An anonymity-revoking e-payment system with a smart card

Yang Bo, Liu Dongsu, Wang Yumin

National Key Laboratory on ISN, Xidian University, Xi’an, 710071, P.R. China

Published online: 4 December 2001 – © Springer-Verlag 2001

Abstract. An untraceable offline e-payment system can offer a degree of customer anonymity; however, it also presents criminals with opportunities, such as laundering money, corruption, and kidnapping. In this paper, we improve on the e-payment system with a smart card proposed by S. Brands, and present an anonymity-revoking e-payment system. On the one hand, the customer’s privacy cannot be compromised by the bank or by the payee. On the other hand, anonymity can be removed by a trusted third party (trustee) with the help of the bank. In this case, the third party can link a payment to a corresponding withdrawal and prevent money laundering and blackmailing.

Keywords: E-payment systems – Smart card – Anonymity revocation

1 Introduction

An efficient e-payment system is an important prerequisite for electronic commerce. The design of such payment systems poses many security-related problems. Apart from the common security requirements such as the prevention of fraud, the protection of the participants’ privacy is an important issue.

In many systems the protection of the user’s privacy relies exclusively on administrative and legal measures. Using cryptographic tools such as blind signatures, it is possible to design e-payment systems that allow participants to remain anonymous during a transaction, without affecting the security of the system. Such systems offer an unconditional privacy protection, but they can be misused by criminals to carry out perfect blackmailing or money laundering.

The concept of a fair payment system, independently proposed in [3], [5], and [6], offers a compromise between the legitimate need for privacy protection and an effective prevention of misuse by criminals. On one hand, the users’ privacy cannot be compromised by the bank or by the merchant. On the other hand, there is a trusted third party, called the trustee, which can (in cooperation with the bank) remove the anonymity of a transaction if the system is being misused by criminals. Furthermore, the trustee is not involved in the transactions. These systems are all based on the payment system described in [2]. In this paper, we improve the system proposed in [1], and present an anonymity-revoking e-payment system.

Brands proposed a payment system in [1]. A tamper-resistant card, issued by the bank, controls a counter that represents the amount of electronic cash carried by the user. The use of a counter ensures that the computation and communication complexity for paying an amount are independent of the specific amount due, and that conversions between multiple currencies can be made at payment time. To ensure privacy of payments, the user inserts his/her smart card into a user-controlled computer, such as a palm-top computer or a personal computer. Cryptographic software in the user-controlled computer ensures that payments are information-theoretically untraceable and unlinkable.

However, there are some faults in the system:

- While a user is withdrawing money at a bank, his/her smart card interacts directly with bank’s computer. Thus, the user must go to the bank with his/her card.
- Before the withdrawal protocol is executed, the user must obtain the certificate issued by the bank.
- It is assumed that the tamper-resistance of the smart card cannot be broken.

This research is supported by the National Natural Science Foundation of China under grant numbers 19931010 and 69972034.
In this paper, we improve on the system, so that the user’s money withdrawal can be executed at his/her own terminal and the issuing of a bank certificate is replaced by the bank’s blind signature. Thus, the system is simpler than the original one because of the use of a signature in the withdrawal protocol.

In order to prevent multiple spending, e.g., payments, we need to rely on physical security. Indeed, a tamper-resistant card could prevent multiple spending by removing or disabling a coin once it is spent. This will prevent abuse in most cases, since the typical criminal will not have the resources to modify the card. Unfortunately, there is no such thing as a truly “tamper-resistant” card. Instead, even with a tamper-resistant card, it is essential to provide cryptographic security to prevent counterfeiting and to detect and identify multiple spenders in case the tamper-protection is somehow defeated.

In order to prevent anonymity being misused by criminals to commit a perfect crime, our system can provide an anonymity-revocation mechanism, in which a trusted third party, called the trustee, can (in cooperation with the bank) remove the anonymity of a transaction if the system is being misused by criminals. Furthermore, the trustee is not involved in the transactions.

