Université de Caen/Basse-Normandie
U.F.R. Sciences

École Doctorale SIMEM

THÈSE

présentée par

Fabien Galand

et soutenue
le 1er décembre 2004

en vue de l'obtention du

Doctorat de l'université de Caen
Spécialité informatique
(Arrêté du 25 avril 2002)

Construction de codes $\mathbb{Z}_{p^k}$-linéaires de bonne distance minimale, et schémas de dissimulation fondés sur les codes de recouvrement

Membres du Jury

M.	Claude Carlet,	Professeur, Université de Paris 8	(Directeur)
M.	Thierry Berger,	Professeur, Université de Limoges	(Rapporteur)
M.	Gilles Zémor,	Maître de conférences (HDR), ENST Paris	(Rapporteur)
Mme	Caroline Fontaine,	Chargée de recherche, Université de Lille 1	
M.	Grigory Kabatiansky,	Chargé de recherche, IITP (Moscou)	
Mme	Brigitte Vallée,	Directrice de recherche, Université de Caen	

Remerciements

De nombreuses personnes ont contribué à l'aboutissement de cette thèse. Bien évidemment, elle n'aurait pu voir le jour sans Claude Carlet qui, bien au-delà de la direction scientifique, a su me faire comprendre, au travers de conseils sans nombre, sa pratique de la recherche.

J'ai également profité d'un environnement des plus favorables, le projet CODES, et suis par là même redevable à Pascale Charpin et à Nicolas Sendrier de m'y avoir hébergé le plus naturellement du monde. Ils ont toujours eu à mon égard une bienveillance qui aura été pour moi un véritable soutien.

J'ai mis à contribution l'intégralité des membres permanents du projet en me tournant, à un moment ou à un autre, vers chacun d'eux pour des explications. J'ai tout particulièrement abusé du temps d'Anne Canteaut, d'une disponibilité et d'une rigueur sans failles, ainsi que de celui de Jean-Pierre Tillich dont la pertinence des commentaires ne cessera de m'émerveiller. Ils ont tous deux grandement participé à débroussailler le présent manuscrit et je les prie de m'excuser de ne pas avoir fait un meilleur usage de leurs remarques.

À côté de la science, l'ambiance régnant dans cette équipe, et notamment la bonhomie teintée d'humour de Daniel Augot, s'est avérée une source inépuisable d'énergie. Que dire de ces moments de détente dans la « salle à café », où j'ai pu profiter non seulement des chefs mais aussi de Marion, Cédric T., Cédric L., Emmanuel, Matthieu, Mathieu, de la nombreuse main-d'œuvre occasionnelle et des badauds de passages ? Je n'oublie pas Christelle, qui a été pour moi d'une aide administrative salvatrice, mais qui a surtout constamment le rire aux lèvres.

Bien que n'appartenant pas au projet, Grigory Kabatiansky y est pour moi associé et n'y dépareillerait pas. Sans lui, la seconde partie ma thèse n'existerait pas et cette collaboration m'honore. Sa clarté, sa rigueur et l'ambiance de travail détendue qu'il arrive à créer et qu'il nourrit de ses innombrables plaisanteries, constituent pour moi un véritable modèle.

Bien que peu présent dans l'équipe caennaise d'algorithmique, j'y ai toujours été accueilli chaleureusement par la joyeuse petite bande de doctorants : Aline, Ben, Bruno, Jérémie, Guillaume, Philippe et Régis. Ma sympathie va en particulier à Aline qui n'a pas été avare de son expérience et de sa vision de la recherche. Je remercie Emmanuel pour la même raison.

C'est à Caen que j'ai effectué mon DEA et que j'ai eu la chance de suivre les cours magistraux de Brigitte Vallée. Je lui suis grandement redevable de ces cours, de son implication dans l'obtention de mon financement et de l'intérêt constant qu'elle a manifesté pour le déroulement de ma thèse. Je suis heureux de la voir participer à mon jury.

Je n'aurais pas pu disposer, pour conclure cette thèse, de conditions plus favorables que celles qu'Hubert Comon-Lundh m'a offertes au sein du Laboratoire spécification et vérification, et du département d'informatique de l'École normale supérieure de Cachan. Je l'en remercie et lui présente ici toutes mes excuses pour avoir autant abusé de son indulgence à l'égard de ma situation.

Je suis reconnaissant à Thierry Berger et à Gilles Zémor d'avoir accepté, non seulement de faire partie de mon jury, mais surtout de rapporter ma thèse. La présence de Caroline Fontaine dans ce même jury m'est des plus agréables et ses remarques sur la seconde partie de mon manuscrit m'ont été très profitables.

Enfin, avant de terminer cette série de remerciements, un mot pour ceux qui m'ont permis de garder les pieds sur terre, contre vents et marées et anneaux de Galois. En première ligne, fidèle parmi les fidèles, l'autre-partie-de-la-coloc, Ahmed, qui m'aura supporté, dans presque toutes les acceptions, probablement beaucoup plus qu'il ne l'aurait souhaité. Cette thèse lui doit tant qu'il s'agit un peu de la sienne. Je regrette légèrement de ne pas l'avoir faite sur le béton, il en serait certainement plus fier et pourrait plus facilement y retrouver sa contribution. Loin d'être seul, il fut épaulé dans sa lourde tâche par des hommes de l'ombre, Fabrice, Yann et Yves. Merci à eux et mes plus plates excuses à ceux que j'ai délaissés, notamment Sengdo. D'un soutien plus récent, mais non moins solide, Nathalie. Outre son rôle de correcteur orthographique hors pair, en chair et en os, je lui dois l'intégralité de mes connaissances en latin. Quelle joie de découvrir Cicéron et sa première *Catilinaire* : « Quousque tandem abutere, Catilina, patientia nostra » ! Ces derniers mois auraient été autrement plus éprouvants sans elle.

Le mot de la fin va à ma famille, ma mère, mon père et mon frère bien sûr, mais je pense surtout à mes grands-parents, disparus lors de ma thèse.

Sommaire

Première partie : codes $\mathbb{Z}_{p^k}$-linéaires

Seconde partie : schémas de dissimulation

Avant-propos

Ce document comprend deux parties correspondant à deux axes de recherches différents : les codes correcteurs d'erreurs et la stéganographie. Dans notre approche, ces deux axes se rejoignent autour des objets étudiés : les codes. Mais, chaque axe se concentre sur l'étude d'un paramètre spécifique : distance minimale pour la correction d'erreur ; rayon de recouvrement pour la stéganographie.

Ainsi, bien que les thèmes de chaque partie soient nettement distincts, c'est un même objet qui est *in fine* le sujet d'étude, mais sous un éclairage différent à chaque fois. Cela illustre la généralité et la richesse des problèmes survenant avec ces objets pourtant simples.

Les résultats de la première partie ont fait l'objet, pour $p = 2$, d'une courte présentation dans [Ga03b] et d'un rapport de recherche plus détaillé [Ga03a]. La seconde partie reprend très largement, tout en les précisant, des travaux menés conjointement avec Grigory Kabatiansky, et publiés dans [GK03a, GK03b]. Les exceptions notables sont les sections 8.3 et 8.6, ainsi que le chapitre 9.

Seconde partie

Schémas de dissimulation fondés sur les codes de recouvrement

Introduction

La confidentialité des communications est le plus souvent assurée par la cryptographie : l'information subit un traitement particulier, appelé chiffrement, visant à la rendre inintelligible par toute personne non autorisée. Cette information, une fois chiffrée, peut être librement transmise au travers d'un canal susceptible d'être écouté : sa confidentialité n'est pas compromise puisque son sens a été complètement masqué.

Une approche orthogonale de la confidentialité consiste à soustraire le message lui-même, et non plus seulement son sens, à une éventuelle surveillance. On cherche alors à dissimuler l'existence d'un message, et c'est précisément ce qui constitue le sujet d'étude de la stéganographie.

Dans les faits, il se trouve que cette manière d'assurer la confidentialité d'une information est antérieure à l'utilisation du chiffrement. Dans son *Enquête*, l'historien grec Hérodote (484-445 av. J.-C.) rapporte ainsi une anecdote qui eut lieu au moment de la seconde guerre médique. En 484 avant notre ère, Xerxès, fils de Darius, roi des Perses, décide de préparer une armée gigantesque pour envahir la Grèce (Livre VII, 5-19). Quatre ans plus tard, lorsqu'il lance l'offensive, les Grecs sont depuis longtemps au courant de ses intentions. C'est que Démarate, ancien roi de Sparte réfugié auprès de Xerxès, a appris l'existence de ce projet et décidé de transmettre l'information à Sparte (Livre VII, 239) : « il prit une tablette double, en gratta la cire, puis écrivit sur le bois même les projets de Xerxès ; ensuite il recouvrit de cire son message : ainsi le porteur d'une tablette vierge ne risquait pas d'ennuis ». Un autre passage de la même œuvre fait également référence à la stéganographie : au paragraphe 35 du livre V, Histiée incite son gendre Aristagoras, gouverneur de Milet, à se révolter contre son roi, Darius, et pour ce faire, « il fit raser la tête de son esclave le plus fidèle, lui tatoua son message sur le crâne et attendit que les cheveux eussent repoussé ; quand la chevelure fut redevenue normale, il fit partir l'esclave pour Milet ».

L'introduction de cette problématique dans les thèmes de recherches académiques doit beaucoup à G. Simmons et son problème des prisonniers (cf. [Sim84]). Simmons envisage le cas de deux prisonniers autorisés à échanger des messages authentifiés, mais non chiffrés. L'algorithme d'authentification est connu et le but des prisonniers est d'échanger des messages planifiant une évasion. Lors de la parution de [Sim84], la question des fuites d'information se posait déjà très fortement et le même auteur détaille dans [Sim98] la manière dont les États-Unis et l'Union soviétique, à la fin des années 1970, au cours de négociations sur un traité de non prolifération des armes nucléaires[1], se sont trouvés confrontés au problème de connaître très précisément quelles données pouvaient être émises par un détecteur. Les protagonistes étudiaient un dispositif devant permettre de détecter la présence de missiles dans les silos, sans révéler les emplacements de ces derniers. Parmi les contraintes imposées, il devait être impossible de modifier l'information émise et également impossible de transmettre plus que le strict nécessaire. Simmons explique, dans [Sim98], de quelle façon il a été amené à étudier ce dispositif et à constater qu'il était possible de transmettre une dizaine de bits sans que cela soit détectable. Ajoutons que cette forme particulière de stéganographie, la dissimulation de messages dans les communications authentifiées, est appelée canal subliminal.

Depuis, de nombreux intérêts, industriels notamment, ont poussé au développement du domaine de la dissimulation d'information. Ces intérêts ne sont pas, en général, directement tournés vers la stéganographie, mais vers des domaines proches, notamment le tatouage et le filigrane[2]. Le premier a pour objet de permettre l'identification de l'entité à l'origine du document, cela correspond au copyright. Des données sont insérées dans les documents, de manière plus ou moins discrète, l'essentiel étant de ne pas nuire à l'usage du document. Ces données doivent être difficiles à retirer. Plus précisément, réussir à les enlever doit aboutir à un document très dégradé. Toutes les copies d'un même document d'origine sont rigoureusement identiques. Tout comme le tatouage, le filigrane a également un but d'identification, mais il ne s'agit plus d'identifier l'émetteur : on souhaite marquer chaque copie distribuée de manière unique. Le filigrane joue donc le rôle de numéro de série. La principale contrainte reposant sur le filigrane est la résistance à la contrefaçon. L'accès à plusieurs copies, comportant chacune une marque différente, ne doit pas permettre de fabriquer une nouvelle copie avec une marque valide. Une copie ainsi formée doit permettre d'identifier au moins l'une des copies ayant servi à sa construction. Cela impose, comme pour le tatouage, une certaine robustesse de l'insertion des filigranes ainsi qu'une importante furtivité.

La stéganographie présente donc un point commun important avec le tatouage et le filigrane : on dispose d'un document et on souhaite y incorporer une information additionnelle sans détériorer de manière notable le document d'origine. Les techniques intervenant lors de cette insertion varient donc très peu d'un domaine à l'autre. Cependant, le cahier des charges de la stéganographie diffère légèrement de celui du tatouage ou du filigrane :

---

[1] Strategic arms limitations talks two (SALT 2), traité qui n'a pas été ratifié.

[2] Nous avons choisi de traduire ainsi respectivement *watermarking* et *fingerprinting*. Signalons que le terme « filigrane » est parfois employé pour *watermarking*.

la dissimulation tient une place plus centrale tandis que d'autres propriétés ne sont pas requises.

Contrairement aux chiffrements, qui s'appliquent sans réserve à tout type de données – bien qu'il soit raisonnable d'être précautionneux avec ce que l'on chiffre –, les algorithmes stéganographiques sont tributaires du format des documents dans lesquels doit avoir lieu l'insertion. Le document d'origine doit être modifié de manière indétectable, ce qui implique de se restreindre à des zones particulières, qui dépendent naturellement du type de document. Le cadre dans lequel nous nous plaçons, et que nous détaillons au chapitre 7, s'applique aux images, en noir et blanc ainsi qu'en couleurs. Nous verrons qu'il est également possible d'appliquer notre approche à tout type de document comportant une partie « relativement » aléatoire.

Tout au long de cette partie, nous abordons la dissimulation d'information par ses liens avec les codes de recouvrement de l'espace de Hamming. Nous modélisons l'adversaire auquel nous sommes confronté de deux manières. Dans un premier temps, au chapitre 8, nous considérons un adversaire passif, ne pouvant qu'observer les documents après insertion. Nous relions ce problème au recouvrement de l'espace de Hamming et utilisons cette équivalence pour construire des schémas asymptotiquement optimaux. Plusieurs schémas existants entrent dans le cadre de ce premier modèle, et nous consacrons le chapitre 9 à mettre explicitement à jour leur liens avec les recouvrements. Ensuite, au chapitre 10, nous introduisons un nouveau modèle, qui généralise le précédent et qui, jusqu'ici, n'avait pas été étudié : nous supposons l'adversaire capable de modifier légèrement les documents stéganographiés. La généralité du problème auquel nous nous ramenons, un mélange de recouvrement et de correction d'erreurs, aboutit presque naturellement à des résultats moins favorables qu'avec un adversaire passif. Toutefois, nous donnons une construction qui, à défaut d'être optimale, est asymptotiquement bonne.

Chapitre 7

Position du problème

Le terme « stéganographie » recouvre un large domaine où la préoccupation centrale est la dissimulation de l'existence d'un message. Lorsque deux entités souhaitent échanger secrètement des messages, deux approches peuvent être envisagées : la première consiste à faire usage de la cryptographie, donc à rendre les messages inintelligibles à autrui ; l'autre, celle suivie par la stéganographie, essaie de tromper autrui en prenant l'apparence de messages anodins. L'approche choisie peut dépendre du contexte dans lequel a lieu la communication : le recours au chiffrement peut être interdit, ou bien les deux protagonistes peuvent vouloir dissimuler jusqu'à l'existence même de l'échange de messages confidentiels. Nous présentons dans ce chapitre une formalisation de ce problème ainsi que le cas particulier que nous étudions et le champ d'application correspondant.

7.1 Cadre général

Un schéma de dissimulation se compose d'un couple d'applications, que nous noterons I et E, servant respectivement à insérer et à extraire les messages, les deux dépendant d'une clef secrète. L'application d'insertion s'applique à un document anodin $\mathbf{v} \in \mathcal{U}$, à un message $\mathbf{x} \in \mathcal{M}$ ainsi qu'à une clef $\mathbf{k} \in \mathcal{K}$, pour donner un document stéganographié $\mathbf{s} \in \mathcal{S}$. L'application E extrait le message dissimulé dans un document, et est par conséquent définie sur $\mathcal{S} \times \mathcal{K}$ et prend ses valeurs dans $\mathcal{M}$. Nous avons donc

1. $\mathrm{I} : \mathcal{U} \times \mathcal{M} \times \mathcal{K} \longrightarrow \mathcal{S}$;
2. $\mathsf{E} : \mathcal{S} \times \mathcal{K} \longrightarrow \mathcal{M}$;
3. et surtout,

$$\forall(\mathbf{v}, \mathbf{x}, \mathbf{k}) \in \mathcal{U} \times \mathcal{M} \times \mathcal{K}, \quad \mathsf{E}(\mathrm{I}(\mathbf{v}, \mathbf{x}, \mathbf{k}), \mathbf{k}) = \mathbf{x} \ ,$$

cette dernière propriété signifiant qu'il est possible de retrouver l'information $\mathbf{x}$, dissimulée par I dans le mot $\mathbf{v}$, à l'aide de l'application E, lorsque l'on connaît la clef $\mathbf{k}$ utilisée.

Le problème à résoudre est de rendre les documents stéganographiés indistinguables de documents originaux, non modifiés. Dans les faits, l'exigence est plus forte : on souhaite rendre $\mathbf{s} = \mathrm{I}(\mathbf{v}, \mathbf{x}, \mathbf{k})$ indistinguable du document original $\mathbf{v}$ et non simplement d'un élément quelconque de $\mathcal{U}$.

Sous ce problème se cache la nécessité de définir ce que l'on entend par « indistinguable ». Formellement, il est possible de recourir à la théorie de l'information comme l'ont fait Cachin et Mittelholzer, respectivement dans [Cac04] et [Miz99], ou encore d'utiliser la théorie de la complexité à la manière de Katzenbeisser et Petitcolas dans [KP02]. Toutefois, ces approches sont surtout destinées à fournir un cadre formel pour définir la sécurité des systèmes stéganographiques et ne possèdent pas d'intérêt pratique lorsque l'on dispose d'un document $\mathbf{s}$ et que l'on souhaite quantifier l'écart avec un autre document $\mathbf{v}$.

D'autre part, il est clair que la nature du document est à prendre en compte pour essayer de définir cette notion. En d'autres termes, il convient d'avoir une description précise des ensembles $\mathcal{U}$ et $\mathcal{S}$. Or ne serait-ce que pour la dissimulation d'information au sein d'images, on ne sait pas décrire formellement $\mathcal{U}$, pour la simple raison qu'on ne possède pas de définition de l'image.

