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

- Whit Diffie and Martin Hellman. New Directions In Cryptography. IEEE Transactions on
  system, Proceedings on Advances in cryptology, p.520-528, February 1990, Santa Barbara,
  California, United States
- Edward Zuk, Remarks on "The Design of a Conference Key Distribution System",
  Proceeding of the Workshop on the Theory and Application of Cryptographic Techniques:
  Advances in Cryptology, p.467-468, December 13-16, 1992
  Ottawa Carleton Institute for Computer Science, Carleton University, Ottawa, Ontario, August
  1994.
- Tzonelih Hwang, Cryptosystem for group oriented cryptography, Proceeding of the
  workshop on the theory and application of cryptographic techniques on Advances in cryptology,
  p.352-360, February 1991, Aarhus, Denmark
- M. Burmester and Y. Desmedt. A Secure And Efficient Conference Key Distribution
  System. In I.B. Damgard, editor, Advances in Cryptology- EUROCRYPT '94, Lecture Notes in
- C.P. Schnorr. Efficient Signature Generation By Smart Cards. Journal of Cryptology,
- CORPORATE NIST, The digital signature standard, Communications of the ACM, v.35
  n.7, p.36-40, July 1992 [doi>10.1145/129902.129904]
- 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
- Bruce Schneier, Applied cryptography (2nd ed.): protocols, algorithms, and source code
- Michael Steiner, Gene Tsudik, Michael Waidner, Refinement and extension of encrypted
  [doi>10.1145/206826.206834
- T. Matsumoto, Y. Takashima, H. Imai. A Method Of Generating Secret Data Common To
  Symposium on Security and Privacy, p.176, May 16-18, 1994

Index Terms

Computer Science, Cryptology
Diffie-Hellman Technique Extended to Efficient and Simpler Group Key Distribution Protocol

Key words

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