Le décodage des codes de Goppa appliqué à la Cryptographie Asymétrique

Tania Richmond

Le décodage des codes de Goppa appliqué à la Cryptographie Asymétrique

Tania RICHMOND
Doctorante en Informatique
Laboratoire Hubert Curien,
18, Rue du Prof. Benoit Lauras,
42000 Saint-Étienne,
France
tania.richmond@univ-st-etienne.fr

Résumé - *Pour sécuriser les systèmes de communication, nous utilisons la Cryptographie. Pour corriger un maximum d'erreurs possible lors des transmissions, nous utilisons les codes correcteurs d'erreurs (et la Théorie des Codes). C'est dans ce contexte que se place mes recherches de thèse. De plus, je m'intéresse à la façon dont les algorithmes sont traduits en programmes pour le logiciel ou en circuits pour le matériel. Grâce à cela, des failles de sécurité peuvent être trouvées, et mon but est de proposer des contre-mesures.*

Mots clés - Décodage linéaire, Codes de Goppa, Cryptographie Asymétrique, Implantation sécurisée, Attaque par canaux cachés.

1 Introduction

1.1 Cryptologie

La cryptologie est l'art de dissimuler un message. Le concept est apparu dans l'Antiquité, notamment avec Jules César. La cryptologie comprend la cryptographie, domaine où l'on cherche des techniques sûres pour cacher une information ; et la cryptanalyse, domaine où l'on cherche des failles dans les techniques utilisées pour cacher un message afin de retrouver de l'information, partielle ou totale, sur le message ou la clef.

1.2 Cryptographie

La cryptographie symétrique est le principe apparu dans l'Antiquité. Elle consiste à chiffrer et déchiffrer en se servant d'une même clef secrète. Ce principe est encore utilisé de nos jours. La cryptographie asymétrique, ou à clef publique, est apparue en 1976 [DH76]. Pour chiffrer un message avec un cryptosystème asymétrique donné, on utilise la clef publique du destinataire. Celui-ci sera alors le seul à pouvoir déchiffrer le cryptogramme grâce à sa clef privée.

1.3 Cryptanalyse

De manière générale, il existe deux concepts d'attaques en cryptanalyse : les attaques passives, lors desquelles un attaquant ne fait qu'observer ce qu'il se passe en prenant des mesures si

nécessaire mais sans intervenir ; et les attaques actives, lors desquelles un attaquant peut modifier le texte chiffré, créer une faute, afin de comprendre ce qu'il se passe dans l'algorithme.

2 Codes correcteurs d'erreurs

2.1 Généralités

On appelle code correcteur d'erreurs une méthode de transformation qui convertit la représentation d'une information en une autre. La théorie des codes sert à enlever le bruit ajouté à un message (les erreurs) lors d'une transmission sur un canal (dit bruité). Afin d'arriver à détecter et corriger les erreurs, l'idée est de rajouter de la redondance d'information à celle déjà contenue dans le message initial. La correction n'est pas possible quand le nombre d'erreurs est trop grand.

2.2 Codes linéaires

Ici, nous nous intéressons uniquement aux codes linéaires. Cela signifie que la redondance est linéairement dépendante de l'information initiale contenue dans le message.
Un code linéaire possède un algorithme d'encodage simple, en temps polynomial (raisonnable). Le problème du décodage d'un code linéaire quant à lui, a été démontré NP-difficile en 1978 dans [BMvT78]. En revanche, il devient plus facile pour certaines classes de codes pour lesquelles il existe des algorithmes de décodage en temps polynomial, d'où l'étude et la construction de ces classes. Les codes de Goppa en sont une.

2.3 Codes en Cryptographie

La famille des codes de Goppa est celle proposée dans le premier cryptosystème à clef publique basé sur les codes correcteurs d'erreurs [McE78]. Elle peut également être utilisée dans un cryptosystème dit dual [Nie86] et dans un schéma de signature [CFS01]. Depuis une dizaine d'années, de nombreux protocoles également basés sur les problèmes de la théorie des codes ont été proposés.
L'objectif de ma thèse est de réaliser une implantation (voire plusieurs) de protocoles cryptographiques basés sur les codes correcteurs d'erreurs sur divers supports, puis d'analyser le comportement de ces implantations face aux attaques par canaux cachés.

3 Attaque par canaux cachés

3.1 Principe

Le principe des attaques par canaux cachés n'est apparu qu'en 1996 [Koc96]. Une attaque par canal caché est une attaque qui exploite les lois de la physique afin d'obtenir de l'information contenue dans des canaux associés à une implantation, un circuit. Le but est d'extraire des secrets manipulés par des cartes à puce ou des composants cryptographiques. Le canal caché n'a pas pour but de transmettre volontairement de l'information. Il laisse s'échapper de l'information, qu'un observateur doit savoir interpréter pour la comprendre. Par contre, des contre-mesures algorithmiques ou physiques peuvent être proposées pour fermer un canal

caché. L'implantation d'un cryptosystème est un compromis entre la sécurité et l'efficacité. C'est pourquoi la cryptanalyse et l'implantation doivent être considérées simultanément.

