

Cryptology ePrint Archive: Report 2011/451

Cryptanalysis and improvement of a biometrics-based multi-server authentication with key agreement scheme

Hakhyun Kim, Woongryul Jeon, Yunho Lee and Dongho Won

Abstract: In 2010, Yoon et al. proposed a robust biometrics- based multi-server authentication with key agreement scheme for smart cards on elliptic curve cryptosystem. In this letter, however, we show that Yoon et al.'s scheme is vulnerable to off-line password guessing attack and propose an improved scheme to prevent the attack.

Category / Keywords: cryptographic protocols /

Date: received 17 Aug 2011

Contact author: hhkim at security re kr

Available formats: [PDF](#) | [BibTeX Citation](#)

Version: 20110820:061138 ([All versions of this report](#))

Discussion forum: [Show discussion](#) | [Start new discussion](#)

[[Cryptology ePrint archive](#)]