On Fair E-cash Systems Based on Group Signature Schemes

Sébastien Canard and Jacques Traoré

France Telecom R&D
42, rue des Coutures, BP6243
14066 Caen Cedex, France
{sebastien.canard, jacques.traore}@francetelecom.com

Abstract. A fair electronic cash system is a system that allows customers to make payments anonymously. Moreover, under certain circumstances, a trusted authority can revoke the anonymity of suspicious transactions. Various fair e-cash systems using group signature schemes have been proposed [4,15,16,18]. Unfortunately, they do not realize coin tracing [4,15,18] (the possibility to trace the coins withdrawn by a customer). In this paper, we describe several failures in the solution of [16] and we present a secure and efficient fair e-cash system based on a group signature scheme. Our system ensures traceability of *double-spenders*, supports coin tracing and provides coins that are unforgeable and anonymous under standard assumptions.

1 Introduction

Many anonymous electronic cash systems have been proposed in the recent years. In these systems, there is no mechanism for the bank, the merchants or any other party to identify the users involved in a transaction. If desirable from a user's point of view, this unconditional anonymity could however be misused for illegal purposes, such as money laundering or perfect blackmailing.
Fair electronic cash systems have been suggested independently by [3] and [17] as a solution to prevent such fraudulent activities. The main feature of these systems is the existence of a trusted authority that can revoke, under specific circumstances, the anonymity of the coins.

Brickell et al. in [3] proposed the first fair off-line electronic cash system. Unfortunately, their scheme requires the participation of the trustee in the withdrawals of coins, which is undesirable in practice. Camenisch, Maurer and Stadler [5] and independently Frankel et al. [11] proposed fair e-cash schemes with an off-line (passive) authority: the participation of the trustee is only required in the set-up of the system and for anonymity revocation. The efficiency and the security (anonymity) of these schemes [3,5,11] have been later improved [12,14]. Unfortunately, the security for the bank (namely the unforgeability of the coins) relies, in these schemes, on non-standard assumptions.

R. Safavi-Naini and J. Seberry (Eds.): ACISP 2003, LNCS 2727, pp. 237–248, 2003.

Group signature schemes have been introduced in 1991 by Chaum and van Heyst [6]. They allow members to sign a document on behalf of the group in such a way that the signatures remain anonymous and untraceable for everyone but a designated authority, who can recover the identity of the signer whenever needed (this procedure is called "signature opening"). Currently, the best group signature scheme is the one of Ateniese et al. [1].
In 1999, Traoré [18] proposed a solution that combine a group signature scheme and a blind signature scheme in order to design a privacy-protecting fair off-line electronic cash system. Unfortunately, his proposal does not realize coin tracing (the possibility to trace the coins withdrawn by a customer). In 2001, Maitland and Boyd [15] proposed a variant of this solution based on the group signature scheme of Ateniese et al. [1]. Very recently, Qiu et al. [16] designed a new electronic cash system, using again a combination of a group signature scheme and a blind signature scheme. However, their solution does not work for various reasons (owing to space limitations, the cryptanalysis of [16] will appear in the full paper). Camenisch and Lysyanskaya [4] proposed a fair electronic cash system where blind signatures are not used (named one-show credentials) but they don't achieve coin tracing.

In this paper, we investigate the same way of using a group signature scheme for designing a fair off-line electronic cash system as [4] do. In fact in [15], [16] and [18], each customer is a member of a group whereas in this paper, a group certificate corresponds to a coin delivered by the bank. This implies a relatively efficient solution which is completely secure and that does not need the use of a blind signature such as other proposals [15,16,18]. Our way of realizing tracing after a double-spending is also different from the solution of [4].
Our paper is organized as follows. In Section 2, we describe our solution and in Section 3, we analyse the security of our proposal.

2 A New Electronic Cash System

In this section, we describe a new fair off-line e-cash scheme based on the group signature scheme of Ateniese et al. [1]. Our fair e-cash scheme however differs from the one of Maitland and Boyd [15] which is based on the same group signature scheme: in their system, the group is formed from the customers that spend the electronic coins, whereas in our system the group is formed from the coins themselves. This difference will allow us, as we will see, to easily incorporate a coin tracing mechanism.
In the simplified model of fair electronic cash that we use, four types of parties are involved: a bank B, a trusted authority T, shops S and customers C. A fair e-cash system consists of five basic protocols, three of which are the same as in anonymous e-cash, namely a withdrawal protocol with which C withdraws electronic coins from B, a payment protocol with which C pays S with the coins he has withdrawn, and a deposit protocol with which S deposits the coins to B.