Université de Limoges

Mémoire d'Habilitation à Diriger des Recherches

(spécialité : mathématiques et applications)

–=–=–=–=–=–=–

Contributions en Mathématiques Discrètes & Applications Cryptographiques

–=–=–=–=–=–=–

Soutenu le 12 novembre 2014 par

François Arnault

Jury

Alain Barthélemy	Directeur de Recherche CNRS à l'Université de Limoges
Thierry Berger	Professeur à l'Université de Limoges
Jean-Marc Couveignes	Professeur à l'Université de Bordeaux (Rapporteur)
Claude Crépeau	Professeur à l'Université de Montréal (Rapporteur)
François Laubie	Professeur à l'Université de Limoges
Jean-Pierre Tillich	Directeur de Recherche à l'INRIA Rocquencourt (Rapporteur)
Denis Simon	Professeur à l'Université de Caen-Basse Normandie (Président)

François ARNAULT
Université de Limoges, Faculté des Sciences & Techniques
Laboratoire XLIM (UMR CNRS 7252)
123, av Albert Thomas, 87060 Limoges Cedex FRANCE
E-Mail : arnault@unilim.fr

Remerciements

Je voudrais tout d'abord remercier Thierry Berger, le chargé de suivi de cet ultime diplôme, mais plus concrètement celui avec qui j'ai partagé les mêmes bureaux pendant de très nombreuses années. Je le remercie pour cette longue collaboration sur les registres à décalages, thème vers lequel je ne me serais probablement pas tourné seul. Mon souci de formalisation précise et de rigueur mathématique a finalement trouvé grande satisfaction à se confronter aux nombreuses idées de Thierry.

Je remercie particulièrement les membres du jury :

• Jean-Marc Couveignes, que j'admire pour son immense savoir mathématique, la qualité de ses travaux, sa gentillesse et sa modestie. Sa relecture et le rapport qu'il a rédigé bien avant la soutenance m'ont apporté bien des encouragements.

• Claude Crépeau qui a aussi accepté et soigneusement accompli cette tâche de rapporteur. Je lui en suis reconnaissant, en particulier pour son expertise sur la partie quantique.

• Jean-Pierre Tillich qui a bien voulu rapporter sur un travail où les mots « code » et « codage » sont absents mais qui n'échappe pas à son large domaine de compétences. Merci Jean-Pierre pour ta lecture attentive et tes questions pertinentes.

• Alain Barthélemy qui a eu la gentillesse d'accepter de participer à un jury de mathématiciens. Je suis heureux de voir que mon travail a pu retenir son attention de physicien.

• François Laubie qui manifeste une certaine bienveillance envers mes travaux, même s'ils ont le défaut d'avoir quelques applications.

• Denis Simon, qui a bien voulu faire partie de ce jury, quelques temps après celui de la thèse d'Aurore. Le plaisir de faire en voiture l'aller-retour Caen-Limoges dans la même journée pourra difficilement le récompenser de son travail.

Ce mémoire est aussi et surtout l'occasion de dire un grand merci à mes co-auteurs : Cédric Lauradoux, Marine Minier, Abdelkader Necer, Erik J. Pickett, Benjamin Pousse et Stéphane Vinatier, grâce à qui j'ai pu partager le plaisir de la recherche, et varier mes centres d'intérêt.

Je remercie chaleureusement Tomasz Paterek qui m'a invité, suite à ma première publication dans le domaine quantique, dans son prestigieux laboratoire CQT à Singapour, m'apportant un formidable encouragement. De plus, il semble que, grâce à lui, nous venons enfin à bout d'un travail inextricable sur l'intrication, débuté à cette occasion.

Je dois beaucoup à mes étudiants en thèse Guilhem Castagnos et Aurore Bernard que j'ai eu le plaisir d'encadrer il y a quelques années, et à Zoé Amblard que je fais maintenant plancher sur une thématique hasardeuse mais prometteuse (le quantique).

Je dois aussi à de nombreux étudiants de DEA, DESS, Master, voire Licence, grâce auxquels j'ai beaucoup appris en préparant des cours pointus sur des domaines très variés, allant des mathématiques dites pures aux travaux pratiques cartes à puces sous Linux, en passant par de très divers problèmes cryptographiques.

Merci enfin à celles et ceux qui, au Département Maths-Info, œuvrent au quotidien pour essayer de nous rendre la vie un peu plus facile : Annie, Catherine, Debora, Henri, Odile, Saloi, Sandrine, Yolande. Merci aussi aux collègues qui, ne travaillant pas forcément dans les mêmes domaines que moi, m'ont manifesté leur sympathie à cette occasion.

Table des matières

Introduction

Ce mémoire présente un panorama d'une activité de recherche étalée sur une quinzaine d'années. Si l'on y rajoute les tests de primalité qui ne sont pas repris ici mais qui ont accompagné mes premiers pas dans la recherche [5][6][7][8], on peut estimer que les domaines abordés sont variés, voire hétéroclites.

Dans cette variété, on peut remarquer que la notion d'aléa est presque toujours présente sous une forme ou sous une autre :

• Les tests de primalité servent avant tout à générer des clés aléatoires. D'autre part, les algorithmes sous-jacents sont probabilistes, dans le sens où ils ont une probabilité d'erreur non nulle (mais maîtrisée), mais souvent aussi dans le sens où ils ont nécessitent de façon essentielle de l'aléa pour fonctionner efficacement.

• Les algorithmes de chiffrement, en particulier ceux étudiés par mon étudiant Guilhem Castagnos [23][24] et ceux attaqués par mon étudiante Aurore Bernard [19] sont probabilistes ; l'aléa y jouant un rôle essentiel pour assurer leur sécurité.

• L'étude des registres à décalage [9][10][11][12][13][14], est clairement dédiée à la production d'aléa.

• Mon domaine de recherche le plus récent et actuellement le plus actif [2][4], autour de l'information quantique, est lié à l'aléa de façon encore plus intime, puisqu'ici la nature manifeste un caractère fondamentalement aléatoire. En particulier, les inégalités de Bell révèlent que cet aléa est incompatible avec notre vision classique du monde physique. Il reste beaucoup à faire pour comprendre les mystères de cet aléa fondamental et apprendre à en exploiter les formidables possibilités que nous commençons à entrevoir.

1. Présentation générale

Chapitre 1

Le chapitre 1 présente le travail effectué avec Guilhem Castagnos, le premier étudiant en thèse dont j'ai entièrement assuré l'encadrement scientifique. Guilhem a soutenu en 2006 un mémoire intitulé « Quelques schémas de cryptographie asymétrique probabiliste » [23].

Chapitre 2

Le chapitre 2 expose un travail en collaboration avec Aurore Bernard, dont j'ai aussi encadré la thèse, soutenue en 2011.

Les formes quadratiques binaires et leur loi de composition découverte par Gauss ont fourni des structures algébriques ayant de nombreuses applications en cryptographie et en théorie des nombres algorithmique (factorisation, logarithme discret).

Aurore et moi avons précisé les liens existant entre les formes de discriminant fondamental D, et celles de discriminant Df^2, où le conducteur f est un entier. On montre que les classes de formes de discriminant D ce scindent en plusieurs classes de formes de discriminant Df^2. Les constructions de ces classes sont explicites, et respectent les structures de groupes découvertes par Gauss. Les classes des formes de discriminant Df^2 se regroupent donc en une relation d'équivalence plus faible, induite par les classes de discriminant D. J'ai approfondi ce travail par la suite.

Cette structure peut être exploitée en cryptographie. Il existe des systèmes de chiffrement, nommés NICE, basés sur des formes quadratiques de discriminant Df^2, dont la sécurité était mal connue. Les systèmes NICE ont été cassés empiriquement par Castagnos et Laguillaumie pendant qu'Aurore élaborait sa thèse. En collaboration avec Nicolas Gama, Aurore a pu déterminer le coût de cette attaque et préciser les conditions de sa réussite, grâce à l'étude précédente.

Chapitre 3

Ce chapitre est issu d'un travail [15] en collaboration avec Stéphane Vinatier et Erik J. Pickett. Stéphane m'avait présenté la construction d'Erik [78], permettant d'obtenir des bases normales autoduales d'extensions de corps en caractéristique quelconque. La question se posait alors de savoir si sa méthode pouvait être implantée dans un algorithme, et de déterminer son efficacité, dans le cas des corps finis. Rappelons que les bases normales autoduales permettent d'obtenir une arithmétique efficace des corps finis, en particulier celles dites de complexité minimale.

Chapitre 4

Ce chapitre expose une série de travaux effectués en commun avec Thierry Berger, Cédric Lauradoux, Marine Minier, Abdelkader Necer, Benjamin Pousse.

Les automates FCSR (pour *Feedback with Carry Shift Registers*) ont été introduits par Klapper & Goresky dans [63]. Ils sont similaires aux classiques LFSR (*Linear Feedback Shift Registers*) qui sont omniprésents dans la conception de générateurs pseudo-aléatoires. La différence essentielle entre les deux types d'automates est que l'addition bit-à-bit employée par les LFSR est une addition modulo 2, alors que celle employée par les FCSR est à propagation de retenues, d'où une fonction de transition non linéaire.

Le chapitre 4 expose divers résultats que nous avons obtenus dans ce domaine. Il commence par présenter une nouvelle méthode de reconstruction d'un automate FCSR à partir de la suite générée, basée sur l'algorithme d'Euclide étendu. Ensuite, le chapitre expose une généralisation utile et éclairante des FCSR, qui étaient auparavant implémentés sous deux formes dégénérées : le mode Fibonacci et le mode Galois. Puis la généralisation est poussée encore plus loin avec les machines 2-adiques. Finalement, on présente un membre F-FCSR-H de la famille FFCSR d'algorithmes de chiffrement à flot que nous avons conçus. Cet algorithme a été retenu dans le projet européen eSTREAM.

Chapitre 5

Mon domaine de recherche le plus récent porte sur la théorie de l'information quantique. Ce domaine se propose d'utiliser les mathématiques discrètes pour sonder et exploiter les étrangetés du monde quantique. Outre l'intérêt fondamental de cette démarche, cela a déjà des applications en cryptographie et pourrait à terme révolutionner nos outils de calcul.

Mon premier travail, en théorie de l'information quantique a été de construire un jeu complet d'inégalités de Bell en dimension quelconque. Cela généralise un résultat important, obtenu en dimension 2 par Werner et Wolf. Les inégalités de Bell permettent de caractériser le caractère réaliste local d'une théorie physique. Leur rôle initial a été de montrer que la mécanique quantique échappe à ce cadre. En effet, certains systèmes quantiques violent ces inégalités. On espère grâce aux nouvelles inégalités, caractériser et mesurer plus finement les propriétés quantiques. Passer de la dimension 2 à une dimension supérieure est important et permet en pratique d'améliorer certaines applications cryptographiques.

Suite à mon travail sur les inégalités de Bell multidimensionnelles [4] et mon investissement personnel dans le domaine de l'information quantique, j'ai proposé un sujet de thèse pour poursuivre ma recherche. Notre travail progresse, avec la description d'une nouvelle variante de protocole d'échange de clés. Tout cela fait l'objet du chapitre 5.

Chapitre 1

Systèmes de chiffrement probabilistes

Ce premier chapitre présente le travail effectué avec mon étudiant Guilhem Castagnos [23][24], dont j'ai encadré la thèse.

Dans sa thèse Guilhem a étudié avec soin le système de chiffrement de Paillier et ses nombreuses variantes (certaines d'entre elles utilisant des courbes elliptiques) et a fait une étude comparative détaillée intégrant leurs coûts qu'il a calculés avec précision. Il a ensuite étudié LUC, un système de chiffrement utilisant des corps quadratiques ou des suites de Lucas, le présentant sous une forme plus claire et mettant mieux en valeur sa sécurité par rapport à celle de RSA. Il a aussi proposé plusieurs systèmes de chiffrement de type Paillier utilisant des corps quadratiques, dont l'un d'entre eux à fait l'objet de la publication [24]. Ce travail est présenté dans la section 1.1 ci-dessous.

Guilhem a aussi développé un cadre général permettant de décrire simultanément les différentes variantes du système de Paillier, et plus généralement de nombreux systèmes probabilistes, et de les classifier. Ce cadre permet en particulier de mieux comparer la sécurité et l'efficacité de ces différentes variantes. Il permet aussi de concevoir en retour d'autres variantes utilisant d'autres groupes cryptographiques. On obtient ainsi d'autres systèmes de chiffrement d'intérêt pratique. L'une des propriétés de l'un de ces systèmes est d'être homomorphe, ce qui est intéressant pour certaines applications en sécurité de l'information (vote électronique, anonymat), d'autant plus que les systèmes homomorphes utilisables en pratique sont rares.

1.1. Schémas probabilistes à clés publiques

Le système de Paillier

Soient p, q deux nombres premiers distincts vérifiant la propriété

$$\mathrm{pgcd}\left(pq, (p-1)(q-1)\right) = 1 \tag{1.1}$$

et posons $N = pq$. Le système de Paillier fait intervenir le groupe $G = (\mathbb{Z}/N^2\mathbb{Z})^*$. Ce groupe est d'ordre $\varphi(N^2) = N\varphi(N) = pq(p-1)(q-1)$. De plus, on a l'isomorphisme chinois

$$f : G \longrightarrow G_p \times G_q \qquad \text{avec} \quad G_p = (\mathbb{Z}/p^2\mathbb{Z})^* \quad \text{et} \quad G_q = (\mathbb{Z}/q^2\mathbb{Z})^*. \tag{1.2}$$

L'hypothèse (1.1) fait qu'un élément de G_p est une puissance N-ième si et seulement s'il est une puissance p-ième, ainsi que la propriété symétrique pour G_q. Il en résulte que l'ensemble G^N des puissances N-ièmes dans G est en bijection par f avec le produit direct des puissances p-ièmes de G_p et des puissances q-ièmes de G_q. En particulier, l'ordre de G^N est $\varphi(N)$, et G^N est caractérisé par

$$G^N = \{x \in G \mid x^\lambda = 1\} \qquad \text{avec } \lambda = \lambda(N) = \mathrm{ppcm}(p-1, q-1).$$

La fonction à sens unique

Dans la décomposition (1.2), les deux facteurs contiennent respectivement des éléments d'ordre p et q. Donc G contient un élément g d'ordre N. Comme N et λ sont premiers entre eux, g^λ est aussi d'ordre N dans G. Pour $k \in \mathbb{Z}$ on a donc

$$g^k \in G^N \Rightarrow g^{\lambda k} = 1 \Rightarrow N \mid k.$$

Donc l'ordre de g modulo G^N est N. Comme G/G^N est d'ordre $N\varphi(N)/\varphi(N) = N$, il en résulte que g est un générateur de G/G^N.

Le système de chiffrement de Paillier utilise la fonction suivante :

$$\mathcal{E} : \begin{cases} \mathbb{Z}/N\mathbb{Z} \times (\mathbb{Z}/N\mathbb{Z})^* \longrightarrow (\mathbb{Z}/N^2\mathbb{Z})^* \\ (m, r) \longmapsto g^m r^N \end{cases}$$

qui est bien définie parce que $g^N = 1$.

Soit U le sous-groupe de G défini par

$$U = \{u \in G \mid u \equiv 1 \bmod N\}$$

et considérons l'application

$$L : \begin{cases} U \longrightarrow \mathbb{Z}/N\mathbb{Z} \\ u \longmapsto \dfrac{u-1}{N}. \end{cases}$$

On voit facilement que $L(u^r) = rL(u)$ pour $u \in U$, $r \in \mathbb{Z}$. De plus, pour $x \in G$, on a $x^\lambda \in U$ (par le petit théorème de Fermat). Considérons en particulier l'élément $\ell = L(g^\lambda) \in \mathbb{Z}/N\mathbb{Z}$. On a $g^\lambda = 1 + N\ell$ dans G. Puisque g^λ est d'ordre N, on voit que

$$1 \neq g^{k\lambda} = 1 + kN\ell \quad \text{dans } G \qquad \text{pour } 0 < k < N.$$

Il en résulte que ℓ est relativement premier à N. On peut donc définir

$$\ell_g : \begin{cases} G \longrightarrow \mathbb{Z}/N\mathbb{Z} \\ z \longmapsto L(z^\lambda)\big(L(g^\lambda)\big)^{-1}. \end{cases}$$

Soient $m \in \mathbb{Z}_N$ et $r \in \mathbb{Z}_N^*$ et posons $c = \mathcal{E}(m, r)$. On a $L(c^\lambda) = (g^{\lambda m} r^{\lambda N} - 1)/N$. Mais comme $r^{\lambda N} \equiv 1$ modulo N^2 on obtient

$$L(c^\lambda) = \frac{g^{\lambda m} - 1}{N} = L(g^{\lambda m}) = mL(g^\lambda).$$

On a donc $\ell_g(c) = m$.

D'autre part, considérons l'homomorphisme de groupes

$$s : \begin{cases} \mathbb{Z}_N^* \longrightarrow G \\ r \longmapsto r^N. \end{cases}$$

Si r appartient au noyau de s alors $r^N \equiv 1$ modulo p^2. On a même $r^p \equiv 1$ modulo p^2 puisque q et $\varphi(p^2)$ sont premiers entre eux. Comme $(\mathbb{Z}/p^2\mathbb{Z})^*$ est cyclique d'ordre $p(p-1)$, l'équation $r^p \equiv 1$ modulo p^2 admet exactement p solutions modulo p^2 (à savoir $1, 1+p, \ldots, 1+(p-1)p$), c'est-à-dire une seule modulo p. Le même raisonnement modulo q^2 et le théorème chinois amènent à la conclusion que l'homomorphisme s est injectif. Remarquons aussi que son image est G^N, et par s^{-1} nous désignerons sa réciproque sur G^N.

De l'injectivité de s, il résulte que l'application $\mathcal{E}$ est bijective et que sa réciproque est $\mathcal{D} = \ell_g \times s^{-1}$. Enfin, il est clair que $\mathcal{E}$ respecte les lois de groupes, c'est donc un isomorphisme.

Sécurité

La fonction $\mathcal{E}$ permet donc de chiffrer des messages appartenant à $\mathbb{Z}/N\mathbb{Z}$ (ou de façon équivalente appartenant à $\mathbb{Z}_N = \{0, 1, \ldots, N-1\}$). La fonction ℓ_g permet de déchiffrer, tout au moins pour quelqu'un qui connaît la valeur de λ et donc la factorisation de N.

La sécurité de ce système correspond à la difficulté de calculer ℓ_g, qui représente la classe du chiffré modulo G^N. Autrement dit, elle repose sur le problème suivant :

1.1.1. — Définition. Soient N un entier RSA et g un entier d'ordre N modulo N^2. Le problème de la *Résidualité Composite* (RC) est celui, étant donné $c \in \mathbb{Z}_{N^2}^*$, de déterminer $\ell_g(c)$.

La sécurité sémantique repose quand à elle sur le problème décisionnel correspondant :

1.1.2. — Définition. Soient N un entier RSA et g un entier d'ordre N modulo N^2. Le problème *Décisionnel de la Résidualité Composite* (DRC) est celui, étant donnés $c, c' \in \mathbb{Z}_{N^2}^*$ de déterminer si $\ell_g(c) = \ell_g(c')$. Autrement dit, déterminer si c et c' appartiennent à la même classe modulo $(\mathbb{Z}_N^*)^N$.

Le système de Paillier simplifié

On peut prendre $g = 1 + N \in G$, car c'est un élément d'ordre N. Cela accélère le chiffrement parce que $g^m = 1 + mN$. Il est ensuite possible de remplacer l'exposant N par un e petit (comme dans RSA) dans la fonction de chiffrement :

$$\mathcal{E} : \begin{cases} \mathbb{Z}/N\mathbb{Z} \times (\mathbb{Z}/N\mathbb{Z})^* \longrightarrow (\mathbb{Z}/N^2\mathbb{Z})^* \\ (m, r) \longmapsto (1 + mN)r^e \end{cases}$$

En effet, puisque $g \equiv 1$ modulo N, le destinataire peut retrouver r à partir de $c = \mathcal{E}(m)$ par

$$r = c^d \bmod N$$

s'il connaît l'inverse d de e modulo λ. Il ne lui reste plus qu'à calculer

$$m = L(cr^D)$$

où D est l'inverse de e modulo $\lambda(N^2) = N\lambda$. Ce schéma a été étudié dans [27].

Le schéma de Castagnos

Le schéma qui vient d'être présenté peut être adapté à d'autres groupes arithmétiques. Cela a été fait pour les courbes elliptiques dans [44]. Le système obtenu présente cependant des coûts de chiffrement/déchiffrement très élevés. Castagnos, suivant une piste que je lui suggérais en tant que directeur de thèse, a étudié l'adaptation de ce schéma aux corps quadratiques. Le schéma obtenu, décrit dans [24], est bien plus intéressant en termes de coût, entre autres par une utilisation appropriée de termes d'une suite de Lucas — dont le calcul est équivalent à une exponentiation modulaire dans un corps quadratique. Voici une brève description du schéma de Castagnos.

On désigne encore par $N = pq$ un entier RSA. Soit e un entier tel que $\operatorname{pgcd}\big(e, (p^2-1)(q^2-1)\big) = 1$. On définit les deux ensembles suivants

$$\Lambda_N := \{x \in \mathbb{Z}_N^* \mid \operatorname{pgcd}(x^2 - 4, N) = 1\},$$
$$\Omega_N := \{x \in \mathbb{Z}_{N^2}^* \mid \operatorname{pgcd}(x^2 - 4, N) = 1\}.$$

La fonction de chiffrement est donnée par

$$\mathcal{E} : \begin{cases} \mathbb{Z}_N \times \Lambda_N \longrightarrow \Omega_N \\ (m, r) \longmapsto (1 + N)^m V_e(r, 1) \pmod{N}^2 \end{cases}$$

où $V_e(r, 1)$ est le terme d'indice e de la suite récurrente définie par

$$V_0 = 2, \quad V_1 = r, \qquad V_{i+1} = rV_i - V_{i-1} \qquad \text{(deuxième suite de Lucas de paramètres } r \text{ et } 1).$$

Pour déchiffrer c, on peut utiliser la méthode suivante. Le destinataire a précalculé les inverses de e modulo $p \pm 1$ et $q \pm 1$, ainsi que celui de p modulo q. On pose

$$r_p := V_{e^{-1} \bmod (p-\epsilon)}(c, 1) \bmod p \qquad \text{et} \qquad r_q := V_{e^{-1} \bmod (q-\eta)}(c, 1) \bmod q.$$

où ϵ et η sont les symboles de Legendre $\epsilon = (c^2 - 4/p)$ et $\eta := (c^2 - 4/q)$. Puis

$$r := r_p + p(r_q - r_p)(p^{-1} \bmod q) \bmod N.$$

Ensuite

$$s_p := c(V_e(r, 1))^{-1} \bmod p^2, \qquad t_p := (s_p - 1)/p, \qquad m_p := t_p q^{-1} \bmod p.$$

et un calcul similaire pour m_q. Enfin, on obtient le message clair m par

$$m := m_p + p(m_q - m_p)(p^{-1} \bmod q) \bmod N.$$

Castagnos a de plus montré que la sécurité sémantique de ce schéma repose sur le problème de décision suivant, où $N = pq$ est un entier RSA et e un entier tel que $\operatorname{pgcd}\big(e, (p^2-1)(q^2-1)\big) = 1$: Pour $c \in \Omega_N$, décider s'il existe $r \in \Lambda_N$ tel que $V_e(r, 1) \equiv c$ modulo N^2.

Chapitre 2

Formes quadratiques

Ce chapitre est issu du travail avec mon étudiante Aurore Bernard. Les sections 2.1 et 2.3 rappellent des faits classiques sur les formes quadratiques binaires. La section 2.2 précise les liens entre les formes quadratiques de discriminant D et celles de discriminant Df^2 [3]. Cela est utile pour l'analyse des systèmes de chiffrement NICE, pour lesquels la clé publique est une forme de discriminant Df^2, et la clé secrète le discriminant D. La section 2.5 présente une nouvelle méthode de réduction des formes quadratiques réelles permettant de minimiser la taille de la matrice de passage [19][20], elle aussi utilisée pour l'attaque de NICE. Enfin, la section 2.6 présente les systèmes de la famille NICE, ainsi que l'attaque étudiée par Aurore Bernard.

2.1. Introduction

Les formes quadratiques binaires ont été initialement considérées par Fermat, Lagrange, Legendre. Puis Gauss, dans les *Disquisitiones Arithmeticae* publiées en 1801, est le premier à leur donner un développement significatif, avec en particulier la loi de composition.

Leurs applications pratiques sont multiples. Elles fournissent une manière explicite de manipuler des idéaux de corps quadratiques (une alternative, pour certaines applications, est fournie par les suites de Lucas). De nombreux algorithmes de factorisation les utilisent : [66], [81], [82], [83] (SQUFOF entre autres). Elles sont aussi utilisées en cryptographie, en particulier pour les systèmes NICE [77] puis [54]. De bonnes références pour les formes quadratiques sont [21], [22], [31], [32], [35], [55] et (avec application à la factorisation) [81].

