Department of Electronics

Cryptography

Fall 2019

Hasan Mahmood

hasan@qau.edu.pk

Week 12 (20, 21 November 2019)

Digital Cash

- Anonymous payments, via cash only
- Is it possible to have electronics cash?
- Duplicate electronics coins
- Double spending
- If coins are recorded as they are spent, anonymity is compromised
- Communications with a central bank could fail temporarily
- Verification required via bank

Properties of Digital Cash

1. The cash can be sent securely through computer networks.
2. The cash cannot be copied and reused.
3. The spender of the cash can remain anonymous. If the coin is spent legitimately, neither the recipient nor the bank can identify the spender.
4. The transaction can be done *offline*, meaning no communication with the central bank is needed during the transaction.
5. The cash can be transferred to others.
6. A piece of cash can be divided into smaller amounts.

Digital Cash System

- Participants:
  - Bank
  - Spender
  - Merchant
  - Fraud Control

Initialization

- Done once by some central authority
- Choose a large prime such that $q=(p-1)/2$
- Let g be the square of a primitive root mode p
- This implies:

$$g^{k_1} \equiv g^{k_2} \pmod{p} \iff k_1 \equiv k_2 \pmod{q}$$

- Two secret exponents are chosen
- g, g_1, and g_2 are made public

Hash Functions

- Two public hash functions are chosen
- H
  - Takes 5-tuple of integers as input and outputs an integer mod q
- H_0
  - Takes a 5-tuple of integers as input and outputs an integer mod q

The Bank

- The bank chooses its secret identity number x and computes

$$h \equiv g^x, \quad h_1 \equiv g_1^x, \quad h_2 \equiv g_2^x \pmod{p}.$$

- The numbers h, h_1 and h_2 are made public
- These numbers identity the bank

The Spender

- The spender chooses a secret identity number *u* and computes the account number

$$I \equiv g_1^u \pmod{p}.$$

- The number *I* is sent to bank, which stores *I* along with the information identifying the spender
- Name, address, ID, etc. stored
- The spender does not send *u* to the bank. The bank sends to the Spender
-

$$z' \equiv (I g_2)^x \pmod{p}$$

The Merchant

- The Merchant chooses an identification number *M* and registers it the bank.

Creating a Coin

- The Spender contacts the bank, asking for a coin
- The bank requires proof of identity (similar to withdrawing classical cash from the bank)
- All coins in this scheme have same value
- A coin is represented by a 6-tuple number

$$(A, B, z, a, b, r).$$

- Most of the effort in this system is needed to preserve anonymity and double spending

Creating a Coin

Here is how the numbers are constructed.

1. The Bank chooses a random number w (a different number for each coin), computes

$$g_w \equiv g^w \text{ and } \beta \equiv (Ig_2)^w \pmod{p},$$

and sends g_w and β to the Spender.

Creating the Coin, Spender Secret Numbers

2. The Spender chooses a secret random 5-tuple of integers

$$(s, x_1, x_2, \alpha_1, \alpha_2).$$

3. The Spender computes

$$\begin{aligned} A &\equiv (Ig_2)^s, \quad B \equiv g_1^{x_1} g_2^{x_2}, \quad z \equiv z'^s, \\ a &\equiv g_w^{\alpha_1} g^{\alpha_2}, \quad b \equiv \beta^{s\alpha_1} A^{\alpha_2} \pmod{p}. \end{aligned}$$

Creating the Coin, Conditions

- Coins with A=1 are not allowed
- This may result in Spender solving the discrete log problem

Spender Calculations

4. The Spender computes

$$c \equiv \alpha_1^{-1} H(A, B, z, a, b) \pmod{q}$$

and sends c to the Bank. Here H is the public hash function mentioned earlier.

5. The Bank computes $c_1 \equiv cx + w \pmod{q}$ and sends c_1 to the Spender.

Spender Calculations

6. The Spender computes

$$r \equiv \alpha_1 c_1 + \alpha_2 \pmod{q}.$$

The coin (A, B, z, a, b, r) is now complete. The amount of the coin is deducted from the Spender's bank account.

Spending the Coin

The Spender gives the coin (A, B, z, a, b, r) to the Merchant. The following procedure is then performed:

1. The Merchant checks whether

$$g^r \equiv a\, h^{H(A,B,z,a,b)} \quad A^r \equiv z^{H(A,B,z,a,b)} b \pmod{p}.$$

If this is the case, the Merchant knows that the coin is valid. However, more steps are required to prevent double spending.

2. The Merchant computes

$$d = H_0(A, B, M, t),$$

where H_0 is the hash function chosen in the initialization phase and t is a number representing the date and time of the transaction. The number t is included so that different transactions will have different values of d. The Merchant sends d to the Spender.

3. The Spender computes

$$r_1 \equiv dus + x_1, \quad r_2 \equiv ds + x_2 \pmod{q},$$

where u is the Spender's secret number, and s, x_1, x_2 are part of the secret random 5-tuple chosen earlier. The Spender sends r_1 and r_2 to the Merchant.

4. The Merchant checks whether

$$g_1^{r_1} g_2^{r_2} \equiv A^d B \pmod{p}.$$

If this congruence holds, the Merchant accepts the coin. Otherwise, the Merchant rejects it.

The Merchant Deposits the Coin in the Bank

A few days after receiving the coin, the Merchant wants to deposit it in the Bank. The Merchant submits the coin (A, B, z, a, b, r) plus the triple (r_1, r_2, d). The Bank performs the following:

1. The Bank checks that the coin (A, B, z, a, b, r) has not been previously deposited. If it hasn't been, then the next step is performed. If it has been previously deposited, the Bank skips to the Fraud Control procedures discussed in the next subsection.

2. The Bank checks that

$$g^r \equiv a\, h^{H(A,B,z,a,b)} \quad A^r \equiv z^{H(A,B,z,a,b)} b, \text{ and } g_1^{r_1} g_2^{r_2} \equiv A^d B \pmod{p}.$$

If so, the coin is valid and the Merchant's account is credited.