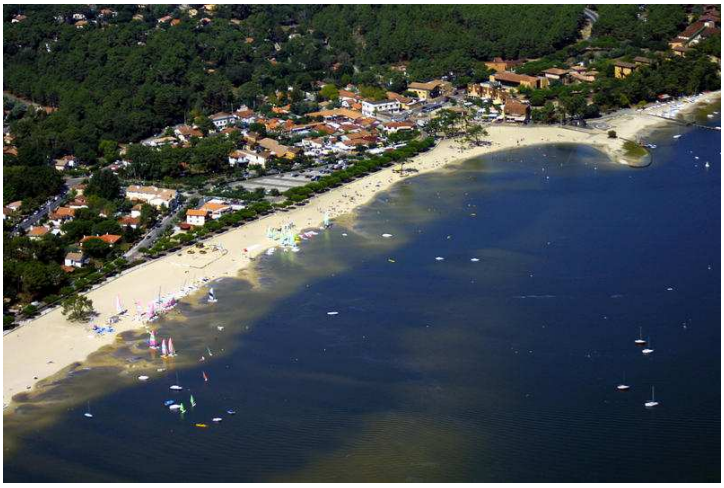
Journées
Codage et Cryptographie
2008



Recueil des résumés

Carcans Maubuisson

17-21 mars 2008

Comité de programme :

Daniel Augot	INRIA Paris-Rocquencourt
Christine Bachoc	Université de Bordeaux I
Claude Carlet	Université Paris 8
Philippe Gaborit	Université de Limoges
Marc Girault	France Télécom, Caen
Laurent Imbert	CNRS - Université de Montpellier 2
Jean-Pierre Tillich	INRIA Paris-Rocquencourt
Gilles Zémor	Université de Bordeaux I

Comité d'organisation :

Christine Bachoc	Université de Bordeaux I
Jean Creignou	Université de Bordeaux I
Gilles Zémor	Université de Bordeaux I

Remerciements :

L'équipe des organisateurs remercie pour leur soutien : le CNRS, l'INRIA, le laboratoire IMB et l'équipe A2X de l'université Bordeaux I, l'université Bordeaux I, l'université de Limoges, la Direction Générale de l'Armement, France Télécom et la région Aquitaine.

Programme

Lundi

9h	**C2 (codage - cryptographie) et biométrie**
10h	*Hervé Chabanne*
10h	A biometric identification scheme with encrypted templates
10h30	*Bruno Kindarji, Julien Bringer et Hervé Chabanne*
Pause	
11h	**Protocoles de retrait d'informations privé (PIR)**
12h	*Carlos Aguilar*
12h	Les preuves de connaissance à divulgation nulle de connaissance sont faciles à utiliser
12h30	*Sebastien Canard, Iwen Coisel et Jacques Traoré*
Repas	
16h	Bornes de la programmation linéaire pour les codes sur les matrices unitaires complexes
16h30	*Jean Creignou et Hervé Diet*
16h30	Codes cycliques tordus sur les anneaux de Galois
17h	*Patrick Solé, Félix Ulmer et Delphine Boucher*
17h	Codes tordus dont le rang ou la distance minimale est prescrite
17h30	*Lionel Chaussade, Félix Ulmer et Pierre Loidreau*
Pause	
18h	Sur des équations clés géneralisées pour l'algorithme de Guruswami-Sudan
18h30	*Daniel Augot*
18h30	Cryptanalysis of a McEliece cryptosystem based on quasi-cyclic LDPC codes
19h	*Ayoub Otmani, Jean-Pierre Tillich et Léonard Dallot*

Mardi

9h	**Résoudre le problème du plus court vecteur d'un réseau euclidien**
10 h	*Damien Stehlé*
10h	Pistes pour l'analyse probabiliste de la réduction des réseaux
10h30	*Brigitte Vallée et Antonio Vera*
Pause	
11h	Attaque de tatouage d'image fondée sur une estimation bayésienne non-linéaire non-paramétrique dans le domaine des ondelettes
11h30	*Larbi Boubchir, Nadia Zerida et Ayoub Otmani*
11h30	Codage et cryptanalyse linéaire
12h	*Benoit Gérard*
12h	Codes LDPC non-binaires hybrides
12h30	*Lucile Sassatelli et David Declercq*
Repas	
14h	**Discussion sur le GDR IM et le groupe de travail C2**
	Claude Carlet, Brigitte Vallée
16h	Algebraic cryptanalysis of curry and flurry using correlated messages
16h30	*Jean-Charles Faugère et Ludovic Perret*
16h30	On the MinRank problem
17h	*Jean-Charles Faugère, Françoise Levy-dit-Vehel et Ludovic Perret*
17h	McEliece cryptosystem; security and implementation
17h30	*Bhaskar Biswas et Nicolas Sendrier*
Pause	
18h	Polynômes de permutation à trappe et chiffrement à clef publique
18h30	*Guilhem Castagnos et Damien Vergnaud*
18h30	Preuve de sécurité concrète du schéma de signature de Courtois, Finiasz et Sendrier
19h	*Léonard Dallot*

Mercredi

9h	**Arithmétique rapide pour la cryptographie des courbes elliptiques**
10 h	*Laurent Imbert*
10h	Attaque DPA contre l'algorithme de Miller
10h30	*Nadia El Mrabet*
Pause	
11h	**Comment compter le nombre de points sur une courbe elliptique ?**
12h	*Christophe Ritzenthaler*
12h	Faster computation of pairings in Edwards coordinates
12h30	*Sorina Ionica et Antoine Joux*
Repas	

Jeudi

9h 10 h	**Une introduction aux codes correcteurs quantiques** *Jean-Pierre Tillich*
10h 10h30	Réconciliation de variables gaussiennes corrélées dans le cadre de protocole de cryptographie quantique *Anthony Leverrier, Romain Alléaume, Joseph Boutros, Gilles Zémor et Philippe Grangier*
Pause	
11h 11h30	Zero-error capacity of quantum channels *Romain Alléaume, Hugues Randriam, Gérard Cohen, Rex A. C. Medeiros et Francisco M. de Assi*
11h30 12h15	Codage des mots de poids constant *Nicolas Sendrier*
Repas	
16h 16h30	Multiplication scalaire de Montgomery pour les courbes de genre 2 en caractéristique 2 *Sylvain Duquesne*
16h30 17h	Codes fonctionnels sur des surfaces quadriques *Frédéric A. B. Edoukou*
17h 17h30	Twisting geometric codes *Majid Farhadi et Marc Perret*
Pause	
18h 18h30	Synthèse des ℓ-séquences décimées *Cédric Lauradoux et Andrea Roeck*
18h30 19h	Cryptanalyse de LFSRs combinés *Frédéric Didier, Yann Laigle-Chapuy*

Vendredi

9h 10 h	**Les canaux numériques à antennes multiples : modèles mathématiques, codage correcteur d'erreurs pour les systèmes MIMO, et leurs caractéristiques informationelles** *Joseph Boutros*
Pause	
10h30 11h	Approximation d'une fonction à l'aide de moins de variables *Anne Canteaut et María Naya-Plasencia*
11h 11h30	Attaques génériques sur les schémas de Feistel avec permutations internes *Joana Treger*
11h30 12h	Produire une collision pour SHA-0 en une heure *Stéphane Manuel et Thomas Peyrin*
Repas	
14 h	**Départ du Bus**

Tutoriels

Exposés tutoriels

C2 (codage - cryptographie) et biométrie

Hervé Chabanne
Sagem Défense Sécurité

Dans ce tutoriel, nous rappelons les principes de l'authentification biométrique et nous expliquons pourquoi le chiffrement des données est nécessaire pour le respect de la vie privée. Nous examinons d'un point de vue pratique les performances et la sécurité des Secure Sketches qui ont été introduits par Juels et Wattenberg en 1999 pour remplacer un matching biométrique par une correction d'erreurs. Nous présentons également différents schémas d'interrogation d'une base de données chiffrée où l'emploi de cryptosystèmes homomorphes est déterminant.
(Une partie du travail présenté a été effectuée lors du projet ANR BACH avec Julien Bringer, David Pointcheval, Malika Izabachène, Qiang Tang et Sébastien Zimmer. Une autre partie a été réalisée avec Julien Bringer, Gérard Cohen, Bruno Kindarji et Gilles Zémor.)
Bibliographie.

1. Julien Bringer, Hervé Chabanne, Malika Izabachène, David Pointcheval, Qiang Tang, Sébastien Zimmer. An application of the Goldwasser-Micali cryptosystem to biometric authentication. In ACISP, volume 4586 of Lecture Notes in Computer Science, pages 96-106. Springer, 2007.

2. Julien Bringer, Hervé Chabanne, Gérard Cohen, Bruno Kindarji, Gilles Zémor. Optimal iris fuzzy sketches. In BTAS, 6 pages. IEEE, 2007.

3. Julien Bringer, Hervé Chabanne, David Pointcheval, Qiang Tang. Extended private information retrieval and its application in biometrics authentications. In CANS, volume 4856 of Lecture Notes in Computer Science, pages 175-193. Springer, 2007.

4. Qiang Tang, Julien Bringer, Hervé Chabanne, David Pointcheval. A formal study of the privacy concerns in biometric-based remote authentication schemes. In ISPEC, à paraître Lecture Notes in Computer Science. Springer, 2008.

5. Julien Bringer, Hervé Chabanne. An Authentication Protocol with Encrypted Biometric Data. In Africacrypt, à paraître Lecture Notes in Computer Science. Springer, 2008.

Le Retrait d'Informations Privé (RIP)
Private Information Retrieval (PIR)

Carlos Aguilar Melchor
XLIM, Université de Limoges
carlos.aguilar@unilim.fr

En général, pour récupérer un élément d'une base de données, un utilisateur envoie une requête indiquant quel élément l'intéresse, puis la base lui renvoie l'élément en question. Quel élément de la base de données intéresse un utilisateur peut être une information que celui-ci souhaite garder secrète, même auprès des administrateurs de la base. Par exemple, la base peut être :

- une bibliothèque électronique, et quels livres nous lisons peut fournir des informations sur nos convictions politiques, ou certains détails de notre personnalité qu'il peut être souhaitable de garder confidentiels ;
- une base de données pharmaceutique, et certains laboratoires clients de la base peuvent désirer qu'on ne puisse pas savoir à quels principes actifs ils s'intéressent ;
- des cours d'actions, et les clients peuvent être des investisseurs ne voulant pas dévoiler quels cours les intéressent.

Une manière évidente de résoudre ce problème consiste pour un utilisateur à télécharger toute la base, et à extraire localement l'information qui l'intéresse. Ceci est en général inacceptable, voir même impossible si la base est de taille extrêmement importante (par exemple une bibliothèque électronique), confidentielle (par exemple, une base de données pharmaceutique), ou rapidement obsolète (par exemple, des cours d'actions).
Un protocole PIR est un protocole permettant à un utilisateur d'obtenir un élément d'une base de données, sans dévoiler aucune information, même aux gestionnaires de la base, sur quel élément particulier l'intéresse, *avec une quantité de données transférées sous linéaire par rapport à la taille de la base.*
Cet axe de recherche est scindé en deux, selon que la base de données sur laquelle le retrait s'effectue soit répliquée ou pas. Nous introduirons d'abord les protocoles PIR opérant sur des bases de données répliquées puis, assez rapidement, nous nous centrerons sur les protocoles opérant sur des bases de données non répliquées. Après un historique des protocoles existants nous commenterons plusieurs utilisations non conventionnelles qui mettent en relief l'intérêt de ces protocoles au delà des applications triviales.

Résoudre le problème du plus court vecteur d'un réseau euclidien

Damien Stehlé
LIP, École Normale Supérieure de Lyon

Un réseau euclidien est l'ensemble des combinaisons linéaires à coefficients entiers de d vecteurs linéairement indépendants dans un $\mathbb{R}^n$. Ces vecteurs forment une base du réseau qu'ils engendrent. Le problème algorithmique le plus naturel lié aux réseaux euclidiens est le problème du plus court vecteur (SVP pour *Shortest Vector Problem*) : étant donnée une base d'un réseau, il s'agit de trouver un vecteur non nul du réseau de norme minimale. Ce problème est NP-difficile sous des réductions randomisées [1], ainsi il y a peu d'espoir de le résoudre efficacement.
Cependant, du fait de son importance dans de nombreuses applications, plusieurs algorithmes le résolvant existent. Nous nous intéresserons à un algorithme en particulier, découvert indépendamment par Kannan [7] et Fincke et Pohst [2]. Cet algorithme repose sur une énumération exhaustive de points à coordonnées entières dans des hyper-ellipsoïdes. Cette recherche exhaustive est la méthode la plus efficace à ce jour pour résoudre SVP en pratique.
SVP est central dans le domaine de la cryptographie à clé publique reposant sur les réseaux euclidiens. Plusieurs primitives cryptographiques reposent sur des instances particulières de de problème. C'est le cas en particulier du cryptosystème NTRU [6]. D'autres fonctions cryptographiques sont possibles grâce aux réseaux, comme la signature, les fonctions de hachage, et même le chiffrement reposant sur l'identité [3]. La cryptanalyse la plus directe de ces primitives consiste à résoudre des variantes affaiblies de SVP sur des réseaux particuliers.
Dans cet exposé, nous décrirons l'algorithme d'énumération et des résultats récents qui en fournissent une analyse précise [4, 5] : si d est la dimension du réseau, la complexité dans le cas le pire de l'algorithme de Kannan est essentiellement $d^{\frac{d}{2e}}$. Nous dresserons un tableau rapide de l'utilisation des réseaux euclidiens pour construire des primitives cryptographies, et enfin nous montrerons comment l'algorithme d'énumération intervient dans la cryptanalyse de ces derniers.

Références

[1] M. Ajtai. The shortest vector problem in L_2 is NP-hard for randomized reductions. In *Proceedings of STOC 1998*, pages 10–19. ACM Press, 1998.

[2] U. Fincke and M. Pohst. A procedure for determining algebraic integers of given norm. In *Proceedings of EUROCAL*, volume 162 of *Lecture Notes in Computer Science*, pages 194–202, 1983.

[3] C. Gentry, C. Peikert, and V. Vaikuntanathan. Trapdoors for hard lattices and new cryptographic constructions. Cryptology ePrint 2007/432, 2007.

[4] G. Hanrot and D. Stehlé. Improved analysis of Kannan's shortest lattice vector algorithm. In *Proceedings of CRYPTO 2007*, volume 4622 of *Lecture Notes in Computer Science*, pages 170–186. Springer-Verlag, 2007.

