Efficient on-line electronic checks

Wei-Kuei Chen

Department of Computer Science and Information Engineering, Ching-Yun University, 229, Chien-Hsin Road, Chung-Li, Taiwan 320, ROC

Abstract

Chaum proposed two electronic check schemes in 1988 and 1989, respectively [Chaum et al., Advances in Cryptology—CRYPTO’88, 1990, pp. 319–327; Efficient Offline Electronic Check, 1989, pp. 294–301]. Both of the two schemes are not efficient. Besides, the face value and payee’s identification information of an electronic check has to be decided before the bank issued electronic check. In this paper, an efficient and practical electronic check scheme is proposed to make it possible for a payer to attach the desired face value and payee’s identification information to his electronic check when paying. The proposed scheme not only keeps the attached information from being forged but also avoids two or more different face value being attached to the same electronic check. Furthermore, the extra computation required for information attachment is just hashing, without any time-consuming computation such as modular exponentiation or inverse computation. Since the cost of hashing computation is cheap, the proposed scheme is very efficient.

© 2004 Elsevier Inc. All rights reserved.

Keywords: Electronic check; One-way function; Digital signatures; Cryptography

1. Introduction

Due to the fast progress of computer technologies, the efficiency of data processing and the speed of information generation have been greatly improved. Moreover, the techniques of networks largely shorten the communicating time among distributed entities. Many advanced network services have been proposed in the literature to take the advantages of the techniques.
Among these services, electronic check system is a new possible service which makes it possible for a payer in a remote site to pay his electronic check (e-check) for some products through electronic communication networks [1,2]. E-checks are modeled on traditional checks. Three parties, a bank, a group of payers, and a group of payees are in a typical electronic check system. If a payer wants to use e-checks, he has to register them with bank in advance. When a payer decides to pay a payee for a product, he has to pay his e-check with designated face value and payee’s identification information to the payee through network.

The concepts of electronic check system were first introduced by Chaum in 1988 [1]. Chaum’s scheme causes an enormous overhead in computation and communication. Therefore Chaum proposed an enhanced scheme to overcome the drawbacks of first scheme [2]. However, the improved scheme is not efficient enough, too. Besides, one major drawback can be found in both of Chaum’s schemes [1,2]. The face value or payee’s identification information of an e-check have to be decided before every e-check issued by the bank. In this paper, an efficient on-line electronic check protocol will be presented. Only several extra hashing operations are required in the proposed scheme. Besides, the face value and payee’s identification information can be attached to an e-check after a payer decided to pay the payee for a product.

The rest of this paper is organized as follows. In Section 2 preliminaries used in this paper are introduced. The proposed protocol is presented in Section 3. Then a brief cryptanalysis is discussed in Section 4. Finally, a conclusion of this paper is given in Section 5.

2. Preliminaries

In this section, preliminaries used in this paper will be introduced.

2.1. One-way hash function

A one-way hash function $H$ is a transformation that takes an input $x$ and returns a fixed-size string $y$. The basic requirements for a cryptographic one-way hash function [5] are shown in the following:

(1) The input can be of any length.
(2) The output has a fixed length.
(3) Given $x$, it is relatively easy to compute $H(x)$.
(4) Given $y$, it is infeasible to compute $x$ such that $H(x) = y$.
(5) It is hard to find $x_1$ and $x_2$ such that $H(x_1) = H(x_2)$.

Examples of well-known hash functions are MD 2, MD 4, MD 5, and SHA [5].
2.2. RSA digital signatures

A cryptographic primitive which is fundamental in authentication, authorization, and non-repudiation is the digital signature [5]. The first digital signature scheme was published by Rivest, Shamir, and Adleman [7]. Two parties, a signer and a group of users, participate in a digital signature protocol. A digital signature is a sequence of bits appended to a digital document and the purpose of digital signature is to provide a method for a signer to bind its identity to a piece of information. When public-key cryptography [3] is used to calculate a digital signature, the signer encrypts the document with its own private key. Anyone with access to the public key of the signer may verify the signature. This technique can prevent authorized messages from being forged. Besides, the signer can link a signature shown for verification to the instance of the protocol which produces that signature. In practical application, to create a digital signature, one usually signs the hashed value of the message instead of the original message itself. This saves a considerable amount of time and avoids the multiplication attacks [5,9,10]. Examples of well known digital schemes are RSA [7], DSA [5], Elgamal [4], Rabin [6], and Schnorr [8].

The RSA cryptosystem [7] is one of the widely used techniques in digital signatures or encryption/decryption algorithms. The details of RSA digital signature scheme are given in the following:

1. Generate two large distinct random prime numbers \( p \) and \( q \), where the sizes of \( p \) and \( q \) are as the same as possible.
2. Compute \( n = pq \) and \( \phi = (p - 1)(q - 1) \).
3. Randomly select an integer \( e \) where \( 1 < e < \phi \) and \( \gcd(e, \phi) = 1 \).
4. Compute \( d \) where \( 1 < d < \phi \) and \( ed \equiv 1 \pmod{\phi} \).
5. The public key is \( (e, n) \); the private key is \( (d, p, q) \).

