Ramanujan Graphs and Random Reducibility of Discrete Log on Isogenous Elliptic curves

Ramarathnam Venkatesan
Microsoft Research

Abstract

Cryptographic applications using an elliptic curve over a finite field compute its order (i.e. the number of points on it) and check if has a large prime divisor, before accepting it. A natural question is if the difficulty of discrete log (DLOG) is the same for all curves with the same order and if so it would justify the above practice. We prove that this is essentially true by showing random reducibility of DLOG among isogenous (having the same order) curves. This reduction works for curves with (almost) the same endomorphism rings, but otherwise it is unclear if such a reduction exists. This suggests that in addition to the order, its conductor may have a role. We briefly look at recommended curves and compare "random" type NIST curves and other special curves from this standpoint.

The random self-reducibility for DLOG over finite fields is well known; the non trivial part here is that one must relate non-isomorphic algebraic groups of two isogenous curves. We construct certain Ramanujan graphs with elliptic curves as nodes and use the rapid mixing of random walks. Our proof relies on the Generalized Riemann Hypothesis. This construction yields similar expander graphs over integers modulo a prime.

Joint work with David Jao (Microsoft Research) Stephen Miller (Rutgers)