droite d'une base linéaire d'une base d'un sous-espace de solutions de degré borné.

Exemple : Attaque de l'échange précédent.

Ève intercepte le polynôme $\boldsymbol{Z'}$ ci-dessus. envoyé par Alice à Bob et cherche à le décomposer sur $\mathcal{S} \star \boldsymbol{Z} \star \mathcal{S}$. Elle calcule le PGCD à gauche

$$\begin{aligned} G &= \alpha^2 X^2 + \alpha^2 X^3 + \alpha^2 X^5 + X^6 + \alpha X^7 + \alpha^2 X^8 + \alpha^2 X^9 + \alpha^2 X^{10} \\ &\quad + X^{16} + X^{17} + \alpha^2 X^{18} \end{aligned}$$

de $\boldsymbol{Z'}$ et $\boldsymbol{P_0} \star \boldsymbol{Z'}$, et le quotient $\boldsymbol{M}$ tel que $\boldsymbol{Z'} = \boldsymbol{G} \star \boldsymbol{M}$.

$$\begin{aligned} \boldsymbol{M} &= X + \alpha X^2 + \alpha X^4 + \alpha^2 X^5 + X^6 + \alpha^2 X^7 + \alpha^2 X^8 + \alpha X^9 \\ &\quad + \alpha^2 X^{10} + X^{12} + X^{13} + \alpha^2 X^{15} + X^{16} + \alpha X^{17} + \alpha X^{18} + \alpha X^{19}. \end{aligned}$$

Elle calcule ensuite une base des solutions du système $\mathbb{F}_2$-linéaire $\boldsymbol{Z} \star V = A \star \boldsymbol{M}$. Dans cet exemple, le système est de dimension 36 et son espace de solutions est de dimension 1 sur $\mathbb{F}_2$ (il est donc réduit à un unique élément). Si la dimension était supérieure (comme c'est le cas en degré plus élevé), elle aurait dû prendre le PGCD à droite des V_i de la base. Elle trouve ici directement une solution $V = \alpha + \alpha X^2 + X^3 + \alpha^2 X^4 + X^5 + X^6 + X^7 + X^8 + X^{10}$ qui est égal au polynôme V_A choisi initialement par Alice. Elle retrouve le polynôme U_A par simple quotient de $\boldsymbol{Z'}$ par V_A puis $\boldsymbol{Z}$ à droite et elle a résolu le problème de décomposition.

7.2.3 Résultats expérimentaux

Bibliothèque de polynômes tordus

Nous avons réalisé une implémentation simple en `C++` basée sur la bibliothèque NTL [65]. Nous n'avons pas cherché à l'optimiser autrement que par les options du compilateur. En particulier, afin de varier les corps finis utilisés, l'implémentation ne tire pas parti des optimisations spécifiques de la bibliothèque NTL pour les corps

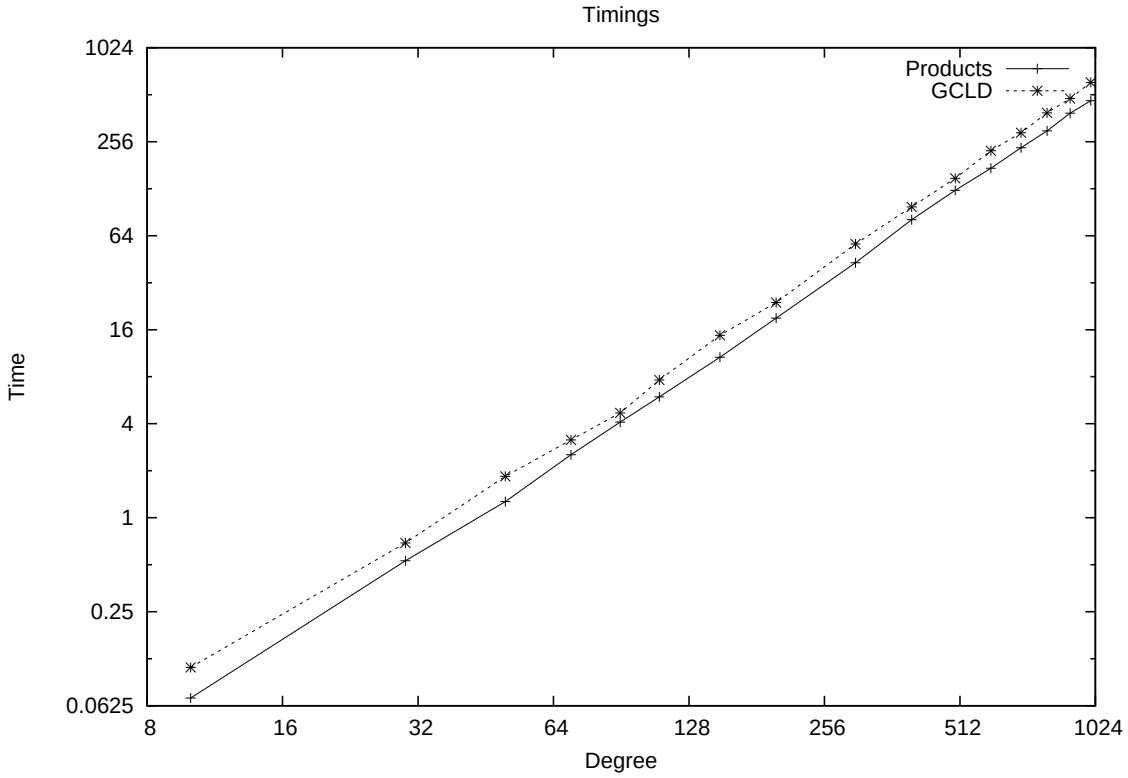

FIGURE 7.1 – Temps de calculs sur $\mathbb{F}_4$, échelles logarithmiques

de caractéristique 2.

La figure 7.1 présente quelques temps de calcul de cette bibliothèque sur un processeur Core i7 à 1.87 GHz, en échelle logarithmique. Il s'agit de réaliser 1000 produits ou calculs de PGCD à gauche de deux polynômes de même degré, celui-ci variant de 10 à 1000. Le caractère non commutatif des polynômes tordus rend l'utilisation d'algorithmes rapides de type Karatsuba pour les produits non triviale. Nous n'avons donc implémenté que les algorithmes naïfs. Cet effet est illustré par le fait que les complexités suivent sensiblement la même loi : après passage au logarithme, le temps de calcul est linéaire en le degré. Les droites correspondantes, pour le PGCD et pour le produit, ont le même coefficient directeur (voisin de 2), ce qui signifie que les complexités de ces algorithmes sont polynomiales de même degré (quadratiques).

