Cryptology ePrint Archive: Report 2011/173

An efficient certificateless short signature scheme from pairings

Debiao He, Jianhua Chen

Abstract: To avoid the inherent key escrow problem in ID-based public key cryptosystem, Al-Riyami and Paterson introduced a new approach called certificateless public key cryptography. Recently, several short certificateless signature schemes are presented to improve the performance. In this paper, we propose an efficient short certificateless signature scheme which is secure against the super adversary. Compared with the related scheme, our scheme has the best performance in both sign algorithm and the verify algorithm.

Category / Keywords: public-key cryptography / Certificateless public key cryptography; Shrot signature; Bilinear pairings; Provable security

Publication Info: The paper has not been published.

Date: received 4 Apr 2011

Contact author: hedebiao at 163 com

Available formats: PDF | BibTeX Citation

Version: 20110405:085821 (All versions of this report)

Discussion forum: Show discussion | Start new discussion

[Cryptology ePrint archive]