Algebraic Analysis of McEliece's Scheme with Binary Quasi-Cyclic Codes

Jean-Charles Faugère[1], Ayoub Otmani[3], Ludovic Perret[1], Frédéric de Portzamparc[1], and Jean-Pierre Tillich[2]

[1] INRIA, Paris-Rocquencourt Center, POLSYS Project
UPMC Univ Paris 06, UMR 7606, LIP6, F-75005, Paris, France
CNRS, UMR 7606, LIP6, F-75005, Paris, France
jean-charles.faugere@inria.fr, ludovic.perret@lip6.fr, ludovic.perret@lip6.fr, fred.portzam@gmail.com
[2] SECRET Project - INRIA Rocquencourt
Domaine de Voluceau, B.P. 105 78153 Le Chesnay Cedex - France
ayoub.otmani@inria.fr, jean-pierre.tillich@inria.fr
[3] GREYC - Université de Caen - Ensicaen
Boulevard Maréchal Juin, 14050 Caen Cedex, France.

Abstract. La cryptographie fondée sur les codes exploite des problèmes difficiles émanant de la théorie des codes pour concevoir des primitives cryptographiques. Le cryptosystème de McEliece est le premier schéma basé sur le codes, et le plus célèbre. C'est un schéma de chiffrement asymétrique inventé en 1978 par R. J. McEliece. En particulier, il a suggéré d'utiliser des codes de Goppa binaires. Ce système repose sur la difficulté d'inverser la fonction de chiffrement, et en particulier, sur la difficulté de retrouver la clef privée à partir de données publiques. Depuis son apparition, il résiste à toute tentative de cryptanalyse, notamment aux attaques dédiées qui inversent la fonction de chiffrement. En revanche, quasiment aucun progrès n'a été constaté autour du problème de retrouver la clef privée à partir uniquement de données publiques. Récemment, les auteurs de [1] montrent que le problème de retrouver la clef privée est équivalent à celui de résoudre un système algébrique de type Vandermonde généralisé. Cette approche algébrique ne se limite d'ailleurs pas qu'au système de McEliece mais aussi à des variantes dites compactes qui proposent des matrices génératrices avec des structures particulières comme la cyclicité, la dyadicité, etc.. Dans cette exposé, on propose de faire le point sur la sécurité – par rapport aux attaques algébriques – d'une version compacte de McEliece utilisant des codes binaires quasi-dyadiques.

References

1. Jean-Charles Faugère, Ayoub Otmani, Ludovic Perret, and Jean-Pierre Tillich. Algebraic cryptanalysis of mceliece variants with compact keys. In Henri Gilbert, editor, EUROCRYPT, volume 6110 of Lecture Notes in Computer Science, pages 279–298. Springer, 2010.