Attaque du cryptosystème

Nous avons vérifié les hypothèses précédentes en pratique avec les paramètres recommandés par [10] et au-delà. Dans tous les cas testés, l'espace des solutions en degré borné admettait exactement une solution de degré minimal (à des $\mathbb{F}_p$-multiples près), et toute autre solution était un de ses multiples par un facteur du centre $\mathcal{C}$. Cela montre incidemment que $\mathcal{A} = \mathcal{C} \star (1,1)$ jusqu'à la borne de degré fixée.

Soit (V_g, A_g) le générateur ainsi calculé. Nous avons vérifié qu'il s'agit bien d'une solution diviseur et que c'est le pgcd à droite d'une base linéaire des solutions de degré borné. Nous avons également vérifié que (V_g, A_g) est le plus gros facteur non central de $(\hat{V}, \hat{A})$. Ce facteur non central peut être extrait en calculant le pgcd à gauche de $(\hat{V}, \hat{A})$ par quelques-uns de ses multiples arbitraires à gauche.

Pour un corps de degré m et des polynômes de degré d, l'attaque a une complexité théorique en $\mathcal{O}\big((md)^3\big)$ (ou $(md)^\eta$ où η est la constante de complexité des algorithmes d'algèbre linéaire). Elle prend une minute en pratique, avec les paramètres recommandés (polynômes de degré 600 sur $\mathbb{F}_4$) sur un PC portable doté d'un processeur Celeron à 2.0 GHz.

7.3 Polynômes tordus modulaires

Les polynômes tordus modulaires forment un autre anneau non commutatif sur lequel il serait tentant d'instancier un protocole Diffie-Hellman. Nous reprenons les notations de la section 6.2 : soit N un polynôme du quasi-centre de degré d. Chaque classe modulo N admet un unique représentant de degré inférieur à d. La multiplication des classes se fait en multipliant les représentants canoniques et en réduisant le produit modulo N. Cette opération est notée $\circ$.

On construit de même un ensemble commutatif $\bar{\mathcal{S}}$ en sélectionnant des classes qui commutent avec un représentant canonique de petit degré δ. Comme δ est une constante petite devant le paramètre de sécurité d, on peut supposer que $2\delta < d$. Dans ce cas, les représentants canoniques commutent en fait sans réduction modulo N. Alors, d'après 6.1.6, ces représentants sont générés par le centre et un polynôme unique $\boldsymbol{P_0}$. Les éléments de $\bar{\mathcal{S}}$ sont des combinaisons polynomiales arbiraitres de $\boldsymbol{P_0}$ sur $\mathcal{C}$ réduites modulo N.

7.3.1 Premières remarques

La proposition 6.2.6 signifie que la relation entre les diviseurs et les multiples est très peu contrainte dans $\mathcal{R}/(N)$. Alors, le fait qu'une classe $\bar{\boldsymbol{Z}}'$ soit calculée comme $\bar{U} \circ \bar{\boldsymbol{Z}} \circ \bar{V}$ n'apporte pratiquement aucune information sur le choix particulier de $\bar{U}$ et $\bar{V}$. Ainsi, on ne peut pas espérer récupérer beaucoup d'information en utilisant les pgcds de $\bar{\boldsymbol{Z}}'$ et $\bar{P}_0 \circ \bar{\boldsymbol{Z}}'$. À l'inverse, comme $\bar{P}$ est assez peu contraint par le choix spécifique de $(\bar{U}, \bar{V})$, nous allons profiter du fait qu'il existe énormément de couples équivalents $(\bar{U}, \bar{V})$.

7.3.2 Attaque de la décomposition modulaire

Étant donnée une classe $\bar{\boldsymbol{Z}}'$, nous recherchons une décomposition $\bar{U} \circ \bar{\boldsymbol{Z}} \circ \bar{V}$ où $\bar{U}$ et $\bar{V}$ sont dans $\bar{\mathcal{S}}$ (c'est-à-dire qu'ils commutent avec $P_0 \mod N$). Il en existe au

moins une par construction de $\bar{\boldsymbol{Z}}'$, on s'attend à ce qu'il y en ait beaucoup d'autres.

Nous visons les couples $(\bar{U}, \bar{V})$ dans $\bar{\mathcal{S}} \times \bar{\mathcal{S}}$ tels que par exemple $\bar{U}$ est premier à gauche avec N. Rappelons tout d'abord qu'il est équivalent d'être premier à gauche ou à droite avec N quand N est dans le quasi-centre (proposition 6.2.7).

Maintenant, pour tout $(\bar{U}, \bar{V})$ dans $\bar{\mathcal{S}} \times \bar{\mathcal{S}}$ où $\bar{U}$ est premier avec N, $\bar{U}$ admet un pseudo-inverse à gauche $\bar{W}$ et on a :

$$\bar{\boldsymbol{Z}}' = \bar{U} \circ \bar{\boldsymbol{Z}} \circ \bar{V} \qquad \Longleftrightarrow \qquad \bar{W} \circ \bar{\boldsymbol{Z}}' = \bar{\boldsymbol{Z}} \circ \bar{V}. \tag{7.3}$$

De plus, $\bar{U}$ commute avec $\bar{P}_0$ si et seulement si $\bar{W}$ commute avec $\bar{P}_0$. Les couples décomposants $(\bar{U}, \bar{V}) \in \bar{\mathcal{S}} \times \bar{\mathcal{S}}$ avec $\bar{U}$ inversible sont donc en bijection avec les solutions $(\bar{W}, \bar{V}) \in \bar{\mathcal{S}} \times \bar{\mathcal{S}}$ de l'équation linéaire $\bar{W} \circ \bar{\boldsymbol{Z}}' = \bar{\boldsymbol{Z}} \circ \bar{V}$ avec $\bar{W}$ inversible.

Il suffit donc d'extraire des solutions du système linéaire un couple $(\bar{W}, \bar{V})$ avec $\bar{W}$ inversible pour que l'attaque soit terminée. Pour cela, nous nous fondons sur la densité de ces couples. Observons tout d'abord que se restreindre aux paires de $\bar{\mathcal{S}}$ ne peut avoir qu'un impact négligeable sur la densité des éléments inversibles. En effet, la condition modulaire de coprimalité est exacte (sans modulo) pour toutes les classes dont le représentant canonique est de degré inférieur strictement à $\deg(N) - \deg(P_0)$. Comme $\deg(P_0)$ est une constante qui reste petite asymptotiquement devant $\deg(N) = d$, la fraction des classes pour lesquelles la condition nécessite une réduction modulo N est négligeable. De plus, nous ne voyons aucune raison pour laquelle la densité des $\bar{W}$ parmi les couples solutions $(\bar{W}, \bar{V})$ de l'équation $\bar{W} \circ \bar{\boldsymbol{Z}}' = \bar{\boldsymbol{Z}} \circ \bar{V}$ (en ne se restreignant pas à $\bar{\mathcal{S}}$) différerait de la densité globale. Ceci motive l'heuristique suivante.

