Cryptology ePrint Archive: Report 2011/192

Short and Efficient Certificate-Based Signature

Joseph K. Liu and Feng Bao and Jianying Zhou

Abstract: In this paper, we propose a short and efficient certificate-based signature (CBS) scheme. Certificate-based cryptography proposed by Gentry \cite{Gentry03} combines the merit of traditional public key cryptography (PKI) and identity based cryptography, without use of the costly certificate chain verification process and the removal of key escrow security concern. Under this paradigm, we propose the shortest certificate-based signature scheme in the literature. We require one group element for the signature size and public key respectively. Thus the public information for each user is reduced to just one group element. It is even shorter than the state-of-the-art PKI based signature scheme, which requires one group element for the public key while another group element for the certificate. Our scheme is also very efficient. It just requires one scalar elliptic curve multiplication for the signing stage. Our CBS is particularly useful in power and bandwidth limited environment such as Wireless Cooperative Networks.

Category / Keywords: public-key cryptography /

Publication Info: This is the full version of Networking 2011 (WCNS)

Date: received 14 Apr 2011

Contact author: ksliu at i2r a-star edu sg