Ephemeral key recovery using index calculus method

R. Padmavathy *
Department of Computer Science and Engineering
National Institute of Technology
Warangal 506 021, India

Chakravarthy Bhagvati †
Department of Computer and Information Sciences
University of Hyderabad
Hyderabad, India

Abstract

The present study investigates the problem of retrieving the ephemeral keys, which are used in the *Discrete Logarithm Problem* (DLP) based public key cryptosystems. The ephemeral key can be retrieved by solving the mathematical hard problem, namely DLP. The DLP defined over a prime field Z_p^* is considered in the present study. An efficient way of computing the DLP for retrieving the ephemeral key by using a new variant of *Index Calculus Method* (ICM) when the factors of $p-1$ are known and small is proposed. The Pohlig-Hellman is the best known method to solve the DLP on the prime field with factors of $p-1$ are small, while the ICM is an efficient method for a general DLP. The ICM has two steps, such as a pre-computation and an individual logarithm computation. In the pre-computation step, the logarithms of elements of a subset of a group, which is known as a factor base is computed and in the individual logarithm step the DLP is computed with the help of pre-computed logarithms of factor base. Since the ephemeral keys are dynamic and changes for every session, once the logarithms of a subset of a group is known, the DLP for the ephemeral key can be obtained by using the individual logarithm step. Therefore, an efficient way of solving the individual logarithm step is presented based on the newly proposed pre-computation method and the performance is analyzed on a comprehensive set of experiments. From the experimental results, it is observed that the individual logarithm (computation) step outperforms the Pohlig-Hellman method on some special cases. The property of generators of prime field is the main motivation for the current study.

Keywords and phrases : *Discrete logarithm problem, index calculus method, Pohlig-Hellman, ephemeral keys.*

* *E-mail*: r_padma3@rediffmail.com
† *E-mail*: chakcs@uohyd.ernet.in

Journal of Discrete Mathematical Sciences & Cryptography
Vol. 13 (2010), No. 1, pp. 29–43