Heuristique 7.3.1 *Parmi les solutions $(\bar{W}, \bar{V}) \in \bar{\mathcal{S}} \times \bar{\mathcal{S}}$ de l'équation $\bar{W} \circ \bar{\boldsymbol{Z}}' = \bar{\boldsymbol{Z}} \circ \bar{V}$, la densité des éléments $\bar{W}$ inversibles est identique à la densité des classes inversibles de $\mathcal{R}_N$.*

Bien que N puisse avoir beaucoup de facteurs gauches irréductibles distincts, ils sont un sous-ensemble de tous les facteurs gauche possibles des polynômes de degré $\deg(N)$. Par conséquent, nous nous attendons à ce que la fraction des classes premières à gauche avec N soit asymptotiquement une constante proche de 1. Intuitivement, pour tout $u < d$, la fraction des multiples à droite des polynômes unitaires L de degré u parmi les polynômes de degré inférieur strictement à d est q^{-u}. La probabilité que deux polynômes de degré $< d$ soient tous deux des multiples à droite de L est approximativement q^{-2u}. La probabilité qu'ils ne partagent pas un facteur gauche commun de degré u est $1 - q^u q^{-2u} = 1 - q^{-u}$. En approchant la probabilité qu'ils soient premier entre eux par la probabilité qu'ils ne partagent pas un facteur gauche commun de degré 1, nous nous attendons à ce que la densité des éléments inversible soit de l'ordre de $1 - 1/q$.

7.3.3 Exemple : matrices sur corps fini

Les matrices sur un corps fini forment un anneau non commutatif bien connu, sur lequel il est tentant de vouloir instancier un cryptosystème reposant sur le problème de décomposition Diffie-Hellman.

L'identification entre matrices sur un corps fini et polynômes tordus modulo $X^N - 1$, rappelée en section 6.3.2, montrent que l'attaque décrite dans la section précédente s'applique parfaitement.

Interprétée en termes de matrices, l'heuristique de l'attaque précédente affirme tout simplement que la densité des matrices inversibles sur $\mathbb{F}_q$ est sensiblement égale à $1-1/q$ (en effet une matrice aléatoire sur $\mathbb{F}_q$ a un déterminant nul avec probabilité $1/q$).

7.3.4 Résultats expérimentaux

Nous avons vérifié les propriétés ci-dessus en pratique. Nous avons échantillonné la densité des éléments inversibles parmi les membres de gauche $\bar{W}$ de l'espace de solutions et parmi les classes. Nous avons trouvé des densité du même ordre dans les deux cas : égales en large caractéristique et effectivement proches de $1 - 1/q$, mais légèrement différentes et plus dépendantes de N (quoique toujours strictement plus petites que 1) en petite caractéristique. Nous avons toujours pu extraire une solution décomposante presque instantanément.

Exemple : Soit $\boldsymbol{N} = X^{11}+X^{13}+X^{17}+X^{19}+X^{21}+X^{23}$ et $P_0 = \alpha+X^3+X^5$, alors N ne commute pas avec P_0, et le PGCD (à droite) de N avec P_0 est égal à P_0 donc P_0 et N ne sont pas premiers entre eux. Soit par exemple $\boldsymbol{Z}$: $\alpha X^6+\alpha^2X^7+X^9+\alpha X^{10}+\alpha^2X^{11}+\alpha^2X^{13}+\alpha X^{14}+X^{15}+\alpha X^{18}+\alpha^2X^{21}$, alors l'équation 7.3 est un système $\mathbb{F}_2$-linéaire en les coefficients de $\bar{W}$ et $\bar{V}$, de dimension $2\deg(\mathbb{F}_4)\deg(N) = 92$. L'espace des solutions est de dimension 22, parmi lesquelles une proportion d'environ 48% des $\bar{W}$ sont premiers avec N et commutent avec P_0 modulo N.

Il est intéressant de remarquer que l'attaque peut être légèrement généralisée. On pourrait chercher à obtenir des solutions décomposantes $(\bar{U}, \bar{V})$ telles que $\bar{U}$ a un pgcd à droite avec N qui ne soit pas nécessairement 1 mais un facteur droit G de N qui commute avec $\boldsymbol{P_0}$ (par exemple, un facteur de N qui soit central). Alors, pour un tel $\bar{U}$, il existe $\bar{W}$ tel que $\bar{W} \circ \bar{U} = \bar{G}$. Comme $\bar{U}$ et $\bar{G}$ commutent avec $\boldsymbol{P_0}$, c'est vrai également de $\bar{W}$. Alors, on calcule simplement les solutions $(\bar{W}, \bar{V}) \in \bar{\mathcal{S}} \times \bar{\mathcal{S}}$ de l'équation $\bar{W} \circ \bar{\boldsymbol{Z}}' = \bar{G} \circ \bar{\boldsymbol{Z}} \circ \bar{V}$, et on extrait les $\bar{W}$ tels que le pgcd à gauche de $\bar{W}$ et N soit G.

Conclusion et perspectives

Dans ce mémoire, nous avons étudié diverses primitives cryptographiques reposant de près ou de loin sur la difficulté du problème Diffie-Hellman.

Encodages algébriques vers courbes elliptiques

Nous avons largement étudié les fonctions d'encodage à temps constant vers des courbes elliptiques $\mathcal{E}$ définies sur $\mathbb{F}_q$ quand $q \equiv 2 \mod 3$, c'est-à-dire quand tout élément de $\mathbb{F}_q$ admet une racine cubique. Les fonctions que nous avons étudiées sont définies algébriquement et réalisent un nombre d'opérations constant quelles que soient les entrées. La littérature proposait alors une seule fonction d'encodage de ce type ([38]). Nous en avons donné un nouvel éclairage, théorique.

Après avoir proposé une méthode systématique pour découvrir de nouvelles fonctions d'encodages basées sur la résolubilité d'équations de degré 3, nous avons donné une interprétation géométrique de toutes les fonctions d'encodage algébriques vers des courbes elliptiques utilisant l'existence d'une racine cubique dans $\mathbb{F}_q$ connues dans la littérature. Nous avons montré que toute fonction d'encodage algébrique correspond en fait à une courbe d'intersection paire avec la duale $\hat{\mathcal{E}}$ de $\mathcal{E}$. Cette théorie nous a permis d'exhiber encore de nouvelles fonctions d'encodage et nous avons donné des arguments permettant d'en proposer une classification.

La théorie des fonctions d'encodage que nous avons proposée est donc exhaustive pour les fonctions d'encodage suivantes :

- corps fini $\mathbb{F}_q$ dans lequel tout élément admet une racine cubique ;
- vers des courbes elliptiques $\mathcal{E}_{\mathbb{F}_q}$;
- fonction algébrique : reposant sur les fonctions rationnelles et les racines cubiques.

