International Journal of Innovative Computing, Information and Control
Volume **6**, Number **12**, December **2010**

ICIC International ©2010 ISSN 1349-4198
pp. 5311–5320

A BATCH VERIFYING AND DETECTING THE ILLEGAL SIGNATURES

Chun-Ta Li[1], Min-Shiang Hwang[2,*] and Shih-Ming Chen[3]

[1]Department of Information Management
Tainan University of Technology
529 Jhong Jheng Road, Yongkang, Tainan 710, Taiwan
th0040@mail.tut.edu.tw

[2]Department of Management Information Systems
National Chung Hsing University
250 Kuo Kuang Road, Taichung 402, Taiwan
*Corresponding author: mshwang@nchu.edu.tw

[3]Department of Information Management
Chaoyang University of Technology
168 Jifong E. Road, Taichung County 413, Taiwan

Received July 2009; revised December 2009

Abstract. *The concept of batch verifying multiple RSA digital signatures is to find a method that multiple digital signatures can be verified simultaneously in only one exponential operation time. In this article, we proposed a new batch verifying multiple RSA digital signatures scheme. The main contribution of the proposed scheme is that it can easily discover where the signature-verification fault is located without re-verifying all individual signatures separately.*

Keywords: Digital signature, Information security, Multiple signatures, PKI, RSA

1. **Introduction.** In 1978, Rivest, Shamir and Adleman proposed a famous asymmetric cryptosystem named RSA [26] which included four main characteristics: user authentication, confidentiality, integrity, and non-repudiation. It can protect the transaction information which can be safely transmitted and avoid the problems of tampering or usurped the information over the network [12, 13, 14, 15]. In addition, it also solved the requirement of user authentication and communication security on networking environments [16, 17, 18, 19, 20, 21, 23, 24].

RSA utilized two different keys to perform encryption and decryption, the public key (e) and the private key (d), respectively. In RSA signature mechanism, both the signer and receiver have the private key and public key of itself own [6, 7, 11, 16, 17, 27, 28, 29]. First of all, the signer used personal private key to sign documents M_i (where $i = 1$ to t) and generated t signatures when the signing process is completed. Then, the signer transmitted t documents and signatures S_i (where $i = 1$ to t and $S_i = M_i^d$) to receiver. After receiving these documents and signatures, the receiver used signer's public key to verify each of these t signatures one by one and checks whether $M_i \overset{?}{=} S_i^e$ holds or not. During authentication and verification phase, it will reduce the computer host's processing ability because it needs to consume a large amount of exponential computation time. Therefore, the concept of batch verifying multiple RSA digital signatures is to find a method that can efficiently improve the performance of verifying multiple RSA digital signatures.