Cryptology ePrint Archive: Report 2011/249

Breaking a certificateless key agreement protocol withour bilinear pairing

W. Han

Abstract: Certificateless public key cryptography simplifies the complex certificate management in the traditional public key cryptography and resolves the key escrow problem in identity-based cryptography. Many certificateless designated verifier signature protocols using bilinear pairings have been proposed. But the relative computation cost of the pairing is approximately twenty times higher than that of the scalar multiplication over elliptic curve group. Recently, He et al. proposed a certificateless authenticated key agreement protocol without pairings and presented that their protocol is secure in the random oracle model. In this paper, we show that their protocol is insecure against the Type I adversary.

Category / Keywords: public-key cryptography / Certificateless cryptography; Authenticated key agreement; Provable security; Bilinear pairings; Elliptic curve

Publication Info: The paper has not been published.

Date: received 19 May 2011, withdrawn 26 Jul 2011

Contact author: hww_2006 at 163 com

Available formats: (-- withdrawn --)

Version: 20110727:035631 (All versions of this report)