Cryptology ePrint Archive: Report 2011/112

An efficient certificateless two-party authenticated key agreement scheme from pairings

Debiao He, Jin Hu

Abstract: Key agreement (KA) allows two or more users to negotiate a secret session key among them over an open network. Authenticated key agreement (AKA) is a KA protocol enhanced to prevent active attacks. AKA can be achieved using a public-key infrastructure (PKI) or identity-based cryptography. However, the former suffers from a heavy certificate management burden while the latter is subject to the so-called key escrow problem. Recently, certificateless cryptography was introduced to mitigate these limitations. We propose an efficient certificateless two-party AKA protocol. Security is proven under the standard computational Diffie-Hellman (CDH) and bilinear Diffie-Hellman (BDH) assumptions. Our protocol is efficient and practical, because it requires only one pairing operation and three scale multiplications by each party. Moreover, the pairing operation and one scale multiplication scale can be pre-computed, then only two scale multiplications are needed to finished the key agreement.

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

Publication Info: The paper has not been published elsewhere.

Date: received 6 Mar 2011, last revised 10 Mar 2011

Contact author: hedebiao at 163 com

Available formats: PDF | BibTeX Citation

Version: 20110310:142118 (All versions of this report)

Discussion forum: Show discussion | Start new discussion

[Cryptology ePrint archive]