PHD THESIS PROPOSAL

POLYNOMIAL SELECTION FOR RSA-1024: SAVING A FACTOR TWO

PAUL ZIMMERMANN

Scientific Context. RSA-512 was factored in 1999 [2], RSA-768 in 2009 [5], we expect RSA-1024 will be factored around 2020-2025, and as for RSA-512 and RSA-768, our team will play a major role in this new record factorization. Since the advent of the Number Field Sieve, major improvements have been made in the polynomial selection stage, by Murphy [6], by Kleinjung [3, 4], and more recently by our team [1]. In this last article, the authors propose a set of polynomials that would give a sieving time for RSA-1024 only about 500 times larger than that for RSA-768 (instead of 1000 times as claimed in [5]). The goal of this PhD thesis is to save (at least) another factor of two in the RSA-1024 sieving time thanks to polynomial selection, and to produce the polynomials that will be used for the factorization of RSA-1024.

Detailed Description. To factor an integer N, the polynomial selection stage has to produce two irreducible polynomials $f(x)$ and $g(x)$ with integer coefficients that share a common root m modulo N. Usually $g(x)$ is a linear polynomial, and for RSA-1024 we expect $f(x)$ will be of degree 6 or 7. The polynomials $f(x)$ and $g(x)$ should have small coefficients (*size property*) and have many roots modulo small primes (*root property*). While several algorithms have been invented to produce good pairs of polynomials, several open problems still remain:

- classical polynomial selection uses a linear polynomial $g(x)$ [3, 4]. Is it possible to find two non-linear polynomials with a better global behaviour [7]?
- polynomial selection algorithms usually first find good *raw* polynomials, then optimize them for size properties, and finally for root properties. It might be better, when optimizing the size properties, to take into account the expected saving one can expect for the root properties;
- in [4], Kleinjung proposes to generate polynomials with a huge skewness, for which *line sieving* would be more appropriate than the now classically used *lattice sieving*;
- finally in [1] the authors propose a new way to find good size properties, but the corresponding global optimization problem still remains unsolved.

Working Environment. The PhD candidate will work at Inria Nancy - Grand Est and LORIA, in the Caramba team. For experiments, she/he will benefit from the CADO-NFS package, which will also be used to implement and test new algorithms and ideas. She/he will also have access to a 768-core cluster.

References

[1] Bai, S., Bouvier, C., Kruppa, A., and Zimmermann, P. Better polynomials for GNFS. *Mathematics of Computation 85* (2016), 861–873.

[2] Cavallar, S., Dodson, B., Lenstra, A. K., Lioen, W., Montgomery, P. L., Murphy, B., te Riele, H., Aardal, K., Gilchrist, J., Guillerm, G., Leyland, P., Marchand, J., Morain, F., Muffett, A., Putnam, C., Putnam, C., and Zimmermann, P. Factorization of a 512–bit RSA modulus. In *Proceedings of Eurocrypt'2000* (Bruges, Belgium, 2000), B. Preneel, Ed., vol. 1807 of *Lecture Notes in Computer Science*, Springer-Verlag, pp. 1–18.

[3] Kleinjung, T. On polynomial selection for the general number field sieve. *Mathematics of Computation 75* (2006), 2037–2047.

[4] Kleinjung, T. Polynomial selection. slides presented at the CADO workshop on integer factorization, 2008.

[5] Kleinjung, T., Aoki, K., Franke, J., Lenstra, A. K., Thomé, E., Bos, J. W., Gaudry, P., Kruppa, A., Montgomery, P. L., Osvik, D. A., te Riele, H., Timofeev, A., and Zimmermann, P. Factorization of a 768-bit rsa modulus. In *CRYPTO 2010 Advances in Cryptology - CRYPTO 2010* (Santa Barbara, USA, 2010), T. Rabin, Ed., vol. 6223 of *Lecture Notes in Computer Science*, Springer-Verlag, pp. 333–350.

[6] Murphy, B. A. *Polynomial Selection for the Number Field Sieve Integer Factorisation Algorithm*. PhD thesis, Australian National University, 1999. 144 pages.

[7] Prest, T., and Zimmermann, P. Non-linear polynomial selection for the number field sieve. *Journal of Symbolic Computation 47*, 4 (2012), 401–409.