3.2 Exemples

Les principales attaques par canaux cachés sont : l'attaque temporelle et l'attaque par consommation d'énergie. L'une exploite les variations de temps de traitement d'un programme, qui dépend de la taille des données ; l'autre la consommation d'énergie du système dans sa globalité de façon instantanée, qui dépend des traitements à effectuer sur les données.
L'étude du cryptosystème de McEliece face à ce type d'attaques n'a commencé qu'il y a 5 ans [STM$^+$08].

4 Objectifs

Le but de ma thèse est d'optimiser les implantations de protocoles cryptographiques basés sur les codes correcteurs d'erreurs afin de proposer des solutions efficaces aux niveaux, de la quantité de ressources utilisées, de la vitesse obtenue, de la consommation d'énergie et de la sécurité. Pour cela, il est nécessaire de rechercher une adaptation des algorithmes (existants) afin d'améliorer leurs implantations dans le matériel [SWM$^+$09, Str10a, Str10b]. En effet, leurs implantations logicielles sont souvent déjà bien étudiées, mais le travail reste à faire d'un point de vue matériel.
Les protocoles basés sur des problématiques de la théorie des codes [BMvT78] sont rapides (en théorie), possèdent une excellente complexité théorique et résisteraient à des attaques quantiques. (À l'heure actuelle, il n'existe pas d'algorithme qui résout ces problèmes en temps polynomial.) Ces protocoles sont dits post-quantiques car ils doivent leur nom à leur résistance face aux attaques réalisables avec un ordinateur quantique. Ces attaques [Sho94, Sho99] permettraient en revanche de résoudre en temps polynomial les problèmes de la factorisation [RSA78] et du logarithme discret (problèmes de base de nombreux cryptosystèmes actuels).
Après avoir dressé un état de l'art des protocoles cryptographiques basés sur les codes correcteurs d'erreurs et les problèmes sur lesquels ils reposent, le travail de cette thèse consiste à connaître les attaques déjà existantes ainsi que les contre-mesures associées [AHPT10, CS10, CYAH$^+$11, MSSS11, SSMS10, Str10c, Str11, STM$^+$08] afin d'en trouver d'autres (en s'en inspirant par exemple). Une autre difficulté est d'adapter les algorithmes pour une implantation matérielle pour qu'ils soient à la fois efficaces et sûrs.
Comme à l'origine Robert J. McEliece prévoyait l'usage des codes de Goppa classiques binaires irréductibles pour son cryptosystème [McE78], nous nous sommes concentrés uniquement sur cette sous-classe de codes linéaires. Nous avons étudié des attaques portant essentiellement sur une utilisation de l'algorithme de Patterson pour le décodage de ces codes (dans le système de chiffrement à clé publique de McEliece).

5 Résultats

L'étude du décodage de la famille des codes de Goppa [Gop70, Ber73], souvent utilisés dans les protocoles cryptographiques, est en cours afin de déterminer quel algorithme (Euclide étendu, Berlekamp-Massey [Mas69], Patterson [Pat75]) est le plus efficace et sûr.

Une implantation partielle a d'ailleurs été commencée. Elle correspond à l'évaluation d'un polynôme dont les racines nous permettent de retrouver les positions d'erreurs. Cette étape est commune aux trois algorithmes. Deux versions de celle-ci ont été réalisées. Elles sont très similaires mais peuvent donner des traces de consommation d'énergie différentes. L'une est la méthode simple, l'autre la méthode de Horner [Hor19].
Des tests d'attaques sont en cours de réalisation afin de déterminer s'il existe des canaux cachés. Si c'est le cas, comment procéder, sinon une contre-mesure pourra être proposée.
L'objectif est d'obtenir une implantation sûre pour le décodage des codes de Goppa et de l'intégrer par la suite à une implantation sécurisée des protocoles cryptographiques y faisant appel, comme [McE78, Nie86]. Ces travaux ont été exposés à Crypt'Archi 2013 [RCFV13] et un article a été soumis et accepté à IndoCrypt 2013 [DCCR].

6 Conclusions et perspectives

La communauté cryptographique s'est principalement intéressée aux protocoles basés sur les problèmes de la théorie des nombres. L'innovation qu'apportent les cryptosystèmes basés sur les codes est forte car un avènement de l'ordinateur quantique rendrait vulnérables tous les autres moyens de sécurisation des données. Quand on sait à quel point la sécurité de celles-ci est importante, on peut comprendre les risques encourus si des alternatives ne sont pas développées.
L'objectif principal est de pouvoir déterminer quel est le meilleur algorithme de décodage pour les codes de Goppa afin d'obtenir une implantation matérielle de l'ensemble du cryptosystème de McEliece.
Ces travaux sont une rencontre entre les Mathématiques (théorie des codes) et l'Informatique (implantation).

7 Remerciements

Je remercie l'équipe *Cryptographie Appliquée et Télécom* du Laboratoire Hubert CURIEN à Saint-Étienne, et en particulier mon directeur de thèse, Viktor FISCHER, ainsi que mon co-encadrant, Pierre-Louis CAYREL. Je tiens également à remercier Pascal VÉRON, de l'Institut de Mathématiques de l'Université du Sud Toulon Var, pour sa collaboration.