7.2 Modèle adopté

Dans l'intégralité de cette seconde partie, les ensembles $\mathcal{U}$ et $\mathcal{S}$ seront pour nous des ensembles de mots binaires de longueur n, donc

$$\mathcal{U} = \mathcal{S} = \mathbb{F}^n \ ,$$

où $\mathbb{F}$ désigne le corps fini à deux éléments. Une mesure naturelle de l'écart entre deux documents, donc ici entre deux mots binaires, est alors la distance de Hamming. L'utilisation de cette métrique se traduit par le fait que toutes les coordonnées d'un mot seront susceptibles d'être modifiées pour qu'on puisse effectuer l'insertion de messages.

D'autre part, on peut, sans restriction, supposer que l'ensemble $\mathcal{M}$ des messages possibles est une partie $\mathbb{F}^r$. Et, pour simplifier, nous prendrons même $\mathcal{M} = \mathbb{F}^r$ lorsque nous construirons des schémas.

Enfin, bien que les schémas doivent dépendre d'une clef secrète, pour respecter le second principe de Kerckhoffs (cf. [Ker83, §II, p. 12]), nous ne ferons pas mention explicite de cette dernière. Usuellement, cette clef sert à construire une permutation utilisée pour le choix de l'ordre dans lequel les bits sont modifiés ; dans certains cas, elle sert également à chiffrer l'information. L'ajout d'une clef aux systèmes que nous présentons est alors simple, puisque pour nous les documents sont des mots binaires où toutes les coordonnées sont modifiables : les coordonnées peuvent être permutées en fonction d'une clef avant l'insertion, et le message peut être inséré non pas directement dans le mot permuté, mais dans la somme coordonnée par coordonnée de ce mot et d'un masque dérivé de la clef. Ces techniques sont classiques et nous les laissons hors de notre champ d'investigation en renvoyant à [KP99, chap. 2] pour une présentation complète.

Formellement, nous retiendrons donc la définition suivante pour un schéma de dissimulation :

DÉFINITION 7.1 *Un schéma de dissimulation permettant de dissimuler des messages de l'ensemble* $\mathcal{M} \subset \mathbb{F}^r$ *dans des mots binaires de longueur* n *en modifiant au plus* T *coordonnées est un couple de fonctions* I *et* E*, vérifiant*

1. $I : \mathbb{F}^n \times \mathcal{M} \longrightarrow \mathbb{F}^n$;
2. $E : \mathbb{F}^n \longrightarrow \mathcal{M}$;
3. $\forall(\mathbf{v}, \mathbf{x}) \in \mathbb{F}^n \times \mathcal{M}, \quad E(I(\mathbf{v}, \mathbf{x})) = \mathbf{x}$;
4. $\forall(\mathbf{v}, \mathbf{x}) \in \mathbb{F}^n \times \mathcal{M}, \quad d_H(\mathbf{v}, I(\mathbf{v}, \mathbf{x})) \leq T$.

La longueur n*, le cardinal* $|\mathcal{M}|$ *et la distorsion maximale* T *constituent les paramètres du schéma, ce que nous noterons* $(n, |\mathcal{M}|, T)$*. Les applications* I *et* E *sont respectivement appelées applications d'insertion et d'extraction.*

Notre problème est alors, pour une longueur n donnée, d'essayer de maximiser le nombre de messages dissimulables lorsque la distorsion maximale T est fixée. Nous verrons aux chapitres 8 et 10 comment il est possible de relier notre problème de dissimulation à des problèmes connus de théorie des codes, et comment exploiter cette relation pour construire de nouveaux schémas.

7.3 État de l'art

Le choix du modèle adopté à la définition 7.1, contrairement à ce qui pourrait sembler de prime abord, n'est pas une restriction drastique, mais va au contraire nous permettre d'englober plusieurs travaux sur la dissimulation dans les images en noir et blanc, à savoir [WL98, WTL00, PCT00, TP01, TP02, Hio03]. Dans ce contexte, une image en noir et blanc est simplement perçue comme un mot binaire de longueur n, et réciproquement on considère, sans aucune restriction, que tout mot binaire représente une image. Limiter le nombre de bits changés lors de l'insertion est alors clairement nécessaire, bien qu'il ne s'agisse dans la pratique que d'une première contrainte comme nous le verrons avec les schémas présentés dans [PCT00, TP01, TP02, Hio03]. De plus, certains travaux sur les images en couleurs rentrent également dans ce cadre (cf. [CJL+03, CJL+04, Wes01]). Certes, contrairement aux cas des travaux précédemment cités, l'image n'est plus assimilée à un mot binaire, mais une sous-partie de cette dernière va correspondre à un mot de $\mathbb{F}^n$.

De manière générale, lorsque l'on souhaite dissimuler de l'information dans un document, on recherche, dans ce document, une partie qui ressemble à de l'aléa. Cette partie peut alors être considérée comme un mot binaire où chaque bit est susceptible d'être changé pour dissimuler de l'information, le reste du document étant inchangé. Dans la mesure où cette partie ressemble à de l'aléa, on pourrait supposer qu'il n'est pas nécessaire de se restreindre sur l'ampleur des modifications et qu'on peut s'autoriser à réécrire toutes les coordonnées. Pourtant, si en première approximation on considère traiter de l'aléa, il ressort rapidement que ce dernier est de piètre qualité et qu'il ne faut pas le modifier trop fortement sous peine d'être aisément détectable, comme le montrent par exemple les analyses de Chandramouli et Memon dans [CM01] et de Fridrich, Goljan et Du dans [FGD01]. Cela justifie le maintient de notre restriction sur le nombre de modifications introduites par la dissimulation, non seulement pour les schémas destinés aux images en noir et blanc, mais également pour ceux traitant des images en couleurs.

Ainsi, nous pourrons également appliquer nos constructions aux images en couleurs, en ne prenant en considération que des parties bien choisies. Par exemple K. Chang, C. Jung, K. Lee, S. Lee et H. Yoo, dans [CJL$^+$03], considèrent une représentation spatiale des images en couleurs, dans laquelle chaque point de l'image est codé par un vecteur d'octets décrivant ce point relativement à une base de décomposition des couleurs (par exemple un codage Rouge-Vert-Bleu, Cyan-Magenta-Jaune-Noir ou encore Teinte-Saturation-Luminance). En assimilant l'ensemble des bits de poids faibles des coordonnées de ces vecteurs à un mot binaire, nous pouvons retrouver leur schéma, comme nous le verrons au chapitre 9. Il est également possible d'appliquer la même démarche à une représentation fréquentielle, dans laquelle on considère l'image après une transformation de Fourier. Autrement dit, l'image est alors décrite par une série de coefficients correspondant à une décomposition sur une base de fonctions. Les bits de poids faible de certains coefficients de cette transformée (choisis selon un modèle psycho-visuel destiné à réduire la visibilité à l'œil nu des changements effectués) joueront le rôle de mots binaire. Il faut préciser que Westfeld, en mettant à profit une remarque de Crandall (voir [Cra98]), utilise cette approche dans [Wes01] sous le nom d'encodage matriciel. Il obtient ainsi un schéma qui est un cas particulier de la construction que nous donnons au chapitre suivant.

Chapitre 8

Modèle avec adversaire passif

Nous commençons notre étude en nous préoccupant uniquement de la dissimulation : notre seule contrainte est donc de minimiser le nombre de modifications nécessaire à l'insertion des messages. Dans ce modèle, que nous appellerons à adversaire passif, les schémas de dissimulation sont proches des codes de recouvrement. Nous allons préciser ce lien, ce qui nous conduira à une borne sur la capacité maximale que peut avoir un schéma et nous donnera un moyen de construire des schémas optimaux atteignant cette limite.

8.1 Problème équivalent

Le problème de l'existence d'un schéma de dissimulation ayant les paramètres (n, M, T) se relie à un problème d'existence de recouvrements de l'espace de Hamming $\mathbb{F}^n$. Un code de recouvrement de rayon ρ de $\mathbb{F}^n$ pour la métrique de Hamming est un code binaire $\mathcal{C}$ tel que tout mot $\mathbf{v} \in \mathbb{F}^n$ soit à une distance de Hamming au plus ρ de $\mathcal{C}$, soit

$$\begin{aligned} d_H(\mathbf{v}, \mathcal{C}) &= \min_{\mathbf{c} \in \mathcal{C}} d_H(\mathbf{v}, \mathbf{c}) \\ &= \min_{\mathbf{c} \in \mathcal{C}} |\{i : v_i \neq c_i\}| \\ &\leq \rho \ . \end{aligned}$$

Nous noterons $(n, |\mathcal{C}|)\rho$ les paramètres d'un tel recouvrement. Lorsque $\mathcal{C}$ est linéaire, son cardinal est de la forme $|\mathcal{C}| = 2^k$, où k est la dimension du code, et nous utiliserons la notation $[n, k]\rho$.

L'application d'extraction E des schémas permet de mettre en lumière la relation existant avec les codes de recouvrement. Considérons un ensemble $E^{-1}(\{\mathbf{x}\})$, où $\mathbf{x}$ est un message dissimulable quelconque, et soit $\mathbf{v}$ un mot quelconque de longueur n. Le schéma étant par hypothèse de distorsion maximale T, cela implique qu'il existe un mot $\mathbf{s}$ vérifiant $E(\mathbf{s}) = \mathbf{x}$ et qui de plus est à une distance de Hamming de $\mathbf{v}$ inférieure ou égale à T. Or l'égalité

$E(\mathbf{s}) = \mathbf{x}$ implique $\mathbf{s} \in E^{-1}(\{\mathbf{x}\})$. En conclusion, l'ensemble $E^{-1}(\{\mathbf{x}\})$ est donc un code de recouvrement de rayon T. Plus précisément, on a :

THÉORÈME 8.1 *Un schéma de dissimulation de paramètres* (n, M, T) *est équivalent à un ensemble de* M *codes de recouvrement, de longueur* n *et de rayon* T*, deux à deux disjoints, dont la réunion est égale à* $\mathbb{F}^n$*.*

PREUVE. Considérons les ensembles $E^{-1}(\{\mathbf{x}\})$, où $\mathbf{x}$ désigne un message dissimulable. Nous avons déjà vu que ces ensembles sont bien des recouvrements de rayon T. Par définition, les ensembles $E^{-1}(\{\mathbf{x}\})$ et $E^{-1}(\{\mathbf{x}'\})$ sont disjoints si et seulement si $\mathbf{x} \neq \mathbf{x}'$. La réunion des $E^{-1}(\{\mathbf{x}\})$ est égale à $\mathbb{F}^n$ car la définition 7.1 page 113 d'un schéma impose à l'application d'extraction d'être définie sur $\mathbb{F}^n$. Pour la réciproque, considérons une famille $\{\mathcal{C}_i\}$ de M recouvrements vérifiant les hypothèses du théorème. Définissons l'application E par

$$E(\mathbf{s}) = \mathbf{i}$$

si $\mathbf{s} \in \mathcal{C}_i$ avec $\mathbf{i}$ représentant l'écriture en base 2 de i. Les $\mathcal{C}_i$ formant une partition de $\mathbb{F}^n$, cette application est bien définie. Les $\mathcal{C}_i$ étant des recouvrements de rayon T, il est possible de définir une application I, qui à un mot $\mathbf{v}$ et un message $\mathbf{i}$ associe un mot $\mathbf{s} \in \mathcal{C}_i$ tel que $d_H(\mathbf{v}, \mathbf{s}) \leq T$. $\square$

COROLLAIRE 8.2 *L'existence d'un schéma de dissimulation de paramètres* (n, M, T) *implique l'existence d'un code de recouvrement de longueur* n *et de rayon* T *dont le cardinal est supérieur où égal à* $2^n/M$*.*

PREUVE. Il suffit pour cela de considérer l'ensemble $E^{-1}(\{\mathbf{y}\})$ de cardinal maximal. En effet, la réunion de tous les $E^{-1}(\{\mathbf{x}\})$ étant d'une part disjointe et d'autre part égale à $\mathbb{F}^n$, il en existe au moins un dont le cardinal est supérieur ou égal à $2^n/M$. $\square$

8.2 CONSTRUCTION PAR DES CODES DE RECOUVREMENT LINÉAIRES

Afin de construire des schémas, nous devons construire des recouvrements disjoints dont la réunion soit l'espace tout entier, $\mathbb{F}^n$. Une solution consiste à utiliser des codes de recouvrement linéaires. Les translatés de ces derniers sont disjoints et leur réunion nous donne bien l'espace $\mathbb{F}^n$. Si le code $\mathcal{C}$ est de dimension k et de longueur n, alors il admet 2^{n-k} translatés disjoints, ce qui signifie que le schéma sera de paramètres $(n, 2^{n-k}, \rho)$, où ρ désigne le minimum des rayons de recouvrement des translatés de $\mathcal{C}$. Or le rayon de recouvrement a la propriété d'être invariant par translation : si le code $\mathcal{C}$ est de rayon de recouvrement ρ, alors tous ses translatés sont également de rayon ρ.

Proposition 8.3 *Soient* $\mathcal{C}$ *un code de rayon de recouvrement* ρ *et* $\mathbf{e}$ *un mot quelconque. Alors le translaté* $\mathbf{e}+\mathcal{C}=\{\mathbf{e}+\mathbf{c} \mid \mathbf{c}\in\mathcal{C}\}$ *est un recouvrement de rayon* ρ.

Preuve. Soit $\mathbf{v}$ un mot. Nous cherchons à prouver qu'il existe un mot $\mathbf{s}\in\mathbf{e}+\mathcal{C}$ à une distance de Hamming inférieure à ρ. Le code étant de rayon ρ, il existe un mot de code $\mathbf{c}$ tel que $\mathrm{d_H}(\mathbf{c},\mathbf{v}-\mathbf{e})\leq\rho$. Or

$$\begin{aligned}\mathrm{d_H}(\mathbf{c},\mathbf{v}-\mathbf{e}) &= \mathrm{w_H}(\mathbf{c}-(\mathbf{v}-\mathbf{e}))\\ &= \mathrm{w_H}((\mathbf{c}+\mathbf{e})-\mathbf{v})\\ &= \mathrm{d_H}(\mathbf{c}+\mathbf{e},\mathbf{v})\end{aligned}$$

Il suffit donc de prendre $\mathbf{s}=\mathbf{c}+\mathbf{e}$. Pour prouver que ρ est bien le rayon de recouvrement, et non un simple majorant, il suffit de considérer un mot $\mathbf{v}$ à distance maximale de $\mathcal{C}$, le mot $\mathbf{v}-\mathbf{e}$ est alors à une distance ρ de $\mathbf{e}+\mathcal{C}$, ce qui conclut la preuve. □

Ainsi, un code linéaire de paramètres $[n,k]\rho$ permet de construire un schéma $(n,2^{n-k},\rho)$.

Examinons maintenant la manière dont nous pouvons définir les applications d'extraction et d'insertion. Le théorème 8.1 incite à faire correspondre message et appartenance à l'un des translatés de $\mathcal{C}$. Autrement dit, tous les mots $\mathbf{s}$ appartenant à un même translaté dissimulent la même information. Or l'appartenance à un translaté donné est simple à caractériser pour des codes linéaires grâce à la notion de syndrome : tous les mots de $\mathbf{s}+\mathcal{C}$ ont le même syndrome que $\mathbf{s}$. Donc, en notant $\mathcal{H}$ une matrice de parité de $\mathcal{C}$, on peut alors définir E par

$$\mathsf{E}(\mathbf{s})=\mathbf{s}\cdot\mathcal{H}^t\ .$$

L'application d'extraction E est donc simplement le calcul du syndrome. Elle est donc linéaire et à $\mathcal{C}$ pour noyau. Un code linéaire admettant plusieurs matrices de parités, il existe différentes manières de définir E. Cependant, les propriétés qui nous intéressent ne dépendent pas d'un choix particulier ; il importe seulement de conserver la même matrice de parité pour un même schéma.

Dans ce type de schéma, l'insertion d'un message $\mathbf{x}$ dans un mot $\mathbf{v}$ consiste à trouver un mot $\mathbf{s}$ dont le syndrome est $\mathbf{x}$ qui soit à une distance inférieure où égale à ρ de $\mathbf{v}$. Un idée naturelle pour définir l'application d'insertion I est alors d'effectuer un décodage de $\mathbf{v}$ dans $\mathcal{C}$. Notons $\mathbf{c}$ le mot résultant de ce décodage. Par définition d'un mot de code, son syndrome est nul. Il suffit donc d'ajouter un mot $\mathbf{e}$ dont le syndrome est $\mathbf{x}$. La proposition suivante complète cette approche.

Proposition 8.4 *Soit* $\mathcal{C}$ *un code binaire linéaire de longueur* n *et de dimension* k. *Notons* $\mathcal{H}$ *une matrice de parité de ce code. Le rayon de recouvrement* *de $\mathcal{C}$ est égal à ρ si et seulement si pour tout mot* $\mathbf{x} \in \mathbb{F}^{n-k}$ *il existe un mot* $\mathbf{e} \in \mathbb{F}^n$ *de poids au plus* ρ.

PREUVE. Soit $\mathbf{x} \in \mathbb{F}^{n-r}$. L'application $\mathbf{v} \mapsto \mathbf{v} \cdot \mathcal{H}^t$ étant surjective, il existe $\mathbf{v}$ tel que $\mathbf{v} \cdot \mathcal{H}^t = \mathbf{x}$. Or $\mathcal{C}$ a un rayon de recouvrement égal à ρ, ce qui signifie qu'il existe $\mathbf{c} \in \mathcal{C}$ vérifiant $d_H(\mathbf{v}, \mathbf{c})$. Le mot $\mathbf{e} = \mathbf{v} - \mathbf{c}$ est par conséquent de poids au plus ρ et son syndrome est $\mathbf{x}$. Nous avons donc prouvé que l'image par l'application $\mathbf{v} \mapsto \mathbf{v} \cdot \mathcal{H}^t$ de l'ensemble des mots de poids au plus ρ est l'espace $\mathbb{F}^{n-r}$. Pour obtenir la réciproque, considérons un mot $\mathbf{v}$ de syndrome $\mathbf{x} = \mathbf{v} \cdot \mathcal{H}^t$. Il existe $\mathbf{e}$ de poids inférieur ou égal à ρ de syndrome $\mathbf{x}$. Le mot $\mathbf{v} - \mathbf{e}$ est de syndrome nul, donc est un élément du code $\mathcal{C}$ et a un poids au plus ρ, ce qui termine la preuve. $\square$

Si le code $\mathcal{C}$ considéré a un rayon de recouvrement ρ, alors d'une part, il existe $\mathbf{c} \in \mathcal{C}$ tel que $d_H(\mathbf{v}, \mathbf{c}) \leq \rho$ et d'autre part, d'après la proposition 8.4, il existe $\mathbf{e}$ tel que $w_H(\mathbf{e}) \leq \rho$ et $\mathbf{e} \cdot \mathcal{H}^t = \mathbf{x}$. Donc le mot $\mathbf{s} = \mathbf{c} + \mathbf{e}$ ainsi obtenu est à une distance de Hamming inférieure à 2ρ du mot d'origine $\mathbf{v}$. Nous avons donc construit un schéma de dissimulation $(n, 2^{n-k}, 2\rho)$ à partir d'un code linéaire de paramètres $[n, k]\rho$.

