Accélération du crible dans CADO-NFS via les arbres de factorisation

Ambroise Fleury

CEA List / LIP6
ambroise.fleury@cea.fr

Ma présentation concernera nos travaux sur l'accélération du crible dans CADO-NFS grâce à la factorisation par lot. CADO-NFS [2] est l'implémentation du crible algébrique derrière les derniers records de factorisation RSA-240 (2019) et RSA-250 (2020). Son temps de calcul est dominé par le crible dont l'objectif est d'identifier rapidement un grand nombre d'entiers friables d'une certaine forme. Marquer les multiples des petits nombres premiers représente une fraction importante du temps total.

Nos travaux explorent l'utilisation d'un algorithme de factorisation par lots [1] dû à Bernstein, qui avait suggéré de l'utiliser pour éviter de cribler les grands nombres premiers. Nous nous intéressons à l'idée inverse, c'est-à-dire l'utiliser pour éviter de cribler les petits premiers qui ne correspondent qu'à une petite partie des bits des nombres candidats et apportent donc peu d'information sur leur friabilité. Un crible partiel ne traitant pas les petits premiers permet d'effectuer un filtrage intermédiaire en éliminant les entiers candidats dont le produit des facteurs inconnus est trop grand, c'est à dire les nombres ayant peu de chance d'être friable. Les arbres de factorisation sont finalement utilisés sur le petit ensemble des candidats survivants afin de compléter leur factorisation et d'éliminer alors une deuxième vague de mauvais candidats.

Nous avons réussi à trouver des bornes telles qu'un nombre assez grand de candidats soient éliminés avant la factorisation par lots pour obtenir un gain de temps mais qu'il y ait en contrepartie assez de survivants pour conserver l'essentiel des candidats. Ceci devrait permettre d'accélérer (un peu) la factorisation des grands entiers.

[1] Daniel J. Bernstein. *How to find small factors of integers*. URL: `http://cr.yp.to/papers.html`.

[2] Fabrice Boudot et al. "Comparing the difficulty of factorization and discrete logarithm: a 240-digit experiment". In: *Advances in Cryptology – CRYPTO 2020*. Ed. by Daniele Micciancio and Thomas Ristenpart. Vol. 12171. Lecture Notes in Computer Science. Santa Barbara CA, United States: Springer, Aug. 2020, pp. 62–91. DOI: `10.1007/978-3-030-56880-1\_3`. URL: `https://hal.inria.fr/hal-02863525`.