International Journal of Innovative Computing, Information and Control
Volume **7**, Number **9**, September **2011**

ICIC International ©2011 ISSN 1349-4198
pp. 5403–5416

A BLIND SIGNATURE BASED ON DISCRETE LOGARITHM PROBLEM

Victor R. L. Shen[1], Yu Fang Chung[2], Tzer Shyong Chen[3] and Yu An Lin[4]

[1]Department of Computer Science and Information Engineering
[4]Graduate Institute of Electrical Engineering
National Taipei University
No. 151, University Rd., San Shia District, New Taipei City 23741, Taiwan
rlshen@mail.ntpu.edu.tw

[2]Department of Electrical Engineering
[3]Department of Information Management
Tunghai University
No. 181, Section 3, Taichung Port Rd., Taichung City 40704, Taiwan
{ yfchung; arden }@thu.edu.tw

Received May 2010; revised September 2010

Abstract. *The concept of a blind signature scheme deals with the request that the signer should sign on a blind message. The characteristic of blind signatures is that the requester enables to derive the signature but the signer disables to link a pair of signatures when the requester releases the signature pair in public. This study proposes a new blind signature scheme based on the discrete logarithm problem and the generalized ElGamal-type digital signature scheme by Harn. With high security, the proposed blind signature scheme meets the requirements like correctness, blindness, unforgeability and untraceability.*

Keywords: Blind signature, Digital signature, Discrete logarithm problem

1. Introduction.

Because the digital signature provides authentication, non-repudiation, data integrity and unforgeability within the world of modern cryptography, it has become a very important research topic [2]. Especially in the large network system, key distributions, authentications and electronic commerce can utilize the digital signature. The blind signature is a variant of the digital signature. In 1983, Dr. D. Chaum first proposed the concept of the blind signature and devised a scheme based on the RSA algorithm [6,8,26,34]. The blind signature can protect people's privacy within a network, especially in an electronic cash payment system [7] or electronic voting system [10]. In the digital signature scheme, there are two participants, namely, the signer and the verifier. The signer first uses a private key to sign a message and then sends this signature to the verifier. After the verifier receives the signature, he/she can use a public key to verify the legitimacy of the signature. In the blind signature scheme, there are three participants, namely, the requester, the signer and the verifier. First, the requester blinds the message and sends the blind message to the signer. After receiving the blind message, the signer can use a private key to sign it and send the blind signature back to the requester. Once the requester receives it, he/she "unblinds" the blind signature to obtain the signature and sends it to the verifier. After the verifier receives the signature, he/she can use a public key to verify the legitimacy of the signature.

The main differences between the digital signature and the blind signature are shown as follows [6,8].