Learning a Zonotope and More : Cryptanalysis of NTRUSign Countermeasures

Léo Ducas * Phong Q. Nguyen †

17 juillet 2012

Les réseaux euclidiens suscitent de plus en plus d'intérêt pour la construction de primitives de cryptographie asymétrique, à la fois pour leurs qualités algorithmiques (calculs simples, parallélisables) et pour leur vertus théoriques (confiance en la difficulté des problèmes sous-jacents).

Dès 1995, un schéma de signature basé sur les réseaux est construit par Goldreich Goldwasser et Halevi, et en 2001, une instanciation efficace, NTRUsign, est proposé. Sa sécurité est rapidement mise en doute : la distribution des signatures révèle l'information lié a la clé secrète. En 2005, Nguyen et Regev formalise ce problème comme "l'apprentissage d'un parallélépipède" ; ils montrent que le lieux des minima des moments d'ordre 4 sont exactement les vecteurs de la clé secrètes, et que ces minima peuvent être trouvé par une descente de gradient étant donné seulement 400 paires messages-signature pour NTRUsign.

Des contremesures heuristiques ont été proposées, et nos travaux s'intéressent à la cryptanalyse de ces contremesures. La contremesure principale, dite méthode de perturbation a été proposées pour la standardisation de NTRUsign, et sa cryptanalyse passe par l'apprentissage d'un "zonotope" (convolution de plusieurs parallélépipèdes). Une analyse locale prouve l'existence de minima proche des vecteurs recherché. En pratique, nous ajoutons a un algorithme spécialisé de "Bounded Distance Decoding" pour corriger l'erreur, nous permettant de retrouver les clé secrète de NTRUsign avec 5000 signatures.

Pour la seconde contremesure, dite technique de déformation, nous montrons que les minima contiennent toujours de l'information sur la clé secrète, bien qu'elle soit différemment utilisable : de façon surprenante, retrouver la clé a partir de ces minima peut se ramener a un problème d'énumération d'isomorphisme de Graphe, énumération qui s'avère facile pour les instances considérées.

Nos travaux démontrent ainsi l'importance d'utiliser des techniques prouvablement sûre pour éviter toute fuite d'information, tel le "Gaussian Sampling" (proposé par GPV en 2008), malgré une impacte significative sur l'efficacité des cryptosystèmes construits.

*ENS, Dépt. Informatique , 45 rue d'Ulm, 75005 Paris, France.

†INRIA and ENS, Dépt. Informatique , 45 rue d'Ulm, 75005 Paris, France. http://www.di.ens.fr/~pnguyen/. Part of this work is supported by the Commission of the European Communities through the ICT program under contract ICT-2007-216676 ECRYPT II.