[5] G. Hanrot and D. Stehlé. Worst-case Hermite-Korkine-Zolotarev reduced lattice bases. Inria Research Report 6422, 2008.

[6] J. Hoffstein, J. Pipher, and J. H. Silverman. NTRU : a ring based public key cryptosystem. In *Proceedings of the 3rd Algorithmic Number Theory Symposium (ANTS III)*, volume 1423 of *Lecture Notes in Computer Science*, pages 267–288. Springer-Verlag, 1998.

[7] R. Kannan. Improved algorithms for integer programming and related lattice problems. In *Proceedings of the 15th Symposium on the Theory of Computing (STOC 1983)*, pages 99–108. ACM Press, 1983.

Quelques pistes pour accélérer les calculs sur les courbes elliptiques

Laurent Imbert,
Laboratoire d'Informatique,
de Robotique et de Microélectronique de Montpellier
(LIRMM), CNRS

Les courbes elliptiques et les jacobiennes de courbes hyperelliptiques de petit genre, définies sur un corps fini, constituent d'excellents outils pour la cryptographie à clé publique. La conception d'un système efficace de signature, d'authentification ou de chiffrement basé sur ce type d'objet, nécessite des algorithmes et des systèmes arithmétiques optimisés. Ces besoins interviennent à plusieurs niveaux :

- au niveau de la courbes elliptiques, l'opération la plus coûteuse étant la multiplication scalaire (l'addition d'un point à lui même un grand nombre de fois) ;
- au niveau du corps fini, essentiellement de deux types : corps de la forme $\mathbb{Z}/p\mathbb{Z}$ ou p est un nombre premier de taille pouvant aller jusqu'à plusieurs centaines de bits, ou extensions de la forme $\mathbb{F}_{2^m}$ où le degré m de l'extension est du même ordre de grandeur que dans le cas premier ;
- au niveau des calculs sur grands nombres (entiers, rationnels, réels, etc) et sur les polynômes ;
- au niveau des choix de codages en machine de ces objets mathématiques et des algorithmes élémentaires qui en découlent.

Les choix d'implémentation sont multiples : forme du modulo pour les corps premiers, représentation des éléments et forme du polynôme irréductible pour les extensions, paramètre des courbes génériques ou famille de courbes particulières, système de coordonnées pour le codage des points, etc. Parmi toutes les combinaisons compatibles, il est bien difficile de définir précisément un cadre optimal.

Dans cet exposé, je présente quelques choix arithmétiques et algorithmiques pour accélérer les calculs sur les courbes elliptiques. Je donne quelques éléments sur les choix de corps finis, je rappelle les algorithmes de multiplication scalaire sur les courbes génériques et je présente quelques familles de courbes particulières avec de bonnes propriétés, comme les courbes de Montgomery, les courbes de Koblitz, les courbes DIK2 et DIK3, et les courbes sous la forme d'Edwards.

Références

[1] D. Hankerson, A. Menezes, and S. Vanstone. *Guide to Elliptic Curve Cryptography*. Springer, 2004.

[2] R. Avanzi, H. Cohen, C. Doche, G. Frey, T. Lange, K. Nguyen, and F. Vercauteren. *Handbook of Elliptic and Hyperelliptic Curve Cryptography*. CRC Press, 2005.

[3] P. L. Montgomery. Speeding the Pollard and elliptic curve methods of factorization. *Mathematics of Computation*, 48(177):243–264, January 1987.

[4] J. A. Solinas. Improved algorithms for arithmetic on anomalous binary curves. Research Report CORR-99-46, Center for Applied Cryptographic Research, University of Waterloo, Waterloo, ON, Canada, 1999. Updated version of the paper appearing in the proceedings of CRYPTO'97.

[5] C. Doche, T. Icart, and D. R. Kohel. Efficient scalar multiplication by isogeny decompositions. In *Public Key Cryptography, PKC'06*, volume 3958 of *Lecture Notes in Computer Science*, pages 191–206. Springer, 2006.

[6] V. Dimitrov, L. Imbert, and P. K. Mishra. The double-base number system and its application to elliptic curve cryptography. *Mathematics of Computation*, 77(262):1075–1104, 2008.

[7] H. M. Edwards. A normal form for elliptic curves. *Bulletin of the American Mathematical Society*, 44(3):393–422, 2007.

[8] D. J. Bernstein and T. Lange. Faster addition and doubling on elliptic curves. In *Advances in cryptology, ASIACRYPT 2007*, volume 4833 of *Lecture Notes in Computer Science*, pages 29–50. Springer, 2007.

Comment construire de bonnes courbes elliptiques ?

Christophe Ritzenthaler
Institut de mathématiques de Luminy

Les courbes elliptiques sont devenues un outil central dans la cryptographie à clé publique. Leurs points rationnels sur un corps fini $\mathbb{F}_{p^n}$ forment en effet un groupe pour lequel le problème du logarithme discret ne connaît pas en général de solution en temps sous-exponentiel. Cela leur confère un avantage évident sur les groupes multiplicatifs $\mathbb{F}_q^*$. Reste à en construire (rapidement) avec un sous-groupe cyclique ayant un ordre premier de taille cryptographique. J'évoquerai dans cet exposé trois grandes catégories d'algorithmes pour atteindre cet objectif :

- Les premiers (élémentaires) construisent la courbe sur un petit corps puis considèrent le groupe sur une extension. Malheureusement dans certains cas des attaques existent et l'on préfère éviter cette construction.
- Les seconds procèdent par tirage aléatoire d'une courbe elliptique puis déterminent rapidement son nombre de points. Les méthodes de comptage ont connu des développements impressionnants durant ces dernières années. On peut distinguer trois groupes :
  1. les méthodes l-adiques initiées par Schoof. Ce sont les seules efficaces lorsque p est grand.
  2. Les méthodes p-adiques autour du relèvement canonique : très efficaces lorsque p est petit, en particulier le cas $p = 2$ grâce à la méthode AGM de Mestre.
  3. Les méthodes p-adiques cohomologiques (algorithme de Kedlaya,...).
- La dernière catégorie regroupe les constructions CM (multiplication complexe par un corps quadratique imaginaire K). On construit une courbe elliptique sur un corps de nombres dont le nombre de points de la courbe réduite modulo p est obtenu par de l'arithmétique élémentaire dans le corps K. On fait alors varier p jusqu'à obtenir les conditions souhaitées sur l'ordre du groupe. Ces courbes (rares) peuvent être construites de trois façons : par des méthodes analytiques qui ont connues des raffinements récents ; par relèvement canonique ; par des techniques mixtes.

Toutes ces méthodes font appel à des résultats profonds de géométrie arithmétique. Mon but sera donc d'en donner l'idée centrale, leur cadre d'application avec leur complexité et records actuels ainsi que les directions des derniers développements.

Références

[1] R. Avanzi, H. Cohen, C. Doche, G. Frey, T. Lange, K. Nguyen, and F. Vercauteren : *Handbook of Elliptic and Hyperelliptic Curve Cryptography*, CRC Press, (2005).

[2] J. Belding, R. Bröker, A. Enge, K. Lauter : Computing Hilbert Class Polynomials, à paraître dans ANTS-VIII, (2008).

[3] A. Chambert-Loir : compter (rapidement) le nombre de solutions d'équations dans les corps fini, Séminaire Bourbaki, **968**, (2007).

[4] D. Hankerson, A. Menezes, and S. Vanstone : *Guide to Elliptic Curve Cryptography*, Springer, (2004).

[5] F. Vercauteren : *Computing zeta functions of curves over finite fields*, PhD thesis, Katholieke Universiteit Leuven, (2003).

Une introduction aux codes correcteurs quantiques

Jean-Pierre Tillich
(INRIA Paris-Rocquencourt)

Depuis la preuve par Shor en 1994 qu'un ordinateur quantique pouvait factoriser les entiers en temps polynomial, de nombreux résultats montrant qu'un tel ordinateur pouvait résoudre un certain nombre de tâches de manière plus efficace qu'un ordinateur classique ont été obtenus. Cependant, la construction d'une telle machine reste un problème largement ouvert : un des problèmes majeurs étant de combattre le phénomène de décohérence affectant les qubits. Ce problème peut néanmoins être traité par l'utilisation de codes correcteurs quantiques.
Nous présenterons dans cet exposé la première construction de codes correcteurs quantiques due à Shor. Nous montrerons ensuite en quoi elle est un cas particulier d'une construction plus générale appelée "codes stabilisateurs". Cette dernière famille de codes correcteurs quantiques a pour particularité d'être très proche des familles de codes linéaires classiques. On peut notamment définir pour de tels codes des équivalents quantiques des matrices génératrices ou de parité et traiter le problème de correction d'erreur comme un problème discret bien que le code correcteur quantique lui-même soit un espace continu. Ceci pourrait faire penser que de nombreux résultats obtenus pour les codes linéaires classiques peuvent être transportés au monde quantique. Ceci n'est que partiellement vrai. Nous montrerons notamment en quoi le phénomène de dégénérescence des erreurs quantiques pose problème pour calculer la capacité de canaux quantiques même très simples.

A tutorial introduction to space-time coding: mathematical models, information theoretical aspects, and coding for MIMO channels

Joseph J. Boutros
Texas A&M University at Qatar

This is a MIMO tutorial intended for mathematicians and coding theorists. Basic results on multiple antenna modulation and coding are presented. A strong background in communication theory or signal processing is not necessary for understanding this MIMO introduction, classical notions from algebraic coding theory and probability theory should suffice.

An old technique used in wireless communication systems to combat fading is to install multiple receive antennas. With enough spacing between antennas (usually half the wavelength) and high scattering in the wireless channel, the fading process is independent from one receive antenna to another. From a coding theory point of view, multiple receive antenna are equivalent to repetition coding. Multiple replica of the same information are created in order to combat fading, erasures, and link outage. In general, a non-trivial error-correcting code of rate $1/L$ would create L replicas and also yield a coding gain that protects against stationary noise. The creation of L replicas by means of receive antennas or any other method is referred to as *L-order diversity*.

More recently, very powerful error-correcting codes have been discovered. Those codes belong to a family referred to as *graph codes*, it includes Low-density parity-check (LDPC) codes and Turbo codes. The maximum possible information rate of single transmit antenna channels has been attained (or at least well approached) by graph codes under iterative message passing decoders.

In order to break the barrier of channel capacity and enable high data rate wireless transmissions (up to 1 Gbit/sec), multiple antennas are used at the transmitter side. This new channel is referred to as *MIMO*, i.e., multiple-input multiple-output channel, in contrast to previous SISO and SIMO channels. When all transmit antennas are conveying independent information streams, the overall transmission rate is multiplied accordingly but the diversity order does not increase. In this case, there is no transmit diversity but a spatial multiplexing gain is obtained. When all transmit antennas are conveying equivalent information streams, the overall diversity order is multiplied accordingly and the potential increase in data rate is sacrificed. At a given trade-off between diversity and multiplexing gain, an optimal space-time code should be full diversity and should exhibit the highest possible coding gain.

The tutorial is structured as follows. The first part of the tutorial explains the basic notion of diversity, then it follows by introducing the MIMO channel model and how its error probability can be characterized.

- Definition of diversity, an example with the erasure channel. Further generalization to diversity in Rayleigh fading channels.
- The multiple antenna channel model. The simplest mathematical model is given.
- Spatial multiplexing and the multiplexing gain.
- Coding gain, transmit and receive diversity in MIMO channels.

In the second part, we briefly present the capacity of a MIMO channel in the information theoretical sense. The influence of the number of antennas is highlighted. The notion of outage is introduced for quasi-static and slowly varying channels. We also show how the MIMO channel can be regarded as a set of parallel channels when perfect channel knowledge is available at transmitter. Bounds on the performance of space-time coding are derived in this part.

- Capacity when channel is unknown at transmitter.
- Outage probability for non-ergodic multiple-antenna channels.
- Capacity when channel is known at transmitter.

In the third part of the tutorial, we start by developing the design criteria for space-time coding. It is shown how codewords must be selected in order to guarantee full diversity and insure a high coding gain. Linear precoders, e.g., those based on unitary transforms, can be employed to create transmit diversity without any sacrifice in data rate but at the cost of a high decoding complexity. After a survey of the principal space-time coding techniques, this part ends with an example illustrating a full-diversity LDPC code.

- Code design criteria for fast and slow fading channels.
- The Singleton bound for block fading channels.
- Linear precoding for transmit diversity under both maximum-likelihood and iterative decoding.
- Brief survey of coding techniques, including space-time trellis coding, space-time block coding, and bit-interleaved coded modulations.
- Example of low-density parity-check codes for MIMO channels.

The literature on analysis and coding for multiple antenna channels is extremely rich. A fine selection of relevant publications in this field is given at the end of the presentation. The slides can be downloaded from the author's web page. What is not presented in this tutorial?

- Frequency selective channels and channels with correlated fadings.
- Receiver and decoder design for MIMO channels, including linear receivers and probabilistic detectors.
- Non-coherent detection, unitary space-time and differential modulations.
- MIMO channels with feedback, multiple access channels, broadcast channels, and relaying channels.

Exposés courts

A biometric identification scheme with encrypted templates

Julien Bringer, Hervé Chabanne et Bruno Kindarji
Sagem Défense Sécurité TELECOM ParisTech, Paris

Biometrics are believed to be unique, which means that someone can be identified from a sample of his biometric trait. For privacy concerns, we provide a way to perform biometric identification using encrypted data. Given a fresh measure of a biometric, our proposal looks for a similar template inside an encrypted database, in an efficient way, with sublinear communication and computation costs. Our construction makes use of Bloom Filters with Storage and Locality-Sensitive Hashing. It is the first application of the search over encrypted data to the field of biometrics.

Mots Clefs : Identification, Biometrics, Privacy, Searchable Encryption, Locality-Sensitive Hashing, Bloom Filter

Les preuves de connaissance à divulgation nulle de connaissance sont faciles à utiliser

Sebastien Canard, Iwen Coisel et Jacques Traoré
Orange Labs R&D
{sebastien.canard, iwen.coisel, jacques.traore}@orange-ft.com

Depuis leur introduction en 1985 par Goldwasser, Micali et Rackoff [3], et leur utilisation en 1988 par Feige, Fiat et Shamir [2], les preuves de connaissance à divulgation nulle de connaissance sont devenues un outil quasi incontournable dans la cryptographie moderne. De nombreuses constructions les utilisent comme briques de base pour l'élaboration de protocoles aux propriétés plus complexes nécessitant par conséquent des preuves de sécurité peu aisées. Il peut donc être intéressant d'avoir des techniques permettant de prouver plus facilement certaines parties de ces preuves complexes comme les preuves de connaissance à divulgation de connaissance. Kiayias, Tsiounis et Yung ont réalisé une première étape dans ce sens en introduisant dans [4] un théorème prouvant la sécurité des preuves de connaissance dans un contexte particulier. Ils prouvent ainsi la sécurité des preuves de connaissance à divulgation nulle de connaissance pour les ensembles de relations de logarithmes discrets *triangulaires* et impliquant plusieurs secrets, c'est-à-dire lorsqu'il est possible d'organiser les relations de la preuve de connaissance de telle sorte que la i-ème relation contienne au plus une nouvelle valeur secrète non présente dans les $i-1$ relations précédentes. Dans [1], nous apportons une extension à ce théorème. Dorénavant, la sécurité des preuves de connaissance est prouvée pour tout ensemble de relations de logarithmes discrets sans aucune restriction. Le relâchement des contraintes sur les relations permet d'augmenter conséquemment le nombre de preuve de connaissances prouvées sûres à l'aide de ce modèle.

