



# Digital Cash

CS 166, Sem. II 2007-2008

# Electronic Payment Schemes

- Schemes for electronic payment are multi-party protocols
- Payment instrument modeled by electronic coin that has a fixed value and can be exchanged with a traditional monetary instrument
- Parties include:
  - Payer (customer)
  - Payee (merchant)
  - Bank

# Transactions



- Transactions in an electronic payment scheme typically include:
  - Withdrawal of coins by customer from the bank
  - Payment of coins by customer to merchant
  - Deposit of coins by merchant into bank
- Online scheme:
  - The bank participates in the payment transaction
- Offline scheme
  - The bank does not participate in the payment transaction

# Goals



- Integrity

- Coins cannot be forged
- Legitimate transactions are honored

- Accountability

- Transactions cannot be later denied
- Disputes can be efficiently settled

- Privacy

- The identity of some parties is not revealed to other parties
- Coins cannot be traced to the payer and/or payee (digital cash)

# Payment with Digital Signatures

- Coins are random identifiers digitally signed by the bank at the time of withdrawal
- The merchant verifies the signature by the bank
- The bank honors deposit of valid coins
- Security and privacy issues:
  - Customer can copy coin and double spend
  - The bank learns about every transaction by customer and merchant

# Private Payment Scheme



- A blind signature allows the signed to sign a message without knowing the message itself
- Basic digital cash scheme:
  - The bank does a blind signature on the coins withdrawn by the customer
  - The merchant verifies the signature and deposits the coins
  - The bank cannot link the coins to the customer

# Blind Signatures with RSA

- The RSA cryptosystem supports a simple and efficient blind signature scheme
- Consider an RSA signing scheme with
  - Public modulus  $N$
  - Public encryption exponent  $e$  and public cryptographic hash function  $h$
  - Secret decryption exponent  $d$
- The bank can create a signature on any value without knowing it

# RSA Blind Signature Protocol

- The customer picks secret random values  $x$  and  $r$ 
  - Coin identifier  $x$
  - Number  $r$  in  $\mathbf{Z}_N$  relatively prime to  $N$

- The customer sends to the bank value

$$y = r^e h(x)$$

- The bank creates signature  $\sigma(y)$  on  $y$

$$\sigma(y) = y^d \bmod N$$

- The customer derives from  $\sigma(y)$  signature  $\sigma(x)$  on  $x$

$$\sigma(x) = \sigma(y) / r \bmod N$$

- Proof

$$\sigma(y) / r \bmod N = r^{ed-1} h(x)^d \bmod N = h(x)^d \bmod N = \sigma(x)$$

# Defenses Against Double Spending

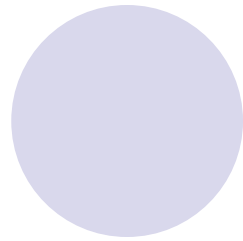
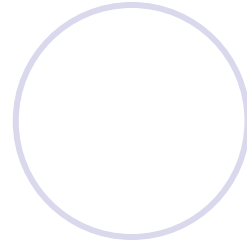
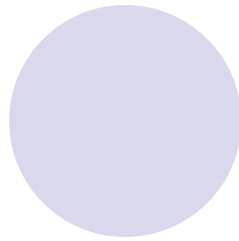
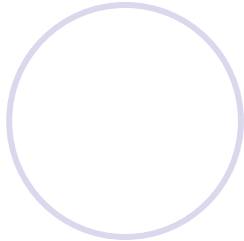
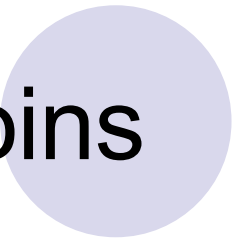
- Online protocol
  - The bank is online during the payment transaction to revoke spent coins
- Offline protocol
  - Withdrawn coins embed encrypted customer identity
  - Deposited coins embed also encrypted merchant identity
  - Double spending caused the identity of the cheating party to be revealed

# Secret Splitting into Shares



- A secret string  $x$  can be split into random values  $y$  and  $z$  as follows
  - Pick a random value  $y$
  - Set  $z = y \oplus x$
- String  $x$  can be reconstructed from  $y$  and  $z$  by setting
  - $x = y \oplus z$
- Both shares  $y$  and  $z$  are random values and are referred to as shares of  $x$
- Neither share reveals any information about secret  $x$

# Coins



- Let  $h$  be a cryptographic hash function
- Given a secret string  $x$ , a commitment pair for  $x$  is a pair  $(a, b)$  such that
  - $a = h(y)$
  - $b = h(z)$
  - $y$  and  $z$  are random shares of  $x$
- Let  $ID$  be a string identifying the customer (e.g., name, address, etc.)
- The coin issued by the bank to the customer consists of
  - Coin identifier  $x$
  - Sequence of  $n$  commitments pairs  $(a_1, b_1), \dots, (a_n, b_n)$  for  $ID$
- The coin does not reveal the identity of the customer

# Withdrawal and Payment

- Withdrawal

- The customer generates and submits  $k$  coins to the bank
- The bank randomly selects  $k - 1$  coins
- The customer reveals to the bank the shares associated with the commitments pairs of the selected coins
- The bank creates a blind signature on the remaining coin
- The coin signed is valid with probability  $1 - 1/k$

- Payment

- The customer gives to the merchant a coin  $\{ x ; (a_1, b_1), \dots, (a_n, b_n) \}$
- The merchant gives to customer a random binary vector  $s_1, \dots, s_n$ , called selector
- The customer reveals to the merchant strings  $P_1, \dots, P_n$  such that

$$h(P_i) = a_i \text{ if } s_i = 0$$

$$h(P_i) = b_i \text{ if } s_i = 1$$

# Deposit and Security Properties

- Deposit

- The merchant deposits with the bank the coin and strings  $P_1, \dots, P_n$
- The bank keeps track of coins and associated strings

- Security properties

- The probability that the selectors provided by two merchants are identical is  $1/2^n$
- Thus, if the customer double spends a coin, then the bank finds out the identity of the customer with probability  $1 - 1/2^n$
- A merchant can double spends a coin without being detected by the bank only if it can find a collision of the hash function

- The scheme does not prevent double spending but detects it and identifies the culprit with high probability

# References

- The electronic cash scheme presented in this lecture is based on the work by David Chaum  
<http://www.chaum.com/>
- D. Chaum, A. Fiat, and M. Naor. *Untraceable Electronic Cash*, in Proc. CRYPTO 1988.  
<http://citeseer.ist.psu.edu/421212.html>
- S. Goldwasser and M. Bellare. *Lecture Notes on Cryptography*, 2002. [Section 11.5]  
<http://www-cse.ucsd.edu/users/mihir/papers/gb.html>