C'est malheureusement moins bon que ce qu'il est possible d'obtenir d'après le théorème 8.1. Il est toutefois possible d'améliorer l'application d'insertion en éliminant le décodage. Nous avons vu que les translatés sont tous de rayon ρ. Il est donc possible de choisir directement un mot $\mathbf{s}$ du translaté $\mathbf{e} + \mathcal{C}$, où $\mathbf{e} \cdot \mathcal{H}^t = \mathbf{x}$, tel que $d_H(\mathbf{s}, \mathbf{v}) \leq \rho$. La preuve de la proposition 8.3 nous donne même la marche à suivre : trouver un mot $\mathbf{c}$ du code dans une boule centrée sur le mot $\mathbf{v} - \mathbf{e}$ et de rayon égal au rayon de recouvrement de $\mathcal{C}$. Dans notre cas, le code étant linéaire, nous pouvons être encore plus précis : il nous suffit de trouver un mot $\mathbf{e}$ de poids au plus ρ dont le syndrome est $\mathbf{x} - \mathbf{v} \cdot \mathcal{H}^t$.

NOTATION 8.5 *Pour tout code $\mathcal{C}$ linéaire de paramètres* $[n, k]\rho$, *nous noterons* $D_{\mathcal{C}}$ *l'application de décodage de syndrome, qui à un mot* $\mathbf{x}$, *associe un mot* $\mathbf{e}$, *tel que* $w_H(\mathbf{e}) \leq \rho$ *et* $\mathbf{e} \cdot \mathcal{H}^t = \mathbf{x}$ *où $\mathcal{H}$ désigne une matrice de parité de $\mathcal{C}$. En l'absence d'ambiguïté sur $\mathcal{C}$, nous noterons simplement* D.

Avec cette notation, nous pouvons reformuler notre construction de la manière suivante :

PROPOSITION 8.6 *Soit $\mathcal{C}$ un code linéaire de paramètres* $[n, k]\rho$. *Le schéma de dissimulation défini par le couple d'applications*

$$
\begin{aligned}
\mathsf{E}(\mathbf{s}) &= \mathbf{s} \cdot \mathcal{H}^t \ , \\
\mathsf{I}(\mathbf{v}, \mathbf{x}) &= \mathbf{v} + \mathrm{D}(\mathbf{x} - \mathsf{E}(\mathbf{v})) \ ,
\end{aligned}
$$

est un schéma $(n, 2^{n-k}, \rho)$.

EXEMPLE 8.7 Considérons le code de Hamming binaire de longueur 7 qui admet pour matrice de parité

$$\mathcal{H} = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix} .$$

Le code de Hamming est de dimension 4 et de rayon de recouvrement 1. La construction de la proposition précédente nous donne donc un schéma $(7, 2^3, 1)$. Cela signifie qu'en changeant au plus une coordonnée dans un mot de 7 bits, on peut dissimuler 8 messages différents. Prenons

$$\mathbf{v} = (\begin{matrix} 1 & 1 & 0 & 0 & 1 & 0 & 0 \end{matrix})$$

et dissimulons le message $\mathbf{x} = (\begin{matrix} 1 & 1 & 1 \end{matrix})$. On a

$$\mathsf{E}(\mathbf{v}) = \mathbf{v} \cdot \mathcal{H}^t = (\begin{matrix} 0 & 1 & 1 \end{matrix}) .$$

Nous cherchons donc un mot $\mathbf{e}$ de syndrome

$$\mathbf{e} \cdot \mathcal{H}^t = \mathbf{x} - \mathsf{E}(\mathbf{v}) = (\begin{matrix} 1 & 0 & 0 \end{matrix}) .$$

Clairement, on peut prendre $\mathbf{e} = (\begin{matrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \end{matrix})$ et le mot $\mathbf{v} + \mathbf{e}$ vérifie bien $\mathsf{E}(\mathbf{v} + \mathbf{e}) = \mathbf{x}$ et $d_H(\mathbf{v} + \mathbf{e}, \mathbf{v}) \leq 1$.

En comparaison, la première approche suggérée nécessite un décodage de $\mathbf{v}$, ce qui donne

$$\mathbf{c} = (\begin{matrix} 1 & 1 & 0 & 0 & 1 & 1 & 0 \end{matrix}) .$$

Ensuite, il faut ajouter un mot $\mathbf{e}'$ dont le syndrome soit égal à $\mathbf{x}$. Le code de Hamming étant de rayon 1, il est possible de le prendre avec un poids au plus 1, en l'occurrence

$$\mathbf{e}' = (\begin{matrix} 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{matrix}) .$$

Finalement, le mot

$$\mathbf{s}' = \mathbf{e}' + \mathbf{c} = (\begin{matrix} 1 & 1 & 0 & 0 & 1 & 1 & 1 \end{matrix})$$

est à une distance 2 du mot d'origine. □

Cependant, l'exemple précédent est trompeur : contrairement à ce qui se passe pour le code de Hamming, de manière générale, résoudre le problème du décodage de syndrome est difficile. Plus précisément, le problème de décision sous-jacent au décodage de syndrome, qui s'énonce de la maniere suivante :

> Soient w un entier, $\mathcal{H}$ une matrice binaire $r \times n$ et $\mathbf{x} \in \mathbb{F}^r$. Existe-t-il un mot $\mathbf{e} \in \mathbb{F}^n$ de poids inferieur ou égal à w verifiant $\mathbf{e} \cdot \mathcal{H}^t = \mathbf{x}$?

est NP-complet. Ce résultat est dû à Berlekamp, McEliece et van Tilborg (cf. [BMT78]). Nous renvoyons également à [Bar98, §4], notamment aux théorèmes 4.1 et 4.6, pour une étude des problèmes de complexité en théorie des codes et à [GJ79] pour une étude générale. Ce résultat signifie que l'on est incapable de trouver une solution avec un algorithme déterministe et polynomial en n, bien qu'il soit possible de vérifier une solution par un algorithme de ce type. Or le problème que nous avons à résoudre pour le calcul de l'application $D_{\mathcal{C}}$ permettrait de répondre à ce problème de décision. Cela n'empêche en rien l'existence de cas particulier, tel le code de Hamming, où un algorithme déterministe et polynomial existe, mais il ne faut pas s'attendre à un algorithme générique. Cela a pour conséquence de rendre impraticable la plupart des schémas fondés sur la proposition 8.6 : plus précisément, on peut considérer qu'un tel schéma n'est utilisable que pour des codes $\mathcal{C}$ ayant un algorithme de décodage de syndrome déterministe et polynomial en la longueur du code.

8.3 Sécurité de la construction

La notion de sécurité d'un système stéganographique n'est pas simple à définir. Nous avons choisi, jusqu'ici, de retenir comme critère principal la modification introduite par l'insertion d'un message dans un mot, ce que nous mesurons par la distance de Hamming. Toutefois, d'autres tentatives pour définir la sécurité de tels systèmes ont eu lieu et nous allons nous intéresser à celle introduite par Cachin dans [Cac04], qui ne concerne que le modèle passif. Notre objectif est de montrer que notre construction de schémas fondés sur les recouvrements linéaires permet l'obtention de systèmes parfaitement sûrs au sens de Cachin.

La sécurité d'un système, telle qu'elle est envisagée dans la définition 1 de [Cac04], est fondée sur la similitude, probabiliste, des entrées et des sorties du système. Autrement dit, la source servant d'entrée possède une distribution de probabilité $\mathcal{P}_{\mathrm{e}}$. Avec cette distribution, la sortie du système suit la distribution $\mathcal{P}_{\mathrm{s}}$. La sécurité du système est alors mesurée par l'entropie relative, également appelée distance de Kullback-Leiber, de ces deux distributions :

$$\mathsf{D}(\mathcal{P}_{\mathrm{s}} \| \mathcal{P}_{\mathrm{e}}) = \sum_{\mathbf{v}} \mathcal{P}_{\mathrm{s}}(\mathbf{v}) \cdot \log\left(\frac{\mathcal{P}_{\mathrm{s}}(\mathbf{v})}{\mathcal{P}_{\mathrm{e}}(\mathbf{v})}\right) \quad .$$

Définition 8.8 ([Cac04, §2, déf. 1]) *Un système stéganographique est dit parfaitement, ou encore inconditionnellement, sûr contre les adversaires passifs, lorsqu'il existe une distribution $\mathcal{P}_e$ telle que*

$$\mathsf{D}(\mathcal{P}_s \| \mathcal{P}_e) = 0 \quad .$$

Cela signifie que l'on souhaite qu'aucun adversaire ne puisse différencier les deux distributions. Bien entendu, cette définition de la sécurité d'un système stéganographique est à mettre en parallèle avec celle d'un système de chiffrement telle qu'elle fut introduite par Shannon dans [Sha49, 2e partie, section 10].

Lorsque l'on applique la construction de la proposition 8.6 page 118 en prenant pour recouvrement un code de Hamming de longueur $n = 2^m - 1$, on obtient un système dont la sécurité est parfaite lorsque $\mathcal{P}_e$ est la distribution uniforme. En effet, la distribution $\mathcal{P}_s$ est alors également uniforme, et par conséquent indistinguable de $\mathcal{P}_e$. Notons S, V et X, trois variables aléatoires. La variable S suit la distributions $\mathcal{P}_s$ tandis que V et X ont une distribution uniforme. La variable X représente le message inséré, tandis que V et S représentent le mot d'origine et le résultat de la dissimulation. Nous supposerons que le message et le mot d'origine sont indépendants – cette hypothèse traduit simplement le fait que

autrement dit les variables V et X sont indépendantes. On a alors

$$P(S = \mathbf{s}) = \sum_{\mathbf{v} \in \mathbb{F}^n} P(S = \mathbf{s} \mid V = \mathbf{v}) \cdot P(V = \mathbf{v}) \ .$$

Or la probabilité $P(S = \mathbf{s} | V = \mathbf{v})$ vaut zéro si $\mathbf{v}$ n'est pas dans la boule fermée de rayon 1, centrée sur $\mathbf{s}$, $\mathbf{v} \notin B_1(\mathbf{s})$, puisque le schéma considéré change au plus une coordonnée pour effectuer l'insertion. Donc,

$$\begin{aligned} P(S = \mathbf{s}) &= \sum_{\mathbf{v} \in B_1(\mathbf{s})} P(S = \mathbf{s} \mid V = \mathbf{v}) \cdot P(V = \mathbf{v}) \\ &= \sum_{\mathbf{v} \in B_1(\mathbf{s})} P\left(X = \mathbf{s} \cdot \mathcal{H}^t \mid V = \mathbf{v}\right) \cdot P(V = \mathbf{v}) \ . \end{aligned}$$

En effet, la probabilité d'avoir $S = \mathbf{s}$ sachant que $V = \mathbf{v}$ est égale à celle d'avoir à inserer le message $\mathbf{s} \cdot \mathcal{H}^t$ puisque une fois $\mathbf{v}$ fixé, il y a bijection entre messages et mots dans la boule de rayon 1. L'indépendance des variables X et V donnent alors

$$P(S = \mathbf{s}) = \sum_{\mathbf{v} \in B_1(\mathbf{s})} P\left(X = \mathbf{s} \cdot \mathcal{H}^t\right) \cdot P(V = \mathbf{v}) \ .$$

Par hypothèse, X et V suivent une distribution uniforme sur des espaces dont le cardinal vaut respectivement 2^m et 2^n, et d'autre part, rappelons que le cardinal d'une boule fermée de rayon 1 en dimension n vaut $n + 1$. Nous avons par conséquent

$$\begin{aligned} P(S = \mathbf{s}) &= (n + 1) \cdot \frac{1}{2^m} \cdot \frac{1}{2^n} \\ &= \frac{1}{2^n} \ . \end{aligned}$$

En d'autres termes, S suit également une distribution uniforme, et notre schéma est donc parfait lorsque $\mathcal{P}_e$, la distribution des mots en entrée, et $\mathcal{P}_m$, la distribution des messages à insérer, sont uniformes.

THÉORÈME 8.9 *Il existe des schémas de dissimulation, pouvant être obtenus par la construction de la proposition 8.6, dont la sécurité est inconditionnelle au sens de Cachin (cf. définition 8.8).*

Cette sécurité inconditionnelle pour les schémas construits avec des codes de Hamming repose essentiellement sur le fait que la probabilité $\mathsf{P}(\mathsf{S} = \mathbf{s} | \mathsf{V} = \mathbf{v})$ est égale à $\mathsf{P}\left(\mathsf{X} = \mathbf{s} \cdot \mathcal{H}^t\right)$, autrement dit sur l'existence d'un unique mot $\mathbf{s}$ pouvant dissimuler un message donné $\mathbf{x}$ dans un mot donné $\mathbf{v}$. Or, cette propriété exprime précisément le caractère parfait du code de Hamming : il y a unicité du décodage jusqu'au rayon de recouvrement, ce dernier étant égal à la capacité de correction. Ce qui est vrai pour les schémas reposant sur le code de Hamming est par conséquent tout aussi valable pour les autres codes parfaits. Malheureusement, cela ne concerne donc que le code de Golay binaire de longueur $n = 23$.

8.4 Borne sur la capacité

Notre objectif dans cette section et la suivante est d'obtenir des constructions de schémas asymptotiquement optimaux. Dans un premier temps, les relations mises à jour à la section 8.2, entre les schémas de dissimulation et les codes de recouvrement, nous servent à traduire les bornes sur les recouvrements en bornes, inférieures et supérieures, sur le nombre maximal de messages d'un schéma. Les bornes sur les recouvrements sont connues pour être atteintes par les recouvrements linéaires ; nous utiliserons ce résultat à la section suivante pour construire nos schémas.

Dans la mesure où un recouvrement linéaire $[n, k]\rho$ donne un schéma $(n, 2^{n-k}, \rho)$, une borne inférieure sur la redondance maximale – ou encore, ce qui est équivalent, sur la dimension minimale – des recouvrements de longueur n et de rayon ρ, conduit à une borne sur le nombre de messages. Notons $r_L(n, \rho)$ le maximum de la redondance pour les codes de recouvrement linéaires de longueur n et de rayon ρ et $m(n, \rho)$ le logarithme du cardinal maximal d'un schéma de longueur n ayant une distorsion maximale ρ. Nous avons donc $r_L(n, \rho) \leq m(n, \rho)$. D'autre part, un schéma (n, M, ρ) conduit à l'existence d'un recouvrement de longueur n, de rayon ρ et de cardinal supérieur ou égal à $2^n/M$, d'après la proposition 8.1. Donc, une borne supérieure sur la redondance maximale – de manière équivalente sur le cardinal minimal – d'un recouvrement de longueur n et de rayon ρ se traduit par une borne supérieure sur $m(n, \rho)$. En notant $r(n, \rho)$ la redondance maximale d'un code de longueur n et de rayon ρ, on a donc $m(n, \rho) \leq r(n, \rho)$.

PROPOSITION 8.10 *Posons*

$$m(n, \rho) = \log\left(\max_{\mathcal{S} \in \mathbf{S}(n,\rho)} |\mathcal{S}|\right)$$

où $\mathbf{S}(n, \rho)$ *désigne l'ensemble des schémas de longueur* n *ayant une distorsion maximale égale à* ρ. *Alors, nous avons*

$$r_L(n, \rho) \leq m(n, \rho) \leq r(n, \rho) \ .$$

COROLLAIRE 8.11 *Notons* V_ρ *le cardinal d'une boule fermée de rayon* ρ *en dimension* n, $V_\rho = \sum_{i=0}^{\rho} \binom{n}{i}$. *On a*

$$m(n, \rho) \leq \log(V_\rho) \ .$$

PREUVE. Il suffit d'appliquer la borne de Hamming (cf. [CHL$^+$97, chap. 6, §1, th. 6.1.2]), qui donne

$$r(n, \rho) \leq \log(V_\rho) \ ,$$

et de conclure avec la proposition précédente. □

Remarquons que le corollaire 8.11 peut également être obtenu directement. En effet, pour un schéma (n, M, ρ), dissimuler l'un des M messages possibles dans un mot $\mathbf{v}$ implique qu'on modifie $\mathbf{v}$ en au plus ρ coordonnées. Or, en modifiant un mot $\mathbf{v}$ de longueur n de cette manière, on obtient V_ρ mots différents, ce qui conduit à l'inégalité $M \leq V_\rho$.

Avant d'examiner le comportement asymptotique de cette borne, précisons qu'il existe des paramètres, avec une longueur finie, pour lesquels elle est atteinte : il s'agit des schémas construits à partir des codes de Hamming et de Golay donnant respectivement des schémas de paramètres $(2^m - 1, 2^{m+1}, 1)$, m entier superieur ou égal à 3, et $(23, 2^{11}, 3)$. Ces codes étant parfaits, ils atteignent, par définition, la borne de Hamming.

COMPORTEMENTS ASYMPTOTIQUES. Nous nous intéressons ici à deux cas. Considérons tout d'abord que le rapport ρ/n est fixé et que la longueur n tend vers l'infini. Un des intérêts de la borne donnée au précédent corollaire de la de la présente page est qu'il existe une majoration classique (voir [MS96, chap. 10, §11, cor. 9]) faisant intervenir la fonction d'entropie binaire, définie par $h(x) = -x \log(x) - (1 - x) \log(1 - x)$, à savoir

$$\log(V_\rho) \leq n \cdot h\left(\frac{\rho}{n}\right) \ .$$

Cette majoration, valable de manière générale pour $\rho/n < 1/2$, a également le bon goût d'être un équivalent asymptotique lorsque n tend vers l'infini et que le rapport ρ/n est fixé, autrement dit lorsque ρ croît linéairement avec n.