Références

[1] S. Canard, I. Coisel, J. Traoré. Complex Zero-Knowledge Proofs of Knowledge are easy to use. *Proceedings of ProvSec'07*, volume 4784 of LNCS, pages 122-137. Springer-Verlag.

[2] U. Feige, A. Fiat, A. Shamir. Zero-knoxledge Proofs of Identity. Journal of Cryptology, 1(2), pages 77-94. 1988.

[3] S. Goldwasser, S. Micali, C.W. Rackoff. The Knowledge Complexity of Interactive Proof Systems. SIAM Journal of Computing, vol. 18(1), pages 186-208. 1989.

[4] A. Kiayias, Y. Tsiounis, M. Yung, Traceable Signatures. *Proceedings of Eurocrypt'04*, volume 3027 of LNCS, pages 571-589. Extended version at e-print cryptology archive report 2004/007, 2004. http://eprint.iacr.org/.

Bornes de la programmation linéaire pour les codes sur les matrices unitaires complexes

Jean Creignou et Hervé Diet
IMB Institut de Mathématiques de Bordeaux
UMR 5251
jean.creignou@math.u-bordeaux1.fr,
herve.diet@math.u-bordeaux1.fr

Les évolutions récentes dans le domaine des communications sans fil ont mis en évidence de nombreux problèmes de théorie des codes. En particulier les codes sur les matrices unitaires sont apparus de manière naturelle dans le cadre des communications MIMO[9]. Grâce à de nombreux auteurs, l'écart a été réduit entre les constructions explicites et les bornes théoriques sur la taille des codes lorsque la distance somme $\Sigma\mathcal{V}$ ou la distance produit $\Pi\mathcal{V}$ est fixée (voir [7], [4], [6] et [8]). La méthode de la programmation linéaire, d'abord introduite par Philippe Delsarte dans le cadre des schémas d'association[3] puis utilisée avec succès dans d'autres espaces [1, 2, 5], est un puissant outil pour améliorer ces bornes. Le but de cet exposé est de montrer comment la connaissance des représentations de $\mathbb{U}_n(\mathbb{C})$ permet, en utisant les polynômes de Schur, l'implémentation de la méthode de la programmation linéaire dans ce cadre. Nous arrivons ainsi à trouver de nouvelles bornes analytiques pour les petits degrés mais aussi à améliorer les bornes numériques pour les degrés supérieurs.

Références

[1] C. Bachoc, *Linear programming bounds for codes in Grassmannian spaces*, IEEE Trans. Inform. Theory, 52-5 (2006), pp. 2111-2125.

[2] A. Barg, P. Purkayastha, *Bounds on ordered codes and orthogonal arrays*, preprint, arxiv:cs.IT/0702033v1.

[3] P. Delsarte, V.I. Levenshtein, *Association schemes and coding theory*, IEEE Transactions on Information Theory, vol. 44, n. 6, pp. 2477-2504, October 1998.

[4] B.M. Hochwald, T.L. Marzetta, T.J. Richardson, W. Sweldens, R. Urbanke, *Systematic design of unitary space-time constellations*, IEEE Transactions on Information Theory, vol. 46, n. 6, pp. 1962-1973, September 2000.

[5] G. A. Kabatiansky, V. I. Levenshtein, *Bounds for packings on a sphere and in space*, Probl. Inform.Transm. 14, pp. 1-17, 1978.

[6] X.B. Liang, X.G. Xia, *Unitary signal constellations for differential space-time modulation with two transmit antennas : Parametric codes, optimal designs and bounds*, IEEE Transactions on Information Theory, vol. 48, n. 8, pp. 2291-2322, August 2002.

[7] G. Han, J. Rosenthal, *Unitary Space-Time Constellation Analysis : An Upper Bound for the Diversity*, IEEE Transactions on Information Theory, vol. 52, n. 10, pp. 4713-4721, October 2006.

[8] A. Shokrollahi, *Design of unitary space-time codes from representations of $SU(2)$*, Information Theory, 2001. Proceedings. 2001 IEEE International Symposium on Volume , Issue , 2001 Page(s):241

[9] L. Zheng, D.N.C. Tse, *Communication on the Grassman manifold: a geometric approach to the noncoherent multiple-antenna channel*, IEEE Transactions on Information Theory, vol. 48, n. 2, pp. 359-383, February 2002.

Codes cycliques tordus sur les anneaux de Galois

Patrick Solé
Université de Nice-Sophia Antipolis
sole@unice.fr

Delphine Boucher et Félix Ulmer
IRMAR Université de Rennes 1

Nous étudions la structure algébrique des codes cycliques tordus sur les anneaux de Galois, en particulier les idéaux bilatères dans des anneaux de polynômes tordus. Nous appliquons ces résultats aux codes constacycliques tordus autoduaux sur $GR(4^2)$. La dualité euclidienne fournit des codes autoduaux sur $\mathbb{Z}_4$; l'hermitienne des réseaux arithmétiques $3-$modulaires et des codes autoduaux sur $\mathbb{Z}_4$ quasi-cycliques. Travail en commun avec Delphine Boucher et Félix Ulmer. Exposé en commun avec Félix Ulmer.

Codes tordus dont le rang ou la distance minimale est prescrite

Lionel Chaussade et Félix Ulmer
IRMAR Université de Rennes 1

Pierre Loidreau
CELAR Rennes

Nous étudierons le lien entre les équations aux différences sur un corps fini et les polynômes tordus. Cette analogie donnera une méthode pour engendrer des θ-codes dont on pourra contrôler le corps de définition et la distance rang. Une approche différente nous permettra de générer des codes BCH tordus dont la distance minimale sera prescrite. Travail en commun avec Pierre Loidreau et Félix Ulmer.

Sur des équations clés géneralisées pour l'algorithme de Guruswami-Sudan

Daniel Augot, Alexander Zeh
INRIA SECRET team
Daniel.Augot@inria.fr, alexander.zeh@inria.fr

Il est classique de décoder les codes BCH, codes de Reed-Solomon, et codes alternants en résolvant une *équation clé*, par l'algorithme d'Euclide par exemple.
Roth et Ruckenstein ont construit une équation clé pour le décodage en liste de Sudan. Cette équation généralise bien l'équation clé, avec une montée en degré et plus d'inconnues.
Dans ce travail, nous étudions la possibilité de dériver une équation clé pour l'algorithme de Guruswami-Sudan, quand des multiplicités entrent en jeu. Nous arrivons en fait à une famille d'équations clés, une pour chaque ordre de multiplicité.
Ces équations permettent de réduire le nombre d'inconnues et d'équations. La difficulté est de conserver une matrice structurée (Hankel par blocs), qui peut se résoudre en temps quadratique. Nous montrons que c'est bien le cas.

Références

[1] M. Sudan, "Decoding of Reed Solomon Codes beyond the Error-Correction Bound," *Journal of Complexity*, vol. 13, no. 1, pp. 180–193, March 1997.

[2] R. M. Roth and G. Ruckenstein, "Efficient decoding of Reed-Solomon codes beyond half the minimum distance," *IEEE Transactions on Information Theory*, vol. 46, no. 1, pp. 246–257, 2000.

[3] G.-L. Feng and K. K. Tzeng, "A generalization of the Berlekamp-Massey algorithm for multisequence shift-register synthesis with applications to decoding cyclic codes," *IEEE Transactions on Information Theory*, vol. 37, no. 5, pp. 1274–1287, 1991.

[4] G. Ruckenstein, "Error decoding strategies for algebraic codes," Ph.D. dissertation, Technion, 2001.

[5] V. Guruswami and M. Sudan, "Improved decoding of Reed-Solomon and algebraic-geometry codes," *IEEE Transactions on Information Theory*, vol. 45, no. 6, pp. 1757–1767, 1999.

[6] G.-L. Feng and K. K. Tzeng, "A new procedure for decoding cyclic and bch codes up to actual minimum distance," *IEEE Transactions on Information Theory*, vol. 40, no. 5, pp. 1364–1374, 1994.

[7] S. Sakata, "n-dimensional Berlekamp-Massey algorithm for multiple arrays and construction of multivariate polynomials with preassigned zeros," in *Applied algebra, algebraic algorithms and error-correcting codes (Rome, 1988)*, ser. Lecture Notes in Computer Science, T. Mora, Ed., vol. 357. Berlin: Springer, 1989, pp. 356–376.

[8] G. Schmidt and V. R. Sidorenko, "Linear Shift-Register Synthesis for Multiple Sequences of Varying Length," May 2006.

[9] G. Schmidt, V. Sidorenko, and M. Bossert, "Decoding Reed-Solomon Codes Beyond Half the Minimum Distance using Shift-Register Synthesis," in *Information Theory, 2006 IEEE International Symposium on*, 2006, pp. 459–463.

Cryptanalysis of a McEliece cryptosystem based on quasi-cyclic LDPC codes

Ayoub Otmani, Léonard Dallot
GREYC - Ensicaen - Université de Caen,
Ayoub.Otmani@info.unicaen.fr
Leonard.Dallot@info.unicaen.fr

Jean-Pierre Tillich
INRIA, Projet Codes,
jean-pierre.tillich@inria.fr

Since the introduction of the McEliece public-key cryptosystem [11], several attempts have been made to propose alternatives to the classical Goppa codes. The main motivation behind all those works is to drastically reduce the amount of bits of the keys, which is a real concern for any concrete deployment. For instance, the parameters suggested in the original cryptosystem, and now outdated, are about 500 Kbits for the public key and 300 Kbits for the private key. The reason of such a quantity of bits comes from the fact that McEliece proposed to use as the public key a generator matrix of a linear block code. He suggested to take a code that admits an efficient decoding algorithm capable to correct up to a certain number of errors, and then mask the structure of the code by applying on the chosen generator matrix two secret linear transformations: a scrambling transformation that sends the chosen generator matrix to another one, and a permutation matrix that reorders the coordinates. The public key is then a random choice among these masked matrices. The private key consists in the two secret transformations and the decoding algorithm. Niederreiter also invented [13] a code-based asymmetric cryptosystem by choosing to describe codes through a parity check matrix. These two systems offer equivalent security guaranties [10]. They both build their security on two criteria: the One-Wayness against Chosen-Plaintext Attack (OW-CPA) thanks to the difficulty of decoding large random linear block codes, and the difficulty of guessing the decoding algorithm from a masked generator matrix. It is worthwhile mentioning that the OW-CPA character is well established as long as appropriate parameters are taken. This is due to two facts: first it is proven in [2] that decoding a random linear code is NP-Hard, and second the best algorithm [5] up to now operates exponentially with the length n of the underlying code. However, the second criteria is not always verified by any class of codes that has a decoding algorithm. For instance, Sidel'nikov and Shestakov proved in [15] that the structure of Generalised Reed-Solomon codes of length n can be recovered in $O\left(n^4\right)$. Sendrier proved that the permutation transformation can be extracted for concatenated codes. Minder and Shokrollahi presented in [12] a structural attack that creates a private key against a cryptosystem based on Reed-Muller codes [14]. All these results lead us to claim that McEliece's original cryptosystem is the most secure solution if one considers code-based cryptography. Additionally, McEliece's system and its Niederreiter homologue have comparable performances that are better than any other competing asymmetric schemes like RSA. Unfortunately they suffer from the same drawback namely, they need very large key sizes as previously remarked. It is therefore crucial to find a method to reduce the representation of a linear code as well as the matrices of the linear transformations.

A possible solution is to take very sparse matrices. This idea has been applied in [4] which examined the implications of using Low Density Parity Check (LDPC) codes. The authors showed that taking sparse matrices for the linear transformations is not a secure solution. Indeed, it is possible to recover the secret code from the public parity check matrix. Another recent trend appeared in code-based public key cryptosystems that tries to use quasi-cyclic codes [7, 1, 9, 8, 6]. This particular family of codes offers the advantage of having a very simple and an efficient way of describing them. One is able to obtain many codewords simply by considering cyclic shifts of a sole codeword. Exploiting this fact leads to much smaller matrices describing the codes. Currently there exist two public-key cryptosystems that are based upon quasi-cyclic codes. The first proposal [7] uses subcodes of a primitive BCH cyclic code. The size of the public key is for this cryptosystem is 20Kbits.

The other one [1] tries to combine these two positive aspects by requiring quasi-cyclic LDPC codes. It also uses linear transformations defined by random sparse circulant matrices. For this particular system, the authors propose a public key size that is about 48Kbits.
In this work, we propose to cryptanalysis this second cryptosystem. We show a structural attack by exploiting some weakness in the particular choice of the linear transformations. This cryptanalysis adopts a polynomial-oriented approach. The attack consists in searching for two polynomials of low weight such that their product is a public polynomial. Our analysis shows that a parity check matrix of the secret code can be recovered with time complexity of $O\left(n^3\right)$ where n is the length of the considered code. For the specific parameters proposed in [1], the structural cryptanalysis implemented in MAGMA software finds the secret key in about 110 seconds on a PC.

Références

[1] M. Baldi and G. F. Chiaraluce. Cryptanalysis of a new instance of McEliece cryptosystem based on QC-LDPC codes. In *IEEE International Symposium on Information Theory*, pages 2591–2595, Nice, France, March 2007.

[2] E. R. Berlekamp, R. J. McEliece, and H. C. A. van Tilborg. On the intractability of certain coding problems. *IEEE Transactions on Information Theory*, 24(3):384–386, 1978.

[3] W. Bosma, J. J. Cannon, and Catherine Playoust. The Magma algebra system I: The user language. *J. Symb. Comput.*, 24(3/4):235–265, 1997.

[4] A. Shokrollahi C. Monico, J. Rosenthal. Using low density parity check codes in the McEliece cryptosystem. In *IEEE International Symposium on Information Theory (ISIT 2000)*, page 215, Sorrento, Italy, 2000.