D'une certaine façon les algorithmes d'encodage algébriques que nous avons proposés, comme ceux de la littérature, sont optimaux : leur complexité est réduite à celle de calculer une exponentiation rapide dans un corps fini. Pour faire plus rapide, il ne faudrait utiliser que des opérations de corps classiques, et donc une paramétrisation rationnelle, ce qui est impossible en genre 1. Néanmoins nous avons proposé une pseudo-paramétrisation des courbes elliptiques hessiennes qui possède la propriété particulière de permettre de calculer *l'ordonnée* d'un point en fonction

du paramètre en utilisant uniquement les équations de corps.

Pour les courbes elliptiques définies sur un corps $\mathbb{F}_q$ avec $q \not\equiv 2 \mod 3$, la question demeure de savoir s'il est possible de faire plus efficace que l'algorithme de Shallue et van de Woestijne décrit à la section 3.2.2.

Encodages algébriques vers des courbes de genre supérieur

Nous avons proposé les premiers encodages algébriques vers de larges familles (dimension 2 sur l'espace de modules) de courbes hyperelliptiques de genre 2 et de genre supérieur. La principale question à ce stade est de trouver des fonctions d'encodage pour presque toutes les courbes de genre 2. L'approche systématique que nous avons proposée n'a pas été poussée très haut en degré et donc en genre : les calculs, en particulier ceux de l'algorithme 4 sont plutôt intimidants.

Pour le genre 2, il serait naturel de chercher à généraliser l'étude géométrique réalisée sur le genre 1 pour expliquer les encodages que nous avons proposés et, éventuellement, d'en trouver de nouveaux. Toutefois, la situation géométrique est plus compliquée, à commencer par la loi de groupe, et il n'est pas garanti que l'on obtienne par dualité toutes les pseudo-paramétrisations possibles, si tant est que cette approche soit fructueuse.

Diffie-Hellman non commutatif

Enfin, nous avons montré que les anneaux de polynômes tordus ne peuvent convenir pour réaliser des cryptosystèmes asymétriques reposant sur le problème de Diffie-Hellman non commutatif. Notre attaque résout le problème Diffie-Hellman sans avoir besoin de retrouver la solution initiale exacte choisie par le participant : elle en trouve simplement une solution équivalente.

La structure des polynômes tordus semble donc trop forte : elle force d'une part une certaine monogénéité de l'ensemble des solutions du problème Diffie-Hellman, d'autre part l'existence d'une division euclidienne permet de démasquer les éléments secret par une simple combinaison de PGCDs bien choisis et d'algèbre linéaire.

Des structures non commutatives sures pour l'implémentation de protocoles asymétriques reposant sur le problème Diffie-Hellman restent encore à trouver. Celles-ci doivent être suffisamment simples pour qu'il soit facile de calculer avec, mais suffisamment complexes et peu structurées pour que le problème Diffie-Hellman ne puisse pas être ramené à un problème d'algèbre linéaire de taille polynomiale.

