The SEMPER Framework for Fair Exchange

Matthias Schunter

University of Saarbrücken
Germany

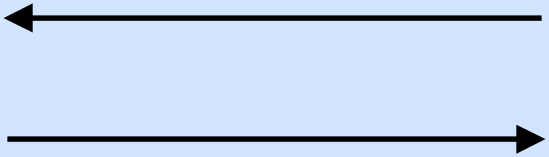
- Introduction
- A Fair Exchange Protocol
- Exchange-Enabling Properties of Transfers
- The SEMPER Framework for Fair Exchange
- Conclusion

Fair Exchange in SEMPER

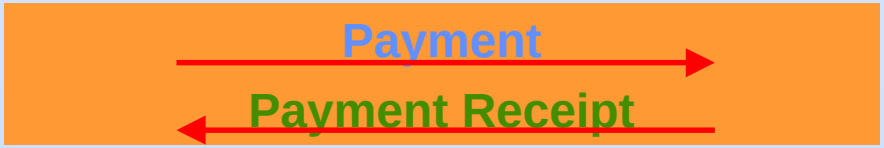
The SEMPER Model:

Buyer

Seller

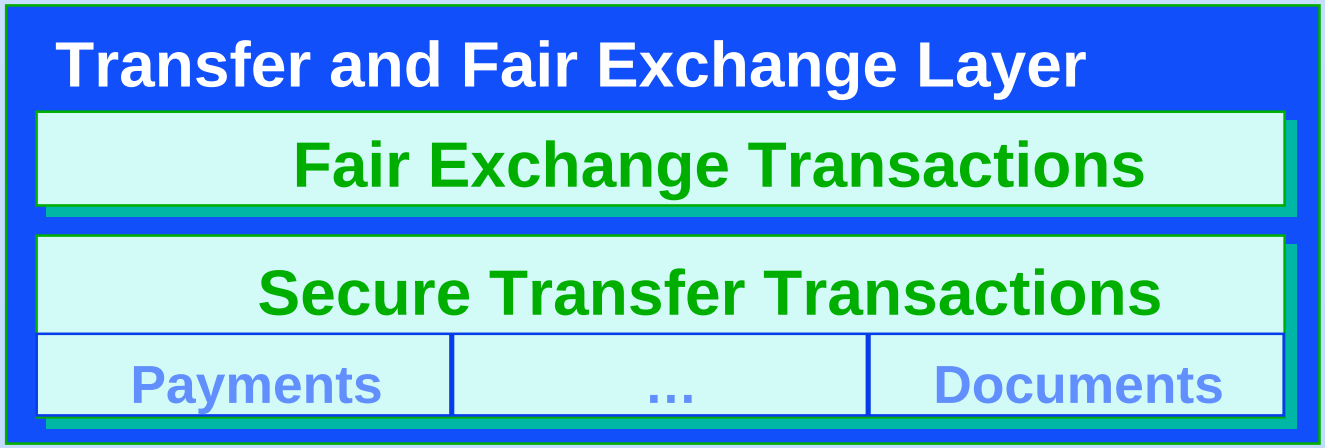


This Talk



The SEMPER Framework:

This Talk



Fair Exchange: Definition and Goals

Buyer

I give: $sign_B(C)$
I want: Signature of Seller under contract *C*

I give: $sign_S(C)$
I want: Signature of Buyer under contract *C*

Seller

Fair Exchange Transaction

If "give=want":

$sign_S(C)$ – – – – – $sign_B(C)$

OR

Else:

failed – – – – – failed

- **Why not use two Transfers?**
  - "Instant" Fairness.
  - Costs of "legal fairness" higher.

Examples & Goals

More Instances of Fair Exchange

- Delivery of valueable data: signature for data.
- Fair purchase: data for payment.
- Payment for receipt: payment for data.
- Contract signing: signature for signature.

Fair Exchange outside SEMPER:

- Protocols for particular instances,
  i.e., dependent from goods to be exchanged
- Inline TP: Limited efficiency and unlimited trust in TP

Goals

- Transfer-based Fair Exchange,
  i.e.,independence from goods
- Optimistic TP: Efficient and limited trust

Example Protocol: Optimistic Contract Signing

Buyer

Seller

Agreement

$m_1 = sign_B(\text{"Let's sign"}: C)$

$m_2 = sign_S(\text{"I agree"}, m_1)$

continue? — continue?

Exchange

$sign_B(C)$

$sign_S(C)$

ok? — ok?

