POLLARD'S RHO ALGORITHM FOR ELLIPTIC CURVES

AARON BLUMENFELD

Abstract. Elliptic curve cryptographic protocols often make use of the inherent hardness of the discrete logarithm problem, which is to solve $kG = P$ for k. There is an abundance of evidence suggesting that elliptic curve cryptography is more secure than the classical case. One reason for this is the best known general-purpose algorithm to solve the elliptic curve discrete logarithm problem is Pollard's Rho algorithm, which has exponential time complexity $O(\sqrt{n})$, where n is the order of the elliptic curve.

In this paper, we explore Pollard's Rho algorithm. In particular, we show that it only requires $O(1)$ space complexity. This is an astronomical improvement over the related Baby-Step Giant-Step algorithm, which requires $O(\sqrt{n})$ time *and* space complexity. We also investigate different methods of defining the sequence of points used in Pollard's Rho algorithm and discuss their effects on efficiency.

References

[1] Washington, Lawrence C., *Elliptic Curves: Number Theory and Cryptography*, Chapman & Hall, Boca Raton, FL, 2nd. Ed., 2008.

[2] Lamb, Nicholas, An Investigation into Pollard's Rho Method for Attacking Elliptic Curve Cryptosystems. 2002.

E-mail address: ablumenf@u.rochester.edu

Date: November 1, 2015.