The Anatomy of a Crypto Protocol

Joshua D. Guttman[1] John D. Ramsdell[2]

[1]Worcester Polytechnic Institute [2]The MITRE Corporation

Thanks to the MITRE-Sponsored Research program and the National Security Agency.

Symposium for Mitchell Wand
24 Aug 2009

Protocols coordinate distribute systems

Despite malicious adversaries

Allow principals to

- Agree selectively on values
- Undertake commitments involving those values
- Coordinate state changes

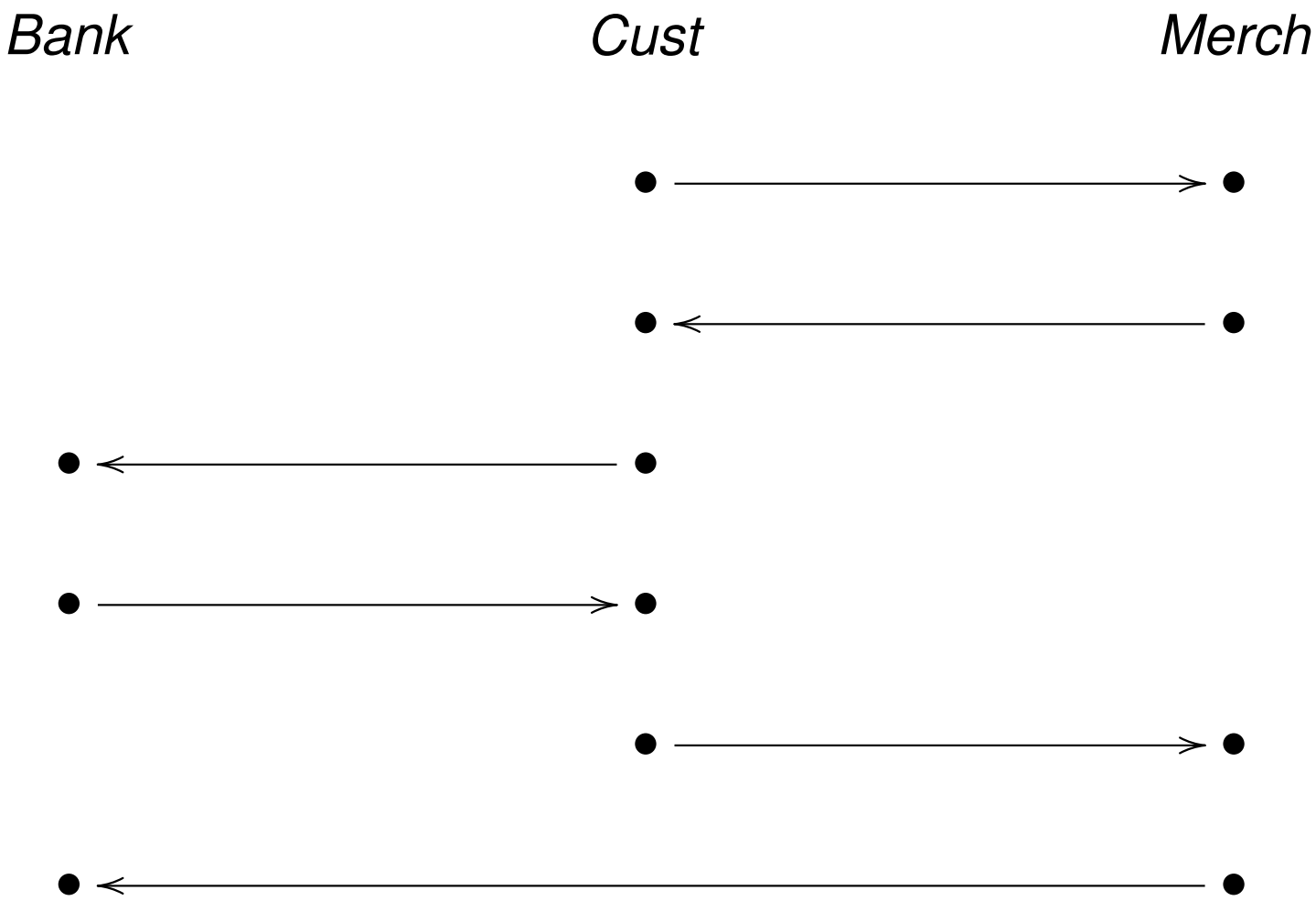
Application-specific crypto protocols

Three claims

- Central to secure distributed systems
- Analysis uses two basic principles: authentication tests
  - Formalized in a small denotational semantics
  - Analysis tool CPSA
- Authentication tests also suggest systematic protocol design methods

