International Journal of Innovative Computing, Information and Control
Volume **5**, Number **10(A)**, October **2009**
ICIC International ©2009 ISSN 1349-4198
pp. 3025–3030

ATTACK AND IMPROVE THE ZHAO-LIU AUTHENTICATED ENCRYPTION SCHEME

Ting-Yi Chang[1] and Mao-Lun Chiang[2]

[1]Graduate Institute of e-Learning
National Changhua University of Education
No.1, Jin-De Road, Changhua City, Taiwan
tychang@cc.ncue.edu.tw

[2]Department of Information Engineering and Informatics
Tzu Chi College of Technology
880, Sec. 2, Chien-Kuo Road, 970 Hualien, Taiwan

Received May 2008; revised October 2008

Abstract. *In this paper, we show that the Zhao-Liu authenticated encryption scheme is vulnerable to a universal forgery attack. This one malicious verifier is able to use previous signatures to forge the signer's authenticated encryption signature on any message. Two simple methods are presented to withstand this attack. One method also additionally provides the convertible property in the Zhao-Liu authenticated encryption scheme, which allows the verifier to convert the signature into an ordinary one. The converted signature can be verified by anyone, without revealing his/her secret key.*

Keywords: Authenticated encryption, Digital signature, Elliptic curve cryptosystem, Universal forgery attack

1. **Introduction.** Paper work is rapidly being replaced, as e-mail, electronic commerce and electronic money become more widespread. Security is an important issue for such an environment. Two basic requirements exist for network security: secrecy and authentication [1, 7, 17]. Secrecy protects sensitive data against eavesdropping and modification. Authentication prevents forgery and unauthorized network access.

An *Authenticated Encryption Scheme* (AES) allows a signer to generate an authenticated ciphertext such that only the designed verifier has the ability to decrypt the signed message and verify its corresponding signature. Nyberg and Ruppel [16] first proposed an AES, based on the discrete logarithm problem. Later, to reduce the computation and communication cost, some schemes [10, 13, 25] were proposed. For distributing the power of a single signing, the multi-user version of AES was motivated by the need that arises in organizations to have a group of members who agree on a message before signing [3, 4, 6, 8, 9, 22].

Unlike traditional digital signature schemes such as RSA [18] and DSA [15], where one signer is allowed to generate a signature for anyone to verify. Because only the designed verifier has the ability to decrypt the signed message and verifies its corresponding signature in AES, the signer can easily repudiate the signature that he/she previously generated. In other words, a third-party cannot play an impartial role to judge the disputable signature, unless the verifier reveals his/her secret key to the third-party. After revealing the verifier's secret key, the third-party acts as the verifier to judge the signature. However, this method is impractical in the real world, because the secret key is revealed.