A NEW MESSAGE-RECOVERY-COMBINED FAIR BLIND SIGNATURE SCHEME WITH PROVABLE SECURITY USING SELF-CERTIFIED PAIRING-BASED CRYPTOSYSTEM

WOEI-JIUNN TSAUR\textsuperscript{1} AND CHIH-HUNG WANG\textsuperscript{2}
\textsuperscript{1}Department of Information Management
Da-Yeh University
No. 168, University Rd., Dacun, Changhua 51591, Taiwan
wjtsaur@yahoo.com.tw
\textsuperscript{2}Department of Computer Science and Information Engineering
National Chiayi University
No. 300, Syuefu Rd., Chiayi City 60004, Taiwan
wangch@mail.nchu.edu.tw

Received October 2010; revised February 2011

ABSTRACT. The fair blind signature scheme indeed plays significant roles in a wide variety of e-commerce and network applications; for example, it can withstand the misapplication of financial crime in electronic cash payment systems. In this paper, we propose a new fair blind signature scheme with message recovery using the self-certified pairing-based public key cryptosystem. Preserving the merits inherent in the pairing-based cryptosystem, it can possess fewer bits to achieve the higher security level. In addition, our new scheme has the advantage that the authentication of the public key can be accomplished with the verification of the fair blind signature in a logically single step due to the use of the self-certified public key cryptosystem. Furthermore, the fairness of blind signature with message recovery can be actually achieved in our proposed scheme. Based on the proposed security proofs and performance evaluation, we affirm that we not only improve the efficiency of the previously proposed schemes, but also achieve the essential properties of blind signature with provable security.

Keywords: Fair blind signature, Provable security, Pairing-based public key cryptosystem, Self-certified public key cryptosystem, Electronic payment system

1. Introduction. The blind signature scheme, first proposed by Chaum [1] in 1983, is a nice technique that allows achieving the properties of unlinkability and anonymity to protect users’ privacy in secure electronic voting and electronic payment systems [2-4]. With the characteristic of the blind signature scheme, a sender can obtain a signature on a message from a signer, but the signer knows nothing about the content of the message, such that the signer cannot link the signature and sender. This kind of property used in the untraceable cash can provide a useful protection of users’ payment privacy; e.g., when an account holder takes e-coins from the bank, the bank knows nothing about what he bought and when he used these e-coins. Contrarily, the credit card payment cannot have this feature, because the card issuer will get a complete purchase notification when the card holder pays by credit. Another application is the e-voting scheme. Since the vote is blindly signed by the trustee, the frauds are preventable and the voter’s selection can be hidden from the vote counting center. Unfortunately, this kind of characteristic may be used to pervert the ability of the scheme, such as black-mailing or money laundering. That is, the blind signature can successfully prevent from linking the withdrawal and the actual