World Academy of Science, Engineering and Technology
International Journal of Mathematical and Computational Sciences
Vol:14, No:12, 2020

Generalization of Blom Key Predistribution Scheme

Authors : Abbas Cheraghi

Abstract : A key predistribution scheme provides one method to distribute secret ahead of time. Blom's scheme is a symmetric threshold key exchange protocol in cryptography. The scheme was proposed by the Swedish cryptographer Rolf Blom. In this kind of scheme, trusted authority gives each user a secret key and a public identifier, which enables any two users to create independently a shared key for communicating between each other. However, if an attacker can compromise the keys of at least Known numbers of users, he can break the scheme and reconstruct every shared key. In this paper generalized Blom's Scheme by multivariate Lagrange interpolation formula. This scheme is a form of threshold secret sharing scheme. In this new scheme, the amount of information transmitted by the trusted authority is independent of the numbers of users. In addition, this scheme is unconditionally secure against any individual user.

Keywords : key predistribution, blom's scheme, secret sharing, unconditional secure
Conference Title : ICSRD 2020 : International Conference on Scientific Research and Development
Conference Location : Chicago, United States
Conference Dates : December 12-13, 2020