International Journal of Innovative
Computing, Information and Control
Volume **7**, Number **1**, January **2011**

ICIC International ©2011 ISSN 1349-4198
pp. **379–394**

A NOVEL GREY DATA GENERATING TECHNIQUE ON ELLIPTIC CURVE CRYPTOSYSTEMS

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

[1]Department of Information Management
National Taiwan University
d97725005@ntu.edu.tw; yslin@im.ntu.edu.tw

[2]Department of Electrical Engineering
Tunghai University
yfchung@thu.edu.tw

Received September 2009; revised February 2010

Abstract. *In a cryptosystem, when the key is lost, the system will not be able to decrypt information or open encrypted documents; as a result, the entire system ceases to function normally. Therefore, this paper aims to propose a solution to the said problem so that the system can revert back to its normal state. Generally, a good cryptosystem fulfills two basic requirements; they are security and confidentiality. If it is easy to use, it will then become popular. Thus, we would like to propose an easy-handling cryptosystem in this paper, which corresponds to these two requirements in addition to being able to easily retrieve lost keys and restore the system to its normal state. Mainly, we combine the concepts of Elliptic Curve Cryptosystem (ECC) and mathematical Grey Model into an algorithm to illustrate how we can use the Grey Model's mathematical formula to reconstruct and recover the secret key when the system's secret key is lost, so that the disabled system can resume its normal operations. Public key cryptosystems are quite familiar to most; the more popular ones are either RSA-based or ECC-based. Here, we suggest ECC because its security is based on the difficulty of solving Elliptic Curve Discrete Logarithm Problem (ECDLP). It has been proven that ECC provides much greater efficiency with order of magnitude roughly 10 times than RSA-based systems according to the key length of 313 bits in ECC giving the same security level as a key length of 4096 bits in RSA. The basic attack on the Internet involves finding or cracking the secret key. But in ECC, an attacker has to derive the secret key from the corresponding public key and therefore he or she inevitably has to face the ECDLP, which is an extremely difficult task. Hence, it is extremely difficult for an attacker to obtain the secret key in our proposed method. On the other hand, the Grey Model can give us a hand on guarding against confidentiality-related security problem. Basically, we make use of a mathematical array hierarchy to calculate and further to reconstruct the hierarchy's original key, regarded as a secret key here. When the secret key is lost, we can retrieve the original secret key by using its original mathematical array through the derivation of a mathematical formula of the Grey Model. Having the Grey Model, we can avoid the confidentiality security problem due to the different settings for the levels and rounding off of decimals. Therefore, even if the array in the bottom level gets hacked, it is still very difficult to derive the original array from the bottom. In fact, it is very difficult to crack anything mathematically, and the characteristics of the confidentiality can be improved. At the same time, this increases the method's confidentiality, making the system more secure.*

Keywords: Public key cryptosystem, Elliptic curve cryptosystem, Data generation, Grey model, ECDLP

1. **Introduction.** In a cryptosystem, when the key is lost, it will be a disaster. Without the secret key, the system will not be able to decrypt information or open encrypted documents; as a result the entire system ceases to function normally. Therefore, how