Considérons maintenant cas que ρ est fixé tandis que n tends vers l'infini. Dans ce cas, pour tout entier positif i, on a l'équivalent

$$\binom{n}{i} \sim \frac{n^i}{i!} ,$$

ce qui donne le développement suivant pour le majorant du corollaire 8.11 :

$$\log(V_\rho) = \rho \log(n) - \log(\rho!) + o(1) .$$

Asymptotiquement, nous avons donc la borne

$$m(n, \rho) \lesssim \rho \log(n) - \log(\rho!) .$$

En résumé,

PROPOSITION 8.12 *Asympotiquement, lorsque la longueur n tend vers l'infini, nous avons :*

1. *pour ρ/n fixé,*
$$m(n, \rho) \lesssim n \cdot h\left(\frac{\rho}{n}\right) ;$$
2. *pour ρ fixé,*
$$m(n, \rho) \lesssim \rho \log(n) - \log(\rho!) .$$

Nous allons voir à la section suivante que ces deux bornes sont fines. En d'autres termes, il existe des schémas dont les paramètres se rapprochent arbitrairement près de ces bornes.

8.5 Schémas asymptotiquement optimaux

Nous donnons des preuves d'existence de schémas optimaux pour les deux formes asymptotiques exposées à la proposition 8.12. Dans le premier cas, où le rapport ρ/n est fixé et où n tend vers l'infini, nous n'obtenons que l'existence, c'est-à-dire que cette preuve est non constructive ; mais pour le second cas, où ρ est fixé et n tend vers l'infini, nous montrons l'existence en proposant une construction effective.

Lorsque le rapport ρ/n est fixé, la redondance maximale des recouvrements linéaires atteint la borne $h(\rho/n)$.

THÉORÈME 8.13 ([DP86, TH. 3]) *Soit un nombre réel $\alpha < 1/2$ fixé. Il existe une suite $(\mathcal{C}_n)$ de codes de recouvrement linéaires, de paramètres $[n, n-r_n]\rho_n$, avec n tendant vers l'infini, tels que $\rho_n = \lfloor \alpha \cdot n \rfloor$ et que leur redondance vérifie*

$$h(\alpha) - O\left(\frac{\log(n)}{n}\right) \le \frac{r_n}{n} \le h(\alpha) .$$

En termes de schéma, cela signifie grâce à la proposition 8.6, que pour tout $\alpha < 1/2$ et quel que soit $\epsilon > 0$, il existe une longueur n telle que l'on puisse avoir un schéma de paramètres $(n, 2^{n\cdot(h(\alpha)-\epsilon)})\rho$ avec $\rho = \lfloor n \cdot \alpha \rfloor$, ce qui règle le premier cas. Le théorème précédent permet, bien entendu, de quantifier plus finement l'écart par rapport à la borne supérieure, mais il y a beaucoup plus intéressant. En fait, on sait que la quasi-totalité des recouvrements linéaires ont une redondance qui atteint asymptotiquement la borne $n \cdot h(\rho/n)$. Plus formellement,

THÉORÈME 8.14 ([BLI90]) *Soit un nombre réel* $\alpha < 1/2$ *fixé. La fraction des codes linéaires, de rayon* $\lfloor \alpha \cdot n \rfloor$ *et de longueur* n*, dont la redondance* r *vérifie*

$$h\,(\alpha) - O\left(\frac{\log(n)}{\sqrt[3]{n}}\right) \leq \frac{r}{n}$$

est supérieure à $1 - 2^{-n\cdot\log(n)}$.

Précisons qu'un résultat semblable, dû à Delsarte et Piret dans [DP86, th. 2], est également vrai pour les recouvrements dans le cas général, et pas uniquement pour ceux ayant la propriété d'être linéaires (pour une synthèse de ces résultats, voir [CHL$^+$97, chap. 12, §1 et §3]). La conséquence importante pour nous est que presque tous les schémas fondés sur les recouvrements linéaires sont optimaux. Pour une « construction », il suffit de prendre un code linéaire au hasard. Le schéma associé est alors proche de l'optimal avec une grande probabilité.

Bien que cette version de la borne soit fine, il est décevant de ne pas avoir de construction effective de schémas ayant de tels paramètres. Certes, les probabilités sont favorables. Il est donc possible de prendre une matrice de parité au hasard. Mais il reste à vérifier que le rayon de recouvrement est bien celui espéré. Le second cas asymptotique est plus clément ; en effet, il est possible de donner une construction totalement effective de schémas optimaux. Cela repose sur deux éléments : d'une part l'existence de codes parfaits et d'autre part la somme directe. Commençons par rappeler cette dernière.

THÉORÈME 8.15 *Soient* $\mathcal{C}_1$ *et* $\mathcal{C}_2$ *des recouvrements de paramètres respectifs* $[n_1, k_1]\rho_1$ *et* $[n_2, k_2]\rho_2$*. Leur somme directe, définie par*

$$\mathcal{C} = \left\{(\mathbf{c}_1, \mathbf{c}_2) \;\middle|\; \mathbf{c}_1 \in \mathcal{C}_1 \quad et \quad \mathbf{c}_2 \in \mathcal{C}_2\right\} \ ,$$

a pour paramètres $[n_1 + n_2, k_1 + k_2]\rho_1 + \rho_2$.

Lorsque cette construction est utilisée avec ρ codes de Hamming de paramètres $[2^r - 1, 2^r - r - 1]1$, on obtient donc un recouvrement de longueur $\rho(2^r - 1)$, de dimension $\rho(2^r - r - 1)$ et de rayon ρ. Le schéma associé est donc de longueur $\rho(2^r - 1)$, de distorsion maximale ρ et peut dissimuler $2^{\rho\cdot r}$

messages différents. Pour une distorson maximale ρ fixée, et r tendant vers l'infini, le logarithme en base 2 du nombre de messages donne

$$\rho \log\left(\frac{n}{\rho}+1\right) \sim \rho\log(n) - \rho\log(\rho) \ ,$$

où $n = \rho(2^r - 1)$. En comparaison, rappelons que la borne supérieure correspondante sur m donnée à la proposition 8.12 est

$$m(\rho, n) \lesssim \rho\log(n) - \log(\rho!) \ .$$

La différence est donc d'au plus $\rho\log(e)$. Ainsi, non seulement cette différence est négligeable devant $m(n, \rho)$, mais surtout elle est constante.

Exemple 8.16 En appliquant cette construction à trois codes de Hamming $[7,4]1$, on obtient la matrice

$$\mathcal{H} = \begin{pmatrix} 1&0&1&0&1&0&1 & & & & & & & & & & & & & & \\ 0&1&1&0&0&1&1 & & & & & & & & & & & & 0 & & \\ 0&0&0&1&1&1&1 & & & & & & & & & & & & & & \\ & & & & & & & 1&0&1&0&1&0&1 & & & & & & & \\ & & & & & & & 0&1&1&0&0&1&1 & & & & & & & \\ & & & & & & & 0&0&0&1&1&1&1 & & & & & & & \\ & & & & & & & & & & & & & & 1&0&1&0&1&0&1 \\ & & & 0 & & & & & & & & & & & 0&1&1&0&0&1&1 \\ & & & & & & & & & & & & & & 0&0&0&1&1&1&1 \end{pmatrix} .$$

Considérons le mot

$$\mathbf{v} = \begin{pmatrix} 1&1&0&0&0&1&0&0&1&1&0&1&0&1&0&0&0&1&1&0&1 \end{pmatrix} .$$

Son syndrome est

$$\begin{pmatrix} 1&0&1&1&1&0&0&1&1 \end{pmatrix} .$$

Si on souhaite dissimuler le message $\mathbf{x} = \begin{pmatrix} 1&1&1&1&1&1&1&1&1 \end{pmatrix}$, on peut prendre

$$\mathbf{e} = \begin{pmatrix} 0&1&0&0&0&0&0&0&0&0&1&0&0&0&1&0&0&0&0&0&0 \end{pmatrix} .$$

Le mot à transmettre

$$\begin{aligned} \mathbf{s} &= \mathbf{v} + \mathbf{e} \\ &= \begin{pmatrix} 1&0&0&0&0&1&0&0&1&1&1&1&0&1&1&0&0&1&1&0&1 \end{pmatrix} \end{aligned}$$

a alors pour syndrome $\mathbf{x}$ et est à une distance 3 de $\mathbf{v}$. $\square$

8.6 Relation avec l'écriture sur les mémoires

Les problèmes de recouvrements auxquels nous avons affaire pour construire des schémas de dissimulation sont semblables à certains problèmes d'écriture sur des mémoires avec contraintes. D'abord introduite par Rivest et Shamir [RS82] pour les mémoires non effaçables (voir également [CHL$^+$97, chap. 17]), l'écriture sur les mémoires a connu de nombreuses variantes. Le principe général est d'encoder l'information devant être stockée sur la mémoire. Nous renvoyons à [CHL$^+$97] pour une étude detaillée.

Dans notre contexte, trois variantes sont pertinentes : les mémoires non effaçables, les mémoires à écritures limitées et la combinaison des deux[1].

La première variante, qui est en fait le problème original auquel s'interessent Rivest et Shamir, cherche à maximiser le nombre de fois que l'on peut utiliser une mémoire sur laquelle seul le passage du bit 0 au bit 1 est autorisé, l'état de départ étant le mot tout à zéro. La seconde autorise tous les changements mais restreint leur nombre. L'objectif est alors d'encoder le plus de messages possible sur un nombre de bits donné. Et enfin, la dernière est celle motivant l'étude de [BP99] que nous retrouverons au chapitre 10.

La seconde variante correspond à notre modèle à adversaire passif et a été étudiée dans [Fel85]. D'une certaine manière, la première variante s'y rattache. En effet, dans l'écriture sur les mémoires non effaçables, on a tout intérêt à minimiser le nombre de bits utilisés à chaque écriture. Cohen, Godlewski et Merkx donnent dans [CGM86] un encodage des messages pour cette variante. Il repose sur l'utilisation des translatés d'un code linéaire pour encoder les messages devant être stockés, ce que les auteurs appellent l'*encodage par translatés* – cela correspond donc à l'utilisation que nous faisons des translatés à la section 8.2 et à l'encodage matriciel de Westfeld (voir section 9.4, 137).

Certains des résultats que nous avons présentés dans ce chapitre peuvent donc être obtenus en réutilisant les travaux déjà effectués sur les mémoires : notre borne supérieure sur le nombre de messages, donnée au corollaire 8.11, peut se déduire de [CHL$^+$97, Th. 18.4.1]. Il est également possible de déduire l'optimalité de sa version asymptotique pour ρ/n fixé à partir de [CHL$^+$97, Th. 18.5.4]. En revanche, lorsque ρ est fixé et que n tend vers l'infini, nos résultats sont nouveaux.

En résumé, nous avons vu, dans ce chapitre sur l'adversaire passif, à quel type de problème était reliée la construction de schémas de dissimulation. L'équivalence obtenue avec un problème de recouvrement nous a permis d'une part de borner le nombre de messages possibles pour un nombre donné de modifications du mot d'origine et d'autre part de donner des schémas asymptotiquement optimaux qui reposent en grande partie sur l'existence

[1]Nous avons traduit assez librement *write-once memories* (WOM) par mémoires non effaçables et *write-reluctant mémories* (WRM) par mémoires à écritures limitées.

de recouvrements linéaires proches de l'optimal.

Nous allons voir au chapitre 10 un modèle plus général : l'adversaire y est actif cette fois-ci ; il peut modifier le mot obtenu après dissimulation. L'existence de schémas reste liée à des problèmes de recouvrements, mais fait également intervenir d'autres contraintes. Cependant, avant d'aborder cette généralisation, nous verrons au cours du chapitre suivant comment les travaux déjà publiés portant sur les images en noir et blanc, mais également en couleurs, peuvent se plier à notre modèle.

Chapitre 9

Réécriture de travaux précédents

Plusieurs schémas traitent des images en noir et blanc, à savoir [WL98, WTL00, PCT00, TP01, TP02, Hio03]. Tous ces schémas présentent une structure de recouvrement que nous allons expliciter dans le présent chapitre. Toutefois, une partie de ces schémas ne rentre pas strictement dans notre cadre, sans pour autant s'éloigner significativement de la ligne directrice. Nous détaillerons les modifications nécessaires à apporter aux schémas de base, construits lors du précédent chapitre, pour retrouver exactement les schémas déjà publiés. D'autre part, il existe des schémas de dissimulation pour les images en couleurs ([CJL$^+$03, CJL$^+$04] et [Wes01]) qui se rapprochent de nos constructions ou, tout au moins, dont une partie se réduit à des recouvrements.

En section préliminaire, nous rappelons les propriétés des codes de Hamming et de Varshamov-Tenengolts, que nous mettrons à contribution au cours des sections suivantes pour analyser les travaux précités. Nous commencerons par ceux entrant exactement dans notre cadre formel, autrement dit par Wu et Lee [WL98] et Pan, Chen et Tseng [PCT00]. Nous passerons ensuite à Tseng et Pan [TP01, TP02] et Hioki [Hio03] qui nécessitent quelques modifications. Enfin nous terminerons par Chang, Jung, Lee, Lee, et Yoo [CJL$^+$03] et Chang, Jung, Lee et Yang [CJL$^+$04], ces deux derniers étant identiques, et Westfeld [Wes01], ces travaux concernant les images en couleurs.

9.1 Codes de Hamming et de Varshamov-Tenengolts

Les deux principaux recouvrements dont nous aurons besoin seront ceux de Hamming et de Varshamov-Tenengolts. L'objet de cette section est de rappeler brièvement les caractéristiques du code de Hamming et de donner une présentation plus complète sur celui de Varshamov-Tenengolts.

Définition 9.1 (Code de Hamming) *Soit* r *un entier strictement supérieur à 1. Tout code binaire linéaire admettant une matrice de parité dont l'ensemble des colonnes est égal à* $\mathbb{F}^r \setminus \{0\}$ *est appelé code de Hamming.*

Le code de Hamming est connu pour être un code parfait corrigeant 1 erreur. Autrement dit, les boules fermées de rayon 1 centrées sur les mots du code de Hamming forment une partition de l'espace. Par conséquent, son rayon de recouvrement est égal à 1. Sa longueur est $2^r - 1$ et sa dimension $2^r - r - 1$. Son décodage est simple : tous les mots binaires non nuls de longueur r sont des colonnes de la matrice de parité, donc il suffit de rechercher la colonne correspondant au syndrome du mot à décoder et on obtient alors la coordonnée à changer pour obtenir un mot du code. De plus, en prenant une forme particulière pour la matrice de parité, on peut éviter la recherche de la colonne. En effet, si on prend la matrice $\mathcal{H}$ dont la j-ème colonne correspond à l'écriture binaire de $j+1$, avec j variant de 0 à $2^r - 2$, le problème du décodage de syndrome devient extrêmement simple : un mot $\mathbf{s}$ de syndrome $\mathbf{x} = \mathbf{s} \cdot \mathcal{H}^t$ peut être obtenu à partir d'un mot $\mathbf{v}$ de syndrome $\mathbf{y} = \mathbf{v} \cdot \mathcal{H}^t$ simplement en modifiant la coordonnée dont l'indice a $\mathbf{x} - \mathbf{y}$ pour écriture binaire.

Bien que le code de Hamming soit un recouvrement de rayon 1, nous aurons à l'utiliser comme un recouvrement de rayon 2 : étant donné $\mathbf{v}$, de syndrome $\mathbf{y}$, nous nous autoriserons à modifier 2 coordonnées pour obtenir le syndrome $\mathbf{x}$ souhaité. Lorsque $\mathbf{z} = \mathbf{x} - \mathbf{y}$ est différent de zéro, en notant $\mathbf{e}_i$ le mot dont seule la coordonnée i est à 1, il y a $n - 1$ couples d'indices (i, j) tels que le mot $\mathbf{e}_i - \mathbf{e}_j$ ait $\mathbf{z}$ pour syndrome. Cela permet, en modifiant plus de coordonnées du mot $\mathbf{v}$ qu'il n'est strictement nécessaire, d'avoir plus de choix possibles pour les modifications et permet de sélectionner le couple minimisant un critère secondaire, comme nous le verrons dans la section 9.3.

Passons maintenant au second recouvrement dont nous aurons besoin dans la suite de ce chapitre. Ce recouvrement étant moins répandu que le code de Hamming, nous le présentons plus en détails.

Définition 9.2 (Code de Varshamov-Tenengolts, [VT65]) *Pour tout couple d'entiers* (x, n) *tel que* $0 \leq x \leq n$*, on appelle code de recouvrement de Varshamov-Tenengolts, et on note* $\mathsf{VT}_x(n)$*, l'ensemble des mots binaires* $\mathbf{c} = (c_1, \ldots, c_n)$ *de longueur* n *vérifiant*

$$S(\mathbf{c}) = \sum_{i=1}^{n} i \cdot c_i \equiv x \pmod{n+1} \ ,$$

où les c_i *sont considérés comme appartenant à* $\{0, 1\} \subset \mathbb{Z}$ *et les opérations sont effectuées dans* $\mathbb{Z}$.

Nous aurons à utiliser ces codes pour $n = 2^r - 1$. Nous allons prouver que dans ces conditions, le rayon de recouvrement de $\mathsf{VT}_x(2^r - 1)$ vaut 2. Pour cela, nous décrivons un algorithme de décodage de $\mathsf{VT}_x(2^r-1)$ modifiant au plus 2 coordonnées.

Notons $\mathbf{e}_i$ le mot dont toutes les coordonnées sont nulles sauf la i-ème. On a alors pour tout mot $\mathbf{v}=(v_1,\dots,v_n)\in\mathbb{F}^n$

$$S(\mathbf{v}+\mathbf{e}_i)=S(\mathbf{v})+(-1)^{v_i}i\ .$$

Plus généralement, pour tout couple d'entiers $i\neq j$, on a

$$S(\mathbf{v}+\mathbf{e}_i+\mathbf{e}_j)=S(\mathbf{v})+(-1)^{v_i}i+(-1)^{v_j}j\ .$$

Considérons alors un mot $\mathbf{v}$ tel que $S(\mathbf{v})\equiv y \pmod{2^r}$. Nous recherchons un mot $\mathbf{s}\in\mathsf{VT}_x(2^r-1)$ à une distance de Hamming inférieure ou égale à 2 de $\mathbf{v}$. Posons $z=x-y \bmod 2^r$. Si $v_z=0$ (respectivement $v_{2^r-z}=1$), le mot $\mathbf{s}=\mathbf{v}+\mathbf{e}_z$ (respectivement $\mathbf{s}=\mathbf{v}+\mathbf{e}_{2^r-z}$) est une solution. Sinon, le principe est de trouver un couple d'indices (i,j) tel qu'en changeant v_i et v_j, c'est-à-dire en ajoutant $\mathbf{e}_i+\mathbf{e}_j$ au mot $\mathbf{v}$, on ajoute z à $S(\mathbf{v})$. Pour ce faire, notons ℓ le plus petit entier positif tel que l'on ait soit $v_{\ell z}=0$, soit $v_{2^r-\ell z}=1$, les indices étant pris modulo 2^r. Un tel entier existe nécessairement d'après les deux lemmes suivants, le premier étant une simple conséquence du théorème de Bezout et le second découlant du premier.