Formes

Une *forme quadratique binaire* est un polynôme homogène à deux variables

$$q(x, y) = ax^2 + bxy + cy^2.$$

Le cas qui nous intéresse, par la richesse de son arithmétique, est celui où les coefficients a, b, c sont entiers. Nous utiliserons souvent le terme abrégé de *forme* pour forme quadratique binaire à coefficients entiers. On suppose de plus que le *discriminant* $\mathrm{disc}(q) = D := b^2 - 4ac$ n'est pas un carré parfait (puisque les propriétés des formes quadratiques de discriminant D sont liées au corps sous-jacent $\mathbb{Q}(\sqrt{D})$). Si $D > 0$, on parle de forme quadratique *réelle*. Si $D < 0$, on parle de forme quadratique *imaginaire*, et on ne s'intéresse dans ce cas qu'aux formes définies positives (i.e. telles que $a > 0$). Nous noterons souvent une forme quadratique en listant ses coefficients $q = (a, b, c)$. Une forme quadratique est dite *primitive* si $\mathrm{pgcd}(a, b, c) = 1$.

Discriminants

2.1.1. — Définitions. J'appelle *discriminant* un entier non carré parfait et congru à 0 ou 1 modulo 4. On appelle *discriminant fondamental* un entier non carré parfait vérifiant

$$\begin{cases} D \equiv 1 \text{ modulo } 4 \\ D \text{ sans facteur carré} \end{cases} \quad \text{ou} \quad \begin{cases} D \equiv 0 \text{ modulo } 4 \\ D/4 \equiv 2 \text{ ou } 3 \text{ modulo } 4 \text{ et sans facteur carré} \end{cases}$$

On montre facilement qu'un discriminant D est fondamental si et seulement si il n'existe pas de discriminant de la forme D/f^2 avec $f > 1$ entier. On montre aussi que D est fondamental si et seulement si toutes les formes quadratiques de discriminant D sont primitives.

Il y a des liens subtils entre les formes de discriminant D et celles de discriminant Df^2 (que j'appelle discriminants *emboîtés*). Ces liens étaient exploités dans les systèmes de chiffrement NICE. Nous reviendrons en détail sur ces liens, ainsi que sur les applications à la cryptanalyse de NICE.

Action, équivalence

Soit q une forme et $M = \left(\begin{smallmatrix} p & r \\ s & t \end{smallmatrix}\right)$ une matrice à coefficients entiers. On note $q \cdot M$ le trinôme q' donné par

$$q'(x,y) = q(px+ry, sx+ty) = q(p,s)x^2 + \big(q(p+r,s+t) - q(p,s) - q(r,t)\big)xy + q(r,t)y^2. \tag{2.1}$$

On obtient ainsi une action à droite sur les formes.

2.1.2. — Proposition. *Si $q' = q \cdot M$ alors* $\operatorname{disc} q' = (\det M)^2 \operatorname{disc} q$.

Lorsque la matrice M est de déterminant 1, c'est-à-dire $M \in \mathrm{SL}_2(\mathbb{Z})$, on dit que q et q' sont (proprement) équivalentes (et on note $q \sim q'$). Deux formes quadratiques équivalentes ont donc même discriminant. D'autre part, si l'une est primitive, l'autre aussi. On montre que l'ensemble $H(D)$ des classes de formes quadratiques primitives de discriminant D est fini et peut-être muni d'une structure de groupe, par la loi de composition de Gauss.

Les matrices $S = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ et $T = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ engendrent le groupe $\mathrm{SL}_2(\mathbb{Z})$. Leur action (et plus généralement, l'action de $T^k = \left(\begin{smallmatrix} 1 & k \\ 0 & 1 \end{smallmatrix}\right)$ avec $k \in \mathbb{Z}$) sur les formes quadratiques est donnée par

$$\begin{aligned}(a,b,c) \cdot S &= (c,-b,a),\\ (a,b,c) \cdot T^k &= (a, b+2ka, c+kb+k^2a).\end{aligned}$$

La *réduction* d'une forme quadratique consiste à appliquer certaines de ces transformations élémentaires afin de parvenir à une forme équivalente « plus simple ».

Réduction des formes imaginaires

La notion de réduction, pour les formes imaginaires, est beaucoup plus simple que pour les formes réelles (le cas de ces dernières fera l'objet d'une étude détaillée dans la section 2.3)

2.1.3. — Définition. Une forme quadratique imaginaire (non nécessairement primitive) $ax^2+bxy+cy^2$ de discriminant D est dite *réduite* si

$$|b| \leqslant a \leqslant c \qquad \text{et en plus } b \geqslant 0 \text{ si l'une des inégalités n'est pas stricte.}$$

Il est facile de voir que toute forme imaginaire réduite de discriminant D vérifie l'inégalité

$$3ac \leqslant |D|, \qquad \text{et même} \qquad a \leqslant \sqrt{|D|/3}. \tag{2.2}$$

Cette majoration a pour première conséquence :

2.1.4. — Théorème. *Soit D un discriminant négatif. Il existe un nombre fini de formes quadratiques réduites de discriminant D.*

L'algorithme suivant utilise des transformations élémentaires pour *réduire* une forme quadratique imaginaire.

2.1.5. — Algorithme. Réduction d'une forme quadratique imaginaire.

Entrée : Une forme quadratique imaginaire $q = (a,b,c)$ de discriminant D.
Sortie : Une forme quadratique réduite équivalente à q.

Répéter
  Appliquer une transformation T^k avec k choisi de telle sorte que $-a < b \leqslant a$
  Si la forme obtenue est réduite alors la retourner et arrêter l'algorithme. FinSi
  Appliquer la transformation S
Fin répéter

On montre que cet algorithme se termine, par l'obtention d'une forme réduite équivalente à q. De plus cette forme réduite équivalente à q est unique :

2.1.6. — Proposition. *Toute forme quadratique imaginaire est équivalente à une unique forme quadratique réduite.*

Enfin, nous utiliserons aussi la notion de forme normale :

2.1.7. — Définition. Une forme quadratique imaginaire $q = (a, b, c)$ est dite *normale* lorsque $-a < b \leqslant a$.

N'importe quelle forme peut-être *normalisée* par l'action d'une matrice T^k. D'autre part, la propriété liée à l'inégalité (2.2) admet une réciproque partielle :

2.1.8. — Proposition. *Toute forme normale telle que $a < \sqrt{|D|/4}$ est réduite.*

2.2. Discriminants emboîtés

Les résultats mis en relief ici sont éparpillés dans [22], [21], [35], mais la notion de formes semi-équivalentes n'y est pas présente explicitement. J'introduis cette notion dans [3], où je rassemble aussi tous les résultats présentés ici, et leurs démonstrations. Nous considérons deux discriminants, D et Df^2 (avec $f \in \mathbb{N}^*$).

Matrices de remontée

Pour g entier tel que $0 \leqslant g < f$, on pose $R_g = \left(\begin{smallmatrix} f & g \\ 0 & 1 \end{smallmatrix}\right)$. On posera aussi $R_f = \left(\begin{smallmatrix} 1 & 0 \\ 0 & f \end{smallmatrix}\right)$. Lorsque $f > 1$, les $f + 1$ matrices R_g sont de déterminant f et sont deux-à-deux non équivalentes sous l'action de $\mathrm{SL}_2(\mathbb{Z})$. De plus, lorsque f est premier, toute matrice $\left(\begin{smallmatrix} p & r \\ s & t \end{smallmatrix}\right)$ à coefficients entiers et de déterminant f se décompose sous la forme $\left(\begin{smallmatrix} p & r \\ s & t \end{smallmatrix}\right) = R_g U$ avec $0 \leqslant g \leqslant f$ et $U \in \mathrm{SL}_2(\mathbb{Z})$, l'entier g étant unique.

La remontée principale

Soient $f \in \mathbb{N}^*$ et $q = ax^2 + bxy + cy^2$ une forme quadratique de discriminant D et telle que $\mathrm{pgcd}(a, f) = 1$. On obtient une forme quadratique de discriminant Df^2 en posant $Q = q \cdot R_f$ (on a donc $Q(x, y) = q(x, fy)$). Il est facile de montrer que, si q est primitive, alors Q l'est aussi. Il est intéressant de savoir que, réciproquement, toute forme primitive de discriminant Df^2 peut être obtenue à équivalence près par cette construction, lorsque f est impair :

2.2.1. — Proposition. *On suppose f impair. Soit Q une forme primitive de discriminant Df^2. Il existe une forme primitive q de discriminant D telle que $Q = q \cdot R_f U$ où $U \in \mathrm{SL}_2(\mathbb{Z})$.*

Formes semi-équivalentes

Ce sont deux formes de discriminant Df^2 qui proviennent de formes équivalentes de discriminant D. De façon précise :

2.2.2. — Définition. Soient Q_1 et Q_2 deux formes primitives de discriminant Df^2. Je dis que Q_1 et Q_2 sont *semi-equivalentes* (ou fondamentalement équivalentes) si il existe deux formes primitives équivalentes q_1 et q_2 de discriminant D, deux entiers g_1 et g_2 avec $0 \leqslant g_1, g_2 \leqslant f$, ainsi que deux $\mathrm{SL}_2(\mathbb{Z})$-matrices U_1, U_2, tels que $Q_i = q_i \cdot R_{g_i} U_i$.

Il est clair que la semi-équivalence est une relation d'équivalence. Aussi que deux formes équivalentes sont semi-équivalentes. On peut en fait contraindre, dans deux directions différentes, la condition apparaissant dans la définition de formes semi-équivalentes. Les cas apparemment particuliers obtenus restent en fait équivalents au cas général (quand f est premier) :

2.2.3. — Théorème ([3]). *On suppose f premier. Soient Q_1 et Q_2 deux formes primitives de discriminant Df^2. Alors chacune des deux conditions suivantes est satisfaite si et seulement si Q_1 et Q_2 sont semi-équivalentes.*

(a) Il existe une forme primitive q de discriminant D, deux entiers g_1 et g_2 avec $0 \leqslant g_1, g_2 \leqslant f$, et deux $\mathrm{SL}_2(\mathbb{Z})$-matrices U_1, U_2 tels que $Q_i = q \cdot R_{g_i} U_i$ (pour $i = 1, 2$).

(b) Il existe deux formes primitives équivalentes q_1 et q_2 de discriminant D et deux $\mathrm{SL}_2(\mathbb{Z})$-matrices V_1, V_2 telles que $Q_i = q_i \cdot R_f V_i$ (pour $i = 1, 2$).

La descente

2.2.4. — Proposition. *On suppose f premier. Soient Q_1 et Q_2 des formes primitives de discriminant Df^2 semi-équivalentes. Soient q_1, q_2 deux formes primitives de discriminant D et M_1, M_2 deux matrices entières de déterminant f telles que $Q_i = q_i \cdot M_i$ (pour $i = 1, 2$). (Les formes q_i et les matrices M_i existent d'après la proposition 2.2.1.) Alors $q_1 \sim q_2$.*

On suppose f premier impair. Pour Q forme quadratique primitive de discriminant Df^2, la proposition 2.2.1 précise qu'il existe une forme quadratique q de discriminant D telle que $q \cdot R_f \sim Q$. La correspondance $Q \mapsto q$ ainsi obtenue définit une application surjective $\pi : H(Df^2) \to H(D)$. L'application π est même un morphisme du groupe de classes $H(Df^2)$ sur le groupe de classes $H(D)$. Cela est utilisé dans les systèmes de chiffrement NICE.

Les autres remontées

Le nombre de formes primitives de discriminant Df^2 que l'on peut obtenir en utilisant les matrices R_g déterminé par le résultat suivant.

2.2.5. — Proposition ([22], Prop. 7.3). *On suppose que f est un nombre premier, que $q = ax^2+bxy+cy^2$ est primitive et que $\gcd(a, f) = 1$. Alors $Q_g = q \cdot R_g$ est primitive pour exactement $f - (D/f)$ valeurs de g (où (D/f) est un symbole de Kronecker).*

Le nombre de classes d'équivalence ainsi construites est donné par la proposition suivante lorsque le discriminant est négatif. (Il sera discuté plus loin dans le cas réel).

2.2.6. — Proposition. *Soient q une forme de discriminant D négatif et f un nombre premier impair. Notons $Q_g = q \cdot R_g$ pour $0 \leqslant g \leqslant f$ et $q(g, 1) \not\equiv 0$ modulo f. Les $f - (D/f)$ formes primitives Q_g obtenues sont deux à deux non-équivalentes, sauf pour les discriminants exceptionnels $D = -3$ et $D = -4$ pour lesquels respectivement exactement 2 et 3 valeurs distinctes de g donnent la même classe d'équivalence.*

Enfin, toutes les classes de formes primitives sont obtenues de cette façon :

2.2.7. — Proposition. *On suppose que f est un nombre premier impair. Soit Q une forme quadratique primitive de discriminant Df^2 et $q \in \pi(Q)$. Alors Q est équivalente à l'une des $q \cdot R_g$ pour un g tel que $f \nmid q(g, 1)$.*

Exemples

Commençons par un exemple à discriminants négatifs, avec $D = -71$ et $f = 5$. On a $(D/f) = 1$ donc chaque forme réduite primitive de discriminant D peut-être remontée en 4 formes réduites primitives de discriminant Df^2. Ces 4 formes sont donc semi-équivalentes.

(1,1,18)	(1, 1, 444),	(18,5,25),	(18,-5,25),	(24,23,24)
(2,1,9)	(2, 1, 222),	(9,-5,50),	(12,-1,37),	(19,-7,24)
(2,-1,9)	(2, -1, 222),	(9,5,50),	(12,1,37),	(19,7,24)
(3,1,6)	(3,-1,148),	(6,-5,75),	(8,-7,57),	(16,-9,29)
(3,-1,6)	(3,1,148),	(6,5,75),	(8,7,57),	(16,9,29)
(4,3,5)	(4,-1,111),	(6,1,74),	(12,-7,38),	(18,-13,27)
(4,-3,5)	(4,1,111),	(6,-1,74),	(12,7,38),	(18,13,27)

Table 2.1. Formes primitives réduites de discriminants -71 et -1775

La table 2.2 donne ensuite un exemple à discriminants positifs, avec $D = 229$ et $f = 5$. Il y a ici 14 formes réduites de discriminant D, réparties en 3 cycles (à gauche dans la table). Il y a 26 formes réduites de discriminant Df^2, réparties en 6 cycles (en lignes, à droite). Ces cycles se regroupent deux par deux en 3 classes de semi-équivalence, correspondant aux 3 classes d'équivalence de discriminant D.

(1,15,-1), (-1,15,1)	(1,75,-25), (-25,75,1) (25,45,-37), (-37,29,33), (33,37,-33), (-33,29,37), (37,45,-25), (-25,55,27), (27,53,-27), (-27,55,25)
(3,13,-5), (-5,7,9), (9,11,-3), (-3,13,5), (5,7,-9), (-9,11,3)	(-9,73,11), (11,59,-51), (-51,43,19), (19,71,-9) (3,71,-57), (-57,43,17), (17,59,-33), (-33,73,3)
(9,7,-5) (-5,13,3) (3,11,-9), (-9,7,5), (5,13,-3), (-3,11,9)	(-3,73,33), (33,59,-17), (-17,43,57), (57,71,-3) (9,71,-19), (-19,43,51), (51,59,-11), (-11,73,9)

Table 2.2. Formes primitives réduites de discriminants 229 et 5725

2.3. Réduction des formes réelles

La réduction des formes réelles est précisément détaillée dans [21]. La situation est bien plus complexe que pour les formes imaginaires. En particulier, aucune notion raisonnable de réduction ne peut produire une seule forme réduite par classe d'équivalence. Mais il existe une notion de réduction, pour laquelle les formes réduites appartenant à une même classe sont organisées en cycle, dont le parcours permet le calcul du régulateur de l'ordre quadratique de même discriminant.

Formes réduites

2.3.1. — Définition. Une forme réelle (a,b,c) de discriminant D est dite *réduite* si

$$\big|\sqrt{D}-2|a|\big| < b < \sqrt{D}. \tag{2.3}$$

De façon équivalente, une forme est réduite si et seulement si

$$0 < b < \sqrt{D} \quad \text{et} \quad \sqrt{D}-b < 2|a| < \sqrt{D}+b. \tag{2.4}$$

Pour tout discriminant D positif, la forme *principale* $\big(1, b, (b^2-D)/4\big)$ de discriminant D, où b l'unique entier de même parité que D tel que $b < \sqrt{D} < b+2$, est une forme réduite. De façon similaire au cas imaginaire, on a des bornes simples qui permettent de voir que le nombre de forme réduites de discriminant D est fini :

2.3.2. — Proposition. *Soit (a,b,c) une forme quadratique réelle réduite, de discriminant D. Alors $ac<0$ et $|a|+|c|<\sqrt{D}$.*

Démonstration — On a $4ac = b^2 - D < 0$ d'après (2.3). Ensuite

$$4|a|(|a|+|c|-\sqrt{D}) = 4|a|^2 + 4|a||c| - 4|a|\sqrt{D} = 4|a|^2 + D - b^2 - 4|a|\sqrt{D} = (2|a|-\sqrt{D})^2 - b^2$$

qui est négatif, toujours d'après (2.3). Donc $|a|+|c|<\sqrt{D}$. □

2.3.3. — Corollaire. *Le nombre de formes réelles réduites de discriminant fixé est fini.*

La notion de réduction est liée aux racines des polynômes associés aux formes. Nous noterons

$$\theta_q^- = \frac{-b-\sqrt{D}}{2a} \qquad \text{et} \qquad \theta_q^+ = \frac{-b+\sqrt{D}}{2a} \tag{2.5}$$

les racines de $q(x,1)$ (on a $a \neq 0$ puisque D n'est pas un carré parfait).

2.3.4. — Proposition. *On note θ^+ et θ^- les racines de $q(x,1)$ définies par (2.5) . Alors q est réduite si et seulement si*

$$|\theta^+| < 1, \qquad |\theta^-| > 1, \qquad \theta^+\theta^- < 0. \tag{2.6}$$

Démonstration — On remarque que $\theta_1\theta_2 = c/a$. Donc la condition $\theta_1\theta_2 < 0$ est équivalente à $ac < 0$, soit $|b| < \sqrt{D}$. On voit alors facilement que (2.4) implique (2.6). Réciproquement, si (2.6) est vérifiée alors la condition $ac < 0$ fournit $|b| < \sqrt{D}$ ainsi que $|\theta_1| = (\sqrt{D}-b)/2|a|$ et $|\theta_2| = (\sqrt{D}+b)/2|a|$. On a donc $\sqrt{D}-b < 2|a|$ et $\sqrt{D}+b > 2|a|$. On obtient alors (2.3). □

2.3.5. — Corollaire. *Soit $q = (a,b,c)$ une forme réelle et $q' = (c,b,a)$. Alors q' est réduite si et seulement si q l'est. En particulier, q est réduite si et seulement si*

$$\big|\sqrt{D} - 2|c|\big| < b < \sqrt{D}. \tag{2.7}$$

Démonstration — On désigne par θ_1 et θ_2 les racines de $f(x,1)$ et de la même façon $\theta_1' = (-b+\sqrt{D})/2c$ et $\theta_2' = (-b-\sqrt{D})/2c$ celles de $f'(x,1)$. On a alors $\theta_1\theta_2' = \theta_1'\theta_2 = 1$. On voit donc que (2.6) est équivalent à $|\theta_1'| < 1$, $|\theta_2'| > 1$ et $\theta_1'\theta_2' < 0$. □

Opérateur de réduction

L'opérateur de réduction est le pas qui est répété lorsqu'on réduit une forme, mais aussi quand on parcourt le cycle de formes réduites. Les formules décrites ici permettent d'implémenter l'algorithme de réduction, mais aussi d'étudier sa complexité.

Pour $a \neq 0$ et b entiers, on désigne par $r_D(b,a)$ l'unique entier r qui vérifie la congruence $r \equiv b$ modulo $2a$ et l'inégalité $-|a| < r < |a|$ lorsque $\sqrt{D}-|a| \leqslant 0$, ou $\sqrt{D}-2|a| < r < \sqrt{D}$ lorsque $\sqrt{D}-|a| > 0$. Autrement dit

$$r = b + 2as \qquad \text{avec} \quad s = s_D(b,a) = \begin{cases} (\operatorname{sgn} a)\left\lfloor \dfrac{-b+|a|}{2|a|} \right\rfloor & \text{si } \sqrt{D} \leqslant |a| \\ (\operatorname{sgn} a)\left\lfloor \dfrac{-b+\sqrt{D}}{2|a|} \right\rfloor & \text{si } \sqrt{D} \geqslant |a| \end{cases} \tag{2.8}$$

On définit l'opérateur ρ de réduction sur les formes réelles de la manière suivante (défini lorsque $c \neq 0$) :

$$\rho(a,b,c) = \big(c, b', (b'^2 - D)/4c\big) \qquad \text{où } b' = r_D(-b,c) = -b + 2cs_D(-b,c).$$

La forme $\rho(a,b,c)$ obtenue est équivalente à (a,b,c). Plus précisément, on a $\rho(a,b,c) = (a,b,c)U$ avec

$$R_s = ST^s = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & s \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & s \end{pmatrix} \qquad \text{avec } s = s_D(-b,c). \tag{2.9}$$

D'autre part, si (a,b,c) est une forme réelle réduite alors $\rho(a,b,c)$ l'est aussi.

2.3.6. — Algorithme. Réduction d'une forme quadratique réelle.

Entrée : Une forme quadratique réelle $q(x,y) = ax^2 + bxy + cy^2$ de discriminant D.
Sortie : Une forme quadratique réduite équivalente à q, et $U \in \mathrm{SL}_2(\mathbb{Z})$ telle que $q' = q \cdot U$.

$U := I$
TantQue q n'est pas réduite Faire
  $q := \rho(q)$
  $U := UR_s$ où R_s est définie par (2.9)
Fin TantQue
Retourner q et U.

On a les relations suivantes, entre les racines d'une forme quadratique q et celles de $\rho(q)$:

$$\theta^+_{\rho(q)} = -s - \theta^+_q \qquad \text{et} \qquad \theta^-_{\rho(q)} = -s - \theta^-_q.$$

2.3.7. — **Théorème.** *Soit $D > 0$ non carré parfait.* • *L'opérateur ρ définit une bijection sur l'ensemble des formes réduites de discriminant D.*

• *Sur cet ensemble, la réciproque de ρ est donnée par l'expression*

$$\rho^{-1}(a,b,c) = \big((b''^2 - D)/4a, b'', a\big) \qquad \text{où } b'' = r_D(-b,a).$$

2.3.8. — **Théorème.** *Soit $D > 0$ non carré parfait. Chaque cycle de la permutation induite par ρ sur l'ensemble des formes réduites de discriminant D correspond à une classe d'équivalence pour la relation $\sim$. Ce cycle est exactement formé des formes réduites appartenant à cette classe.*

2.3.9. — **Remarque.** La longueur d'un cycle de formes réelles réduites est toujours impaire puisque les coefficients de x^2 et de y^2 d'une forme réduite sont de signes contraires et que ces signes alternent à chaque itération de ρ.

Formes normales

2.3.10. — **Définition.** Une forme réelle (a,b,c) de discriminant D est dite *normale* si

$$\begin{cases} -|a| < b \leqslant |a| & \text{si } \sqrt{D} \leqslant |a|, \\ \sqrt{D} - 2|a| < b < \sqrt{D} & \text{si } |a| < \sqrt{D}. \end{cases}$$

2.3.11. — **Remarques.** (a) Les inégalités (2.4) impliquent que $\max(\sqrt{D} - 2|a|, 0) < b < \sqrt{D}$. On en déduit aisément que toute forme réduite est normale.

(b) On peut voir que q est normale si et seulement si $-1 \leqslant (\operatorname{sgn} a)(\theta^+_q + \theta^-_q) < 1$ avec $|\theta^+_q - \theta^-_q| \leqslant 1$, ou $0 < (\operatorname{sgn} a)\theta^+_q < 1$ avec $|\theta^+_q - \theta^-_q| > 1$.

(c) Une forme réelle de discriminant D peut être normalisée en lui appliquant l'opérateur T^s, où $s = s_D(b,a)$ est défini par (2.8).

2.4. Automorphismes et unités fondamentales

2.4.1. — **Définitions.** Soit q une forme. Un opérateur $U \in \mathrm{SL}_2(\mathbb{Z})$ est appelé *automorphisme (propre) de q* si $qU = q$.

Les automorphismes de q sont liés a l'équation de Pell :

$$u^2 - Dv^2 = 4 \tag{2.10}$$

puisque, si u, v est une solution de cette équation, alors

$$U_q(u,v) := \begin{pmatrix} \frac{u-bv}{2} & -cv \\ av & \frac{u+bv}{2} \end{pmatrix}$$

est un automorphisme de q. On a même le théorème suivant ([21] page 28) :

2.4.2. — **Théorème.** *Soit q une forme primitive de discriminant D. L'application $(u,v) \mapsto U_q(u,v)$ est une bijection entre les solutions de l'équation de Pell (2.10) et les automorphismes de q.*

En termes d'unités d'ordres quadratiques, on a aussi la proposition suivante (adaptée de [21] page 161). Je dis qu'une unité est *propre* lorsque sa norme est $+1$.

2.4.3. — **Proposition.** *Il y a bijection entre les solutions de l'équation de Pell et les unités propres de l'ordre de discriminant D, donnée par la formule $(u,v) \mapsto (u + v\sqrt{D})/2$.*

L'équation de Pell admet toujours les solutions triviales $(u,v) = (\pm 2, 0)$, ce qui correspond aux automorphismes $\pm I$. Dans le cas où le discriminant D est < -4, il n'y a pas d'autres solutions. Pour le discriminant $D = -4$, il y a deux autres automorphismes $\pm\left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$. Pour le discriminant $D = -3$, les automorphismes non triviaux sont $\pm\left(\begin{smallmatrix} 0 & -1 \\ 1 & 1 \end{smallmatrix}\right)$ et $\pm\left(\begin{smallmatrix} 1 & 1 \\ -1 & 0 \end{smallmatrix}\right)$.

