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

ICIC International ©2009 ISSN 1349-4198
pp. **3887–3900**

FAST RANDOMIZATION SCHEMES FOR CHAUM BLIND SIGNATURES

Chun-I Fan[1], Chih-I Wang[2] and Wei-Zhe Sun[1]

[1]Department of Computer Science and Engineering
National Sun Yat-sen University
70, Lienhai Rd., Kaohsiung 80424, Taiwan
cifan@faculty.nsysu.edu.tw

[2]Department of Information Management
Fooyin University
151, Chinhsueh Rd., Ta-liao, Kaohsiung 83102, Taiwan

Received June 2008; revised November 2008

Abstract. *Chaum's blind signature scheme is the first and well-known technique to achieve the unlinkability between the blind signatures generated by the signer and the corresponding signatures shown for verification by users. Due to the unlinkability property, the technique has been applied to untraceable electronic cash and anonymous electronic voting systems to protect the privacy of users. However, it does not meet the randomization property that is a prerequisite of modern blind signatures for reducing the threat of coercion or bribe against the security of anonymous electronic voting systems based on blind signatures. This manuscript presents a quite efficient randomization solution for Chaum's blind signatures. Compared with Chaum's scheme, the computation cost is only increased by 0.7% in the proposed randomized Chaum blind signature scheme.*
Keywords: Blind signatures, Electronic voting, Electronic cash, Information security, Cryptology

1. **Introduction.** In a digital signature scheme, the signature is the proof of the signer, and no one else can deliberately sign the message. This property is usually referred to as the *unforgeability* property. Based on the RSA signatures [36], Chaum proposed the first blind signature scheme in 1982 [9] to achieve the unlinkability property. Two parties, a signer and a group of users, participate in a blind signature protocol. It is briefly described below. A user blinds a message chosen by herself/himself, and then submits the blinded message to the signer to request the signature on the blinded message. The signer signs the blinded message, and sends the signing result, called the blind signature, back to the user. Finally, the user unblinds the blind signature to obtain the signer's signature on her/his chosen message. The signer's signature on the message can be verified by checking if the corresponding public verification formula with the signature-message pair as parameter is true. In a blind signature scheme, it is information-theoretically impossible for the signer to link a signature shown for verification to the instance of the signing protocol which produces the corresponding blind signature. This is the *unlinkability* property [9, 23, 32, 33]. Due to the unlinkability and unforgeability properties, blind signatures have been widely used in many advanced services where anonymity is indispensable such as anonymous electronic voting [6, 19, 21, 22, 25, 28, 29] and untraceable electronic cash systems [5, 10, 14, 23, 27].

In a blind signature scheme, Ferguson [23] suggested that the signer had better inject one or more randomization factors into the message on which it is about to sign such