Short E-Cash

Man Ho Au[1], Sherman S.M. Chow[2,⋆], and Willy Susilo[3]

[1] Department of Computer Science,
The University of Hong Kong, Pokfulam, Hong Kong
mhau@cs.hku.hk
[2] Department of Computer Science,
Courant Institute of Mathematical Sciences,
New York University, NY 10012, USA
schow@cs.nyu.edu
[3] Center for Information Security Research,
School of Information Technology and Computer Science,
University of Wollongong, Wollongong 2522, Australia
wsusilo@uow.edu.au

Abstract. We present a bandwidth-efficient off-line anonymous e-cash scheme with traceable coins. Once a user double-spends, his identity can be revealed and all his coins in the system can be traced, *without* resorting to TTP. For a security level comparable with 1024-bit standard RSA signature, the payment transcript size is only 512 bytes. Security of the proposed scheme is proven under the q-strong Diffie-Hellman assumption and the decisional linear assumption, in the random oracle model. The transcript size of our scheme can be further reduced to 192 bytes if external Diffie-Hellman assumption is made. Finally, we propose a variant such that there exists a TTP with the power to revoke the identity of a payee and trace all coins from the same user, which may be desirable when a malicious user is identified by some non-cryptographic means.

Keywords: E-cash, Coin-traceability, Bilinear Pairing.

1 Introduction

To conduct business transaction over the Internet, one of the ways to make payment is to use e-cash. The simplest model of an e-cash scheme involves three types of parties: *banks* B, *shops* S, and *customers* C. An e-cash scheme is a set of protocols which includes *withdrawal* (by C from B), *purchase* (by C to S) and *deposit* (by S to B). In the electronic world, all objects are represented by data; e-cash is by no means an exception. Special design can be incorporated in real cash to prevent counterfeiting, but it is easy to duplicate e-cash. Thus it is necessary to prevent a user from spending the same coin twice (*double-spending*).

Resembling real cash, it is desirable that the shop can accept a payment autonomously, without consult any other parties, possibly the bank. E-cash scheme

⋆ Corresponding author.

S. Maitra et al. (Eds.): INDOCRYPT 2005, LNCS 3797, pp. 332–346, 2005.

satisfying this property is described as an *off-line* one. The coins are most probably spent in two different shops when they are double-spent. It is kind of impossible for the shops to check for double-spending on their own. Instead, the bank checks for double-spending when the shops deposit the coins. Either the shops will get the real payment, or the bank will identify the double-spender. On the other hand, honest spenders cannot be slandered to have double spent (*exculpability*), and when the shops deposit the money from the payee, the bank should not be able to trace who the actual spender is (*anonymity).*

Many e-cash systems allow the identification of double-spender have been proposed, but most of them rely on the existence of a trusted third party (TTP) to *revoke* the anonymity (so as to identify the double-spender) when double-spending occurs. The revocation is done probably with the help of a *database* maintained by the bank, where certain tracing information obtained during the withdrawal protocol are stored. This information is usually in an *encrypted* form that is believed to be decryptable by the TTP only.

Even though a secure e-cash system prevents the TTP from slandering an honest spender, the revocation feature gives the TTP an elusive power to revoke the anonymity of honest spender as well. To remove this high level of trust, an anonymous e-cash scheme should support owner-tracing without TTP. Identity of double spender should be revoked while the identity of honest user is always protected. To further punish the double spender, all coins spent (and possibly to be spent) by a cheating user can be linked while the withdrawals and payments of an honest user remains unlinkable. That is, certain information can be put in a blacklist so that the coin from the double-spenders can be recognized when it is spent. Moreover, such coin-tracing can only be (instead of trusted to be) performed after double-spending has occurred.

Recent proposal by Camenisch, Hohenberger and Lysyanskaya [8] supports traceability of owner and coin without a TTP. Moreover, their scheme (hereinafter referred as CHL scheme) has the distinctive feature that a user can withdraw more than one coin in a single withdrawal protocol, and these coins can be spent in an unlinkable manner. Put it in a more formal way, 2^ℓ coins can be withdrawn with the cost of $O(\ell \cdot k)$ instead of $O(2^\ell \cdot k)$, where k is a security parameter. As a result, a "compact electronic wallet" is made possible.

Our Contributions.

- We propose three short e-cash systems with different features:
  1. identification and coin-tracing of double-spender without TTP.
  2. even shorter payment transcript size.
  3. owner-tracing and coin-tracing of honest users with the help of a TTP.
- We reinvestigate the efficiency of the CHL scheme, which includes the bandwidth requirements in payment and deposit protocol, and also the bank's storage requirement. We compare it with our proposal for typical usage.

Organization. Next two sections discuss related works and technical preliminaries. We define our security model in Section 4. The constructions of the e-cash systems are presented in Section 5, accompanied by a comparison of our proposal with the CHL scheme. We conclude the paper in Section 6.