Cryptology ePrint Archive: Report 2011/079

Identity-based Digital Signature Scheme Without Bilinear Pairings

He Debiao, Chen Jianhua, Hu Jin

Abstract: Many identity-based digital signature schemes 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. In order to save the running time and the size of the signature, we propose an identity based signature scheme without bilinear pairings. With both the running time and the size of the signature being saved greatly, our scheme is more practical than the previous related schemes for practical application.

Category / Keywords: public-key cryptography / Digital signature, Identity-based cryptography, Bilinear pairings, Elliptic curve

Publication Info: The paper has not been published.

Date: received 16 Feb 2011

Contact author: hedebiao at 163 com