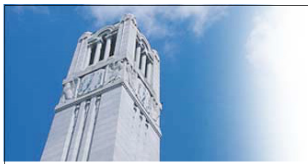


NC STATE UNIVERSITY Computer Science

CSC 774 Advanced Network Security

Topic 3.3: Fair Exchange

Outline

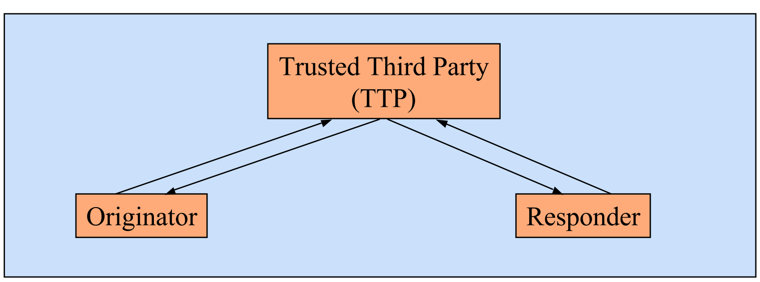
- Overview of Fair Exchange
- Optimistic Fair Exchange
  - A General Protocol
  - Optimized Protocol
    - Contract signing
- Self-study
  - Optimized Protocols
    - Certified mail
    - Payment for receipt
    - Fair purchase

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

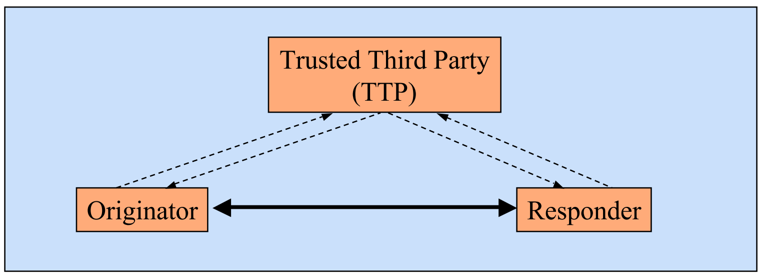
Traditional Fair Exchange

- 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

- $item_X$: the item X wants to send
- $descr_X$: a description of $item_X$
- $expect_X(descr_X, descr_Y)$:
  - Evaluate to true if X is satisfied with exchanging $item_X$ with $item_Y$.
- fits(descr, item)
  - Evaluate to true if the description fits the item
- h(): hash function
- (*key*, *comm*) = commit(*item*)
  - Generate a commitment *comm* to *item*, and also generate a *key*, without which it's impossible to get the item.
  - Verifiable encryption.
- open(*item*, *key*, *comm*)
  - Use *key* to open the *item* whose commitment is *comm*.

Generic Exchange Protocol (Cont')

O T R

In: $item_O$, $descr_O$, $expect_O$

In: $item_R$, $descr_R$, $expect_R$

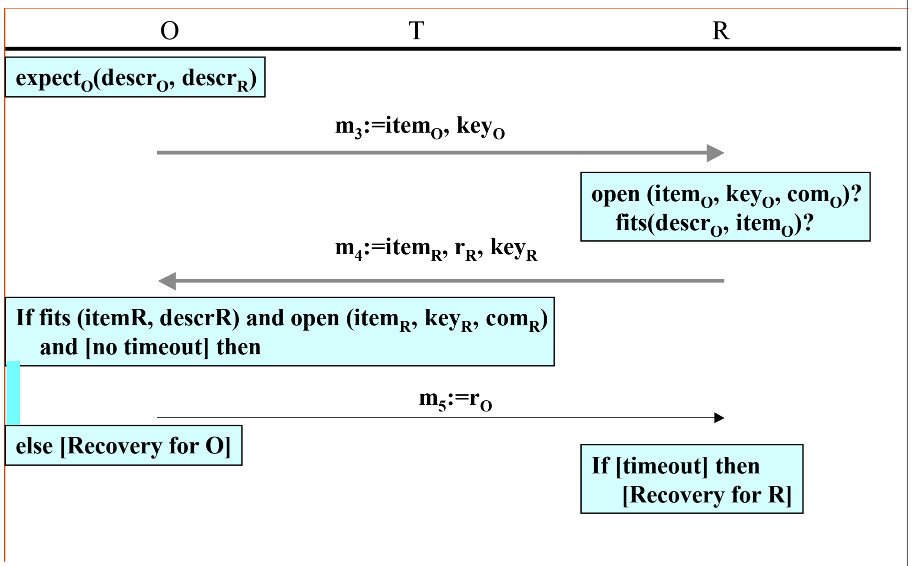
Choose y_O (recovery authenticator)
r_O (NRR authenticator)
randomly; determine T
(key_O, com_O) := commit ($item_O$)