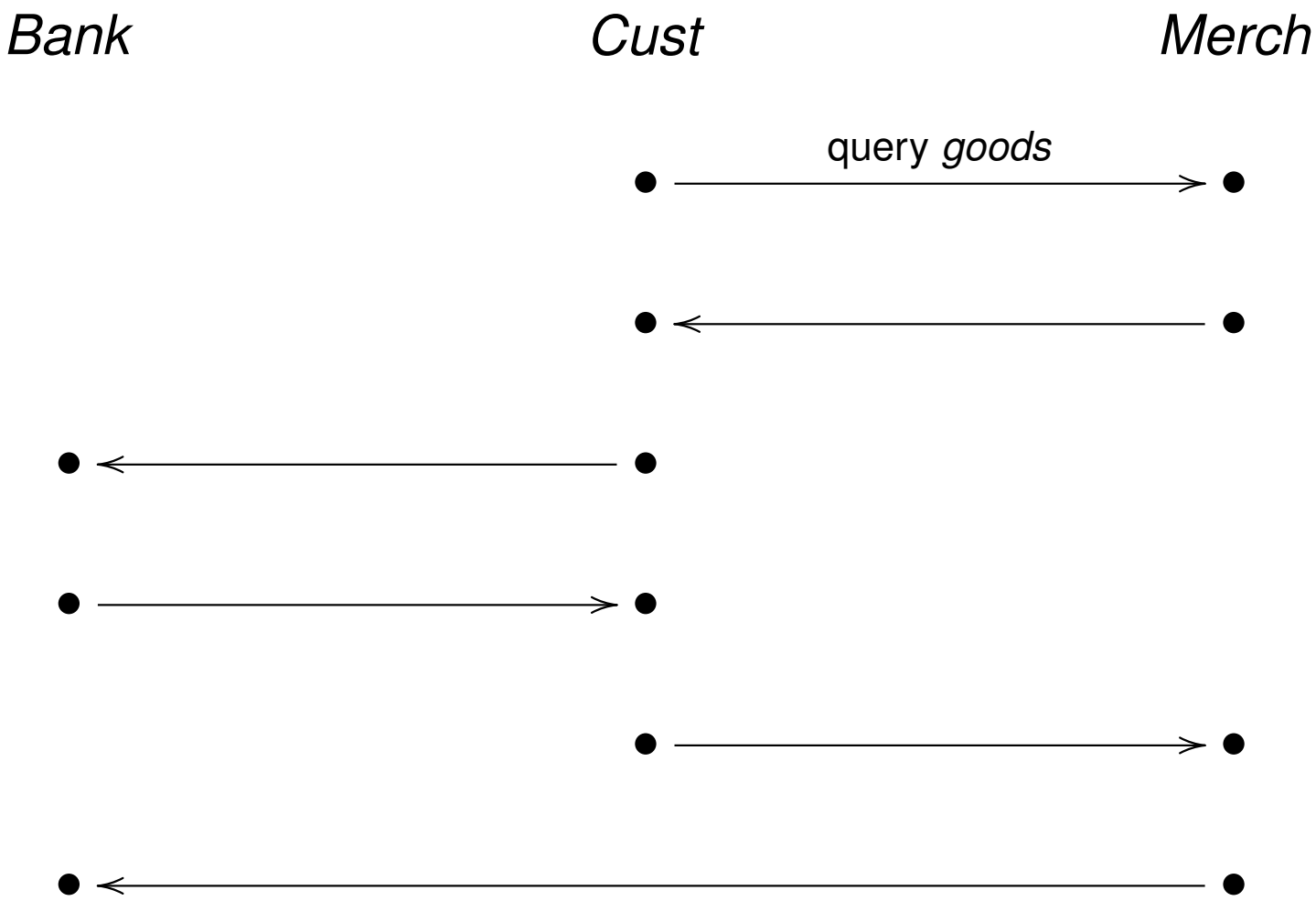
Electronic Purchase

Using a money order: *EPMO*



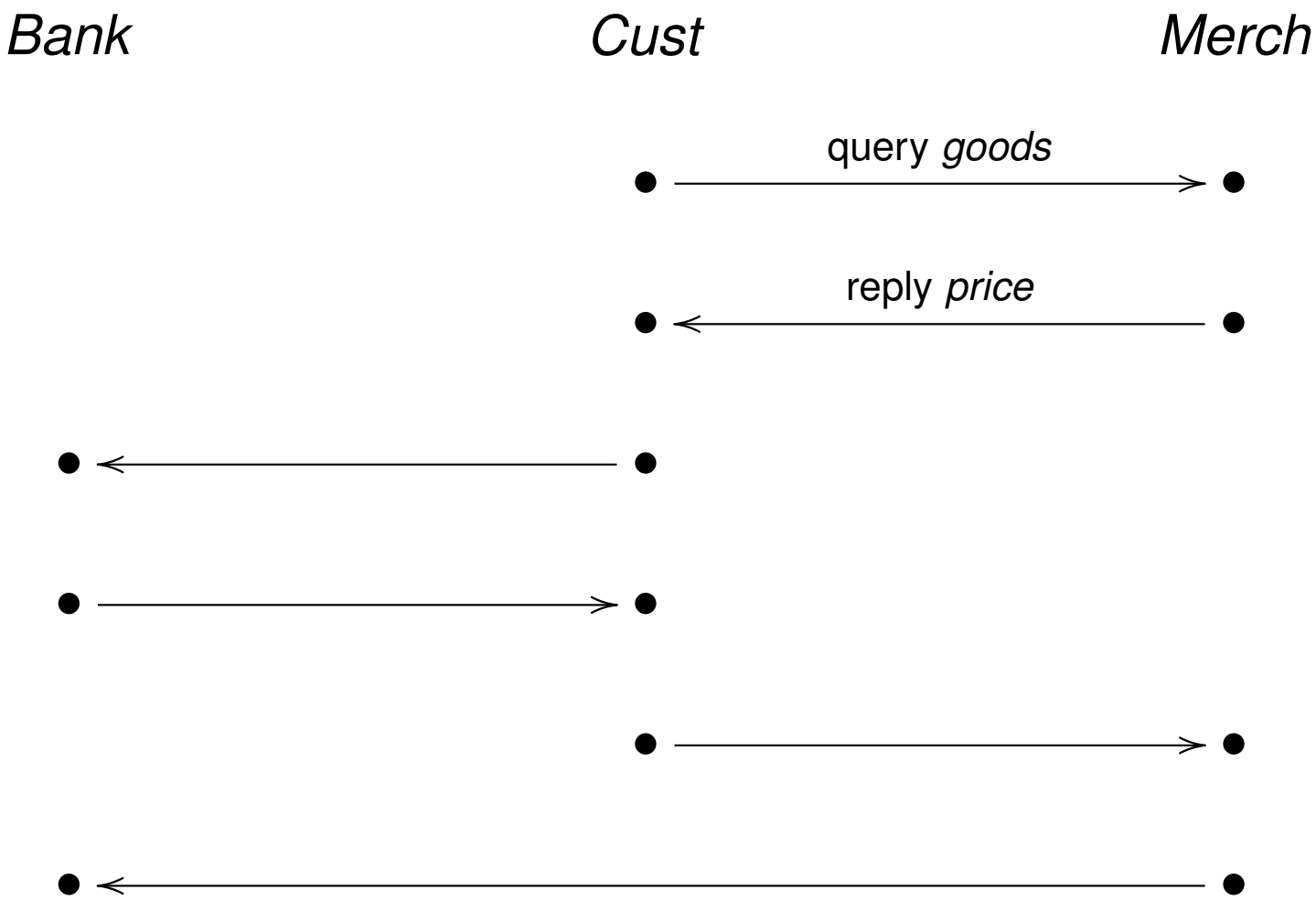
Electronic Purchase

Using a money order: *EPMO*



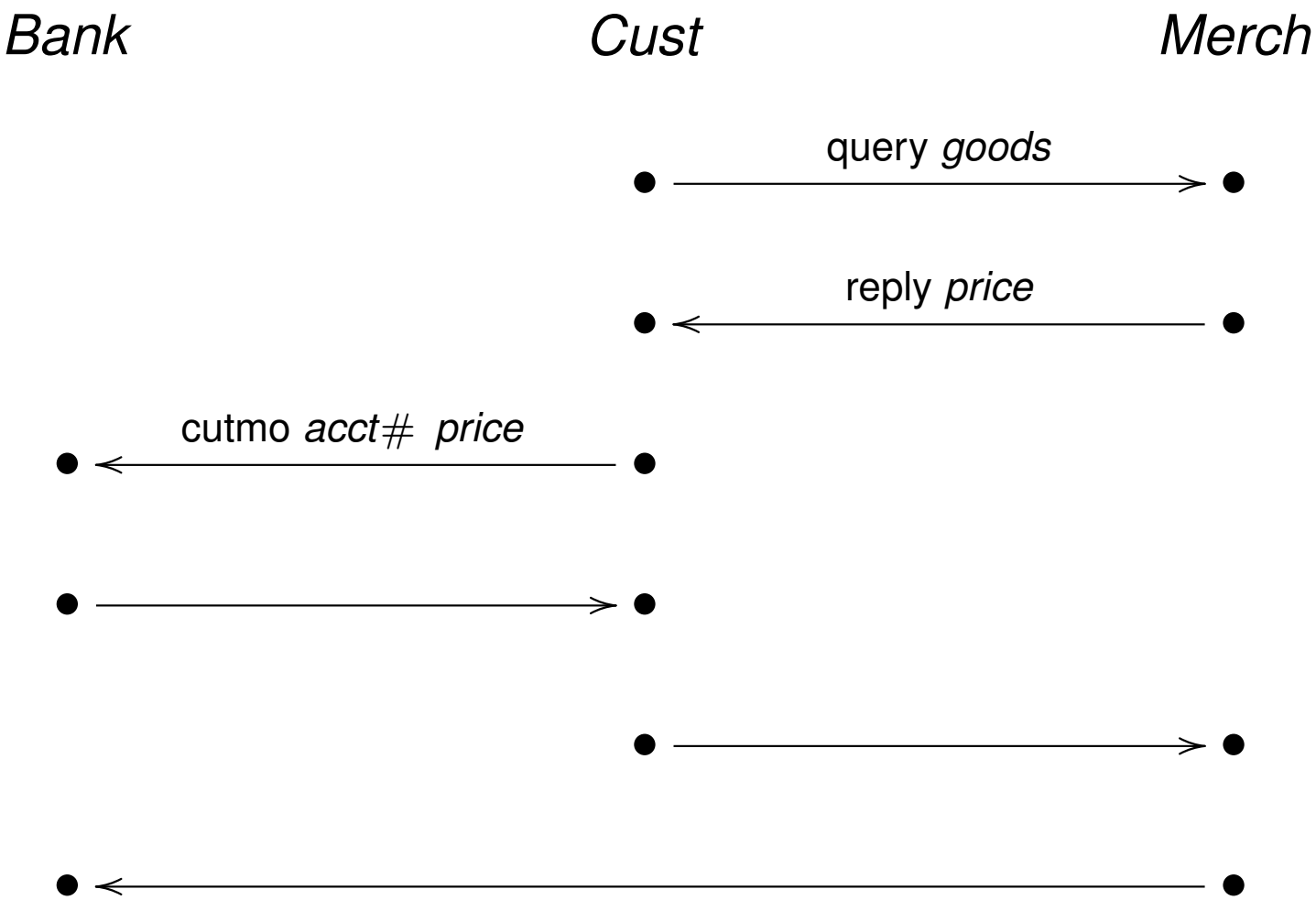
Electronic Purchase

Using a money order: *EPMO*



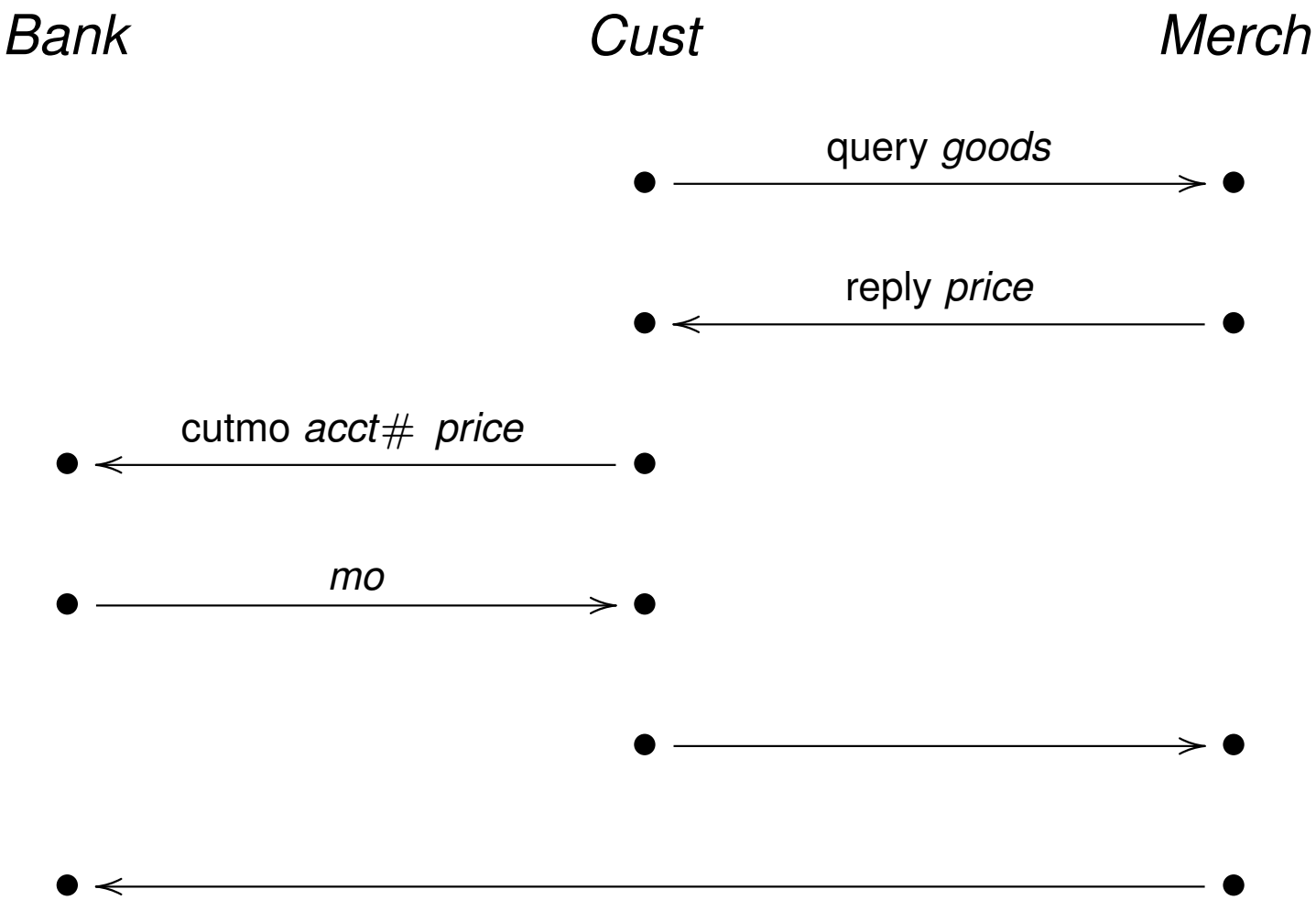
Electronic Purchase

Using a money order: *EPMO*



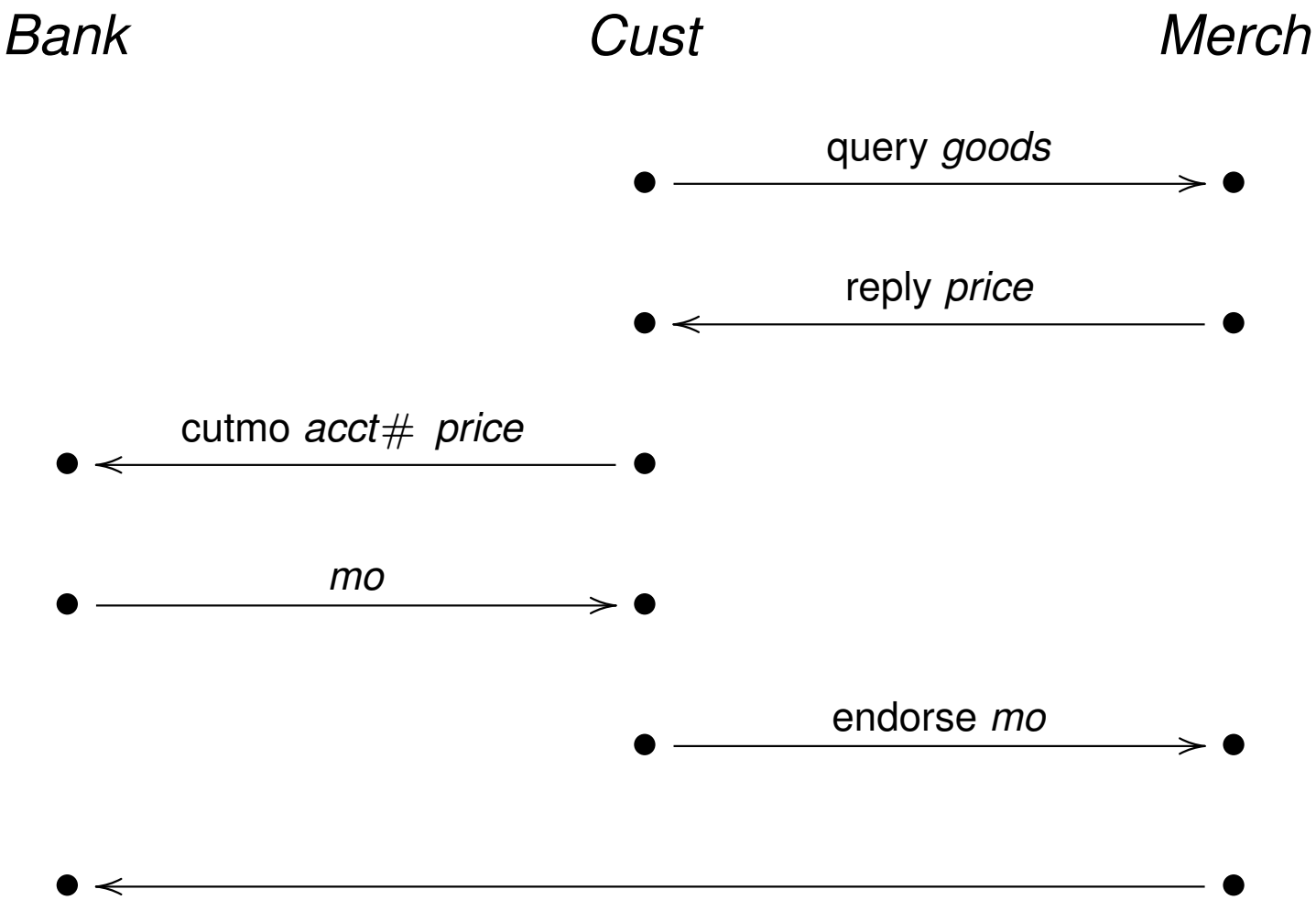
