Fair E-Cash: Be Compact, Spend Faster*

Sébastien Canard[1], Cécile Delerablée[2], Aline Gouget[3], Emeline Hufschmitt[4], Fabien Laguillaumie[5], Hervé Sibert[6], Jacques Traoré[1], and Damien Vergnaud[7]

[1] Orange Labs R&D, 42 rue des Coutures, BP6243, F-14066 Caen Cedex, France
[2] UVSQ, 45 Avenue des Etats-Unis, 78035 Versailles Cedex, France
[3] Gemalto, 6 rue de la Verrerie, 92190 Meudon, France
[4] Thalès Communications, 160 boulevard de Valmy, 92704 Colombes, France
[5] GREYC - Université de Caen-Basse Normandie, France
[6] ST-Ericsson, 9-11 rue Pierre-Felix Delarue, 72100 Le Mans Cedex 9, France
[7] École normale supérieure – C.N.R.S. – I.N.R.I.A., France

Abstract. We present the first *fair e-cash system* with a compact wallet that enables users to spend efficiently k coins while only sending to the merchant $\mathcal{O}(\lambda \log k)$ bits, where λ is a security parameter. The best previously known schemes require to transmit data of size at least linear in the number of spent coins. This result is achieved thanks to a new way to use the Batch RSA technique and a tree-based representation of the wallet. Moreover, we give a variant of our scheme with a less compact wallet but where the computational complexity of the spend operation does not depend on the number of spent coins, instead of being linear at best in existing systems.

Keywords: Fair e-cash, privacy-preserving, batch RSA, blind signature.

1 Introduction

Electronic cash systems allow users to withdraw electronic coins from a bank, and then to pay merchants using these coins preferably in an off-line manner, i.e. with no need to communicate with the bank or a trusted party during the payment. Finally, the merchant deposits the coins he has received to the bank.

An e-cash system should provide user anonymity against both the bank and the merchant during a purchase in order to emulate the perceived anonymity of regular cash. However, it seems that the necessity to fight against money laundering encourages the design of fair e-cash systems where a trusted party can, at any time when it's needed, revoke the anonymity of users. We thus focus on the design of fair e-cash systems. In order to reach the privacy target while being reasonably practical, it is necessary to focus on the efficiency of the most repeated protocol, namely the spending one between the user and the merchant. It should also be possible to withdraw or spend several coins more efficiently than repeating a single withdrawal or spending protocol. At last, we must pay attention to the compactness of the data that are exchanged in all protocols.

* This work has been financially supported by the French Agence Nationale de la Recherche and the TES Cluster under the PACE project while 2nd author was working at Orange Labs and 4th author at ENS.

P. Samarati et al. (Eds.): ISC 2009, LNCS 5735, pp. 294–309, 2009.

Related Works. The compact e-cash system [1] has recently aroused a new interest in e-cash by proposing the first e-cash system permitting a user to efficiently withdraw a wallet with 2^L coins such that the space required to store these coins, and the complexity of the withdrawal protocol, are proportional to L rather than to 2^L. Another possibility of efficient withdrawal is also given in [2]. These schemes fulfill all security properties usually required in the non-fair setting but do not consider the efficiency of the spending phase. One solution to improve it is to manage a wallet that contains coins with several monetary values [3]. The main drawback of this solution is that the user must choose during the withdrawal protocol how many coins he wants for each monetary value. In [4], the initial compact e-cash scheme is modified to improve the spending phase; however, the overall cost is still linear in the number of spent coins and, again, the paper only consider non-fair e-cash. Consequently, there exists no privacy-preserving fair e-cash system allowing the user to both (i) withdraw compact wallets and (ii) spend several coins while the transmitted data size is less than linear in the number of spent coins.

Our Contributions. This paper presents a fair e-cash system with a compact wallet that allows users to spend efficiently k coins while sending to the merchant only $\mathcal{O}(\lambda \log k)$ bits, with λ a security parameter, while preserving the privacy of the users. Our proposal makes use of two main cryptographic building blocks: *blind signatures* [5] and *batch cryptography* [6]. The concept of blind signature is the essence of many e-cash systems [7,8,9]. However, many of these suffer from a lack of efficiency since they usually use the cut-and-choose method in order to identify double-spenders [7]. The Batch RSA method makes it possible to efficiently obtain multiple RSA signatures of multiple messages. Batch cryptography has been used to build several e-cash systems, in order to get additional properties [10,11], to decrease the amount of processing done by the merchant [12], or to improve the efficiency of the withdrawal process at the cost of the linkability of coins withdrawn together [13].

To the best of our knowledge, our proposal is the most efficient (fair) e-cash system in terms of wallet storage size, computational complexity of spending and spending transfer size, which is strongly unforgeable. Note that the level of anonymity achieved by our scheme is strong but it is not perfect. Indeed it is strong because it is impossible to link (i) a withdrawal protocol with a user identity, (ii) a spending protocol to a withdrawal protocol, and (iii) two spending protocols but only under specific constraints. The anonymity property achieved by our scheme cannot be perfect since some information related to the coin number (with respect to the wallet) leaks during the spending phase.

2 Security Model

2.1 Algorithms

A fair e-cash system involves four kinds of players: a user $\mathcal{U}$, a bank $\mathcal{B}$, a merchant $\mathcal{M}$ and a judge $\mathcal{J}$. Each user is able to withdraw a wallet with ℓ coins. Such