Cryptology ePrint Archive: Report 2011/634

Security of Multiple-Key Agreement Protocols and Propose an Enhanced Protocol

Mohammad Sabzinejad Farash and Mahmoud Ahmadian Attari and Majid Bayat1

Abstract: Multiple key agreement protocols produce several session keys instead of one session key. Most of the multiple key agreement protocols do not utilize the hash functions in the signature schemes used for identification. Not using hash function in these protocols causes that the protocols do not satisfy some requirement security properties. In this paper we review the multiple key agreement protocols and perform attacks on some of them. Then we introduce a new multiple key agreement protocol and show that the proposed protocol is more secure than the existent multiple key agreement protocols.

Category / Keywords: cryptographic protocols / agreement protocols, Multiple-key agreement protocols, Signature schemes

Date: received 24 Nov 2011

Contact author: sabzinejad at tmu ac ir

Available formats: PDF | BibTeX Citation

Version: 20111126:040226 (All versions of this report)