Annexe A

Code Maple pour les pseudo-paramétrisations

Cette annexe regroupe le code Maple qui effectue les calculs décrits au chapitre 5.

```
#Equation of the Hessian cubic
Hessian:=X^3+Y^3+Z^3-3*a*X*Y*Z;

#The modular invariant of the Hessian cubic
Ja:=27*a^3*(a+2)^3*(a^2-2*a+4)^3/(a-1)^3/(a^2+a+1)^3;

#The equation of the dual curve
Hx:=diff(Hessian,X);Hy:=diff(Hessian,Y);Hz:=diff(Hessian,Z);
with(Groebner):sys:=[Hessian,Hx-U,Hy-V,Hz-W];
#DualHess:=gbasis(sys,plex(X,Y,Z,U,V,W,a))[1];
DualHess:=12*W^2*V^2*U^2*a+V^6-3*W^2*V^2*U^2*a^4-2*W^3*V^3+4*a^3*W^3*V^3+
4*a^3*W^3*U^3+4*a^3*V^3*U^3-2*W^3*U^3-2*V^3*U^3+U^6+W^6-
6*V^4*W*U*a^2-6*a^2*V*U^4*W-6*a^2*W^4*U*V;

#The  Gauss map
GAUSSHESS:=proc(V) subs([X=V[1],Y=V[2],Z=V[3]],[Hx,Hy,Hz]); end proc;

#Flexes
r:=RootOf(x^2+x+1,x);
fle:=[[0,-1,1],[-1,1,0],[1,0,-1],[-r^2,1,0],[1,0,-r^2],[0,-r^2,1],[-r,1,0],
[1,0,-r],[0,-r,1]];

#Flex tangents
FLE:=evala(map(GAUSSHESS,fle));
```

```
#Looking for concurrent flex tangents
with(LinearAlgebra);
RES:=1;
for i1 from 1 to 7 do
for i2 from i1+1 to 8 do
for i3 from i2+1 to 9 do
RES:=RES*evala(factor(Determinant(Matrix(3,[FLE[i1],FLE[i2],FLE[i3]]))));
end do;end do;end do;
print(roots(RES));

#Looking for coconic flex tangents
QUAD:=proc(V) [V[1]^2,V[2]^2,V[3]^2,V[1]*V[2],V[1]*V[3],V[2]*V[3]]; end proc;
QFLE:=evala(map(QUAD,FLE));

for i1 from 1 to 4 do
for i2 from i1+1 to 5 do
for i3 from i2+1 to 6 do
for i4 from i3+1 to 7 do
for i5 from i4+1 to 8 do
for i6 from i5+1 to 9 do
M:=evala(Matrix(6,[QFLE[i1],QFLE[i2],QFLE[i3],QFLE[i4],QFLE[i5],QFLE[i6]]));
ind:=[op({1,2,3,4,5,6,7,8,9} minus {i1,i2,i3,i4,i5,i6})];
N:=evala(Matrix(3,[fle[ind[1]],fle[ind[2]],fle[ind[3]]]));
dM:=evala(Determinant(M));dN:=evala(Determinant(N));
if dM=0 then
print([ind,evala(Determinant(N)),evala(factor(evala(NullSpace(M))))]);
end if;
end do;end do;end do;end do;end do;end do;

#Looking for a unicursal quartic
Quartic:=c400*U^4+c040*V^4+c004*W^4+c310*U^3*V+c301*U^3*W+c031*V^3*W
+c130*U*V^3+c103*U*W^3+c013*V*W^3+c220*U^2*V^2+c202*U^2*W^2
+c022*V^2*W^2+c211*U^2*V*W+c121*U*V^2*W+c112*U*V*W^2;

temp:=collect(subs([U=U+a*W,V=V+W],Quartic),{U,V,W},distributed);

sys:=[coeff(temp,W^4),  coeff(coeff(temp,W^3),U), coeff(coeff(temp,W^3),V),
coeff(coeff(temp,W^2),U^2), coeff(coeff(temp,W^2),V^2),
coeff(coeff(coeff(temp,W^2),U),V),
subs([U=FLE[2][1],V=FLE[2][2], W=FLE[2][3]],Quartic),
```

```
subs([U=FLE[3][1],V=FLE[3][2], W=FLE[3][3]],Quartic),
subs([U=FLE[4][1],V=FLE[4][2], W=FLE[4][3]],Quartic),
subs([U=FLE[5][1],V=FLE[5][2], W=FLE[5][3]],Quartic),
subs([U=FLE[6][1],V=FLE[6][2], W=FLE[6][3]],Quartic),
subs([U=FLE[7][1],V=FLE[7][2], W=FLE[7][3]],Quartic),
subs([U=FLE[8][1],V=FLE[8][2], W=FLE[8][3]],Quartic),
subs([U=FLE[9][1],V=FLE[9][2], W=FLE[9][3]],Quartic)];

sys:=evala(sys);

ic:=solve(sys,[c400,c040,c004,c310,c301,c031,c130,c103,c013,c220,
c202,c022,c211,c121,c112]);
assign(ic);c400:=1;print(Quartic);

#Finding a parameterization of this unicursal quartic
temp:=factor(solve(factor(subs([U=a+u,V=1+t*u,W=1],Quartic)/u^3),u));
deno:=-denom(temp);

Ut:=collect( factor((a+z)*deno)  ,t);
Vt:=collect( factor((1+t*z)*deno)  ,t);
Wt:=deno;

#Solution of the cubic equation to recover  Farashai's parameterization
temp:=collect(subs(Z=1,(collect(subs(X = t*Y-a*t^2*Z, Hessian),
[Y,Z])))/(t^3+1),Y);
s1 := factor(-coeff(temp, Y, 2));
s2 := factor(coeff(temp, Y, 1));
s3 := factor(-coeff(temp, Y, 0));
Delta := factor(81*s3^2-54*s1*s2*s3-3*s1^2*s2^2+12*s1^3*s3+12*s2^3);
delta := 9*(1+a^3*t^3)/(1+t^3);
R := factor(s1^3+27/2*s3-9/2*s1*s2-3/2*delta);
factor(-27*(a^3*t^3+1)/(t^3+1)/R);
Rp := factor(s1^3+27/2*s3-9/2*s1*s2+3/2*delta);

#Intersecting the dual curve with a line
H:=collect(factor(subs([X=i+1,Y=i-t,Z=t-1-(a+1)*i],Hessian)),i);
H:=collect(factor(H/(-a+1)),i);
h:=collect(H/coeff(H,i,3),i);

DI:=factor(-3*discrim(h,i));
```

```
#The conic arising from  the discriminant
eqC :=(4*t*a^3+9*t^2*a^2+9*a^2+6*t*a^2+9*t^2*a+30*t*a+9*a+9*t^2+9+14*t)
-s^2*(1+a+a^2);
eqCp:=factor(subs([t=T/W,s=S/W],-eqC*W^2));

Es:=diff(eqCp,S);Et:=diff(eqCp,T);Ew:=diff(eqCp,W);
A:=[3,1,0];B:=[3,0,1];
TA:=factor(subs([S=3, T=1, W=0],[Es,Et,Ew]/2));
TB:=factor(subs([S=3, T=0, W=1],[Es,Et,Ew]/2));
AB:=[-1,3,3];
Dt:=[AB[1]*j+TB[1],AB[2]*j+TB[2],AB[3]*j+TB[3]];
eqDt:=Dt[1]*S+Dt[2]*T+Dt[3]*W;

#Looking for a parameterization of this conic
lprint(factor(subs(T=-Dt[1]*S/Dt[2]-Dt[3]*W/Dt[2],eqCp)));

#Call m1  the non trivial factor
m1:=(S*a^5+7*S*a^4+19*S*a^3-3*j*S*a^2+26*S*a^2-3*j*S*a+20*S*a-3*j*S+8*S-
78*a^2*W+24*j*W*a+2*j*W*a^3+12*j*W*a^2-3*j^2*W-21*a^4*W-60*a*W-3*a^5*W-
57*a^3*W+16*j*W-24*W);

SW:=factor(solve(m1,S));
TW:=factor(solve(subs(S=SW,eqDt)   ,T));
Wj:=denom(SW);
Sj:=factor(subs(W=Wj,SW));
Tj:=factor(subs(W=Wj,TW));

#Solving the cubic equation
Dj:=factor(subs(t=Tj/Wj,DI));
dj:= 9*(3*a^5+21*a^4+57*a^3-2*j*a^3+78*a^2-12*j*a^2+60*a-24*j*a+24-16*j+3*j^2)
*(-j+3*a^2+3*a+3)*j/(a^3+6*a^2+12*a-3*j+8)^2/(a^2+a+1)^3;

tj:= factor(Tj/Wj);
s1:= factor(subs(t=tj, -coeff(h,i,2)));
s2:= factor(subs(t=tj, coeff(h,i,1)));
s3:= factor(subs(t=tj, -coeff(h,i,0)));

factor(s1^2-3*s2);
```