Example: Recovery with TP

Buyer

Seller

Agreement

$m_1 = sign_B(\text{"Let's sign"}: C)$

$m_2 = sign_S(m_1)$

Exchange

$sign_B(C)$

$sign_S(C)$

Recovery

Third Party

$A := (m1, m2)$

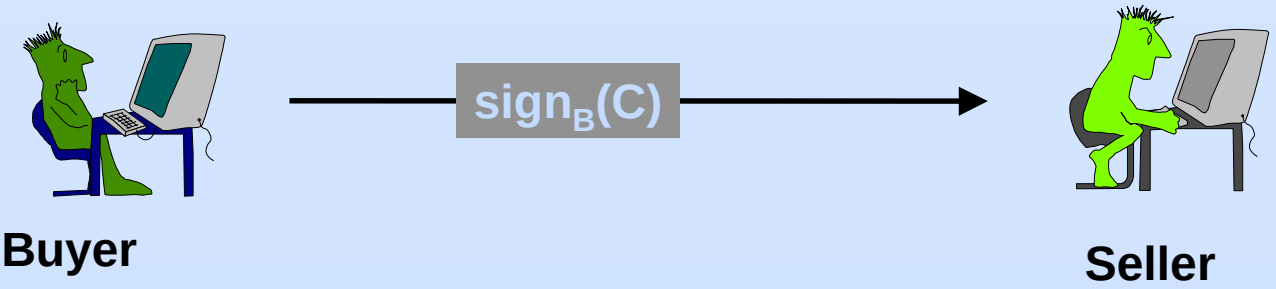
$sign_B(C)$

$sign_T(A)$

$sign_B(C)$

Exchange-Enabling Properties of Signatures

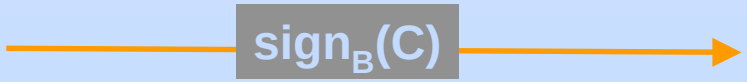
Transfer



Recovery:

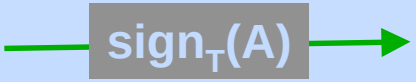
Observable Transfer

- TP can *observe* status of Transfer



Generateable Transfer

- TP can *redo* the Transfer



Revocable Transfer

- TP can *undo* the Transfer

Exchange-Enabling Properties: More Examples

Observability

- Messages: Forward.
- e-cash: Verify and forward.
- Signatures: Verify and forward.

