Université de Caen Basse-Normandie

Laboratoire GREYC

GREYC ALGORITHMIQUE

Proposition de stage d'initiation à la recherche :

SAT et cryptanalyse.

Fabien Laguillaumie & Arnaud Lallouet

Lieu du stage :
Laboratoire GREYC
Université de Caen Basse-Normandie - Campus 2
Boulevard du Maréchal Juin - BP 5186
14032 Caen cedex - France
`https://www.greyc.fr/`

Durée du stage : 3 mois

Sujet : L'utilisation des algorithmes de résolution de problèmes de *satisfaisabilité* (problèmes SAT) pour casser des systèmes cryptographiques remonte à la fin des années 90. En général, leur efficacité n'est pas décisive, mais l'approche d'une cryptanalyse *via* un encodage en un problème SAT donne parfois des résultats surprenants ou contre-intuitifs.

Cette approche peut être adoptée sur des systèmes cryptographiques très variés comme les fonctions de hachage [MZ06], les chiffrements à flots [SNC09] ou des cryptosystèmes multivariés [BCJ07].

Les algorithmes de résolution des problèmes SAT (SAT solvers) sont de plus en plus nombreux, et de plus en plus sophistiqués. L'objectif de ce stage est d'étudier l'impact de certains de ces SAT solvers sur différents systèmes cryptographiques, en commençant par se faire la main sur de petites instances du système HFE [Pat95, Pat96], qui se traduisent assez simplement en instances du problème SAT.

Références

[BCJ07] G. Bard, N. Courtois and C. Jefferson. *Efficient Methods for Conversion and Solution of Sparse Systems of Low-Degree Multivariate Polynomials over GF(2) via SAT-Solvers.* Cryptology ePrint Archive, Report 2007/024, 2006. Available at : `http://eprint.iacr.org/2007/024.pdf`

[MZ06] I. Mironov and L. Zhang. *Applications of SAT Solvers to Cryptanalysis of Hash Functions.* Proc. of SAT 2006, Springer LNCS Vol. 4121, pp. 102–115 (2006)

[Pat95] J. Patarin. *Cryptanalysis of the Matsumoto and Imai Public Key Scheme of Eurocrypt'88*, Proc. of Crypto'95, Springer LNCS Vol. 963, pp. 248–261 (1995)

[Pat96] J. Patarin. *Hidden Fields Equations (HFE) and Isomorphisms of Polynomials (IP) : two new families of Asymmetric Algorithms*, Proc. of Eurocrypt'96, Springer LNCS Vol. 1070, pp. 33–48 (1996)

[SNC09] M. Soos, K. Nohl and C. Castelluccia. *Extending SAT solvers to cryptographic problems.* Proc. of SAT 2009, Springer LNCS Vol. 5584, pp. 244-257 (2009)