Dans le cas d'un discriminant positif, parcourir le cycle d'une forme réduite en appliquant l'opérateur ρ permet de déterminer l'automorphisme fondamental propre, et donc l'unité fondamentale propre.

2.5. Une variante de la réduction des formes réelles

Cette section se rapporte au travail de thèse [19] d'Aurore Bernard.

En plus des matrices $S = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ et $T = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ qui engendrent le groupe $\mathrm{SL}_2(\mathbb{Z})$, nous utiliserons aussi les matrices $Z = \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$ et $X = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$ de déterminant -1 (donc $S = XZ = -ZX$). On a donc en particulier, pour $q = (a, b, c)$,

$$qS = (c, -b, a), \qquad qT^k = (a, b + 2ak, ak^2 + bk + c), \qquad qZ = (a, -b, c) \qquad \text{et} \quad qX = (c, b, a).$$

L'action des matrices ci-dessus se traduit par une action sur les racines :

$$S : \theta_q^{\pm} \mapsto -1/\theta_q^{\pm}, \qquad T_h : \theta_q^{\pm} \mapsto \theta_q^{\pm} - h, \qquad Z : \theta_q^{\pm} \mapsto -\theta_q^{\mp}, \qquad X : \theta_q^{\pm} \mapsto 1/\theta_q^{\mp}.$$

Le principe de cet nouvelle réduction est de relâcher légèrement la contrainte sur les matrices de passage de chaque étape à la suivante. Celles-ci vont être dans $\mathrm{GL}_2(\mathbb{Z})$ au lieu d'être restreintes à $\mathrm{SL}_2(\mathbb{Z})$. Si besoin, en utilisant la matrice X de déterminant -1 à l'étape finale, la matrice de réduction globale pourra être ramenée dans $\mathrm{SL}_2(\mathbb{Z})$. Le gain est l'obtention de matrices de passage à coefficients plus petits qu'avec la réduction de Gauss.

Formes semi-réduites

2.5.1. — Définition. Nous dirons qu'une forme réelle (a, b, c) est *semi-réduite* lorsque

$$\big|\sqrt{D} - 2|a|\big| < |b| < \sqrt{D}. \tag{2.11}$$

Une forme réelle (a, b, c) est donc semi-réduite si et seulement si $(a, |b|, c)$ est réduite.

Formes semi-normales

2.5.2. — Définition. Une forme réelle (a, b, c) est dite *semi-normale* si elle est normale ou si la forme conjuguée $(a, -b, c)$ est normale. Cette condition s'écrit encore

$$\text{Il existe } \varepsilon = \pm 1 \text{ tel que } \begin{cases} -|a| < \varepsilon b \leqslant |a| & \text{si } \sqrt{D} \leqslant |a|, \\ \sqrt{D} - 2|a| < \varepsilon b < \sqrt{D} & \text{si } |a| < \sqrt{D}. \end{cases}$$

2.5.3. — Remarque. La remarque 2.3.11(a) peut être étendue : toute forme semi-réduite est semi-normale.

La thèse d'Aurore Bernard introduit encore une autre définition proche :

2.5.4. — Définition. Une forme (a, b, c) est *BG-normale* si et seulement si l'une ou l'autre des conditions suivantes est vérifiée :

$$\sqrt{D} - 2|a| < (\operatorname{sgn} a)b < \sqrt{D} \qquad \text{(type I)}$$
$$-\sqrt{D} < (\operatorname{sgn} a)b < 2|a| - \sqrt{D} \qquad \text{(type II)}$$

En désignant par ζ_q^+ et ζ_q^- respectivement la plus grande et la plus petite racines de $q(x, 1)$, c'est-à-dire

$$\zeta_q^{\pm} = \theta_q^{\pm \operatorname{sgn} a} = \frac{-b \pm (\operatorname{sgn} a)\sqrt{D}}{2a},$$

on peut écrire qu'une forme est BG-normale si et seulement si $0 < \zeta_q^+ < 1$ (type I) ou $-1 < \zeta_q^- < 0$ (type II).

2.5.5. — Proposition. *Toute forme semi-normale est BG-normale ([19], prop. 4.1). Une forme BG-normale avec $|a| \leqslant \sqrt{D}$ est semi-normale.*

Opérateur de BG-réduction

On définit l'opérateur ρ' de BG-réduction sur les formes réelles de la manière suivante. Soient $h^\pm$ les deux entiers

$$\begin{cases} h^- = \left\lceil \dfrac{-b-(\operatorname{sgn} c)\sqrt{D}}{2c} \right\rceil = \left\lceil \zeta_{qX}^- \right\rceil \\ h^+ = \left\lfloor \dfrac{-b+(\operatorname{sgn} c)\sqrt{D}}{2c} \right\rfloor = \left\lfloor \zeta_{qX}^+ \right\rfloor \end{cases}$$

et soit h celui des deux qui a plus petite valeur absolue. On définit

$$\rho'(q) = q \cdot XT^h.$$

On a alors l'algorithme de réduction suivant. On part d'une forme BG-normale de type I (si (a,b,c) est BG-normale de type II, partir de $(a,-b,c)$ qui est BG-normale de type I). On itère l'opérateur ρ' jusqu'à obtenir une forme semi-réduite. L'algorithme se termine en un nombre fini d'étapes, et la matrice de passage obtenue satisfait de meilleures bornes que pour une réduction classique.

Bornes de réduction

Pour une matrice $U = \left(\begin{smallmatrix} p & r \\ s & t \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{Z})$, on notera $|U| = \max\{|p|,|r|,|s|,|t|\}$. Dans [18], on trouve le résultat suivant.

2.5.6. — Théorème. *Soit $q=(a,b,c)$ une forme normale de discriminant D (positif ou négatif). On pose $K = \max\{|a|,|b|,|c|\}$. Alors, la matrice de passage U obtenue par l'algorithme de réduction 2.3.6 de q à sa réduite vérifie :*

$$|U| \leqslant K\left(1+\frac{1}{\sqrt{|D|}}\right).$$

En fait, dans le cas $D<0$, la borne obtenue par ces auteurs est un peu meilleure : $|U| \leqslant \frac{2K}{\sqrt{|D|}}$.

La réduction proposée par Bernard et Gama ([19] théorème 4.2) permet d'obtenir une majoration bien meilleure :

2.5.7. — Théorème. *Soit $q=(a,b,c)$ une forme de discriminant $D>0$ et BG-normale de type I.*

- *Le procédé de réduction se termine en au plus $\frac{\log(|a|/\sqrt{D})}{2\log(\phi)}+4$ itérations de ρ', où $\phi=(1+\sqrt{5})/2$.*
- *Notons (a',b',c') la forme semi-réduite et $U = \left(\begin{smallmatrix} p & r \\ s & t \end{smallmatrix}\right)$ la matrice de passage obtenues. Alors U satisfait*

$$|U| \leqslant 4\sqrt{|a/a'|} \qquad et \qquad |prst|^{1/4} \leqslant \sqrt{|st|} \leqslant \sqrt{21|a|/\sqrt{D}}.$$

Dans le cas imaginaire (on suppose donc $a,c>0$), Bernard ([19], Théorème 4.1) obtient aussi une meilleure borne :

2.5.8. — Théorème. *Soit $q=(a,b,c)$ une forme normale de discriminant $D<-4$. Soit $q'=(a',b',c')$ la réduite de q et $U = \left(\begin{smallmatrix} p & r \\ s & t \end{smallmatrix}\right)$ telle que $q\cdot U = q'$. Alors, U est égale à $\pm I$, ou à $\pm ZX = \pm\left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$, ou bien vérifie*

$$|U| \leqslant \sqrt{\frac{\max\{9a,25c\}}{3a'}} \qquad et \qquad |prst|^{1/4} \leqslant \sqrt{2|st|} \leqslant 4\left|\frac{ac}{3D}\right|^{1/4}.$$

Démonstration — Puisque $\det U = \pm 1$, on voit facilement que $st=0$ si et seulement si $U=\pm I$ ou $\pm ZX$. Supposons donc que $st\neq 0$. On a alors

$$a' = ap^2+bps+cs^2 = as^2\left(\left(\frac{p}{s}+\frac{b}{2a}\right)^2+\frac{|D|}{4a^2}\right) \geqslant s^2\frac{|D|}{4a}. \tag{2.12}$$

On en déduit $s^2 \leqslant 4aa'/|D|$. De la même façon, on a $t^2 \leqslant 4cc'/|D|$, donc

$$(st)^2 \leqslant 16\frac{aca'c'}{D^2} \leqslant 16\frac{ac}{3|D|}.$$

puisque $a'c' \leqslant |D|/3$ d'après (2.2). Cela prouve la dernière inégalité de l'énoncé. Toujours d'après (2.2), on a $t^2 \leqslant 4c/3a'$, et aussi $s^2 \leqslant 4a/3c' \leqslant 4a/3a'$. Puisque $a' \leqslant a$ et $s^2 \geqslant 1$, l'équation (2.12) donne $|p/s+b/2a| \leqslant 1$. Comme $|b/2a| \leqslant 1/2$ (q est normale), on obtient $|p/s| \leqslant 3/2$. Mais $\det U = 1$, donc on a $p/s - r/t = 1/st$ donc $|r/t| \leqslant 5/2$. Donc $|pr| \leqslant (15/4)|st|$, ou encore $|prst| \leqslant (15/4)(st)^2 \leqslant (2st)^2$, ce qui prouve la deuxième inégalité. On a obtenu aussi $r^2 \leqslant (25/4)t^2 \leqslant 25c/3a'$ et $p^2 \leqslant (9/4)s^2 \leqslant 9a/3a'$, donc la majoration de $|U|$. □

2.6. Le système de chiffrement Nice

Le système Nice a été introduit dans [50] et repris dans [77]. Le langage qui y est employé est celui d'idéaux dans des corps quadratiques imaginaires, mais on le présente ici avec le langage des formes quadratiques.

Principe

Soit p un nombre premier congru à 3 modulo 4. Alors $D = -p$ est un discriminant, qui est utilisé comme discriminant de base. Le discriminant emboîté sera $-pf^2$, où f est une autre nombre premier. On impose $f > \sqrt{p/3}$, de telle sorte que toute forme quadratique $ax^2 + bxy + cy^2$ réduite de discriminant p vérifie $\operatorname{pgcd}(a, f) = 1$, d'après la borne (2.2). Le discriminant $-pf^2$ est public, mais ses facteurs p et f sont privés, et assez grands pour échapper aux méthodes de factorisation connues. Les longueurs de p et f sont tout de même publiques (c'est utile pour le choix de M et de r dans le chiffrement décrit ci-dessous). On utilisera la surjection de descente $\pi : H(-pf^2) \to H(-p)$ décrite dans la section 2.2. La clé publique est aussi constituée d'un élément de $\ker \pi$, représenté par une forme réduite H.

On encode le message à chiffrer dans une forme quadratique normale M de discriminant $-pf^2$ et de premier coefficient $a < \sqrt{p/4} < \sqrt{pf^2/4}$ donc réduite (voir la proposition 2.1.8). On choisit un entier r au hasard tel que $r < f - 1 \leqslant f - (-p/f)$. Le message chiffré est la forme réduite $C \sim MH^r$. En résumé, M et C sont deux formes réduites et semi-équivalentes.

Pour déchiffrer, on calcule une forme c de discriminant $-p$ telle que $c \cdot R_f = C \cdot T^k$ pour un k convenable (il s'agit simplement de choisir k de telle sorte que le coefficient b de $C \cdot T^k$ soit divisible par f). On réduit c en c', et on normalise ensuite la forme $c' \cdot R_f$ (elle sera même réduite).

Expliquons pourquoi cette dernière forme normale obtenue est M. Il existe une forme normale m de discriminant $-p$ telle que $m \cdot R_f = M \cdot T^{k'}$. On voit que m et M ont même coefficient de tête a (les actions de $T^{k'}$ et de R_f ne changent pas ce coefficient). La forme m est réduite parce que $a < \sqrt{p/4}$. Comme M et C sont semi-équivalentes, on a obtenu $c' = m$ en réduisant c. On en déduit directement a. Normaliser $c' \cdot R_f$ permet de compléter M.

Voici un exemple scolaire (i.e. à taille de clés réduite) de chiffrement Nice. Pour $p = 1\,000\,099$ et $f = 1013$, il y a 187 formes réduites primitives de discriminant $-p$ et 189 618 de discriminant $-pf^2$. Parmi ces dernières, 179 vérifient la contrainte $a \leqslant \sqrt{p/4}$ qui leur donne le statut de clair possible. Choisissons arbitrairement parmi elles le message clair $M = (449, 445, 571\,420\,261)$. La clé publique $K = (289\,825, -175\,463, 911\,807)$ appartenant au noyau de π sera utilisée. On peut alors chiffrer M en $C \sim MK^{400} \sim (148\,993, 104\,089, 1\,740\,191)$.

Pour déchiffrer, on calcule $c \sim \pi(C) \sim (449, 121, 565)$, puis on réduit $(449, 121f, 565f^2)$. La forme obtenue est M.

Arguments initiaux de sécurité

La cryptanalyse de Nice revient à trouver une forme réduite M semi-équivalente à C dont le coefficient de tête est petit. Ce problème est nommé *Hidden Kernel Problem* dans la littérature. On peut l'attaquer directement si on sait évaluer la surjection π. Cette surjection π est calculable pour qui connaît la factorisation de $-pf^2$. La réciproque est vraie aussi, ce qui rend l'attaque cette directe impossible :

2.6.1. — Théorème ([77]). *Supposons qu'on ait un oracle pour π. Alors on obtient la factorisation de $-pf^2$ en temps probabiliste polynomial.*

Ce résultat est évident avec notre formulation utilisant les formes quadratiques, puisque le discriminant d'une forme $\pi(Q)$ est le facteur $-p$ de pf^2. Il l'est toutefois moins avec la présentation initiale utilisant le langage des idéaux, dans lequel le coefficient c de y^2 n'est pas représenté.

Dans l'article original [77], les auteurs s'interrogent aussi sur l'éventualité que la connaissance de H puisse aider à factoriser pf^2. Ils évoquent le calcul d'une forme ambiguë (il n'y a qu'une classe ambiguë non triviale dans le cas de NICE), puis le calcul de l'ordre de H (qui pourrait fournir cette forme ambiguë) avec l'algorithme de Hafner/Mc Curley, donc le coût serait pire qu'une factorisation directe. Ils concluent rapidement que les algorithmes connus ne semblent pas permettre de factoriser pf^2.

L'attaque de Castagnos/Laguillaumie

Pourtant, une attaque efficace de NICE a été présentée :

2.6.2. — Théorème [25]. *Soient D un discriminant fondamental négatif distinct de -3 et de -4, et f un premier impair. Tout élément non trivial de $\ker\pi$ contient un représentant de norme f^2.*

On peut l'énoncer en termes explicites de formes quadratiques : toute forme quadratique de discriminant Df^2 semi-équivalente mais non équivalente à la forme unité, est équivalente à une forme dont le coefficient de tête est f^2.

Pour exploiter ce résultat dans une attaque, il faut s'assurer que l'on trouvera la forme dont le coefficient de tête est f^2 par réduction. Puisque Df^2 n'est probablement pas assez grand pour que cela fonctionne directement, on agrandit à nouveau le discriminant. Pour cela, on choisit un entier r vérifiant $r > 2f/\sqrt{p}$ (on connaît les tailles de p et f) et $\mathrm{pgcd}(r, 2pf) = 1$. On introduit le nouveau discriminant $-pf^2r^2$ et on note π' la surjection canonique $\pi' : H(-pf^2r^2) \to H(-pf^2)$. On a le résultat suivant (traduit ici dans le langage des formes quadratiques) :

2.6.3. — Théorème [25]. *Soient D un discriminant fondamental négatif distinct de -3 et de -4, et f un premier impair. Soit r tel que $\mathrm{pgcd}(r, 2pf) = 1$ et $r > 2f/\sqrt{|D|}$. Soit H une forme de discriminant Df^2 semi-équivalente à la forme unité. Soit $\mathcal{H}$ une forme de discriminant Df^2r^2 telle que $\pi'(\mathcal{H}) = H$. Alors $\mathcal{H}^{\varphi_D(r)}$ est équivalente à la forme unité ou bien à une forme réduite dont le coefficient de tête est f^2.*

Ici, la fonction φ_d est définie par $\varphi_D(r) = r\prod_{s|r}\left(1-(D/s)\frac{1}{s}\right)$ où le produit est sur les facteurs premiers s de r.

Explicitons l'attaque sur l'exemple ci-dessus. Choisissons $r = 3\,000\,983$. On a $\varphi_{-p}(r) = r - 1$ (car r est premier et $(-p/r) = 1$). On peut remonter K en une forme G de discriminant $-pf^2r^2$ en posant (par exemple) $G = K \cdot R_6 = (2610134667904709425, 9910557295571, 10292729)$. Il suffit alors de réduire la forme G^{r-1} pour obtenir $(1026169, 847881, 2251697637571840795)$, dont le coefficient de tête est f^2.

NICE réel

On prend pour discriminant fondamental un nombre premier p pour lesquels les cycles de formes réduites sont courts (premier de Schinzel [80]). Le deuxième discriminant est pf^2 où f est un autre premier impair. Le message clair est encodé dans un entier a tel que $(p/a) = 1$ avec une méthode incorporant de la redondance (il faudra au déchiffrement exploiter cette redondance pour retrouver le clair initial, malgré l'existence de plusieurs formes réduites par cycle). Une forme M de discriminant pf^2 et de coefficient de tête a est ensuite construite. Le chiffré C est une forme réduite prise aléatoirement dans le cycle d'un CH^r où $H \in \ker\pi$ (on peut même choisir délibérément $H = 1$) et r aléatoire. En résumé, le chiffré C est une forme réduite semi-équivalente, voire équivalente, à M.

Pour déchiffrer, on calcule une forme réduite $c \sim \pi(C)$, et on parcourt le cycle (court) de c. L'entier a est coefficient de tête de l'une des formes du cycle de c, et est reconnu grâce à l'encodage redondant.

Voici encore un exemple scolaire. On prend pour discriminant fondamental $p = 100\,109$, et $f = 10\,009$. Il y a 19 cycles de formes réduites de discriminant p, et 38 de discriminant pf^2. L'espace des clairs possibles

(respectant la contrainte $a \leqslant \sqrt{p/4}$) possède 202 éléments. Choisissons arbitrairement la valeur $a = 145$ encodant le message clair. On construit la forme $M = (145, 3166593, -2787071)$ ayant a comme coefficient de tête. Il y a d'autres formes réduites dans le cycle de M, à savoir

$$(29, 3166833, -831715), \quad (133, 3166811, -443269), \quad (79, 3166811, -746263)$$

(ainsi que celles ayant mêmes coefficients en valeur absolue). Cela illustre la nécessité d'utiliser une méthode de redondance (non spécifiée ici) pour reconnaître a lors du déchiffrement. Choisissons d'utiliser la forme $K = (1232405, 949803, -1851421)$, élément de $\ker \pi$, comme clé publique. On obtient le chiffré $C \sim MK^r \sim (91247, 3134095, -565433)$ (avec $r = 400$).

Pour déchiffrer, on calcule $\pi(C) \sim (29, 291, -133) = c$, puis on parcourt le (demi)-cycle de c :

$$(29, 291, -133), \quad (-133, 241, 79), \quad (79, 233, -145), \quad (-145, 57, 167),$$
$$(167, 277, -35), \quad (-35, 283, 143), \quad (143, 289, -29).$$

On y trouve le coefficient de tête de M (au signe près puisqu'on a parcouru qu'un demi-cycle).

Attaque

L'attaque précédente a été adaptée au cas de Nice réel [26]. On y trouve en particulier un algorithme `HomogeneousCoppesmith`, inspiré de [34] qui permet de trouver les solutions (u, v) de $f^2 \mid Q(u, v)$ telles que $|u|, |v| = (\operatorname{disc} Q)^{1/9}$.

L'attaque consiste alors à choisir une forme Q du cycle principal de discriminant pf^2 et chercher u, v tels que $f^2 \mid Q(u, v)$ avec cet algorithme. Si aucune solution n'est trouvée, on itère avec une autre forme Q, choisie au hasard.

Le travail d'Aurore Bernard a permis de montrer que, si l'on parcourt le cycle au lieu de choisir les formes Q au hasard, on parvient sans trop attendre sur une forme Q qui permet de trouver une solution à $f^2 \mid Q(u, v)$, en utilisant une variante de `RationalBonehDurfeeHowgraveGraham` de `HomogeneousCoppersmith`, qui fonctionne lorsque $|uv| = O(\operatorname{disc} Q)^{2/9}$.

La proposition 2.2.6 s'énonce différemment dans le cas réel, puisqu'il existe des automorphismes non triviaux qui font que deux remontées peuvent être équivalentes. On a alors ([22] Th. 7.4 ; voir aussi [19] Th. 5.4) :

2.6.4. — Proposition. *Soient q une forme de discriminant $D > 0$ et f tel* $\operatorname{pgcd}(f, 2a) = 1$. *Soient F l'automorphisme (propre) fondamental de q, et s le plus petit entier tel que $F^s \equiv I$ modulo f. Le nombre de classes d'équivalence distinctes de formes primitives de discriminant Df^2 obtenues par la construction $q \cdot R_g$ avec $g \in \mathbb{Z}$ est $\varphi_D(f)/s$.*

Soient q une forme de discriminant $D > 0$, et F son automorphisme fondamental. On pose $k_0 = \infty$, puis on définit k_i tel que $FQ_{k_{i-1}} = Q_{k-i}$ (avec $0 \leqslant k_i < f$). Les formes $q \cdot Q_{k_i}$ pour $i = 0, \cdots, s-1$ sont différentes remontées équivalentes, et régulièrement réparties sur le cycle de q. On les désigne sous le nom de *ceinture de q*, et le choix de n'importe laquelle d'entre elles pour Q fait que l'attaque ci-dessus fonctionne. Le travail d'Aurore Bernard a donc prouvé que l'attaque fonctionne toujours, et a amélioré son coût.

Chapitre 3

Bases normales autoduales explicites pour les corps finis

Ce chapitre est issu d'un travail [15] en collaboration avec Stéphane Vinatier et Erik J. Pickett. Stéphane m'avait présenté la construction d'Erik [78], permettant d'obtenir des bases normales autoduales d'extensions de corps en caractéristique quelconque. La question se posait alors de savoir si sa méthode pouvait être implantée dans un algorithme, et de déterminer son efficacité, dans le cas des corps finis. Rappelons que les bases normales autoduales permettent d'obtenir une arithmétique efficace des corps finis, en particulier celles dites de complexité minimale.

Il a fallu repenser la méthode d'Erik de façon plus concrète avant d'envisager une programmation en MAGMA. Nous avons pu alors énumérer les bases normales autoduales de certaines extensions de corps finis de façon assez efficace (cette énumération devient nécessairement laborieuse pour des extensions de taille modeste puisque le nombre de telles bases croît très rapidement), et étudier leur complexité. En plus d'avoir obtenu une méthode explicite pour construire ces bases, nous avons pu ainsi étendre des tables déjà publiées [57][72].

Les sections 3.2 et 3.3 exposent la méthode d'Erik telle que nous l'avons repensée, et la section 3.4 présente les expériences que nous avons menées avec cette méthode.

3.1. Introduction

Soient $\mathbb{F}_q$ un corps fini et $\mathbb{F}_{q^n}$ une extension.

Bases duales, normales

Soient $A = (\alpha_0, \ldots, \alpha_{n-1})$ et $B = (\beta_0, \ldots, \beta_{n-1})$ deux $\mathbb{F}_q$-bases de $\mathbb{F}_{q^n}$. On dit que les bases A et B sont *duales* si

$$\mathrm{tr}(\alpha_i \beta_j) = \begin{cases} 1 & \text{lorsque } i = j \\ 0 & \text{sinon} \end{cases} \tag{3.1}$$

Pour A base fixée, il y a une unique base B vérifiant (3.1), nommée la *base duale de A*. La base duale de A permet d'obtenir les coordonnées dans A d'un élément en utilisant la trace :

3.1.1. — Proposition. *Soit $u = \sum_{i=0}^{n-1} u_i \alpha_i$ un élément exprimé dans la base A, et B la base duale de A. Alors $u_i = \mathrm{tr}(u\beta_i)$.* □

Une base de $\mathbb{F}_{q^n}$ sur $\mathbb{F}_q$ est dite *normale* si elle est de la forme $(\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}})$. En utilisant une telle base pour représenter les éléments de $\mathbb{F}_q$ l'opération $x \mapsto x^q$ et le calcul de trace deviennent des opérations de coût quasiment nul. Tout élément α de $\mathbb{F}_{q^n}$ tel que $\mathrm{pgcd}(X^n - 1, \sum_{i=0}^{m-1} \alpha^{q^i} X^{m-i-1}) = 1$ ([69]) engendre une base normale. La base duale d'une base normale est normale aussi. Toute extension de corps finis possède une base normale [68].