The Schnorr signature protocol [3] is described in Sect. 2, which will be used in our system. The new system is described in Sect. 3, followed by a discussion on its security in Sect. 4.

2 The Schnorr signature protocol

Let symbol \(\parallel\) denote the concatenation of two (binary) strings, \(\varepsilon\) is the empty string. By \(\alpha \in_R Z_q\) we mean that \(\alpha\) is chosen uniformly at random from \(Z_q\). We assume the availability of a collision-resistant hash function \(H : \{0,1\}^* \rightarrow \{0,1\}^l\) (e.g., \(l = 160\)).

Let \(G_q\) be a finite cyclic group of order \(q\) and let \(g\) be a generator of \(G_q\), such that computing discrete logarithms to the base \(g\) is intractable.

Let \(x \in Z_q\) be secret key of a signer and \(y = g^x\) be his/her public key.

A Schnorr signature for a message \(m\) is a pair \((c, s)\), with \(c \in \{0,1\}^l\) and \(s \in Z_q\) satisfying the verification equation

\[
c = H (m\|g^c)\]

and such a signature can be generated only if one knows the secret key \(x\), by choosing \(r\) at random from \(Z_q\) and computing \((c, s)\) according to

\[
c = H (m\|g^r)\quad s \equiv r - cx \pmod{q}.
\]

Basically, a Schnorr signature with respect to a public key \((g, y)\) is a proof (depending on the message \(m\) to be signed) that the signer knows the discrete logarithm of the public key \(y\) to the base \(g\).

A (message-dependent) proof of equality of the discrete logarithm of \(h_1\) to the base \(g_1\) and the discrete logarithm of \(h_2\) to the base \(g_2\), denoted \(PLOGEQ(m, g_1, h_1, g_2, h_2)\), is a pair \((c, s)\) satisfying the following condition:

\[
PLOGEQ (m, g_1, h_1, g_2, h_2) = (c, s)
\]

with

\[
c = H (m\|g_1\|2\|h_1\|h_2\|g_1^c\|g_2^s)\]

Such a proof can be computed if and only if one knows the discrete logarithms \(\log_{g_1} h_1\) and \(\log_{g_2} h_2\) and they are both equal to the same value \(x\). To generate a proof, one first chooses \(r\) at random from \(Z_q\) and computes \((c, s)\) according to

\[
c = H (m\|g_1\|2\|h_1\|h_2\|g_1^c\|g_2^s)\quad s \equiv r - cx \pmod{q}.
\]

Note that the message \(m\) can be the empty string.

3 A payment system

3.1 The setup of the system

The system consists of four parties (a bank \(B\), a user \(U\), a merchant \(M\), and a trustee \(T\)), in which the trustee is involved in the opening of an account, but not in transactions, and the user holds an electronic wallet (its smart card is issued by the bank when the user opens his/her account in the bank). An electronic wallet is made of two parts [2, 4]:

- A small hand-held computer or the user PC, indicated by \(C\).
- A tamper-resistant card (such as a smart card) issued by the bank, indicated by \(S\).

The electronic wallet works in such a way that \(S\) and \(C\) pass through \(C\) to prevent \(S\) leaking the user’s private information during a transaction (e.g., the identity of the user).

\(B\) independently generates two numbers \(x, y \in_R Z_q\), and a number \(g_0 \in_R G_q \setminus \{1\}\), and also determines a collision-free hash function \(H (\cdot)\). The values \(g_0, h = g_0^x, g_1 = g_0^y\) and the function \(H (\cdot)\) are published, while \(x, y\) are kept secret.

\(B\) also sets up an account database to store information about account holders, and a deposit database to store relevant information from deposit payment transcripts, which is irrelevant to the user’s identity. The deposit database is only used in the deposit protocol to prevent multiple spending.

Let \(x_T \in Z_q^*\), \(y_T = g_0^{x_T}\) be \(T’s\) secret key and corresponding public key. Let \(Sig_T (\cdot)\) be \(T’s\) signature algorithm such that anyone can verify \(T’s\) signature using \(T’s\) public key.