Digital Cash

8th February 2003

This project is based on the protocol number 4, described in [SCHN96], p. 142. Basically this protocol implements an electronic cash system, in which the digital cash cannot be copied or reused more than once and the privacy of the customer's identity is guaranteed.

Implementation:

The system allows money transaction between three parties: Customer, Merchant and Bank. The electronic cash (ecash) used during these transactions is a file which contains:

- the amount of the transaction involved
- a uniqueness string number
- identity strings which contain the identity of the customer (this information remains secret unless the customer tries to use the ecash illicitly more than once);
- bank's signature (before the customer can use the ecash) The services provided for each party is described as follows:

Customer

- generates N orders for each money order the customer wants to make and assigns a different random uniqueness string number for each of the N ecash money orders
- implements the secret splitting and bit commitment protocols used to generate the identity strings that describe the customer's name, address and any other piece of identifying information that the bank wants to see.
- implements a blind signature protocol for all N money orders

- automatically complies to reveal the half of the identity string chosen by the merchant

Merchant

- verification of the legitimacy of the bank's signature
- random generator of the selector string, which determines the half of the identity string the customer is required to reveal

Bank

- random choice of 1 out of N money orders sent by the customer to remain unopened
- an algorithm that certifies that all the N-1 money orders have been filled with valid information
- a procedure to certify that the orders received from merchants have not been used previously and storage of the uniqueness string and identity strings of the orders in a database file
- Appropriate measures against reuse of the ecash