Review of the book

"Codage, cryptologie et applications"

Bruno Martin

Presses Polytechniques et Universitaires Romandes

2004

ISBN: 2-88074-569-1

Eric Diehl

VP Security Systems &Technologies, Technicolor

2013-10-01

What the book is about

Le livre décrit les principes mathématiques de base de la cryptologie et des codes correcteurs. Une fois les principes compris, il aborde leurs usages au domaine des télécommunications. Le livre est en français.

The book succinctly describes the mathematical principles of cryptography and error-correcting codes. Once these principles are introduced, it presents their use in some to telecommunication applications. The book is written in French.

What the book is like

Chapter 1: *Théorie de l'information*

Le premier chapitre est une très brève introduction à la théorie de l'information. On présente les notions de quantité d'information, d'entropie de l'information et du taux, les codages pour canaux non bruités et canaux bruités. Les deux théorèmes de Shannon sont énoncés sans explication.

Chapter 2: *Compression de données*

Ce chapitre est une brève introduction à la compression. Il présente l'algorithme de RLE (Run Length Encoding), d'analyse statistique d'Huffman et les deux variantes de Ziv – Lempel (LZ77, LZ78). L'explication de LZ77 est pédagogiquement bien faite. Les exemples cités commencent à vieillir (MS-DOS !, pas de rar…).[1] L'introduction cite qu'il existe une nouvelle catégorie de procédé : méthodes heuristiques mais malheureusement ne les abordent pas.

[1] Il est vrai que le livre date de 2004.

Chapter 3: *Généralités sur la théorie des codes*

Ce très court chapitre donne quelques bases. Il définit la distance de Hamming et les boules. Avec quelques exemples, il essaie d'introduire les problèmes de codage à longueur fixe et de décodage (notamment en illustrant les incertitudes.)

Chapter 4: *Codes linéaires*

Ce chapitre définit ce qu'est un code linéaire, puis présente le décodage par classes latérales et par syndrome. Il clôt par la présentation de certaines propriétés qui seront utiles dans les chapitres suivants.

Les chapitres suivants sur les codes ont tous la même structure. Ils donnent la définition du code, comment le construire, comment le décoder, pour terminer sur des observations spécifiques.

Chapter 5: *Codes de Hamming*

Le code est présenté à l'aide d'un exercice sur la matrice de génération Ham(3) et le décodage est aussi illustré par un exemple. Ensuite le chapitre aborde Hamming étendu (qui permet de détecter 2 erreurs sans pouvoir les corriger).

Chapter 6: *Codes de Golay étendu*

Ce chapitre présente un code plus complexe, Golay, qui fut utilisé pour les transmissions de la sonde spatiale Voyager. C'est un code de longueur 24, de dimension 12 et qui peut corriger jusqu'à 3 erreurs. Deux exemples illustrent son décodage.

Chapter 7: *Codes de Reed-Muller*

Ce chapitre présente un exemple de code inductif : les codes de Reed Muller. Le but est de présenter un code inductif.

Chapter 8: *Codes cycliques*

Ce chapitre débute par un bref rappel sur les anneaux et les représentations polynomiales. Ensuite il introduit le codage et décodage en utilisant un code Hamming (7, 4, 3). Puis il cite brièvement trois exemples (sans les approfondir).

Chapter 9: *Codes correcteurs de paquets d'erreurs*

Le chapitre montre la différence entre décoder des erreurs aléatoires et décoder des erreurs par paquet. Ainsi, il introduit les techniques d'entrelacement qui permettent de diminuer l'impact d'un paquet d'erreurs car le paquet n'affecte pas un même mot d'information. Ensuite, l'auteur aborde l'entrelacement avec retard et l'entrelacement croisé.

Chapter 10: *Introduction aux codes convolutifs*

Le chapitre présente le codage par arbre de codage et par diagramme de transition. Il introduit la notion de distance libre pour connaitre la performance du code et son décodage.

Chapter 11: *Applications des codes correcteurs dans l'industrie*

L'auteur parcourt très rapidement l'exemple du disque compact audio (à base de code Reed-Solomon à entrelacement croisé), passe sur le CD-ROM, le Minitel (sigh !) et aborde le CRC. Il explore plus en détail le codage de la voix dans le standard GSM.

Chapter 12: *Théorie de la complexité*

Bien entendu, le chapitre commence d'abord par la machine de Turing déterministe et la classe P, puis les machines de Turing non-déterministes et les classes NP, coNP et NP complet. Ensuite, il présente brièvement quelques problèmes NP complet.

Chapter 13: *Complexité des problèmes de théorie des codes*

bb.

Chapter 14: *Complexité des problèmes de cryptographie*

Le chapitre montre que le problème des sous-ensembles est NP. Il aborde le problème de la primalité en s'étendant sur les « récents » progrès de l'algorithme d'Agrawal et al., et énonce le problème du log discret.

Chapter 15: *Introduction à la cryptologie historique*

Il aborde différents algorithmes de chiffrement mono-alphabétiques ainsi que leur cryptanalyse. Il passe ensuite aux chiffres poly-alphabétiques avec Vigénère ainsi que sa cryptanalyse. Il termine par les chiffres à transposition.