A.1 Courbes elliptiques sous forme de Weierstrass

```
#Equation of the Weierstrass cubic
Weier:=Y^2*Z-X^3-a*X*Z^2-b*Z^3;

#The equation of the dual curve
Wx:=diff(Weier,X);Wy:=diff(Weier,Y);Wz:=diff(Weier,Z);
with(Groebner):sys:=[Weier,Wx-U,Wy-V,Wz-W];
DualWeier:=gbasis(sys,plex(X,Y,Z,U,V,W,a))[1];

#The  Gauss map
GAUSSWEIER:=proc(V) subs([X=V[1],Y=V[2],Z=V[3]],[Wx,Wy,Wz]); end proc;

#Flexes
psi3:=3*x^4 + 6*a*x^2 + 12*b*x-a^2;
xx:=RootOf(psi3,x);
yy:=RootOf(y^2-xx^3-a*xx-b,y);

fleW:=[[0,1,0],[xx,yy,1]];

#Flex tangents
FLEW:=evala(map(GAUSSWEIER,fleW));

#Looking for a unicursal quartic
WQUARTIC:=d400*U^4+d040*V^4+d004*W^4+d310*U^3*V+d301*U^3*W+d031*V^3*W
+d130*U*V^3+d103*U*W^3+d013*V*W^3+d220*U^2*V^2+d202*U^2*W^2
+d022*V^2*W^2+d211*U^2*V*W+d121*U*V^2*W+d112*U*V*W^2;

d004:=0; d013:=0;d103 := 0; d202 := 0; d112 :=0; d022 := 0;

temp:=evala(subs([U=FLEW[2][1],V=FLEW[2][2], W=FLEW[2][3] ], WQUARTIC));
temp0:=coeff(temp,yy,0);
temp1:=coeff(temp,yy,1);
sys := [numer(coeff(temp0,xx,0)),numer(coeff(temp0,xx,1)),
numer(coeff(temp0,xx,2)),numer(coeff(temp0,xx,3)),
numer(coeff(temp1,xx,0)),numer(coeff(temp1,xx,1)),
numer(coeff(temp1,xx,2)),numer(coeff(temp1,xx,3))];

temp:=solve(sys,[d400,d040,d310,d301,d031,d130,d220,d211,d121]);
assign(temp);d400:=1;print(WQUARTIC);
```

```
#Parameterisation of this quartic
temp:=factor(solve(factor(subs([U=u,V=t*u,W=1],WQUARTIC)/u^3),u));
deno:=denom(temp);

Ut:=collect( factor((temp)*deno)  ,t);
Vt:=collect( factor((t*temp)*deno)  ,t);
Wt:=deno;

#Solution of the cubic equation to recover Icart's parameterization
temp := subs(Z=1,Weier);
temp := collect(numer(factor(subs(Y = 1/6/t^3-a*t/2-X/t, temp))), X);
temp :=  collect(temp/coeff(temp,X,3),X);
s1 := factor(-coeff(temp,X,2));
s2 := factor(coeff(temp,X,1));
s3 := factor(- coeff(temp,X,0));
Delt := factor(81*s3^2-54*s1*s2*s3-3*s1^2*s2^2+12*s1^3*s3+12*s2^3);
delt:= 1/12*(-1-108*b*t^6-18*a*t^4+27*a^2*t^8)/t^6;
R := factor(s1^3+27*s3/2-9/2*s1*s2-3*delt/2);
Rp := factor(s1^3+27*s3/2-9/2*s1*s2+3*delt/2);


#Plotting the intersection between the unicursal quartic
#and the dual of the cubic
with(plots,display);
with(plots,implicitplot);

a:=1; b:=1;

z1 := implicitplot(subs(W=1,WQUARTIC),U=-2..2,V=-2..2,
numpoints = 100000,axes = none,color=red,  resolution = 4000, thickness = 2);
z2 := implicitplot(subs(W=1,DualWeier),U=-2..2,V=-2..2,
numpoints = 100000,axes = none,color=black, resolution = 4000, thickness = 2);

display({z1,z2});
```

Index

Bibliographie

[1] George Salmon (1819-1904). *A treatise on the higher plane curves, intended as a sequel to a treatise on conic sections*. Hodges, Dublin, 1873.

[2] Manindra Agrawal, Neeraj Kayal, and Nitin Saxena. PRIMES is in P. *Ann. of Math*, 2 :781–793, 2002.

[3] Arnaud Beauville. Counting rational curves on $K3$ surfaces. *Duke Math. J.*, 97(1) :99–108, 1999.

[4] D. J. Bersntein, D. Kohel, and T. Lange. Twisted Hessian curves. http://www.hyperelliptic.org/EFD/g1p/auto-twistedhessian.html.

[5] D. Boneh and M. Franklin. Identity-Based Encryption from the Weil Pairing. In Joe Kilian, editor, *Advances in Cryptology – CRYPTO ' 2001*, volume 2139 of *Lecture Notes in Computer Science*, pages 213–229. Springer-Verlag, Berlin Germany, 2001.

[6] Dan Boneh, Antoine Joux, and Phong Q. Nguyen. Why textbook ElGamal and RSA encryption are insecure. In Tatsuaki Okamoto, editor, *ASIACRYPT*, volume 1976 of *Lecture Notes in Computer Science*, pages 30–43. Springer, 2000.

[7] Dan Boneh, Ben Lynn, and Hovav Shacham. Short signatures from the Weil pairing. In *Proceedings of the 7th International Conference on the Theory and Application of Cryptology and Information Security : Advances in Cryptology*, ASIACRYPT '01, pages 514–532, London, UK, UK, 2001. Springer-Verlag.

[8] R. L. Borger. On De Moivre's quintic. *The American Mathematical Monthly*, 15(10) :171–174, 1908.

[9] W. Bosma, J. Cannon, and C. Playoust. The Magma Algebra System I : The user language. *J. Symb. Comput.*, 24(3/4) :235–265, 1997.

[10] Delphine Boucher, Philippe Gaborit, Willi Geiselmann, Olivier Ruatta, and Felix Ulmer. Key exchange and encryption schemes based on non-commutative skew polynomials. In Nicolas Sendrier, editor, *PQCrypto*, volume 6061 of *Lecture Notes in Computer Science*, pages 126–141. Springer, 2010.

[11] Charles Bouillaguet, Jean-Charles Faugère, Pierre-Alain Fouque, and Ludovic Perret. Practical cryptanalysis of the identification scheme based on the iso-

morphism of polynomial with one secret problem. In Catalano et al. [18], pages 473–493.

[12] Victor Boyko, Philip D. MacKenzie, and Sarvar Patel. Provably secure password-authenticated key exchange using Diffie-Hellman. In Preneel [60], pages 156–171.

[13] Eric Brier, Jean-Sébastien Coron, Thomas Icart, David Madore, Hugues Randriam, and Mehdi Tibouchi. Efficient indifferentiable hashing into ordinary elliptic curves. In Tal Rabin, editor, *CRYPTO*, volume 6223 of *Lecture Notes in Computer Science*, pages 237–254. Springer, 2010.

[14] Egbert Brieskorn and Horst Knörrer. *Plane algebraic curves*. Birkhäuser Verlag, Basel, 1986. Translated from the German by John Stillwell.

[15] Ran Canetti, Oded Goldreich, and Shai Halevi. The random oracle methodology, revisited. *J. ACM*, 51(4) :557–594, 2004.

[16] David G. Cantor. Computing in the jacobian of a hyperelliptic curve. *Mathematics of Computation*, 48.

[17] G. Cardona and J. Quer. Curves of genus 2 with group of automorphisms isomorphic to D_8 or D_{12}. *Trans. Amer. Math. Soc.*, 359 :2831–2849, 2007.

[18] Dario Catalano, Nelly Fazio, Rosario Gennaro, and Antonio Nicolosi, editors. *Public Key Cryptography - PKC 2011 - 14th International Conference on Practice and Theory in Public Key Cryptography, Taormina, Italy, March 6-9, 2011. Proceedings*, volume 6571 of *Lecture Notes in Computer Science*. Springer, 2011.

[19] Jung Hee Cheon and Byungheup Jun. A polynomial time algorithm for the braid Diffie-Hellman conjugacy problem. In Dan Boneh, editor, *CRYPTO*, volume 2729 of *Lecture Notes in Computer Science*, pages 212–225. Springer, 2003.

