# Recent Advances in Electronic Cash Design

Aline Gouget

Security Labs, Gemalto,
6, rue de la Verrerie, F-92190 Meudon, France.
aline.gouget@gemalto.com

**Abstract.** Electronic cash (or e-cash) is an electronic payment solution that is usually viewed as an attempt to emulate electronically the main characteristics of regular cash. In particular, e-cash and other payment solutions should protect the privacy of users during a purchase. The main distinction of e-cash with respect to other electronic payment systems is that electronic coins are stored on a device controlled by the user, e.g. a smart card or a personal computer hard disk. Since the introduction by Chaum [10, 11] of unconditionally untraceable electronic money, e-cash systems have been extensively studied. Recent work has mainly focused on the efficiency of the protocols with respect to several notions of anonymity. In this talk, we will review the main recent results and also discuss the possibility to transfer a coin without involving the bank which is considered as an important characteristic of regular cash.

## Overview of e-cash schemes

E-cash systems usually assume that the same bank is responsible for giving out electronic coins and for later accepting them for deposit. Users can download a number of electronic coins from the bank using a withdrawal protocol, and next pay one or more merchants with them in a spending protocol. Merchants can later exchange electronic coins for regular cash on their bank account using a deposit protocol.

As it is easy to duplicate electronic data, an e-cash system requires a mechanism that prevents a user from spending the same coin twice without being identified, and it must also prevent a merchant from depositing the same coin twice. E-cash systems allow merchants to check the validity of coins, whereas the detection of double spending is performed by the bank. Indeed, double-spending cannot be checked by the merchant during a payment protocol, as the coins delivered by the bank can be spent at several merchants.

E-cash systems can be categorized into two groups according to whether the bank is *on-line* or not in the spending protocol. In on-line e-cash, a merchant only accepts a coin if the bank confirms that the coin has not been previously spent, and the deposit protocol must be performed immediately after the spending protocol. This scenario is often considered as being very restrictive in practice, especially for low-value payments. In off-line e-cash, the merchant does not need to interact with the bank before accepting a coin from the user. Indeed, during the spending of a coin, the merchant only checks the validity of the coin. Nevertheless, the merchant is guaranteed that the bank will accept the coin or the bank will be able to identify and punish the cheater.

E-cash should provide user anonymity against both the bank and the merchant during a purchase in order to emulate the perceived anonymity of regular cash transaction. When a double-spending is detected, the identity of the cheater must be retrieved. Off-line e-cash schemes can also be categorized into two groups according to whether the revocation of the cheater identity is either done by a trusted party, e.g. a judge, (in this case the revocation of the spender identity is always "technically feasible" by the trusted party), or technically possible only in case of a double-spending.

The main security properties usually considered in e-cash schemes are the unforgeability of coins, the anonymity of users, the unlinkability of spends, the identification of double-spenders and the impossibility for the bank to falsely accuse (with a proof) honest users. Many e-cash schemes have been proposed in the literature, which fulfill some of the security properties previously mentioned, in the on-line or off-line setting, involving a judge or not. Only few of them consider the possibility to transfer a coin from a user to another user without involving the bank.

### Towards a *practical* e-cash scheme

Most recent work has focused on the efficiency of protocols, i.e. the efficiency of the algorithms executed during a protocol and the compactness of the data exchanged between all actors. A major challenge in e-cash is to provide an efficient solution to spend several coins at the same time, i.e., more efficiently than iterating the spending protocol over each coin".

The main significant improvement has been done by Camenisch et al. [4] by introducing the compact e-cash scheme that allows a user to withdraw efficiently a wallet containing $2^L$ coins such that the space required to store these coins and the complexity of the withdrawal protocol are proportional to $(L + k)$ rather than $(k \cdot 2^L)$, where $L$ is a fixed parameter of the system and $k$ is a security parameter. This scheme fulfills the anonymity and unlinkability properties usually required for electronic cash systems. The main drawback of the compact e-cash system is that it does not address the possibility for spending several coins at the same time without iterating the execution of the spending protocol. We will review recent improvements and variants of the compact e-cash scheme that have been proposed [19, 7, 3, 1].

Divisible e-cash schemes attempt to address the problem of the *divisibility of a coin* by allowing a user to withdraw a coin of monetary value $2^L$ and then to spend this coin in several times by dividing the value of the coin. The aim is to allow a user to spend a coin of monetary value $2^\ell$ more efficiently than repeating $2^\ell$ times a spending protocol. Many off-line *divisible e-cash* systems have been proposed in the literature (e.g. [17, 13, 14, 16, 9, 15, 5, 2]). We will review the main advantages and drawbacks of theses schemes.

