Cryptology ePrint Archive: Report 2011/478

An efficient certificateless authenticated key agreement scheme

Debiao He, Sahadeo Padhye, Jianhua Chen

Abstract: Due to avoiding the key escrow problem in the identity-based cryptosystem, certificateless public key cryptosystem (CLPKC) has received a significant attention. As an important part of the CLPKC, the certificateless authenticated key agreement (CLAKA) scheme also received considerable attention. Most CLAKA schemes are built from bilinear mappings on elliptic curves which need costly operations. To improve the performance, several pairing-free CLAKA schemes have been proposed. In this paper we propose a new pairing-free CLAKA scheme. Compared with the related schemes our scheme has better performance. We also show our scheme is provably secure in a very strong security model, i.e. the extended Canetti-Krawczyk (eCK) model.

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

Publication Info: The paper has not published.

Date: received 2 Sep 2011, last revised 17 Dec 2011

Contact author: hedebiao at 163 com