Cryptology ePrint Archive: Report 2011/411

Comments on a password authentication and update scheme based on elliptic curve cryptography

Debiao He

Abstract: The security of a password authentication and update scheme based on elliptic curve cryptography proposed by Islam et al. [S.K. Hafizul Islam, G.P. Biswas, Design of improved password authentication and update scheme based on elliptic curve cryptography, Mathematical and Computer Modelling (2011), doi:10.1016/j.mcm.2011.07.001] is analyzed. Three kinds of attacks are presented in different scenarios.

Category / Keywords: Password authentication, Elliptic curve cryptography, offline password guessing attack, stolen-verifier attack and privileged insider attack

Publication Info: The paper has not been published.

Date: received 17 Jul 2011, last revised 5 Aug 2011

Contact author: hedebiao at 163 com