Title	Study on New E-cash Systems
Author(s)	広橋, 浩司
Citation	
Issue Date	1999-03
Type	Thesis or Dissertation
Text version	author
URL	http://hdl.handle.net/10119/1224
Rights	
Description	Supervisor:岡本 栄司, 情報科学研究科, 修士

Study on New E-cash Systems

Koji HIROHASHI

School of Information Science,
Japan Advanced Institute of Science and Technology

February 15, 1999

Keywords: *E-cash, Off-line, Schoenmakers Blind Signature, Partially Blind Signature, Message Recovery.*

Electronic cash systems (e-cash systems) have become one of the most important research in both practical and theoretical viewpoints. The features of e-cash systems are the following points:

1. A coin consists of some electronic data.

2. The coin can be transferred through networks.

E-cash systems mainly contain the following schemes:

- **Withdrawal:** A user withdraws an e-cash from a bank.
- **Payment:** Using the e-cash, the user buys something at a shop.
- **Deposit:** The shop deposits the e-cash to his bank account.

In addition, there are the following payment methods:

- **On-line Payment:** When a user buys something at a shop, the shop links to a bank in order to check the validity of the received e-cash, and then deposits the e-cash. That is, both *payment* and *deposit* are simultaneously executed in an on-line manner.
- **Off-line Payment:** When a user pays an e-cash to a shop, the procedure between the user and the shop can be performed without linking to a bank. The shop deposits the received e-cash afterward.

However, since the on-line e-cash systems require that the shop confirms the validity of the received e-cash by linking to the bank, their systems are not practical from the viewpoints of turn-around-time, communication cost and database-maintenance cost. Therefore, the off-line e-cash systems are preferable from the practical viewpoint. Hereafter, we consider only *off-line payment.*

Off-line e-cash systems should also satisfy the following properties:

- **Independence:** The security of e-cash must not depend on any physical conditions. Then, the coin can be transferred through networks.
- **Security:** Nobody can copy (reuse) or forge coins.
- **Privacy (Untraceability):** The privacy of a user should be protected in the payment. That is, the relationship between the user and his purchases must be untraceable by anyone else.

In [22], Schoenmakers presented the blind signature scheme utilizing Schnorr signature scheme [21]. This scheme has the following feature:

- The signer makes the signature using the different private key for each verifier.

In [1], Abe and Fujisaki introduced the concept of *partially blind signature*, which holds the following property:

- Using the clear part in a message, which is the common information between a signer and each verifier, the signer creates the signature on the message. Therefore, he can assure himself that the message contains accurate information, and then signs the message.

Afterward, Abe and Camenisch proposed *partially blind signature* scheme [2] based on Schnorr signature scheme, which is related with the discrete logarithm problem.

Unlike the e-cash systems [3,4,11,12,18,19,22], Miyazaki and Sakurai presented the new e-cash system [14] utilizing the two signature schemes [2,22]. However, this e-cash system allows anyone to forge coins. The reason is that a user can make the coin, which satisfies the verification equations, even if he does not know the private keys a bank uses in the withdrawal scheme. Therefore, we introduced the e-cash system [13] with the feature of the two signature [2,22], and then solved the problem in the e-cash system [14]. Unfortunately, this system is in danger of allowing a user to forge coin value in the withdrawal.

In [16,17], Nyberg and Rueppel introduced the signature scheme, which holds the following feature:

- **Message Recovery:** A message can be conveyed within a signature and can be recovered at a verifier's site. That is, the message need not be hashed or sent along with the signature, which saves storage space and communication bandwidth.

The previous signature schemes based on the discrete logarithm problem, such as ElGamal [9] and Schnorr signature schemes, cannot realize this property.

Utilizing the feature of this signature, Nguyen, Mu and Varadharajan proposed the e-cash system [15] with *message recovery* unlike the previous e-cash systems [3,4,7],[11]-[13],[18,19,22]. However, this e-cash system allows the forgery of coins as well as the system presented in [14].

In this paper, we have examined the actual problems in the e-cash systems [14,15], and then proposed two new *untraceable off-line* e-cash systems. One is the new e-cash system with the properties of the two blind signatures presented in [2,22], which are based on Schnorr signature scheme, and is the system made by improving [13]. The other is the new e-cash system with the feature of Nyberg-Rueppel signature, which provides *message recovery.* Moreover, We have estimated the security in our e-cash systems from the viewpoints of *completeness*, *user's privacy in the payment*, *forgery of coins* and *double-spending detection.* Considering the cost of communication and computation, our systems are more efficient than other e-cash systems [3,11,12].