Electronic Purchase

Using a money order: *EPMO*



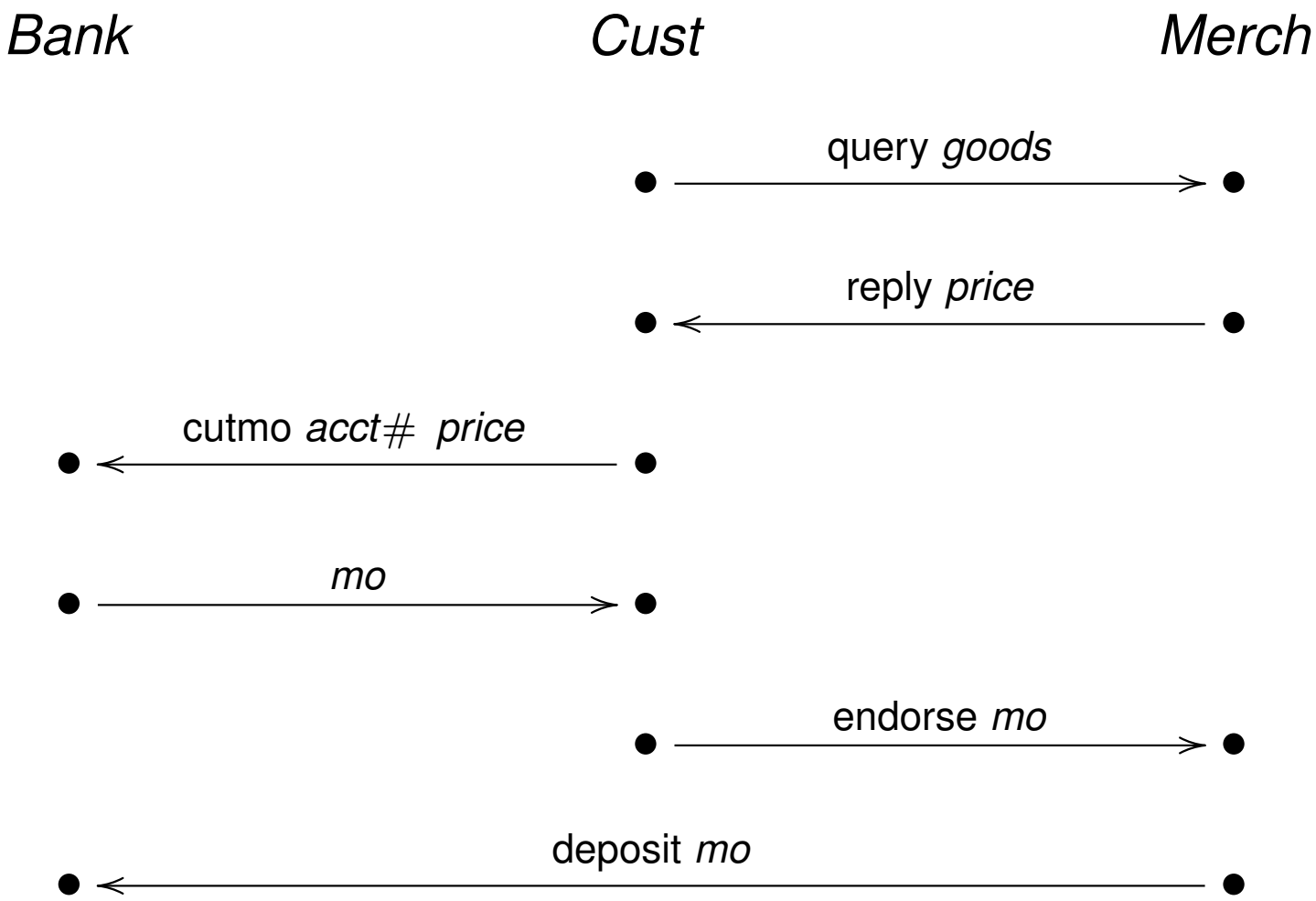
Electronic Purchase

Using a money order: *EPMO*



Electronic Purchase

Using a money order: *EPMO*



EPMO Goals

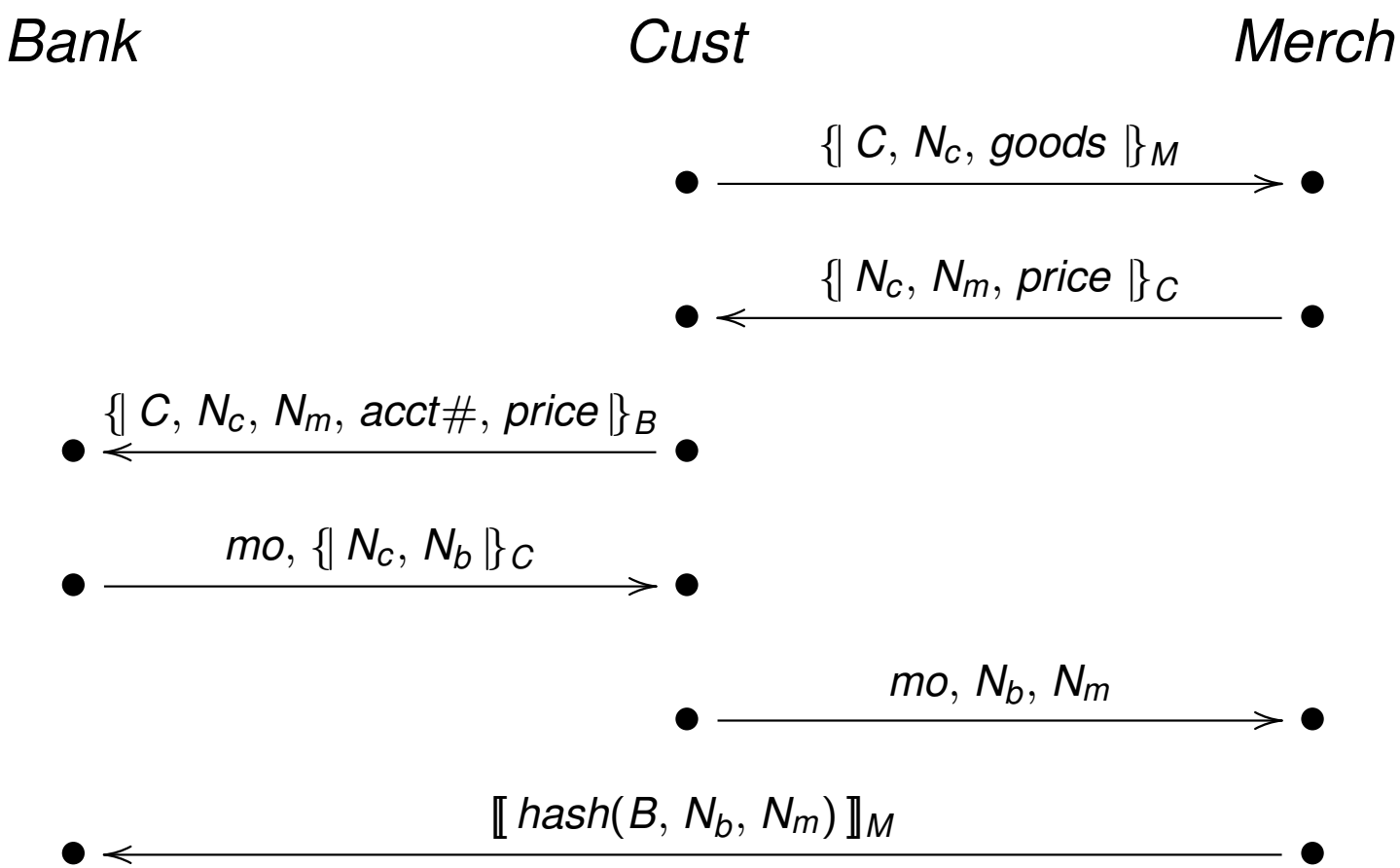
- *Cust*, *Merch*, *Bank* agree on:
  - principal identities
  - *price*
- *Cust*, *Merch* agree on *goods*
- *Cust*, *Bank* agree on *acct#*
- Beyond that, full confidentiality

