Discrete Logarithm Factory

Haetham Al Aswad[**]

Université de Lorraine, CNRS, Inria Nancy, France

One of the major problems in asymmetric cryptography is the discrete 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 with extension degree n greater than one ($n > 1$).

Considering non prime finite fields (i.e with extension degree n greater than one) 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. Pairing constructions can work with prime extensions, such as $\mathbb{F}_{p^2}$ and $\mathbb{F}_{p^3}$ or composite extensions, 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 Extended Tower variant (exTNFS) is asymptotically the most efficient one. We present an algorithm to quickly compute discrete logarithms in a wide range of finite fields at the cost of a unique precomputation. The original idea was the Factorization Factory introduced by Coopersmith [**?**] to deal with the integer factorisation problem. This idea can be adapted to the discrete logarithm in prime finite fields (i.e. with extension degree equal to one), this is done in the thesis of Barbulescu [**?**]. Our work generalises the Factory idea to the discrete logarithm in finite fields of any extension degree. Our algorithm can be viewed as a way of dividing the tasks of the Number Field Sieve into two parts, a precomputation part that only depends on the order of magnitude of the finite field, and a computation part that is specific to the finite field we deal with. This is done by exploiting the Galois group of a certain polynomial which garantees some properties in a wide range of characteristics.

The algorithm applies on various variants of NFS, perhaps the most notable one is the Extended Tower variant (exTNFS) when the extension degree is composite. Given $\mathbb{F}_{p^n}$ a finite field of size $Q = p^n$ where p is prime and n is composite. The cost of computing a discrete logarithm in $\mathbb{F}_{p^n}$ using exTNFS is $\mathrm{L}_Q\left(1/3, 1.75\right)$. Given a table that can be computed once and for all with a complexity of $L_Q(1/3, 1.94)$, our algorithm allows to compute discrete logarithms in a wide range of finite fields with a complexity of $\mathrm{L}_Q\left(1/3, 1.37\right)$ for each finite field.

Key words: Public Key Cryptography. Discrete Logarithm. Finite Fields. Tower Number Field Sieve. Discrete Logarithm Factory.

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