Chapter 16: *Cryptologie technique à clé secrète*

Ce chapitre démarre avec le one-time pad expliquant pourquoi il est robuste, puis continue avec les machines à rotors, et les Feistel et conclut sur une longue description du DES.

Chapter 17: *Cryptanalyse différentielle et linéaire des chiffres itérés*

Ce chapitre propose une bonne introduction à la cryptanalyse différentielle et la cryptanalyse linéaire. A mon avis, c'est le meilleur chapitre du livre.

Chapter 18: *Deux chiffres robustes : IDEA et AES*

Ce chapitre décrit brièvement les algorithmes IDEA et AES.

Chapter 19 : Différents modes de fonctionnement

Le chapitre présente les modes ECB, CFB, CBC et OFB. On notera l'absence par exemple du CTR.

Chapter 20 : Cryptographie à clé publique

La cryptographie asymétrique est introduite par la présentation de l'algorithme Merkle-Hellman basé sur le problème du sac à dos. Il explique le problème du sac à dos et comment on peut le transformer en un crypto système. Ensuite, il fait une présentation classique du RSA et une très brève de l'algorithme El Gamal.

Chapter 21 : signatures numériques

Ce chapitre introduit les propriétés escomptées d'une signature numérique. Il présente rapidement les signatures par RSA, par El Gamal et enfin DSS.

Chapter 22 : *Fonctions de hachage*

Ce chapitre introduit les propriétés escomptées d'une fonction de hachage. Grace au paradoxe de l'anniversaire, il explique comment dimensionner une telle fonction pour réduire les risques de collision. Il décrit le hachage par log discret, compressif, MD5 et SHA-1. De bien entendu, les sections sur les attaques datent car elles sont antérieures aux travaux de Wang.

Chapter 23 : *Sûreté des chiffres à clé publique*

Cette section présente des attaques sur Merkle – Hellman (présenté au chapitre 20), sur la factorisation RSA et comment calculer le logarithme discret d'El Gamal. Tout d'abord, il introduit les réseaux arithmétiques, la réduction de réseaux de dimension 2 (notamment la méthode de Gauss), la réduction de réseaux de dimension supérieure à 3, et enfin la méthode de Lenstra, Lenstra et Lovasz (LLL). Ensuite, il applique LLL à Merkle – Hellman. Il explore ensuite la factorisation de nombres premiers avec la méthode du crible quadratique. Il aurait été intéressant de donner les performances. Pour le log discret, il présente les méthodes de Shanks et Polard. La première partie est probablement la section la plus approfondie de ce livre.

Chapter 24 : *Génération de suites pseudo-aléatoires*

La section n'aborde que les générateurs pseudo-aléatoires basés sur le schéma Blum et Micali. Il aurait été intéressant de citer au moins d'autres méthodes, tels que LFSR (qui est décrit dans l'annexe A) ou Yarrow.

Chapter 25 : *Certification*

Ce chapitre introduit l'attaque Man In The Middle puis rapidement les certificats numériques de clé publique (avec X509). Le chapitre est très court pour un tel sujet.

Chapter 26 : *Gestion des clés*

Le chapitre aborde la gestion des clés. Il décrit brièvement quelques méthodes de distribution de clés secrètes présentées dans ISO 11770-2. Ensuite, il présente le mécanisme d'établissement de clé de session de Diffie Hellman. Le chapitre est trop court pour un tel sujet.

Chapter 27 : *Applications de la cryptographie à la sécurité des réseaux*

Ce dernier chapitre propose une introduction à certaines contraintes de sécurité des communications (confidentialité, intégrité et disponibilité[2]). Il présente le modèle ISO. La dernière partie décrit Kerberos, IPSec et PGP.

Recommendation

Le livre n'a pas défini son lectorat. De fait, il n'est pas assez détaillé, ni approfondi pour un public averti. Par exemple, certains chapitres sont trop succincts. Pour les débutants et étudiants, le livre exige des bonnes bases mathématiques. Il n'accompagne pas le lecteur néophyte dans la compréhension des principes et démonstrations. De plus, les exemples applicatifs sont trop simplifiés et ne montrent pas la complexité de concevoir un système sécurisé. Le livre datant de 2004, les exemples sont parfois obsolètes et le livre n'est plus à jour quant aux dernières avancées.

Chaque chapitre a des références bibliographiques qui permettent d'approfondir le sujet. Une mention spéciale pour la très bonne introduction à l'analyse différentielle.

The book does not define its target audience. Thus, it is not enough detailed for a skilled audience. Some chapters are too short. For beginners and students, the book requires mathematical background that they will have to find elsewhere. The book does not really help unskilled readers to grasp the principles and mathematical demonstrations. The examples are too simplified and do not highlight the difficulty of designing secure systems. The book was published in 2004, so the examples are sometimes obsolete. Furthermore, the book is not up to date with the latest progress in the field.

Each chapter proposes a bibliography to expand on the topic. A special mention for the good introduction to differential analysis.

The reviewer is VP Security System & Technologies at Technicolor.