Lemme 9.3 *Soit r un entier strictement positif. Pour tout entier z, $0<z<2^r$, il existe un entier ℓ tel que $\ell z\equiv 2^{r-1} \pmod{2^r}$.*

Preuve. D'après le théorème de Bezout, il existe un entier $u\in[1,2^r-1]$ tel que

$$u\cdot z\equiv \mathrm{pgcd}(z,2^r) \pmod{2^r}\ .$$

Or, comme $z\neq 0$, le $\mathrm{pgcd}(z,2^r)$ est de la forme 2^t où t est un entier positif, éventuellement nul, au plus égal à $r-1$ puisque $z\neq 0$. Il suffit donc de prendre $\ell=2^{r-1-t}u$. □

Lemme 9.4 *Pour tout mot $\mathbf{v}=(v_1,\dots,v_{2^r-1})\in\mathbb{F}^{2^r-1}$ et pour entier z, $0<z<2^r$, l'ensemble des entiers ℓ tels que $v_{\ell z}=0$ ou $v_{2^r-\ell z}=1$ est non vide, les indices étant considérés modulo 2^r.*

Preuve. D'après le lemme 9.3 ci-dessus, il existe un entier ℓ vérifiant $\ell z\equiv 2^{r-1} \pmod{2^r}$. Pour un tel ℓ, on a $\ell z\equiv 2^r-\ell z \pmod{2^r}$, ce qui implique $v_{\ell z}=v_{2^r-\ell z}=v_{2^{r-1}}$, les indices étant pris modulo 2^r. Or, le mot $\mathbf{v}$ étant binaire, $v_{2^{r-1}}$ ne peut prendre que deux valeurs, à savoir 0 ou 1, ce qui prouve que l'ensemble considéré est non vide. □

L'entier ℓ étant pris minimal, nous avons donc $v_{(\ell-1)z}=1$ et $v_{2^r-(\ell-1)z}=0$ (rappelons que par hypothèse nous sommes dans le cas où $v_z=1$ et $v_{2^r-z}=0$, ce qui implique $\ell\geq 2$). Changer l'une de ces coordonnées soustrait $(\ell-1)z$ à

$S(\mathbf{v})$, et modifier $v_{\ell z}$ ou bien $v_{2^r-\ell z}$ y ajoute ℓz. Par conséquent, si $v_{\ell z} = 0$, les mots

$$\mathbf{v} + \mathbf{e}_{\ell z} + \mathbf{e}_{(\ell-1)z} \ ,$$
$$\mathbf{v} + \mathbf{e}_{\ell z} + \mathbf{e}_{2^r-(\ell-1)z}$$

sont deux solutions, sinon

$$\mathbf{v} + \mathbf{e}_{2^r-\ell z} + \mathbf{e}_{(\ell-1)z} \ ,$$
$$\mathbf{v} + \mathbf{e}_{2^r-\ell z} + \mathbf{e}_{2^r-(\ell-1)z}$$

le sont.

Bien que les codes de Varshamov-Tenengolts soient, en général, non linéaires, il est possible de construire un schéma de dissimulation à partir de ces derniers. En effet, la famille $\{\mathsf{VT}_0(2^r-1), \mathsf{VT}_1(2^r-1), \ldots, \mathsf{VT}_{2^r-1}(2^r-1)\}$ est constituée de recouvrements de longueur $2^r - 1$, de rayon 2 dont la réunion disjointe est l'ensemble $\mathbb{F}^n$. D'après le théorème 8.1 page 116, nous avons donc un schéma de paramètres $(2^r - 1, 2^r, 2)$. En fait, ce schéma est très proche de ceux construits à partir de recouvrements linéaires, l'application $\mathbf{v} \mapsto S(\mathbf{v})$ jouant ici le rôle du syndrome.

9.2 Les schémas [WL98] et [PCT00]

Après avoir rappelé les propriétés des recouvrements de Hamming et de Varshamov-Tenengolts, nous allons considérer les différents schémas existant qui peuvent entrer dans notre formalisme. Nous commençons, dans cette section, par présenter les schémas se réduisant complètement à des recouvrements. Nous verrons ensuite à la section 9.3 une autre série imposant quelques nouvelles contraintes auxiliaires.

[WL98]. Wu et Lee ont proposé dans [WL98] un schéma dissimulant 1 bit dans des blocs de longueur n. L'image est découpée en mots de n bits, un mot $\mathbf{k}$ est choisi pour servir de clef et l'information, se composant d'un seul bit, est dissimulée dans le produit bit à bit des mots avec la clef $\mathbf{k}$, plus précisément dans la parité de la somme des coordonnées de ce produit. En terme de recouvrement, cela revient à considérer le recouvrement $\mathcal{C}$ ayant pour matrice de parité une matrice de dimension $1 \times n$, dont la seule ligne est $\mathbf{k}$. Le code $\mathcal{C}$ a pour paramètres $[n, n-1]1$ et ce schéma a donc $(n, 2, 1)$ pour paramètres.

[PCT00]. Ce schéma, dû à Pan, Chen et Tseng, dissimule r bits dans des mots binaires de longueur $n = 2^r - 1$, en modifiant au plus deux bits. La clef est composée de deux parties. La première est un mot binaire $\mathbf{k}$ de longueur n

utilisé pour faire un ou-exclusif avec le mot $\mathbf{v}$ dans lequel s'effectue l'insertion. L'information est ainsi dissimulée dans $\mathbf{v}+\mathbf{k}$. L'autre partie de la clef est une permutation σ de l'ensemble $\{1, 2, \ldots, n\}$. L'information est alors dissimulée dans la somme

$$\sum_{i=1}^{n} (v_i \oplus k_i) \cdot \sigma(i) \pmod{n+1} \ ,$$

où $\oplus$ correspond à l'addition binaire, les autres opérations étant effectuées dans $\mathbb{Z}/(n+1)\mathbb{Z}$ en assimilant $\mathbb{F}^n$ à $\{0, 1\} \subset \mathbb{Z}$. Dans le principe, cela revient à utiliser le recouvrement de Varshamov et Tenengolts (cf. définition 9.2). Si on prend la clef $\mathbf{k}$ égale à zéro et la permutation σ égale à l'identité, l'information est dissimulée dans

$$S(\mathbf{v}) = \sum_{i=1}^{n} v_i \cdot i \pmod{n+1}$$

et cette somme sert justement à définir le recouvrement de Varshamov-Tenengolts et si on néglige la clef, ce que nous avons fait depuis le début de notre propos pour nos schémas de dissimulation, celui proposé par [PCT00] se réduit au schéma fondé sur la famille $\{VT_0(2^r - 1), \ldots, VT_{2^r-1}(2^r - 1)\}$, donné à la section 9.1.

9.3 Les schémas [TP01, TP02] et [Hio03]

Les schémas [WL98] et [PCT00] que nous venons de voir se réduisent directement à des schémas constructibles par des recouvrements. Nous allons voir que ce n'est pas le cas de tous les schémas, tout en mettant bien en lumière la place centrale des recouvrements dans les propositions de [TP01, TP02] et [Hio03]. L'approche est identique dans ces schémas : il existe de manière générale plusieurs solutions au problème de l'insertion, en d'autres termes, il existe plusieurs mots $\mathbf{s}$ vérifiant $E(\mathbf{s}) = \mathbf{x}$ et $d_H(\mathbf{s}, \mathbf{v}) \leq T$; un critère auxiliaire est alors utilisé pour déterminer quelle solution $\mathbf{s}$ peut être retenue, et le cas échéant empêche l'insertion faute de solution satisfaisante.

[TP01, TP02]. Tseng et Pan ont repris dans [TP01] et [TP02] le schéma exposé par Pan, Chen et Tseng que nous avons détaillé lors de la précédente section. La base du schéma est toujours un recouvrement de Varshamov-Tenengolts, mais le décodage est sensiblement différent, à la suite d'une contrainte ajoutée sur les modifications acceptables. Jusqu'à présent, nous n'avions qu'une contrainte quantitative sur les modifications. Nous introduisons maintenant une contrainte qualitative, qui restreint les modifications possibles à des zones considérées comme propices à la dissimulation.

Pour présenter cette contrainte, il est préférable de considérer les mots binaires de $\mathbb{F}^n$ comme des matrices binaires de dimensions $a \times b$. Ainsi, une matrice représente un bloc de pixels connexes dans l'image originale. Notons $\mathbf{v} = (v_{i,j})$ une telle matrice, un coefficient $v_{i,j}$ ne peut être modifié que si l'un des coefficients $v_{i\pm1,j\pm1}$ vaut $1 \oplus v_{i,j}$. Cette restriction a pour objet d'éviter de modifier une coordonnée se trouvant au beau milieu d'une zone uniforme : on ne peut plus modifier que les zones frontières.

La représentation des blocs d'images sous la forme de matrices nécessite d'adapter légèrement les codes VT. Posons $r = \lfloor \log(ab+1) \rfloor$. Une application surjective w définie sur $[1, a] \times [1, b]$ à valeurs dans $[1, 2^r - 1]$ est utilisée pour attribuer un poids à chaque coordonnée, ainsi l'application S devient

$$S(\mathbf{v}) = \sum_{\substack{1 \le i \le a \\ 1 \le j \le b}} v_{i,j} \cdot w(i, j) \ .$$

Pour tout entier positif $x < 2^r$, l'ensemble des matrices binaires $\mathbf{v}$ vérifiant $S(\mathbf{v}) \equiv x \pmod{2^r}$ est encore un recouvrement de rayon 2 et le décodage est semblable à celui exposé à la section 9.1 pour les codes de Varshamov-Tenengolts. Essentiellement, si $S(\mathbf{v}) \equiv y \pmod{2^r}$ et que l'on souhaite obtenir $\mathbf{s}$ tel que $d_H(\mathbf{v}, \mathbf{s}) \le 2$ et $S(\mathbf{s}) \equiv x \pmod{2^r}$ alors, en posant $z = x - y$, on recherche un couple d'indices (i_+, j_+) vérifiant soit

$$w(i_+, j_+) \equiv \ell z \pmod{2^r} \quad \text{et} \quad v_{i_+,j_+} \text{ vaut } 0 \text{ et est modifiable,}$$

soit

$$w(i_+, j_+) \equiv 2^r - \ell z \pmod{2^r} \quad \text{et} \quad v_{i_+,j_+} \text{ vaut } 1 \text{ et est modifiable.}$$

On recherche ensuite un couple (i_-, j_-) vérifiant soit

$$w(i_-, j_-) \equiv (\ell - 1) z \pmod{2^r} \quad \text{et} \quad v_{i_-,j_-} \text{ vaut } 1 \text{ et est modifiable,}$$

soit

$$w(i_-, j_-) \equiv 2^r - (\ell - 1) z \pmod{2^r} \quad \text{et} \quad v_{i_-,j_-} \text{ vaut } 0 \text{ et est modifiable.}$$

Modifier v_{i_+,j_+} ajoute ℓz modulo 2^r à $S(\mathbf{v})$ et modifier v_{i_-,j_-} y soustrait $(\ell - 1)z$ modulo 2^r. Le mot $\mathbf{s}$ ainsi obtenu est donc une solution à notre problème. Toutefois, rien n'assure l'existence des couples (i_+, j_+) et (i_-, j_-).

D'autre part, un problème se pose pour l'extraction de l'information dissimulée : comment savoir si un bloc contient de l'information ou non puisque ce schéma n'arrive pas à insérer systématiquement des données ? Ce problème est résolu par l'utilisation du bit de poids faible de x, le message à insérer : lorsque l'insertion est possible, le message est nécessairement un entier pair, donc seuls $r-1$ bits de x véhiculent de l'information utile. Lorsque l'insertion échoue, $\mathbf{v}$ est tout de même modifié en un mot $\mathbf{v}'$ de manière à avoir $S(\mathbf{v}')$ impair. Cela se fait sur une coordonnée (i, j) telle que $w(i, j)$ est impair et que $v_{i,j}$ est modifiable. Afin de s'en assurer, l'application w est choisie telle que chaque bloc 2×2

$$\begin{pmatrix} w(i,j) & w(i,j+1) \\ w(i+1,j) & w(i+1,j+1) \end{pmatrix} \tag{*}$$

contienne au moins un coefficient impair. Ainsi, hormis pour le mot tout à 0 ou tout à 1, il est toujours possible de modifier la parité de $S(\mathbf{v})$. Pour terminer, les mots tout à 0 et tout à 1 ne sont pas utilisés et sont simplement sautés.

Clairement, la quantité d'information dissimulée par un tel schéma ne dépend plus uniquement du recouvrement utilisé, mais dépend également du mot dans lequel s'effectue la dissimulation. Toutefois, le recouvrement donne toujours une borne : lorsque l'insertion peut être effectuée, au plus 2 bits sont modifiés parmi n pour dissimuler $r = \lfloor \log(n) \rfloor - 1$ bits.

[Hio03]. Hioki propose une modification du schéma précédent. En premier lieu, l'application w est maintenant à valeurs dans $\mathbb{F}^r \setminus \{0\}$, tout en restant surjective. Ensuite il remplace l'application $S(\mathbf{v}) = \sum v_{i,j} \cdot w(i,j)$ par $S'(\mathbf{v}) = \bigoplus v_{i,j} \cdot w(i,j)$. On est donc passé d'une somme rationnelle à une somme de mot binaire, et par là-même d'un code de Varshamov-Tenengolts à un code de Hamming, du moins dans le principe. En effet, comme avec le schéma précédent, la longueur des mots ne permet pas toujours d'utiliser exactement un code de Hamming. Si l'application w est injective, alors la longueur est de la forme $2^m - 1$ et on a un code de Hamming. Dans le cas contraire on a une longueur pour laquelle le code de Hamming n'existe pas et le code utilisé est obtenu en ajoutant des colonnes à la matrice de parité d'un code de Hamming.

Le code utilisé est de rayon 1 et il est par conséquent possible de ne modifier qu'une seule coordonnée dans les mots pour y insérer des messages. Cependant, la contrainte sur la proximité d'un coefficient opposé étant maintenue, tous les coefficients ne peuvent être modifiés et, pour augmenter le nombre de mots dans lesquels l'insertion peut être effectuée, on accepte de modifier deux coordonnées.

L'insertion d'un message $\mathbf{x}$ s'effectue donc en recherchant deux couples (i_-, j_-), (i_+, j_+) tels que d'une part chaque coefficient v_{i_-,j_-} et v_{i_+,j_+} soit modifiable et d'autre part $w(i_+, j_+) \oplus w(i_-, j_-) = \mathbf{x}$. Remarquons que, contrairement à [PCT00], il n'y a pas de contrainte sur les valeurs de v_{i_-,j_-} et v_{i_+,j_+}. Cela provient de la linéarité de S, propriété qui n'est pas vérifiée pour [PCT00]. Toutefois, là encore, la contrainte d'adjacence d'un coefficient opposé pour pouvoir modifier une coordonnée empêche d'assurer l'existence des deux couples d'entiers recherchés. La coordonnée d'indice zéro du mot $\mathbf{x}$ est mise à zéro pour une réussite, tout comme pour [TP01], et un coefficient est tout de même modifié en cas d'échec pour que le bit de poids faible de $S'(\mathbf{v})$

soit non nul. Suivant Tseng et Pan, cela est assuré si l'on prend une application w telle que chaque matrice de la forme de (*) (voir page précédente) ait un coefficient dont la coordonnée d'indice zéro soit 1. Les mots tout à 1 et tout à zéro sont également ignorés.

A priori, un tel schéma, fondé sur le code de Hamming, devrait présenter de meilleurs paramètres qu'un schéma reposant sur le code de Varshamov-Tenengolts, à savoir $(2^r-1, 2^r, 1)$ au lieu de $(2^r-1, 2^r, 2)$, donc deux fois moins de bits modifiés pour une longueur et un nombre de bits insérés identiques. Cependant, ce n'est pas le cas : ce schéma, lorsque l'insertion est possible dans un bloc, modifie au plus 2 bits parmi n pour dissimuler $r = \lfloor \log(n) \rfloor - 1$ bits. Il y a tout de même un intérêt à l'utilisation du code de Hamming, comme nous l'avons remarqué ci-dessus : les contraintes sur $\mathbf{v}$ pour pouvoir effectuer l'insertion d'un message sont moins restrictives, ce qui se traduit par un échec de l'insertion moins fréquent.

9.4 Les schémas [CJL+03, CJL+04] et [Wes01]

Nous nous sommes intéressé, lors des deux précédentes sections, aux travaux traitant des images en noir et blanc. Nous considérons dans celle-ci les schémas s'appliquant aux images en couleurs.

[CJL+03, CJL+04]. Ce schéma s'applique à des images en couleurs, dans une représentation spatiale. Bien que cela n'ait que peu d'importance, la représentation choisie ici est le RVB. Chaque point de l'image est donc représenté par trois valeurs entières indiquant les proportions relatives de rouge, de vert et de bleu. L'image est séparée en trois plan, un pour chaque composante et seul le bit de poids faible de chaque composante est pris en compte. Le schéma de Tseng et Pan est alors appliqué successivement aux plans bleu, rouge et vert, dans cet ordre, qui sont considérés comme des images en noir et blanc. L'argument avancé pour le choix de cet ordre est la grande sensibilité de l'œil humain à la luminance, définie par

$$Y = 0.299R + 0.587V + 0.114B \quad .$$

L'ordre retenu est donc l'ordre d'influence croissante des composantes RVB sur la luminance.

Clairement, ce schéma se généralise à toute représentation spatiale, sans modification majeure. Il est cependant préférable d'appliquer le schéma de Hioki à la place de celui de Tseng et Pan.

