Cryptology ePrint Archive: Report 2012/725

Cryptanalysis of an efficient certificateless two-party authenticated key agreement protocol

Qingfeng Cheng

Abstract: Recently, He et al. (Computers and Mathematics with Applications, 2012, 64(6): 1914-1926) proposed a new efficient certificateless two-party authenticated key agreement protocol. They claimed their protocol was provably secure in the extended Canetti-Krawczyk (eCK) model. In this paper, we will show that their protocol is insecure. A type I adversary, who obtains one party's ephemeral private key, can impersonate the party to cheat the other party and compute the shared session key successfully. For overcoming this weakness, we also propose a simple countermeasure.

Category / Keywords: cryptographic protocols / Authentication, Certificateless cryptography, Key agreement, Two-party, Ephemeral key compromise attack, Key replacement attack

Date: received 28 Dec 2012

Contact author: qingfengc2008 at sina com

Available formats: PDF | BibTeX Citation

Version: 20121228:170851 (All versions of this report)

Discussion forum: Show discussion | Start new discussion

[Cryptology ePrint archive]