An overview on the discrete logarithm problem in finite fields

Razvan Barbulescu (CNRS, Paris 6, Paris 7)

The discrete logarithm problem (DLP) in the multiplicative group of finite fields has been studied since long in the case of prime fields. Using the analogy between number fields and function fields, the algorithms to tackle the case of fields F_{q^n} where q is small compared to q^n have copied the prime case and one obtained similar complexities. Due to a quasi-polynomial algorithm which makes use of the Frobenius automorphism, the small characteristic case lost its utility in cryptology. The remaining hardest case, sometimes called the gap, has been for long the intermediate case, F_{p^n} where neither p not n are small.

There are to lines of development to adapt algorithms for F_p to arbitrary F_{p^n}. On the one hand, Hellman used number fields to adapt Index calculus to F_{p^2} when $p \equiv 3 \pmod 4$. The idea generalizes and can be used to tackle fields $\mathrm{F}_{p^{\kappa\eta}}$ with the same complexity as the fields F_{P^κ} where $P \approx p^\eta$ is a prime. On the other hand, one adapted the number field sieve by selecting differently the polynomials : instead of using two polynomials with a common root modulo p we require them to have a common irreducible factor modulo p which has degree n. This is a hard problem which is often solved with LLL.

The utilisation of pairings in cryptology requires that the DLP in F_{p^n} is hard. In 2001 the key sizes were estimated under the hypothesis that the DLP is at least as hard as factoring integers of the same bit size. The pairing-friendly elliptic curves which were studied for efficiency purposes rely on the difficulty of DLP in a particular set of finite fields : F_{p^k} when p has a polynomial form and k has small proper factors. A combination of the two directions of developmet presented above allows to tackle these fields with a complexity below that of factoring. A precise estimation of B. and Duquesne made new key size estimations, which correspond roughly to doubling then in order to keep the announced security.

References

[BD18] Razvan Barbulescu and Sylvain Duquesne. Updating key size estimations for pairings. *Journal of Cryptology*, 2018.

[BGGM15] Razvan Barbulescu, Pierrick Gaudry, Aurore Guillevic, and François Morain. Improving NFS for the discrete logarithm problem in non-prime finite fields. In *Advances in Cryptology - EURO-*

CRYPT 2015, volume 9056 of *Lecture Notes in Comput. Sci.*, pages 129–155, 2015.

[BGK15] Razvan Barbulescu, Pierrick Gaudry, and Thorsten Kleinjung. The Towed Number Field Sieve. In *Advances in Cryptology – ASIACRYPT 2015*, volume 9453 of *Lecture Notes in Comput. Sci.*, pages 31–55, 2015.

[KB16] Taechan Kim and Razvan Barbulescu. The extended tower number field sieve: A new complexity for the medium prime case. In *Advances in Cryptology – CRYPTO 2016*, volume 9814 of *Lecture notes in computer science*, pages 543–571, 2016.