International Journal of Innovative
Computing, Information and Control
Volume **7**, Number **10**, October **2011**

ICIC International ©2011 ISSN 1349-4198
pp. 5717–5730

A SECURE CONFERENCE KEY PROTOCOL OVER ECC-BASED GREY SYSTEMS

Tzer-Long Chen[1], Yu-Fang Chung[2] and Frank Y. S. Lin[1]

[1]Department of Information Management
National Taiwan University
No. 1, Sec. 4, Roosevelt Road, Taipei 10617, Taiwan
d97725005@ntu.edu.tw; yslin@im.ntu.edu.tw

[2]Department of Electrical Engineering
Tunghai University
No. 181, Sec. 3, Taichung Port Road, Taichung 40704, Taiwan
yfchung@thu.edu.tw

Received June 2010; revised January 2011

Abstract. *In the current environment, there are only a limited number of third-parties that general users can trust in terms of authentication and verification. Often, the self-acclaimed independent third-parties are the parties from where information outflow occurs. While current public key encryption systems have numerous algorithms that have been protecting confidential data for several years, these systems are often met with hardware difficulties for information protection on the Internet and commercial applications. In order to meet the various needs of the environment, often several cryptography modules are combined or merged to achieve the effect of covering each others' deficiencies. This is a very common practice. The proposed method in this article is applicable for preventing information outflow with the introduction of third parties during a bi-party communication, in circumstances where bi-party communication is met with network environment difficulties, and also when the third party is not a trusted controller, or there are no controllers at all. While current systems operate on the back of trusted third-party administrators as is a common security mechanism for managing the public key and confidential data, often even with management, there are still probabilities of insecurity that threaten system security on the whole. To prevent this and also adapt to environment needs, the proposed method combines the grey system theory with the ECC method. This method can verify the credibility of senders' identity when the legitimate third party is no longer trusted, thus preventing malicious third-party intrusions. The concept of this method is based on the well-known Digital Signature Algorithm (DSA) concept from which the Diffie-Hellman Key Agreement mechanism is derived to manage a common conference key in a mutual communication agreement. When the user can communicate mutually between themselves without the need for a third-party intermediary, the solution to intervention and theft of confidential data by third-parties becomes plausible. With flexibility in calculation, one can set his/her access protocol for the modules to confuse malicious users and increase the difficulty of acquiring the keys illegally. In addition, by combining the ECC public key system, with ECC's short and low computational properties, the proposed method improves on the encryption and decryption operation efficiency. This method is thus a system set to establish a secure and efficient conference key system by combining the properties of the ECC public key system with the grey system theory.*

Keywords: Conference key, Elliptic curve cryptosystem, Digital signature algorithm, Grey system

1. **Introduction.** With the current increasing frequency of network intrusions, information security and protection issues have received increasing attention. The degree of