An optimal generic algorithm for the discrete log problem

(Hendrik Hubrechts)

We present the algorithm of Pohlig and Hellman together with Shanks Baby Step Giant Step that computes the discrete log in a finite group, which has as essential time complexity the square root of the largest prime dividing the group order. This is an example of a generic algorithm, one that works for every group of a given order. Then we prove Shoups result that such a generic algorithm for the DLP cannot be substantially faster. Even an apparently trivial task as the choice-decision-Diffie-Hellman problem cannot be solved efficiently with a generic algorithm, as we will show.