Abstract

Ever since 2-party Diffie-Hellman exchange was first proposed in 1976, there have been efforts to extend its simplicity and elegance to a group setting. Notable solutions have been proposed by Michael Steiner Gene Tsudik Waidner (in 1996) and Recently G.P. Biswas was proposed a contributory group key agreement protocol for generation of multiparty key and compared with other protocol and satisfactory results obtained.

In this paper an m-party DH key distribution for group (improved group DH) was proposed by modifying G.P. Biswas protocol and we argued that our protocol is optimal with respect to most of the aspects of protocol complexity and also it's security discussed.
Reference

- Stefan A. Brands. An Efficient Off-line Electronic Cash System Based On The Representation Problem., CWI (Centre for Mathematics and Computer Science), Amsterdam, The Netherlands, 1993

Index Terms

Computer Science  Cryptology
Key words

Diffie-Hellman technique
DDH problem
key distribution
key exchange operations
secure data transmission