Cryptology ePrint Archive: Report 2011/653

An Improved Certificateless Authenticated Key Agreement Protocol

Haomin Yang and Yaoxue Zhang and Yuezhi Zhou

Abstract: Recently, Mokhtarnameh, Ho, Muthuvelu proposed a certificateless key agreement protocol. In this paper, we show that their protocol is insecure against a man-in-the-middle attack which is a severe disaster for a key agreement protocol. In addition, the authors claimed that their scheme provides a binding a long-term public key with a corresponding partial private key. In fact, their protocol does not realize the binding. We propose an improved key agreement protocol based on the protocol proposed by Mokhtarnameh, Ho and Muthuvelu. The improved protocol can resist a man-in-the-middle attack as well as satisfy the desired security properties for key agreement. It truly realizes the one-to-one correspondence between the long-term public key and the partial private key of a user. If there are two different, working long-term public keys for the same identity, the key generation center will be identified as having misbehaved in issuing both corresponding partial private keys.

Category / Keywords: cryptographic protocols / certificateless public key cryptography; key agreement; man-in-the-middle attack;bilinear pairing.

Date: received 3 Dec 2011, last revised 3 Dec 2011

Contact author: yanghm07 at mails tsinghua edu cn

Available formats: PDF | BibTeX Citation

Version: 20111209:204951 (All versions of this report)

Discussion forum: Show discussion | Start new discussion