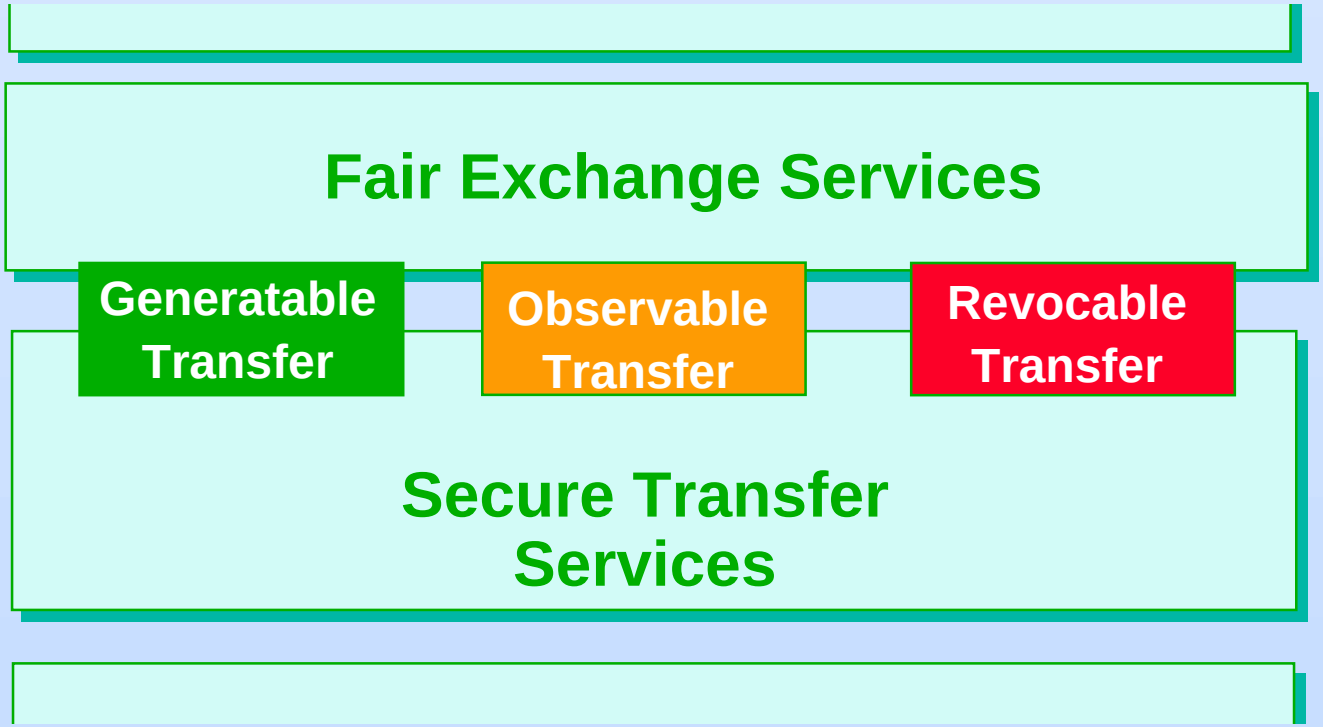
Generatability

- Signatures: Agreement authorizes TP to signs on behalf.
- e-cash: Agreement contains encrypted coin "verifiable encryption"

Revocability

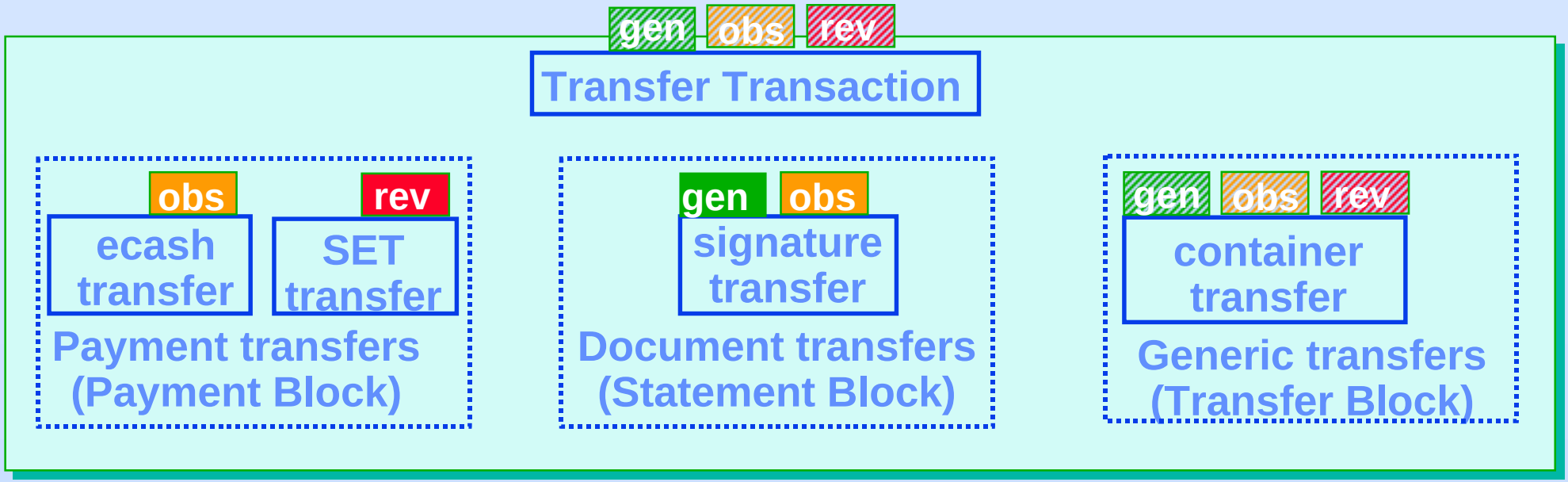
- Credit-card payments: Enable TP to revoke payment.

