Cryptology ePrint Archive: Report 2013/006

Cryptanalysis of a pairing-free identity-based authenticated group key agreement protocol for imbalanced mobile networks

Qingfeng Cheng

Abstract: Recently, Isalam and Biswas proposed a new group key agreement (GKA) protocol for imbalanced mobile networks. In this letter, we will show that Isalam et al.'s GKA protocol is not secure.

Category / Keywords: group key agreement, imbalanced mobile networks, ephemeral key compromise attack, perfect forward secrecy

Date: received 6 Jan 2013, last revised 6 Jan 2013

Contact author: qingfengc2008 at sina com