$EPMO_1$

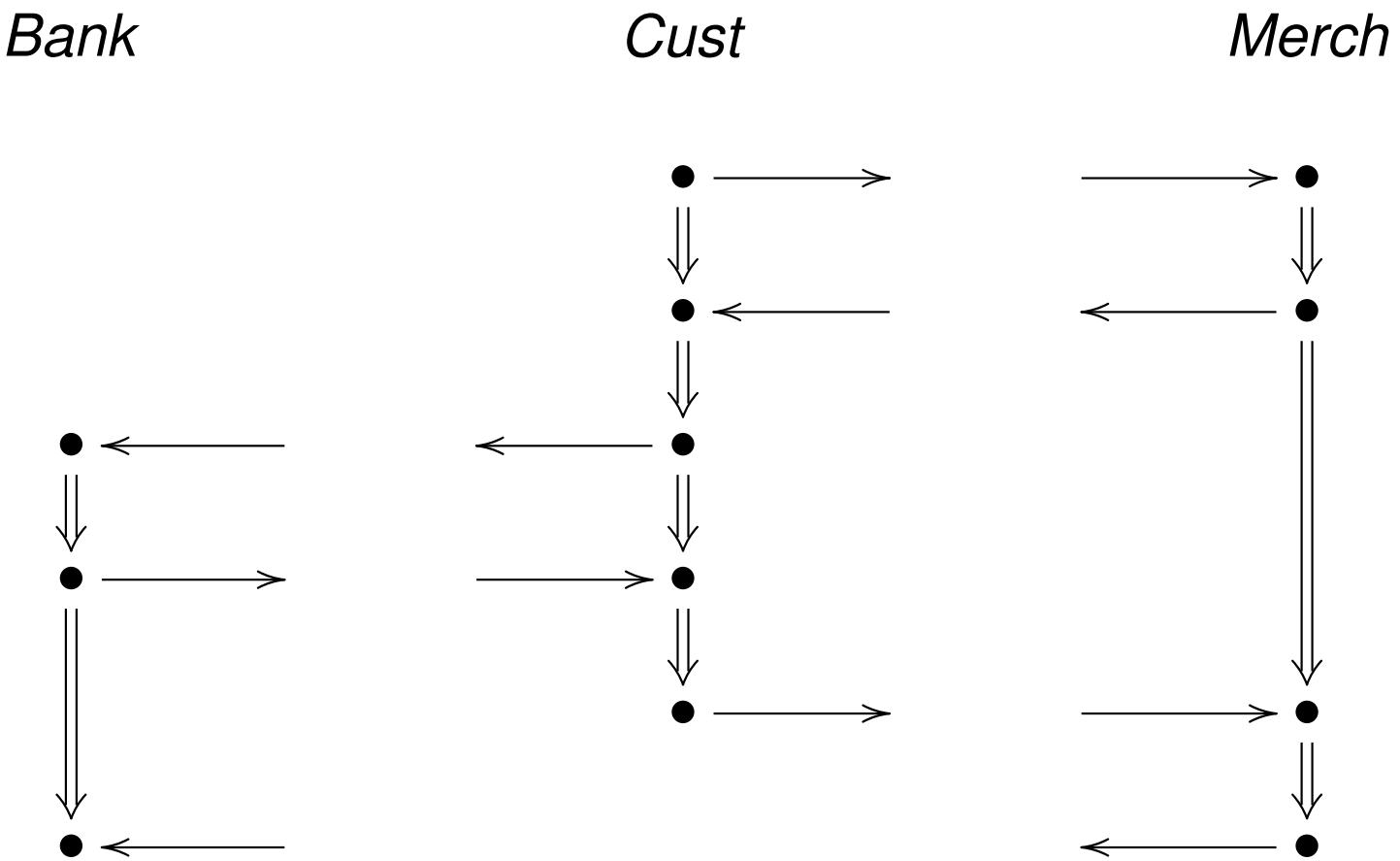
$\{\!|\ -\ |\!\}_P$ means encr. with P's public key