Complexité

Le calcul du produit de deux éléments de $\mathbb{F}_{q^n}$ exprimés dans la base $(\alpha^{q^i})_{0 \leqslant i \leqslant n-1}$ est obtenu par bilinéarité à partir des produits

$$\alpha^{q^i} \cdot \alpha^{q^j} = \sum_{k=0}^{n-1} \lambda_{i,j}^{(k)} \alpha^{q^k}.$$

Par normalité de la base, les *constantes de structure* $\lambda_{i,j}^{(k)}$ vérifient la relation $\lambda_{i+\ell,j+\ell}^{(k+\ell)} = \lambda_{i,j}^{(\ell)}$ pour tous entiers i, j, k, ℓ (les additions d'indices étant pris modulo n). On peut donc se contenter de stocker seulement n^2 de ces n^3 coefficients, par exemple la matrice de la multiplication par α, qui contient les coefficients $\lambda_{i,0}^{(k)}$, ou bien la *matrice de structure*, qui contient les $\lambda_{i,j}^{(0)}$.

Le coût de la multiplication de deux éléments de $\mathbb{F}_{q^n}$ dans cette représentation est associé au nombre de coefficients non nuls dans l'une (ou l'autre) de ces matrices. Ce nombre est nommé *complexité de* α [74]. Il est au moins égal à $2n-1$, comme cela a été montré dans [76] et dans le cas d'égalité, on dit que la base normale engendrée par α est *optimale*. L'existence de bases normales optimales a été étudiée dans [45].

Bases normales autoduales

Certaines bases ont la propriété d'être leur propre duale. De telles bases n'existent pas pour toutes les extensions, comme le précise ce résultat de [67].

3.1.2. — Théorème. *L'extension $\mathbb{F}_{q^n}$ de $\mathbb{F}_q$ possède une base normale autoduale si et seulement si l'une des deux conditions suivantes est vérifiée.*

- *Le degré n est impair.*
- *$n \equiv 2$ modulo 4 et q pair.*

S'il est facile de trouver des bases normales, le problème de la construction de bases normales autoduales est plus complexe. Wang traite complètement le cas q pair et n impair dans [88]. Jungnickel [57] calcule les bases normales autoduales sur les extensions de $\mathbb{F}_2$ de degré $\leqslant 47$ et tabule les meilleures complexités.

3.2. Reformulation du problème de la construction

Dans le cas d'une base normale autoduale engendrée par α, la matrice de structure est donnée par

$$M_\alpha = \left(\operatorname{tr}(\alpha^{1+q^i+q^j})\right)_{0\leqslant i,j\leqslant n-1}. \tag{3.2}$$

La complexité de α est le nombre de coefficients non nuls de cette matrice.

Soit donc A une base normale engendrée par α. On cherche une base B normale autoduale engendrée par β et sous la forme $B = AP$ où P est une matrice $n \times n$ à coefficients dans $\mathbb{F}_q$. Le fait que A et B soient normales entraîne que P et P^{-1} sont circulantes :

$$P^{-1} = \begin{pmatrix} \rho_0 & \rho_{n-1} & \cdots & \rho_2 & \rho_1 \\ \rho_1 & \rho_0 & \rho_{n-1} & & \rho_2 \\ \vdots & \rho_1 & \rho_0 & \ddots & \vdots \\ \rho_{n-2} & & \ddots & \ddots & \rho_{n-1} \\ \rho_{n-1} & \rho_{n-2} & \cdots & \rho_1 & \rho_0 \end{pmatrix}. \tag{3.3}$$

On montre alors ([57] 5.5.3) que la base normale B est autoduale si et seulement si

$$(P^{-1})^t \cdot P^{-1} = \left(\operatorname{tr}(\alpha^{q^i+q^j})\right)_{0\leqslant i,j\leqslant n-1}. \tag{3.4}$$

Cette condition peut s'écrire sous forme d'un système d'équations

$$\rho_0\rho_k + \cdots + \rho_{n-1}\rho_{n-1+k \bmod n} = \operatorname{tr}(\alpha\alpha^{q^k}) \qquad \text{pour } k = 0, \ldots, n-1. \tag{3.5}$$

On considère alors l'algèbre de groupe $\mathbb{F}_q[G]$, où G est ici le groupe de Galois de l'extension $\mathbb{F}_{q^n} : \mathbb{F}_q$, engendré par l'automorphisme de Frobénius ϕ. La conjugaison $u \mapsto \overline{u}$ dans $\mathbb{F}_q[G]$ est l'application linéaire obtenue à partir de $g \mapsto g^{-1}$ pour $g \in G$. La correspondance qui à $v = \sum_{i=0}^{n-1} \rho_i\phi^i$ associe la matrice (3.3) est un isomorphisme de l'algèbre $\mathbb{F}_q[G]$ sur celle des matrices circulantes. Les coefficients de $v\overline{v}$ sont alors les membres gauches du système (3.5). En posant $R = \sum_{k=0}^{n-1} \operatorname{tr}(\alpha\alpha^{q^k})\phi^k$, l'équation (3.5) devient $v\overline{v} = R$. En explicitant la construction, on obtient :

3.2.1. — Proposition ([78][88]). *Soit α engendrant une base normale. On pose*

$$R=\sum_{g\in G}\mathrm{tr}\left(\alpha g(\alpha)\right)\cdot g\in\mathbb{F}_q[G]. \tag{3.6}$$

Alors l'extension admet une base normale autoduale si et seulement si l'équation $v\overline{v}=R$ admet une solution $v\in\mathbb{F}_q[G]$. Dans ce cas, v admet un inverse w et l'élément $\beta=w\circ\alpha$ est générateur d'une base normale autoduale.

L'algèbre de groupe $\mathbb{F}_q[G]$

Le groupe de Galois de $\mathbb{F}_{q^n}$ sur $\mathbb{F}_q$ est cyclique d'ordre n. La $\mathbb{F}_q$-algèbre $A=\mathbb{F}_q[G]$ est isomorphe au quotient $\mathbb{F}_q[X]/(X^n-1)$. Posons $n=p^e n_1$, où p est la caractéristique de $\mathbb{F}_q$. On peut écrire $X^n-1=(X^{n_1}-1)^{p^e}$ avec $X^{n_1}-1$ sans facteurs carrés.

Le cas $n=p^e$

Dans ce cas, l'algèbre $\mathbb{F}_q[G]$ est isomorphe à $\mathbb{F}_q[X]/(X-1)^n$. Soit ϵ l'application d'*augmentation* $A\ni\sum_{g\in G}\rho_g g\mapsto\sum_{g\in G}\rho_g\in\mathbb{F}_q$. Les éléments de A qui sont inversibles sont ceux dont l'image par ϵ est non nulle. Donc, le groupe des inversibles $A^\times$ est d'ordre $q^{n-1}(q-1)$. Plus précisément, il est le produit direct de $\mathbb{F}_q^*$ par U, l'image réciproque de 1 par ϵ.

Si $p=2$, alors $e=1$ et $n=2$ d'après le théorème 3.1.2. Il suffit de prendre $\beta\in\mathbb{F}^{q^2}$ tel que $\mathrm{tr}(\beta)=1$ pour obtenir un générateur d'une base normale autoduale.

On suppose maintenant p impair. On peut voir alors que $\epsilon(R)=\mathrm{tr}(\alpha)^2$ donc la décomposition de R dans le produit direct ci-dessus est de la forme $R=\mathrm{tr}(\alpha)^2\cdot(1+(X-1)R_0)$ Le deuxième facteur est aussi un carré puisqu'il appartient au groupe U d'ordre impair. Donc $R=\theta^2$. Si $R=v\overline{v}$ alors $\overline{\theta}^2=\theta^2$. Donc $\overline{\theta}/\theta$ est une racine de l'unité appartenant au groupe U d'ordre impair. Donc $\overline{\theta}=\theta$.

Cela montre que trouver une solution de l'équation $v\overline{v}=R$ (s'il en existe) revient à un calcul de racine carrée dans A. Cela peut être réalisé par un calcul modulo $X-1$ puis par une remontée à la Hensel.

3.3. Le cas $\mathrm{pgcd}(n,q)=1$

Dans ce cas, le théorème 3.1.2 précise que n est impair. Le polynôme X^n-1 est sans facteurs carrés et se factorise en facteurs irréductibles sur $\mathbb{F}_q$:

$$X^n-1=\prod_{i=1}^{\sigma}f_i(X)\prod_{j=1}^{\tau}g_j(X)\cdot g_j^*(X) \tag{3.7}$$

où g_j^* est le polynôme réciproque (à un facteur constant près) de g_j et où les f_i sont autoréciproques (encore à un facteur constant près). Il s'agit de transposer l'équation $R=v\overline{v}$ dans ce produit, la résoudre, et remonter la solution dans $\mathbb{F}_q[G]$ en utilisant le théorème des restes chinois. C'est ce que nous précisons dans cette section.

Classes cyclotomiques

Soit m l'ordre de q modulo n. Le corps $\mathbb{F}_{q^m}$ contient une racine primitive n-ième ω de 1. Dans l'ensemble $\{0,\ldots,n-1\}$ on définit les *classes d'équivalence cyclotomiques* : $s\sim s'$ s'il existe k tel que $s\equiv q^k s'$ modulo n. On a alors :

3.3.1. — Proposition. *(a) Si ω^s est racine d'un facteur irréductible de X^n-1, alors ses autres racines sont les $\omega^{s'}$ avec $s'\sim s$.*

(b) Les ω^s avec $s\sim(n-s)$ sont racines des facteurs autoréciproques f_i. Les ω^s avec $s\not\sim n-s$ sont racines des facteurs des g_j qui ne sont pas autoréciproques.

(c) Le nombre de classes cyclotomiques est le nombre $\sigma+2\tau$ de facteurs irréductibles de X^n-1.

(d) Les facteurs autoréciproques f_i, hormis $f_1=X-1$, sont de degré pair.

Décomposition de Maschke

La factorisation (3.7) permet de décomposer l'algèbre $\mathbb{F}_q[X]/(X^n-1)$ en un produit de $\sigma+2\tau$ corps :

$$\mathbb{F}_q[X]/(X^n-1) \simeq \prod_{i=1}^{\sigma} \mathbb{F}_q[X]/\big(f_i(X)\big) \times \prod_{j=1}^{\tau} \Big(\mathbb{F}_q[X]/\big(g_j(X)\big) \times \mathbb{F}_q[X]/\big(g_j^*(X)\big)\Big). \tag{3.8}$$

Chaque facteur de cette décomposition est une extension de $\mathbb{F}_q$ contenue dans $\mathbb{F}_{q^m}$. L'application $\mathbb{F}_q[X]/(f) \ni u(x) \mapsto u(\omega^s) \in \mathbb{F}_q(\omega^s)$, où f désigne un f_i ou un g_j, et $s \in \{0,\dots n-1\}$ avec $f(\omega^s)=0$ est un isomorphisme de corps. On a alors :

3.3.2. — Proposition. *Soit S un ensemble de représentants des classes cyclotomiques. L'application*

$$\begin{cases} \mathbb{F}_q[X]/(X^n-1) \longrightarrow \displaystyle\prod_{s\in S} \mathbb{F}_q(\omega^s) \\ \qquad\qquad u(X) \longmapsto \big(u(\omega^s)\big)_{s\in S} \end{cases} \tag{3.9}$$

est un isomorphisme de $\mathbb{F}_q$-algèbres. □

Il s'agit d'une forme de transformée de Fourier discrète. Le cas usuel correspondant à celui où $\omega \in \mathbb{F}_q$ et donc où les facteurs simples sont n copies de $\mathbb{F}_q$. Pour $u(X)=\sum_{t=0}^{n-1} u_t X^t$, on a $\hat{u}_s = u(\omega^s) = \sum_{t=0}^{n-1} u_t \omega^{st}$.

Transformée de Fourier

D'un point de vue pratique, il est plus confortable de calculer une composante pour chaque s tel que $0 \leqslant s \leqslant n-1$, et donc de définir l'application $\mathcal{F}$:

$$\mathcal{F} : \begin{cases} \mathbb{F}_q[X]/(X^n-1) \longrightarrow (\mathbb{F}_{q^m})^n \\ \qquad\qquad u(X) \longmapsto \big(u(\omega^s)\big)_{0\leqslant s\leqslant n-1}. \end{cases} \tag{3.10}$$

C'est un homomorphisme de $\mathbb{F}_q$-algèbres, de matrice $H(\omega) = (\omega^{ij})_{0\leqslant i,j\leqslant n-1}$. L'application réciproque $\overline{\mathcal{F}}$ a pour matrice $H(\omega^{-1})$.

$$\overline{\mathcal{F}} : \begin{cases} (\mathbb{F}_{q^m})^n \longrightarrow \mathbb{F}_{q^m}[X]/(X^n-1) \\ (r_0,\dots,r_{n-1}) \longmapsto \displaystyle\sum_{t=0}^{n-1} u_t X^t \quad \text{avec } u_t = \textstyle\sum_{i=0}^{n-1} r_i \omega^{-ti} \end{cases} \tag{3.11}$$

parce que $\overline{\mathcal{F}}\big(\mathcal{F}(u)\big) = nu$ pour chaque $u \in \mathbb{F}_q[X]/(X^n-1)$.

L'équation $v\overline{v} = R$

L'application de conjugaison induite par $X \mapsto X^{n-1}$ sur $\mathbb{F}_q[X]/(X^n-1)$ est donnée par $\omega \mapsto \omega^{-1}$, elle sera parfois ici notée J.

Soit R défini par (3.6). Soit R_s la s-coordonnée de $\mathcal{F}(R)$. On a donc $R_s = \sum_{i=0}^{n-1} \mathrm{tr}(\alpha^{1+q^i})\omega^{si}$. Trois lemmes permettent de traiter respectivement les trois cas possibles : le cas $s=0$, le cas $0 \not\sim s \not\sim n-s$, le cas $0 \not\sim s \sim n-s$.

3.3.3. — Lemme (3.5 dans [78]). *Pour $v_0 = \mathrm{tr}(\alpha)$, on a $v_0\overline{v_0} = R_0$.*

3.3.4. — Lemme (3.6 dans [78]). *Soit $s' \in S$ tel que $s' \sim n-s$. On a $R_s = R_{s'}$. En posant $v_{s,s'} = (R_s, 1) \in \mathbb{F}_q(\omega^s) \times \mathbb{F}_q(\omega^{s'})$, on a $v_{s,s'}\overline{v_{s,s'}} = (R_s, R_{s'})$.*

3.3.5. — Lemme (3.7 dans [78]). *Soit $s \in S$ tel que $0 \neq s$ et $s \sim n-s$. Le corps $\mathbb{F}_q(\omega)$ est stable sous l'action de la conjugaison J. Soit $Z = \{z \in \mathbb{F}_q(\omega) \mid J(z) = z\}$. Nous distinguons trois cas.*

(a) Dans le cas où R_s admet une racine carré v_s dans Z, alors $v_s\overline{v_s}=R_s$.
(b) Dans le cas où ni R_s ni $-R_s$ n'ont de racine carrée dans Z (mais $-R_s$ en a bien une v_s dans $\mathbb{F}_q(\omega^s)$), on a $v_s\overline{v_s}=R_s$.
(c) Dans le cas où R_s n'a pas de racine carrée dans Z mais où il existe $u\in Z$ tel que $u^2=-R_s$, il existe $u'\in\mathbb{F}_q(\omega^s)$ tel que $u'^2=R_s$. Il existe aussi un entier n tel que $-n$ est un carré η^2 non nul modulo la caractéristique p de $\mathbb{F}_q$, mais $-(n-1)$ n'est pas une carré modulo p. Il existe un entier ν tel que $\nu^2\equiv n-1$ modulo p. Posons $v_s=(u+\nu u')/\eta$. Alors $v_s\overline{v_s}=R_s$.

Changement de base normale autoduale

Nous avons adopté ici une stratégie expérimentale. Pour de petites valeurs de q et n, nous avons explicité toutes les bases normales autoduales, et calculé la complexité de chacune d'entre elles. Pour cela, nous avons explicité comment trouver toutes les bases normales autoduales à partir d'une seule d'entre elles. Pour $v=\sum_{g\in G}v_g g\in\mathbb{F}_q[G]$ et $\gamma\in\mathbb{F}_{q^n}$, nous notons $v\circ\gamma=\sum_{g\in G}v_g g(\gamma)$.

3.3.6. — Proposition. *Soient α générateur d'une base normale de $\mathbb{F}_{q^n}$ sur $\mathbb{F}_q$ et $w\in\mathbb{F}_q[G]$. Soit $\beta=w\circ\alpha$.*
(a) β engendre une base normale de $\mathbb{F}_{q^n}$ sur $\mathbb{F}_q$ si et seulement si w est inversible dans $\mathbb{F}_q[G]$.
(b) Supposons que α engendre une base normale autoduale. Alors la base engendrée par β est normale autoduale si et seulement si $w\overline{w}=1$.

3.3.7. — Proposition. *Soit A une base normale autoduale de $\mathbb{F}_{q^n}$ sur $\mathbb{F}_q$, et P une matrice sur $\mathbb{F}_q$, non singulière et de taille $n\times n$. la base $B=AP$ est normale autoduale si et seulement si la matrice P est orthogonale circulante.*

Résolution de $v\overline{v}=1$

La décomposition (3.9) permet d'obtenir les solutions de cette équation. Soit $V(X)\in\mathbb{F}_q[X]/(X^n-1)$. Pour $s\in S$, on note V_s le composant $V(\omega^s)$ correspondant au facteur $F_q(\omega^s)$ dans cette décomposition. En utilisant les lemmes 3.3.3, 3.3.4 et 3.3.5, on obtient :

3.3.8. — Proposition. *Le polynôme $V(X)$ vérifie l'équation $V(X)V(X^{n-1})=1$ modulo X^n-1 si et seulement si :*

$$\begin{aligned} V(1)&=\pm 1 && \textit{(lorsque } s=0\textit{)},\\ V(\omega^s)V(\omega^{-s})&=1 && \textit{lorsque } s\not\sim n-s,\\ V(\omega^s)^{q^{r/2}+1}&=1 && \textit{lorsque } 0\neq s\sim n-s\textit{, où } r \textit{ est tel que } \mathbb{F}_q(\omega^s)=\mathbb{F}_{q^r}. \end{aligned}$$

Le cardinal du groupe des solutions de $v\overline{v}=1$ est en fait aussi le nombre de matrices circulantes orthogonales de taille $n\times n$. C'est aussi le nombre de bases normales autoduales de $\mathbb{F}_{q^n}$ sur $\mathbb{F}_q$. Cela permet de retrouver le résultat suivant obtenu dans [58] en utilisant des formules données par [70] :

3.3.9. — Théorème. *Utilisons la décomposition (3.7) de X^n-1 sur $\mathbb{F}_q$. Le nombre*[1] *de bases orthonormales autoduales de $\mathbb{F}_{q^n}$ sur $\mathbb{F}_q$ est donné par*

$$2^a\prod_{i=1}^{\sigma}(q^{c_i}+1)\prod_{j=1}^{\tau}(q^{d_j}-1)\qquad \text{avec}\ \begin{cases} a=0 \textit{ pour } q \textit{ pair, et } a=1 \textit{ pour } q \textit{ impair}\\ 2c_i=\deg f_i \textit{ et } d_j=\deg g_j \end{cases}$$

[1] *Dans [58], deux bases dont l'une est obtenue par permutation cyclique des éléments de la première sont considérées comme une seule et même base. Nous n'utilisons pas la même convention, ce qui se traduit par un facteur n supplémentaire dans les formules de dénombrement.*

3.4. Expérimentations

Algorithmes

Ces résultats permettent d'énumérer (relativement) rapidement les bases normales autoduales d'une extension $\mathbb{F}_{q^n} : \mathbb{F}_q$ de corps finis. Nous avons implémenté (en `Magma`) le cas où $\mathrm{pgcd}(n, q) = 1$ et celui où n est une puissance de la caractéristique de $\mathbb{F}_q$.

Étape 1. Calculer les q-classes cyclotomiques de l'ensemble $\{0, \dots, n-1\}$.

Étape 2. Soit m la taille de la plus grande classe (celle qui contient 1). Choisir ω d'ordre n dans $\mathbb{F}_{q^m}$.

Étape 3. Construire les matrices $H(\omega) = (\omega^{ij})_{1 \leqslant i \leqslant j}$ et $H(\omega^{-1})$.

Étape 4. Rechercher un élément normal β dans $\mathbb{F}_{q^n}$ (cela est déjà implémenté en `Magma`, selon la méthode présentée dans [74]).

Étape 5. Calculer $R \in \mathbb{F}_q[G]$ défini par (3.6). En utilisant la matrice $H(\omega)$, calculer l'image R' de R par $\mathcal{F}$ dans $(\mathbb{F}_{q^m})^n$.

Étape 6. Utiliser les lemmes 3.3.3, 3.3.4 et 3.3.5 pour trouver une solution $v' \in \mathrm{Im}\,\mathcal{F} \subseteq (\mathbb{F}_q^m)^n$ de $v'\overline{v'} = R'$. Ramener v' dans $\mathbb{F}_q[G]$ en utilisant la matrice $H(\omega^{-1})$ pour obtenir v tel que $v\overline{v} = R$. Calculer $w = v^{-1}$.

Étape 7. Calculer $\gamma = w \circ \beta$.

Étape 8. Utiliser la proposition 3.3.8 pour trouver des générateurs (et leurs ordres) du groupe U des solutions de $u\overline{u} = 1$ dans $\mathbb{F}_q[G]$.

Étape 9. Pour chaque u dans U (les énumérer en utilisant les générateurs), calculer : un générateur $\gamma = (uw) \circ \beta$ d'une base normale autoduale ; la matrice de multiplication $\left(\mathrm{tr}(\gamma^{1+q^i+q^j})\right)_{i,j}$; et la complexité de γ. En tenir compte pour mettre à jour la meilleure complexité trouvée jusqu'à cette itération et la liste des meilleures bases normales autoduales.

Étape 10. Finalement, retourner la meilleure complexité obtenue et le nombre de fois où elle l'a été.

Tables

Nous disons qu'une base normale autoduale est meilleure qu'une autre lorsque sa complexité est plus basse. La table suivante liste les complexités des meilleures bases normales autoduales, obtenues par construction exhaustive, pour quelques petits paramètres impairs q et n. Le facteur indiqué entre parenthèses précise que plusieurs familles de bases de meilleure complexité ont été obtenues (une famille contient $2n$ bases de même complexité, engendrées par $\pm\alpha^{q^i}$ avec $0 \leqslant i \leqslant n-1$).

Le coût de la construction exhaustive nous a contraints à laisser certaines cases vides.

$q \backslash n$	3	5	7	9	11	13	15	17	19	21	23	25
3	**7**	13	25	**37**	55(2)	67	−−	91	172	−−	127	135
5	6	**13**	25	46	64	85	−−	157	153	150		
7	6	16	**19**	41	61	96	87			−−		
11	6	13	25	52	**31**	100	78					
13	6	13	25	51(4)	64	**37**						
17	8	13	25	51(5)	64	100		−−				
19	8	13	31	51	67				−−			

Pour $q = 2^r$, nous avons calculé une table similaire. Le multiplicateur indiqué entre parenthèses indique encore le nombre de familles de meilleure complexité, mais ici chaque famille contient n bases. Les valeurs

pour $q = 2$ sont déjà présentes dans [57] et [72] (avec une petite erreur typographique).

$q\backslash n$	3	5	7	9	11	13	15	17	19	21	23	25	27	29
2	5	9	21	17	21	45	45	81	117(2)	105	45	93	141	57
4	5	9	21	17	21	45	45	81	117(2)	105	45	93		
8	9(3)	9	21	45(3)	21	45	81(3)	81						
16	5	9	21	17	21	45								
32	5	19(15)	21	17	21									
64	9(21)	9	21	45(3)										
128	5	9	37(98)											
256	5	9												

Chapitre 4

Registres à retenues

Les automates FCSR (pour *Feedback with Carry Shift Registers*) ont été introduits par Klapper & Goresky dans [63]. Ils sont similaires aux classiques LFSR (*Linear Feedback Shift Registers*) qui sont omniprésents dans la conception de générateurs pseudo-aléatoires. La différence essentielle entre les deux types d'automates est que l'addition bit-à-bit employée par les LFSR est une addition modulo 2, alors que celle employée par les FCSR est à propagation de retenues, d'où une fonction de transition non linéaire.

Ce chapitre expose une série de travaux effectués en commun avec Thierry Berger, Cédric Lauradoux, Marine Minier, Abdelkader Necer, Benjamin Pousse. La section 4.1 présente des résultats classiques complétés par un travail publié dans [9][11]. La section 4.2 présente une nouvelle méthode [13] de reconstruction d'un automate FCSR à partir de la suite générée, basée sur l'algorithme d'Euclide étendu. La section 4.3 présente une généralisation [10][11] utile et éclairante des FCSR, qui étaient auparavant implémentés sous deux formes dégénérées : le mode Fibonacci et le mode Galois. Nous avons par ailleurs publié un travail similaire ([12] non présenté dans ce mémoire) sur les LFSR. La section 4.4 pousse la généralisation encore plus loin [14]. Finalement, la section 4.5 présente un membre F-FCSR-H de la famille FFCSR d'algorithmes de chiffrement à flot que nous avons conçus. Cet algorithme a été retenu dans le projet européen eSTREAM [38]

4.1. Automate FCSR

Un automate FCSR est constitué de deux registres (ensemble de cellules) : un *registre principal* M et un *registre de retenues* C. Le nombre de cellules du registre principal est la *longueur du FCSR*, que l'on notera ici n. Le contenu de chaque cellule du registre principal est un bit noté m_i, avec $0 \leqslant i < n$. Le registre de retenues contient ℓ cellules avec $\ell < n$. Le contenu de ces cellules est un bit noté c_i où i parcourt un sous-ensemble I de $\{0, \ldots, n-2\}$ de cardinal ℓ. On posera souvent par convention $c_i = 0$ lorsque $i \notin I$. On posera $d = \sum_{i=0}^{n-1} d_i 2^i$ avec $d_i = 1$ si la cellule c_i existe ($i \in I_d$) ainsi que $d_{n-1} = 1$; et $d_i = 0$ pour les autres indices. On nomme *entier de rétroaction* du FCSR l'entier (négatif) $q = 1 - 2d$. L'automate FCSR — en architecture Galois — est un circuit de division par q, représenté par le schéma suivant.