### On the transferability property in e-cash

The transferability property of a coin, meaning that received cash can be spent later without involving the bank, is seen as a fundamental property of regular cash. However, it has received only little attention in the electronic setting. This lack of interest for transferable e-cash may be explained by the result given in [12] showing that it is impossible to transfer a coin without increasing its size. However, the main advantage of the transferability of e-cash would be the decrease of the number of communications between the bank and all users. We will review the main advantages and drawbacks of transferable e-cash schemes that have been proposed in the literature [17, 18, 12, 6, 8].

## References

1. M. Ho Au, W. Susilo, and Y. Mu. Practical compact e-cash. In *Information Security and Privacy, ACISP 2007*, volume 4586 of *LNCS*, pages 431–445, 2007.
2. M. Ho Au, W. Susilo, and Y. Mu. Practical anonymous divisible e-cash from bounded accumulators. In *Financial Cryptography and Data Security, 2008*, volume 5143 of *LNCS*, 2008.
3. M. Ho Au, Q. Wu, W. Susilo, and Y. Mu. Compact e-cash from bounded accumulator. In *Topics in Cryptology - CT-RSA 2007*, volume 4377 of *LNCS*, pages 178–195, 2007.
4. J. Camenisch, S. Hohenberger, and A. Lysyanskaya. Compact e-cash. In *Advances in Cryptology - EUROCRYPT 2005*, volume 3494 of *LNCS*, pages 302–321, 2005.
5. S. Canard and A. Gouget. Divisible e-cash systems can be truly anonymous. In *Advances in Cryptology - EUROCRYPT 2007*, volume 4515 of *LNCS*, pages 482–497, 2007.
6. S. Canard and A. Gouget. Anonymity in Transferable E-cash. In *Applied Cryptography and Network Security, ACNS 2008*, volume 5037 of *LNCS*, pages 207–223, 2008.

7. S. Canard, A. Gouget, and E. Hufschmitt. A handy multi-coupon system. In *Applied Cryptography and Network Security, ACNS 2006*, volume 3989 of *LNCS*, pages 66–81, 2006.
8. S. Canard, A. Gouget, and J. Traoré. Improvement of Efficiency in (Unconditional) Anonymous Transferable E-Cash. In *Financial Cryptography and Data Security, 2008*, volume 5143 of *LNCS*, 2008.
9. A. Hui Chan, Y. Frankel, and Y. Tsiounis. Easy come - easy go divisible cash. In *Advances in Cryptology - EUROCRYPT '98*, volume 1403 of *LNCS*, pages 561–575, 1998.
10. D. Chaum. Blind signatures for untraceable payments. In *Crypto'82*, Plenum Press, pages 199–203. Springer, 1982.
11. D. Chaum. Blind signature system. In *Crypto'83*, Plenum Press, page 153. Springer, 1983.
12. D. Chaum and T.P. Pedersen. Transferred Cash Grows in Size. In *Eurocrypt'92*, volume 658 of *LNCS*, pages 390–407. Springer, 1992.
13. S. D'Amiano and G. Di Crescenzo. Methodology for digital money based on general cryptographic tools. In *Advances in Cryptology - EUROCRYPT '94*, volume 950 of *LNCS*, pages 156–170, 1994.
14. T. Eng and T. Okamoto. Single-term divisible electronic coins. In *Advances in Cryptology - EUROCRYPT '94*, volume 950 of *LNCS*, pages 306–319, 1994.
15. T. Nakanishi and Y. Sugiyama. Unlinkable divisible electronic cash. In *Information Security ISW 2000*, volume 1975 of *LNCS*, pages 121–134, 2000.
16. T. Okamoto. An efficient divisible electronic cash scheme. In *Advances in Cryptology - CRYPTO '95*, volume 963 of *LNCS*, pages 438–451, 1995.
17. T. Okamoto and K. Ohta. Universal electronic cash. In *Advances in Cryptology - CRYPTO '91*, volume 576 of *LNCS*, pages 324–337, 1991.
18. H. van Antwerpen. Electronic Cash. Master's thesis, CWI, 1990.
19. V.K. Wei. More compact e-cash with efficient coin tracing. Cryptology ePrint Archive, Report 2005/411, 2005. http://eprint.iacr.org/.