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

ICIC International ©2009 ISSN 1349-4198
pp. **3861–3873**

AN EFFICIENT FAIR ELECTRONIC PAYMENT SYSTEM BASED UPON NON-SIGNATURE AUTHENTICATED ENCRYPTION SCHEME

Jen-Ho Yang[1] and Chin-Chen Chang[2]

[1]Department of Information and Electronic Commerce
Kainan University
Luzhu, Taoyuan County, 33857, Taiwan
jenhoyang@mail.knu.edu.tw

[2]Department of Computer Science and Information Engineering
Feng Chia University
Taichung, 40724, Taiwan
ccc@cs.ccu.edu.tw

Received June 2008; revised November 2008

Abstract. *In this paper, we first propose a non-signature authenticated encryption scheme, which accomplishes the message authentication, confidentiality, and integrity for communications on an open channel. Compared with the related works, the proposed scheme does not require constructing the digital signature so that the computation costs can be reduced. Based upon the non-signature authenticated encryption scheme, we further propose a fair electronic payment system such that the payment information can be securely transmitted on Internet. Moreover, the proposed electronic payment system can solve the synchronization problem between the payer and the merchant. Therefore, the transaction fairness of the payer and the merchant can be efficiently accomplished in off-line environments. According to the above-mentioned advantages, the proposed electronic payment system provides an efficient and practical payment tool for electronic transactions.*

Keywords: Electronic payment systems, Authenticated encryption schemes, Elliptic curve cryptosystems

1. **Introduction.** With the development of computer technology, more and more traditional transactions are replaced by electronic transactions to make human life more convenient. In electronic transactions, payers can accomplish the transactions by computers or mobile devices on Internet anytime and anywhere. On the other hand, the merchant can eliminate the cost of maintaining a physical store. Thus, the electronic transaction becomes more and more popular such that it changes people's purchasing behaviors today. For example, people can buy an electronic image through the Internet. In this case, they need to employ some useful image coding, watermarking, and noise reduction schemes [4, 11, 26] to accomplish the electronic transactions. The most important component of electronic transactions is the electronic payment. Generally, the electronic payment systems can be categorized into three types: electronic credit card, electronic cash, and electronic check [18].

The above-mentioned payment systems have different properties and requirements, and each of them has its own advantages and disadvantages for different applications. In electronic cash systems, the payer has to pay the bill before he receives the goods from the merchant. In electronic credit card and electronic check systems, the merchant has to offer the goods before he gets the money from the payer. From the above descriptions, these payment systems have the common problem, which is the synchronization problem