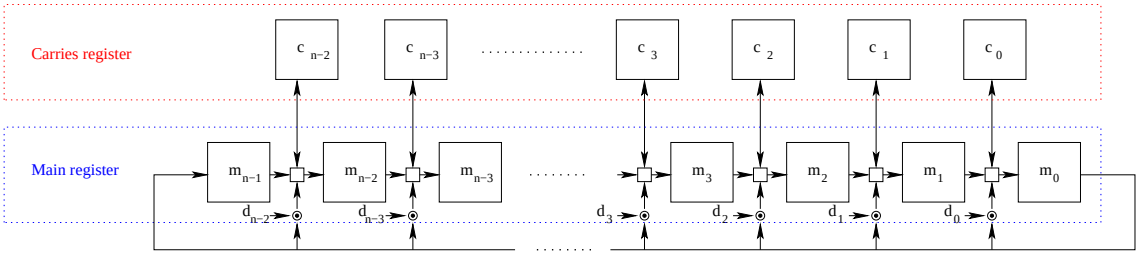

Figure 4.1. Un automate FCSR

Le symbole carré entre deux cellules du registre principal représente un additionneur :

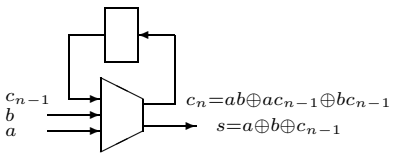

Figure 4.2. Additionneur

Il prend en entrée trois bits c_i, m_{i+1} et m_0 et calcule la somme sur deux bits. Le bit de poids faible sera le nouveau m_i et le bit de poids fort sera le nouveau c_i :

$$m_i(t+1) + 2c_i(t+1) = c_i(t) + m_{i+1}(t) + m_0(t).$$

La fonction de transition de l'automate est complètement décrite par les formules suivantes :

$$\begin{array}{lll} \text{Pour } i \in I & : & m_i(t+1) = m_{i+1}(t), \\ \text{Pour } i \in \{0,\dots,n-2\} \setminus I & : & \begin{cases} m_i(t+1) = c_i(t) \oplus m_{i+1}(t) \oplus m_0(t), \\ c_i(t+1) = c_i(t)m_{i+1}(t) \oplus m_{i+1}(t)m_0(t) \oplus c_i(t)m_0(t), \end{cases} \\ \text{Pour } i = n-1 & : & m_{n-1}(t+1) = m_0(t). \end{array}$$

Ce qui peut être résumé par les seules formules :

$$\begin{cases} m_i(t+1) = c_i(t) \oplus d_i m_{i+1}(t) \oplus d_i m_0(t), \\ c_i(t+1) = c_i(t)m_{i+1}(t) \oplus d_i m_{i+1}(t)m_0(t) \oplus c_i(t)m_0(t). \end{cases}$$

Voici un exemple, avec $n = 8$, et $d = 174 = 128 + 32 + 8 + 4 + 2$ (soit $l = 4$).

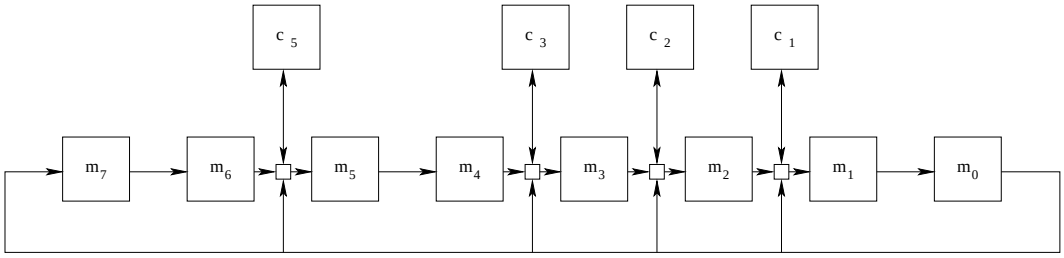

Figure 4.3. Un exemple d'automate FCSR

Développement 2-adique

L'étude des LFSR, est intimement liée à celle des suites récurrentes linéaires sur $\mathbb{F}_2$, et celle des séries rationnelles. Pour des raisons similaires, l'étude des FCSR est liée aux entiers 2-adiques. En particulier, les résultats suivants sont bien connus, et ont été introduits dans la littérature cryptographique par Goresky et Klapper [48][64].

4.1.1. — Théorème [64]. *Soient $S = (s_n)_{n\in\mathbb{N}}$ une suite binaire et s l'entier 2-adique de développement S. Alors la suite S est ultimement périodique si et seulement si il existe deux entiers p, q avec q impair tels que $s = p/q$. De plus la prépériode de S est de longueur nulle (S est périodique) si et seulement si $pq \leqslant 0$ et $|p| \leqslant |q|$.*

4.1.2. — Théorème [64]. *Soient S une suite binaire ultimement périodique et $s = p/q$ avec q impair et $\mathrm{pgcd}(p, q) = 1$ l'entier 2-adique de développement S. La période de S est l'ordre de 2 modulo q.*

La notion de complexité linéaire bien connue pour les suites générées par des registres sans retenue se scinde en deux notions très légèrement différentes si on veut l'adapter aux registres à retenues :

4.1.3. — Définitions [64]. Soit S une suite binaire ultimement périodique (et p, q les entiers vérifiant les conditions du théorème précédent).
(a) La *complexité 2-adique de S*, est donnée par $\log_2\big(\max(|p|, |q|)\big)$.
(b) L'*envergure 2-adique* de S est la longueur (le nombre de cellules du registre principal) minimale des FCSR générant S. C'est aussi le nombre de bits nécessaires pour représenter $\max(|p|, |q|)$.

Suites engendrées par un FCSR

Il est bien connu que la suite binaire générée par un FCSR (dont on extrait les termes de la cellule m_0), est le développement 2-adique d'une fraction rationnelle. Nous avons d'abord généralisé dans [9] ce résultat à l'ensemble des cellules du registre principal, et explicité des relations entre les fractions associées à chaque cellule.

On considère un FCSR de longueur n et d'entier de rétroaction q. On pose $m(t) = \sum_{i=0}^{n-1} m_i(t)2^i$ et $c(t) = \sum_{i\in I_d} c_i(t)2^i$. Les entiers $m(t)$ et $c(t)$ sont désignés sous le terme de contenus des registres principal et de retenues à l'instant t. On dit aussi que l'automate est dans l'état $\big(m(t), c(t)\big)$. On pose aussi $p(t) = m(t) + 2c(t)$, que l'on appelle parfois le *contenu algébrique* de l'automate FCSR. On vérifie que les valeurs avant et après une transition de l'automate satisfont la relation $2p(t+1) \equiv p(t)$ modulo q. De plus, si le FCSR est initialement dans l'état (m, c) alors la suite générée par le FCSR est l'expansion 2-adique de p/q, où $p = m + 2c$ est le contenu algébrique initial. On a plus généralement le résultat suivant [9], où les suites $M_i = (m_i(t))_{t\in\mathbb{N}}$ sont les suites générées par les différentes cellules du registre principal (avec $0 \leqslant i \leqslant n-1$).

4.1.4. — Théorème [9]. *On considère un FCSR de longueur n et d'entier de rétroaction $q = 1 - 2d$ dont le registre principal génère les suites M_i définies ci-dessus. Pour chaque i tel que $0 \leqslant i \leqslant n-1$, il existe un entier p_i tel que la suite M_i soit le développement 2-adique de p_i/q. De plus, les p_i sont reliés par les formules suivantes.*

$$p_i = \begin{cases} qm_i(0) + 2p_{i+1} & \text{si } d_i = 0, \\ q\big(m_i(0) + 2c_i(0)\big) + 2(p_{i+1} + p_0) & \text{si } d_i = 1. \end{cases}$$

ℓ-suites

Parmi les suites générées par les FCSR, celles dont la période est maximale nous intéressent particulièrement, dans le cadre de la génération de pseudo-aléa. Tout d'abord, rappelons une définition bien connue par la communauté étudiant les LFSR.

4.1.5. — Définition. Une *suite à longueur maximale*, ou *m-suite*, est une suite binaire périodique engendrée par un LFSR de polynôme de rétroaction primitif.

Une notion similaire, associée aux FCSR, est la suivante.

4.1.6. — Définition. Une ℓ-suite est une suite périodique $S = (s_t)_{t\in\mathbb{N}}$ de la forme

$$(A2^{-t} \bmod q) \bmod 2$$

où q est un premier impair tel que 2 soit primitif modulo q, et $q \nmid A$.

Les ℓ-suites ont largement été étudiées. On peut trouver un résumé détaillé de leurs propriétés dans [49]. On a en particulier ce résultat concernant la distribution homogène des blocs binaires de longueur fixée, dans la période d'une ℓ-suite :

4.1.7. — Théorème. *Soit $S = (s_t)_{t\in\mathbb{N}}$ une ℓ-suite. Soient p, q tels que la fraction p/q ait pour développement 2-adique la suite S, avec q premier impair. Soit $k \in \mathbb{N}^*$. Le nombre $n(B)$ d'occurrences de chaque bloc binaire B de longueur k dans une période de S vérifie*

$$\left\lfloor \frac{q}{2^k} \right\rfloor \leqslant n(B) \leqslant \left\lfloor \frac{q}{2^k} \right\rfloor + 1.$$

Génération de pseudo-aléa

Les automates FCSR produisent des suites dont les propriétés statistiques sont similaires à celles de suites aléatoires, ce qui en fait de bonnes briques de base pour des générateurs pseudo-aléatoires. Elles se différencient toutefois de suites purement aléatoires par leur complexité 2-adique faible. La section suivante montre que la connaissance de peu de termes d'une suite générée par un FCSR permet de reconstruire le FCSR et donc de déterminer la suite entière. Cette « faiblesse » liée à leur structure, similaire à celle des LFSR employés seuls, devient un atout parce qu'elle permet de prouver certains résultats utiles (le théorème précédent en est un exemple, ceux de la section 4.3 en sont d'autres). Au final, cela nous a permis de définir et étudier la famille de générateurs aléatoires F-FCSR (voir la section 4.5).

4.2. Reconstruction d'un FCSR générant une suite donnée

Dans [64], les auteurs décrivent un algorithme qui permet de déterminer les paramètres d'un FCSR à partir de la suite qu'il génère. Cet algorithme est dérivé de celui de Berlekamp-Massey utilisé pour les LFSR mais adapté aux FCSR à l'aide de méthodes d'approximations p-adiques dues à De Weger et Mahler. Nous avons dans [13] décrit un algorithme alternatif, cette fois basé sur l'algorithme d'Euclide étendu, réalisant la même tâche, mais plus simple à mettre en œuvre.

Utilisation de l'algorithme étendu d'Euclide

La version étendue de l'algorithme d'Euclide calcule le pgcd d de deux entiers positifs a et b et les coefficients de Bézout associés, par les formules suivantes.

$$\begin{cases} r_0 = a \\ u_0 = 1 \\ v_0 = 0 \end{cases} \text{ et } \begin{cases} r_1 = b \\ u_1 = 0 \\ v_1 = 1 \end{cases} \text{ puis, pour } i \geqslant 2, \begin{cases} r_{i+1} = r_{i-1} - q_i r_i \\ u_{i+1} = u_{i-1} - q_i u_i \\ v_{i+1} = v_{i-1} - q_i v_i \end{cases} \text{ (division euclidienne de } r_{i-1} \text{ par } r_i)$$

jusqu'à obtenir un reste r_t nul.

4.2.1. — Proposition. *Avec les notations ci-dessus, on a les propriétés suivantes :*

- *(1) Pour tout* $i \in \{0, \ldots, t\}$, $u_i a + v_i b = r_i$.
- *(2) Pour tout* $i \in \{0, \ldots, t-1\}$, $u_i v_{i+1} - u_{i+1} v_i = (-1)^i$.
- *(3) La suite des* r_i *est positive et strictement décroissante.*
- *(4) On a* $u_i \geqslant 0$ *et* $v_i \leqslant 0$ *pour* i *pair. On a* $u_i \leqslant 0$ *et* $v_i \geqslant 0$ *pour* i *impair.*
- *(5) Les suites des* $|u_i|$ *et des* $|v_i|$ *sont croissantes (à partir du rang 1 pour* $|u_i|$*).*
- *(6) On a* $|u_{i+1} r_i| \leqslant b$ *et* $|v_{i+1} r_i| \leqslant a$*, ainsi que* $|u_i r_{i+1}| \leqslant b$ *et* $|v_i r_{i+1}| \leqslant a$ *pour tout* $i \leqslant t-1$.

En appliquant l'algorithme d'Euclide étendu aux entiers 2^k et à l'entier rationnel S_k obtenu en tronquant un entier 2-adique de la forme p/q (q impair) au rang k de son développement 2-adique, on peut retrouver les entiers p et q. C'est le principe de la reconstruction d'un FCSR à partir de la suite qu'il génère :

Algorithme de reconstruction "EEAapprox"

Entrée : un entier $\Lambda > 0$ et les $k = 2\Lambda + 3$ premiers termes d'une suite binaire S.
Sortie : deux entiers p, q de longueur binaire $\leqslant \Lambda$ tels que p/q soit une approximation de S à l'ordre k ; ou « Erreur » s'il n'existe pas de tels entiers.

$k := 2\Lambda + 3$
$(r_0, u_0, v_0) := (2^k, 1, 0)$
$(r_1, u_1, v_1) := (\sum_{i=0}^{k-1} s_i 2^i, 0, 1)$
TantQue $r_1 > 2^{k/2}$ Faire
    $(s, t) :=$ quotient et restes euclidiens de r_0 divisé par r_1
    $(u_2, v_2) := (u_0 - s u_1, v_0 - s v_1)$
    $(r_0, u_0, v_0) := (r_1, u_1, v_1)$
    $(r_1, u_1, v_1) := (t, u_2, v_2)$
FinTantQue
Si $|v_1| \leqslant 2^{k/2}$ Alors
    Retourner (r_1, v_1) (pour (p, q)).
Sinon
    Retourner « Erreur » (l'envergure 2-adique de S est $> \Lambda$)

La validité de cet algorithme est assurée par le résultat suivant, que nous avons publié dans [13] :

4.2.2. — Théorème. *Soit* S *une suite binaire ultimement périodique non nulle d'envergure 2-adique* Λ*. Alors il est possible de déterminer des entiers* p, q*, avec* q *impair,* $\mathrm{pgcd}(p, q) = 1$ *et* $0 < |p|, |q| < 2^\Lambda$ *en temps* $O(\Lambda^2)$ *en appliquant l'algorithme ci-dessus aux* k *premiers termes de* S *avec* $k = 2\Lambda + 3$.

4.3. FCSR annulaires

Dans la littérature, on trouve deux types de FCSR. Dans le mode « Galois » (décrit ci-dessus), la rétroaction y est représentée par des connexions $m_0 \to m_i$. Dans le mode « Fibonacci », la rétroaction y est représentée par des connexions $m_i \to m_{n-1}$. Les deux constructions sont équivalentes : chaque FCSR en mode Galois peut être remplacé par un FCSR en mode Fibonacci générant la même suite, et réciproquement. Mais en fait, comme nous l'avons détaillé dans [10], ces deux architectures peuvent être vues comme deux cas extrêmes d'un mode plus général et plus souple que nous avons appelé le mode annulaire. De plus, les principales propriétés arithmétiques des FCSR peuvent être reformulées (avec quelques subtilités intéressantes) et démontrées dans ce cadre général. En plus de son intérêt unificateur évident, ce point de vue a eu des retombées pratiques puisqu'il a permis de contrer une attaque sur les générateurs F-FCSR (voir la section 4.5).

Le mode Galois

Étudions d'abord l'évolution du contenu du registre principal d'un FCSR en mode Galois. On part de la formule de la fonction de transition, entre les bits du registre principal et de retenues :

$$m_i(t+1) + 2c_i(t+1) = m_{i+1}(t) + m_0(t) + c_i(t) \tag{4.1}$$

en chaque i où intervient une rétroaction. On désigne par $M_i(t)$ et $C_i(t)$ les suites (identifiées à des entiers 2-adiques) observées à partir de l'instant t, autrement dit

$$M_i(t) = \sum_{k=0}^{\infty} m_i(t+k) \cdot 2^k, \qquad \text{et} \qquad C_i(t) = \sum_{k=0}^{\infty} c_i(t+k) \cdot 2^k. \tag{4.2}$$

En sommant sur k, la formule de transition passe aux suites (l'addition est dans l'anneau $\mathbb{Z}_2$ des entiers 2-adiques) :

$$M_i(t+1) + 2C_i(t+1) = M_{i+1}(t) + M_0(t) + C_i(t).$$

Mais $C_i(t) = c_i(t) + 2C_i(t+1)$, donc la formule se simplifie :

$$M_i(t+1) = M_{i+1}(t) + M_0(t) + c_i(t)$$

en toutes les positions où il y a rétroaction. Là où il n'y a pas de rétroaction, on a tout simplement $M_i(t+1) = M_{i+1}(t)$. En passant aux vecteurs $M(t) = (M_0(t), \ldots, M_{n-1}(t)) \in \mathbb{Z}_2^n$ et $c(t) = (c_0(t), \ldots, c_{n-1}(t))$, on a alors

$$M(t+1) = TM(t) + c(t) \tag{4.3}$$

où T est la matrice compagnon obtenue à partir du d de rétroaction :

$$T = \begin{pmatrix} d_0 & 1 & 0 & \cdots & 0 \\ d_1 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ d_{n-2} & 0 & 0 & \ddots & 1 \\ d_{n-1} & 0 & 0 & \cdots & 0 \end{pmatrix}. \tag{4.4}$$

Le mode annulaire

La matrice compagnon (4.4) (nulle en dehors de la sur-diagonale de 1 et de coefficients dans la colonne gauche) est (un peu abusivement) appelée la matrice de transition du FCSR. Dans le cas d'une architecture Fibonacci, la matrice de transition est nulle en dehors d'une sur-diagonale de 1, et de coefficients dans la dernière ligne. Entre ces deux extrêmes, il est possible d'imaginer une architecture hybride, avec des propriétés similaires, et dont nous avons montré l'intérêt cryptographique.

Dans [10] et [14], nous avons pris en compte des matrices T de forme plus générale. Nous avons considéré le cas d'une matrice T avec une sur-diagonale cyclique (pour garder la structure annulaire de registre à décalage) mais avec des 1 en plus dispersés dans le reste de la matrice.

4.3.1. — Définition. Un *automate 2-adique* est une machine possédant un registre binaire de taille finie n (le registre principal) et un registre de (au plus) n retenues (pas toujours binaires) mis à jour à chaque top d'horloge par une fonction de transition de la forme :

$$\left.\begin{aligned} m_i(t+1) &= T_i m(t) + c_i(t) \bmod 2 \\ c_i(t+1) &= \lfloor (T_i m(t) + c_i(t))/2 \rfloor \end{aligned}\right\} \qquad \text{pour } 0 \leqslant i < n.$$

Cela revient à écrire (puisque le registre principal est binaire) :

$$m_i(t+1) + 2c_i(t+1) = T_i m(t) + c_i(t) \qquad \text{pour } 0 \leqslant i < n. \tag{4.5}$$

La matrice T de taille $n \times n$ dont les lignes sont les T_i sera appelée (abusivement) la *matrice de transition* de l'automate. La fonction de transition s'écrit alors de manière compacte :

$$m(t+1) + 2c(t+1) = Tm(t) + c(t). \tag{4.6}$$

Les trois résultats suivants ont été montrés dans [10][11][14] :

4.3.2. — Théorème. *Les entiers 2-adiques $M_i(t)$ correspondant aux suites observées dans les cellules du registre principal et définis par (4.2) vérifient encore la relation (4.3).*

4.3.3. — Théorème. *La suite $M_i = (m_i(t))_{t\in\mathbb{N}}$ observée dans chaque cellule du registre principal (pour $0 \leqslant i \leqslant n-1$) est le développement d'un entier 2-adique de la forme p_i^*/q où $q = \det(I - 2T)$.*

Comme dans les modes Galois et Fibonacci, bien que de façon plus subtile, on observe encore une division par 2 du contenu algébrique lors de chaque transition :

4.3.4. — Théorème. On pose

$$p(t) = m(t) + 2c(t) \qquad \text{et} \qquad p^*(t) = -(2T - I)^* p(t).$$

Alors, pour tout $t \in \mathbb{N}$, on a $p^*(t) \equiv 2p^*(t+1)$ modulo q.

Les FCSR construits sur ce modèle annulaire ont des avantages sur les constructions classiques Fibonacci et Galois, que nous avons exploités dans l'ultime version des générateurs F-FCSR (section 4.5). Outre le fait de contrer l'attaque décrite dans [52], la souplesse de la nouvelle représentation permet de les implémenter avec des circuits électroniques ayant de meilleures caractéristiques (temps de transition, lissage des variations de courant, résistance aux attaques par canaux cachés, meilleure diffusion des différences…), comme cela a aussi été détaillé dans [14].

FCSR semblables

Enfin, la notion de FCSR semblables est utile pour les classifier.

4.3.5. — Définition. Soient deux automates 2-adiques de matrices de transition respectives (celles intervenant dans (4.6)) T et T'. On dit que les deux automates sont *semblables* si il existe une matrice P à coefficients entiers et de déterminant ± 1 telle que $T' = PTP^{-1}$.

4.3.6. — Proposition. *On a $M'(t) = PM(t)$ et $Pc(t)$ qui vérifient (4.3). On a $A' = PAP^{-1}$ et $A'^* = PA^*P^{-1}$. On a aussi $p'(t) = Pp(t)$ et $p'^*(t) = Pp^*(t)$.*

4.4. Machines 2-adiques

Cette section se rapporte aussi à l'article [14]. Nous avons souhaité englober les résultats sur les FCSR annulaires dans une théorie encore plus large.

4.4.1. — Définition. Une *machine 2-adique*, avec un vecteur d'entrée u de taille k bits et un vecteur de sortie b de taille ℓ bits est une machine à états (avec un ensemble d'états non nécessairement fini) telle que
• Les états sont composés de deux parties : le *contenu* $m \in \{0,1\}^n$ *du registre principal*, et le *contenu* $c \in \mathbb{Z}_2^n$ *du registre de retenues*.
• La fonction de transition est déterminée par deux matrices A et X à entrées dans $\mathbb{Z}_2$ et de tailles respectives $n \times n$ et $n \times k$ et son expression est

$$\begin{cases} z(t) = Am(t) + c(t) + Xu(t), \\ m(t+1) = z(t) \bmod 2, \\ c(t+1) = z(t) \operatorname{div} 2. \end{cases}$$

• La fonction de sortie est spécifiée par une matrice Y de taille $\ell \times n$:

$$v(t) = Ym(t).$$

Pour $1 \leqslant i \leqslant n$ nous notons $M_i(t)$ and $C_i(t)$ les entiers 2-adiques développés par les cellules de l'automate à partir de l'instant t :

$$M_i(t) = \sum_{s=0}^{\infty} m_i(t+s) \cdot 2^s \qquad \text{et} \qquad C_i(t) = \sum_{s=0}^{\infty} c_i(t+s) \cdot 2^s \tag{4.7}$$

et, pour $1 \leqslant i \leqslant k$

$$U_i(t) = \sum_{s=0}^{\infty} u_i(t+s) \cdot 2^s$$

les entiers 2-adiques soumis en entrée. On note de plus $M = (M_1, \ldots, M_n)$, $C = (C_1, \ldots, C_n)$ and $U = (U_1, \ldots, U_k)$ les vecteurs correspondants. On montre alors que la relation suivante est vérifiée :

$$M(t+1) = AM(t) + c(t) + XU(t). \tag{4.8}$$

Lorsque l'entrée $XU(t)$ est nulle, les entiers 2-adiques $M_i(t)$ s'écrivent $p_i^*(t)/q$ où $p_i^*(t) \in \mathbb{Z}_2$ et $q = \det(I - 2A)$ est un entier 2-adique impair. Plus précisément, le vecteur $p^*(t) = (p_1^*(t), \ldots, p_n^*(t))^t$ est égal à $(I-2A)^*\big(m(t)+2c(t)\big)$. (Ici, $*$ désigne la matrice adjointe.) Enfin, on peut encore montrer que le vecteur p^* subit une division par 2 modulo q à chaque transition :

$$2p^*(t+1) \equiv p^*(t) \pmod{q}.$$

Dans le cas général (avec une entrée non nulle), on peut exprimer le vecteur 2-adique de la sortie en fonction de celui de l'entrée :

$$V(t) = Y(I-2A)^{-1}\big(m(t)+2c(t)\big) + 2Y(I-2A)^{-1}XU(t).$$

Machines équivalentes

La notion de FCSR semblables s'étend aux machines 2-adiques, avec des propriétés intéressantes.