$[\![-]\!]_P$ means digital signature

$mo = [\![\, hash(C,\ N_c,\ N_b,\ N_m,\ price)\,]\!]_B$

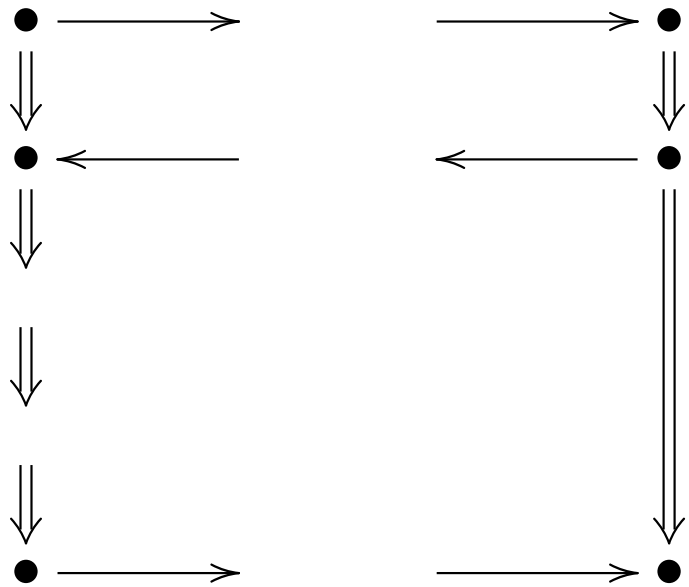


The Strand Space point of view

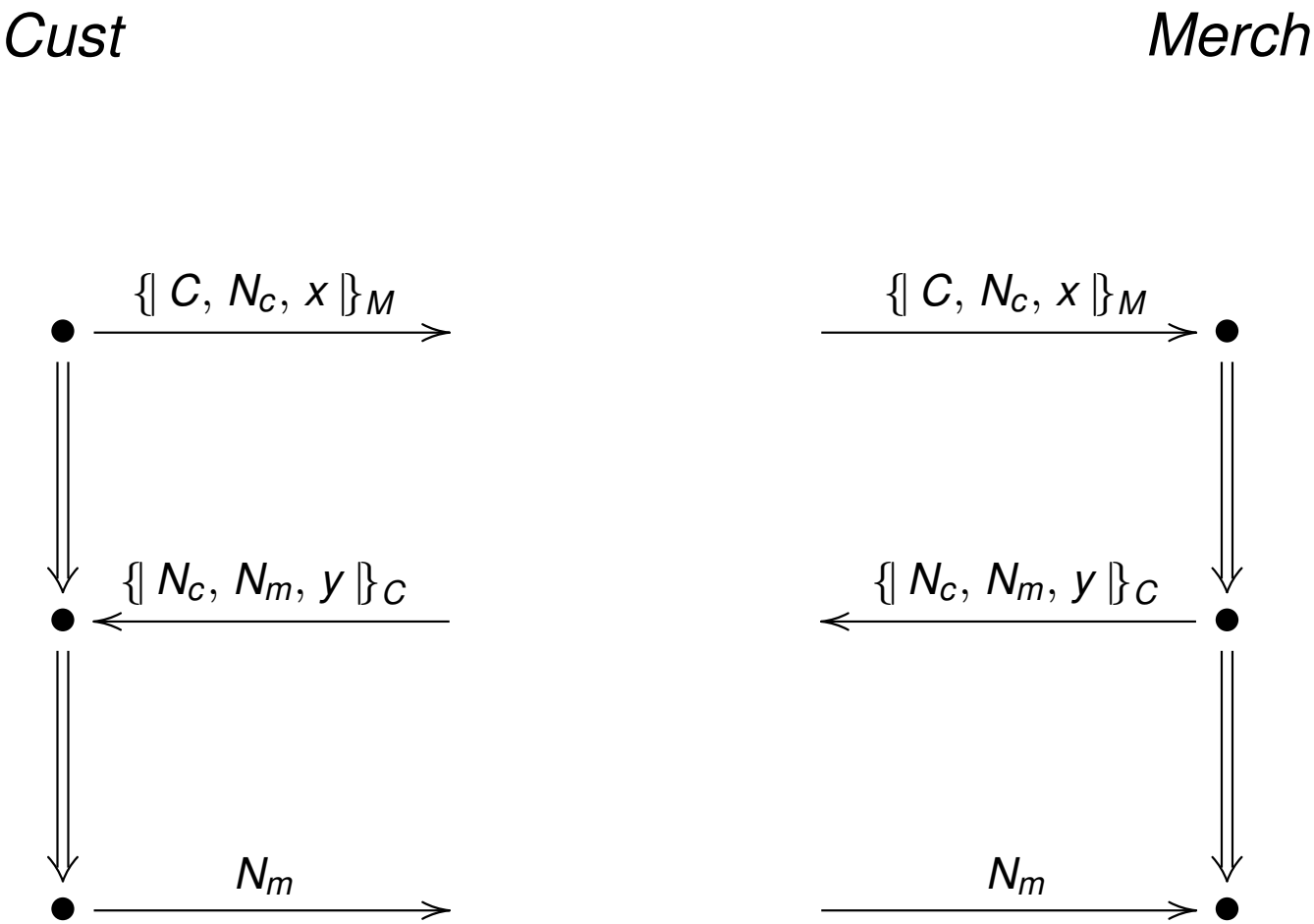


Simplification: Customer-merchant subprotocol

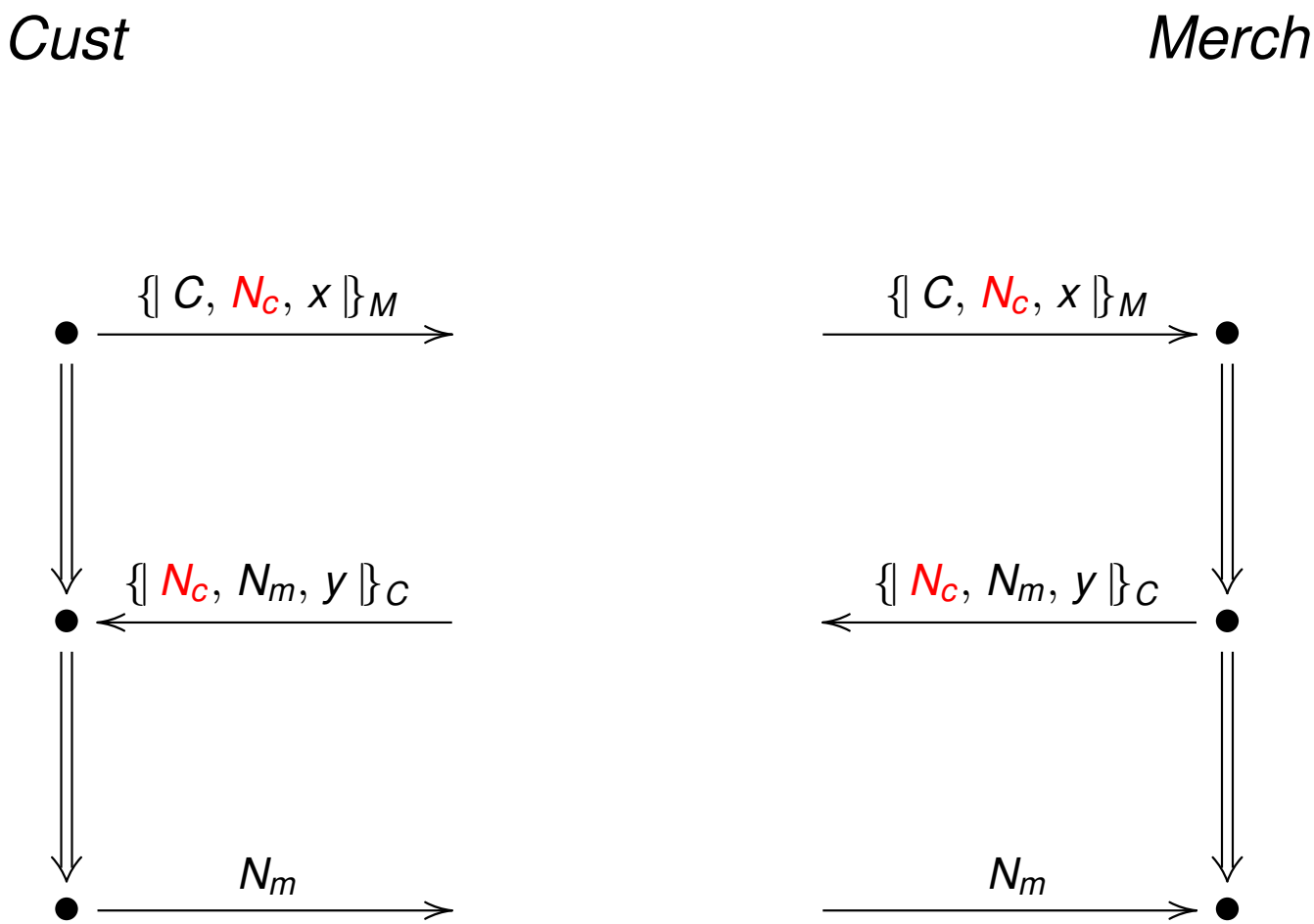
Bank *Cust* *Merch*



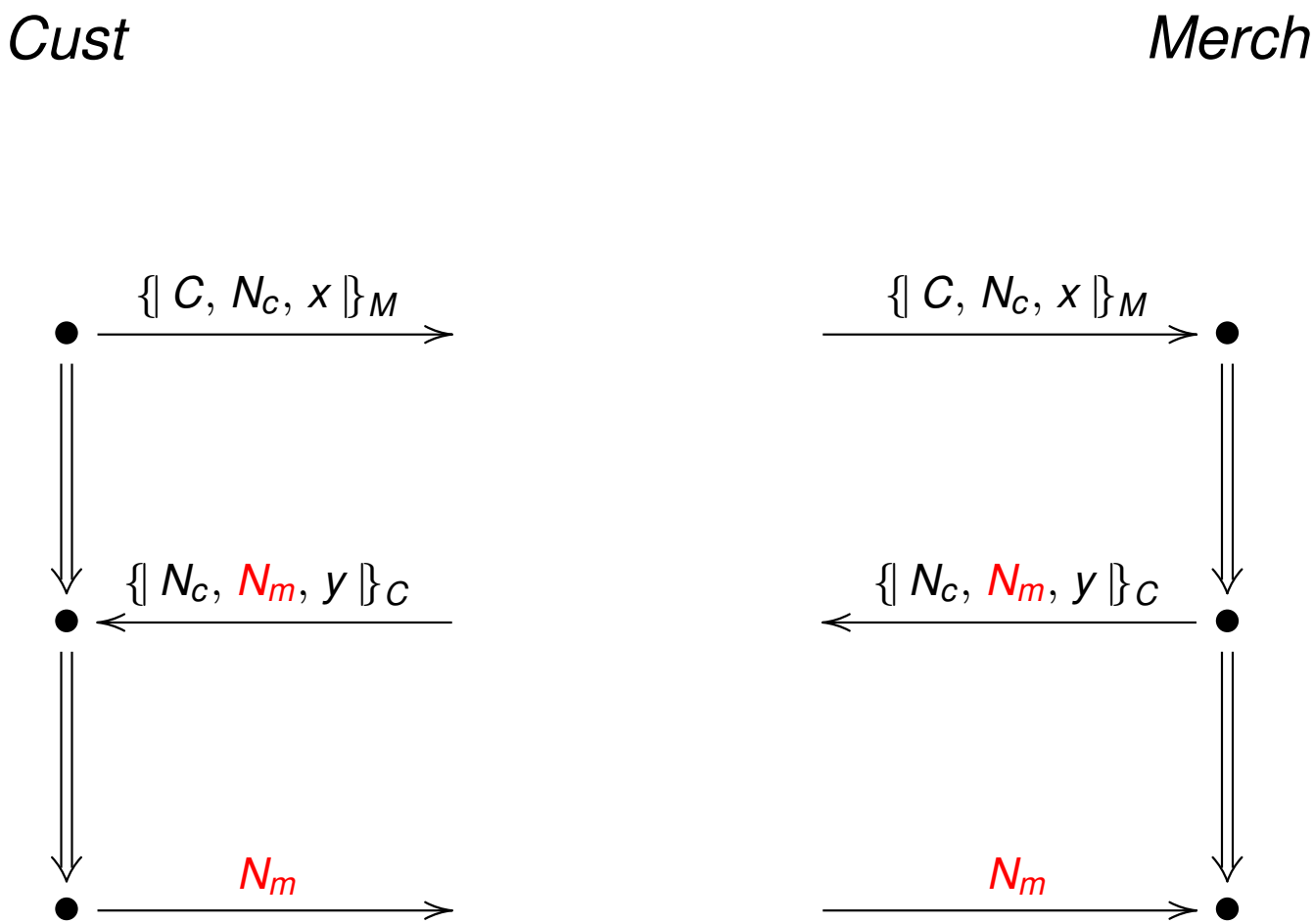
$EPMO_1$ customer-merchant subprotocol



$EPMO_1$: How customer tests merchant



$EPMO_1$: How merchant tests customer

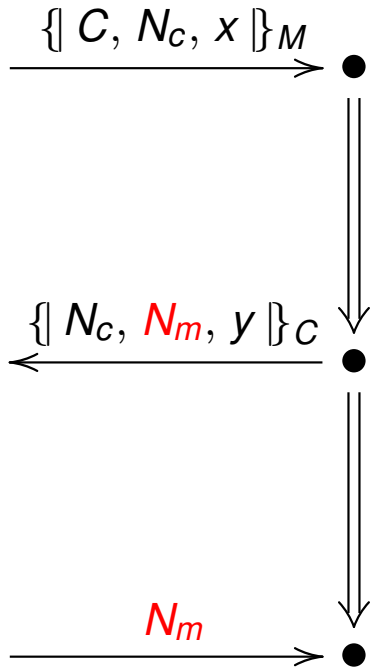


Nonce sent encrypted

Authentication test pattern

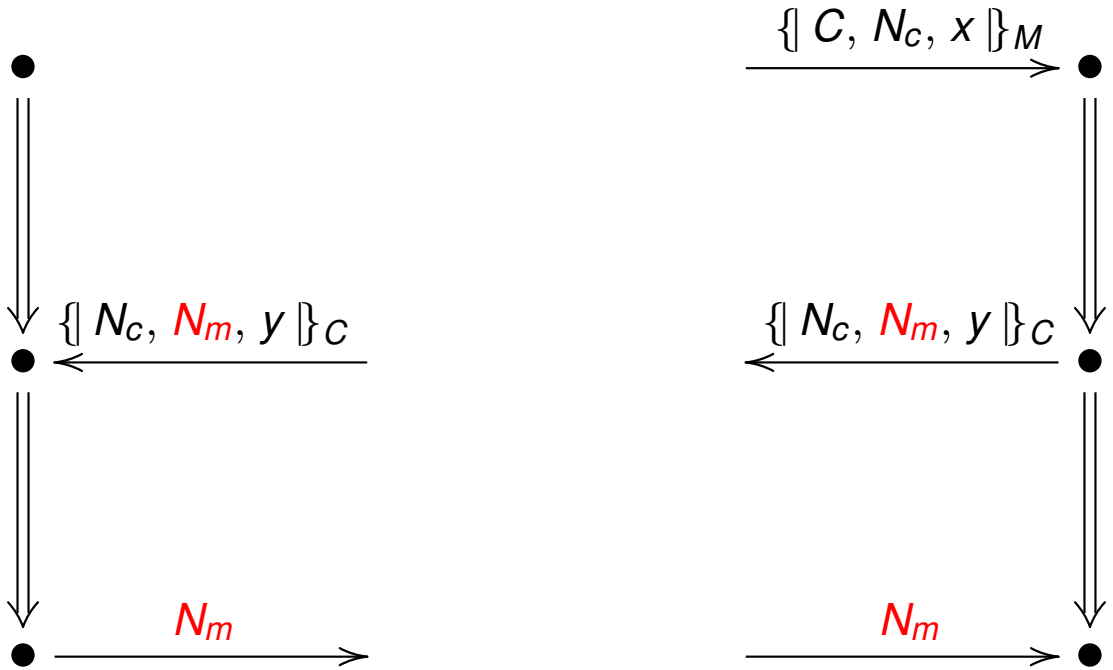
- When a freshly chosen value N is:
  - Sent inside encryption
    $$\{\!|\ \cdots N \cdots\ |\!\}_K$$
  - Received later outside this form
- Infer: either
  - Decryption key K^{-1} is compromised, or else
  - A regular participant received
    $$\{\!|\ \cdots N \cdots\ |\!\}_K$$
    and retransmitted N in another form

$EPMO_1$: What does the merchant learn?



