Individual Discrete Logarithm with Sublattice Reduction

Haetham Al Aswad[**] and Cécile Pierrot

Université de Lorraine, CNRS, Inria Nancy, France

One of the major problems in asymmetric cryptography is the discret logarithm problem. Given a cyclic group G, a generator $g \in G$ and a target $T \in G$, solving the discrete logarithm problem in G means finding an integer x modulo $|G|$ such that $g^x = T$. Our work deals with the hardness of this problem when the considered group $G = \mathbb{F}_{p^n}^*$ is the invertible elements in a finite field where the extension degree n is a composite integer.

Considering finite fields with composite extensions is highly motivated by pairing-based cryptography. Nowadays pairings are deployed in the marketplace, for example in the Elliptic Curve Direct Anonymous Attestation protocol that is embedded in the current version of the Trusted Platform Module: TPM2.0 Library, released in 2019. The security of this kind of protocol relies on both the discrete logarithm problem in the group of points of an elliptic (pairing-friendly) curve, and on the discrete logarithm problem in a non prime finite field, which means where the extension degree $n > 1$. Pairing constructions can work with prime extensions, such as $\mathbb{F}_{p^2}$ and $\mathbb{F}_{p^3}$ but composite extensions are common, such as $\mathbb{F}_{p^4}$, $\mathbb{F}_{p^6}$ and $\mathbb{F}_{p^{12}}$.

The Number Field Sieve and its numerous variants is the best algorithm to compute discrete logarithms in finite fields of medium and large characteristics. When the extension degree n is composite and the characteristic p is of medium size, the Tower variant (TNFS) is asymptotically the most efficient one. Our work deals with the last main step of TNFS, namely the individual logarithm step, that computes a smooth decomposition of a given target T in the finite field thanks to two distinct phases: an initial splitting step, and a descent tree.

We improve on the current state-of-the-art Guillevic's algorithm [Gui19] dedicated to the initial splitting step for composite n. While still exploiting the proper subfields of the target finite field, we modify the lattice reduction subroutine that creates a lift in a number field of the target T. Our main idea is to use sublattices to lower the dimension of the considered vectors that help to construct lifted elements of T. Our algorithm returns lifted elements with lower degrees and coefficients, resulting in lower norms in the number field. The lifted elements are not only much likely to be smooth because they have smaller norms, but it permits to set a smaller smoothness bound for the descent tree. Asymptotically, our algorithm is faster and works for a larger area of finite fields than [Gui19], being now relevant even when the characteristic p is such that $L_{p^n}(1/3) \leq p < L_{p^n}(1/2)$. Besides, we prove that in large characteristic finite fields, using an enumeration algorithm like Schnorr-Euchner's one instead of lattice reduction is asymptotically optimal for the individual logarithm step.

In practice, we conduct experiments on 500-bit and 700-bit composite finite fields: our method becomes more efficient as the largest non trivial divisor of n grows, being thus particularly adapted to even extension degrees. For instance, with a 500-bit target finite field $\mathbb{F}_{p^{46}}$, we manage to decrease the norms as follows: a regular lift of a target T in the number field gives lifted elements with a 824-bit norm. Applying [Gui19] would create 568-bit candidates to test for smoothness, whereas our algorithms returns 537-bit candidates in the number field, in average.

Key words: Public Key Cryptography. Discrete Logarithm. Finite Fields. Tower Number Field Sieve. Initial Splitting Step. Smoothing Step.

References

[Gui19] Aurore Guillevic. Faster individual discrete logarithms in finite fields of composite extension degree. *Math. Comput.*, 88(317):1273–1301, 2019.

[**] Speaker. PhD student partially funded by the French Ministry of Army - AID Agence de l'Innovation de Défense.