



Peppercorn Micropayments via better "Lottery Tickets"

Ron Rivest (with Silvio Micali)

MIT Laboratory for Computer Science

Financial Cryptography Conference
Rump Session 2002

(See Proceedings RSA 2002)

Outline

(English law says a *peppercorn* is smallest amount that can be paid in a contract)

- Talk
  - Improve lottery tix with two ideas:
    - »Non-interactivity via recipient signatures
    - »User-fairness via serial numbers
- Demo

The need for small payments

- "Pay-per-click" purchases on Web:
  - Music, video, information

- Mobile commerce ($20G by 2005)
  - Location-based info services, gaming, sodas, parking
- Infrastructure accounting:
  - bandwidth

Payment Framework:

Payment System
Provider (PSP), Bank

Authori-
zation

Deposit(s)

Payment(s)

User Alice

Merchant Bob

Dimensions to consider:

- Aggregation (*global)*
- PSP on-line or off-line ? *(off-line)*
- Interactive vs. non-interactive *(non)*
- Computation Cost *(cheap)*
- User-fairness *(fair)*
- … (many other issues, too)

Aggregation

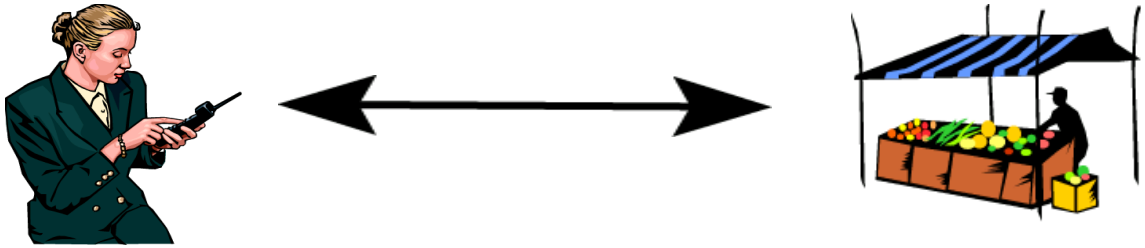
- To reduce cost, micropayments should be aggregated into fewer macropayments.
- Possible levels of aggregation:
  - None: PSP sees every payment
  - Session-level: aggregate all payments in one user/merchant session
  - Global: Payments aggregated across users and merchants
- Can be deterministic or statistical.

On-line vs. Off-line

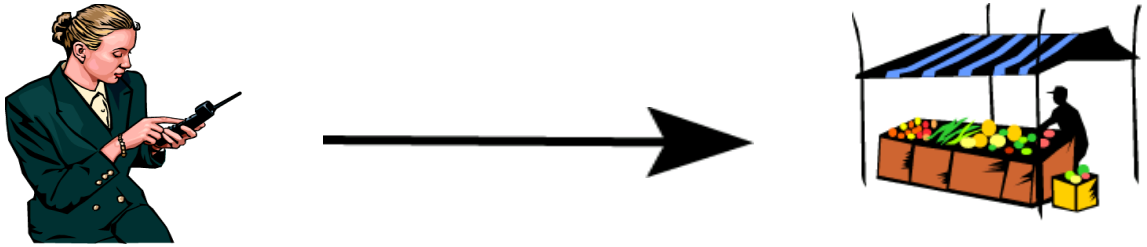
- On-line PSP authorizes each payment or session.
- Off-line PSP not needed to initiate session or make payment
  (e.g. pay taxi)

Interactive vs. Non-interactive

- Interactive:
  Payment protocol is *two-way* :



- Non-interactive:
  Payment protocol is *one-way*
  (e.g. anti-spam payment in email):

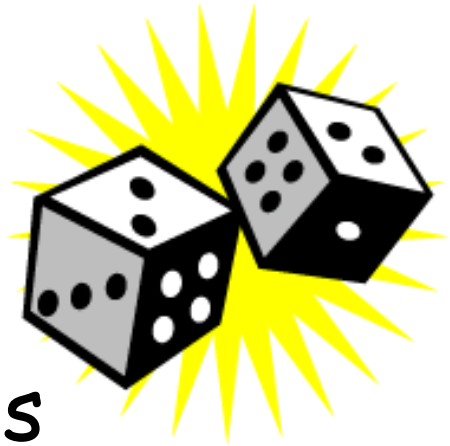


Computation Cost

- Digital signatures are still relatively "expensive" --- but *much cheaper than they used to be!*
- It now seems reasonable to base micropayments on digital signatures. (E.g. Java card in cell phone)
- User and merchant are anyways involved with each transaction; digital signatures add only a few milliseconds.
- On-line/Off-line signature can also help.

Previous Work: Lottery Tickets

- "Electronic Lottery Tickets as Micropayments" – Rivest FC '97 (similar to "Transactions using Bets" proposal by Wheeler '96)
- Payments are *probabilistic*
- First schemes to provide <u>global aggregation:</u> payments aggregated across all user/merchant pairs.



"Lottery Tickets" Explained

- Assume all payments are for one cent.
- Merchant gives user y = hash(x)
- User writes check: "Pay Merchant $1 if two low-order digits of $hash^{-1}(y)$ are 75." (Signed by user, with cert from PSP.)
- Merchant "wins" $1 with probability 1/100. Expected value of payment is 1 cent.
- Bank sees only 1 out of every 100 payments. (A plus for user privacy!)

Our "Peppercorn" Proposal

- Peppercorn improves lottery ticket scheme, making it:
  - Non-interactive
    (by using merchant signatures)
  - Fair to user:
    user never "overcharged"
    (by using serial numbers)

Non-interactive

- Revised check:
  "Pay Merchant $1 if
  two low-order digits of
  the hash of Merchant's digital signature on this check are 75."
- Merchant's deterministic signature scheme unpredictable to user.
- Merchant can convince PSP to pay.

Optimization for less Signing

- "Pay Merchant $1 if the two low-order digits of the hash of Merchant's digital signature on *the date of* this check are 75."
- Merchant only signs once a day.

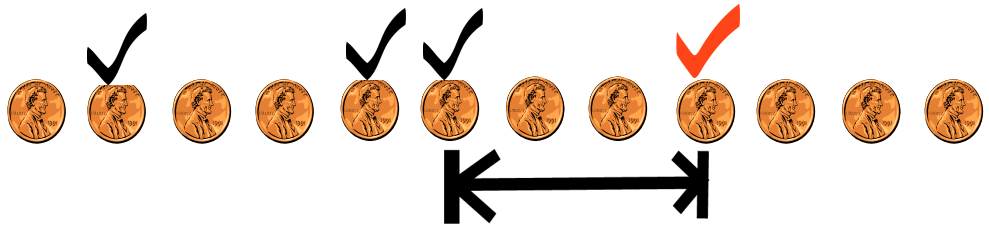
User Fairness: No "Overcharging"

- Concern: unlucky user might pay $1 for his first one-cent payment!
- A payment scheme is *user-fair* if user never pays more than he would if all payments were deterministic one-cent checks.

Achieving User-Fairness

- User must sequence number his payments: 1, 2, …
- When merchant turns in winner with sequence number N, user charged

  N – (last N seen) cents



User charged three cents for ✓

User-Fairness (continued)

- Merchant is still paid $1 for each winning payment.
- Users severely penalized for using duplicate sequence numbers.

Conclusion

- Peppercorn micropayment scheme
  - Is *highly scalable* : bank supports *trillions* of micropayments by processing only *billions* of transactions
  - Provides *global* aggregation
  - Supports *off-line non-interactive* payments
  - Is *user-fair* and quite *private*
  - Uses digital signatures, but lightly.

(DEMO)

(The End)