[Wes01]. Le schéma F5 dû à Westfeld diffère nettement de tous les schémas que nous avons présentés dans ce chapitre : les images cessent d'être vues spatialement et sont, dans F5, considérées sous un jour fréquentiel, à savoir le format JPEG (cf. [Wal91]). Cette représentation est obtenue en appliquant une transformée en cosinus discrète à une représentation spatiale. Chaque plan de la représentation spatiale est découpé en blocs de 8 pixels sur 8 pixels et la transformée de chaque bloc B calculée par la relation

$$\widehat{B}(u,v) = \frac{1}{4}\lambda(u)\lambda(v)\sum_{i=0}^{7}\sum_{j=0}^{7}B(i,j)\cos\left(\frac{(2i+1)\cdot u\cdot\pi}{16}\right)\cos\left(\frac{(2j+1)\cdot v\cdot\pi}{16}\right) ,$$

où $\lambda(x) = 1$ si $x = 0$ et $1/\sqrt{2}$ sinon. Les valeurs des coefficients de B sont supposées être entières, et dans un intervalle de la forme $[-2^l, 2^l - 1]$. La transformation réciproque est définie par

$$B(i,j) = \frac{1}{4}\sum_{u=0}^{7}\sum_{v=0}^{7}\lambda(u)\lambda(v)\widehat{B}(u,v)\cos\left(\frac{(2i+1)\cdot u\cdot\pi}{16}\right)\cos\left(\frac{(2j+1)\cdot v\cdot\pi}{16}\right) .$$

Dans cette représentation fréquentielle, un bloc de 8×8 pixels est un vecteur de longueur 64. Ce vecteur contient les coefficients de la transformée après arrondi. Rigoureusement, les $\widehat{B}(u,v)$ sont des nombres réels, potentiellement avec une écriture binaire infinie. Ces derniers sont donc arrondis, de manière plus ou moins fine, en fonction d'un modèle psycho-visuel décrivant la sensibilité de l'œil humain selon les différentes fréquences. Ainsi, à chaque couple (u,v) correspond une valeur $q(u,v)$ et le coefficient arrondi est défini par

$$\overline{B}(u,v) = \left[\frac{\widehat{B}(u,v)}{q(u,v)}\right]$$

(essentiellement, le caractère non conservatif du format JPEG provient de cette étape d'arrondi).

Ces coefficients arrondis servent à construire un mot binaire $\mathbf{v}$, dont le syndrome correspond à l'information dissimulée $\mathbf{y}$. Si $\mathbf{y}$ n'est pas le message souhaité, $\mathbf{v}$ est modifié et cette modification est traduite sur les coefficients. La modification sur $\mathbf{v}$ se fait exactement par un schéma obtenu avec la proposition 8.6 page 118 avec un code de Hamming. Cette étape, qui constitue le corps de la dissimulation, est appelée *encodage matriciel* par Westfeld. Précisons que la matrice $\mathcal{H}$ utilisée est obtenue en prenant l'écriture binaire de j pour la $(j-1)$-ème colonne, avec $j \in [1, 2^r - 1]$, l'entier r dépendant du nombre de blocs disponibles et de la longueur du message $\mathbf{x}$. Cette matrice particulière permet, comme nous l'avons rappelé dans la première section de ce chapitre, de simplifier les calculs.

Généralement, les coefficients arrondis $\overline{B}(u,v)$ ont une distribution en cloche (cf. [Wes01]) et pour préserver cette forme, le schéma de Westfeld ne se contente pas de modifier le bit de poids faible des coefficients, il décrémente leur valeur absolue. Cela nécessite d'ignorer les coefficients nuls puisque qu'on ne peut les changer. Autrement dit, ces coefficients ne servent pas à construire le mot $\mathbf{v}$. D'autre part, lorsque le résultat d'une modification est l'annulation d'un coefficient, donc lorsque au départ $|\overline{B}(u,v)| = 1$, la modification est conservée, mais l'insertion ayant échoué on recommence en ignorant le coefficient $\overline{B}(u,v)$ dans la construction de $\mathbf{v}$. En effet, on ne dispose d'aucun moyen de distinguer le cas où le zéro a été obtenu à la suite de l'insertion de celui où il existait auparavant. Cela pose un problème pour l'extraction du message sauf si on ignore purement et simplement les zéros. L'inconvénient est que cela amène à introduire un plus grand nombre de modifications.

Enfin, pour terminer la description de F5, décrivons la construction du mot $\mathbf{v}$ à partir des coefficients arrondis. En premier lieu, les coefficients nuls et ceux correspondant à la fréquence $u = v = 0$ sont ignorés. Ensuite, une série de $2^r - 1$ coefficients arrondis est transformée en vecteur binaire en appliquant à chaque coefficient la fonction

$$f(c) = \begin{cases} 0 & \text{pour } c \text{ impair negatif, ou bien pair positif,} \\ 1 & \text{sinon.} \end{cases}$$

Le choix de cette fonction est également influencé par la volonté de préserver la forme en cloche de la distribution des coefficients arrondis.

Westfeld attribue à Crandall [Cra98] l'idée d'utiliser l'encodage matriciel dans le but de réduire le nombre de coordonnées à changer. Dans cette communication, Crandall présente de manière informelle le principe des schémas de dissimulation fondés sur les recouvrements linéaires en donnant l'exemple du schéma fondé sur le code de Hamming binaire de longueur 7 et signale clairement le rayon de recouvrement comme paramètre essentiel. Toutefois, sa présentation ne donne pas plus de détails.

Chapitre 10

Modèle avec adversaire actif

Jusqu'ici, nous avons concentré notre attention sur la dissimulation, à l'exclusion de tout autre problème. Nous allons maintenant étudier la dissimulation en imposant une certaine robustesse dans l'insertion du message. Nous supposons qu'après l'insertion, le mot peut être modifié et, malgré cela, nous souhaitons pouvoir extraire l'information dissimulée sans dégradation de cette dernière. Il ne suffit plus de minimiser le nombre de changements nécessaire à l'insertion, il faut en plus que le résultat de l'insertion puisse être légèrement modifiable sans que cela nuise à la récupération du message inséré. Cela nous conduit à un problème, plus général mais aussi plus complexe que celui du modèle passif, qui englobe le problème de la correction d'erreurs et celui du recouvrement pour la métrique de Hamming.

10.1 Problème équivalent

La résistance d'un schéma est en fait une contrainte de distance entre les mots résultant de la dissimulation de messages différents. Considérons le mot $\mathbf{s} = \mathrm{I}(\mathbf{v}, \mathbf{x})$, obtenu par insertion de $\mathbf{x}$ dans $\mathbf{v}$. Le mot $\mathbf{s}$ pouvant être modifié en t coordonnées, aucun mot de la boule fermée de rayon t centrée en $\mathbf{s}$, notée $B_t(\mathbf{s})$, ne peut être associé à un autre message que $\mathbf{x} = \mathsf{E}(\mathbf{s})$. Dans le cas contraire, on ne pourrait retrouver le message dissimulé. Nous avons donc la condition suivante sur l'application d'extraction :

$$\begin{aligned} \mathsf{E}\left(B_t(\mathbf{s})\right) &= \{\mathsf{E}(\mathbf{s})\} \\ &= \{\mathbf{x}\} \ . \end{aligned}$$

Cela implique que les boules $B_t(\mathbf{s})$ et $B_t(\mathbf{s}')$ ne s'intersectent pas, et cela pour tout couple $(\mathbf{s}, \mathbf{s}')$ de mots résultant de la dissimulation de messages différents. Cela revient à imposer une distance d'au moins $2t + 1$ entre $\mathbf{s}$ et $\mathbf{s}'$.

Ce problème, sous cette formulation, est connu sous le nom de « code correcteur d'erreurs centré » et fut introduit par Bassalygo et Pinsker dans [BP99] : on cherche à coder un message $\mathbf{x}$ en restant dans une boule de rayon T centrée sur un mot $\mathbf{v}$ et l'on souhaite pouvoir corriger t erreurs. Les entiers t et T sont des paramètres du code, le message $\mathbf{x}$ et le centre $\mathbf{v}$ sont des paramètres de l'application d'encodage. Le problème de recouvrement est donc toujours présent, il faut qu'il existe un mot encodant $\mathbf{x}$ dans la boule de centre $\mathbf{v}$ et de rayon T, et cela quels ques soient le message $\mathbf{x}$ et le mot $\mathbf{v}$. Mais une contrainte supplémentaire apparaît : la correction de t erreurs ; elle se traduisant par une distance minimale d'au moins $2t+1$ entre les M recouvrements permettant l'encodage des M messages différents.

NOTATION 10.1 *Nous noterons* (n, M, T, t) *les paramètres d'un schéma de dissimulation de distorsion maximale* T*, de longueur* n*, ayant* M *messages dissimulables et résistant à des modifications d'au plus* t *coordonnées, et nous appellerons le paramètre* t *la résistance du schéma.*

La motivation donnée par Bassalygo et Pinsker pour l'étude des codes correcteurs d'erreurs centrés est une application à l'écriture sur les mémoires : pour des raisons variées, il est possible que le nombre de bits que l'on peut modifier lors d'une écriture soit limité. Lorsque, de plus, des erreurs sont susceptibles de se produire lors de la lecture, nous avons affaire aux codes correcteurs d'erreurs centrés. Cette problématique, qui est une généralisation des mémoires à écritures limitées, est à peine esquissée dans [CHL$^+$97, chap. 18, §8] : seul l'équivalent de notre proposition 10.6, c'est-à-dire une borne inférieure asymptotique sur le nombre de messages, y est mentionné.

10.2 Borne sur le nombre de messages

On connaît une borne supérieure sur le cardinal d'un code centré reposant sur le lemme suivant :

LEMME 10.2 ([BP99, §1 LEMME 1]) *Soient* T *et* t *deux entiers positifs, avec* $T \geq t$*. Notons* $\mathcal{V}_a(Y)$ *l'ensemble des mots situés à une distance au plus* t *de l'ensemble* Y*,*

$$\mathcal{V}_t(Y) = \bigcup_{\mathbf{u} \in Y} B_t(\mathbf{u}) \ .$$

Alors, tout ensemble Y *satisfait l'inégalité*

$$\frac{|\mathcal{V}_T(Y)|}{|\mathcal{V}_t(Y)|} \leq \frac{|V_T|}{|V_t|} \ ,$$

où V_ρ *désigne le volume de la boule fermée de rayon* ρ*.*

Nous allons appliquer ce lemme à un ensemble $\mathsf{Y} = \mathsf{E}^{-1}(\{\mathbf{x}\})$, où E est l'application d'extraction d'un schéma de paramètres (n, M, T, t). Cet ensemble Y un recouvrement de rayon T, donc

$$\left|\mathcal{V}_T\left(\mathsf{E}^{-1}(\{\mathbf{x}\})\right)\right| = 2^n \ .$$

D'autre part, les M recouvrements étant deux à deux distants d'au moins $2t+1$, nous avons

$$M \leq \frac{2^n}{\left|\mathcal{V}_t\left(\mathsf{E}^{-1}(\{\mathbf{x}\})\right)\right|} \ ,$$

pour tout $\mathbf{x}$. D'après le lemme précédent,

$$\frac{2^n}{\left|\mathcal{V}_t\left(\mathsf{E}^{-1}(\{\mathbf{x}\})\right)\right|} \leq \frac{|V_T|}{|V_t|} \ .$$

Cela donne donc

Proposition 10.3 *Soit* $\mathbf{S}(n, T, t)$ *l'ensemble des schémas de longueur* n*, de distorsion maximale* T *et dont la résistance vaut* t *et posons*

$$m(n, T, t) = \log\left(\max_{\mathcal{S} \in \mathbf{S}(n,T,t)} |\mathcal{S}|\right) \ ,$$

Nous avons

$$m(n, T, t) \leq \log(V_T) - \log(V_t) \ .$$

Comportements asymptotiques. De même que pour le modèle avec adversaire passif, nous allons nous intéresser à deux cas différents. Tout d'abord, lorsque les paramètres T et t croissent linéairement avec la longueur n, nous avons

$$m(n, T, t) \lesssim n \cdot \left(h\left(\frac{T}{n}\right) - h\left(\frac{t}{n}\right)\right) \ ,$$

en utilisant le même équivalent asymptotique de $\log(V)$ que celui déjà utilisé pour la proposition 8.12 page 124. Nous avons donc, comme pour le modèle avec adversaire passif, une croissance linéaire du majorant.

L'autre cas d'intérêt est celui où la distorsion T et la résistance t sont fixées, tandis que la longueur n tend vers l'infini. Dans ce cas, nous obtenons

$$m(n, T, t) \lesssim (T - t) \cdot \log(n) - \log\left(\frac{T!}{t!}\right) \ .$$

Proposition 10.4 *Asymptotiquement, lorsque la longueur* n *tend vers l'infini, nous avons :*

1. *pour* $\frac{T}{n}$ *et* $\frac{t}{n}$ *fixés,*

$$m(n, T, t) \lesssim n \cdot \left(h\left(\frac{T}{n}\right) - h\left(\frac{t}{n}\right) \right) \quad ;$$

2. *pour* T *et* t *fixés,*

$$m(n, T, t) \lesssim (T - t) \cdot \log(n) - \log\left(\frac{T!}{t!}\right) \quad .$$

10.3 Schémas asymptotiquement proches de l'optimal

Les bornes asymptotiques, données à la section précédente, sont relativement fines, même si la situation est moins favorable que pour le modèle à adversaire passif. Rappelons que pour ce dernier, les deux variantes asymptotiques de la borne supérieure étaient atteintes. Lorsque l'on autorise des modifications après insertion, les résultats ne sont pas les mêmes : les schémas que nous obtenons n'atteignent pas ces bornes. Toutefois, l'écart par rapport à la borne n'est pas trop important.

Nous avons rappelé au théorème 8.14 page 125 qu'avec une très grande probabilité un code linéaire de longueur n et de redondance $n \cdot h(\alpha)$ a un rayon $n \cdot \alpha$. Or il existe un résultat analogue pour la distance minimale (voir, par exemple, [Bar98, §1.3, lemme 1.2] pour une preuve) :

Théorème 10.5 *La probabilité qu'un code linéaire de longueur* n *et de redondance* $n \cdot h(\alpha)$ *ait une distance minimale* $n \cdot \alpha$ *tend vers 1 lorsque* n *tend vers l'infini.*

Donc, avec une grande probabilité, un code linéaire $\mathcal{C}_0$, de longueur n et de redondance $n \cdot h(2\beta)$, a une distance minimale $n \cdot (2\beta)$ et ses sous-codes de redondance $n \cdot h(\alpha)$ sont des recouvrements de rayon $n \cdot \alpha$, avec $\alpha \geq 2\beta$. Si on note $\mathcal{C}$ un tel sous-code, alors ce dernier admet

$$2^{n \cdot (h(\alpha) - h(2\beta))}$$

translatés dans $\mathcal{C}_0$. Chaque translaté est un recouvrement de rayon $n \cdot \alpha$ d'après la proposition 8.3 page 117 et, en tant que sous-codes disjoints d'un code de distance minimale $n \cdot (2\beta)$, ils sont deux à deux à une distance d'au moins $n \cdot (2\beta)$. L'ensemble des translatés de $\mathcal{C}$ ainsi construits est donc un schéma de paramètres $(n, 2^{n \cdot (h(\alpha) - h(2\beta))}, n \cdot \alpha, n \cdot \beta)$, avec $2\beta \leq \alpha \leq 1/2$.

Proposition 10.6 *Asymptotiquement, lorsque la longueur* n *tend vers l'infini et les rapports* $\frac{T}{n}$ *et* $\frac{t}{n}$ *sont fixés, on a*

$$m\left(n, \frac{T}{n}, \frac{t}{n}\right) \gtrsim n \cdot \left(h\left(\frac{T}{n}\right) - h\left(2\frac{t}{n}\right) \right).$$

Une illustration explicite de cette construction de recouvrements suffisamment éloignés les uns des autres est donnée, pour une distance égale à 3, par Zémor et Cohen dans [ZC91] en vue d'une application aux codes d'écriture sur les mémoires non effaçables résistants à une erreur. Le code utilisé est un code de Hamming et le sous-code est, dans un premier temps, un code BCH 2-correcteur, puis ensuite un code BCH 3-correcteur. Les paramètres, traduits pour les schémas de dissimulation, sont respectivement $(2^r-1, 2^r-1-2r, 3, 1)$ et $(2^r-1, 2^r-1-2r, 5, 1)$.

Lorsque la distorsion T et la résistance t sont fixées, et que la longueur tend vers l'infini, bien que nous ne puissions pas non plus prouver que notre borne soit fine, nous pouvons au moins donner une construction explicite, et non probabiliste, de schémas s'en approchant. Pour cela, nous allons procéder dans le sens inverse de celui utilisé ci-dessus : nous allons construire un recouvrement linéaire de rayon T, puis nous allons rechercher des translatés à une distance d'au moins $2t+1$ les uns des autres. Comme pour le modèle à adversaire passif, nous prenons pour recouvrement linéaire une somme directe de T codes de Hamming de paramètres $[n, n-r]1$, avec $n = 2^r - 1$, ce qui donne un recouvrement $\mathcal{C}$ de paramètres $[n \cdot T, (n-r) \cdot T]T$. Les différents translatés de $\mathcal{C}$ forment une partition de $\mathbb{F}^{n \cdot T}$, et chaque translaté est uniquement déterminé par le syndrome de ses mots. Le syndrome d'un mot de $\mathbb{F}^{n \cdot T}$ est un élément de $\mathbb{F}^{r \cdot T}$ que nous allons identifier à un mot de $\mathbb{F}_{2^r}^T$. Afin de sélectionner des translatés suffisamment éloignés les uns des autres, nous allons utiliser un code $\mathbf{C}$ de longueur T sur $\mathbb{F}_{2^r}$ corrigeant t erreurs. Nous ne retiendrons que les translatés de $\mathcal{C}$ dont le syndrome est un mot de ce code. Soit λ, défini sur $\mathbb{F}^r$ et à valeurs dans $\mathbb{F}_{2^r}$, un isomorphisme d'espaces vectoriels sur $\mathbb{F}$. Nous noterons Λ l'application de $(\mathbb{F}^r)^T \simeq \mathbb{F}^{r \cdot T}$ dans $\mathbb{F}_{2^r}^T$ qui étend λ coordonnée par coordonnée.

