Cryptology ePrint Archive: Report 2011/347

An efficient certificateless authenticated key agreement protocol without bilinear pairings

Debiao He

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 authenticated key agreement 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, several certificateless authenticated key agreement protocols without pairings were proposed to improve the performance. In this paper, we propose a new certificateless authenticated key agreement protocol without pairing. The user in our just needs to compute five scale multiplication to finish the key agreement. We also show the proposed protocol is secure in the random oracle model.

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

Publication Info: The paper has not published

Date: received 20 May 2011, withdrawn 1 Aug 2011

Contact author: hedebiao at 163 com

Available formats: (-- withdrawn --)

Version: 20110801:142304 (All versions of this report)

Discussion forum: Show discussion | Start new discussion

[Cryptology ePrint archive]