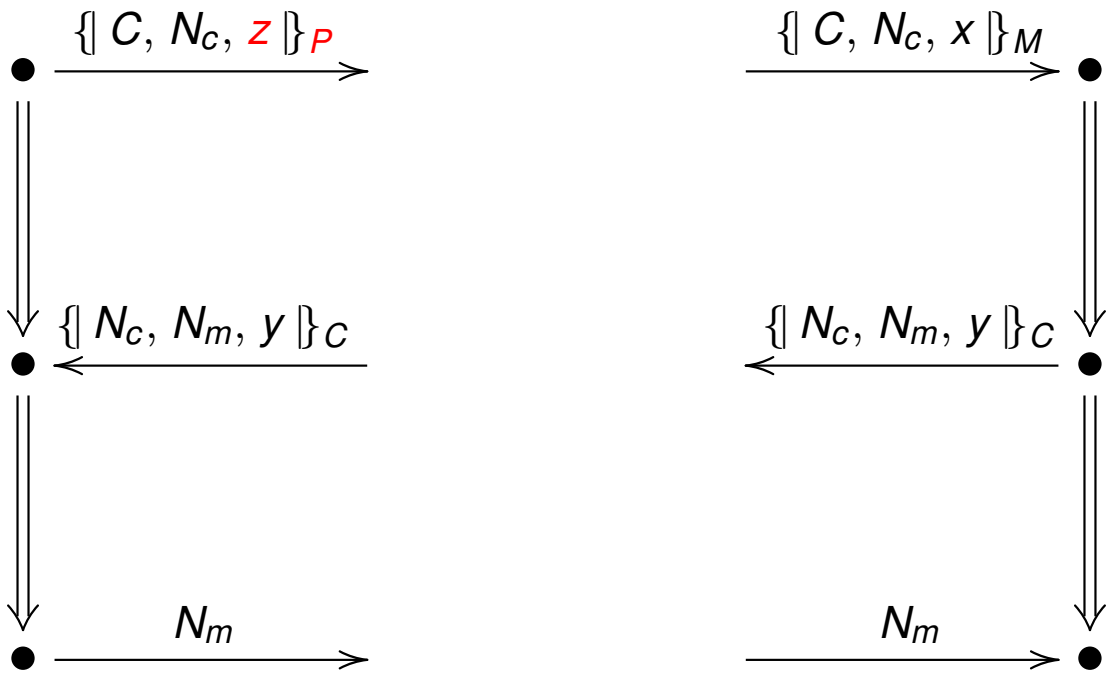
$EPMO_1$: What does the merchant learn?

If N_m freshly chosen, C's decryption key uncompromised

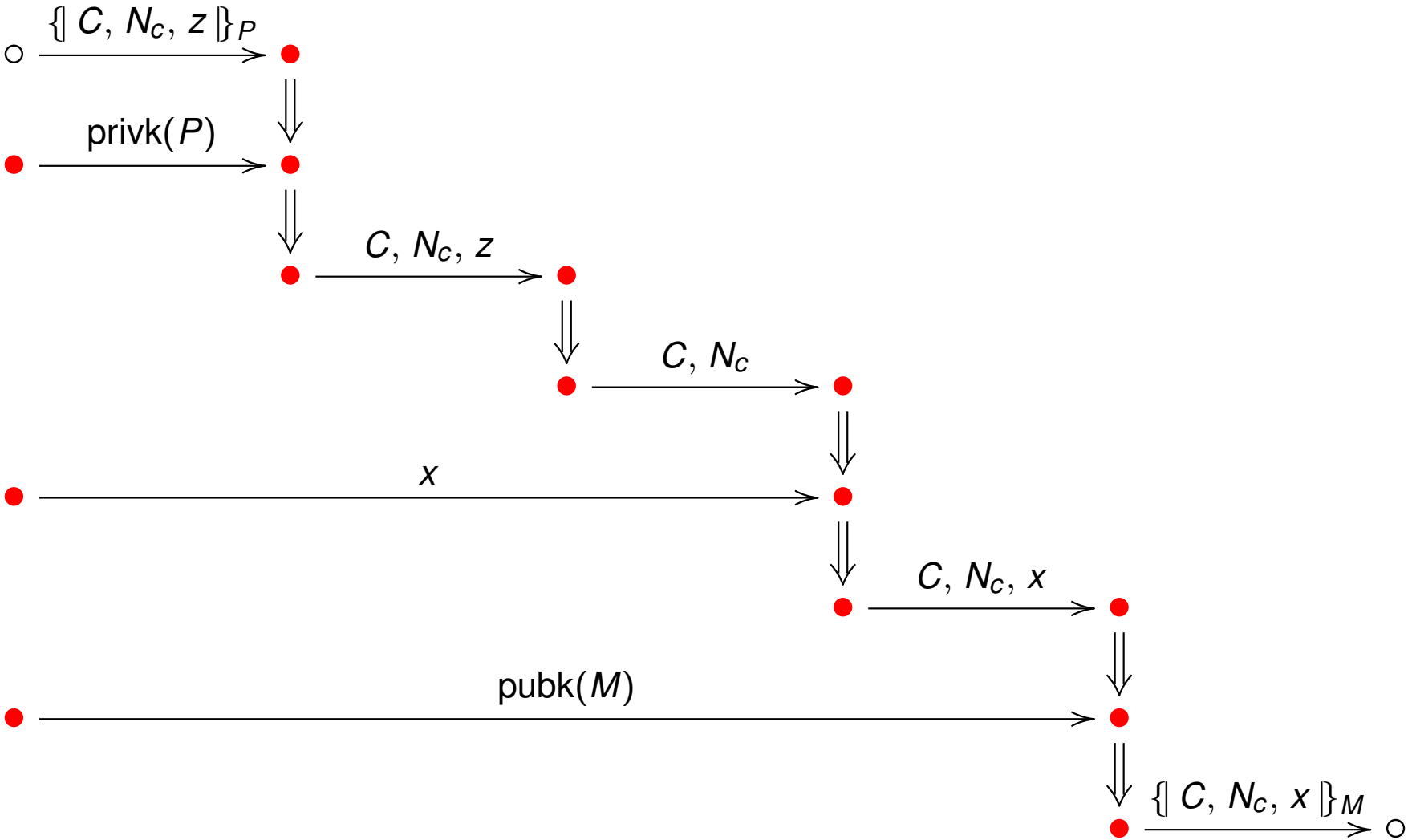


$EPMO_1$: What does the merchant learn?

