International Journal of Innovative
Computing, Information and Control
Volume **7**, Number **10**, October **2011**

 ISSN 1349-4198
pp. 6001–6018

NEARLY OPTIMAL RANDOMIZED BLIND SIGNATURE SCHEME BASED ON MODULAR MULTIPLICATIVE GROUP OVER INTEGERS

Chun-I Fan* and Wei-Zhe Sun

Department of Computer Science and Engineering
National Sun Yat-sen University
No. 70, Lienhai Rd., Kaohsiung 80424, Taiwan
*Corresponding author: cifan@faculty.nsysu.edu.tw

Received May 2009; revised March 2010

Abstract. *Due to the unforgeability and unlinkability properties, blind signatures are the underlying key techniques of untraceable electronic cash systems and anonymous electronic voting protocols. This manuscript will present an extremely efficient randomized blind signature scheme that is especially suitable for the environments where the computation capabilities of users are limited, like mobile commerce and smart-card transactions. Not only does the signer perform merely one modular exponentiation computation, but also the proposed scheme can be demonstrated as being nearly optimal in the computation and communication cost of each user among the randomized blind signature schemes based on a finite commutative group over integers with modular multiplication as the operator, such as ElGamal-like, Rabin-like or RSA-like randomized blind signature schemes. Furthermore, we formally define the unlinkability, the unforgeability and the randomization properties of the proposed scheme and provide formal proofs for these properties under the random oracle model.*

Keywords: Blind signatures, Electronic voting, Electronic commerce, Security and privacy, Cryptology

1. **Introduction.** The concept of blind signatures was first introduced by Chaum [6] to prevent digital signatures from being forged and protect the privacy of users. Based on the RSA cryptosystem [41], Chaum proposed a blind signature scheme to achieve the unlinkability property [6]. By means of the techniques of blind signatures, an untraceable electronic cash system was proposed in [7]. Based on the RSA cryptosystem, Ferguson [22] introduced another blind signature scheme tailored for his untraceable electronic cash system. In [4], the authors proposed a blind signature scheme based on the Discrete Logarithm Problem, and it is derived from a variation of DSA [32]. The authors of [4] also presented a blind signature scheme based on Nyberg-Rueppel signature scheme [33]. Based on Okamoto's protocol of [34] and Schnorr's protocol of [42], a blind signature scheme was proposed in [36]. The authors of [36] presented another blind signature scheme based on Okamoto's protocol [34] and Guillou-Quisquater protocol [24]. In 1997, based on the Square Root Problem [40], two blind signature schemes are proposed in [37]. In all of the above schemes [4, 6, 22, 36, 37], it is necessary for a user to perform a large number of computations to obtain and verify a signature.

In general, two kinds of roles, a signer and a group of users, participate in a blind signature protocol. A user blinds a message by performing an encryption-like process (or a blinding process) on the message, and then submits the blinded message to the signer to request the signer's signature on it. The signer signs on the blinded message by using its signing function, and then sends the signed result, called the blind signature, back to the user. Finally, the user unblinds the blind signature to obtain the signer's signature on the