An Efficient Electronic Cash Scheme with Multiple Banks Using Group Signature

Article *in* International journal of innovative computing, information & control: IJICIC · July 2012

CITATIONS
2

READS
54

4 authors, including:

Chun-I Fan
National Sun Yat-sen University
146 PUBLICATIONS **1,230** CITATIONS
SEE PROFILE

Wen-shenq Juang
National Kaohsiung First University of Science and Technology
52 PUBLICATIONS **1,096** CITATIONS
SEE PROFILE

International Journal of Innovative Computing, Information and Control
Volume **8**, Number **7(A)**, July **2012**

ICIC International ©2012 ISSN 1349-4198
pp. **4469–4482**

AN EFFICIENT ELECTRONIC CASH SCHEME WITH MULTIPLE BANKS USING GROUP SIGNATURE

Ming-Te Chen[1], Chun-I Fan[1,*], Wen-Shenq Juang[2] and Yi-Chun Yeh[2]

[1]Department of Computer Science and Engineering
National Sun Yat-sen University
No. 70, Lienhai Road, Kaohsiung 80424, Taiwan
ecsemtchen@gmail.com; *Corresponding author: cifan@faculty.nsysu.edu.tw

[2]Department of Information Management
National Kaohsiung First University of Science and Technology
No. 2, Jhuoyue Road, Nanzih, Kaohsiung 811, Taiwan
wsjuang@ccms.nkfust.edu.tw; u9724830@nkfust.edu.tw

Received March 2011; revised July 2011

Abstract. *In 2008, an electronic cash scheme with multiple banks based on group signatures was proposed by Wang et al. They adopted a group blind signature scheme based on bilinear pairings to generate the electronic cash and it can be verified by the bilinear pairings operation. However, we find some security problems in their approach. By the way, the cost of communication and computation in their scheme can be improved further. Hence, we propose an efficient and secure e-cash scheme from bilinear pairings with multiple banks. Not only can our approach solve all the security problems in Wang et al.'s scheme but also offer lower computation and communication cost.*
Keywords: Blind group signature, Bilinear pairing, E-cash, Multiple banks

1. **Introduction.** With the flourishing development of the Internet technology, the phenomenon of people performing financial transactions via the Internet is gradually popular in the e-commerce environment. This situation is called electronic payment service [10, 14, 15, 20]. Because of the insecure Internet environment, customers will face any kinds of security threats when performing electronic payment service with banks. A malicious attacker can carry out eavesdropping, tampering, stealing or performing other illegal acts on the customers' transaction data when they are doing this service with banks. Then it will result in that consumers' sensitive privacy information (such as customers' identity and password of financial cards) is stolen and she/he can impersonate one of customers to withdraw e-cash from banks. In order to prevent these threats happening, the electronic payment services must consider the security requirements including the authentication of customers, confidentiality of e-cash, and non-repudiation of e-cash.

When a customer pays her/his e-cash to a merchant, it should make that the merchant and the bank do not know who pays the e-cash anonymously. By the way, the merchant should be able to check the e-cash fast by using efficient e-cash verification method. In 1983, the first electronic cash (e-cash) was proposed by Chuam [5] and it adopted the blind signature as the building primitive.

In the meanwhile, there were some signature schemes [2, 3, 23, 25] and some electronic cash payment mechanisms [16, 21, 24] also proposed. For the growing emphasis on the privacy protection of customers in electronic payment systems, the blind signature seems to be a perfect solution. Nevertheless, the blind signature cannot offer the fully anonymity