

Abstract

In this article we present a generalized version of divide and conquer approach for contributory group Diffie-Hellman key exchange (DHKE) scheme. In particular, we devise an efficient way to establish a mutual secret key for multiple participants that uses a quasilinear amount of exponentiations with respect to the number of participants. The correctness of our protocol is proven using mathematical induction. We also compute its complexity in terms of total exponentiations within the protocol, analyze several important computational characteristics, and analyze the security of the protocol against passive attack. Moreover, we provide a comprehensive comparison of our protocol with other existing contributory schemes. Finally, we present an adaptation of our protocol for Megrelishvili group key agreement as a variant of DHKE procedure.

Keywords—divide and conquer approach, contributory group key distribution scheme