

An improved simple user authentication scheme for grid computing*

Cheng-Chi Lee¹

Hsien-Ju Ko^{2,†}

Shun-Der Chen¹

¹*Department of Library and Information Science*

Fu Jen Catholic University

510 Jhongjheng Rd., Sinjhuang City

Taipei County 24205

Taiwan, R.O.C.

²*Department of Photonics and Communication Engineering*

Asia University

No. 500, Lioufeng Road

Wufeng Shiang, Taichung

Taiwan, R.O.C.

Abstract

Recently, Lu proposed a simple user authentication scheme for grid computing. The proposed scheme only requires a one-way hash function and server's private key, which is very simple and efficient. However, the authors will show that their scheme is vulnerable to offline password guessing attack. An attacker can obtain correct passwords of the users by using this attack. To defend this attack, we will propose a simple improved scheme for grid computing. We will show that our scheme for grid computing is simple and efficient in contrast to others.

Keywords: *Elliptic curve cryptosystem, grid computing, security, user authentication*