If N_m freshly chosen, C's decryption key uncompromised

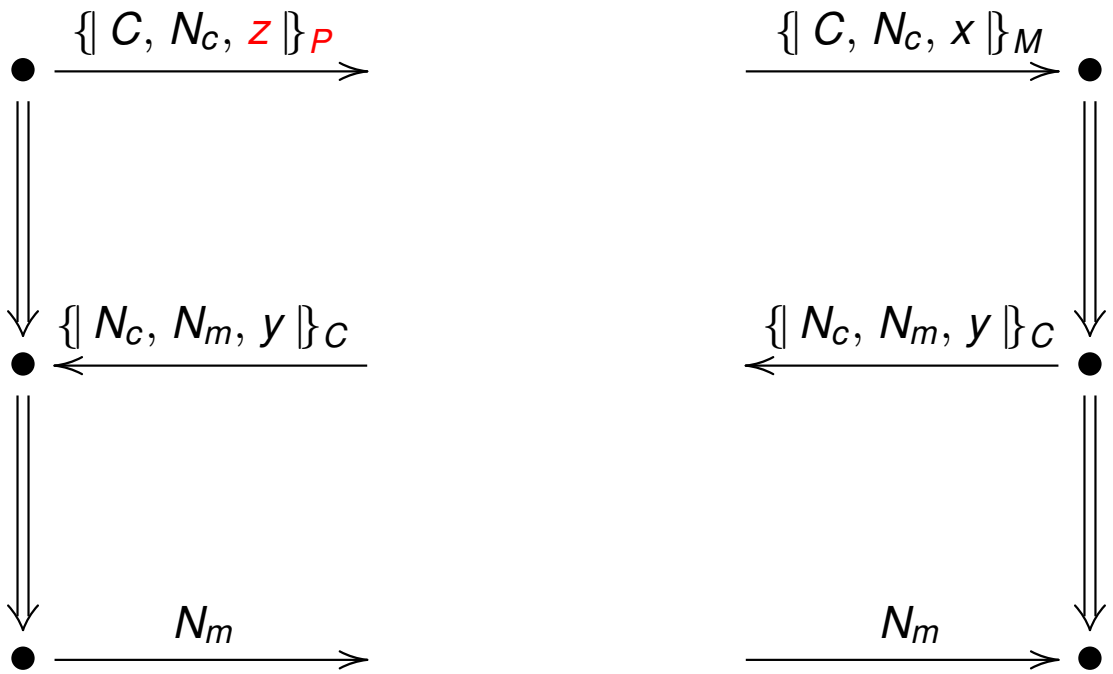


$EPMO_1$: How this is possible

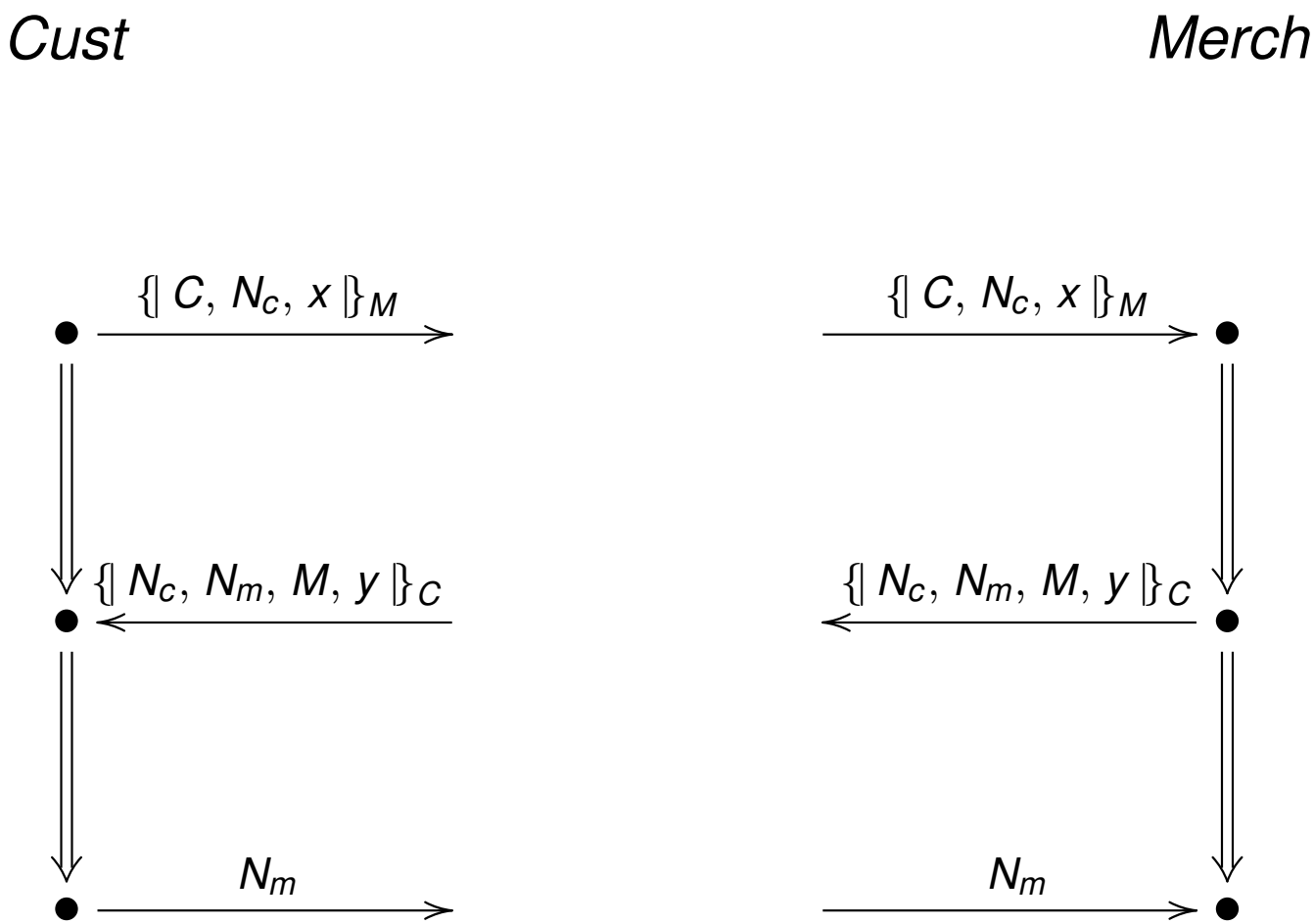


$EPMO_1$: What does the merchant learn?

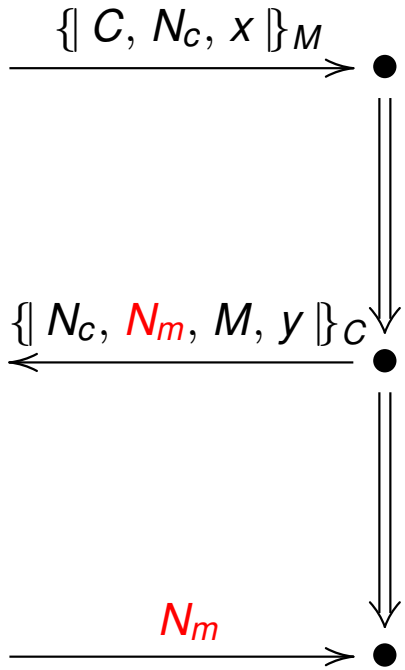
If N_m freshly chosen, C's decryption key uncompromised



$EPMO_2$ customer-merchant subprotocol

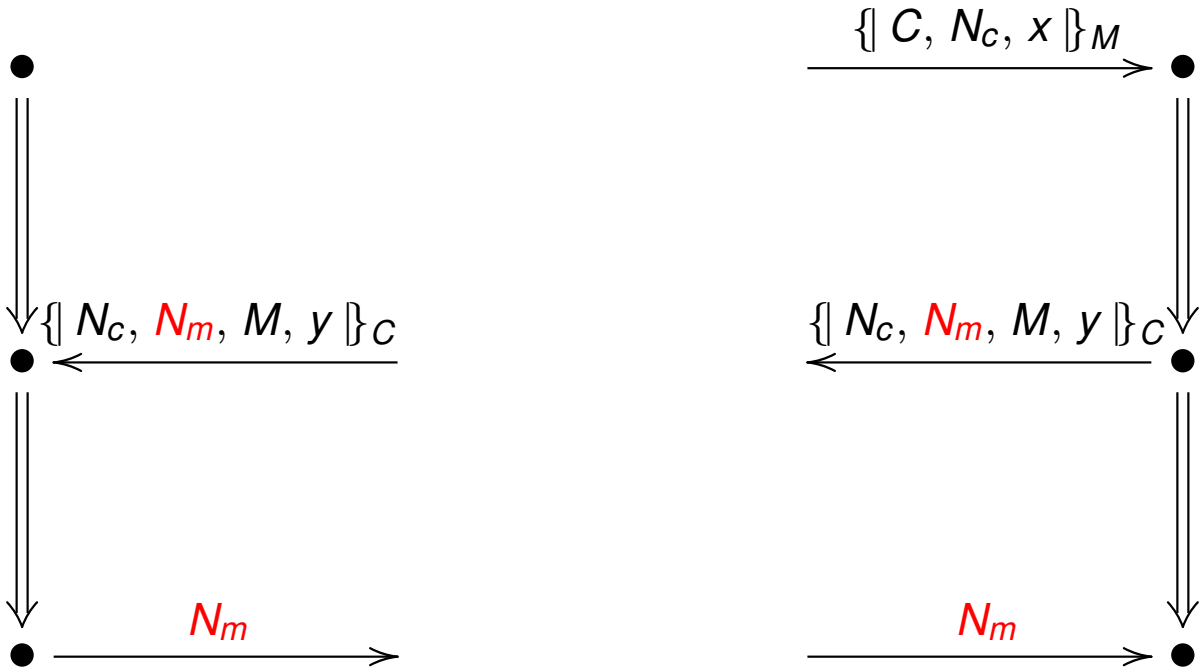


$EPMO_2$: What does the merchant learn?



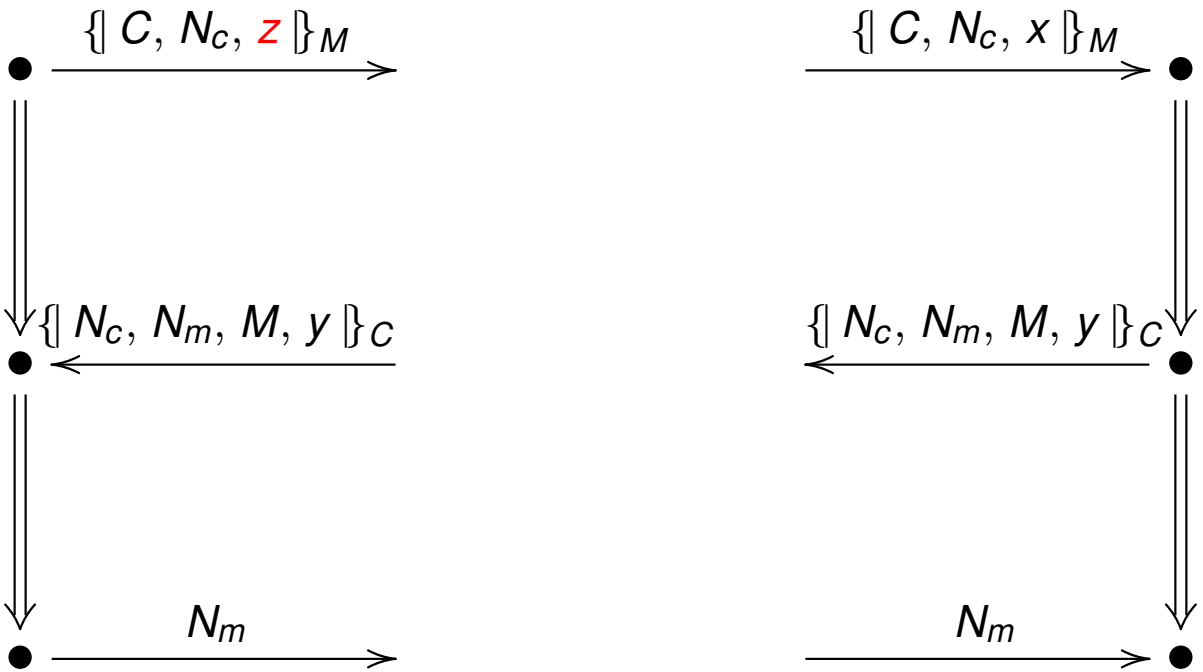
$EPMO_2$: What does the merchant learn?

If N_m freshly chosen, C's decryption key uncompromised



$EPMO_2$: What does the merchant learn?

