Discrete Logarithms in Small Characteristic Finite Fields: a Survey of Recent Advances*

Antoine Joux

Sorbonne Universités, UPMC Université Paris 6, Paris, France
Antoine.Joux@m4x.org

Abstract

The discrete logarithm problem is one of the few hard problems on which public-key cryptography can be based. It was introduced in the field by the famous Diffie–Hellman key exchange protocol. Initially, the cryptographic use of the problem was considered in prime fields, but was readily generalized to arbitrary finite fields and, later, to elliptic or higher genus curves.

In this talk, we survey the key technical ideas that can be used to compute discrete logarithms, especially in the case of small characteristic finite fields. These ideas stem from about 40 years of research on the topic. They appeared along the long road that leads from the initial belief that this problem was hard enough for cryptographic purpose to the current state of the art where it can no longer be considered for cryptographic use. Indeed, after the recent developments started in 2012, we now have some very efficient practical algorithms to solve this problem. Unfortunately, these algorithms remain heuristic and one important direction for future research is to lift the remaining heuristic assumptions.

1998 ACM Subject Classification F.2.1 Numerical Algorithms and Problems

Keywords and phrases Cryptography, Discrete logarithms, Finite fields

Digital Object Identifier 10.4230/LIPIcs.STACS.2017.3

Category Invited Talk

* This work has been supported in part by the European Union's H2020 Programme under grant agreement number ERC-669891.