International Journal of Innovative
Computing, Information and Control
Volume **7**, Number **6**, June **2011**

ICIC International ©2011 ISSN 1349-4198
pp. 3295–3301

AN IDENTITY-BASED CRYPTOSYSTEM FOR ENCRYPTING LONG MESSAGES

Jiqiang Liu[1], Sheng Zhong[2,*], Lei Han[1] and Haifan Yao[2]

[1]Department of Computer and Information Technology
Beijing Jiaotong University
No. 3, Shangyuan Residence, Haidian District, Beijing 100044, P. R. China

[2]Department of Computer Science and Engineering
University at Buffalo
Amherst NY 14260, USA
*Corresponding author: szhong@buffalo.edu

Received November 2009; revised February 2010

Abstract. *Traditionally, when we encrypt long messages using a public key cryptosystem, we need an additional symmetric key cryptosystem to encrypt the message first. Then, the corresponding symmetric key is encrypted using the public key cryptosystem. To eliminate this requirement, public key cryptosystems for encrypting long messages have been designed. However, none of the existing public key cryptosystems for long messages is identity-based. In this paper, we give the first identity-based cryptosystem for encrypting long messages. Our cryptosystem is highly efficient in that it only needs 1 bilinear map operation for encrypting a long message. Furthermore, we show that computing any part of the plaintext message encrypted using our cryptosystem is as hard as breaking Boneh and Franklin's standard identity-based cryptosystem, even if the adversary knows all other parts of the message. We also extend our work to achieve chosen ciphertext security.*

Keywords: Cryptosystem, Identity-based, Long messages, Encryption, Public key

1. **Introduction.** Traditionally, when we need to encrypt long messages using a public key cryptosystem, we need to use an additional symmetric key cryptosystem: First, we encrypt the message using the symmetric key cryptosystem. Then, the symmetric key is encrypted using the public key cryptosystem. However, the need for the additional cryptosystem is clearly undesirable [1]. To eliminate this requirement, public key cryptosystems for encrypting long messages have been designed. Hwang, Chang and Hwang [1] introduced an ElGamal-like asymmetric cryptosystem for encrypting long messages (see [2] for details about ElGamal cryptosystem). Zhong [3] improved its efficiency and gave a formal proof of security. However, as far as we know, none of the existing public key cryptosystems for long messages is identity-based.

Identity-Based cryptosystem is a type of asymmetric cryptosystems that allows us to use an entity's identity as its public key. It is first presented to simplify management in a network systems by Shamir [4], but Shamir did not give an efficient scheme. Based on bilinear maps between groups, Boneh and Franklin proposed the first efficient and secure method for Identity-Based Encryption (IBE) [5], and Waters presented an efficient IBE scheme that is fully secure without random oracles [6]. Some Identity-Based Signature schemes were also proposed based on Bilinear Pairing recently [7-9]. Since then, Identity-Based cryptosystem was widely applied in many areas, such as key management [10], mutual authentication [11], etc. However, bilinear map operations are pretty expensive in computation [12]. It would be impractical if we directly used the Boneh-Franklin