Références

[AHPT10] R.M. Avanzi, S. Hoerder, D. Page, and M. Tunstall. Side-channel attacks on the mceliece and niederreiter public-key cryptosystems. 2010.

[Ber73] E. Berlekamp. Goppa codes. *Information Theory, IEEE Transactions on*, 19(5) :590–592, 1973.

[BMvT78] E. Berlekamp, R. McEliece, and H. van Tilborg. On the inherent intractability of certain coding problems. *IEEE Transactions on Information Theory*, 24(3) :384 – 386, may 1978.

[CFS01] N. T. Courtois, M. Finiasz, and N. Sendrier. How to achieve a mceliece-based digital signature scheme. 2248 :157–174, 2001.

[CS10] P.-L. Cayrel and F. Strenzke. Side channels attacks in code-based cryptography. *COSADE 2010 - First International Workshop on Constructive Side-Channel Analysis and Secure Design*, Session 2 : Side-Channel Attacks II :24–28, 2010.

[CYAH+11] P.-L. Cayrel, S.M. Yousfi Alaoui, G. Hoffmann, M. Meziani, and R. Niebuhr. Recent progress in code-based cryptography. *Information Security and Assurance*, 200 :21–32, 2011.

[DCCR] V. Dragoi, P.-L. Cayrel, B. Colombier, and T. Richmond. Polynomial structures in code-based cryptography.

[DH76] W. Diffie and M. Hellman. New directions in cryptography. *Information Theory, IEEE Transactions on*, 22(6) :644–654, 1976.

[Gop70] V. D. Goppa. A new class of linear correcting codes. *Problemy Peredachi Informatsii*, 6(3) :24–30, 1970.

[Hor19] W. G. Horner. A new method of solving numerical equations of all orders, by continuous approximation. *Philosophical Transactions of the Royal Society of London*, 109 :308–335, 1819.

[Koc96] P. Kocher. Timing attacks on implementations of diffie-hellman, rsa, dss, and other systems. In *Advances in Cryptology (CRYPTO'96)*, pages 104–113. Springer, 1996.

[Mas69] J. Massey. Shift-register synthesis and BCH decoding. *Information Theory, IEEE Transactions on*, 15(1) :122–127, 1969.

[McE78] R.J. McEliece. A public-key cryptosystem based on algebraic coding theory. *DSN progress report*, 42(44) :114–116, 1978.

[MSSS11] H. Molter, M. Stöttinger, A. Shoufan, and F. Strenzke. A simple power analysis attack on a McEliece cryptoprocessor. *Journal of Cryptographic Engineering*, 1(1) :29–36, April 2011.

[Nie86] H. Niederreiter. Knapsack-type cryptosystems and algebraic coding theory. *Problems of control and information theory*, 15(2) :159–166, 1986.

[Pat75] N. Patterson. The algebraic decoding of goppa codes. *IEEE Transactions on Information Theory*, 21(2) :203–207, 1975.

[RCFV13] T. Richmond, P.-L. Cayrel, V. Fischer, and P. Véron. A secure implementation of a goppa decoder. In *Cryptographic architectures embedded in reconfigurable devices-Cryptarchi 2013*, 2013.

[RSA78] R.L. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2) :120–126, 1978.

[Sho94] P.W. Shor. Algorithms for quantum computation : discrete logarithms and factoring. In *Foundations of Computer Science, 1994 Proceedings., 35th Annual Symposium on*, pages 124 –134, nov 1994.

[Sho99] P.W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM review*, 41(2) :303–332, 1999.

[SSMS10] A. Shoufan, F. Strenzke, H. Molter, and M. Stöttinger. A timing attack against patterson algorithm in the mceliece pkc. *Information, Security and Cryptology–ICISC 2009*, 5984 :161–175, 2010.

[STM+08] F. Strenzke, E. Tews, H. G. Molter, R. Overbeck, and A. Shoufan. Side Channels in the McEliece PKC. *Post-Quantum Cryptography*, 5299(5299/2008) :216–229, October 2008.

[Str10a] F. Strenzke. How to implement the public Key Operations in Code-based Cryptography on Memory-constrained Devices. *IACR Cryptology ePrint Archive*, 2010 :465, 2010.

[Str10b] F. Strenzke. A smart card implementation of the mceliece pkc. *Information Security Theory and Practices. Security and Privacy of Pervasive Systems and Smart Devices*, 6033 :47–59, 2010.

[Str10c] F. Strenzke. A timing attack against the secret permutation in the mceliece pkc. *Post-Quantum Cryptography*, 6061 :95–107, 2010.

[Str11] F. Strenzke. Timing attacks against the syndrome inversion in code-based cryptosystems. 2011.

[SWM+09] A. Shoufan, T. Wink, H. G. Molter, S. A. Huss, and F. Strenzke. A novel processor architecture for mceliece cryptosystem and fpga platforms. In *ASAP*, pages 98–105. IEEE, 2009.