International Journal of Innovative Computing, Information and Control
Volume **6**, Number **2**, February **2010**

ICIC International ©2010 ISSN 1349-4198
pp. 501–508

A NOVEL METHOD OF GREY DATA GENERATING TECHNIQUES IN CRYPTOSYSTEM

Victor R. L. Shen[1], Yu-Fang Chung[2] and Tzer-Shyong Chen[3]

[1]Department of Computer Science and Information Engineering
Graduate Institute of Electrical Engineering
National Taipei University
151, University Rd., Sansia, Taipei County 237, Taiwan
rlshen@mail.ntpu.edu.tw

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

[3]Department of Information Management
Tunghai University, Taiwan
arden@thu.edu.tw

Received August 2008; revised December 2008

Abstract. *This study integrates the grey data generating techniques used in grey system theory with a hot and new cryptosystem that is believed would make new breakthroughs in information security. The concepts of lock generation and single-double replacement ladder are applied in our study to create a new cryptosystem. In this paper we are presenting the grey system theory, our proposed approach to creating the new cryptosystem, the cryptographic algorithms for our cryptosystem, and an illustrative example to prove its feasibility.*

Keywords: Grey system theory, Grey generation, Encryption system, Decryption system

1. **Introduction.** The academic article entitled “Extension Set and Mutual Exclusion Problems” [1] was published by Professor Cai, a leading Chinese scholar, in 1983. Further studies [2-4] were conducted in 1984 by the same. Another scholar, Professor Deng, published academic articles relating to grey system theory [7] in 1982. Further studies [8] were initiated by the same in 1989 and were almost completed by 1994. On the basis of references [7,8], solutions to problems can be found.

According to grey system theory, using the grey data generating methods [10,17], a reasonable rule set can be developed from a set of disordered data. The rule set can be applied in analyzing, predicting, and controlling the system states. This is considered to be one of the basic applications of grey system theory. The grey system theory also contains important and valuable encryption and decryption methods. This study attempts to integrate grey data generating techniques with a cryptosystem that has lock generation and a sum-difference mixed ladder. The ladder is equivalent to a set of numerical data patterns.

The rest of this paper is ordered into five sections, namely, Section 2, 3, 4, 5, and 6. Section 2 presents the basic definitions in grey system theory. Section 3 introduces the required lock generation and ladder generation in our approach. Section 4 describes a cryptosystem with lock generation and single-double replacement ladder, which contains an encryption algorithm and a decryption algorithm. Section 5 presents an illustrative