[5] A. Canteaut and F. Chabaud. A new algorithm for finding minimum-weight words in a linear code: Application to McEliece's cryptosystem and to narrow-sense BCH codes of length 511. *IEEE Transactions on Information Theory*, 44(1):367–378, 1998.

[6] P.L. Cayrel, A. Otmani, and D. Vergnaud. On Kabatianskii-Krouk-Smeets Signatures. In *Proceedings of the first International Workshop on the Arithmetic of Finite Fields (WAIFI 2007)*, Springer Verlag Lecture Notes, pages 237–251, Madrid, Spain, June 21–22 2007.

[7] P. Gaborit. Shorter keys for code based cryptography. In *Proceedings of the 2005 International Workshop on Coding and Cryptography (WCC 2005)*, pages 81–91, Bergen, Norway, March 2005.

[8] P. Gaborit and M. Girault. Lightweight code-based authentication and signature. In *IEEE International Symposium on Information Theory (ISIT 2007)*, pages 191–195, Nice, France, March 2007.

[9] P. Gaborit, C. Lauradoux, and N. Sendrier. Synd: a fast code-based stream cipher with a security reduction. In *IEEE International Symposium on Information Theory (ISIT 2007)*, pages 186–190, Nice, France, March 2007.

[10] Y. X. Li, R. H. Deng, and X.-M. Wang. On the equivalence of McEliece's and Niederreiter's public-key cryptosystems. *IEEE Transactions on Information Theory*, 40(1):271–273, 1994.

[11] R. J. McEliece. *A Public-Key System Based on Algebraic Coding Theory*, pages 114–116. Jet Propulsion Lab, 1978. DSN Progress Report 44.

[12] L. Minder and A. Shokrollahi. Cryptanalysis of the Sidelnikov cryptosystem. In *Eurocrypt 2007*, volume 4515 of *Lecture Notes in Computer Science*, pages 347–360, Barcelona, Spain, 2007.

[13] H. Niederreiter. Knapsack-type cryptosystems and algebraic coding theory. *Problems Control Inform. Theory*, 15(2):159–166, 1986.

[14] V.M. Sidelnikov. A public-key cryptosystem based on binary Reed-Muller codes. *Discrete Mathematics and Applications*, 4(3), 1994.

[15] V.M. Sidelnikov and S.O. Shestakov. On the insecurity of cryptosystems based on generalized Reed-Solomon codes. *Discrete Mathematics and Applications*, 1(4):439–444, 1992.

Pistes pour l'analyse probabiliste de la réduction des réseaux

Brigitte Vallée et Antonio Vera
GREYC, Université de Caen

L'algorithme de réduction des réseaux dû à Gauss, construit, à partir d'une base d'un réseau de dimension 2, et en temps polynomial, une base "minimale" du réseau. Cet algorithme est central, car il est à la base du célèbre algorithme LLL de réduction de réseaux, qui résout le même genre de problème pour une dimension quelconque: l'algorithme LLL construit, à partir d'une base d'un réseau de dimension n quelconque, et en temps polynomial, une base du réseau, formée de vecteurs assez courts et assez orthogonaux. L'algorithme LLL est très utilisé, mais son comportement probabiliste est très mal compris.
Le projet ANR LAREDA cherche à élucider ce comportement probabiliste de l'algorithme LLL. Il faut commencer par la dimension 2, et cet exposé décrira des premiers résultats qui décrivent à la fois l'exécution de l'algorithme et sa configuration de sortie. Nous expliquerons aussi comment ces résultats constituent une première étape pour décrire le comportement de l'algorithme LLL.

Attaque de tatouage d'image fondée sur une estimation bayésienne non-linéaire non-paramétrique dans le domaine des ondelettes

Larbi Boubchir,Nadia Zerida, et Ayoub Otmani
GREYC UMR 6072 CNRS
ENSICAEN-Université de Caen
larbi.boubchir@greyc.ensicaen.fr ,
nadia.zerida@info.unicaen.fr ,
ayoub.otmani@info.unicaen.fr .

Le laboratoire WAVILA (*Watermarking Virtual Laboratory*) du réseau d'excellence européen ECRYPT a mis en place du 17 octobre 2007 au 17 janvier 2008 le deuxième épisode du challenge BOWS-2 (Break Our Watermarking System 2nd Ed.) [1]. BOWS-2 est aussi soutenu par le projet ANR Nebbiano. Le but est d'évaluer la robustesse et l'efficacité d'un nouvel algorithme de tatouage d'images proposé par Teddy Furon et Patrick Bas [2]. L'idée est de proposer une technique d'attaque de tatouage d'images permettant d'enlever la marque de trois images tout en ayant un PSNR supérieur à 20dB entre l'image marquée et celle attaquée.

Nous proposons une approche d'attaque de type débruitage basée sur un estimateur bayésien non-linéaire non-paramétrique formulé dans le cadre des transformées multi-échelles parcimonieuses notamment les ondelettes. Dans cette approche, nous proposons un modèle statistique *a priori* adapté à la modélisation des coefficients d'ondelettes d'une image marquée en absence et en présence du bruit. Il s'agit du modèle Formes K de Bessel (FKB) [3].

La réalisation de notre approche est effectuée en deux étapes : Premièrement, nous ajoutons un bruit additif blanc gaussien à l'image marquée et nous appliquons l'estimateur bayésien FKB de type *maximum a posteriori* (MAP) [4] ce qui nous conduit à obtenir une image attaquée non marquée avec un PSNR supérieur à 20dB. Deuxièmement, nous proposons un algorithme permettant d'améliorer la qualité visuelle de l'image attaquée afin de maximiser le PSNR. L'idée est d'exploiter l'information contenue dans l'image de différence entre l'image marquée et celle attaquée. Des résultats seront présentés permettant d'évaluer notre approche d'attaque.

Références

[1] http://bows2.gipsa-lab.inpg.fr/

[2] T. Furon and P. Bas, *Broken Arrows*, 2008 (paper under submission).

[3] J. Fadili and L. Boubchir, *Analytical Form for a Bayesian Wavelet Estimator of Images Using the Bessel K Forms Densities*, IEEE Transactions on Image Processing, Vol. 12, No 2, pp 231-240, 2005.

[4] L. Boubchir and J. Fadili, *Bayesian Denoising Based on the MAP Estimator in Wavelet-domain Using Bessel K Form Prior*, In Proc. of IEEE ICIP'2005; the IEEE International Conference on Image Processing, Vol. 1, pp 113-116, 2005.

Codage et cryptanalyse linéaire

Benoit Gérard
Equipe SECRET
INRIA Rocquencourt

La cryptanalyse linéaire est une attaque à clair connu qui consiste à tirer profit de l'existence d'équations linéaires probabilistes faisant intervenir des bits de clair et de chiffré ainsi que des bits de la clé ayant servi au chiffrement.
Cette idée, suggérée par Henri Gilbert, est utilisée par Matsui pour la cryptanalyse du DES [Mat93]. Dans [Mat93], Matsui présente deux types d'attaques : une attaque directe utilisant une équation sur le DES à 8 tours et une attaque dite 'par distingueur' utilisant une équation sur le DES à 7 tours. La principale amélioration apportée depuis est l'utilisation de plusieurs équations.
Les algorithmes proposés pour la cryptanalyse à plusieurs équations imposent un nombre important de restrictions sur celles-ci à l'exception de celui de *Biryukov et al.* [BCQ04]. Les équations obtenues ne faisant pas intervenir tous les bits de clé, il est proposé de calculer la vraisemblance de chaque sous-clé puis de trier la liste et effectuer une recherche exhaustive sur les bits restants dans cet ordre. Le travail présenté apporte deux améliorations, la première diminue la complexité de cet algorithme et la seconde porte sur l'estimation du nombre de couples clair/chiffré nécessaires à l'attaque.
L'idée principale est de considérer la recherche de la sous-clé la plus vraisemblable comme un problème de décodage sur le canal gaussien.
On va donc utiliser des techniques de décodage afin de ne regarder qu'une faible proportion des sous-clés tout en gardant une forte probabilité de trouver la bonne de façon à diminuer sensiblement la complexité de l'algorithme [BCQ04].
Pour ce qui est de l'étude du nombre de couples nécessaires, de même, on va faire appel aux méthodes de théorie des codes correcteurs et s'intéresser à l'entropie de la variable aléatoire correspondant à la bonne sous-clé connaissant les couples clair/chiffré. L'étude de cette grandeur permet d'être moins pessimiste que dans [BCQ04] où l'étude est faite sur le rang moyen de la bonne sous-clé après le tri par vraisemblance.
On présentera les résultats obtenus sur un exemple jouet : le DES restreint à 8 tours.

Références

[BCQ04] Alex Biryukov, Christophe De Cannière, and Michaël Quisquater. On Multiple Linear Approximations. In *CRYPTO 2004*, LNCS, pages 1–22. Springer–Verlag, 2004.

[Mat93] Mitsuru Matsui. Linear cryptanalysis method for DES cipher. In *EUROCRYPT '93*, LNCS, pages 386–397. Springer–Verlag, 1993.

Codes LDPC non-binaires hybrides

Lucile Sassatelli et David Declercq
ETIS - ENSEA/UCP/CNRS UMR-8051 - 95014 Cergy, FRANCE
{sassatelli,declercq}@ensea.fr

Les codes LDPC sont des codes pseudo-aléatoires approchant la capacité du canal. L'intérêt des codes LDPC non-binaires, par rapport aux binaires, apparait pour des trames courtes ou des modulations d'ordre élevé [1, 2]. Cependant, les codes LDPC binaires et non-binaires ont des qualités différentes. Nous avons introduit une nouvelle famille de codes LDPC, les codes LDPC hybrides, dont l'intérêt repose sur la combinaison des avantages des familles de codes LDPC binaires et non-binaires. Ce compromis est réalisé par le mélange de symboles de différents ordres au sein d'un même mot de code. On présentera les résultats obtenus jusqu'ici, concernant à la fois l'étude asymptotique et à taille finie. On introduira les propriétés de symétrie et d'invariance par applications linéaires qui permettent de prouver le comportement à seuil de ces codes, ainsi que l'analyse de type EXIT chart pour concevoir de bons codes LDPC hybrides. Des simulations à tailles finies montrent l'intérêt de cette nouvelle famille très générale de codes LDPC, notamment pour les application bas rendements où ils concurrencent les codes existants comme les Turbo Hadamard.

Condition de Stabilité

Introduite dans [3], la condition de stabilité est une condition nécessaire et suffisante pour que la probabilité d'erreur ne soit pas bornée par une constante strictement positive lorsque le nombre d'itérations tend vers l'infini, sachant qu'elle a déjà décru sous une certaine valeur à une itération donnée. On montre le théorème suivant :

Théorème : La probabilité d'erreur des codes de la famille définie par $\pi(i,j,k,l)$, converge vers zero si et seulement si $\Omega\Delta < 1$ avec $\Omega = \sum_{j,k,l} \pi(i=2,k,j,l)\frac{q_k-1}{q_l-1}(j-1)$, $\Delta = \sum_{k,l} \pi(k,l)\frac{1}{q_l-1}\sum_{i=1}^{q_k-1}\int\sqrt{p(y|\delta(i))p(y|\delta(0))}dy$ où $p(y|\delta(i))$ correspond aux probabilités de transition du canal. On montre ainsi qu'un code hybride peut être stable quand le code non-binaire non-hybride construit sur le corps d'ordre maximum ne l'est pas.

Optimisations asymptotique et à taille finie

Nous avons dérivé les équations d'évolution de l'information mutuelle des codes LDPC hybrides pour le canal BI-AWGN, ce qui, par optimisation sous contrainte, nous a permis de concevoir des codes intéressants.Pour de faibles rendements, on applique en plus une technique d'optimisation à taille finie [4]. Les codes LDPC hybrides sont d'excellents concurrents aux meilleurs codes existants pour ces rendements [5].

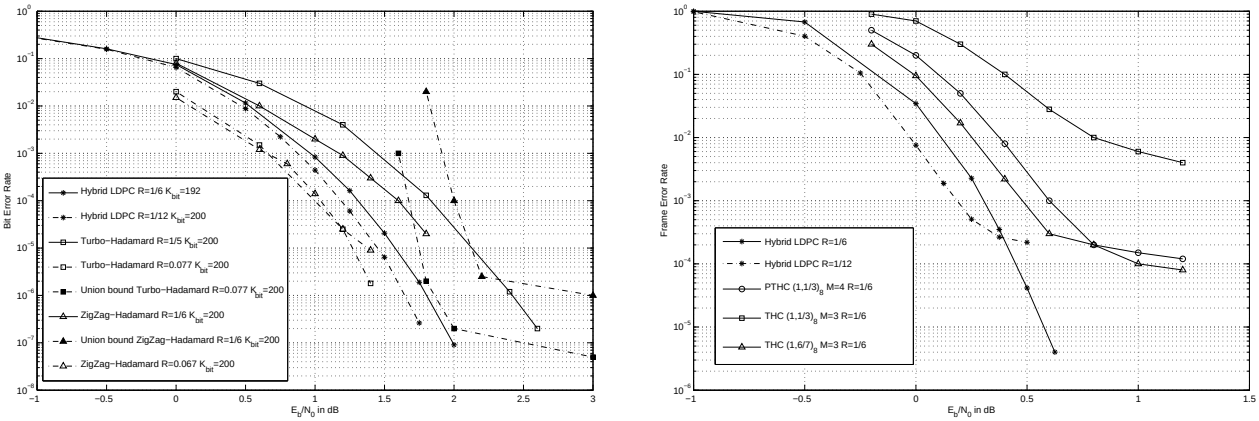


Figure de gauche : nombre de bits d'information $K_{bit} = 200$ Figure de droite : $K_{bit} = 1000$

Références

[1] X.-Y. Hu and E. Eleftheriou, *Binary Representation of Cycle Tanner-Graph GF(2^q) Codes*, Proceedings of IEEE International Conference on Communications, pp. 528-532, Paris, France, June, 2004

[2] A. Bennatan and D. Burshtein, *Design and Analysis of Nonbinary LDPC Codes for Arbitrary Discrete-Memoryless Channels*, IEEE Transactions on Information Theory, vol.52, n.2, pp.549-583, February, 2006

[3] T.J. Richardson and A. Shokrollahi and R. Urbanke, *Design of Capacity-Approaching Irregular LDPC Codes*, IEEE Transactions on Information Theory, vol.47, n.2, pp.619-637, February, 2001

[4] C. Poulliat and M. Fossorier and D. Declercq, *Design of regular (2,dc)-LDPC codes over GF(q) using their binary images*, accepted in IEEE Transactions on Communications, 2007

[5] L. Ping and W.K. Leung and K.Y. Wu, *Low-rate turbo-Hadamard codes*, IEEE Transactions on Information Theory, vol.49, n.12, pp.3213-3224, December, 2003

Algebraic cryptanalysis of curry and flurry using correlated messages

J.-C. Faugère et L. Perret
LIP6 Université Paris 6

In [1], Buchmann, Pyshkin and Weinmann have described two families of Feistel and SPN block ciphers called Flurry and Curry respectively. These two families of ciphers are fully parametrizable and have a sound design strategy against classical statistical attacks (i.e. linear and differential attacks). In addition, the encryption process can be easily described by a set of algebraic equations. These ciphers are then targets of choices for algebraic attacks. In particular, the authors of [1] have reduced the key-recovery problem to the problem of changing the order of a Gröbner basis. We have investigated the possibility of using a small number of suitably chosen pairs of message/ciphertext for improving algebraic attacks. It turns out that this approach permits to go one step further in the (algebraic) cryptanalysis of Flurry and Curry. From our experiments, we estimate that this last approach is of polynomial-time complexity when the S-box is a power function. For instance, we have been able to break a 128-bit Flurry – with 7 rounds – in less that one hour using an efficicient Gröbner bases algorithm; namely F_5 [2].

