Chapter 14

by

David G. Messerschmitt

Electronic payments

by

David G. Messerschmitt

Electronic payments: the players

Consumer

Merchant

Financial institutions

Physical tokens representing value

Some forms of spending money

Credit

Debit

Check

Cash

Loan

Withdrawal

Demand deposit

Withdrawal

Cash reserves

Questions about value tokens

• Who will back the value?
• How is fraud, counterfeiting, etc. prevented?
• Will value restored if lost or stolen?
• Is it subject to regulation?
• Who pays for the system?
• Is it traced?

Policy dilemmas

• Multiplicity of incompatible payment systems?
• Tracing and auditing:
  – Criminal prosecution
  – Taxation
    vs
  – Personal privacy
Some privacy initiatives

- Open Profiling Standard
- TRUSTe
- Anonymous digital cash

Electronic credit and debit

- Standard authentication, confidentiality, and non-repudiation techniques can be used
  - Asymmetric encryption and certificates
- Framework must take into account different institutions involved
- Example: Secure Electronic Transactions (SET) of Visa/Mastercard

Participants

- Consumer (cardholder)
- Merchant
- Acquirer: financial institution acting as transaction clearinghouse for merchant
- Issuer: financial institution that issued consumer credit/debit card
- Association: Visa or Mastercard

SET chain of trust

SET order/payment protocol

Smartcard
Prepaid smartcard options

- Memory card
  - Memory plus password/PIN protection
- Shared-secret
  - Mutual authentication of any terminal sharing the secret
- Signature-carrying
  - Carries signatures created by institution
- Signature-creating
  - Hardware to create signature based on secret key

Smartcard merits

- Memory
  - Closed system: single institution
  - No authentication of terminal
- Shared-secret
  - Requires encapsulated module in terminal, one to carry each card secret
  - One secret per institution implies that all cards of that institution can be compromised

Smartcard merits (con’t)

- Signature
  - Terminals need only public keys
  - Easy to handle multiple institutions
- All but signature-carrying have unique card identity, and hence institutions can invade privacy by linking transactions

Hard vs. digital cash

Digital cash

010110101101010111010110101
011010110101011010110101011
0101011010101101111011111
011010000001010101011010101

Since digital cash is represented by data, it is easily replicated. How do we prevent:

- Counterfeiting?
- Multiple spending?

What is a digital cash token?

Unique identifier

Value attribute

Bank digital signature

Prevents spending more than once

Prevents counterfeiting
Financial institution perspective

Consumer’s demand deposit → Digital cash liability

Branch ATM → Digital branch

Currency in wallet → Currency in smartcard

Merchant → Digital cash

Merchant’s demand deposit → May return as more digital cash

Digital cash must be deposited

Hard currency

Consumer wallet → Consumer smartcard

Merchant → Digital cash

Deposit → Withdraw as new digital cash

Spend

Merchant → Withdraw

Spending anonymity

Withdrawal and deposit are traceable, but can we break the chain somewhere?

Possible characteristics of digital cash

- Anonymity of consumer
  - Merchant knows who paid, but that information is not inherent to the digital cash itself
  - Financial institution knows what merchant deposited
- Attribution of cheating
  - Double spending
- Authorized traces

Message digest

Message → MD algorithm → Message digest

- MD is a fixed length (128 or 160 bit) summary of message
- One way: message cannot be recovered from MD
- Collision-free: computationally infeasible to find a message corresponding to a given MD

Supplements

by

David G. Messerschmitt
Digital signature based on a message digest

Message → Encrypt secret key → Signature

Signature generation

Decrypt public key → Compare

Signature checking

MD

Dual signature

Consumer
Offer

Merchant
Merchant can verify binding of offer and authorization, does not see offer

Acquirer

Acquirer can verify binding of offer and authorization, does not see offer

MD

Compare

Signature generation

Payment authorization

MD

Spending anonymity

Create $$, including identifier

Repeat n times

Cut and choose one

Blind signature

If the consumer’s software creates the digital cash, and the bank signs it blindly, the bank will not see the identifier. The cut and choose protocol assures the bank the $$ is proper.

Blind signature analogy

Carbon
Token

Put token and carbon in envelope

Present to bank for embossing

Remove token from envelope

Consumer gets bank to sign cash token without observing contents

Cut and choose protocol

$$

$$

$$

$$

$$

Randomly choose one, check others

Blind signature

Although the bank can’t see what it is signing, with the cut and choose the incentive for the consumer is to generate legitimate instances of digital cash.