Cryptology ePrint Archive: Report 2011/336

Weakness in an ECC-based AKA Protocol for Wireless Mobile Communications

Debiao He

Abstract: With the rapid progress of wireless mobile communication, the authenticated key agreement protocol has attracted an increasing amount of attention. However, due to the limitations of bandwidth and storage of the mobile devices, most of the existing authenticated key agreement protocols are not suitable for wireless mobile communication. Quite recently, Lo et al. have presented an efficient authenticated key agreement protocol based on elliptic curves cryptography and included their protocol in 3GPP2 specifications. However, in this letter, we show that Lo et al.'s protocol can't resist the off-line password guessing attack. We also propose an efficient countermeasure to withstand the attacks.

Category / Keywords: Authenticated key agreement; Off-line password guessing attack; Wireless mobile communication; 3GPP2

Publication Info: The paper has not been published.

Date: received 21 Jun 2011, last revised 24 Jul 2011

Contact author: hedebiao at 163 com