4.4.2. — Définition. On dit que deux machines 2-adiques $\mathcal{M}$ et $\mathcal{M}'$ sont semblables lorsque il existe une matrice inversible P à coefficients dans $\mathbb{Z}_2$, telle que

$$A' = P^{-1}AP, \qquad X' = P^{-1}X, \qquad Y' = YP.$$

Nous avons alors montré que, si les contenus des registres des deux machines à l'instant 0 satisfait $m(0) + 2c(0) = P\big(m'(0) + 2c'(0)\big)$, et si les deux entrées sont égales $U = U'$, alors
• Les deux machines ont même rétroaction : $\det(I - 2A) = \det(I - 2A')$.
• Les deux vecteurs d'entiers 2-adiques développés par les deux registres principaux vérifient $M(0) = PM'(0)$.
• Les vecteurs de sortie vérifient $V(0) = PV'(0)$.

Mémoire requise pour l'implantation

La conception d'automates de chiffrement à flot correspondant à différentes classes appartenant à ce même cadre global est longuement détaillée dans [14]. On y étudie aussi la taille mémoire nécessaire pour que ces machines fonctionnent, en dégageant en particulier les cas où cette taille reste bornée.

4.5. F-FCSR

L'objectif que nous avons visé était de définir un algorithme de chiffrement symétrique rapide, aisément implantable en *hardware* (mais aussi intéressant en *software*). Il s'agit d'un algorithme de chiffrement *à flot* où une suite $S = (s_t)_{t\in\mathbb{N}}$ chiffrante binaire pseudo-aléatoire est générée. Cette suite permet de chiffrer un message clair formé d'un train binaire $X = (x_t)_{0\leqslant t<N}$ par masquage : le chiffré $Y = (y_t)_{0\leqslant t<N}$ est défini par $y_t = x_t \oplus s_t$ (pour $0 \leqslant t < N$). L'opération de déchiffrement est identique à celle du chiffrement : $x_t = y_t \oplus s_t$.

Le cœur des générateurs de type F-FCSR (pour FCSR filtré) que nous avons proposés dans [9] est un automate FCSR. Nous notons q son entier de rétroaction, et n la longueur du registre principal.

La suite filtrante est obtenue en utilisant un filtre linéaire, entre différentes suites générées par le registre principal. Un tel filtre est défini par un entier $F = \sum_{i=0}^{n-1} f_i 2^i$ où $f_i = 1$ lorsque la suite M_i est sélectionnée pour participer à la génération de la suite chiffrante, et $f_i = 0$ sinon. Cela suffit pour masquer la structure 2-adique du FCSR. La suite chiffrante $S = (s_t)_{t\in\mathbb{N}}$ générée par F-FCSR est donc définie par

$$s_t = \sum_{i=0}^{n-1} f_i m_i(t).$$

Pour les générateurs F-FCSR, nous avons en fait simplement choisi $F = d = (|q| + 1)/2$. D'autre part, pour le choix de q et d nous avons recommandé :

- q est un nombre premier (négatif).
- L'ordre de 2 modulo q est $|q| - 1$.
- $(|q| - 1)/2$ est premier.
- Le poids de Hamming de d est environ $n/2$.

F-FCSR-H

L'entier $|q|$ que nous avons choisi pour la proposition F-FCSR-H à eSTREAM [38] est un entier de 161 bits :

$$q = -199352459131827501532804161134421503646014008796 3$$

pour obtenir un FCSR de longueur $n = 160$. Le poids de Hamming de $d = (|q| + 1)/2$ est 83, donc le registre de retenues comporte 82 cellules. Le filtre proposé est alors $F = d$ qui s'écrit, en hexadécimal,

$$F = (\text{ae985dff 26619fc5 8623dc8a af46d590 3dd4254e})_{16}.$$

Ce filtre se décompose en 8 sous-filtres (le sous-filtre j est obtenu en sélectionnant le bit j dans chaque octet de F) :

$$\begin{aligned}
F_0 &= (0011\ 0111\ 0100\ 1010\ 1010)_2, & F_4 &= (0111\ 0010\ 0010\ 0011\ 1100)_2,\\
F_1 &= (1001\ 1010\ 1101\ 1100\ 0001)_2, & F_5 &= (1001\ 1100\ 0100\ 1000\ 1010)_2,\\
F_2 &= (1011\ 1011\ 1010\ 1110\ 1111)_2, & F_6 &= (0011\ 0101\ 0010\ 0110\ 0101)_2,\\
F_3 &= (1111\ 0010\ 0011\ 1000\ 1001)_2, & F_7 &= (1101\ 0011\ 1011\ 1011\ 0100)_2.
\end{aligned}$$

Cela permet de générer 8 bits pseudo-aléatoires à chaque transition de l'automate FCSR. Précisément, le bit b_i extrait (avec $0 \leqslant i \leqslant 7$) est exprimé par

$$b_i = \bigoplus_{j=0}^{19} f_i^{(j)} m_{8j+i} \qquad \text{avec } F_i = \sum_{j=0}^{19} f_i^{(j)} 2^j.$$

Initialisation du générateur

La méthode utilisée pour initialiser le générateur F-FCSR-H avec la clé et l'IV est la suivante. La clé K est de longueur $k = 80$ bits et l'IV de longueur $v = 80$ bits aussi.
(1) Initialiser le registre principal avec la clé et l'IV :

$$M := K + 2^{80} \cdot IV = (0^{80-v} \| \mathrm{IV} \| K).$$

(2) Initialiser à 0 le registre de retenues :

$$C := 0 = (0^{82}).$$

(3) Obtenir 20 octets d'initialisation en itérant (pour $0 \leqslant i \leqslant 19$) les deux opérations : appliquer la fonction de transition au FCSR et utiliser le filtre pour obtenir un octet S_i.
(4) Réinitialiser le registre principal à l'aide de ces 20 octets :

$$M := \sum_{i=0}^{19} S_i = (S_{19} \| \cdots \| S_1 \| S_0).$$

(5) Appliquer 162 fois la fonction de transition à l'automate (ne pas extraire de suite chiffrante durant cette étape).

L'automate est alors prêt pour générer la suite chiffrante : un nouvel octet sera généré à chaque nouvelle transition.

Sélection eSTREAM

L'algorithme F-FCSR-H a figuré parmi les quatre candidats retenus en 2008 par le projet européen eSTREAM [38], comme algorithme de chiffrement *hardware*. Il a toutefois fait l'objet d'une attaque [52] ultérieurement. Cette attaque sera finalement contrée par l'utilisation d'automates en mode annulaire, qui sont décrits dans la section 4.3.

Chapitre 5

Information quantique

Mon domaine de recherche le plus récent porte sur la théorie de l'information quantique. Ce domaine se propose d'utiliser les mathématiques discrètes pour sonder et exploiter les étrangetés du monde quantique. Les cryptographes peuvent être amenés à s'intéresser aux lois de la mécanique quantique pour au moins trois raisons. (a) Ces lois ont ouvert la voie à des algorithmes cryptographiques et des protocoles spécifiquement quantiques, dont la sécurité repose sur des postulats physiques. (b) Elles ouvrent une voie vers une nouvelle classe d'algorithmes qui contient des méthodes rapides de factorisation et de logarithme discret (dues à Shor [85]), et qui rendront obsolètes les protocoles à clés publiques reposant sur ces deux problèmes algorithmiques si des ordinateurs quantiques sont construits un jour. (c) Alors que la génération d'aléa vrai est seulement approchable par les méthodes déterministes, la mécanique quantique semble donner à l'aléa une existence fondamentale.

La section 5.1 expose l'incompatibilité entre le réalisme local et le formalisme quantique, en s'appuyant sur les inégalités de Bell dues à Clauser, Horne, Shimony, Holt (CHSH). La section 5.2 présente les inégalités de Bell obtenues pour n parties dans le cas dichotomique par Werner & Wolf [89] et Żukowski & Brukner [92]. La section 5.3 présente les inégalités de Bell homogènes que j'ai publiées dans [4]. La section 5.4 présente un travail en cours [2], utilisant les inégalités homogènes pour améliorer un protocole d'échange de clés.

5.1. Réalisme local et inégalités CHSH

Les inégalités de Bell sont des outils qui mettent en évidence l'incompatibilité entre la description classique du monde physique et sa description quantique. Cette incompatibilité est matérialisée par le phénomène d'*intrication* prévu par la mécanique quantique (et observé par l'expérience). Lorsque plusieurs particules sont intriquées, les issues de mesures sur ces différentes particules sont corrélées d'une façon que les lois de la physique classique ne peuvent expliquer. Les lois classiques sont conformes en particulier au cadre du *réalisme local*.

Le réalisme local

On considère un système physique, constitué de plusieurs parties (spatialement séparées), notées $\mathcal{A}$, $\mathcal{B}$, $\mathcal{C}\ldots$ Pour chacune des parties, un expérimentateur (Alice, Bob, Claude...) est susceptible de faire une mesure de son choix. Les lois classiques incluent les deux principes suivants, que l'on regroupe sous le terme de réalisme local.

(1) Le réalisme (ou objectivité). Chaque mesure ne fait que révéler une grandeur qui existe indépendamment de son observation.

(2) Le principe de l'action locale. L'action de chaque expérimentateur n'influence aucunement les grandeurs mesurées par les expérimentateurs distants.

La conjonction de ces deux hypothèses est couramment désignée sous le terme de *Réalisme Local*. Les *inégalités de Bell* sont des inégalités qui sont satisfaites si le système admet une description réaliste locale, et qui sont violées pour certains systèmes quantiques. Probablement, les inégalités de Bell les plus simples et les plus éclairantes sont celles, couramment appelées CHSH (pour Clauser/Horne/Shimony/Holt), formulées dans [30].

Les inégalités CHSH

Alice et Bob réalisent des expériences sur un système constitué de deux parties distantes $\mathcal{A}$ et $\mathcal{B}$. Alice a le choix entre deux mesures X_A et Z_A sur $\mathcal{A}$, et Bob a le choix entre deux mesures X_B et Z_B sur $\mathcal{B}$. Les mesures X_A, Z_A, X_B et Z_B sont dichotomiques : leurs issues sont ± 1. Dans le cadre réaliste local, la quantité

$$T := X_A X_B + X_A Z_B + Z_A X_B - Z_A Z_B$$

est parfaitement définie. On voit facilement qu'elle ne peut prendre que les valeurs ± 2. Pour plusieurs échantillons préparés de façon identique, son espérance vérifie donc

$$-2 \leqslant E(T) \leqslant 2. \tag{5.1}$$

Ce sont les inégalités CHSH. Si on veut obtenir $E(T)$ expérimentalement (à partir d'un échantillon formé d'un grand nombre de systèmes identiquement préparés) on prendra soin de ne faire qu'une seule mesure sur chaque partie, puisque la deuxième mesure pourrait être faussée. Ainsi $E(T)$ est évalué sous la forme $E(X_A X_B) + E(X_A Z_B) + E(Z_A X_B) - E(Z_A Z_B)$, en divisant l'échantillon en quatre sous-échantillons.

Le cadre quantique

Dans un cadre quantique, considérons deux particules de spin 1/2 dans l'état habituellement noté $|\psi\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$. Ce système est dit *intriqué* puisque des corrélations sont observées entre le résultat des mesures effectués par Alice sur la première particule et de celles effectués par Bob sur la deuxième particule (bien que les deux particules soient distantes l'une de l'autre). Plus précisément, pour cet état $|\psi\rangle$, si Alice mesure le sens du spin de la première particule dans une direction donnée (c'est une mesure dont l'issue est ± 1) et si Bob mesure le sens du spin de la deuxième particule dans la même direction, alors les issues obtenues par Alice et Bob sont nécessairement opposées.

Plus généralement, le formalisme quantique montre que si Alice et Bob mesurent les spins de leurs particules respectives dans les directions portées par les vecteurs unitaires respectifs $\overrightarrow{a}$ et $\overrightarrow{b}$, alors la corrélation entre les deux spins est donnée par $E(S_{\overrightarrow{a}} S_{\overrightarrow{b}}) = -\overrightarrow{a} \cdot \overrightarrow{b}$. Pour la configuration de la figure 5.1, on a

$$E(T) = -\overrightarrow{a}_1 \cdot \overrightarrow{b}_1 - \overrightarrow{a}_1 \cdot \overrightarrow{b}_2 - \overrightarrow{a}_2 \cdot \overrightarrow{b}_1 + \overrightarrow{a}_2 \cdot \overrightarrow{b}_2 = -\sqrt{2}/2 - \sqrt{2}/2 - \sqrt{2}/2 - \sqrt{2}/2 = -2\sqrt{2}. \tag{5.2}$$

La valeur de $E(T)$ obtenue dans ce cadre sort donc de l'intervalle $[-2, 2]$ autorisé par le cadre classique. Le cadre quantique et le cadre réaliste local sont **incompatibles**. Les expériences réalisées pour déterminer à quel cadre se conformait la nature ont toutes confirmé le cadre quantique, au détriment du cadre classique (même si certains relèvent la possibilité de failles dans la démarche expérimentale).

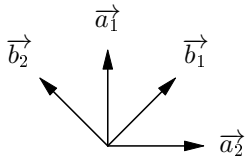

Figure 5.1. Les directions des mesures de spin choisies par Alice et Bob

Jeu complet d'inégalités

En permutant les parties et/ou les mesures dans les deux inégalités CHSH, on obtient huit inégalités qui, comme cela a été montré dans [41], forment un jeu *complet*. Cela signifie que les corrélations observées peuvent être simulées par un modèle réaliste local si et seulement si les huit inégalités sont toutes vérifiées.

5.2. Généralisation à n parties

Les auteurs des deux articles [89] et [92] ont obtenu une généralisation de ce jeu complet au cas de n-parties (toujours avec deux mesures dichotomiques X_i et Z_i pour chacune d'elles). Les inégalités qu'ils ont obtenues s'expriment à l'aide de la transformée de Walsh-Hadamard $\hat{f}$ des fonctions booléennes :

La transformée de Walsh-Hadamard

Nous notons $\mathcal{F}_n$ l'ensemble des fonctions de $\{0,1\}^n$ dans $\mathbb{R}$. Cet ensemble contient celui des « fonctions booléennes en notation multiplicative », c'est-à-dire celles qui prennent leurs valeurs dans ± 1, qui nous intéressera plus particulièrement. Pour $f \in \mathcal{F}_n$, la fonction $\hat{f} \in \mathcal{F}_n$ définie par

$$\hat{f}(r) = \sum_{s\in\{0,1\}^n} (-1)^{r\cdot s} f(s) \qquad (\text{où } r\cdot s = \textstyle\sum_{i=1}^n r_i s_i)$$

est appelée la *transformée de Walsh-Hadamard* de f. On peut retrouver la fonction f à partir de sa transformée $\hat{f}$ par la *transformée de Walsh-Hadamard inverse* :

$$f(s) = \frac{1}{2^n}\langle \hat{f}, \ell_s\rangle = \frac{1}{2^n}\sum_{r\in\{0,1\}^n} (-1)^{r\cdot s}\hat{f}(r).$$

Le polytope du réalisme local

Les inégalités de Bell obtenues par Werner & Wolf et Żukowski & Brukner s'écrivent :

$$\sum_{s\in\{0,1\}^n} \hat{f}(s)E(M_s) \leqslant 2^n \qquad \text{où } M_s = \textstyle\prod_{i=1}^n X_i Z_i^{1-s_i}. \tag{5.3}$$

Il y en a donc 2^{2^n} (dont certaines sont triviales) et elles définissent un polytope Ω dans $\mathbb{R}^{2^n}$. Les inégalités obtenues forment un système complet : le vecteur formé des espérances $E(M_s)$ (pour $s \in \{0,1\}^n$) appartient au polytope Ω si et seulement si ces espérances peuvent être obtenues dans un cadre réaliste local.

Illustration pour $n = 2$

Voici les tables de vérités des 16 fonctions booléennes à deux variables et de leurs transformées de Walsh-Hadamard.

xy	f_0	f_1	f_2	f_3	f_4	f_5	f_6	f_7	f_8	f_9	f_{10}	f_{11}	f_{12}	f_{13}	f_{14}	f_{15}
00	1	1	1	1	1	1	1	1	−1	−1	−1	−1	−1	−1	−1	−1
01	1	1	1	1	−1	−1	−1	−1	1	1	1	1	−1	−1	−1	−1
10	1	1	−1	−1	1	1	−1	−1	1	1	−1	−1	1	1	−1	−1
11	1	−1	1	−1	1	−1	1	−1	1	−1	1	−1	1	−1	1	−1
xy	$\hat{f}_0$	$\hat{f}_1$	$\hat{f}_2$	$\hat{f}_3$	$\hat{f}_4$	$\hat{f}_5$	$\hat{f}_6$	$\hat{f}_7$	$\hat{f}_8$	$\hat{f}_9$	$\hat{f}_{10}$	$\hat{f}_{11}$	$\hat{f}_{12}$	$\hat{f}_{13}$	$\hat{f}_{14}$	$\hat{f}_{15}$
00	4	2	2	0	2	0	0	−2	2	0	0	−2	0	−2	−2	−4
01	0	2	−2	0	2	4	0	2	−2	0	−4	−2	0	2	−2	0
10	0	2	2	4	−2	0	0	2	−2	0	0	2	−4	−2	−2	0
11	0	−2	2	0	2	0	4	2	−2	−4	0	−2	0	−2	2	0

Ces transformées de Fourier permettent de retrouver les huit inégalités CHSH en utilisant la formulation (5.3), ainsi que huit inégalités triviales (par exemple $4E(X_A X_B) \leqslant 4$).

5.3. Les inégalités multidimensionnelles

Les inégalités de Bell décrites ci-dessus ont été obtenues en considérant des mesures dichotomiques. Les mesures dichotomiques non dégénérées sont décrites, en mécanique quantique, par des opérateurs sur un espace de Hilbert de dimension 2. Ces opérateurs agissent sur un vecteur d'état qui décrit un système quantique élémentaire nommé *qubit*. Les qubits sont une sorte d'équivalent quantique du bit classique.

Le cas multidimensionnel correspond aux mesures à d issues possibles avec $d \geqslant 2$. Les mesures sont décrits par des opérateurs sur un espace de Hilbert de dimension d. Un tel état est souvent appelé un *qudit*.

L'utilisation de qudits peut présenter des avantages par rapport à celle de qubits. En particulier, les inégalités de Bell faisant intervenir des qutrits ($d = 3$) sont plus « résistantes au bruit » ce qui signifie que

les expériences visant à tester le réalisme local peuvent être plus fiables. Les qudits permettent aussi de fabriquer des protocoles cryptographiques plus robustes. Enfin, les différentes formes d'intrication quantique restent imparfaitement étudiées, et il est vraisemblable que le cas des qudits ne peut pas toujours se ramener à celui des qubits.

Certaines inégalités de Bell avait été obtenues pour le cas multidimensionnel ($d \geqslant 3$). Mais les efforts pour obtenir un jeu complet étaient restés vains. Nous avons obtenu un tel jeu complet, directement inspiré du cas $d = 2$, et qui partage avec lui la même élégance. Les inégalités que nous avons obtenues s'expriment à l'aide de la transformée de Fourier discrète.

La transformée de Fourier discrète

La transformée de Fourier discrète multidimensionnelle généralise simplement la transformée de Walsh-Hadamard. On note $d \geqslant 2$ le « nombre de points » ($d = 2$ dans le cas de la transformée de Walsh-Hadamard). Les fonctions booléennes sont remplacées par les fonctions de $\mathbb{Z}_d^n$ dans l'ensemble des $\mathcal{U}$ des racines complexes d-ièmes de l'unité. Il y a d^{d^n} telles fonctions. Nous notons $\mathcal{F}_{n,d}$ l'ensemble des fonctions de $\mathbb{Z}_d^n$ dans $\mathbb{C}$, et ω une racine primitive complexe d-ième de l'unité.

La transformée de Fourier discrète de $f \in \mathcal{F}_{n,d}$ est définie par

$$\hat{f}(r) = \sum_{s \in \mathbb{Z}_d^n} \omega^{r \cdot s} f(s).$$

On obtient les valeurs de la fonction $\hat{f}$ en appliquant la matrice $H_d^{\otimes n} = \left(\omega^{r \cdot s}\right)_{r,s \in \mathbb{Z}_d^n}$ au vecteur colonne des valeurs de f. Autrement dit, la transformée de Fourier peut-être vue comme un endomorphisme de l'espace vectoriel $\mathcal{F}_{n,d}$, de matrice $H^{\otimes n}$. Soit $H_d^{*\otimes n}$ la matrice $(\omega^{-r \cdot s})_{r,s \in \mathbb{Z}_d^n}$. On vérifie que $H_d^{\otimes n} H_d^{*\otimes n} = d^n I$. Donc, on peut retrouver f à partir de $\hat{f}$:

$$f(s) = \frac{1}{d^n} \sum_{r \in \mathbb{Z}_d^n} \omega^{-r \cdot s} \hat{f}(r).$$

Les inégalités homogènes

On considère ici un système physique à n parties. Pour chaque partie i, deux mesures X_i et Z_i sont envisagées. Ces mesures ont chacune $d \geqslant 2$ issues possibles, et nous supposons (sans perdre en généralité) que ces issues sont les puissances de ω.

Notons $\operatorname{Hull} \mathcal{U}$ l'enveloppe convexe de l'ensemble $\mathcal{U}$ des racines d-ièmes de l'unité. Dans [4] nous avons obtenu, dans le cadre réaliste local, les conditions suivantes :

$$\sum_{r \in \mathbb{Z}_d^n} \hat{f}(r)\, E\Big(\prod_{i=1}^{n} X_i^{r_i} Z_i^{d-1-r_i} \Big) \in d^n \cdot \operatorname{Hull} \mathcal{U},$$

où X_i et Z_i sont les deux mesures associées à la partie i et où f désigne n'importe quelle fonction de $\mathbb{Z}_d^n$ dans $\mathcal{U}$. Ces conditions se traduisent en termes d'inégalités :

$$\operatorname{Re}\left(\frac{\exp(i\pi/d)}{\cos(\pi/d)} \sum_{r \in \mathbb{Z}_d^n} \hat{f}(r)\, E\Big(\prod_{i=1}^{n} X_i^{r_i} Z_i^{d-1-r_i} \Big) \right) \leqslant d^n \tag{5.4}$$

Nous nommons ces inégalités, inégalités de Bell homogènes (puisqu'elles sont associées aux polynômes homogènes $\mathcal{P}_f$ définis juste ci-après). Ces d^{d^n} inégalités définissent un polytope dans $\mathbb{C}^{d^n}$.

Notons que, dans le cas spécial $d = 2$, on retrouve exactement les inégalités et le polytope obtenus par Werner & Wolf et Żukowski & Brukner. Le fait que ce dernier polytope puisse être défini dans un espace réel étant lié au fait que l'enveloppe convexe des racines carrées de l'unité est contenue dans $\mathbb{R}$.

Nous nommons polynômes de Bell homogènes les polynômes

$$\mathcal{P}_f = \sum_{r\in\mathbb{Z}_d^n} \hat{f}(r) M_r \qquad \text{où } M_r := \prod_{i=1}^{n} X_i^{d-1-r_i} Z_i^{r_i}.$$

Remarquons que les polynômes $\mathcal{P}_f$ peuvent être définis récursivement : si $\mathcal{Q}_0,\ldots,\mathcal{Q}_{d-1}$ sont des polynômes de Bell homogènes en les $2(n-1)$ variables X_i, Z_i (avec $1 \leqslant i \leqslant n-1$), alors on obtient un polynôme de Bell homogène en $2n$ variables par l'opération à d arguments notée ici $\bowtie$:

$$\mathcal{Q}_0 \bowtie \cdots \bowtie \mathcal{Q}_{d-1} := \sum_{r_n=0}^{d-1} \left(\sum_{t=0}^{d-1} \omega^{r_n t} \mathcal{Q}_t \right) X_n^{d-1-r_n} Z_n^{r_n}.$$

De plus, tout polynôme de Bell homogène en les $2n$ variables X_i et Z_i (pour $1 \leqslant i \leqslant n$) peut être obtenu par cette méthode.

Le domaine réaliste local

Les espérances $E(M_s)$, pour $s \in \mathbb{Z}_d^n$, forment un vecteur de $\mathbb{C}^{d^n}$. Le domaine Ω réaliste local est la partie de $\mathbb{C}^{d^n}$ qui est accessible par ce vecteur avec la contrainte du réalisme local. Nous avons montré que ce domaine est le polytope défini par les inégalités de Bell homogènes.

Pour cela, nous avons utilisé le fait que la transformée de Fourier considérée ci-dessus, en plus d'être un endomorphisme de $\mathbb{C}^{d^n}$, est une similitude. On en déduit [4] alors la proposition suivante :

5.3.1. — Proposition. *Soit Γ un polytope de $\mathbb{C}^{d^n}$ contenant l'origine. On note $\widehat{\Gamma}$ son image par DFT (c'est aussi un polytope, par linéarité de DFT). On a alors la relation suivante entre leurs polytopes duaux :*

$$\widehat{\Gamma^\circ} = d^n\, \widehat{\Gamma}^\circ.$$

Considérons le polytope Π de $\mathbb{C}^{d^n}$, dont les sommets sont les $u\pi$ où u décrit $\mathcal{U}$ et π décrit la base canonique de $\mathbb{C}^{d^n}$. Grâce à la proposition 5.3.1, on montre que le polytope dual de Ω est obtenu à l'aide du dual de Π et de la transformée de Fourier :

$$\Omega^\circ = \frac{1}{d^n} \widehat{\Pi^\circ}.$$

Au final, nous avons montré dans [4] que les facettes du polytope Ω sont exactement celles définies par les inégalités (5.4). Nos d^{d^n} inégalités forment donc un jeu complet.