Références

[1] J. Buchmann, A. Pyshkin, and R-P Weinmann *Block Ciphers Sensitive to Gröbner Basis Attacks.* Topics in Cryptology - CT RSA'06, Lecture Notes in Computer Science, vol. 3860, Springer–Verlag, pp. 313–331, 2006.

[2] J.-C. Faugère. *A New Efficient Algorithm for Computing Gröbner Basis without Reduction to Zero:* F_5. Proceedings of ISSAC, pp. 75–83. ACM press, July 2002.

On the MinRank problem

J.-C. Faugère et L. Perret
LIP6 Université Paris 6

F. Levy-dit-Vehel
Ecole Nationale Supérieure
de Techniques Avancées Paris 15

In this talk, we shall present the MinRank [1] problem and its known complexity. Then we will give a slightly different statement of it, that permits to link it with other problems from coding theory, namely Maximum Likelihood Decoding problem and Rank Decoding problem. The MinRank problem is also used for designing an efficient authentication scheme [1].

In a second part, we shall show two ways to solve Minrank : one that uses the kernel of an appropriate linear mapping, that works in $O(q^{\lceil m/n \rceil} r m^\omega)$, and the other by means of reducing the problem to the MQ (Multivariate Quadratic) problem [1]. We will focus our attention to this last attack and present a fresh view of this well-known approach. This a work in progress, but we already obtained encouraging experimental results using Gröbner bases techniques.

Références

[1] N. Courtois. *Efficient Zero-knowledge Authentication Based on a Linear Algebra Problem MinRank.* Advances in Cryptology – ASIACRYPT 2000, Lecture Notes in Computer Science, vol. , Springer–Verlag, pp. –, 2000.

McEliece cryptosystem; security and implementation

Bhaskar Biswas et Nicolas Sendrier
INRIA Rocquencourt
{first name}.{last name}@inria.fr

Though it is old and considered fast, the implementation of McEliece public-key encryption scheme has never been thoroughly studied. We consider that problem here and we provide a careful implementation together with the state of the art in cryptanalysis. This provides a reference for measuring speed and scalability of this cryptosystem. Compared with other, number-theory based, public key scheme, we demonstrate a gain of a factor at least 5 to 10.
McEliece encryption scheme was proposed in 1978 [3]. During the thirty years that have elapsed since, its security, as a one way trapdoor encryption scheme has never been seriously threatened.
Most of the previous works have been devoted to cryptanalysis and to semantic security [1, 2] but very few have examined implementation issues. The goal of our work is to examine that last point in details.
Implementing a (public key) cryptosystem is a tradeoff between security and efficiency. Though the public key size is rather large, the McEliece encryption scheme possesses some strong features. It has a good security reduction and low complexity algorithms for encryption and decryption. As a consequence, it is concievable, compared with number-theory based cryptosystems, to gain an order of magnitude in performance.
Here we consider a slightly modified version of the scheme (which we call *hybrid*). It has two modifications, the first increases the information rate by putting some data in the error pattern. The second reduces the public key size by making use of a generator matrix in row echelon form. It can be shown that the same security reduction as for the original system holds in our scheme.
We have fully implemented the cryptosystem and we will prove that this modified system has the same security while it is faster than the original. We will show this system has information rate close to 1 and the keysize is reduced. We will also provide extensive simulation results, from which the trade off between the system parameters and security can be observed and can be compared with other existing systems as well.

Références

[1] A. Canteaut and F. Chabaud. A new algorithm for finding minimum-weight words in a linear code: Application to McEliece's cryptosystem and to narrow-sense BCH codes of length 511. *IEEE Transactions on Information Theory*, 44(1):367–378, January 1998.

[2] K. Kobara and H. Imai. Semantically secure McEliece public-key cryptosystems -Conversions for McEliece PKC-. In K. Kim, editor, *PKC'2001*, number 1992 in LNCS, pages 19–35. Springer-Verlag, 2001.

[3] R. J. McEliece. A public-key cryptosystem based on algebraic coding theory. *DSN Prog. Rep.,* Jet Prop. Lab., California Inst. Technol., Pasadena, CA, pages 114–116, January 1978.

Polynômes de permutation à trappe et chiffrement à clef publique

Guilhem Castagnos
GREYC, Ensicaen,
guilhem.castagnos@info.unicaen.fr

Damien Vergnaud
Département d'informatique, ENS,
damien.vergnaud@ens.fr

Soit n le produit de deux grands nombres premiers, et e un entier premier avec $\varphi(n)$. Il est bien connu que le polynôme X^e de $\mathbf{Z}/n\mathbf{Z}[X]$ induit une permutation de $(\mathbf{Z}/n\mathbf{Z})^\times$. Le schéma de chiffrement RSA peut être vu comme l'évaluation de ce polynôme. De plus, ce polynôme a une trappe : connaissant d tel que $ed \equiv 1 \pmod{\varphi(n)}$, on peut inverser l'évaluation de ce polynôme en n'importe quel point de $(\mathbf{Z}/n\mathbf{Z})^\times$. Pour finir, ce polynôme est évaluable rapidement, grâce aux algorithmes d'exponentiation modulaire.
D'autres polynômes de $\mathbf{Z}/n\mathbf{Z}[X]$ satisfont ces propriétés. Ces polynômes proviennent de l'adaptation de RSA dans d'autres groupes, comme le groupe des points d'une courbe elliptique avec le système proposé par Demytko en 1993 (cf. [Dem93]), ou le groupe des entiers quadratiques de norme 1, avec le système LUC, proposé par Smith et Lennon la même année (cf. [SL93]). Ce dernier système est très proche de ceux décrits par Müller et Nöbauer dans [MN81, MN86]) en utilisant les polynômes de Dickson et de celui proposé par Rubin et Silverberg (cf. [RS03]) en utilisant la paramétrisation du tore algébrique T_2, qui lui même coïncide avec les schémas utilisant les fonctions de Rédei (cf. [Var88, LM84]).
Tous ces polynômes permettent de construire des systèmes de chiffrement à sens unique dans le cadre d'attaques à messages clairs choisis, sous réserve que leur inversion ponctuelle soit difficile. Dans cet exposé, en combinant plusieurs polynômes de permutations, nous présenterons de nouveaux problèmes algorithmiques, tous qissus du problème général suivant : soient P et Q deux polynômes de $\mathbf{Z}/n\mathbf{Z}[X]$, permutations de $(\mathbf{Z}/n\mathbf{Z})^\times$, soit R un polynôme de $\mathbf{Z}/n\mathbf{Z}[X, Y]$, étant donné $P(a)$ et $Q(b)$, calculer $R(a, b)$.
Nous présenterons les propriétés de ces problèmes et leur complexité algorithmique. Nous utiliserons ensuite ces problèmes pour construire des protocoles de chiffrement à clé publique sémantiquement sûrs sous l'hypothèse de l'insolubilité de leurs variantes décisionnelles. Nous proposerons plusieurs protocoles sûrs sous une attaque à chiffrés choisis adaptative dans le modèle de l'oracle aléatoire. Enfin, la technique proposée nous permettra de construire le protocole prouvé sûr sous une attaque à chiffrés choisis non-adaptative (dans le modèle standard de sécurité) le plus efficace connu.

Références

[Dem93] N. Demytko : A New Elliptic Curve Based Analogue of RSA. *In Proc. of Eurocrypt' 93*, p. 40-49, 1994.

[LM84] R. Lidl et W. B. Muller : Permutation Polynomials in RSA Cryptosystems. *In Proc. of Crypto' 83*, p. 293-301, 1984.

[MN81] W. B. Müller et R. Nöbauer : Some remarks on public-key cryptosystems. *Sci. Math. Hungar.*, vol. 16, p. 71-76, 1981.

[MN86] W. B. Müller and R. Nöbauer : Cryptanalysis of the Dickson-scheme. *In Proc. of Eurocrypt' 85*, p. 50-51, 1986.

[RS03] K. Rubin et A. Silverberg : Torus-Based Cryptography. *In Proc. of Crypto' 03*, p. 349-365, 2003.

[SL93] P. Smith et M. J .J Lennon : LUC: A new public key system. *In Proc. of the Ninth IFIP Int. Symp. on Computer Security (1993)*, p. 103-117, 1993.

[Var88] V. Varadharajan : Permutation Polynomials based Cryptosystems. *International Journal of Computer Mathematics*, vol. 23, p. 237-250, 1988.

Preuve de sécurité concrète du schéma de signature de Courtois, Finiasz et Sendrier

Léonard Dallot
GREYC, UMR 6072, Caen, France
leonard.dallot@info.unicaen.fr

La cryptographie fondée sur la théorie des codes a été introduite par R. J. McEliece en 1978 [McE78], deux ans après l'introduction de la cryptographie a clef publique en 1976. En 1986, H. Niederreiter a proposé un cryptosystème équivalent [Nie86], mais ce n'est qu'en 2001 que N. Courtois, M. Finiasz et N. Sendrier ont proposé le premier schéma de signature utilisable en pratique fondé sur la théorie des codes [CFS01]. Même si des arguments concrets de sécurité sont donnés, aucune preuve de sécurité formelle n'est fournie.
L'exposé montrera que, sous réserve d'une légére modification du schéma de signature, sa sécurité contre une forge existentielle lors d'une attaque à messages choisis dans le modèle de l'oracle aléatoire peut être reliée à la difficulté de deux problèmes de la théorie des codes : l'indistingabilité des codes de Goppa permutés [SenRHDR] d'une part et le problème du décodage borné paramétré pour les codes de Goppa [FinPhD] d'autre part.

Références

[Nie86] Niederreiter, H., *Knapsack-type Cryptosystems and Algebraic Coding Theory*, Problems of Control and Information Theory, vol.15, n.2, pp. 159–166, 1986.

[CFS01] Courtois, N., Finiasz, M. and Sendrier, N., *How to achieve a* McE*liece-based Digital Signature Scheme* Asiacrypt 2001 vol. 2248, pp. 157–174", Springer 2001.

[FinPhD] Finiasz, M., *Nouvelles constructions utilisant des codes correcteurs d'erreurs en cryptographie à clef publique"*, PhD Thesis, INRIA – Ecole Polytechnique, oct 2004, http://www-rocq.inria.fr/codes/Matthieu.Finiasz/research/2004/finiasz-these.pdf

[McE78] McEliece, R. J. *A Public-Key Cryptosystem Based on Algebraic Coding Theory*, DSN Progress report # 42-44", Jet Propulsion Laboratory, Pasadena, Californila 1978.

[SenRHDR] Sendrier, N., *Cryptosystèmes à clé publique basés sur les codes correcteurs d'erreurs*, Habilitation à diriger les recherches, Université Pierre et Marie Curie, Paris 6, Paris, France.

Attaque DPA contre l'algorithme de Miller

Nadia El Mrabet
Université Montpellier II
LIRMM , UMR CNRS 5506

Le couplage est une notion mathématique qui fait son apparition en cryptographie dans les années 90. Il s'agit d'une application bilinéaire qui à deux points d'une courbe elliptique associe un élément d'un corps fini. Les couplages ont permis de simplifier des protocoles existant comme les schémas de signature courte, et la création de protocole originaux, par exemple la cryptographie basée sur l'identité de Boneh-Franklin.

Au départ, lors de l'utilisation des couplages, aucun secret n'était directement impliqué, par conséquent les attaques à canaux cachés ne représentaient pas une menace pour un schéma cryptographique utilisant les couplages. Avec l'apparition de la cryptographie basée sur l'identité, une des deux entrée lors de l'exécution de l'algorithme du couplage est secrète. Le but de la présentation est de mettre en place une attaque DPA afin de retrouver l'entrée secrète lors de l'exécution d'un algorithme de couplage fondé sur l'algorithme de Miller.

Les deux premiers couplages à avoir été utilisés sont les couplages de Tate et Weil. L'algorithme de Miller est l'étape centrale du calcul de ces deux couplages.
Le principe de l'attaque DPA est d'analyser les courbes de consommation électrique lors de l'exécution d'un algorithme afin d'en déduire des propriétés du secret utilisé. Une attaque DPA dans le cas particulier de l'algorithme de Duursma et Lee a été présentée par Page et Vercauteren, nous proposons de généraliser cette attaque à l'algorithme de Miller, aussi bien en coordonnées affines qu'en coordonnées jacobiennes et projectives.

