Outline

• Overview of Fair Exchange
• Optimistic Fair Exchange
  – A General Protocol
  – Optimized Protocol
    • Contract signing
• Self-study
  – Optimized Protocols
    • Certified mail
    • Payment for receipt
    • Fair purchase

Fair Exchange

• A fair exchange should guarantee that at the end of the exchange
  – Either each party has received what it expects to receive,
  – Or no party has received anything
• Examples
  – Certified mail
  – Contract signing
  – Payment
Traditional Fair Exchange

- ISO proposals
  - Use a TTP to ensure fairness
- Limitations
  - TTP is heavily involved
  - Bottleneck
  - Single point of failure

Optimistic Fair Exchange

- Assumptions
  - Most participants are honest
- Allow participants to exchange without TTP
- Fall back to TTP when there are failures
  - Dishonest participants, communication failures, etc.

Three Phases of Optimistic Fair Exchange

- Phase 1
  - The parties try to exchange items without a TTP
- Phase 2
  - The parties try to exchange items through a TTP
- Phase 3
  - Each computer outputs all evidence and any participant may visit a court
Degree of Fairness

- Strong (true) fairness
  - If the TTP is able to
    - Undo a transfer of an item (revocability)
      - Example: revoke a signed contract
    - Produce a replacement for it (Generatability)
      - Example: generate a replacement of a receipt
- Weak fairness
  - If the TTP can only produce affidavits
  - Requires an external dispute resolution system
    - Example: court

Generic Exchange Protocol

- Two stages
  - Stage 1 (Two flows)
    - The originator O and the recipient R promise each other
      an exchange of items
  - Stage 2 (Three flows)
    - Exchange the items along with non-repudiation tokens

Notations

- \(\text{item}_x\): the item \(X\) wants to send
- \(\text{descr}_x\): a description of \(\text{item}_x\)
- \(\text{expect}_x(\text{descr}_x, \text{descr}_y)\):
  - Evaluate to true if \(X\) is satisfied with exchanging \(\text{item}_x\) with \(\text{item}_y\).
- \(\text{fits}(\text{descr}, \text{item})\):
  - Evaluate to true if the description fits the item
- \(h()\): hash function
- \((\text{key}, \text{comm}) = \text{commit}(\text{item})\)
  - Generate a commitment \(\text{comm}\) to \(\text{item}\), and also generate a
    \(\text{key}\), without which it’s impossible to get the item.
    - Verifiable encryption.
- \(\text{open}(\text{item}, \text{key}, \text{comm})\)
  - Use \(\text{key}\) to open the \(\text{item}\) whose commitment is \(\text{comm}\).
Generic Exchange Protocol (Cont’)

**O**  **T**  **R**

In: \(\text{item}_O, \text{descr}_O, \text{expect}_O\)

Choose \(y_O\) (recovery authenticator)
\(r_O\) (NRR authenticator)
randomly; determine \(T\)
\((\text{key}_O, \text{com}_O) := \text{commit} (\text{item}_O)\)

\(m_1 := \text{sign}_O(T, R, \text{key}_O, \text{com}_O, \text{descr}_O)\)

If not \(\text{expect}_R(\text{descr}_R, \text{descr}_O)\)
then:

Choose \(y_R\) (recovery authenticator)
\(r_R\) (NRR authenticator)
randomly;
\((\text{key}_R, \text{com}_R) := \text{commit} (\text{item}_R)\)

\(m_2 := \text{sign}_R(T, \text{key}_R, \text{com}_R, \text{descr}_R)\)

\(m_3 := \text{sign}_O(O, \text{key}_O, \text{com}_O, \text{descr}_O)\)

\(m_4 := \text{sign}_R(O, \text{key}_R, \text{com}_R, \text{descr}_R)\)

If \([\text{fits}(\text{descr}_R, \text{item}_R)]\) and \([\text{open}(\text{item}_R, \text{key}_R, \text{com}_R)]\)
and \([\text{no timeout}]\) then:

\(m_5 := r_O\)

If \([\text{timeout}]\) then:

[Recovery for R]
Else [Recovery for O]

**Output:**

NRO Token: \((m_1, \text{key}_O, \text{com}_O)\)
NRR Token: \((m_1, m_2, r_O)\)

**Output:**

NRO Token: \((m_1, \text{key}_O, \text{com}_O)\)
NRR Token: \((m_1, m_2, r_O)\)

**Question:**

- Why can these tokens guarantee NRO or NRR?
Recovery for O

If [the received messages fit together] then
  retransmit $m_3$, observable by T

If [retransmit invalid] then abort
  else if not [timeout] then
    retransmit $m_4$, observable by T
    open $(item_R, key_R, com_R)$?
    fits $(item_R, descr_R)$?
    $m_5$
  else
    $m_T := sign_T(h(m_~))$

Question

• Can this recovery protocol guarantee
  – Strong fairness for O?
  – Weak fairness for O?

Recovery for R

If [the received messages fit together] then
  retransmit $m_3$, observable by T

open $(item_R, key_R, com_R)$?
  fits $(item_R, descr_R)$?
  $m_5$
else
  $m_T := sign_T(h(m))$
Question

• Can this recovery protocol guarantee
  – Strong fairness for R?
    •
  – Weak fairness for R?
    •

Types of items

• Confidential data
  – Data that will be released during the protocol
  – Example: Software
• Public data
  – Data that will be released even if the protocol execution fails
  – Purpose: fair exchange of non-repudiation tokens.
  – Example: contract
• Payments
  – A payment sub-protocol that is executed to transfer value from payer to payee
  – Example: PayWords

Types of Items (Cont’d)

• Generatable
  – The TTP can produce a replacement of the item
• Revocable
  – The TTP can undo the transfer of the item

<table>
<thead>
<tr>
<th></th>
<th>Public Data</th>
<th>Conf. Data</th>
<th>Payment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Generatable</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Revocable</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Exchange Types

<table>
<thead>
<tr>
<th>Public Data</th>
<th>Conf. Data</th>
<th>Payment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Contract Signing</td>
<td>Certified Mail</td>
<td>Payment with Receipt</td>
</tr>
<tr>
<td>Conf. Data</td>
<td>Exchange of Goods</td>
<td>Fair Purchase</td>
</tr>
<tr>
<td>Payment</td>
<td>Currency Exchange</td>
<td></td>
</tr>
</tbody>
</table>

Optimized Protocol -- Contract Signing

In: contract_O

Choose t_O randomly; determine T

m_1 := sign_T(T, R, h(t_O), t, contract_O)

Choose t_R randomly; contract_R = contract_O

m_2 := sign_R(h(m_1), h(t_R))

m_T := h(t_O)

m_3 := m_2

m_2

Contract Signing (Cont'd)

If [timeout] then

m_T := m_1, m_2, t_R

If [the received messages fit together] then

m_T := m_1

If [response] then

m_T := m_3

else

m_T := sign_T(h(m_1))
<table>
<thead>
<tr>
<th>O</th>
<th>R</th>
</tr>
</thead>
<tbody>
<tr>
<td>contract _P (m_P, m_R)</td>
<td>contract _P (m_P, o_Q)</td>
</tr>
</tbody>
</table>

**Question:**
- Why can these tokens guarantee NRO or NRR?