Cryptology ePrint Archive: Report 2011/333

Cryptanalysis of a key agreement protocol based on chaotic Hash

Debiao He

Abstract: With the rapid development of theory and application of chaos, more and more researchers are focusing on chaos based cryptosystems. Recently, Guo et al.'s [X. Guo, J. Zhang, Secure group key agreement protocol based on chaotic Hash, Information Sciences 180 (2010) 4069–4074] proposed a secure key agreement protocol based on chaotic Hash. They claimed that their scheme could withstand various attacks. Unfortunately, by giving concrete attacks, we indicate that Guo et al.'s scheme is vulnerable to the off-line password guessing attack. The analysis shows Guo et al.'s scheme is not secure for practical application.

Category / Keywords: cryptographic protocols / Chaos; Hash function; Key agreement; Chebyshev; Password guessing attack

Publication Info: The paper has not published.

Date: received 18 Jun 2011

Contact author: hedebiao at 163 com