Faster computation of pairings in Edwards coordinates

Sorina Ionica et Antoine Joux
Laboratoire PRiSM
Université de Versailles

Recently Edwards introduced a new normal form for elliptic curves, showing that the addition law on an elliptic curve actually has a surprisingly simple and symmetric form. In this presentation, we make use of a slightly generalized result of Lange and Bernstein (**1**) who showed that all elliptic curve defined over a field k of characteristic different from 2 is birationally equivalent over some extension of k to an Edwards curve, i.e. a curve of the form $x^2 + y^2 = 1 + dx^2y^2$ with $d \notin \{0, 1\}$. They showed that the Edwards addition law corresponds to the standard addition law on the birationally equivalent elliptic curve and gave explicit adding and doubling formulas faster than those of any other known forms for eliptic curves.
The algorithm used in pairing computation was given by Miller and resembles to the double-and-add method for finding a point multiple. It is then natural to wonder whether it would be possible to express pairing computation in Edwards coordinates. Up to now, it was usually most efficient to use Jacobian coordinates for pairing computation, as it is explained by Koblitz and Menezes in [2]. They count the number of field multiplications and squarings that appear in the doubling part of the Miller algorithm. The difficulty when trying to express the Miller algorithm in Edwards coordinates is that it is hard to find the equations of the two rational functions that appear when adding two points on the Edwards curve. Our idea is to describe a morphism of degree 4 from the Edwards curve to a curve of the form $S^2P = (1 + dP)^2 - 4P$. This curve has an equation of total degree 3 and just like for the Weierstrass form, we can easily compute the equations of the two lines that appear when doubling a point T, i.e. the line l tangent to the curve at point T and the vertical line v that passes through $2T$. We then take the pullback of l and v on the Edwards curve.
The output of our algorithm is the pairing, up to a 4-th power. Just like in [2], we first examine the case of the embedding degree $k = 1$ and then the case $k \geq 2$. In both cases we show that pairing computation in Edwards coordinates is faster than in Jacobian coordinates.

Références

[1] Daniel J. Bernstein, Tanja Lange, Faster addition and doubling on elliptic curves, Asiacrypt 2007

[2] Neal Koblitz and Alfred Menezes, Pairing-Based Cryptography at High Security Levels,IMA Int. Conf, 2005, pages 13-36

Réconciliation de variables gaussiennes corrélées dans le cadre de protocole de cryptographie quantique

Anthony Leverrier, Romain Alléaume,
TELECOM ParisTech

Joseph Boutros
Texas A&M University at Qatar

Philippe Grangier
Laboratoire Charles Fabry
Institut d'Optique, Palaiseau, France

Gilles Zémor
Université de Bordeaux I

Les protocoles de cryptographie quantiques sont composés de trois étapes principales. Les parties légitimes, Alice et Bob, commencent par s'échanger des états quantiques qui, une fois mesurés, leur permettent d'obtenir des variables aléatoires corrélées X et Y. Un éventuel espion a accès à une variable aléatoire Z également corrélée à X. Ensuite, lors de la phase dite *de réconciliation*, Alice envoie de l'information supplémentaire à Bob sur un canal public authentifié. Connaissant Y, Bob est alors capable de retrouver la valeur de X. Enfin, lors de l'*amplification de confidentialité*, Alice choisit aléatoirement une fonction de compression g et l'annonce à Bob. Le secret partagé est alors $g(X)$. La taille du secret peut en principe être arbitrairement proche de $I(X;Y) - I(X;Z)$ [1].
La plupart des protocoles utilisent des états quantiques discrets : X et Y sont alors des chaînes de bits corrélées et la réconciliation consiste simplement pour Alice à envoyer à Bob le syndrome de X pour un code linéaire C [2]. Une alternative à ces protocoles propose d'encoder l'information sur des états continus [3], auquel cas X et Y deviennent des vecteurs gaussiens corrélés. Dans ce cas, le choix de code C utilisé pour réaliser la réconciliation est plus délicat et doit satisfaire différentes exigences. D'abord, le code doit approcher la capacité du canal entre Alice et Bob et doit révéler le moins d'information possible sur X à l'espion. Ceci peut en théorie être réalisé en choisissant un code sphérique aléatoire. Cependant, on souhaite également que le choix du code, sa description et son décodage soient réalisables efficacement. Nous étudions ici un codage multidimensionnel qui répond à ces critères en exploitant la structure algébrique des octonions en dimension 8.

Références

[1] J. Csiszar, I.; Korner. Broadcast channels with confidential messages. *Information Theory, IEEE Transactions on*, 24(3):339–348, May 1978.

[2] A. D. Wyner. The wire-tap channel. *Bell System Technical Journal*, 54:1355–1387, 1975.

[3] F. Grosshans, G. Van Assche, J. Wenger, R. Brouri, N. J. Cerf, and P. Grangier. Quantum key distribution using gaussian-modulated coherent states. *Nature*, 421:238, 2003.

Zero-error capacity of quantum channels

Romain Alléaume, Hugues Randriam, Gérard Cohen
Département Informatique et Réseaux,
TELECOM ParisTech

Rex A. C. Medeiros, Francisco M. de Assi
Departamento de Engenharia Elétrica,
Universidade Federal de Campina Grande,
Brazil

Unlike the capacity of classical channels, the capacity of quantum channels can be defined in different ways, depending on the information to be carried (classical or quantum), the available physical resources (entanglement, classical feedback channels, etc.) and the communication protocol [1]. Recently, Medeiros and Assis defined a new kind of capacity for quantum channels, the so called quantum zero-error capacity (QZEC) [2]. The QZEC stands for the maximum amount of classical information that can be transmitted per channel use with probability of error equal to zero. Our work was motivated by a paper from Shannon [3] introducing the zero-error capacity for discrete memoryless classical channels. For a survey on the classical zero-error information theory, see [4].
Consider a quantum channel $\mathcal{E}(\cdot) \equiv \{E_a\}$ on a d-dimensional Hilbert space. Given a set $\mathcal{S}$ of input states, we say that $\rho_i, \rho_j \in \mathcal{S}$ are *non-adjacent* if the Hilbert spaces spanned by the supports of $\mathcal{E}(\rho_1)$ and $\mathcal{E}(\rho_2)$ are orthogonal. In a more intuitive way, two states are non-adjacent iff they are separable (distinguishable) at the channels output. A quantum channels has positive QZEC iff there exist at least two non-adjacent input states on a given $\mathcal{S}$. We can also define n-length tensor product sequences of states in $\mathcal{S}$, i.e., $\mathcal{S}^{\otimes n}$. We had shown that non-adjacency relations between such sequences depend only on the adjacency relations of states in $\mathcal{S}$ (see Fig. 1).

$$\begin{array}{rcl} \mathcal{E}(\overline{\rho}_i) & = & \mathcal{E}(\rho_{i_1}) \otimes \cdots \otimes \left(\mathcal{E}(\rho_{i_k})\right) \otimes \cdots \otimes \mathcal{E}(\rho_{i_n}) \\ \mathcal{E}(\overline{\rho}_j) & = & \mathcal{E}(\rho_{j_1}) \otimes \cdots \otimes \left(\mathcal{E}(\rho_{j_k})\right) \otimes \cdots \otimes \mathcal{E}(\rho_{j_n}) \end{array}$$

Figure 1: Two distinguishable tensor product sequences $\mathcal{E}(\overline{\rho}_i)$ and $\mathcal{E}(\overline{\rho}_j)$. The distinguishibility of the sequences depends only on the distinguisibility of the states $\mathcal{E}(\rho_{i_j})$.

For convenience, we define the QZEC in terms of graph theory. Given a set $\mathcal{S}$, we can construct a characteristic graph $\mathcal{G}$ as follows: take as many vertices as $||\mathcal{S}||$ and connect two vertices if the corresponding input states in $\mathcal{S}$ are non-adjacent.

Definition 1 *The zero-error capacity of the quantum channel $\mathcal{E}$ is*

$$C^{(0)}(\mathcal{E}) = \sup_{\mathcal{S}} \sup_{n} \frac{1}{n} \log \omega\left(\mathcal{G}^n\right), \tag{1}$$

where $\omega(\mathcal{G})$ is the clique number of the graph $\mathcal{G}$, and $\mathcal{G}^n$ is the Shannon's $n-$product graph of $\mathcal{G}$.

The graph $\mathcal{G}^n$ can be viewed as a graph whose vertices are indexes of the sequences $\mathcal{S}^{\otimes n}$, and we connect two vertices if the corresponding sequences are non-adjacent. The set $\mathcal{S}$ achieving the supremum in Eq. (1) is called an *optimum* $\mathcal{S}$. Figure 2 shows a block diagram of a quantum zero-error communication system.

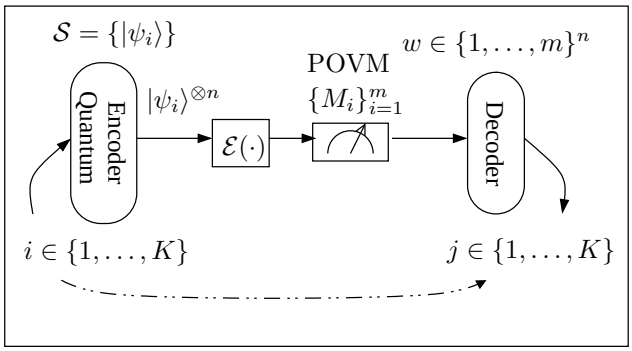


Figure 2: General representation of a zero-error communication system [5].

In terms of zero-error capacity, quantum channels exhibits all features and behaviors of classical channels. For example, we can readily construct a quantum channel $\mathcal{E}$ which gives rise the pentagon as characteristic graph for the set $\mathcal{S}$ attaining the QZEC [6]. This implies that the QZEC of this channel can only be reached by using a quantum code of length two. In this context, one question arises: is the QZEC a non-trivial generalisation of the classical ZEC? What non-trivial means in this context is not straigthforward to define, but we are in particular considering the following property that we believe is true for some quantum channels:

Proposition 1

A quantum channel is considered non-trivial, from the zero-error capacity viewpoint, if none of the sets $\mathcal{S}$ attaining the sup in Eq. (1) are orthogonal sets.

We have recently found a mathematically motivated quantum channel for which we claim (but did not fully prove yet) that the capacity can only be reached by a set of non-orthogonal quantum states [6]. Such channel is defined in a Hilbert of dimension five, and the following set

$$\mathcal{S} = \{|0\rangle, |1\rangle, |2\rangle, |3\rangle, |v\rangle\}; \quad |v\rangle = \frac{|3\rangle + |4\rangle}{\sqrt{2}}$$

gives rise to the pentagon as characteristic graph, as illustrated in Fig. 3(a). It is important to point out that if we replace the non-orthogonal state $|v\rangle$ by the state $|4\rangle$, and hence get a set of orthogonal states, the maximum transmission rate of any zero-error quantum code is below $\frac{1}{2}\log 5$, the zero-error capacity of the pentagon. These situations are illustrated in Fig. 3.

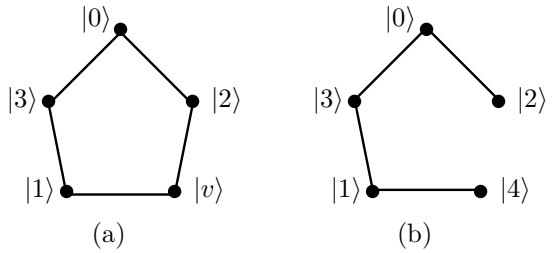


Figure 3: (a) Characteristic graph $\mathcal{G}$ for the subset $\mathcal{S}$ containing non-adjacent input states. (b) Characteristic graph for a subset $\mathcal{S}'$ of mutually orthogonal input states. In this case the transmission rate is less than $C^{(0)}$(pentagon) for any zero-error quantum code with alphabet $\mathcal{S}'$.

The behavior of this quantum channel is counterintuitive and has no classical equivalent. One may think that if we choose only orthogonal, and hence distinguishable states at the channel input, we can transmit at least the same amount of information per channel use. Cleary, this is not the case for the computational basis $\{|0\rangle, \ldots, |4\rangle\}$ of the Hilbert space of dimension five, since the state $|v\rangle$ in Fig. 3(a) is a superposition of the states $|3\rangle$ and $|4\rangle$.

Références

[1] M. A. Nielsen and I. L. Chuang. *Quantum Computation and Quantum Information.* Cambridge University Press, Cambridge, 2000.

[2] R. A. C. Medeiros and F. M. de Assis. *Int. J. Quant. Inf.*, 3(1):135–139, 2005.

[3] C. E. Shannon. *IRE Trans. Inform. Theory*, IT-2(3):8–19, 1956.

[4] J. Körner and A. Orlitsky. *IEEE Trans. Info. Theory*, 44(6):2207–2229, 1998.

[5] R. A. C. Medeiros, R. Alléaume, G. Cohen, and F. M. de Assis. *quant-ph/0611042.*

[6] R. A. C. Medeiros, R. Alléaume, H. Randriam, G. Cohen, and F. M. de Assis. *In preparation*

Codage des mots de poids constant

Nicolas Sendrier
CRI Paris-Rocquencourt, équipe SECRET,
Nicolas.Sendrier@inria.fr

Soit $W_{n,t}$ l'ensemble des mots binaires de longueur n et de poids t. Le problème que nous nous posons est de trouver un code binaire (dans le sens de la théorie de l'information) de l'ensemble $W_{n,t}$ muni d'une distribution uniforme. Ce code sera une application injective $f : W_{n,t} \to \{0,1\}^*$ qui associe à tout mot de poids constant une séquence binaire. Le codage associé $F : W_{n,t}^* \to \{0,1\}^*$ transforme une suite quelconque d'éléments de $W_{n,t}$ en une séquence binaire (par concaténation des mots de code): $F(x_1, \ldots, x_k) = f(x_1) \parallel \ldots \parallel f(x_k)$.
Le codage F doit être injectif (pour éviter les ambiguïtés au décodage), nous demanderons ici qu'il soit en plus surjectif, c'est-à-dire que toute séquence binaire puisse se décoder en une suite de lettre de $W_{n,t}$. Le décodage permet ainsi de coder une information binaire quelconque en un, ou plusieurs, mots de poids constant. Ceci sera particulièrement utile dans certains cryptosystèmes basés sur les codes correcteurs d'erreurs. Par exemple, dans le cryptosystème de Niederreiter [3], l'ensemble des textes clairs est de la forme $W_{n,t}$. De même, un tel codage est utile pour mettre en œuvre les conversions sémantiquement sûres du système de McEliece [2, 1].
La qualité d'une solution se mesurera essentiellement à partir de deux critères:

- la complexité des procédures de codage et de décodage,
- la longueur moyenne des mots de codes (optimalité).

Nous présenterons trois algorithmes, dont l'un est nouveau, résolvant ce problème. Tous trois ont été implantés dans des conditions comparables et représentent des compromis différents entre temps d'exécution et optimalité. Leurs mérites respectifs seront comparés.

1. Méthode énumérative [4].
2. Méthode récursive [5].
3. Méthode dichotomique (nouvel algorithme).

Références

[1] K. Kobara and H. Imai. Semantically secure McEliece public-key cryptosystems -Conversions for McEliece PKC-. In K. Kim, editor, *PKC'2001*, number 1992 in LNCS, pages 19–35. Springer-Verlag, 2001.

[2] R. J. McEliece. A public-key cryptosystem based on algebraic coding theory. *DSN Prog. Rep.,* Jet Prop. Lab., California Inst. Technol., Pasadena, CA, pages 114–116, January 1978.