LEMME 10.7 *Soit $\mathcal{C}$ la somme directe de T codes de Hamming de longueur $n = 2^r - 1$. En notant $\mathcal{H}$ la matrice de parité de $\mathcal{C}$ définie par*

$$\mathcal{H} = \begin{pmatrix} \mathcal{H}_{\mathrm{H}} & & \\ & \ddots & \\ & & \mathcal{H}_{\mathrm{H}} \end{pmatrix}$$

où $\mathcal{H}_{\mathrm{H}}$ est une matrice de parité du code de Hamming de longueur n et E l'application qui, à un mot $\mathbf{s}$, associe son syndrome,

$$E(\mathbf{s}) = \mathbf{s} \cdot \mathcal{H}^t \quad ,$$

nous avons alors pour tout mot $\mathbf{s} \in \mathbb{F}^{n \cdot T}$ et pour tout entier $t \in [0, T]$

$$\Lambda \circ E\left(B_t^{2, n \cdot T}(\mathbf{s})\right) \subset B_t^{2^r, T}(\Lambda \circ E(\mathbf{s}))$$

où $B_\rho^{q,n}(\mathbf{v})$ désigne la boule fermée de rayon ρ et de centre $\mathbf{v}$ dans l'espace $\mathbb{F}_q^n$.

Preuve. Soient $\mathbf{s}$ et $\mathbf{e}$ deux mots de $\mathbb{F}^{n\cdot T}$, avec $w_H(\mathbf{e}) \leq t$. Nous allons prouver l'inégalité

$$d_H(\Lambda \circ E(\mathbf{s}), \Lambda \circ E(\mathbf{s}+\mathbf{e})) \leq t \ ,$$

qui est une formulation équivalente du lemme. Posons

$$\mathbf{s} = (\mathbf{s}_1, \ldots, \mathbf{s}_T) \ ,$$
$$\mathbf{e} = (\mathbf{e}_1, \ldots, \mathbf{e}_T) \ ,$$

où les $\mathbf{s}_i$ et $\mathbf{e}_i$ sont dans $\mathbb{F}^n$. Avec ces notations, nous avons

$$\Lambda \circ E(\mathbf{s}) = \big(\lambda(\mathbf{s}_1 \cdot \mathcal{H}_H^t), \ldots, \lambda(\mathbf{s}_T \cdot \mathcal{H}_H^t)\big) \ ,$$
$$\Lambda \circ E(\mathbf{s}+\mathbf{e}) = \big(\lambda((\mathbf{s}_1+\mathbf{e}_1) \cdot \mathcal{H}_H^t), \ldots, \lambda((\mathbf{s}_T+\mathbf{e}_T) \cdot \mathcal{H}_H^t)\big) \ .$$

Cela donne donc

$$\begin{aligned} d_H(\Lambda \circ E(\mathbf{s}), \Lambda \circ E(\mathbf{s}+\mathbf{e})) &= \sum_{i=0}^{T} d_H\Big(\lambda\left(\mathbf{s}_i \cdot \mathcal{H}_H^t\right), \lambda\left(\mathbf{s}_i \cdot \mathcal{H}_H^t + \mathbf{e}_i \cdot \mathcal{H}_H^t\right)\Big) \\ &= \left|\Big\{ i \mid \lambda\left(\mathbf{s}_i \cdot \mathcal{H}_H^t\right) \neq \lambda\left(\mathbf{s}_i \cdot \mathcal{H}_H^t + \mathbf{e}_i \cdot \mathcal{H}_H^t\right)\Big\}\right| \ . \end{aligned}$$

L'application λ étant bijective, on peut écrire

$$d_H(\Lambda \circ E(\mathbf{s}), \Lambda \circ E(\mathbf{s}+\mathbf{e})) = \left|\Big\{ i \mid \mathbf{e}_i \cdot \mathcal{H}_H^t \neq 0 \Big\}\right| \ .$$

Or, le mot $\mathbf{e}$ étant de poids au plus t, il ne peut y avoir que t mots $\mathbf{e}_i$ non nuls et il y a donc au plus t produits $\mathbf{e}_i \cdot \mathcal{H}_H^t$ non nuls, ce qui donne bien l'inégalité annoncée. □

Théorème 10.8 *Soient $\mathcal{C}$ la somme directe de T codes de Hamming de longueur $n = 2^r - 1$ et $\mathbf{C}$ un code de longueur T sur $\mathbb{F}_{2^r}$ corrigeant t erreurs. Les recouvrements $\mathcal{C}_\mathbf{x} = E^{-1}(\{\mathbf{x}\})$, $\Lambda(\mathbf{x}) \in \mathbf{C}$, sont de rayon T et deux à deux distants d'au moins $2t+1$.*

Preuve. Les ensembles $E^{-1}(\{\mathbf{x}\})$ sont toujours de rayon T puisque ce sont encore des translatés d'un recouvrement de rayon T – en l'occurrence il s'agit ici du code $\mathcal{C}$. Pour montrer qu'ils sont deux à deux distants d'au moins $2t+1$, nous allons prouver qu'aucun mot $\mathbf{v}$ à une distance inférieure ou égale à $2t$, bien que strictement positive, d'un ensemble $E^{-1}(\{\mathbf{x}\})$, $\Lambda(\mathbf{x}) \in \mathbf{C}$, ne peut appartenir à aucun des recouvrements de la famille $\mathcal{F} = (E^{-1}(\{\mathbf{z}\}))_{\Lambda(\mathbf{z})\in\mathbf{C}}$. Soient $\mathbf{x}$ un mot tel que $\Lambda(\mathbf{x}) \in \mathbf{C}$ et $\mathbf{v} \in \mathbb{F}^{n\cdot T}$, n'appartenant pas à $E^{-1}(\{\mathbf{x}\})$, mais à une distance au plus $2t$ de cet ensemble. Il existe donc un mot $\mathbf{s}$ dans le recouvrement $E^{-1}(\{\mathbf{x}\})$, de manière équivalente $E(\mathbf{s}) = \mathbf{x}$, tel que $d_H(\mathbf{s}, \mathbf{v}) \leq 2t$. Le lemme 10.7 implique alors $\Lambda \circ E(\mathbf{v}) \in B_{2t}^{2^r,T}(\Lambda(\mathbf{x}))$. Par hypothèse, le code $\mathbf{C}$ corrigeant t erreurs, sa distance minimale est au moins égale à $2t+1$, et par conséquent $\Lambda(x)$ est l'unique mot du code $\mathbf{C}$ appartenant à $B_{2t}^{2^r,T}(\Lambda(\mathbf{x}))$. Ainsi, $\Lambda \circ E(\mathbf{v})$ n'est pas un mot de $\mathbf{C}$ et donc

$$\mathbf{v} \notin \bigcup_{\Lambda(\mathbf{z}) \in \mathbf{C}} E^{-1}(\{\mathbf{z}\}) \ .$$

Cela étant vrai pour tout mot $\mathbf{v}$ du voisinage $\mathcal{V}_{2t}(E^{-1}(\{\mathbf{x}\}))$ n'appartenant pas au recouvrement $E^{-1}(\{\mathbf{x}\})$ lui-même, cela implique que $E^{-1}(\{\mathbf{x}\})$ est à une distance d'au moins $2t+1$ de tout autre recouvrement appartenant à la famille $\mathcal{F}$. Cela ne dépendant pas du mot $\mathbf{x}$, nous en déduisons que les recouvrements de $\mathcal{F}$ sont à une distance d'au moins $2t+1$ les uns des autres. $\square$

Lorsque $2t < T < 2^r$, on peut prendre pour $\mathbf{C}$ un code de Reed-Solomon de longueur T, corrigeant t erreurs sur $\mathbb{F}_{2^r}$. Ce dernier ayant $2^{r\cdot(T-2t)}$ mots, nous obtenons

Corollaire 10.9 *Pour T et t fixés, lorsque n tend vers l'infini, nous avons*

$$m(n, T, t) \gtrsim (T - 2t)\log(n) \ .$$

Détaillons les applications d'insertion et d'extraction pour la construction que nous venons de donner. En utilisant encore la bijection λ de $\mathbb{F}^r$ dans $\mathbb{F}_{2^r}$, étendue coordonnée par coordonnée en Λ, nous avons

$$\begin{array}{cccc} E: & \mathbb{F}^{n\cdot T} & \longrightarrow & \mathbb{F}^{r\cdot T} \\ & \mathbf{s} & \longmapsto & \mathbf{s}\cdot\mathcal{H}^t \end{array}$$

$$\begin{array}{cccc} I: & \Lambda^{-1}(\mathbf{C}) \times \mathbb{F}^{n\cdot T} & \longrightarrow & \mathbb{F}^{r\cdot T} \\ & (\mathbf{x}, \mathbf{v}) & \longmapsto & \mathbf{v} + D_{\mathcal{C}}(\mathbf{x} - E(\mathbf{v})) \end{array}$$

Ces applications sont quasiment identiques à celles que nous avons définies à la proposition 8.6 page 118 pour les schémas du modèle passif. La seule différence, essentielle cependant, est le domaine de définition de l'application d'insertion I qui dans le cas du modèle actif est restreint à $\Lambda^{-1}(\mathbf{C})$.

Toutefois, l'application d'extraction donnée ici n'inclut pas la correction des erreurs. Si le mot $\mathbf{s} = I(\mathbf{x}, \mathbf{v})$ est modifié en au plus t coordonnées, $E(\mathbf{s})$ ne vaut pas $\mathbf{x}$. Pour corriger l'erreur, il faut effectuer un décodage de $\Lambda \circ E(\mathbf{s})$ dans $\mathbf{C}$, et si effectivement $\mathbf{s}$ a été modifié en au plus t coordonnées, alors le mot obtenu $\mathbf{z}$ après ce décodage est $\Lambda(\mathbf{x})$.

Exemple 10.10 Nous reprenons pour $\mathcal{C}$ une somme de trois codes de Hamming de longueur 7 et utilisons comme matrice de parité celle définie à l'exemple 8.16 page 126. Nous allons utiliser pour $\mathbf{C}$ un code de Reed-Solomon de longueur 3 sur $\mathbb{F}_{2^3}$ corrigeant une seule erreur. En notant α

une racine du polynôme irréductible X^3+X+1, on peut prendre le code de Reed-Solomon engendré par la matrice

$$G = \begin{pmatrix} 1 & 1 & 1 \\ 0 & \alpha & \alpha^2 \end{pmatrix} .$$

Pour l'application λ, de $\mathbb{F}^3$ dans $\mathbb{F}_{2^3}$, nous utiliserons

$$\lambda(a_0, a_1, a_2) = a_0 + a_1\alpha + a_2\alpha^2 .$$

Le syndrome du mot

$$\mathbf{v} = \begin{pmatrix} 1100010 & 0110101 & 0001101 \end{pmatrix}$$

est alors

$$E(\mathbf{v}) = \begin{pmatrix} 101 & 110 & 011 \end{pmatrix}$$

et son image par Λ donne

$$\Lambda \circ E(\mathbf{v}) = \begin{pmatrix} 1+\alpha^2 & 1+\alpha & \alpha+\alpha^2 \end{pmatrix} .$$

Supposons que le message $\mathbf{x}$ à dissimuler corresponde au mot

$$\Lambda(\mathbf{x}) = \begin{pmatrix} 1 & 1 & 1 \end{pmatrix} \in \mathbf{C} ,$$

donc $\mathbf{x} = \begin{pmatrix} 100 & 100 & 100 \end{pmatrix}$. Nous cherchons alors un mot de poids au plus 3 dont le syndrome $\mathbb{F}^9$ soit

$$\mathbf{x} - E(\mathbf{v}) = \begin{pmatrix} 001 & 010 & 111 \end{pmatrix} .$$

Le mot

$$\mathbf{e} = \begin{pmatrix} 0001000 & 0100000 & 0000001 \end{pmatrix}$$

vérifie les hypothèses recherchées. On peut donc prendre

$$\begin{aligned} \mathbf{s} &= \mathbf{v} + \mathbf{e} \\ &= \begin{pmatrix} 1101010 & 0010101 & 0001100 \end{pmatrix} . \end{aligned}$$

Supposons maintenant que le mot $\mathbf{s}$ soit modifié en une coordonnée, par exemple la première, donnant ainsi le mot

$$\mathbf{s}' = \begin{pmatrix} 0101010 & 0010101 & 0001100 \end{pmatrix} .$$

Son syndrome est

$$E(\mathbf{s}') = \mathbf{u} = \begin{pmatrix} 000 & 100 & 100 \end{pmatrix} ,$$

dont l'image par Λ, valant $\begin{pmatrix} 0 & 1 & 1 \end{pmatrix}$, n'est plus un mot du code $\mathbf{C}$. Le résultat d'un décodage de $\mathbf{u}$ dans $\mathbf{C}$ redonne bien $\Lambda(\mathbf{x})$ et par conséquent $\mathbf{x}$. Remarquons qu'il n'y a pas de moyen pour retrouver le mot $\mathbf{s}$ à partir de $\mathbf{s}'$. Cela étant, ce n'est pas problématique puisque l'information n'est pas contenue dans $\mathbf{s}$ lui même, mais dans son syndrome qui, lui, peut être retrouvé. $\square$

Conclusion et perspectives

Cette partie relie le problème de la dissimulation d'information dans un document où tout bit est modifiable à des problèmes fondés sur le recouvrement, dans un cadre formel présenté au chapitre 7. Deux modèles de dissimulation sont envisagés.

Les résultats obtenus pour le premier modèle, celui que nous appelons à adversaire passif, sont satisfaisants : après réduction de notre problème de dissimulation au recouvrement de l'espace de Hamming, nous proposons des construction de schémas asymptotiquement optimaux. Ces résultats reposent en grande partie sur l'existence de recouvrements linéaires optimaux. De plus, tout code de recouvrement linéaire, constructible et décodable en temps polynomial en sa longueur, donne lieu, grâce à notre équivalence, à un schéma de dissimulation efficace. Toutefois, obtenir de tels codes est un problème difficile et nous n'avons une solution complète que lorsque la distorsion maximale est logarithmique en la longueur. D'autre part, loin d'être contraignant, notre modèle inclut de nombreux travaux comme nous l'avons montré au chapitre 9.

Le modèle à adversaire actif reste plus ouvert. Il constitue une généralisation du modèle précédent et équivaut au problème des codes correcteurs centrés. Ce dernier problème comprend celui des codes correcteurs en blocs. Or, dans ce domaine, et contrairement à ce qui se passe pour les recouvrements, la question de l'optimalité des codes linéaires est ouverte. Malgré cela, nous donnons une construction de schémas asymptotiquement bons, c'est-à-dire dont le logarithme du nombre de messages ne diffère, asymptotiquement de notre borne supérieure, que d'une constante multiplicative. Toutefois, rien ne prouve ni la finesse de la borne, ni l'optimalité de la construction. De futurs résultats sont donc envisageables dans cette direction.

Nous avons voulu, lorsque l'adversaire est susceptible d'intervenir, corriger toutes les erreurs de poids au plus $\mathtt{t}$. Une autre approche consiste à vouloir corriger le plus d'erreurs possible, c'est-à-dire à minimiser le nombre de motifs d'erreurs pour lesquels il n'est pas possible de corriger les erreurs introduites. Cela revient à assimiler notre adversaire à un canal binaire symétrique. Ce problème n'a pas encore été étudié dans le cas des codes centrés. En revanche, il est résolu pour les codes en blocs linéaires par le théorème de Shannon pour le canal binaire symétrique (cf. par exemple [Gal68, th. 6.2.1]) : à la condition que le taux de transmission soit inférieur à la capacité du canal, qui est directement liée à la probabilité d'erreur, il est possible de rendre la probabilité d'erreur après décodage aussi faible que souhaitée, au prix d'une longueur de code tendant vers l'infini. Ce résultat suggère qu'il en va de même pour les codes centrés.

Notre étude a porté sur le cas binaire, ce qui nous a amené naturellement à considérer des recouvrements binaires. L'utilisation de codes non binaires est une autre possibilité, mais dans ce cas, le modèle de dissimulation est certainement à améliorer, de même que la métrique utilisée.

Bibliographie

[An96a] R.J. Anderson (sld), *Proceedings of the workshop on information hiding,* Springer-Verlag, LNCS, vol. 1174, 1996, 306 p.

[An96b] R.J. Anderson, « Stretching the limits of steganography », dans [An96a], p. 39–48.

[AK98] E.F. Assmus et J.D. Key, « Polynomial codes and finite geometries », dans V.S. Pless et W.C. Huffman, *Handbook of coding theory,* North-Holland, 1998, p. 1269–1346.

[AP98] R.J. Anderson et F.A.P. Petitcolas, « On the limits of steganography », *IEEE Journal on Selected Areas in Communications*, vol. 16, n° 4, 1998, p. 474–481.

[AR02] N. Aydin et D.K. Ray-Chaudhuri, « Quasi-cyclic codes over $\mathbb{Z}_4$ and some new binary codes », *IEEE Transactions on Informations Theory*, vol. 48, n° 7, 2002, p. 2065–2069.

[Bar98] A. Barg, « Complexity issues in coding theory », dans V.S. Pless et W.C. Huffman, *Handbook of coding theory,* North-Holland, 1998, p. 649–754.

[Ber68] E. Berlekamp, *Algebraic coding theory,* McGraw-Hill, 1968.

[Bla72] I.F. Blake, « Codes over certain rings », *Information and Control*, vol. 20, 1972, p. 396–404.

[Bla75] I.F. Blake, « Codes over integer residue rings », *Information and Control*, vol. 29, n° 4, 1975, p. 295–300.

[Bli90] V.M. Blinovsky, « Asymptotically exact uniform bounds for spectra of cosets of linear codes », *Problems of Information Transmission*, vol. 26, n° 1, 1990, p. 83-86. (traduit du russe, *Problemy Peredachi Informatsii*, vol. 26, n° 1, 1990, p. 99–103).

[Bos] N. Boston, *A mathematical foundation for watermarking.* Preprint. (`http://www.math.wisc.edu/~boston/bostonpreps.html`).

[Bro98] A.E. Brouwer, « Bounds on the size of linear codes », dans V.S. Pless et W.C. Huffman, *Handbook of coding theory,* North-Holland, 1998, p. 295–461.

[BGM+96] W. Bender, D. Gruhl, N. Morimoto et A. Lu, « Techniques for data hiding », *IBM System Journal*, vol. 35, n° 3–4, 1996, p. 313–336.