[20] Henri Cohen and Gerhard Frey, editors. *Handbook of elliptic and hyperelliptic curve cryptography*. CRC Press, 2005.

[21] R.S. Coulter, G. Havas, and M. Henderson. Giesbrecht's algorithm, the HFE cryptosystem, and Ore's ps-polynomials. In *Computer Mathematics : Proceedings of the Fifth Asian Symposium (ASCM 2001) (K. Shirayanagi and K. Yokoyama, eds.), Lecture Notes Series on Computing, vol. 9, World Scientific*, pages 36–45, 2001.

[22] Jean-Marc Couveignes. Quelques mathématiques de la cryptologie à clés publiques (Journées annuelles de la SMF). *Nouvelles méthodes mathématiques pour la cryptographie*, 2007.

[23] Jean Marc Couveignes and Jean-Gabriel Kammerer. The geometry of flex tangents to a cubic curve and its parameterizations. *J. Symb. Comput.*, 47(3) :266–281, 2012.

[24] D. A. Cox. *Galois theory*. Pure and Applied Mathematics (New York). Wiley-Interscience [John Wiley & Sons], Hoboken, NJ, 2004.

[25] Whitfield Diffie and Martin E. Hellman. New directions in cryptography. *IEEE Transactions on Information Theory*, 22(6) :644–654, 1976.

[26] Vivien Dubois and Jean-Gabriel Kammerer. Cryptanalysis of cryptosystems based on non-commutative skew polynomials. In Catalano et al. [18], pages 459–472.

[27] David S. Dummit and Richard M. Foote. *Abstract algebra*. John Wiley & Sons Inc., Hoboken, NJ, third edition, 2004.

[28] R. R. Farashahi and M. Joye. Efficient Arithmetic on Hessian Curves. In *Public Key Cryptography - PKC 2010*, volume 6056 of *Lecture Notes in Computer Science*, pages 243–260. Springer, 2010.

[29] Reza Rezaeian Farashahi. Hashing into Hessian Curves. Cryptology ePrint Archive, Report 2010/373, 2010. http://eprint.iacr.org/.

[30] Reza Rezaeian Farashahi, Pierre-Alain Fouque, Igor Shparlinski, Mehdi Tibouchi, and José Felipe Voloch. Indifferentiable deterministic hashing to elliptic and hyperelliptic curves. *Math. Comput.*, 82(281), 2013.

[31] Pierre-Alain Fouque and Mehdi Tibouchi. Deterministic encoding and hashing to odd hyperelliptic curves. In Joye et al. [44], pages 265–277.

[32] W. Fulton and R. Weiss. *Algebraic curves : an introduction to algebraic geometry*. Mathematics lecture note series. Benjamin, 1969.

[33] Taher El Gamal. A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Transactions on Information Theory*, 31(4) :469–472, 1985.

[34] I. M. Gelfand, M. M. Kapranov, and A. V. Zelevinsky. *Discriminants, resultants, and multidimensional determinants*. Mathematics : Theory & Applications. Birkhäuser Boston Inc., Boston, MA, 1994.

[35] Mark Giesbrecht. Factoring in skew-polynomial rings over finite fields. *J. Symb. Comput.*, 26(4) :463–486, 1998.

[36] J. W. P. Hirschfeld. Codes on curves and their geometry. *Rend. Circ. Mat. Palermo (2) Suppl.*, (51) :123–137, 1998.

[37] J. W. P. Hirschfeld, G. Korchmáros, and F. Torres. *Algebraic curves over a finite field*. Princeton Series in Applied Mathematics. Princeton University Press, Princeton, NJ, 2008.

[38] Thomas Icart. How to hash into elliptic curves. In Shai Halevi, editor, *CRYPTO*, volume 5677 of *Lecture Notes in Computer Science*, pages 303–316. Springer, 2009.

[39] Thomas Icart. Elliptic curve point generation algorithms and applications, PhD Thesis of the University of Luxembourg, 2010.

[40] Jun-Ichi Igusa. Arithmetic variety of moduli for genus two. *Annals of Mathematics*, 72(3) :612–649, Nov. 1960.

[41] Waterloo Maple Incorporated. Maple. http://www.maplesoft.com/. Waterloo, Ontario, Canada.

[42] David P. Jablon. Strong Password-only Authenticated Key Exchange. *SIGCOMM Comput. Commun. Rev.*, 26(5) :5–26, October 1996.

[43] Antoine Joux. A One Round Protocol for Tripartite Diffie-Hellman. *J. Cryptology*, 17(4) :263–276, 2004.

[44] Marc Joye, Atsuko Miyaji, and Akira Otsuka, editors. *Pairing-Based Cryptography - Pairing 2010 - 4th International Conference, Yamanaka Hot Spring, Japan, December 2010. Proceedings*, volume 6487 of *Lecture Notes in Computer Science*. Springer, 2010.

[45] Jean-Gabriel Kammerer, Reynald Lercier, and Guénaël Renault. Encoding points on hyperelliptic curves over finite fields in deterministic polynomial time. In Joye et al. [44], pages 278–297.

[46] Ki Hyoung Ko, Sangjin Lee, Jung Hee Cheon, Jae Woo Han, Ju-Sung Kang, and Choonsik Park. New public-key cryptosystem using braid groups. In Mihir Bellare, editor, *CRYPTO*, volume 1880 of *Lecture Notes in Computer Science*, pages 166–183. Springer, 2000.

[47] Neal Koblitz. Elliptic curve cryptosystems. *Mathematics of Computation*, 48(177) :203–209, January 1987.

[48] Neal Koblitz. *Algebraic aspects of cryptography*, volume 3 of *Algorithms and Computation in Mathematics*. Springer-Verlag, Berlin, 1998. With an appendix by Alfred J. Menezes, Yi-Hong Wu and Robert J. Zuccherato.

[49] Paul C. Kocher, Joshua Jaffe, and Benjamin Jun. Differential power analysis. In Michael J. Wiener, editor, *CRYPTO*, volume 1666 of *Lecture Notes in Computer Science*, pages 388–397. Springer, 1999.

[50] Abhinav Kumar. *K3 surfaces of high rank*. ProQuest LLC, Ann Arbor, MI, 2006. Thesis (Ph.D.)–Harvard University.

[51] Junho Lee and Naichung Conan Leung. Yau-Zaslow formula on $K3$ surfaces for non-primitive classes. *Geom. Topol.*, 9 :1977–2012 (electronic), 2005.

[52] Karl Mahlburg. An overview of braid group cryptography. http://www.math.wisc.edu/~boston/mahlburg.pdf, 2004.

[53] Ueli M. Maurer, Renato Renner, and Clemens Holenstein. Indifferentiability, impossibility results on reductions, and applications to the random oracle me-

thodology. In Moni Naor, editor, *TCC*, volume 2951 of *Lecture Notes in Computer Science*, pages 21–39. Springer, 2004.

