Chapter 3
Digital Money and Electronic Check Security

Kannan Balasubramanian
Mepco Schlenk Engineering College, India

ABSTRACT

Digital money represents a new payment instrument for e-commerce. More than any other payment instrument, it demands development of a variety of new security techniques for both macro and micropayments. This chapter gives an overview of selected mechanisms for securing digital money transactions. This chapter deals with signature mechanisms using Cryptography. The reader is asked to refer to the Digital signature Standard (DSS) (nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf) for an introduction to Digital Signatures.

PAYMENT TRANSACTION UNTRACEABILITY

When a customer withdraws traditional money from an ATM or at a bank counter, the serial numbers of the notes are normally not recorded. For this reason, payment transactions cannot be linked to a certain customer. Digital coins also have serial numbers and are sometimes represented by unique numbers satisfying specific conditions. Since these numbers exist in only digital form (i.e., not printed on physical notes), it is very easy to create a log record saying which customer obtained which serial numbers. Thus it is possible to observe the electronic payment transactions made by a certain customer by simply looking for these numbers. To prevent this, special mechanisms are needed.

A cryptographic mechanism that can be used to blind (obscure) the connection between the coins issued and the identity of the customer who originally obtained them was proposed in (Chaum et.al, 1988). The mechanism, which provides both payer anonymity and payment transaction untraceability, is based on the RSA signature and is called a blind signature. It is patented and used in the Internet payment software by eCash (http://www.ecashtechonologies.com).
This type of signature is called blind since the signer cannot see what he signs. The basic scenario is the same as in RSA: $d$ is the signer’s private key, $e$ and $n$ are the signer’s public key. There is an additional parameter, $k$, called the blinding factor and chosen by the message (e.g., the digital money serial numbers) provider:

Provider blinds the message $M$:

$$M' = M^e \mod n;$$

Signer computes the blind signature:

$$S' = (M')^d \mod n = k M^d \mod n;$$

Provider removes the blinding factor:

$$S = S' / k = M^d \mod n.$$

The signer usually wants to check if the message $M$ (e.g., a vote or digital coin) is valid. For this purpose, the provider prepares $n$ messages and blinds each one with a different blinding factor. The signer then chooses $n - 1$ messages at random and asks the provider to send the corresponding blinding factors. The signer checks the $n - 1$ messages; if they are correct, he signs the remaining message.

Note that electronic coins blinded in this way can only be used in an online payment system; in order to prevent double spending, it must be checked in a central database whether the coin has already been spent.

- **Exchanging Coins:** The NetCash system (http://nii-server.isi.edu:80/info/netcash) was developed by the Information Sciences Institute of the University of Southern California. The payer anonymity and payment transaction untraceability mechanism it provides are based on trusted third parties. There is a network of currency servers that exchange identity-based coins for anonymous coins, after confirming validity and checking for double spending. This type of anonymity is weaker than the blind signature mechanism from the previous section because:

  ◦ With blind signature, it is not possible to determine the user’s identity, even if all parties conspire;

  ◦ With currency servers, if all parties conspire, including the currency servers involved in the transaction, it is possible to determine who spent the money.

In NetCash, the customer is free to choose a currency server he trusts. However, there must be at least one trusted and honest server to exchange coins for the customer, otherwise the anonymity mechanism does not work. The mechanism based on blind signatures does not need a trusted third party.

**PROTECTION AGAINST DOUBLE SPENDING**

Digital coins can be copied easily and arbitrarily often. This can be done by anybody since they are simply electronically stored numbers. If a payer obtains a valid coin in a legal way, he may try to spend