The Fair Exchange Framework – Overview



- Transfer Layer provides Transfers with Exchange-enabling Properties
- Fair Exchange protocols use the properties to guarantee fairness

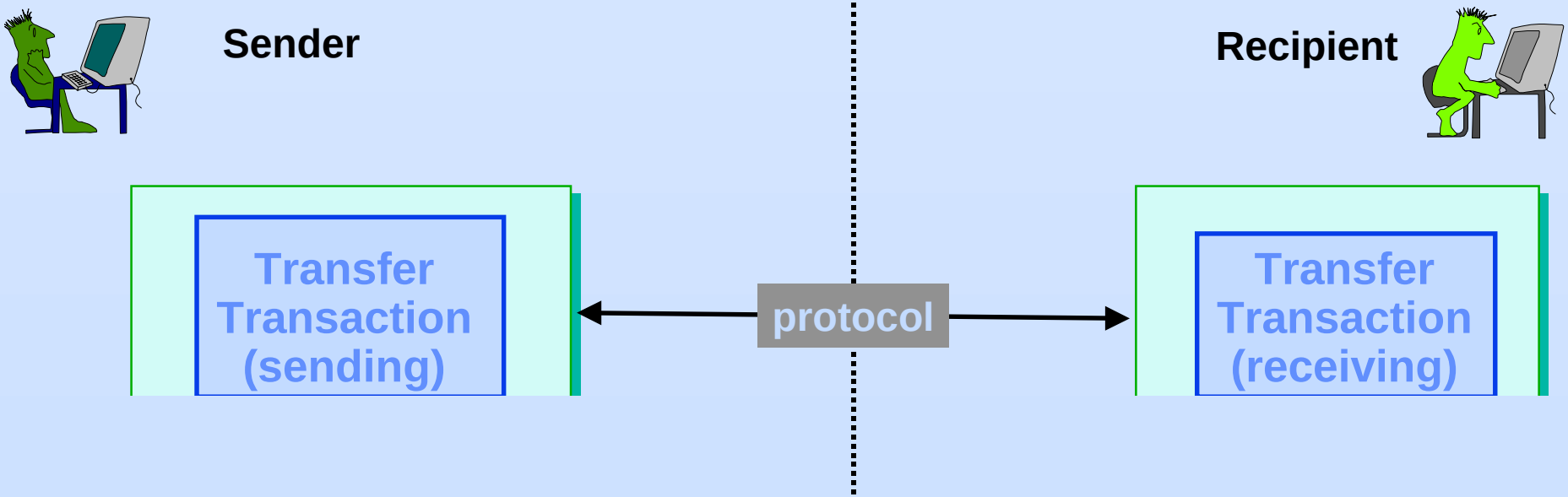
The Fair Exchange Framework – Transfers of Goods



Transfer Transactions:

- Any transfer may provide any subset of the properties
- If a transfer does not provide any property, it cannot be exchanged
- Properties of transfers may depend on the goods to be transferred:
  dynamic negotiation

Using Transfers



User's Point of View

Sender:

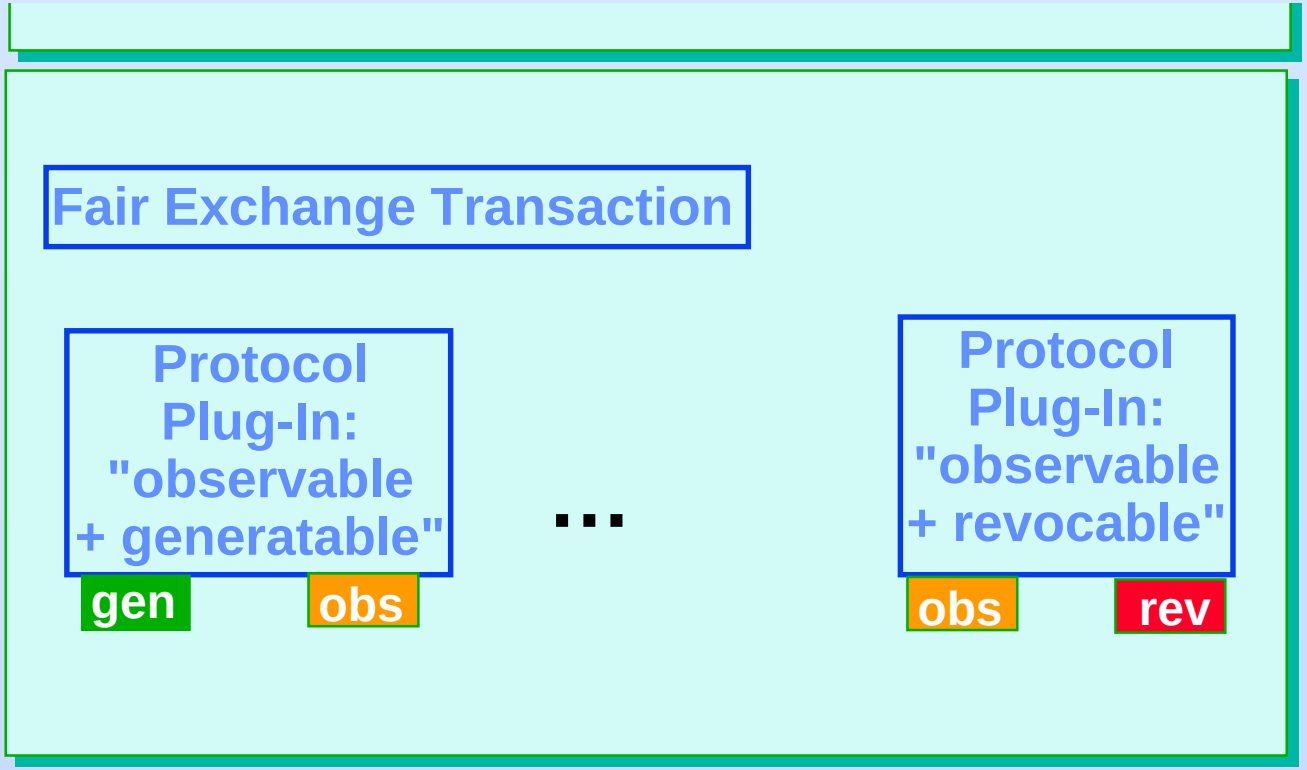
1. Ask the item to be sent for an appropriate transfer transaction.
2. Start it.

