A quasi-polynomial algorithm for discrete logarithm in finite fields of small characteristic.

Emmanuel Thomé (INRIA, Nancy)

We present a new discrete logarithm algorithm, in the same vein as in recent works by Joux, using an asymptotically more efficient descent approach. The main result gives a quasi-polynomial heuristic complexity for the discrete logarithm problem in finite field of small characteristic. By quasi-polynomial, we mean a complexity of type $n^{O(\log n)}$ where $n$ is the bit-size of the cardinality of the finite field. Such a complexity is smaller than any $L(\varepsilon)$ for $\varepsilon > 0$. It remains super-polynomial in the size of the input, but offers a major asymptotic improvement compared to $L(1/4 + o(1))$. 