Violation

Les inégalités de Bell permettent de cerner le domaine accessible aux modèles réalistes locaux. C'est ce que font les inégalités que nous avons découvertes. Cependant, les premières inégalités de Bell ont été historiquement introduites afin de montrer que la mécanique quantique ne rentrait pas dans ce cadre. Il est naturel de chercher à savoir si la mécanique quantique viole aussi nos inégalités.

Il y a une difficulté qui apparaît pour $d \geqslant 3$. Les inégalités obtenues contiennent des monômes ou les deux mesures X_i et Z_i associées à une même partie apparaissent. Or, en mécanique quantique, deux telles mesures sont en général incompatibles et ne peuvent être obtenues simultanément.

Nous avons contourné ce problème en utilisant des opérateurs de mesure unitaires, au lieu des opérateurs hermitiens habituellement préférés dans la littérature. Cela est en cohérence avec l'esprit de notre démarche, dans laquelle nos opérateurs sont supposés avoir des valeurs propres dans $\mathcal{U}$ (ces valeurs propres sont les issues des mesures), au lieu d'avoir des valeurs propres réelles comme cela est habituellement supposé. En utilisant des opérateurs de mesure unitaires, leur produit est lui-même un opérateur unitaire et peut être considéré comme une troisième mesure. Les opérateurs unitaires que nous avons choisis pour nos calculs sont bien connus en théorie de l'information quantique, sous le nom d'opérateurs de Pauli (ou de spin) généralisés. Il sont représentés par les produits

$$Z,\ X,\ XZ,\ \ldots,\ XZ^{d-1} \tag{5.5}$$

où X et Z sont les matrices

$$X = \begin{pmatrix} 0 & 0 & \cdots & 1 \\ 1 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 1 & 0 \end{pmatrix} \qquad \text{et} \qquad Z = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & \omega & \ddots & 0 \\ \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & \cdots & \omega^{d-1} \end{pmatrix}.$$

Dans ce cadre, il est possible de calculer la violation de nos inégalités par la mécanique quantique. Cette démarche soulève le problème de l'interprétation physique de cette troisième mesure par rapport aux deux autres (son issue ne peut/doit pas être interprétée comme le produit des issues des deux autres). Malgré le manque de consensus sur cette interprétation, il est remarquable que les facteurs de violation que nous avons calculés sont en principe testables expérimentalement et que, dans les cas particuliers où les produits d'observables incompatibles disparaissent (voir la fin de cette section), nous retrouvons des facteurs de violation qui étaient déjà connus.

Le cas $d = 3$

Dans ce cas, on peut écrire les inégalités homogènes de Bell sous la forme

$$-2\,\mathrm{Re}\Big(\sum_{r\in\mathbb{Z}_3^n} \hat{f}(r) E(X_1^{2-r_1} Z_1^{r_1} X_2^{2-r_2} Z_2^{r_2} X_3^{2-r_3} Z_3^{r_3})\Big) \leqslant 3^n.$$

Nous avons utilisé `Magma` pour lister les polynômes homogènes de Bell, et calculer des facteurs de violation pour de petites valeurs du nombre de parties n. Pour $n = 1$, il y a déjà 27 polynômes homogènes de Bell, qui peuvent être listés sous forme compacte par la formule

$$u\big(3M + (v-1)(X^2 + XZ + Z^2)\big) \tag{5.6}$$

où $u, v \in \{1, \omega, \omega^2\}$ et $M \in \{X^2, XZ, Z^2\}$.

Pour $n = 2$, il y a 19683 polynômes homogènes de Bell. Le plus grand facteur de violation obtenu est 3 avec, par exemple, le polynôme de Bell

$$3\Big((\omega^2-1)X_1^2 X_2 Z_2 + (\omega^2-1)X_1 Z_1 X_2^2 + (1-\omega)Z_1^2 Z_2^2\Big)$$

obtenu en choisissant la fonction f définie par

$$f(1,2) = f(2,1) = f(2,2) = 1, \quad f(0,1) = f(1,0) = f(1,1) = \omega, \quad f(0,0) = f(0,2) = f(2,0) = \omega^2.$$

Lien avec d'autres inégalités

Dans le cas $d = 3$, on trouve un certain nombre d'inégalités de Bell dans la littérature. L'une des plus connue [28] est nommée « CHSH pour les qutrits » (ou CHSH-3). En conservant nos notations, on peut l'écrire sous la forme

$$S \leqslant 2 \tag{5.7}$$

avec

$$S = \mathrm{Re}\big(E(X_1X_2) + E(X_1Z_2) - E(Z_1X_2) + E(Z_1Z_2)\big) + \frac{1}{\sqrt{3}}\,\mathrm{Im}\big(E(X_1X_2) - E(X_1Z_2) - E(Z_1X_2) + E(Z_1Z_2)\big).$$

Nous montrons dans [4] que cette inégalité peut être exactement obtenue en sommant deux de nos inégalités homogènes. Dans cette somme, les termes contenant des mesures incompatibles se neutralisent. La violation de l'inégalité CHSH-3 peut alors s'interpréter comme résultant des violations de deux de nos inégalités. Cela éclaire par exemple la constatation jugée auparavant surprenante selon laquelle la violation maximale de CHSH-3 est observée pour des états quantique qui ne sont pas « maximalement intriqués ». En fait chacune des deux inégalités homogènes concernées est bien maximalement violée par un état maximalement intriqué, mais pas par le même. La violation maximale de la somme est alors obtenue par un état qui réalise un compromis entre deux états maximalement intriqués.

5.4. Échanges quantiques de clés

La cryptographie quantique exploite les propriétés quantiques pour obtenir des protocoles de communication dont la sécurité repose sur des postulats physiques. Les deux protocoles les plus connus sont des protocoles d'échange de clés, dans lesquels deux parties Alice et Bob utilisent un canal quantique pour obtenir une clé secrète partagée. Les postulats de la physique quantique impliquent que toute écoute du canal quantique par un attaquant peut être détectée. Ces deux protocoles sont ceux de Bennett & Brassard [17] et de Ekert [40]. Nous nous sommes intéressés au protocole d'Ekert et à ses variantes.

Le protocole Ekert'91

Alice et Bob utilisent une source de paires de qubits intriqués, disons dans l'état $(|01\rangle - |10\rangle)/\sqrt{2}$. Dans le protocole original [40], Alice et Bob utilisent chacun trois bases de mesure. Je préfère attribuer à chaque partie 4 bases de mesure, notées A_k et B_k ($0 \leqslant k \leqslant 3$), qui correspondent à des mesures de spin dans des directions repérées par les angles $k\pi/4$ (cela correspond à la configuration de la figure 5.1).

Alice et Bob choisissent chacun indépendamment, et pour chaque paire reçue, une base de mesure. Notons A_a et B_b les bases choisies. Les (mesures des) paires pour lesquelles $a = b$ sont retenues pour former les bits de clé, puisque les résultats des mesures obtenus par Alice et Bob sont identiques. Les paires pour lesquels a et b sont de parité contraire correspondent à deux configurations de type (5.2) qui violent CHSH. Alice et Bob calculeront donc les espérances suivantes pour déceler la présence d'un attaquant éventuel :

$$E(A_0B_1) + E(A_0B_3) + E(A_2B_1) - E(A_2B_3) \quad \text{et} \quad E(A_1B_0) + E(A_1B_2) + E(A_3B_0) - E(A_3B_2). \tag{5.8}$$

Les paires pour lesquelles a et b sont différents mais de même parité sont ignorées. En résumé, en notant k les configurations participant directement à la clé, c_1, c_2 les configurations utilisées pour vérification par CHSH, on peut les représenter par la matrice

	B_0	B_1	B_2	B_3
A_0	k	c_1		c_1
A_1	c_2	k	c_2	
A_2		c_1	k	c_1
A_3	c_2		c_2	k

Si a et b sont choisis indépendamment et avec probabilités uniformes, la proportion de paires utilisées pour k et c sont respectivement $1/4$ et $1/2$ (contre $2/9$ et $4/9$ dans le protocole original).

En l'absence de toute perturbation extérieure, les paires sont utilisées pour détecter une éventuelle écoute par un attaquant donneraient des valeurs proches de $-2\sqrt{2}$ pour (5.8), correspondant à une violation de l'inégalité CHSH d'un facteur $v = \sqrt{2}$. Dans la pratique, les imperfections des détecteurs vont altérer cette valeur. Si on assimile cette altération à un bruit aléatoire, la violation résultante est donnée par $(1-F)v$ où F est la proportion de bruit introduit. Tant que ce facteur reste supérieur à 1, la présence d'un attaquant pourra être détectée. La proportion de bruit F pour laquelle l'action de l'attaquant devient indécelable est donc $F = 1 - 1/v$. Dans le protocole d'Ekert, $F = 1 - 1/\sqrt{2} \simeq 0.293$. Si on peut modifier le protocole de telle sorte que cette proportion F soit plus grande, on obtient un protocole meilleur car il sera encore plus difficile pour un attaquant de rester discret.

CHSH-3

L'utilisation de qutrits permet d'améliorer cette proportion F. C'est ce qui est fait dans [36] où le protocole 3DEB est défini. Il utilise une inégalité similaire à CHSH, mais liée à des mesures trichotomiques (à trois issues possibles). La version tridimensionnelle de CHSH apparaît dans [60] exprimée en termes de probabilités conjointes (les A_a et B_b sont des mesures trichotomiques) :

$$\begin{aligned} &p(A_1 = 2, B_1 = 1) + p(A_1 = 2, B_2 = 1) - p(A_2 = 2, B_1 = 1) + p(A_2 = 2, B_2 = 1) \\ &+p(A_1 = 1, B_1 = 2) + p(A_1 = 1, B_2 = 2) - p(A_2 = 1, B_1 = 2) + p(A_2 = 1, B_2 = 2) \\ &+p(A_1 = 2, B_1 = 2) + p(A_1 = 1, B_2 = 1) - p(A_2 = 2, B_1 = 2) + p(A_2 = 2, B_2 = 2) \\ &-p(A_1 = 1) - p(A_1 = 2) - p(B_2 = 1) - p(B_2 = 2) \leqslant 0 \end{aligned} \tag{5.9}$$

En supposant que les trois issues des mesures sont les racines cubiques de l'unité $1, \omega, \omega^2$, on peut exprimer [28] la même inégalité en termes de corrélations sous la forme $S \leqslant 2$ avec

$$S = \mathrm{Re}\big(E(A_1B_1)+E(A_1B_2)-E(A_2B_1)+E(A_2B_2)\big)+\frac{1}{\sqrt{3}}\,\mathrm{Im}\big(E(A_1B_1)-E(A_1B_2)-E(A_2B_1)+E(A_2B_2)\big)$$

On peut en fait voir que

$$S = -\frac{2}{9}\,\mathrm{Re}\,T$$

avec

$$T = 3\big((\omega^2-1)E(A_1^2B_1^2)+(\omega-1)E(A_1^2B_2^2)+(1-\omega^2)E(A_2^2B_1^2)+(\omega^2-1)E(A_2^2B_2^2)\big) \tag{5.10}$$

ce qui permet de réécrire cette inégalité sous la forme $\mathrm{Re}(-T) \leqslant 9$.

L'état $\frac{1}{\sqrt{3}}\big(|00\rangle+|11\rangle+|22\rangle\big)$ viole CHSH-3 d'un facteur $v = (6+4\sqrt{3})/9 \simeq 2.873/2$ (pour des bases de mesure convenables) ce qui correspond à un niveau de bruit de $F = 1-1/v = (11-6\sqrt{3})/2 \simeq 0.304$ (estimé numériquement dans [59], déterminé analytiquement dans [29]). On peut même obtenir [43] une violation de CHSH-3 d'un facteur $(1+\sqrt{11/3})/2 \simeq 1.457$ encore plus grand en utilisant un état non maximalement intriqué. Cela autorise un bruit de $F = (7-\sqrt{33})/4 \simeq 0.314$.

Le protocole 3DEB

Voici donc ce protocole utilisant des qutrits proposé dans [36]. Voir aussi [61]. Alice utilise les bases de mesure A_a (pour $a = 0,1,2,3$) qui sont les bases $\mathcal{B}_\theta$ avec $\theta = \zeta_{12}^a$. Bob utilise les bases B_b (pour $b = 0,1,2,3$) qui sont les $\mathcal{B}_\theta$ avec $\theta = \zeta_{12}^{-b}$. Pour $a = b$, Alice et Bob peuvent obtenir des bits de clé car les issues des mesures obtenues par Alice et Bob sont opposées. Les paires $(a,b) = (0,1),(0,3),(2,1),(2,3)$, correspondent à une configuration où l'inégalité CHSH-3 est violée d'un facteur $v = (6+4\sqrt{3})/9 \simeq 2.873/2$ (en dehors de toute perturbation). Idem pour les paires $(a,b) = (1,0),(1,2),(3,0),(3,2)$. Le mesures obtenues par Alice et Bob correspondant à ces paires leur permettront de détecter un écoute. Comme noté ci-dessus, la proportion F de bruit tolérable est meilleure que pour le protocole original d'Ekert.

Notre proposition

Les inégalités de Bell homogènes nous permettent de définir un protocole dans lequel la proportion F de bruit tolérable est encore meilleure. Nous proposons pour cela d'utiliser l'inégalité $-\frac{2}{9}\,\mathrm{Re}(T_1) \leqslant 1$ trouvée dans [4] avec

$$\begin{aligned} T_1 =& -(2\omega+4)E(A_1^2B_1^2)+(\omega-1)E(A_1^2B_1B_2)+(4\omega+2)E(A_1^2B_2^2)\\ &+(\omega-1)E(A_1A_2B_1^2)-(2\omega+1)E(A_1A_2B_1B_2)+(4\omega-1)E(A_1A_2B_2^2)\\ &+(\omega+5)E(A_2^2B_1^2)+(\omega+2)E(A_2^2B_1B_2)+(\omega-1)E(A_2^2B_2^2)\end{aligned}$$

qui est violée d'un facteur $\simeq 1.693$ par l'état $\frac{1}{\sqrt{3}}\big(|00\rangle+|11\rangle+|22\rangle\big)$ lorsqu'on utilise les mêmes bases de mesure que 3DEB. On obtient donc une résistance au bruit de $\simeq 0.409$.

Le tableau suivant (où $A_{00} := A_0^2$, $A_{02} := A_0A_2$,...) indique quelles paires de mesures permettent à Alice et Bob d'obtenir des bits de clés, et quelles paires leur serviront à détecter un éventuel attaquant.

	B_{00}	B_{02}	B_{22}	B_{11}	B_{13}	B_{33}
A_{00}	k			c	c	c
A_{02}		k		c	c	c
A_{22}			k	c	c	c
A_{11}	c	c	c	k		
A_{13}	c	c	c		k	
A_{33}	c	c	c			k

Notre proposition nécessite d'implémenter des dispositifs de mesure pour les produits de deux observables, tel A_{02}. Or, nous avons montré qu'un tel dispositif peut être réalisé en modifiant très légèrement le dispositif *tritter* [93] de détection utilisé habituellement pour un observable en dimension 3.

Conclusion et perspectives

En guise de conclusion, voici quelques commentaires sur la notion d'aléa, que m'ont inspiré ces années passées à le côtoyer.

1. Nombres aléatoires

Qu'est-ce qu'un nombre aléatoire ou une suite de bits aléatoire ? Tenter de répondre à cette question de façon satisfaisante reste l'objet de recherches (auxquelles je n'ai pas directement contribué) et de questionnements malgré un historique bien rempli.

Notons que la théorie des probabilités contourne soigneusement le problème (ce qui n'enlève rien à sa valeur), en définissant la notion d'*espace probabilisé* par une série d'axiomes que doivent vérifier les *probabilités*. Celles-ci sont alors des valeurs de fonctions, objet de nature parfaitement déterministe. De ce point de vue, l'aléatoire est modélisé par des concepts déterministes.

Pour la question de la définition de l'aléa, rappelons qu'il existe en fait plusieurs types de réponses. Un panorama intéressant en est exposé dans [87]. Voici quelques possibilités.

(1) On peut donner une définition intuitive basée sur la façon d'obtenir l'aléa, donc recourir à une expérience physique. Par exemple, la suite de 80 bits

10010110 10110101 01101011 11001100 00100101 00110110 00010100 01111011 01010100 00011111 (1)

est aléatoire parce qu'elle est le résultat de 80 tirages à pile ou face que j'ai effectués. Ce genre de définition est bien peu satisfaisante pour un mathématicien mais je la trouve empiriquement très défendable puisque chacun a une intuition assez nette de ce qu'est un tirage à pile ou face.

Bien sûr, la suite que j'ai obtenue n'avait pas plus de chances d'apparaître que la suite

11111111 11111111 11111111 11111111 11111111 11111111 11111111 11111111 11111111 11111111 (2)

qui elle, est parfaitement suspecte. (On peut aussi se demander si la suite (1) reste aléatoire, maintenant qu'elle fait partie de ce manuscrit, et n'est donc plus appropriée pour un usage cryptographique.) D'où le besoin de proposer une définition qui porte sur la suite elle-même, et non pas sur la façon de l'obtenir. Cette voie, suivie par Borel, von Mises, Wald, Church, peut être ouverte par l'assertion simplifiée suivante :

(2) Une suite de bits aléatoires est une suite qui ne vérifie pas de propriétés statistiques improbables.

Il reste à préciser ce qu'est une propriété statistique improbable, et donc « indésirable ». Mais là, le diable se cache dans les détails. L'exemple de la suite (2) illustre que le fait d'avoir un poids de Hamming élevé est une propriété indésirable, pour une suite « aléatoire ». Mais il y a une infinité d'autres propriétés que l'on peut déclarer indésirable. La notion de *nombres normaux* introduite par Émile Borel en 1909 en inclut une classe importante (mais pour des suites infinies) pour ne retenir que des suites ayant une certaine régularité statistique.

Le problème est alors d'inclure suffisamment de propriétés statistiques improbables (toutes ?). Cette phrase de D.H. Lehmer écrite en 1951 fait écho à l'embarras devant cette nécessité : « *A random sequence is a vague notion embodying the idea of a sequence in which each term is unpredictable to the uninitiated and whose digits pass a certain number of tests, traditional with statisticians and depending somewhat on the uses to which the sequence is to be put.* »

On doit à Church de nous avoir partiellement sortis de l'embarras en dégageant le principe essentiel selon lequel les propriétés statistiques à considérer doivent être effectivement calculables (sinon aucune suite ne serait aléatoire). Le lien entre aléa et calculabilité introduit par ce principe est illustré par le test universel de Maurer [73] qui fournit un algorithme pour vérifier si une suite est aléatoire, selon ce critère. Ce type de définition a un grand intérêt pratique, car cela permet de tester des générateurs aléatoires et de démasquer certains générateurs défectueux.

Les limites de ces définitions à base de propriétés statistiques apparaissent toutefois lorsqu'on les applique à des suites comme celle des décimales binaires de π. Cette suite est effectivement calculable et ne convient pas à un usage cryptographique. Pourtant, elle passe tous les tests statistiques standards (ou que l'on n'a pas construits spécialement pour elle). Cela mène à introduire une autre classe de définitions, basées sur l'incompressibilité (voie ouverte par Kolmogorov mais aussi Solomonoff, Chaitin). De façon (encore) informelle :

(3) Une suite de bits aléatoires est une suite qui n'a pas de description algorithmique plus courte que la donnée explicite de la suite.

Cette définition peut-être précisée à l'aide de la notion de complexité introduite par Kolmogorov [65]. Cette classe de définitions améliore la précédente : un résultat de Martin-Löf montre qu'une suite aléatoire au sens de Kolmogorov passe tous les tests statistiques (en un sens asymptotique).

Malheureusement, c'est une propriété difficile à tester (c'est même un problème indécidable). C'est grave pour les applications, puisque souvent on désire des suites « aléatoires » qui soient générées par des algorithmes simples et rapides. Ce type de définition reste donc lui aussi insatisfaisant.

C'est visiblement ce que pensait John von Neumann en 1963 : « *Any one who considers arithmetical methods of producing random digits is, of course, in a state of sin. For, as has been pointed out several times, there is no such thing as a random number — there are only methods to produce random numbers, and a strict arithmetic procedure of course is not such a method.* »

Il reste un point positif dans cette citation : il y a des méthodes pour **produire** des nombres aléatoires. Et on sait très heureusement définir précisément (mais de façon asymptotique) la notion de générateur (pseudo)-aléatoire sûr dans un sens cryptographique. On attend essentiellement deux choses d'un tel générateur. (1) La connaissance de l'aléa produit dans le passé ne permet pas à l'attaquant de prévoir celui qui va venir. (2) L'aléa produit par le générateur reste algorithmiquement indistinguable d'un générateur d'aléa « vrai » (c'est-à-dire satisfaisant les contraintes d'uniformité et d'indépendance énoncées par la théorie des probabilités). Par bonheur, un résultat de Yao [91] unifie ces deux exigences en montrant qu'elles sont équivalentes. La cohérence de la notion de générateur pseudo-aléatoire s'en trouve renforcée.

Cette notion de générateur (pseudo)-aléatoire nous ramène à l'idée initiale de définir l'aléa comme le résultat d'un processus physique, tout en la rendant reproductible en spécifiant un algorithme. Toutefois l'existence de générateurs aléatoires, respectant cette définition, reste hypothétique puisque étroitement reliée [51] à l'existence de fonctions à sens-unique, elle-même non prouvée...

L'accumulation des difficultés rencontrées pour définir la notion de nombre aléatoire peut laisser perplexe. Pourquoi restons nous si maladroits pour formaliser quelque chose qui peut paraître aussi banal que le résultat d'un lancer de dés ? D'autre part, on ne peut plus ignorer aujourd'hui que l'aléa joue un rôle dans la nature bien plus fondamental que celui qu'on a voulu lui attribuer. Cela pour au moins deux raisons :

• Les algorithmes probabilistes (qui utilisent de l'aléa) nous sont indispensables pour résoudre efficacement certains problèmes (exemple simple : trouver un non carré modulo un nombre premier). La classe de complexité **RP** est désormais considérée comme celle des problèmes résolubles en pratique.

• L'essence fondamentalement aléatoire de la nature est inscrite dans les principes de la mécanique quantique, et prouvée par la violation des inégalités de Bell. Les physiciens en viennent aujourd'hui à chercher à expliquer comment le déterminisme apparent du monde macroscopique émerge de l'aléa quantique. C'est un point de vue radicalement opposé à l'approche mathématique classique qui, comme nous l'avons évoqué, modélise l'aléa à partir de concepts déterministes.

La physique bénéficie des développements mathématiques mais, en retour, les mathématiques ont largement été influencées par des découvertes physiques. En ce sens, je me pose la question : nous mathématiciens, en suivant ceux qui se sont appliqués à fonder la discipline sur des axiomes de nature rigoureusement déterministe, avons-nous totalement appréhendé le caractère fondamental de l'aléa ?

2. Perspectives

Le potentiel des inégalités homogènes de Bell me semble immense. Tout d'abord, d'un point de vue théorique, elles forment un jeu complet d'inégalités — c'est-à-dire qu'elles caractérisent complètement le réalisme local, jeu qui était très recherché. D'autre part, l'existence des ces inégalités donne une explication simple à une

interrogation récurrente [75] dans les articles sur les inégalités de Bell : certaines inégalités sont maximalement violées par des états non maximalement intriqués.

Pour les applications, j'en entrevois beaucoup, et je vais en développer ici quelques unes. Nous avons déjà proposé, avec Zoé, un nouveau protocole [2] de distribution de clés les exploitant, le gain étant une forte amélioration de la résistance au bruit par rapport aux protocoles existants.

Liens avec d'autres inégalités

Il reste à préciser les liens avec d'autres inégalités de Bell présentes dans la littérature. J'ai fait ce travail pour l'inégalité CHSH-3 [28] et pour l'inégalité CGLMP [33] avec $d = 3$. Il semble qu'il y ait un lien intéressant avec l'inégalité à mesures multiples étudiée dans [56]. Il est probable de plus, que ce lien soit exploitable pour définir une variante de notre protocole de distribution de clé, utilisant moins d'appareils de mesure. Zoé et moi y réfléchissons déjà.

Production d'aléa vrai

Puisque la physique quantique donne à l'aléa un statut très différent de celui suggéré par la physique classique, de nombreuses perspectives sont ouvertes à ce sujet. Je compte en aborder certaines.

Tout d'abord, certains auteurs [71][79] ont déjà remarqué que la violation des inégalités de Bell permet de garantir que de l'aléa vrai est généré lors de certains processus, et de quantifier la quantité d'aléa produit.

Le *jeu de Bell* est un exemple de tel processus. Alice et Bob possèdent deux boîtes (dispositifs probabilistes non communicants, pouvant partager un secret préalable). Leurs entrées respectives sont des bits $x, y \in \{0, 1\}$, et leurs sorties respectives $a, b \in \{1, -1\}$. Alice et Bob gagnent au jeu de Bell lorsque l'identité

$$ab = (-1)^{xy} \tag{3}$$

est satisfaite.