[BMT78] E. Berlekamp, R.J. McEliece et H.C.A. van Tilborg, « On the inherent intractability of certain coding problems », *IEEE Transactions on Informations Theory*, vol. 29, n° 3, 1978, p. 384–386.

[BP99] L.A. Bassalygo et M.S. Pinsker, « Centered error-correcting codes », *Problems of Information Transmission*, vol. 35, 1999, p. 25–31. (traduit du russe, *Problemy Peredachi Informatsii*, vol. 35, n° 1, 1999, p. 30–37).

[BR00] J.T. Blackford et D.K. Ray-Chaudhuri, « A transform approach to permutation groups of cyclic codes over galois rings », *IEEE Transactions on Informations Theory*, vol. 46, n° 7, 2000, p. 2350–2358.

[BSC95] A. Bonnecaze, P. Solé et A.R. Calderbank, « Quaternary quadratic residue codes and unimodular lattices », *IEEE Transactions on Informations Theory*, vol. 41, n° 2, 1995, p. 366–377.

[Cac04] C. Cachin, « An information-theoretic model for steganography », *Information and Computation*, vol. 192, n° 1, 2004, p. 41–56. (version préliminaire dans [An96a, p. 306–318]).

[Car95] C. Carlet, « On $\mathbb{Z}_4$-duality », *IEEE Transactions on Informations Theory*, vol. 41, n° 5, 1995, p. 1487–1494.

[Car98] C. Carlet, « $\mathbb{Z}_{2^k}$-linear codes », *IEEE Transactions on Informations Theory*, vol. 44, n° 4, 1998, p. 1543–1547.

[Car99] C. Carlet, « On Kerdock codes », *Contemporary Mathematics*, vol. 255, 1999, p. 155-163.

[Coh83] G.D. Cohen, « A nonconstructive upper bound on covering radius », *IEEE Transactions on Informations Theory*, vol. 29, n° 3, 1983, p. 352–353.

[Cra98] R. Crandall, *Some notes on steganography*, 1998. Envoyé à la Steganography Mailing List. (`http://os.inf.tu-dresden.de/~westfeld/crandall.pdf`).

[CGM86] G. Cohen, P. Godlewski et F. Merkx, « Linear binary codes for write-once memories », *IEEE Transactions on Informations Theory*, vol. 32, n° 5, 1986, p. 697–700.

[CH97] I. Constantinescu et W. Heise, « A metric for codes over residue class rings », *Problems of Information Transmission*, vol. 33, n° 3, 1997, p. 208–213. (traduit du russe, *Problemy Peredachi Informatsii*, vol. 33, n° 3, 1997, p. 22–28).

[CHL+97] G. Cohen, I. Honkala, S. Litsyn et A. Lobstein, *Covering codes,* North-Holland, 1997.

[CJL+03] K. Chang, C. Jung, K. Lee, S. Lee et H. Yoo, « High quality perceptual information hiding technique for color images », dans *Proceedings of the Pacific Rim Workshop on Digital Steganography (STEG)*, 2003. (http://www.know.comp.kyutech.ac.jp/STEG03/STEG03-PAPERS/).

[CJL+04] K. Chang, C. Jung, S. Lee et W. Yang, « High quality perceptual steganographic techniques », dans *Proceedings of the 2003 International Workshop on Digital Watermarking*, éd. par T. Kalker, I.J. Cox et Y.M. Ro, Springer-Verlag, LNCS 2939, 2004, p. 518–531.

[CKL+96] I.J. Cox, J. Killian, T. Leighton et T. Shamoon, « A secure, robust watermark for multimedia », dans [An96a], p. 183–206.

[CLP97] A.R. Calderbank, W.-C.W. Li et B. Poonen, « A 2-adic approach to the analysis of cyclic codes », *IEEE Transactions on Informations Theory*, vol. 43, n° 3, 1997, p. 977–986.

[CM01] R. Chandramouli et N. Memon, « Analysis of lsb based image steganography techniques », dans *Proceedings of the IEEE International Conference on Image Processing*, vol. 3, 2001, p. 1019–1022.

[CMK+96] A.R. Calderbank, G. McGuire, P.V. Kumar et T. Helleseth, « Cyclic codes over $\mathbb{Z}_4$, locator polynomials and Newton's identities », *IEEE Transactions on Informations Theory*, vol. 42, n° 1, 1996, p. 217–226.

[CS95] A.R. Calderbank et N.J.A. Sloane., « Modular and p-adic cyclic codes », *Designs, Codes and Cryptography*, vol. 6, 1995, p. 21–35.

[DGL+01] I.M. Duursma, M. Greferath, S.N. Litsyn et S.E. Schmidt, « A $\mathbb{Z}_8$-linear lift of the binary Golay code and a non-linear binary $(96, 2^{37}, 24)$ code », *IEEE Transactions on Information Theory*, vol. 47, n° 4, 2001, p. 1596–1598.

[DP86] P. Delsarte et P. Piret, « Do most binary linear codes achieve the goblick bound on the covering radius ? », *IEEE Transactions on Informations Theory*, vol. 32, n° 6, 1986, p. 826–828.

[Fel85] M.R. Fellows, *encoding graphs in graphs,* Thèse de doctorat de l'université de californie, 1985.

[FGD01] J. Fridrich, M. Goljan et R. Du, « Detecting lsb steganography in color and gray-scale images », *Magazine of IEEE Multimedia*, vol. 8, n° 4, 2001, p. 22-28.

[FJM+96] E. Franz, A. Jerichow, S. Muller, A. Pfitzmann et I. Stierand, « Computer based steganography », dans [An96a], p. 7–21.

[Ga03a] F. Galand, *codes $\mathbb{Z}_{2^k}$-linéaires,* Rapport de recherche INRIA, janvier 2003.

[Ga03b] F. Galand, « On the minimum distance of some families of $\mathbb{Z}_{2^k}$-linear codes », dans *Proceedings of the 15th AAECC International Symposium*, éd. par M. Fossorier, T. Høholdt et A. Poli, Springer-Verlag, LNCS 2643, 2003, p. 235–243.

[Gal04] F. Galand, « Stéganographie », dans *Traité de sécurité des systèmes d'information*, Techniques de l'ingénieur, 2004.

[Gal68] R.G. Gallager, *Information theory and reliable communication,* Wiley, 1968, 608 p.

[GG99] J. von zur Gathen et J. Gerhard, *Modern computer algebra,* Cambridge University Press, 1999.

[GJ79] M.R. Garey et D.S. Johnson, *Computers and intractability : a guide to the theory of NP-completeness,* Freeman, 1979, 338 p.

[GK03a] F. Galand et G. Kabatiansky, « Information hiding by coverings », dans *Proceedings of the IEEE Information Theory Workshop*, 2003, p. 151–154.

[GK03b] F. Galand et G. Kabatiansky, « Steganography via covering codes », dans *Proceedings of the IEEE International Symposium on Information Theory*, 2003, p. 192.

[GS99] M. Greferath et S.E. Schmidt, « Gray isometries for finite chain rings and a nonlinear ternary $(36, 3^{12}, 15)$ code », *IEEE Transactions on Information Theory*, vol. 45, n° 7, 1999, p. 2522–2524.

[Hio03] H. Hioki, « A modified CPT scheme for embedding data into binary images », dans *Proceedings of the Pacific Rim Workshop on Digital Steganography (STEG)*, 2003. (`http://www.know.comp.kyutech.ac.jp/STEG03/STEG03-PAPERS/`).

[Hun80] T.W. Hungerford, *Algebra,* Springer-Verlag, 1980.

[HKC+94] R. Hammons, P.V. Kumar, A.R. Calderbank, N.J.A. Sloane et P. Solé, « Kerdock, Preparata, Goethals and other codes are linear over $\mathbb{Z}_4$ », *IEEE Transactions on Information Theory*, vol. 40, n° 2, 1994, p. 301–319.

[HKM+96] T. Helleseth, P.V. Kumar, O. Moreno et A.G. Shanbhag, « Improved estimates via exponential sums for the minimum distance of $\mathbb{Z}_4$-linear trace codes », *IEEE Transactions on Informations Theory*, vol. 42, n° 4, 1996, p. 1212–1216.

[HL00] T. Honold et I. Landjev, « Linear codes over finite chain rings », *The Electronic Journal of Combinatorics*, vol. 7, n° 1, 2000.
(`http://www.combinatorics.org/Volume\_7/v7i1toc.html`).

[HN99] T. Honold et A.A. Nechaev, « Weighted modules and representations of codes », *Problems of Information Transmission*, vol. 35, n° 3, 1999, p. 205–223. (traduit du russe, *Problemy Peredachi Informatsii*, vol. 35, n° 3, 1999, p. 18–39).

[Kas69] T. Kasami, « Weight distribution of Bose-Chaudhuri-Hocquenghem codes », *Combinatorial Mathematics and its Applications*, 1969, p. 335–357.

[Ker72] A.M. Kerdock, « A class of low-rate nonlinear codes », *Information and Control*, vol. 20, 1972.

[Ker83] A. Kerckhoffs, « La cryptographie militaire », *Journal des sciences militaires*, 1883, p. 5–38.

[KHC95] P.V. Kumar, T. Helleseth et A.R. Calderbank, « An upper bound for Weil exponential sums over Galois rings and applications », *IEEE Transactions on Informations Theory*, vol. 41, n° 2, 1995, p. 456–468.

[KL97] P. Kanwar et S.R. López-Permouth, « Cyclic codes over the integers modulo p^m », *Finite Fields and Their Applications*, vol. 3, 1997, p. 334–352.

[KN92] A.S. Kuzmin et A.A. Nechaev, « Construction of noise-stable codes using linear recurrent sequences over Galois rings », *Russian Mathematical Surveys*, vol. 47, n° 5, 1992, p. 189–190. (traduit du russe, *Uspehi Mat. Nauk.*, vol. 47, n°5, 1992, p. 183–184).

[KN94] A.S. Kuzmin et A.A. Nechaev, « Linearly presentable codes and Kerdock codes over arbitrary Galois fields of characteristic 2 », *Russian Mathematical Surveys*, vol. 49, n° 5, 1994, p. 183–184. (traduit du russe, *Uspehi Mat. Nauk.*, vol. 49, n°5, 1994, p. 165-166).

[KP02] S. Katzenbeisser et F. Petitcolas, « On defining security in steganographic systems », dans *Security and Watermarking of Multimedia Contents*, éd. par E.J. Delp et P.W. Wong, The International Society for Optical Engineering (SPIE), Proceedings of SPIE 4675, 2002, p. 50–56.

[KP99] S. Katzenbeisser et F.A.P. Petitcolas (sld), *Information hiding techniques for steganography and digital watermarking,* Artech House, 1999, 220 p.

[Lin99] J.H. van Lint, *Introduction to coding theory,* 3e édition, Springer-Verlag, 1999.

[Lit98] S.N. Litsyn, « An updated table of the best binary codes known », dans V.S. Pless et W.C. Huffman, *Handbook of coding theory,* North-Holland, 1998, p. 463–498.

[LN97] R. Lidl et H. Niederreiter, *Finite fields,* 2e édition, Cambridge University Press, Encyclopedia of Mathematics and its Applications, vol. 20, 1997.

[Mac74] B.R. MacDonald, *Finite rings with identity,* Dekker, 1974.

[Miz99] T. Mizzelholzer, « An information-theoretic approach to steganography and watermarking », dans *Proceedings of the Workshop on Information Hiding*, Springer-Verlag, LNCS 1768, 1999.

[MS96] F.J. MacWilliams et N.J.A. Sloane, *The theory of error-correcting codes,* 3e édition, North-Holland, 1996.

[Nec91] A.A. Nechaev, « Kerdock codes in a cyclic form », *Discrete Mathematics and Applications*, vol. 1, no 4, 1991, p. 365–384. (traduit du russe, *Diskretnaya Matematika*, vol. 1, no 4, 1989, p. 123–139).

[Pit96] I. Pitas, « A method for signature casting on digital images », dans *Proceedings of the IEEE International Conference on Image Processing*, vol. 3, 1996, p. 215–218.

[Pre68] F.P. Preparata, « A class of optimum nonlinear double-error correcting codes », *Information and Control*, vol. 16, no 4, 1968, p. 378–400.

[PCT00] H.-K. Pan, Y.-Y. Chen et Y.-C. Tseng, « A secure data hiding scheme for two-color images », dans *Proceedings of the IEEE Symposium on Computers and Communication*, 2000, p. 750–755.

[PQ96] V.S. Pless et Z. Qian, « Cyclic codes and quadratic residue codes over $\mathbb{Z}_4$ », *IEEE Transactions on Information Theory*, vol. 42, no 5, 1996, p. 1594–1600.

[PW95] O. Papini et J. Wolfmann , *Algèbre discrète et codes correcteurs,* Springer-Verlag, Mathématiques & Applications, vol. 20, 1995.

[PWW01] G. Pan, Y. Wu et Z. Wu, « A novel data hiding method for two-color images », dans *Proceedings of the International Conference on Information and Communications Security*, Springer-Verlag, LNCS 2229, 2001, p. 261–270.

[RS82] R.L. Rivest et A. Shamir, « How to reuse a "write-once" memory », *Information and Control*, vol. 55, no 1–3, 1982, p. 1–19.

[RS94a] B.S. Rajan et M.U. Siddiqi, « Transform domain characterization of cyclic codes over $\mathbb{Z}_m$ », *Applicable Algebra in Engineering, Communication and Computing*, vol. 5, no 5, 1994, p. 261–275.

[RS94b] B.S. Rajan et M.U. Siddiqi, « A generalized DFT for abelian codes over $\mathbb{Z}_m$ », *IEEE Transactions on Informations Theory*, vol. 6, n° 40, 1994, p. 2082–2090.

[Sha49] C.E. Shannon, « Communication theory of secrecy systems », *Bell System Technical Journal*, vol. 28, n° 4, 1949, p. 656–715.

[Sha79] P. Shankar, « On BCH codes over arbitrary integer rings », *IEEE Transactions on Informations Theory*, vol. 25, n° 4, 1979, p. 480–483.

[Sim84] G.J. Simmons, « The prisoners' problem and the subliminal channel », dans *Proceedings of Crypto'83 - Advances in Cryptology*, éd. par D. Chaum, Plenum Press, 1984, p. 51–67.

[Sim98] G.J. Simmons, « The history of subliminal channels », *IEEE Journal on Selected Areas in Communication*, vol. 16, n° 4, 1998, p. 452–462.

[Spi77] E. Spiegel, « Codes over $\mathbb{Z}_m$ », *Information and Control*, vol. 35, n° 1, 1977, p. 48–51.

[Spi78] E. Spiegel, « Codes over $\mathbb{Z}_m$, revisited », *Information and Control*, vol. 37, n° 1, 1978, p. 100–104.

[Săl99] A. Sălăgean-Mandache, « On the isometries between $\mathbb{Z}_{p^k}$ and $\mathbb{Z}_p^k$ », *IEEE Transactions on Information Theory*, vol. 45, n° 6, 1999, p. 2146–2148.

[SM95] D.R. Stinson et J.L. Massey, « An infinite class of counterexamples to a conjecture concerning nonlinear resilient functions », *Journal of Cryptology*, vol. 8, n° 3, 1995, p. 167–173.

[SSD+00] V.M. Sidelnikov, A.Yu. Serebriakov, A.G. Dyachkov et P.A. Vilenkin, *Methods of constructing steganographical channel*, 2000. Manuscript.

[STO94] R.G. van Schyndel, A.Z. Trikel et C.F. Osborne, « A digital watermark », dans *Proceedings of the IEEE International Conference on Image Processing*, vol. 2, 1994, p. 86–90.

[TP01] Y.-C. Tseng et H.-K. Pan, « Secure and invisible data hiding in 2-color images », dans *Proceedings of the IEEE Infocom*, vol. 2, 2001, p. 887-896.

[TP02] Y.-C. Tseng et H.-K. Pan, « Data hiding in 2-color images », *IEEE Transactions on Computers*, vol. 51, 2002, p. 873-880.

[TV91] M.A. Tsfasman et S.G Vlăduţ, *Algebraic-geometric codes,* Kluwer Academic Publishers, Mathematics and its Applications, 1991, 667 p.

[VT65] R.R. Varshamov et G.M. Tenengolts, « Codes which correct single asymmetric errors », *Automation and Remote Control*, vol.

26, n^o 2, 1965, p. 286–290. (Translated from Russian, *Avtomatika i Telemekhanika*, vol. 26, n^o 2, 1965, p. 288–292).

[Wal91] G. WALLACE, « The JPEG still picture compression standard », *Communications of the ACM*, vol. 34, n^o 4, 1991, p. 30-44.

[Wan97] Z.-X. WAN, *Quaternary codes,* World Scientific, Series on Applied Mathematics, vol. 8, 1997.

[Was82] S.K. WASAN, « On codes over $\mathbb{Z}_m$ », *IEEE Transactions on Informations Theory*, vol. 28, n^o 1, 1982, p. 117–120.

[Wes01] A. WESTFELD, « Capacity despite better steganalysis (F5 - A steganographic algorithm) », dans *Proceedings of the Workshop on Information Hiding*, Springer-Verlag, LNCS , 2001, p. 289–302.

[Wic98] S.B. WICKER, « Deep space applications », dans V.S. PLESS et W.C. HUFFMAN, *Handbook of coding theory,* North-Holland, 1998, p. 2119–2200.

[Wol99] J. WOLFMANN, « Negacyclic and cyclic codes over $\mathbb{Z}_4$ », *IEEE Transactions on Informations Theory*, vol. 45, n^o 7, 1999, p. 2527–2532.

[WL98] M.Y. WU et J.H. LEE, « A novel data embedding method for two-color facsimile images », dans *Proceedings of the International Symposium on Multimedia Information Processing*, 1998.

[WTL00] M. WU, E. TANG et B. LIU, « Data hiding in digital binary image », dans *Proceedings of the IEEE International Conference on Multimedia & Expo*, vol. 1, 2000, p. 393-396.

[ZC91] G. ZÉMOR et G. COHEN, « Error-correcting wom-codes », *IEEE Transactions on Informations Theory*, vol. 37, n^o 3, 1991, p. 730–734.

Index

Table des figures

Liste des tableaux

Table des matières

Première partie : codes $\mathbb{Z}_{p^k}$-linéaires

Seconde partie : schémas de dissimulation