[3] H. Niederreiter. Knapsack-type crytosystems and algebraic coding theory. *Prob. Contr. Inform. Theory*, 15(2):157–166, 1986.

[4] J. P. M. Schalkwijk. An algorithm for source coding. *IEEE Transactions on Information Theory*, 18(3):395–399, May 1972.

[5] N. Sendrier. Encoding information into constant weight words. In *IEEE Conference, ISIT'2005*, Adelaide, Australia, September 2005.

Multiplication scalaire de Montgomery pour les courbes de genre 2 en caractéristique 2

Silvain Duquesne
Université Montpellier II
LIRMM , UMR CNRS 5506
France

L'algorithme de multiplication scalaire de Montgomery sur une courbe elliptique permet de faire cette opération (fondamentale en cryptographie basée sur les courbes elliptiques) de façon efficace et résistante aux attaques par canaux cachés. Elle a été généralisée il y a quelques années au cas du genre 2 de différentes manières par T. Lange, P. Gaudry et moi-même dans le cas de la grande caractéristique. Dans le cas des courbes elliptiques le cas le plus intéressant est cependant celui de la caractéristique 2. Malheureusement les outils utilisés en caractéristique impaire ne peuvent pas être utilisés tels quels en caractéristique 2.

La méthode que j'ai utilisée en caractéristique impaire est basée sur l'utilisation de la surface de Kummer d'une courbe hyperelliptique de genre 2. Je propose ici une généralisation de cette surface de Kummer au cas de la caractéristique 2 qui permet de développer un algorithme de multiplication scalaire de Montgomery pour toutes les courbes de genre 2 en caractéristique 2.
L'algorithme obtenu est compétitif avec les méthodes connues jusqu'à présent pour la multiplication scalaire et possède en plus des propriétés supplémentaires comme la résistance aux attaques par canaux cachés. Il devient même particulièrement intéressant en terme de performances pour certains types de courbes.

Codes fonctionnels sur des surfaces quadriques

Frédéric A. B. Edoukou
CNRS, Institut de Mathématiques de Luminy
edoukou@iml.univ-mrs.fr

On étudie le code fonctionnel $C_2(X)$ défini sur une surface (algébrique) quadrique X sur le corps fini $\mathbb{F}_q$, de la même manière que l'a faite V. Goppa sur les courbes. La distance minimale de $C_2(X)$ est déterminée par le nombre de points $\#X_{Z(Q)}(\mathbb{F}_q)$ de l'intersection de X avec les surfaces quadriques $\mathcal{Q}$. Le nombre de points dans l'intersection de deux quadriques qui est utilisé pour estimer la distance minimale a été étudié par H. P. F. Swinnerton-Dyer, Y. Aubry, D. B. Leep et bien d'autres auteurs. Dans cet exposé nous donnons une estimation plus précise de ce nombre, ce qui nous permet d'en déduire non seulement la distance minimale de ce code, mais aussi les trois premiers poids et la structure géométrique des quadriques correspondantes.
Les méthodes utilisées sont celles développées dans les deux premiers chapitres de ma Thèse de Doctorat (2007) excepté le cas de l'intersection de deux surfaces quadriques elliptiques. Un traitement plus subtil basé d'une part sur une caractérisation des surfaces quadriques non-singulières due à I. Shafarevitch, d'autres parts l'étude des diviseurs sur une surface, et enfin l'utilisation de la borne de Weil et les améliorations qu'en ont faites Y. Aubry et M. Perret pour le cas des courbes non-lisses, permet de résoudre ce cas. On obtient alors des codes aussi bon que ceux qu'on pourrait construire selon les tables de Brouwer.

Références

[1] Y. Aubry, Reed-Muller codes associated to projective algebraic varieties. In "Coding Theory and Algebraic Geometry and Coding Theory ". (Luminy, France, June 17-21, 1991). Lecture Notes in Math., Vol. 1518 Springer-Verlag, Berlin, (1992), 4-17.

[2] Y. Aubry and M. Perret, On the characteristic polynomials of the Frobenuis endomorphism for projective curves over finite fields, Finite Fields and Theirs Applications 10, (2004), 412-431.

[3] F. A. B. Edoukou, Codes correcteurs d'erreurs construits à partir des variétés algébriques. Thèse de Doctorat, Université de la Méditerranée, Marseille, France, 2007.

[4] F. A. B. Edoukou, Codes by forms of degree 2 on quadric surfaces, IEEE Transcations on Information Theory, Vol. 54 Issue 2, February 2008.

[5] J. W. P. Hirschfeld, Finite projective spaces of three dimensions, Clarendon press. Oxford 1985.

[6] D. B. Leep and L. M. Schueller, Zeros of a pair of quadric forms defined over finite field. Finite Fields and Their Applications 5, (1999), 157-176.

[7] I. R. Shafarevich, Basic algebraic geometry 1, Springer-Verlag, 1994.

[8] H. P. F. Swinnerton-Dyer, Rational zeros of two quadratic forms, Acta Arithmetica 9 (1964), 261-270.

Twisting geometric codes

Majid Farhadi et Marc Perret
Laboratoire Émile Picard,
Université de Toulouse II, UMR 5219,
farhadi@univ-tlse2.fr , perret@univ-tlse2.fr

The aim of this paper is to explain how, starting from a Goppa code $C(X, G, P_1, ..., P_n)$ and an unramified cyclic covering $\pi : Y \to X$ of degree m, one can twist the initial code to another one $C(X, G + D_\chi, P_1, ..., P_n)$ (where D_χ is a non-principal degree 0 divisor on X associated to a character χ of $Gal(Y/X)$), in the hope that $\ell_X(G + D_\chi) > \ell_X(G)$. We give, using a MAGMA program, several examples where this occurs, and where both the initial and twisted codes have the same minimum distance, so that the initial codes have been improved.

Références

[1] N. Borne.– *Une formule de Riemann-Roch equivariante pour les courbes*, Thèse, Université Bordeaux 1, Janvier 2000.

[2] A. Garcia, F. Torres.–*On unramified covering of maximal curves*,Proceeding AGCT-10

[3] V.D. Goppa.– *Geometry and Codes*, in: Mathematics and its Applications,vol 24. Kluwer Academic Publisher, Dordrechet-Bo ston-London,1988

[4] E. Kani.– *The Galois-module structure of the space of holomorphic differentials of a curve* , J. Reine Angew. Math. 367 pp. 187–206, 1986

[5] J.P. Serre.– *Groupes algébriques et corps de classes.* Hermann, Paris 1959.

[6] H. Stichtenoth.– *Algebraic function fields and codes*, Springer-Verlag,Berlin, 1993.

[7] M. Tsfasman, S. Vladut.– *Algebraic-Geometric Codes*, Kluwer, Dordrecht, 1991.

Synthèse des ℓ-séquences décimées

Cédric Lauradoux
Université de Princeton

Andrea Röck
Équipe SECRET
INRIA Paris–Rocquencourt

La génération à haut débit des séquences pseudo–aléatoires est un sujet important dans le domaine des télécommunications. La décimation de la séquence originale permet de générer les sous–séquences en parallèle et ainsi d'augmenter le débit du générateur pseudo–aléatoire. Cette méthode a déjà été bien étudiée dans le cas des registres à décalage à rétroaction linéaire (*LFSRs*). Nous examinons la synthèse des sous–séquences, c'est à dire la complexité en portes logiques et la taille de la mémoire, qui sont générées par des registres à décalage avec retenues (*Feedback with Carry Shift Registers – FCSRs*).
Soit $S = (s_0, s_1, s_2, \dots)$ la séquence originale. La décimation d'ordre $d \geq 1$ de S est définie par les sous–séquences $S_d^i = (s_i, s_{i+d}, s_{i+2d}, \dots)$ pour $0 \leq i < d$. Notre but est la production en parallèle des sous–séquences S_d^i. Il y a deux méthodes pour la synthèse des sous–séquences. La première construit un LFSR pour chaque sous–séquence S_d^i via l'algorithme de Berlekamp–Massey [Mas69]. La deuxième méthode duplique les rétroactions et décompose en sous–registres [LE71].
Nous avons appliquer ces deux méthodes aux FCSRs. Les propriétés de corrélation des décimation des ℓ–séquences ont déjà été beaucoup étudiées [GK97]. Comme pour les LFSRs il existe des algorithmes de synthèse qui déterminent le plus petit FCSR qui génère une séquence, par exemple [ABN04]. Cependant, la taille des FCSRs correspondant aux sous–séquences et générés de cette manière est en général beaucoup plus grande que celle du FCSR original. Si la première méthode n'est pas satisfaisante, la méthode qui consiste à dupliquer les rétroactions est efficace.

Références

[ABN04] F. Arnault, T.P. Berger, and A. Necer. Feedback with Carry Shift Registers synthesis with the Euclidean Algorithm. *IEEE Transactions on Information Theory*, 50(5), 2004.

[GK97] M. Goresky and A. Klapper. Arithmetic crosscorrelations of feedback with carry shift register sequences. *IEEE Transactions on Information Theory*, 43(4):1342–1345, 1997.

[LE71] A. Lempel and W.L. Eastman. High Speed Generation of Maximal Length Sequences. *IEEE Trans. on Computer*, 2:227–229, 1971.

[Mas69] J.L. Massey. Shift-register synthesis and BCH decoding. *IEEE Trans. on Information Theory*, 15:122–127, 1969.

Cryptanalyse de LFSRs combinés

Frédéric Didier - Yann Laigle-Chapuy [a]
Équipe SECRET,
INRIA Paris-Rocquencourt

Les registres à décalage à rétroaction linéaire (LFSRs en anglais) sont un composant important dans la conception de nombreux algorithmes de chiffrements à flots. Nous étudions ici un modèle classique de registres multiples combinés par une fonction booléenne, et proposons une attaque par distingueur permettant de retrouver l'état initial.
Le modèle étudié ici est le générateur par combinaison de LFSR. Plusieurs registres à décalage à rétroaction linéaire, de longueurs variables, sont combinés par une fonction booléenne de filtrage F à n entrées réparties parmi les différents registres. Le but de l'attaquant est alors de retrouver les états internes initiaux des LFSRs à partir de la suite chiffrante.
Ce modèle a beaucoup été étudié et de nombreuses attaques existent. On peut classer les différentes attaques proposées et trois grandes catégories, les attaques par compromis temps-mémoire, les attaques algébriques, et les attaques par corrélations. C'est dans cette dernière famille, dont les idées remontent aux travaux de Siegenthaler[1] que se situe notre méthode.
Le premier point clé de cette attaque est l'existence d'un biais liant les entrées et les sorties de la fonction de filtrage :

$$Pr\left(F(x_1)+\cdots+F(x_{2k})=0 | x_1+\cdots+x_{2k}=0\right) \geq \frac{1}{2}\left(1+2^{-n(k-1)}\right)$$

Le principe de l'attaque est alors simple. On va effectuer une recherche exhaustive sur certains registres. Pour chaque initialisation, on calcule suffisamment de $2k$-uplets $(x_{t_1},\ldots,x_{t_{2k}})$ dont la somme est 0. On vérifie alors l'existence du biais attendu. S'il n'est pas présent, l'initialisation choisie n'était pas bonne et on recommence.
Nous détaillerons chaque phase de l'attaque en montrant comment l'utilisation de la structure des LFSR peut être utilisée pour obtenir une complexité parmi les meilleures existantes.

Références

[1] Thomas Siegenthaler. Decrypting a class of stream ciphers using ciphertext only. *IEEE Trans. Computers*, 34(1):81–85, 1985.

[a] Ce travail est en parti financé par le CELAR/DGA

Approximation d'une fonction à l'aide de moins de variables

Anne Canteaut et María Naya-Plasencia
INRIA équipe SECRET
Anne.Canteaut@inria.fr, Maria.Naya_Plasencia@inria.fr

Certains générateurs pseudo-aléatoires pour le chiffrement à flot sont constitués de n composants indépendants dont les sorties sont combinées au moyen d'une fonction booléenne non-linéaire f. Un cas typique est celui du générateur par combinaison de LFSRs, mais on trouve la même construction avec des registres à rétroaction non-linéaire par exemple dans le chiffrement à flot Achterbahn soumis à eSTREAM. L'avantage d'une remise à jour de l'état interne par sous-parties indépendantes est qu'elle permet de gérer un état de taille relativement grande en conservant une faible complexité de mise en œuvre. Toutefois, la principale faiblesse de cette construction est sa vulnérabilité aux attaques par corrélation puisqu'il devient possible de retrouver certaines parties de l'état interne en faisant abstraction des autres. Ces attaques reposent usuellement sur l'existence d'une approximation de la fonction de combinaison par une fonction qui ne dépend que d'un sous-ensemble des variables d'entrées de la fonction f, le nombre minimal de variables d'une telle approximation étant égal à $t+1$ où t est l'ordre de résilience de la fonction f.
Ainsi, les différentes variantes d'Achterbahn ont été successivement cryptanalysées dans [2, 1, 3] par la mise en évidence de relations de parité biaisées entre les bits de la suite chiffrante. Ces relations sont construites à partir de diverses approximations de la fonction par une fonction à k variables avec $t < k < n$. L'analyse de la complexité de ces attaques et leur optimisation sont liées d'une part à la détermination de la distance entre f et l'ensemble des fonctions ne dépendant que d'un sous-ensemble des variables d'entrées, et d'autre part l'estimation du biais d'une relation de parité dérivée d'une approximation donnée. Ce deuxième point est un problème délicat : en particulier, la même relation peut être obtenue à partir d'approximations très différentes (et de biais différents) comme le montrent les attaques présentées dans [1] et [3].
Dans ce travail, nous étudions donc ces deux questions et nous donnons notamment des bornes supérieures sur ces deux quantités, la distance entre f et les fonctions à k variables et le biais d'une relation de parité, bornes qui dépendent de la non-linéarité de la fonction f. Ceci implique en particulier que, si f possède une non-linéarité élevée, elle sera loin de toutes les fonctions dépendant d'un petit nombre de variables. Ce résultat généralise ainsi la propriété mise en évidence par Canteaut et Trabbia et par Zhang, qui montre que la meilleure approximation d'une fonction t-résiliente par une fonction à $(t+1)$ variables est réalisée par une fonction affine.

Références

[1] M. Hell & T. Johansson. " Cryptanalysis of Achterbahn-128/80 ". *IET Information and Security*, 1(2):47–52, 2007.

[2] T. Johansson, W. Meier, & F. Muller. " Cryptanalysis of Achterbahn ". in *Fast Software Encryption - FSE 2006*, LNCS 4047, pp. 1–14. Springer, 2006.