RSA digital signature scheme consists of two types of participants, the signer, and a group of users. The signer signs a document to obtain the signature by using its private key, and the user verifies the signature by using the corresponding public key. The technique of digital signature can prevent authorized messages from being forged, so it can be adopted to assign some essential messages which can not be deliberately altered in the practical communication systems [7,9,10].

3. The proposed scheme

Based on the RSA digital signature scheme described in Section 2, the proposed electronic check scheme is introduced as follows. The face value and payee’s identification information are attached to e-check during paying. The
proposed protocol consists of three parties (a bank, a group of payers, and a group of payees) and four stages (initializing, delegating, paying, and depositing). The bank and the payers of the proposed protocol are regarded as the signer and the users of the digital signature scheme of Section 2, respectively. The protocol is described below.

(1) **Initializing phase**
Initially, all customers perform an account establishment protocol with the bank to open an account in the bank. Besides, the bank randomly selects two distinct large primes \( p \) and \( q \), and computes \( n = pq \). Through the same key generation as the initializing stage of the RSA protocol shown in Section 2, the public key \((e, n)\) and private key \((d, p, q)\) of the bank are generated, respectively. Suppose the payee’s identification information is account number and its possible value is between 1 and \( k \). In addition, let the maximum face value of every e-check be \( w \) dollars.

(2) **Delegating phase**
Let \( \| \) be the string concatenation operator. A payer randomly selects four messages \( x_1, x_2, x_3, \) and \( x_4 \) where \( 1 \leq i \leq 4 \), are kept secret. The payer computes and submits \( a = H(m)(\mod n) \) to the bank where \( m = H^w(x_1)\|H^w(x_2)\|H^k(x_3)\|H^k(x_4) \). Note that different one-way hash function \( H_i \) can be applied to different \( x_i \). To simplify presentation, we apply the same \( H \) to all of the \( x_i \). After receiving the message \( a \) from the payer, the bank computes \( s = (a^d \mod n) \) and sends the signing result \( s \) to the payer. The tuple \((m, s)\) is an e-check in the scheme, and it can be verified by checking whether \( s^e = H(m)(\mod n) \) or not.

(3) **Paying phase**
When the payer decides to attach the face value \( a, a \leq w \), and payee’s account number \( b, b \leq k \), to the e-check \((m, s)\), he computes \( \beta_1 = H^a(x_1) \), \( \beta_2 = H^{w-a}(x_2) \), \( \beta_3 = H^b(x_3) \), and \( \beta_4 = H^{k-b}(x_4) \). And then he sends the payee the face value attached e-check \((a, b, s, \beta_1, \beta_2, \beta_3, \beta_4)\).

(4) **Depositing phase**
After receiving \((a, b, s, \beta_1, \beta_2, \beta_3, \beta_4)\), the 7-tuple can be verified by checking if \( s^e = H(H^{w-a}(\beta_1)\|H^a(\beta_2)\|H^{k-b}(\beta_3)\|H^b(\beta_4))(\mod n) \). If the above formula holds, then the payee sends the 7-tuple to the bank for double-spending checking. If the e-check \((a, b, s, \beta_1, \beta_2, \beta_3, \beta_4)\) is not found in bank’s database, the bank adds \( a \) dollars to the payee’s account \( b \) and deducts \( a \) dollars from the payer’s account.

4. **Discussions**

In this section the correctness and unforgeability of the proposed scheme is examined.
(1) Correctness

In the delegating stage of the proposed scheme, the payer computes \( s = (a\text{mod}\, n) \), so that \( s^e = H(m)(\text{mod}\, n) \). Besides, \( H^{w-a}(\beta_1)H^a(\beta_2)H^{k-b}(\beta_3)H^b(\beta_4) = H^w(x_1)H^w(x_2)H^k(x_3)H^h(x_4) = m \). Hence, if \( (a, b, s, \beta_1, \beta_2, \beta_3, \beta_4) \) is an e-check produced by the proposed protocol, then we have that \( s^e = H(H^{w-a}(\beta_1)H^a(\beta_2)H^{k-b}(\beta_3)H^b(\beta_4))(\text{mod}\, n) \).

(2) Unforgeability

The proposed scheme is based on RSA digital scheme [7]. Hence, the difficulty of forging a tuple \( (m, s) \) such that \( s^e = H(m)(\text{mod}\, n) \) depends on the security of RSA cryptosystem.

5. Conclusions

A scheme that provides an easily implemented solution for efficient and practical electronic check systems is presented in this paper. A payer can attach the desired face value and payee’s account number to his e-check for a product, so the scheme is practical. Besides, since only several extra hashing computations are required to perform the attachment operation, the proposed scheme is very efficient.

References