Factoring RSA of 240 decimal digits and computing discrete logarithms in a 240-decimal-digit prime field with the same software and hardware.

Aurore Guillevic*[1]

[1]Inria Nancy - Grand Est – Institut National de Recherche en Informatique et en Automatique – France

Résumé

Joint work with Fabrice Boudot, Pierrick Gaudry, Nadia Heninger, Emmanuel Thomé, Paul Zimmermann
(https://caramba.loria.fr/dlp240-rsa240.txt)
In December 2019 were announced two new record computations: the factorization of RSA-240 (240 digits, 795 bits) and discrete logarithm computation in a prime field of the same size, with the same software, running on the same platforms. This is the first time that integer factorization (IF) and discrete logarithm (DL) of the same size are computed together. The previous RSA factorization record was in Dec. 2009 by Kleinjung et al., who factorized RSA-768 (bits, 232 decimal digits). The previous DL record computation was in June 2016 by Kleinjung et al., for a prime field of 768 bits: there were seven years between RSA factorization and DL computation records of the same size, and ten years between the two RSA factorization records.

The best known algorithm to address challenges of this size is the Number Field Sieve, designed in the 90's, first for integer factorization, then adapted to discrete logarithm computation. The free software Cado-NFS implements the NFS algorithm, and has been developed for ten years. The same software modules were used, with different parameters, on four different computing ressources in EU and US, to achieve the two records. Thanks to algorithmic variants well-suited for large sizes, and fine tuning of the parameters, the DL record was actually three times faster than expected compared to the previous DL record, when comparing on the same hardware. Moreover our work shows that computing a discrete logarithm is not much harder
than a factorization of the same size.

In this talk, I will present the Number Field Sieve and its variants for IF and DL. Then I will present our algorithmic improvements, some of the software properties, and parameter options chosen for the records. Finally I will discuss on expectations on how the computations would scale for larger records.

*Intervenant