A comparison of pairing-friendly curves at the 192-bit security level

Aurore Guillevic[1]

[1]Université de Lorraine, CNRS, Inria, LORIA, Nancy, France

February 19, 2019

Abstract

Pairings on elliptic curves are involved in signatures, NIZK, and recently in blockchains (ZK-SNARKS). These pairings take as input two points on an elliptic curve E over a finite field, and output a value in an extension of that finite field. Usually for efficiency reasons, this extension degree is a power of 2 and 3 (such as 12,18,24), and moreover the characteristic of the finite field has a special form. The security relies on the hardness of computing discrete logarithms in the group of points of the curve and in the finite field extension.

In 2013-2016, new variants of the function field sieve and the number field sieve algorithms turned out to be faster in certain finite fields related to pairing-based cryptography. Now small characteristic settings (with $\mathrm{GF}(2^{4n})$, $\mathrm{GF}(3^{6m})$) are discarded, and the situation of $\mathrm{GF}(p^k)$ where p is prime and k is small (in practice from 2 to 54) is unclear.

The asymptotic complexity of the Number Field Sieve algorithm in finite fields $\mathrm{GF}(p^k)$ (where p is prime) and its Special and Tower variants is given by an asymptotic formula of the form $A^{c+o(1)}$ where A depends on the finite field size ($\log p^k$), $o(1)$ is unknown, and c is a constant between 1.526 and 2.201 that depends on p, k, and the choice of parameters in the algorithm.

In this talk, we adapt to higher k the previous work [2, 3] that refines the approaches of Menezes-Sarkar-Singh [4] and Barbulescu-Duquesne [1] to estimate the cost of a hypothetical implementation of the Special-Tower-NFS in $\mathrm{GF}(p^k)$ for small k. We consider the 192-bit security level and update the parameter sizes for pairing-based cryptography with k in $\{12, 16, 18, 24\}$. Then we compare the pairing efficiency on these curves. If time allows it, we will also consider embedding degrees 15, 21, 27.

References

[1] Razvan Barbulescu and Sylvain Duquesne. Updating key size estimations for pairings. *Journal of Cryptology*, Jan 2018. `https://hal.archives-ouvertes.fr/hal-01534101v2`.

[2] Aurore Guillevic, Simon Masson, and Emmanuel Thomé. Cocks–pinch curves of embedding degrees five to eight and optimal ate pairing computation. In preparation, 2019.

[3] Aurore Guillevic and Shashank Singh. On the α value of polynomials in the tower number field sieve algorithm. In preparation, 2019.

[4] Alfred Menezes, Palash Sarkar, and Shashank Singh. Challenges with assessing the impact of NFS advances on the security of pairing-based cryptography. In Raphael C.-W. Phan and Moti Yung, editors, *Mycrypt Conference, Revised Selected Papers*, volume 10311 of *LNCS*, pages 83–108, Kuala Lumpur, Malaysia, December 1-2 2016. Springer. `http://eprint.iacr.org/2016/1102`.