Defending against Pohlig-Hellman attacks

Martin Lysoe Sommerseth and Haakon Hoeiland
martin.sommerseth@hotmail.no, haakoho@stud.ntnu.no

October 29, 2015

1 Abstract

The Pohlig-Hellman algorithm is an algorithm that solves the discrete logarithm problem. The algorithm simplifies the problem by solving the elliptic curve discrete logarithm problem (ECDLP) in the prime subgroups of the point $\langle P \rangle$. The difficulty of solving the ECDLP in its prime order subgroups is no harder than solving the ECDLP in $\langle P \rangle$[1][2].

In our paper we will present the Pohlig-Hellman algorithm and its applications. We will discuss its complexity and how to construct the elliptical curves in order to defend against the Pohlig-Hellman attack.

2 References

1. Hankerson, Menezes, Vanstone: "Guide to Elliptic Curve Cryptography", Chapter 4.1.1, 2004, Springer-Verlag New York, Inc.

2. Novotney: "Weak Curves In Elliptic Curve Cryptography", 2010, http://wstein.org/edu/2010/414/projects/novotney.pdf