Recipient:

1. Instantiate a generic receiver.
2. Start it.
3. Retrieve received item.

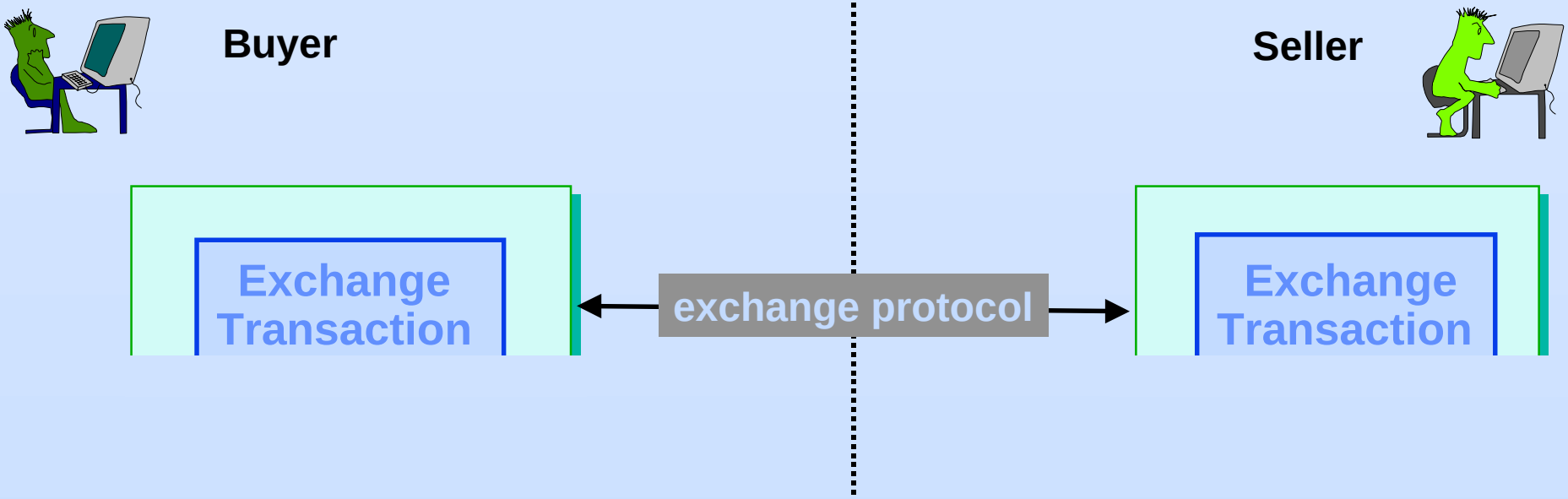
The Fair Exchange Framework – Exchanges

Fair Exchange Layer:



Secure Transfer Layer:

