Journal de Théorie des Nombres
de Bordeaux **12** (2000), 293–307

Cryptography based on number fields with large regulator

par Johannes BUCHMANN, Markus MAURER
et Bodo MÖLLER

Résumé. Nous introduisons une variante du protocole de signature et d'identification de Fiat-Shamir, basée sur la difficulté pratique qu'il y a à calculer des générateurs des idéaux principaux dans les corps de nombres. Nous montrons en outre comment utiliser les heuristiques de Cohen-Lenstra-Martinet pour les groupes de classes dans le but de construire des corps de nombres dans lesquels le calcul de générateurs des idéaux principaux est encore hors d'atteinte.

Abstract. We explain a variant of the Fiat-Shamir identification and signature protocol that is based on the intractability of computing generators of principal ideals in algebraic number fields. We also show how to use the Cohen-Lenstra-Martinet heuristics for class groups to construct number fields in which computing generators of principal ideals is intractable.

Johannes Buchmann, Markus Maurer, Bodo Möller
Technische Universität Darmstadt
Fachbereich Informatik
Alexanderstr. 10
64283 Darmstadt
Germany
E-mail : {buchmann,mmaurer,moeller}@cdc.informatik.tu-darmstadt.de

Manuscrit reçu le 17 avril 2000.