Speeding up the Pollard's Rho algorithm

Silje Christensen (christensen@umail.ucsb.edu)
Simen Johnsrud (simejo@umail.ucsb.edu)

November 2015

1 Abstract

In order to understand the threat model of elliptical curve cryptographic schemes it is important to have the knowledge of how you can attack it. Pollard's Rho algorithm is one possible way to solve the elliptic curve discrete logarithm problem (ECDLP)[1]. The algorithm was introduced in 1978 [2], and during the past four decades there have been several modifications to the original implementation to reduce the time and storage complexity.

In our paper we aim to give the reader an overview of the Pollard's Rho algorithm in order to understand how we can speed it up. We will start by looking at the basic concepts of it, and then study the existing methods which can be applied to reduce the complexity.

2 References

1. Hankerson, Menezes, Vanstone (2004) "Guide to Elliptic Curve Cryptography". Springer.

2. Pollard, J. M. (1978). "Monte Carlo methods for index computation (mod p)". Mathematics of Computation