Using Fair Exchanges



User's Point of View

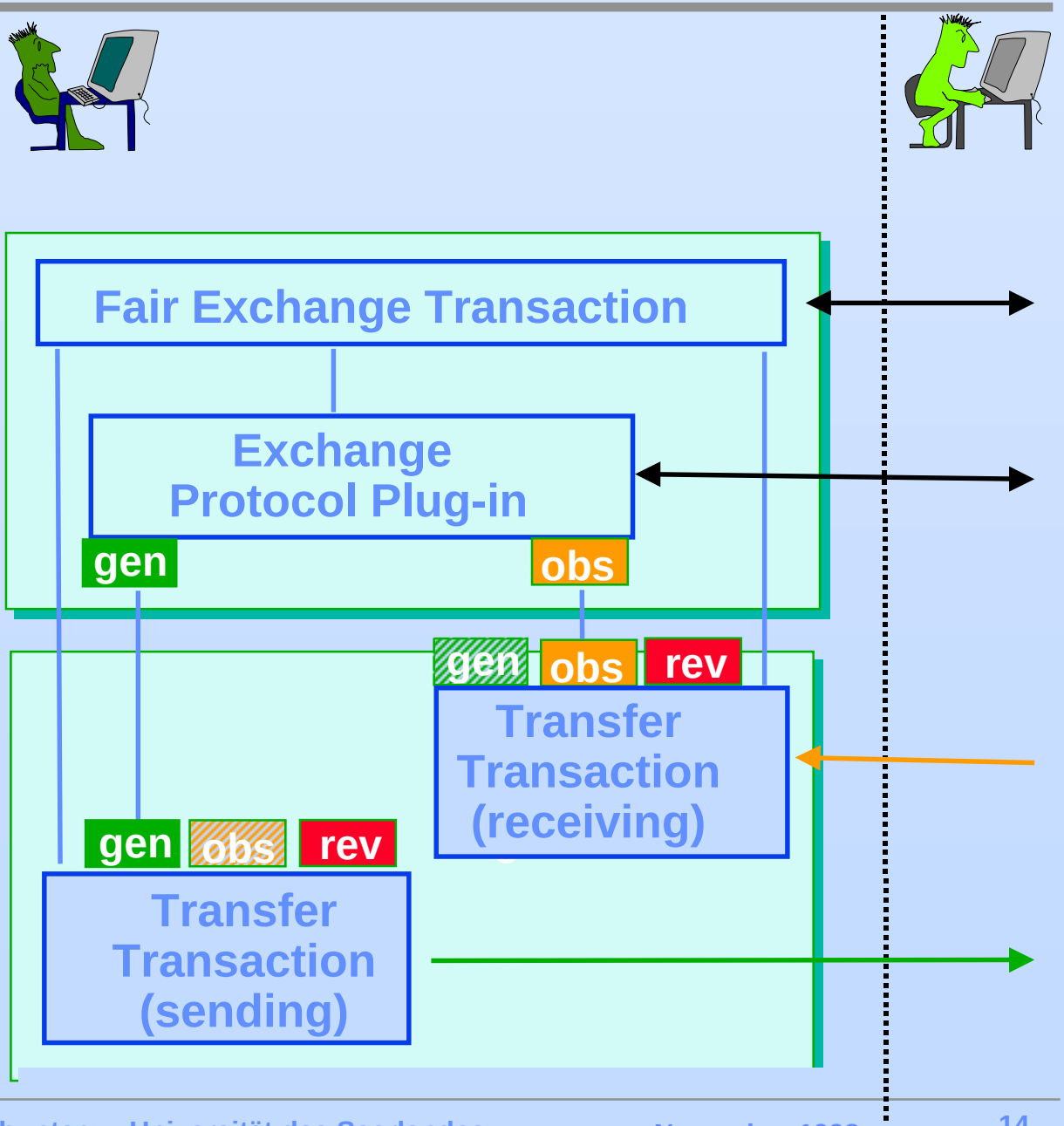
Both:

1. Instantiate fair exchange transaction
2. Input item to be sent
3. Input description of item to be expected
4. Start it
5. Retrieve the result ("failed" or received items)

The Fair Exchange Framework in Action

Activities for Fair Exchange:

1. Exchange Transaction instantiates transfers (sender+receiver)
2. Transfer Transactions negotiate enabled properties
3. Exchange Transactions negotiate protocol
4. Selected protocol runs.



Conclusion

The SEMPER Framework for Fair Exchange

- Guaranteed Fairness
- Open and Extensible
- Enables Efficient Optimistic Protocols:
  TP only needed in case of failure