Computers and Electrical Engineering 35 (2009) 757–763

Contents lists available at ScienceDirect

Computers and Electrical Engineering

journal homepage: www.elsevier.com/locate/compeleceng

# An on-line electronic check system with mutual authentication

Chin-Chen Chang, Shih-Chang Chang, Jung-San Lee *

*Department of Information Engineering and Computer Science, Feng Chia University, 100 Wenhwa Rd., Seatwen, Taichung 40724, Taiwan, ROC*

ARTICLE INFO

*Article history:*
Received 6 August 2007
Received in revised form 18 October 2008
Accepted 6 February 2009
Available online 21 March 2009

*Keywords:*
E-check
Mutual authentication
One-way hash function
Blind signature
RSA cryptosystems

ABSTRACT

Electronic check (e-check) is an important component of electronic commerce. It was first proposed by Chaum in 1988. Till now, engineers have provided many improvements to enhance the security and functionality of the e-check system. The face value of a check and the identification of a payee, however, have to be determined previously in these improved versions. This results in the inflexibility of the system. In this paper, we aim to propose a novel e-check mechanism which allows a payer attaching the face value and the information of a payee to an e-check when dealing with a transaction. The security of this novel system is based on several cryptographic techniques including the secure one-way hash function, blind signature, and RSA cryptosystems.



## 1. Introduction

With rapid development of network technologies, an electronic payment system has deeply involved in people's daily lives. Generally, the electronic payment system can be categorized into three types: on-line credit card payment, electronic cash (e-cash), and electronic check (e-check) [5,8,15]. Among them, an on-line credit card payment system is the most popular one since it always is acceptable while we travel around the world and use it to deal a transaction. However, the amount limitation of the credit card often makes the payment inflexible while a large sum of money is involved in a transaction. Furthermore, the loss of the credit card may lead to the illegal usage of it. On the other hand, an e-cash payment system possesses the advantages including anonymity and low cost. Hence, it is suitable for micro-payment in the electronic commerce. Unfortunately, it suffers from the weaknesses as an electronic credit card payment does. In particular, anyone who can obtain the e-cash is able to use it to deal with a transaction since there is no personal information attached to the e-cash. Therefore, the loss of the e-cash will cause more serious problem than that of the credit card does.

An e-check system is a new commerce service which makes it possible for a payer in a remote site to deal a transaction through networks [3,4]. There exist three main parties involved in a typical electronic check system: a trusted bank, the payer, and the payees. If a payer wants to join an e-check system, he has to register at a trust bank in advance. The trusted bank takes the responsibility for issuing e-checks for the payer. Then the payer can pay for a transaction using the e-check with decided face value and payee's identification information through network.

The concept of electronic check system was first introduced by Chaum in 1988 [4]. Chaum's scheme, however, requires heavy computation overheads in constructing e-checks. In 1989, Chaum proposed an off-line e-check system to overcome the drawbacks of first scheme [3]. Nevertheless, these two methods do not allow a payer to determine the face value of the e-check and the identification of the payee on the nail while dealing a transaction [3,4]. This results in the inflexibility of the electronic payment system. In 2005, Chen [5] proposed an efficient on-line electronic check to overcome the above-mentioned problems. However, we find that Chen's method can not achieve the most important requirement to develop an e-check system. Hence, we aim to present a novel on-line electronic check method in this article. The novel version

* Corresponding author. Tel.: +886 4 24517250x3767; fax: +886 4 27066495.
*E-mail addresses:* ccc@cs.ccu.edu.tw (C.-C. Chang), M9405071@cs.ccu.edu.tw (S.-C. Chang), ljs@cs.ccu.edu.tw (J.-S. Lee).

0045-7906/$ - see front matter © 2009 Elsevier Ltd. All rights reserved.
doi:10.1016/j.compeleceng.2009.02.007

can not only overcome the above-mentioned problems but also provide the mutual authentication between a payer and a payee to enhance the system security. Besides, the new method can achieve the following requirements.

We then describe the requirements that the new method shall confirm.

(1) **Uniqueness:** An e-check must be appended with the payer's identity**.** This provides the uniqueness of the e-check. With this property, a trusted bank can easily find the corresponding data to verify the e-check.
(2) **Robustness:** Only a legal payer and a trusted bank can cooperate to generate e-checks. Since there is often a large amount of money involved in the transaction, this requirement shall be confirmed to prevent the e-check from being forged by the imposters.
(3) **Mutual authentication:** Not only a payee can verify the identity of a payer, but also a payer shall be able to authenticate a payee. This can help enhance the security of the payment system.
(4) **Non-repudiation:** No payer can deny an e-check once he has used in dealing a transaction with a payee.

The rest of this article is organized as follows. The preliminaries are described in Section 2. Our proposed method is given in Section 3. Next, we analyze the security of our scheme in Section 4, followed with discussions in Section 5. Finally, we make some conclusions in Section 6.

## 2. Preliminaries

In this section, we introduce three cryptographic techniques used in our proposed electronic check mechanism: Chaum's blind signature, one-way hash function [9], and RSA digital signature.

### 2.1. Blind signature

In 1983, Chaum first proposed the main idea of blind signature [1,2]. In Chaum's blind signature scheme, there are two main participants, the signer and the client. The detailed process of Chaum's blind signature scheme is described as follows:

Step 1: The client selects a random number $r$ and computes

$$m' = mr^e \bmod n,$$

where $\gcd(n, r) = 1$. The client then sends the computation result to the signer.

Step 2: Upon receiving the message sent by the client, the signer computes

$$s' = (m')^d \bmod n$$

and then sends the result to the client.

Step 3: When receiving the message sent by the signer, the client can obtain the signature $s$ by computing the following equation:

$$s = s'r^{-1} \bmod n = ((mr^e \bmod n)^d \bmod n) r^{-1} \bmod n = m^d \bmod n.$$

### 2.2. RSA digital signature

In the real world, there are many digital signature schemes [6,7,9,10,12–14]. And, the RSA cryptosystem [11] is one of the most widely used techniques in digital signatures or encryption/decryption algorithms. The details of RSA digital signature scheme are shown as follows:

Step 1: The signer generates two large distinct random primes $p$ and $q$.

Step 2: The signer then computes

$$n = p \cdot q \text{ and } \phi(n) = (p-1) \cdot (q-1).$$

Step 3: The signer randomly selects an integer $e$ such that $1 < e < \phi(n)$ and $\gcd(e, \phi(n)) = 1$. $(e, n)$ is the public key of the signer.

Step 4: The signer computes the private key of the signer $d$ such that $e \cdot d \equiv 1 (\bmod \phi(n))$, where $1 < d < \phi(n)$.

Step 5: For the message $m$, the signer generates the signature $s$ as follows,

$$s = (m)^d \bmod n.$$

The signer subsequently sends the signature $s$ to the user.

Step 6: After receiving the signature, the user can verify the signature by checking if the following equation holds

$$m = (s)^e \bmod n.$$