[54] B.R. McDonald. *Finite rings with identity*. Pure and applied mathematics. M. Dekker, 1974.

[55] Victor S. Miller. Use of elliptic curves in cryptography. In Hugh C. Williams, editor, *CRYPTO*, volume 218 of *Lecture Notes in Computer Science*, pages 417–426. Springer, 1985.

[56] Oystein Ore. Theory of noncommutative polynomials. *Annals of Mathematics*, 34(3) :480–508, July 1933.

[57] Jacques Patarin. Hidden fields equations (HFE) and isomorphisms of polynomials (IP) : Two new families of asymmetric algorithms. In *EUROCRYPT*, pages 33–48, 1996.

[58] Ludovic Perret. A fast cryptanalysis of the isomorphism of polynomials with one secret problem. In Ronald Cramer, editor, *EUROCRYPT*, volume 3494 of *Lecture Notes in Computer Science*, pages 354–370. Springer, 2005.

[59] Carl Pomerance. A tale of two sieves. *Notices Amer. Math. Soc*, 43 :1473–1485, 1996.

[60] Bart Preneel, editor. *Advances in Cryptology - EUROCRYPT 2000, International Conference on the Theory and Application of Cryptographic Techniques, Bruges, Belgium, May 14-18, 2000, Proceeding*, volume 1807 of *Lecture Notes in Computer Science*. Springer, 2000.

[61] Matthias Schütt and Tetsuji Shioda. Elliptic surfaces. In *Algebraic geometry in East Asia—Seoul 2008*, volume 60 of *Adv. Stud. Pure Math.*, pages 51–160. Math. Soc. Japan, Tokyo, 2010.

[62] J. Rafael Sendra and Sevilla David. Radical parametrizations of algebraic curves by adjoint curves. *Journal of Symbolic Computation*, 46(9) :1030–1038, 2011.

[63] J. Rafael Sendra, Franz Winkler, and Sonia Pérez-Díaz. *Rational algebraic curves, A computer algebra approach*, volume 22 of *Algorithms and Computation in Mathematics*. Springer, Berlin, 2008.

[64] Andrew Shallue and Christiaan van de Woestijne. Construction of rational points on elliptic curves over finite fields. In Florian Hess, Sebastian Pauli, and Michael E. Pohst, editors, *ANTS*, volume 4076 of *Lecture Notes in Computer Science*, pages 510–524. Springer, 2006.

[65] Victor Shoup. NTL : A library for doing number theory. Available at http://www.shoup.net/ntl.

[66] Vladimir Shpilrain and Alexander Ushakov. The conjugacy search problem in public key cryptography : unnecessary and insufficient. Cryptology ePrint Archive, Report 2004/321, 2004. http://eprint.iacr.org/.

[67] J.H. Silverman. *The Arithmetic of Elliptic Curves.* Graduate Texts in Mathematics. Springer, 2009.

[68] M. Skalba. Points on elliptic curves over finite fields. *Acta Arith*, 117 :293–301, 2005.

[69] Henning Stichtenoth. *Algebraic Function Fields and Codes.* Springer Publishing Company, Incorporated, 2nd edition, 2008.

[70] M. Ulas. Rational points on certain hyperelliptic curves over finite fields. *Bull. Polish Acad. Sci. Math.*, (55) :97–104, 2007.

[71] Baosen Wu. The number of rational curves on $K3$ surfaces. *Asian J. Math.*, 11(4) :635–650, 2007.

[72] O. Zariski. Sull'impossibilità di risolvere parametricamente per radicali un'equazione algebrica $f(x, y) = 0$ di genere $p > 6$ a moduli generali. Atti Accad. Naz. Lincei Rend., Cl. Sc. fis. Mat. Natur., serie VI, 3 :660–666, 1926.

Résumé

L'objet de cette thèse est l'étude de diverses primitives cryptographiques utiles dans des protocoles Diffie-Hellman.
Nous étudions tout d'abord les protocoles Diffie-Hellman sur des structures commutatives ou non. Nous en proposons une formulation unifiée et mettons en évidence les différents problèmes difficiles associés dans les deux contextes.
La deuxième partie est consacrée à l'étude de pseudo-paramétrisations de courbes algébriques en temps *constant* déterministe, avec application aux fonctions de hachage vers les courbes. Les propriétés des courbes algébriques en font une structure de choix pour l'instanciation de protocoles reposant sur le problème Diffie-Hellman. En particulier, ces protocoles utilisent des fonctions qui hachent directement un message vers la courbe. Nous proposons de nouvelles fonctions d'encodage vers les courbes elliptiques et pour de larges classes de fonctions hyperelliptiques. Nous montrons ensuite comment l'étude de la géométrie des tangentes aux points d'inflexion des courbes elliptiques permet d'unifier les fonctions proposées tant dans la littérature que dans cette thèse.
Dans la troisième partie, nous nous intéressons à une nouvelle instanciation de l'échange Diffie-Hellman. Elle repose sur la difficulté de résoudre un problème de factorisation dans un anneau de polynômes non commutatifs. Nous montrons comment un problème de décomposition Diffie-Hellman sur un groupe non commutatif peut se ramener à un simple problème d'algèbre linéaire pourvu que les éléments du groupe admettent une représentation par des matrices. Bien qu'elle ne soit pas applicable directement au cas des polynômes tordus puisqu'ils n'ont pas d'inverse, nous profitons de l'existence d'une notion de divisibilité pour contourner cette difficulté. Finalement, nous montrons qu'il est possible de résoudre le problème Diffie-Hellman sur les polynômes tordus avec complexité polynomiale.

In this thesis, we study several cryptographic primitives of use in Diffie-Hellman like protocols. We first study Diffie-Hellman protocols on commutative or noncommutative structures. We propose an unified wording of such protocols and bring out on which supposedly hard problem both constructions rely on.
The second part is devoted to the study of pseudo-parameterization of algebraic curves in deterministic *constant* time, with application to hash function into curves. Algebraic curves are indeed particularly interesting for Diffie-Hellman like protocols. These protocols often use hash functions which directly hash into the curve. We propose new encoding functions toward elliptic curves and toward large classes of hyperelliptic curves. We then show how the study of the geometry of flex tangent of elliptic curves unifies the encoding functions as proposed in the litterature and in this thesis.
In the third part, we are interested in a new instantiation of the Diffie-Hellman key exchange. It relies on the difficulty of factoring in a non commutative polynomial ring. We show how to reduce a Diffie-Hellman decomposition problem over a noncommutative group to a simple linear algebra problem, provided that group elements can be represented by matrices. Although this is not directly relevant to the skew polynomial ring because they have no inverse, we use the divisibility to circumvent this difficulty. Finally, we show it's possible to solve the Diffie-Hellman problem on skew polynomials with polynomial complexity.