m_1:=$sign_O$(T, R, h(y_O), h(r_O), t, com_O, $descr_O$) →

If not $expect_R$($descr_R$, $descr_O$) then
Abort;
Choose y_R (recovery authenticator)
r_R (NRR authenticator)
randomly;
(key_R, com_R) := commit ($item_R$)

← **m_2:=$sign_R$(O, h(m_1), h(y_R), h(r_R), com_R, $descr_R$)**

Generic Exchange Protocol (Cont'd)

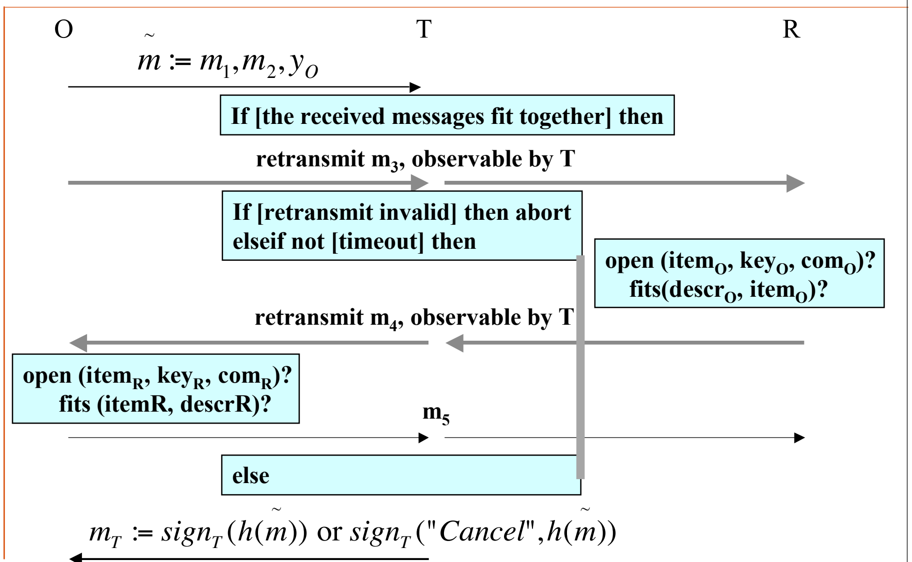


Generic Exchange Protocol (Cont'd)

O	R
Output: **item$_R$** **NRO Token: (m_2, key$_R$, com$_R$)** **NRR Token: (m_1, m_2, r_R)**	**Output:** **item$_O$** **NRO Token: (m_1, key$_O$, com$_O$)** **NRR Token: (m_1, m_2, r_O)**