[3] M. Naya-Plasencia. " Cryptanalysis of Achterbahn-128/80 ". in *Fast Software Encryption - FSE 2007*, LNCS 4593, pp. 73–86. Springer, 2007.

Attaques génériques sur les schémas de Feistel avec permutations internes

Joana Treger Laboratoire PRiSM
Université de Versailles

Les schémas de Feistel ont été conçus pour construire des permutations de $[1, 2^{2n}]$, à partir d'applications (aussi appelées *fonctions internes*) de $[1, 2^n]$. Ils sont utilisés en cryptographie pour construire des permutations pseudo-aléatoires, en considérant une succession de tels schémas.
Soient $f_1, \ldots, f_k$ des applications sur $[1, 2^n]$ et $[L, R]$ un message de $[1, 2^{2n}]$. Un schéma de Feistel à k tours, utilisant $f_1, \ldots, f_k$ comme fonctions internes est défini par $\psi^k(f_1, \ldots, f_k) := \psi(f_k) \circ \ldots \circ \psi(f_1)$, où $\psi(f_i)([L, R]) = [R, L \oplus f_i(R)]$.
Luby et Rackoff [[L-R(1998)]] ont initié toute une série de recherches sur les schémas de Feistel, y compris sur des structures directement dérivées des schémas de Feistel classiques (i.e. avec fonctions internes). Cependant, très peu de travaux ont été réalisés sur les schémas de Feistel avec bijections internes, malgré un comportement différent de ces schémas et leur utilisation dans la conception d'algorithmes symétriques.
Je me suis intéressée aux attaques génériques sur les schémas de Feistel avec bijections internes. Il s'agit de déterminer, en fonction du nombre de tours, le nombre de calculs nécessaires pour distinguer ce schéma d'une permutation aléatoire (ou d'un générateur de permutations aléatoires) sur $[1, 2^{2n}]$. Plus précisément, je me suis intéressée aux attaques dites "attaques deux points", utilisant des corrélations entre des paires de messages.
La technique utilisée pour obtenir ces attaques est basée sur le calcul du nombre de k-uplets de bijections $(f_1, \ldots, f_k)$, tel que, pour un couple d'entrées/sorties donné, $\psi^k(f_1, \ldots, f_k)$ appliqué aux entrées, donne les sorties correspondantes. On calcule, à l'aide d'une formule générale, la valeur précédente pour tous les couples d'entrées/sorties possibles, ce qui permet d'en déduire les meilleures attaques deux points.
Pour un nombre de tours $k \leq 5$, la complexité des attaques obtenues (sauf pour 3 tours) est la même que pour les schémas de Feistel classiques, malgré des attaques différentes (voir [[Pat(2001)]]). Pour $k > 5$, les résultats sont souvent différents ; par exemple, pour 6 tours, les attaques ne sont a priori plus en $\mathcal{O}(2^{2n})$ comme dans le cas des schémas de Feistel classiques, mais en $\mathcal{O}(2^{3n})$.

Références

[L-R(1998)] M. Luby, R. Rackoff. How to construct pseudorandom permutations from pseudorandom functions. *SIAM Journal on Computing*, volume 17 n.2, pages 373–386, 1988.

[Pat(2001)] J. Patarin. Generic Attacks on Feistel Schemes. Asiacrypt'2001, editor, *Advances in Cryptology*, volume 2248, pages 222–238, 2001.

Produire une collision pour SHA-0 en une heure

Stéphane Manuel
Equipe SECRET - INRIA Paris-Rocquencourt
stephane.manuel@inria.fr

Thomas Peyrin
PRISM - France Télécom R&D

Une fonction de hachage cryptographique prend comme argument une chaîne de caractères de longueur finie arbitraire et renvoie une empreinte de taille fixée. Elle doit de plus vérifier un certain nombre de propriétés dont la résistance aux attaques par préimage, deuxième préimage et collision. En 1993, le NIST publia le premier standard de fonction de hachage dénommé SHA-0, qui fut rapidement remplacé en 1995 par une variante baptisée SHA-1. Bien que SHA-0 ne soit pas utilisée en pratique, son design très proche de celui de SHA-1 en a fait un objet privilégié d'étude pour toute la famille de fonctions SHA.

La première attaque par collision publiée contre SHA-0 fut menée par Chabaud et Joux en 1998. Elle consistait à trouver des chemins différentiels linéaires composés de collisions locales entrelacées. Cette attaque fut successivement améliorée par Biham et Chen en 2004 puis Biham *et al.* en 2005, par l'introduction des bits neutres puis de la technique des blocs multiples. Cela permit d'exhiber la première collision pour SHA-0 construite sur deux messages constitués de 4 blocs. En 2005, Wang *et al.* introduisirent une caractéristique non-linéaire, obtenue "à la main", ainsi que des techniques de modification de message. Cette nouvelle approche conduisit à des collisions sur des messages constitués de 2 blocs, dont les premiers blocs sont identiques. En 2006, Naito *et al.* réutilisèrent la caractéristique non-linéaire de Wang *et al.* avec une nouvelle technique dite de modification sous-marine pour produire une nouvelle collision pour SHA-0 avec une complexité théorique en 2^{36}. Leur attaque possède en pratique une complexité de l'ordre de $2^{40,3}$ appels à la fonction SHA-0. Depuis 2006 aucune autre attaque contre SHA-0 n'a été publiée. Cependant, de nouveaux outils sont apparus: un outil automatisé capable de générer des caractéristiques non-linéaires (De Cannière et Rechberger) et la technique des boomerangs (Joux et Peyrin). C'est en s'appuyant sur la mise en œuvre de ces techniques que conjointement avec Thomas Peyrin nous avons proposé à la conférence FSE 2008 la meilleure attaque par collision connue contre SHA-0.

En relâchant la dernière condition sur le vecteur de perturbations, on gagne par rapport aux attaques précédentes plusieurs degrés de liberté supplémentaires dans la recherche de bonnes caractéristiques linéaires L. On peut dès lors monter une attaque par blocs multiples formée d'une quasi-collision et d'une pseudo-collision. Cela implique l'utilisation de 2 caractéristiques non-linéaires différentes NL_1 et NL_2. En implémentant pour SHA-0 l'outil de De Cannière et Rechberger on construit ces 2 caractéristiques de façon automatisée pour chacun des vecteurs de perturbations qui semble intéressant. Une fois un bon triplet (L, NL_1, NL_2) sélectionné on entame la phase de recherche de collision. C'est ici qu'intervient la technique des boomerangs de Joux et Peyrin. En ajoutant des caractéristiques auxiliaires, on réduit la complexité de la recherche de collision. Au final pour cette attaque, la complexité théorique est 2^{33} et la complexité pratique est $2^{33,6}$ évaluations de la fonction, soit environ une heure de calcul sur un PC standard.

Titres

Auteurs

Liste des participants

Carlos Aguilar	XLIM-DMI, Université de Limoges	carlos.aguilar@unilim.fr
Boufeldja Allailou	Université Paris 8	b_allailou@yahoo.fr
Romain Alléaume	ENST Paris	romain.alleaume@enst.fr
François Arnault	XLIM-DMI, Université de Limoges	francois.arnault@xlim.fr
Daniel Augot	SECRET, INRIA-Rocquencourt	Daniel.Augot@inria.fr
Christine Bachoc	IMB, Université Bordeaux I	Christine.Bachoc@math.u-bordeaux1.fr
Pierre Barthélémy	IML, Université de Marseille	barthelemy@iml.univ-mrs.fr
Thierry Berger	XLIM-DMI, Université de Limoges	thierry.berger@unilim.fr
Aurore Bernard	XLIM-DMI, Université de Limoges	aurore.bernard@xlim.fr
Bhaskar Biswas	SECRET, INRIA-Rocquencourt	Bhaskar.Biswas@inria.fr
Céline Blondeau	SECRET, INRIA-Rocquencourt	Celine.Blondeau@inria.fr
Larbi Boubchir	GREYC, Université de Caen	larbi.boubchir@greyc.ensicaen.fr
Joseph Boutros	Texas A& M University at Qatar	boutros@tamu.edu
Anne Canteaut	SECRET, INRIA-Rocquencourt	Anne.Canteaut@inria.fr
Claude Carlet	Université Paris 8	claude.carlet@inria.fr
Guilhem Castagnos	GREYC, Université de Caen	guilhem.castagnos@info.unicaen.fr
Hervé Chabanne	SAGEM	herve.chabanne@sagem.com
Christophe Chabot	XLIM-DMI, Université de Limoges	christophe.chabot@xlim.fr
Pascale Charpin	SECRET, INRIA-Rocquencourt	Pascale.Charpin@inria.fr
Lionel Chaussade	Université de Rennes 1	lionel.chaussade@univ-rennes1.fr
Yoann Choyer	Lab. Émile Picard, Univ. Toulouse 3	yoann.choyer@laposte.net
Gérard Cohen	ENST, Paris	cohen@enst.fr
Iwen Coisel	Orange Labs R& D, Caen	iwen.coisel@orange-ftgroup.com
Jean Creignou	IMB, Université Bordeaux I	Jean.Creignou@math.u-bordeaux1.fr
Léonard Dallot	GREYC, Université de Caen	leonard.dallot@info.unicaen.fr
Hervé Diet	IMB, Université BordeauxI	Herve.Diet@math.u-bordeaux1.fr
Sylvain Duquesne	I3M, Université Montpellier 2	duquesne@math.univ-montp2.fr
Frédéric Edoukou	IML, Université de Marseille	edoukou@iml.univ-mrs.fr
Moulay Abdelaziz El Aabid	MAATICAH, Université Paris 8	elaabid@hotmail.com
Nadia El Mrabet	LIRMM - I3M, Université de Montpellier	elmrabet@lirmm.fr
Jean-Charles Faugère	INRIA SALSA / LIP6	Jean-Charles.Faugere@inria.fr
Cédric Faure	SECRET, INRIA-Rocquencourt	Cedric.Faure@inria.fr
Rafael Fourquet	MAATICAH Université Paris 8	rafael.fourquet@gmail.com
Laurent Fousse	Université Grenoble 1	laurent.fousse@imag.fr
Philippe Gaborit	XLIM-DMI, Université de Limoges	gaborit@unilim.fr
Benoit Gérard	SECRET, INRIA-Rocquencourt	Benoit.Gerard@inria.fr
Marc Girault	France Télécom / Orange Labs	marc.girault@orange-ftgroup.com
Laurent Imbert	LIRMM, Université de Montpellier	Laurent.Imbert@lirmm.fr
Sorina Ionica	PRISM,, Université de Versailles	sorina.ionica@prism.uvsq.fr
Thomas Izard	LIRMM, Université de Montpellier	thomas.izard@lirmm.fr
Amandine Jambert	Orange Labs R& D, Caen	amandine.jambert@orange-ftgroup.com
Bruno Kindarji	Sagem Sécurité, TELECOM ParisTech	bruno.kindarji@polytechnique.org
Pierre-Vincent Koseleff	IMJ, UPMC	koseleff@math.jussieu.fr
Patrick Lacharme	Université de Toulon	lacharme@univ-tln.fr
Yann Laigle-Chapuy	SECRET, INRIA-Rocquencourt	Yann.Laigle-Chapuy@inria.fr
Franck Landelle	DGA/CELAR	landelle.franck@laposte.net
Anthony Leverrier	Telecom ParisTech	anthony.leverrier@enst.fr
Pierre Loidreau	CELAR, Rennes	pierre.loidreau@m4x.org

Stéphane Manuel	SECRET, INRIA-Rocquencourt	Stephane.Manuel@inria.fr
Emmanuel Mayer	CELAR, Rennes	Emmanuel.Mayer@dga.defense.gouv.fr
Nicolas Méloni	Université de Toulon	nicolas.meloni@univ-tln.fr
Sihem Mesnager	MAATICAH, Université Paris 8	sihem.mesnager@univ-paris8.fr
Matthias Meulien	XLIM, Université de Limoges	matthias.meulien@xlim.fr
Bertrand Meyer	IMB, Université Bordeaux I	Bertrand.Meyer@math.u-bordeaux1.fr
Ivan Morel	ARENAIRE, Ens Lyon	ivan.morel@ens-lyon.fr
Ayoub Otmani	GREYC, Université de Caen	Ayoub.Otmani@info.unicaen.fr
Ludovic Perret	UPMC / LIP6 / INRIA SALSA	Ludovic.Perret@lip6.fr
Maria Naya Plasencia	SECRET, INRIA-Rocquencourt	Maria.Naya-Plasencia@inria.fr
Benjamin Pousse	XLIM-DMI, Université de Limoges	benjamin.pousse@xlim.fr
Guénaël Renault	UPMC / LIP6 / INRIA SALSA	guenael.renault@lip6.fr
Philippe Ravache	LITIS, Université de Rouen	philippe.ravache@etu.univ-rouen.fr
Christophe Ritzenthaler	IML, Université de Marseille	ritzenth@iml.univ-mrs.fr
Andrea Roeck	SECRET, INRIA-Rocquencourt	Andrea.Roeck@inria.fr
Lucile Sassatelli	ETIS - ENSEA/UCP	sassatelli@ensea.fr
Nicolas Sendrier	SECRET, INRIA-Rocquencourt	Nicolas.Sendrier@inria.fr
Patrick Solé	I3S, Sophia-Antipolis	sole@i3s.unice.fr
El Mamoun Souidi	Université Mohammed V Agdal Rabat	souidi@fsr.ac.ma
Damien Stehlé	ENS Lyon	damien.stehle@ens-lyon.fr
Jean-Pierre Tillich	SECRET, INRIA-Rocquencourt	Jean-Pierre.Tillich@inria.fr
Arnaud Tisserand	LIRMM, Université de Montpellier	arnaud.tisserand@lirmm.fr
Joana Treger	PRiSM, Université de Versailles	jot@prism.uvsq.fr
Félix Ulmer	IRMAR, Université de Rennes	felix.ulmer@univ-rennes1.fr
Brigitte Vallée	GREYC, Université de Caen	brigitte.vallee@info.unicaen.fr
Alexandre Venelli	ERISCS, Université de Marseille	alexandre.venelli@laposte.net
Auguste Venkiah	ETIS, UCP	venkiah@ensea.Fr
Damien Vergnaud	ENS, Paris	damien.vergnaud@ens.fr
Marion Videau	LORIA, Université Nancy 1	marion.videau@loria.fr
Julien Zamor	ENSTA, Paris	julienzamor@gmail.com
Gilles Zémor	IMB, Université Bordeaux I	Gilles.Zemor@math.u-bordeaux1.fr