Cryptology ePrint Archive: Report 2013/030

On the security of an identity-based authenticated group key agreement protocol for imbalanced mobile networks

Haiyan Sun

Abstract: Recently, Islam and Biswas proposed a pairing-free identity-based authenticated group key agreement protocol for imbalanced mobile networks. However, in this letter, we point out that this protocol cannot resist passive attack, and cannot provide forward secrecy for joining operation and backward secrecy for leaving operation.

Category / Keywords: passive attack, forward secrecy, backward secrecy

Date: received 21 Jan 2013

Contact author: wenzhong2520 at gmail com