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

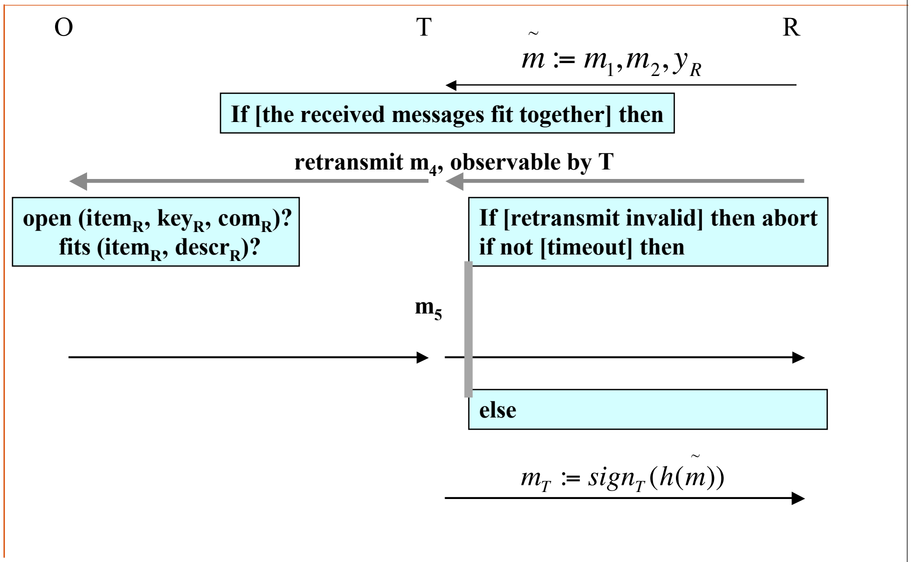
Recovery for O



Question

- Can this recovery protocol guarantee
  - Strong fairness for O?
    - ______
  - Weak fairness for O?
    - ______

Recovery for R



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

	Public Data	Conf. Data	Payment
Generatable			
Revocable			

Exchange Types

	Public Data	Conf. Data	Payment
Public Data	Contract Signing	Certified Mail	Payment with Receipt
Conf. Data		Exchange of Goods	Fair Purchase
Payment			Currency Exchange

Optimized Protocol -- Contract Signing

O T R

In: contract_O

In: contract_R

Choose o_O randomly; determine T

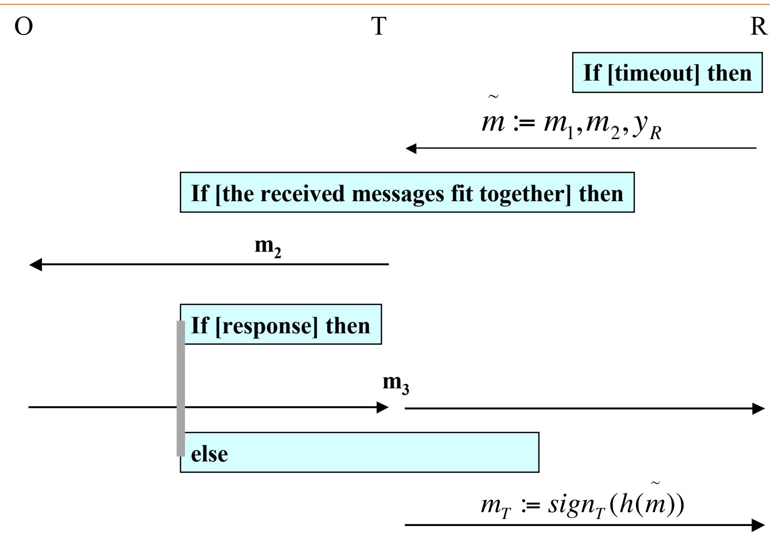
$m_1 := \text{sign}_O(T, R, h(o_O), t, \text{contract}_O)$ (O → R)

Choose yR randomly.
$\text{contract}_R = \text{contract}_O$?

$m_2 := \text{sign}_R(h(m_1), h(y_R))$ (R → O)

$m_3 := o_O$ (O → R)

Contract Signing (Cont'd)



Contract Signing (Cont'd)

O	R
Output: **contractR, (m1, m2)**	**Output:** **contractR, (m1, o_O)**

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