Dans un cadre classique, Alice et Bob peuvent se mettre d'accord au préalable pour que les sorties a et b soit égales. Ils gagnent alors au jeu avec probabilité $3/4$ (si les entrées sont choisies au hasard uniforme), donc l'espérance de leur gain est $1/2$. On ne peut pas améliorer ce score en restant dans le cadre classique.

Mais tout change dans un cadre quantique. Alice et Bob peuvent décider d'utiliser des paires de qbits intriqués dans l'état

$$|\Psi\rangle = \alpha|00\rangle + \beta|11\rangle \qquad \text{avec } \alpha = \cos\phi \text{ et } \beta = \sin\phi.$$

On considère alors l'observable

$$\cos\theta Z + \sin\theta X = \begin{pmatrix} \cos\theta & \sin\theta \\ \sin\theta & -\cos\theta \end{pmatrix} = P^+ - P^-$$

avec P^+ et P^- projecteurs :

$$P^+ = \begin{pmatrix} c^2 & cs \\ cs & s^2 \end{pmatrix} \quad \text{et} \quad P^- = \begin{pmatrix} s^2 & -cs \\ -cs & c^2 \end{pmatrix} \qquad \text{où } \begin{cases} c = \cos(\theta/2) \\ s = \sin(\theta/2) \end{cases}.$$

Lorsque Alice utilise les deux mesures repérées par les angles $\theta_A = 0$ et $\pi/2$, et que Bob utilise les mesures repérées par $\theta_B = \theta$ ou $-\theta$, on calcule que les probabilités des sorties ab en fonctions des entrées xy sont données par le tableau suivant.

$xy\backslash ab$	$++$	$+-$	$-+$	$--$
00	$\alpha^2 c^2$	$\alpha^2 s^2$	$\beta^2 s^2$	$\beta^2 c^2$
01	$\alpha^2 c^2$	$\alpha^2 s^2$	$\beta^2 s^2$	$\beta^2 c^2$
10	$\frac{1}{2}(\alpha c + \beta s)^2$	$\frac{1}{2}(\alpha c - \beta s)^2$	$\frac{1}{2}(\alpha s - \beta c)^2$	$\frac{1}{2}(\alpha s + \beta c)^2$
11	$\frac{1}{2}(\alpha c - \beta s)^2$	$\frac{1}{2}(\alpha c + \beta s)^2$	$\frac{1}{2}(\alpha s + \beta c)^2$	$\frac{1}{2}(\alpha s - \beta c)^2$

Table 1. Probabilités des résultats de mesures dans le plan `xz`

En particulier, pour un état Ψ maximalement intriqué ($\alpha = \beta = \sqrt{2}/2$), et les bases de mesure habituellement utilisées pour obtenir la violation maximale de l'inégalité CHSH : ($\theta = \pi/4$, $c = \sqrt{2+\sqrt{2}}/2$, $s = \sqrt{2-\sqrt{2}}/2$), les plus grandes de ces probabilités valent $(2+\sqrt{2})/8 \simeq 0.427$. La min-entropie correspondante est d'environ 1.23 bits. On peut considérer cette min-entropie comme la quantité minimale d'aléa produit.

On peut minorer la min-entropie aussi dans le cas général, en fonction du gain au jeu de Bell. Les probabilités

$$\begin{cases} P(a = + \mid x = 0) = \alpha^2, \\ P(a = - \mid x = 0) = \beta^2, \end{cases} \qquad \begin{cases} P(a = + \mid x = 1) = \alpha^2 c^2 + \beta^2 s^2, \\ P(a = - \mid x = 1) = \alpha^2 s^2 + \beta^2 c^2. \end{cases}$$

sont toutes majorées : $P(a \mid x) \leqslant \max(\alpha^2, \beta^2)$. D'autre part, l'espérance du gain au jeu de Bell est donnée par $G/4$ avec

$$G = E(A_0, B_0) + E(A_0, B_1) + E(A_1, B_0) - E(A_1, B_1)$$

et les valeurs du tableau montrent aussi que $G = 2\big(\cos\theta + \sin(2\phi)\sin\theta\big)$. Cette valeur est maximisée pour $\sin(2\phi) = \tan\theta$ et on obtient (lorsque $0 \leqslant \phi \leqslant \pi/4$ donc $\alpha^2 \leqslant \beta^2$) :

$$G \leqslant G_{\max} = 2\sqrt{1 + \sin^2(2\phi)},$$

Finalement, on obtient $P(a \mid x) \leqslant \alpha^2 \leqslant \frac{1}{2}\left(1 + \sqrt{2 - G_{\max}^2/4}\right)$. Un attaquant connaissant l'entrée (x, y) peut alors deviner la sortie (a, b) avec probabilité majorée par cette même borne. Autrement dit, la min-entropie du bit a généré est donnée par : $1 - \log_2\left(1 + \sqrt{2 - G_{\max}^2/4}\right)$.

De telles bornes peuvent probablement être obtenues à l'aide des inégalités de Bell homogènes. Cela permettrait de quantifier la quantité d'aléa produit à l'aide de certains dispositifs utilisant des qudits.

Brisons des tabous

Les inégalités de Bell homogènes que j'ai décrites dans [4] ont la particularité de briser deux tabous qui semblent planer sur la littérature en rapport avec ce sujet. Le premier de ces tabous est celui de l'utilisation de fonctions de corrélations à valeurs complexes, dont l'interprétation physique a pu sembler délicate (mais qui peut être argumentée [42]). Le second, qui me paraît assez durement ancré dans la communauté scientifique, est celui de la multiplication de deux opérateurs d'observables quantiques qui ne commutent pas. Alors que de tels produits interviennent de façon essentielle dans la démonstration du principe d'incertitude de Heisenberg, ils semblent bannis du reste de la littérature et le terme d'observables « incompatibles » universellement utilisé est pris au pied de la lettre. Ce tabou est — me semble-t-il — lié à la tradition de restreindre les observables à des opérateurs hermitiens (pour avoir des issues réelles aux mesures physiques). Pourtant, une partie de la communauté sait depuis longtemps que le formalisme quantique fonctionne avec des opérateurs normaux. L'utilisation d'opérateurs unitaires dans les inégalités de Bell homogènes contribue, je l'espère, à briser ce tabou, d'autant plus que, comme je l'ai montré, ce produit peut avoir un sens physique, dans le sens où on peut le mesurer expérimentalement.

Il me semble que l'existence des inégalités de Bell homogènes devrait contribuer à faire prendre conscience à la communauté que l'habitude de ne considérer que des observables hermitiens — même si elle est justifiée d'un point de vue expérimental — est maladroite, voire inadaptée, pour décrire certains aspects quantiques fondamentaux.

Bibliographie

[1] A. Acín, T. Durt, N. Gisin, J.L. Latorre : *Quantum non-locality in two three level systems.* Physical Review A, 65, 052325 (2002).

[2] Z. Amblard, F. Arnault : *A qutrit quantum key distribution protocol with better noise resistance.* Submitted.

[3] F. Arnault : *Formes quadratiques de discriminants emboîtés.* arXiv:1402.0344 [math.NT], 2014.

[4] F. Arnault : *A complete set of multidimensional Bell inequalities.* Journal of Physics A, Mathematical and Theoretical 45, 255304, 2012.

[5] F. Arnault : *The Rabin-Monier theorem for Lucas pseudoprimes.* Mathematics of Computation, vol. 218(66), 869–881, 1997.

[6] F. Arnault : *Constructing Carmichael numbers which are strong pseudoprimes to several bases.* Journal of Symbolic Computation 20(2), 151–161, 1995.

[7] F. Arnault : *The Rabin-Miller primality test : Composite numbers which pass it.* Mathematics of Computation 64(209), 355–361, 1995.

[8] F. Arnault : *Sur quelques tests probabilistes de primalité.* Thèse de l'Université de Poitiers, 1993.

[9] F. Arnault, T.P. Berger : *Design and properties of a new pseudorandom generator based on a filtered FCSR automaton.* IEEE Transactions on Computers 54(11), 1374–1383, 2005.

[10] F. Arnault, T.P. Berger, C. Lauradoux, M. Minier, B. Pousse : *A new approach for FCSRs.* Lecture Notes in Computer Science 5867 (SAC'09), 433–448, 2009.

[11] F. Arnault, T.P. Berger, M. Minier : *Some results on FCSR automata with application to the security of FCSR-based pseudorandom generators.* IEEE, Transactions on Information Theory, 54(2), 836–840, 2008.

[12] F. Arnault, T.P. Berger, M. Minier, B. Pousse : *Revisiting LFSRs for cryptographic applications.* IEEE, Transactions on Information Theory, 57(12), 8195–8113, 2011.

[13] F. Arnault, T.P. Berger, A. Necer : *Feedback with Carry Shift Registers synthesis with the Euclidean algorithm.* IEEE Trans. Inform. Theory, 50(5), 910-916, 2004.

[14] F. Arnault, T.P. Berger, B. Pousse : *A matrix approach for FCSR automata.* Cryptography and Communications (Discrete Structures, Boolean functions and Sequences) 3, 109–139, 2011.

[15] F. Arnault, E.J. Pickett, S. Vinatier : *Construction of self-dual normal bases and their complexity.* Finite Fields and Their Applications 18, 458–472, 2012.

[16] J.S. Bell : *On the Einstein Podolsky Rosen paradox.* Physics 1, 195–200, 1964.

[17] C.H. Bennett, G. Brassard : *Quantum cryptography: public key distribution and coin tossing.* In Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, 175-179, 1984.

[18] I. Biehl, J. Buchmann : *An analysis of the reduction algorithms for binary quadratic forms.* In: Voronoï's impact on modern science, 71–98, 1999.

[19] A. Bernard : *Formes quadratiques binaires et applications cryptographiques.* Thèse de Doctorat, Université de Limoges, 2011.

[20] A. Bernard, N. Gama : *Smallest reduction matrix of binary quadratic forms.* Proceedings of ANTS 2010, 32–49, 2010.

[21] J. Buchmann, U. Vollmer : *Binary Quadratic Forms, an algorithmic approach.* Algorithms and Computation in Mathematics, Vol. 20, Springer, 2007.

[22] D.A. Buell : *Binary Quadratic Forms, Classical theory and modern computations.* Springer, 1989.

[23] G. Castagnos : *Quelques schémas de cryptographie asymétrique probabiliste.* Thèse de Doctorat, Université de Limoges, 2006.

[24] G. Castagnos : *An efficient probabilistic public-key cryptosystem over quadratic fields quotients.* Finite Fields and their Applications 13, 563–576, 2007.

[25] G. Castagnos, F. Laguillaumie : *On the security of cryptosystems with quadratic decryption: the nicest cryptanalysis.* Proceedings of Eurocrypt'09.

[26] G. Castagnos, F. Laguillaumie, A. Joux, P.Q. Nguyen : *Factoring with quadratic forms: nice cryptanalyses.* Proceedings of Asiacrypt'09.

[27] D. Catalano, R. Gennaro, N. Howgrave-Graham, P.Q. Nguyen : *Paillier's cryptosystem revisited.* Proceedings of the 8th ACM conference on Computer and Communications Security (CCS'01), 206–214, 2001.

[28] J.-L. Chen, D. Kaszlikowski, L.C. Kwek, C.H. Oh : *Wringing out new Bell inequalities for three-dimensional systems (qutrits).* Modern Physics Letters A 17, 2231, 2002.

[29] J.-L. Chen, D. Kaszlikowski, L.C. Kwek, C.H. Oh, M. Żukowski : *Entangled three-state systems violate local realism more strongly than qubits: an analytical proof.* Physical Review A 64, 052109 (2001).

[30] J.F. Clauser, M.A. Horne, A. Shimony, R.A. Holt : *Proposed experiment to test local hidden variables theories.* Physical Review Letters 23, 880, 1969.

[31] H. Cohen : *A Course in Computational Algebraic Number Theory.* Springer-Verlag, GTM 138, 1993.

[32] H. Cohn : *A Second Course in Number Theory.* John Wiley & Sons, 1962.

[33] D. Collins, N. Gisin, N. Linden, S. Massar, S. Popescu : *Bell inequalities for arbitrarily high-dimensional systems.* Physical Review Letters 88, 040404 (2002).

[34] D. Coppersmith : *Small solutions to polynomial equations, and low exponent RSA vulnerabilities.* Journal of Cryptology 10(4), 233-260, 1997.

[35] D.A. Cox : *Primes of the Form $x^2 + ny^2$.* Wiley-Interscience, John Wiley & Sons, 1989.

[36] T. Durt, N.J. Cerf, N. Gisin, M. Żukowski : *Security of quantum key distribution with entangled qutrits.* Physical Review A 67, 012311 (2003).

[37] T. Durt, K. Kaszlikowski, M. Żukowski : *Violations of local realism with quantum systems described by N-dimensional Hilbert spaces up to $N = 16$.* Physical Review A 64, 024101.

[38] eSTREAM : *ECRYPT call for stream cipher primitives.* `http://www.ecrypt.eu.org/stream/call/`, 2005.

[39] A. Einstein, B. Podolsky, N. Rosen : *Can quantum-mechanical description of physical reality be considered complete?.* Physical Review 47, 777, 1935.

[40] A.K. Ekert : *Quantum cryptography based on Bell's theorem.* Physical Review Letters 67, 661 (1991).

[41] A. Fine : *Hidden variables, joint probabilities, and the Bell inequalities.* Physical Review Letters 48, 291, 1982.

[42] L-B. Fu : *General correlation functions of the Clauser-Horne-Shimony-Holt inequality for arbitrarily high-dimensional systems.* Physical Review Letters 92, 130404 (2004).

[43] L.-B. Fu, J.-L. Chen, X.-G. Zhao : *Maximal violation of the Clauser-Horne-Shimony-Holt inequality for two qutrits.* Physical Review A 68, 022323 (2003).

[44] D. Galindo, S. Martín, P. Morillo, J.L. Villar : *An efficient semantically secure elliptic curve cryptosystem based on KMOV.* Proceedings of Workshop on Coding and Cryptography (WCC'03), 213–221, 2003.

[45] S. Gao, H.W. Lenstra Jr : *Optimal normal bases.* Designs, Codes and Cryptography 2, 315–323, 1992.

[46] C.F. Gauss : *Disquisitiones Arithmeticae (traduction).* Springer, 1986.

[47] W. Geiselmann, D. Gollmann : *Self-dual bases in* $\mathbb{F}_{q^n}$. Design, Codes and Cryptography 3, 333-345, 1993.

[48] M. Goresky, A. Klapper : *Fibonnacci and Galois representation of feedback with carry shift registers.* IEEE Transactions on Information Theory 48, 2826–2836, 2002.

[49] M. Goresky, A. Klapper : *Algebraic shift register sequences.* Cambridge University Press, 2012.

[50] M. Hartmann, S. Paulus, T. Takagi : *NICE – New ideal coset encryption.* Proceedings of CHES'99, LNCS 1717, 328–339, 1999.

[51] J. Håstad, R. Impagliazzo, L.A. Levin, M. Luby : *A pseudorandom generator from any one-way function.* SIAM Journal on Computing 28(4), 1364–1396, 1999.

[52] M. Hell, T. Johansson : *Breaking the F-FCSR-H stream cipher in real time.* Lectures Notes in Computer Science 5350 (Asiacrypt'08), 557–569, 2008.

[53] K. Ireland, M. Rosen : *A Classical Introduction to Modern Number Theory.* Springer-Verlag, New York, 2nd edition 1990.

[54] M.J. Jacobson Jr, R. Scheidler, D. Weimer : *An adaptation of the NICE cryptosystem to real quadratic orders.* Proceedings of Africacrypt'08, LNCS 5023, 191–208, 2008.

[55] M.J. Jacobson Jr, H.C. Williams : *Solving the Pell equation.* Canadian Mathematical Society, Springer, 2009.

[56] S-W. Ji, J. Lee, J. Lim, K. Nagata, H-W.Lee : *Multisetting Bell inequality for qudits.* Physical Review A 78, 052103 (2008).

[57] D. Jungnickel : *Finite fields : structure and arithmetics.* B.I. Wissenschaftsverlag, 1993.

[58] D. Jungnickel, A.J. Menezes, S.A. Vanstone : *On the number of self-dual bases of* $GF(q^n)$ *over* $GF(q)$. Proceeding of the AMS, vol. 109(1), 23–29, 1990.

[59] D. Kaszlikowski, P. Gnaciński, M. Żukowski, W. Miklaszewski, A. Zeilinger : *Violations of local realism by two entangled N-dimensional systems are stronger than for two qubits.* Physical Review Letters 85, 4418 (2000).

[60] D. Kaszlikowski, L.C. Kwek, J.L. Chen, M. Żukowski, C.H. Oh : *Clauser-Horne inequality for three-state systems.* Physical Review A 65, 032118 (2002).

[61] D. Kaszlikowski, D.K.L. Oi, M. Christandl, K. Chang, A. Ekert, L.C. Kwek, C.H. Oh : *Quantum cryptography based on qutrit Bell inequalities.* Physical Review A 67, 012310 (2003).

[62] D.E. Knuth : *The Art of Computer Programming. Tome 2 : Semi-numerical algorithms.* Addison-Wesley, 1973.

[63] A. Klapper, M. Goresky : *2-adic shift registers.* Lecture Notes in Computer Science 809 (Fast Software Encryption), 174–178, 1994.

[64] A. Klapper, M. Goresky : *Feedback shift registers, 2-adic span, and combiners with memory.* Journal of Cryptology 10, 111–147, 1997.

[65] A.N. Kolmogorov : *On tables of random numbers.* Sankhyā, Ser. A 25, 369–376, 1963.

[66] D.H. Lehmer, E. Lehmer : *A new factorization technique using quadratic forms.* Mathematics of Computation 28, 625–635, 1974.

[67] A. Lempel, G. Seroussi : *Factorization of symmetric matrices and trace-orthogonal bases in finite fields.* SIAM Journal of Computing 9, 758–767, 1980.

[68] H.W. Lenstra Jr, R.J. Schoof : *Primitive normal bases for finite fields.* Mathematics of Computation 48(117), 217–231, 1987.

[69] R. Lidl, H. Niederreiter : *Introduction to finite fields and their applications.* Cambridge University Press, 1986.

[70] F.J. MacWilliams : *Orthogonal circulant matrices over finite fields, and how to find them.* Journal of Combinatorial Theory 10, 1–17, 1971.

[71] Ll. Masanes, S. Pironio, A. Acín : *Secure device-independent quantum key distribution with causally independent measurement devides.* Nature Communications 2, 238, 1244 (2011).

[72] A.M. Masuda, L. Moura, D. Panario, D. Thomson : *Low complexity normal elements over finite fields of characteristic two.* IEEE Transactions on Computers 57(7), 990–1001, 2007.

[73] U.M. Maurer : *A universal statistical test for random bit generators.* Journal of Cryptology 5, 89–105, 1992.

[74] A.J. Menezes, I.F. Blake, S. Gao, R.C. Mullin, S.A. Vanstone, T. Yaghoobian (eds) : *Applications of finite fields.* Kluwer Academic Publishers, 1993.

[75] A.A. Méthot, V. Scarani : *An anomaly of non-locality.* Quantum Information and Computation 7(1), 157–170 (2007).

[76] R.C. Mullin, L.M. Omyszchuk, S.A. Vanstone, R.M. Wilson : *Optimal bases in* GF(p^n). Discrete Appl. Math. 22 (2), 149–161, 1989.

[77] S. Paulus, T. Takagi : *A new public-key cryptosystem over a quadratic order with quadratic decryption time.* Journal of Cryptology 13(2), 263–272, 2000.

[78] E.J. Pickett : *Construction of self-dual integral normal bases in abelian extensions of finite and local fields.* International Journal of Number Theory 6(7), 1565–1588, 2010.

[79] S. Pironio, A. Acín, S. Massar, A. Boyer de la Giroday, D.N. Matsukevich, P. Maunz, S. Ohmschenk, D. Hayes, L. Luo, T.A. Manning, C. Monroe : *Random numbers certified by Bell's theorem.* Nature 464, 1021 (2010).

[80] A. Schinzel : *On some problems of the arithmetical theory of continued fractions.* Acta Arithmeticae 6, 393–413, 1961.

[81] R.J. Schoof : *Quadratic Fields and factorization.* Computational Methods in Number Theory, part II, H.W. Lenstra, R Tijdeman (ed.). Mathematical Centre Tracts 155, Amsterdam, 235–286, 1982.

[82] C.P. Schnorr, H.W. Lenstra : *A Monte Carlo factoring algorithm with linear storage.* Mathematics of Computation 167(43), 289–311, 1984.

[83] D. Shanks : *Five number-theoretic algorithms.* Proceedings of the Second Manitoba Conference on Numerical Mathematics, 51–70, 1972.

[84] C.E. Shannon : *Communication theory of secrecy systems.* Bell Syst. Tech. J. 28, 656–715, 1949.

[85] P. Shor : *Polynomial-time algorithms for prime factorization and discrete logarithm problems.* SIAM Journal of Computing 26, 1484–1509, 1997.

[86] T. Tian, W.-F. Qi : *Linearity properties of binary FCSR sequences.* Design, Codes and Cryptography 52, 249–262 (2009).

[87] S.B. Volchan : *What is a random sequence?.* American Mathematical Monthly 109, 46–63, 2002.

[88] C.C. Wang : *An algorithm to design finite field multipliers using a self-dual normal basis.* IEEE Transaction on Computers 38(10), 1989.

[89] R.F. Werner, M.M. Wolf : *All-multipartite Bell-correlation inequalities for two dichotomic observables per site.* Physical Review A 64, 032112, 2001.

[90] H. Wang, P. Stankovski, T. Johansson : *A generalized birthday approach for efficiently finding linear relations in ℓ-sequences.* Design, Codes and Cryptography, 1–17, 27 juin 2013.

[91] A.C. Yao : *Theory and applications of trapdoor functions.* Proceedings of 23rd IEEE symposium on foundations of computer science, 1982, 80–91.

[92] M. Żukowski, Č. Brukner : *Bell's theorem for general N-qubit states.* Physical Review Letters 88, 210401, 2002.

[93] M. Żukowski, A. Zeilinger, M.A. Horne : *Realizable higher-dimensional two-particle entanglements via multiport beam splitters.* Physical Review A 55, 2564, 1997.

Résumé

Ce mémoire dresse un panorama du travail de recherche effectué par l'auteur après sa thèse de Doctorat. Il développe divers outils de mathématiques discrètes, avec le souci de les rendre effectifs d'un point de vue algorithmique. De nombreuses applications en relation avec la cryptographie sont détaillées. La théorie et les applications y sont étroitement mêlées.

Les domaines mathématiques abordés sont tout d'abord l'arithmétique modulaire et celle des corps quadratiques. Puis les formes quadratiques de Gauss sont considérées, avec en particulier une étude détaillée des liens entre formes de discriminants *emboîtés*. La réduction des formes quadratiques réelles est aussi réexaminée. Les applications cryptographiques présentées sont des variantes du système cryptographique de Paillier et d'autres systèmes de chiffrement probabilistes, ainsi qu'une étude de la cryptanalyse du système de chiffrement NICE.

Les extensions de corps finis sont aussi présentes avec la construction de bases normales autoduales, basée sur l'étude de la structure de l'algèbre de groupe associée au groupe de Galois. En pratique, cette étude contribue à obtenir une arithmétique efficace pour les corps finis.

Suit alors une partie importante consacrée aux registres à décalages, et plus précisément aux FCSR, qui sont similaires aux très répandus LFSR mais dont la fonction de transition préserve et propage la retenue de l'addition. Leur analyse mathématique est ici basée sur l'interprétation des suites générées en termes de développements d'entiers 2-adiques. La notion de FCSR est ensuite généralisée, en particulier avec l'introduction et l'étude des FCSR annulaires. Ce travail est appliqué à la conception de générateurs pseudo-aléatoires et de méthodes de chiffrement à flot. Notamment, l'utilisation de circuits FCSR filtrés par une fonction linéaire est proposée, et l'un des algorithmes conçus sera finaliste du projet européen ESTREAM dans la catégorie chiffrement *hardware*. L'intérêt pratique des FCSR annulaires est illustré par le gain en performances des générateurs aléatoires qui les utilisent et par leur résistance à une attaque à laquelle succombent les FCSR classiques.

Une deuxième partie importante concerne des travaux récents en information quantique. La frontière entre le monde classique et le monde quantique est explorée et précisée avec la formulation de nouvelles inégalités de Bell, formées à partir de polynômes homogènes. Ces inégalités forment un jeu complet, dans le sens où le polytope complexe qu'elles définissent est exactement le domaine compatible avec une théorie physique réaliste locale. Par l'étude de la façon dont son violées ces inégalités en utilisant des observables quantiques unitaires, ce travail confirme l'intérêt d'étudier les systèmes quantiques multidimensionnels (qudits) par rapport à seule considération d'objets binaires. Ce travail est ensuite appliqué à la conception d'un nouveau protocole quantique de distribution de clés, offrant la meilleure résistance au bruit. D'autres applications sont esquissées.

Le mémoire se termine par quelques réflexions sur la notion d'aléa en mathématiques et en cryptographie ainsi que sur les nouvelles perspectives offertes par la physique quantique. Il argumente aussi pour inciter la communauté à considérer l'utilisation d'opérateurs observables normaux (en particulier unitaires) au lieu de se restreindre trop souvent aux opérateurs hermitiens.