International Journal of Innovative Computing, Information and Control
Volume **5**, Number **11(A)**, November **2009**

ICIC International ©2009 ISSN 1349-4198
pp. 3911–3922

AN EFFICIENT AND PROVABLY SECURE ID-BASED SIGNATURE SCHEME WITH BATCH VERIFICATIONS

Yuh-Min Tseng, Tsu-Yang Wu and Jui-Di Wu

Department of Mathematics
National Changhua University of Education
Jin-De Campus, Chang-Hua City 500, Taiwan
{ ymtseng; d94211001 }@cc.ncue.edu.tw; oooready@gmail.com

Received June 2008; revised November 2008

Abstract. *A secure signature scheme with providing variant batch verifications extremely improves the verification performance for many cooperative and distributed applications. The identity (ID)-based public key system can simplify certificate management as compared to certificated-based public key systems. With the advent of the ID-based public key system using bilinear pairings defined on elliptic curves, many ID-based signature schemes have been proposed. Recently, Cha and Cheon proposed a new ID-based signature scheme which is more efficient than the previously proposed schemes, but their scheme does not offer batch verifications for multiple signatures because their scheme suffers from forgery attacks for batch verifications. To repair this drawback, Yoon et al. proposed a secure ID-based signature scheme with batch verifications. However, Yoon et al.'s scheme requires more computational time than Cha and Cheon's scheme. In this paper, we propose an efficient and provably secure ID-based signature scheme supporting variant kinds of batch verifications. In the random oracle model and under the computational Diffie-Hellman assumption, we show that our scheme is secure against existential forgery attacks under various kinds of batch verifications. According to performance analysis, our scheme with batch verifications has the best performance as compared to the previously proposed schemes.*

Keywords: Security, Bilinear pairings, ID-based, Signature, Batch verification

1. **Introduction.** A signature scheme is one of the important primitives in modern cryptography. A signature scheme is an important mechanism for providing both identity and message authentications [9,10,23,24,33]. For improving verification performance of many cooperative and distributed applications [11,18,34,35], a signature scheme with the ability to verify multiple signatures simultaneously is called the signature scheme with batch verifications. A secure signature scheme with supporting variant batch verifications extremely decreases the verification time of authentications. In the past, based on the certificate-based public key systems, many various kinds of multi-signature schemes with batch verifications have been studied [3,4,20,22,26-28].

Shamir [31] firstly introduced the idea of ID-based public key system to simplify key management of the certificated-based public key system. The security of Shamir's ID-based system is based on the factorization problem, so the disadvantage of this ID-based system is that the user's secret key has to be generated by one specific key generator center. In 2001, Boneh and Franklin [5,6] proposed an ID-based encryption scheme using bilinear maps (pairings) defined on elliptic curves. The security of this new ID-based system is based on the discrete logarithm problem. In this case, the user's secret key can be generated by several sub-centers using a threshold scheme. With the advent of bilinear pairings defined on elliptic curves, many ID-based cryptographic schemes [1,12-16,32,36]