Parallel Implementation of Pohlig-Hellman to Compute Discrete Logarithms

International Journal of Computer Applications
Foundation of Computer Science (FCS), NY, USA

Volume 166
Number 3

Year of Publication: 2017

Authors:
Aditya Sakre, Amit Gurbani, Pooja Dedwal, J. V. Katti

10.5120/ijca2017913941

Abstract

Almost half of the world is now connected to the Internet and it has become an integral part of our day to day life. The usage of Internet varies from personal communication to high level business transactions. So security of these Internet services is necessary to maintain Confidentiality, Integrity and Availability. To achieve this there were various cryptographic algorithms proposed. But security of these algorithms needs to be verified. The integer factorization problem, the finite field discrete logarithm problem and the elliptic curve discrete logarithm problem are essential mathematical problems that the practical public key cryptographic systems are based on. ElGamal is one of the cryptographic algorithm, based on discrete logarithms. Pohlig-Hellman algorithm is used for computing discrete logarithms. This paper proposes the parallel implementation of Pohlig-Hellman algorithm to observe improvement in execution time as compared to sequential execution. Paper also analyses the effect of key on execution time.

References
1. Mrs. Santoshi Pote and Mrs. Jayashree Katti 2015 “Attacks on Elliptic Curve Cryptography Discrete Logarithm Problem (EC-DLP)”.
2. Lawrence C. Washington university of Maryland “Elliptic Curves Number Theory and Cryptography”.
4. Joppe W.BOS, Alina Dudeanu, Dimitar Jetchev, “Collision bounds for the additive pollard rho algorithm for solving discrete logarithms”.

Index Terms

Computer Science        Algorithms

Keywords

Discrete Logarithm Problem, Pohlig-Hellman, Multithreading.