If N_m freshly chosen, C's decryption key uncompromised

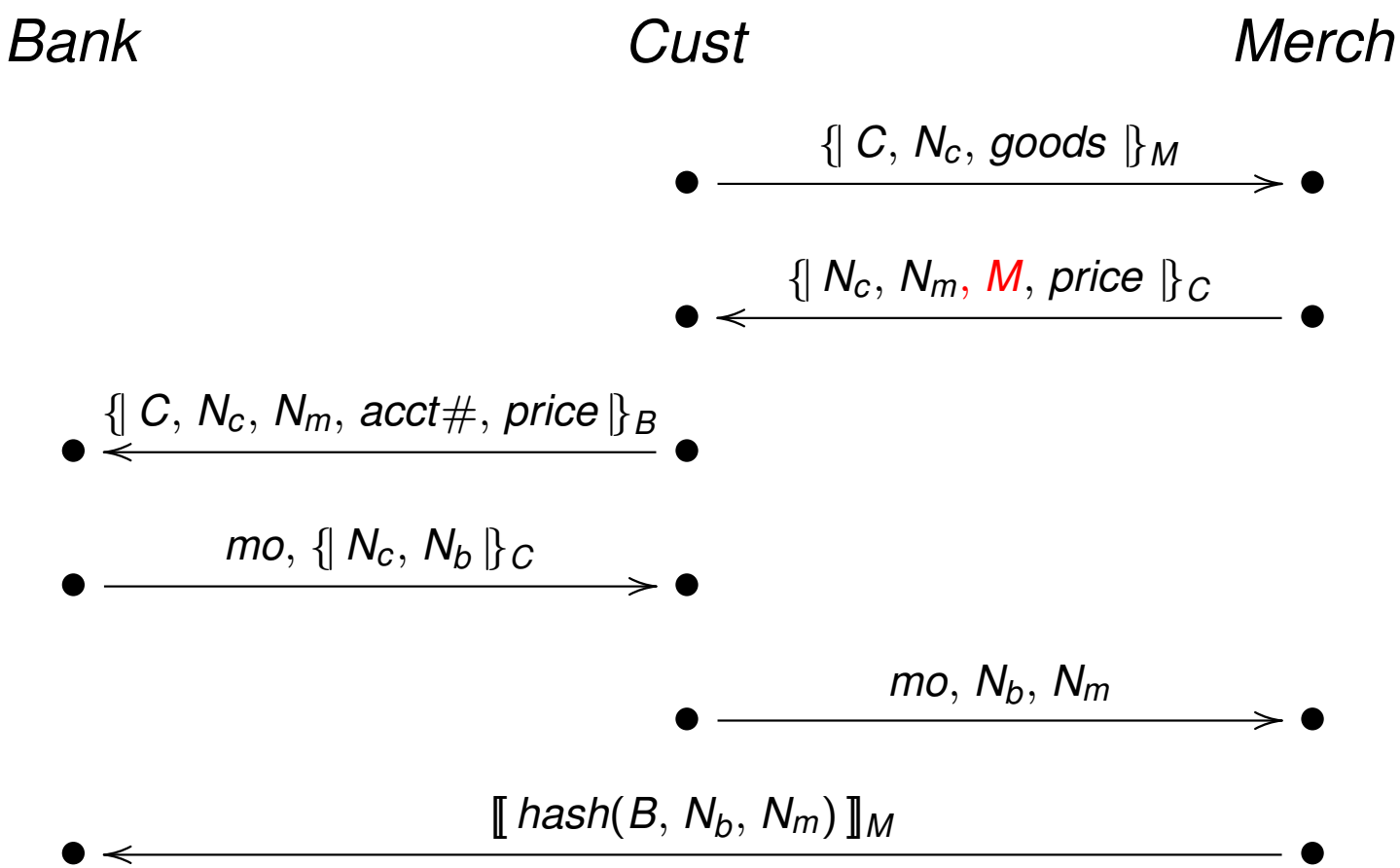


$EPMO_2$

$\{\!|\ -\ |\!\}_P$ means encr. with P's public key

$[\![-]\!]_P$ means digital signature

$mo = [\![\, hash(C,\ N_c,\ N_b,\ N_m,\ price)\,]\!]_B$



Small denotational semantics

For crypto protocols

- Skeletons $\mathbb{A}$:
  - Partial executions (see previous slides)
  - Some skeletons are *realized*

Small denotational semantics

For crypto protocols

- Skeletons $\mathbb{A}$:
  - Partial executions (see previous slides)
  - Some skeletons are *realized*
- Homomorphisms H:
  Structure-preserving maps

$$H : \mathbb{A} \mapsto \mathbb{B}$$

Small denotational semantics

For crypto protocols

- Skeletons $\mathbb{A}$:
  - Partial executions (see previous slides)
  - Some skeletons are *realized*
- Homomorphisms H:
  Structure-preserving maps

$$H : \mathbb{A} \mapsto \mathbb{B}$$

- Test-solving transition relation:

$$\mathbb{A} \rightsquigarrow \mathbb{B}$$

Small denotational semantics

For crypto protocols

- Skeletons $\mathbb{A}$:
  - Partial executions (see previous slides)
  - Some skeletons are *realized*
- Homomorphisms H:
  Structure-preserving maps

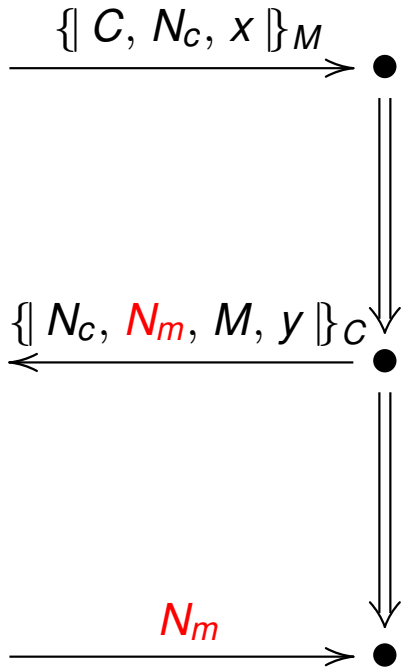
$$H : \mathbb{A} \mapsto \mathbb{B}$$

- Test-solving transition relation:

$$\mathbb{A} \rightsquigarrow \mathbb{B}$$

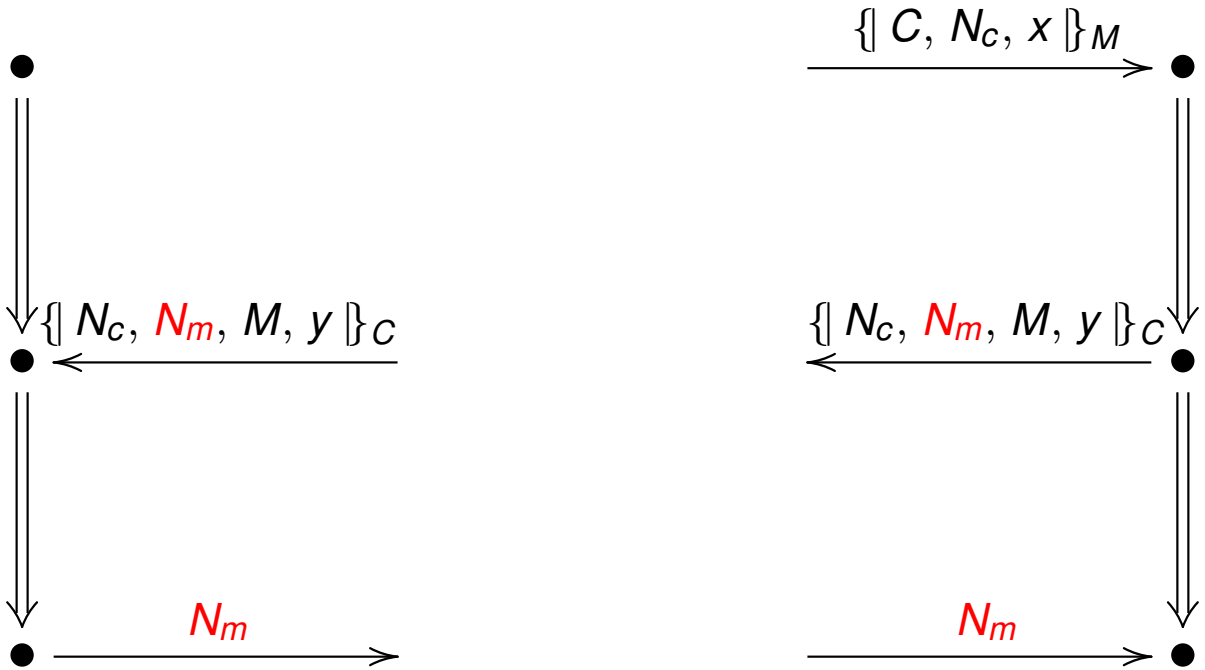
$\mathbb{A}$ is realized iff every test in $\mathbb{A}$ is solved

$EPMO_2$: What does the merchant learn?



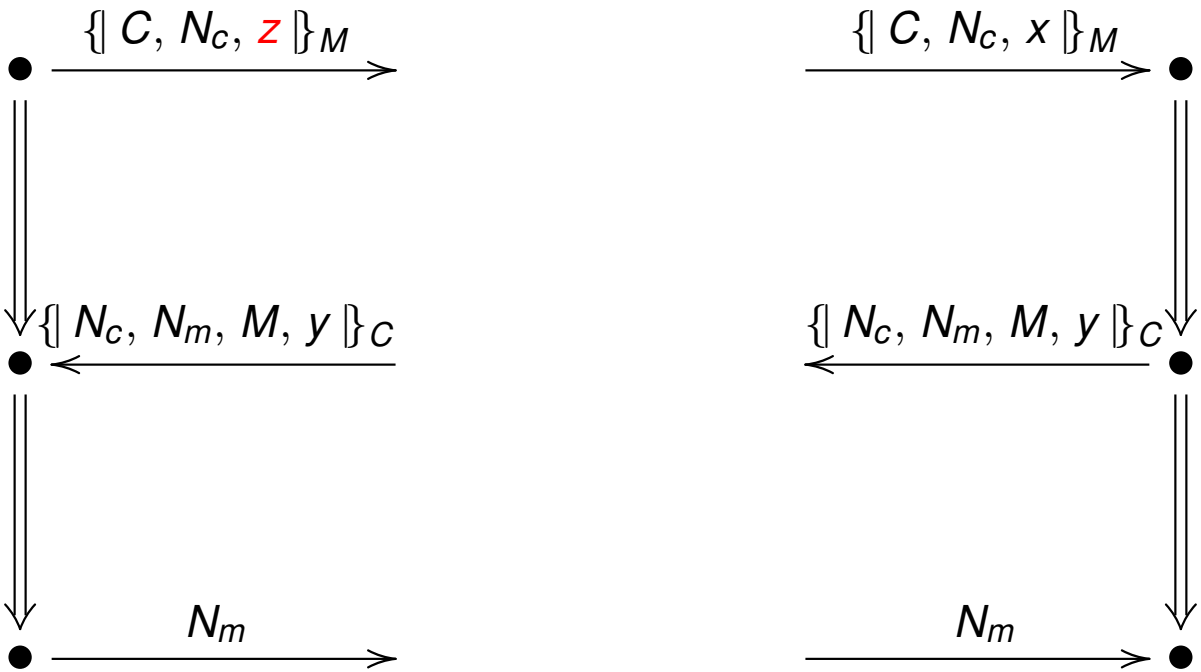
$EPMO_2$: What does the merchant learn?

If N_m freshly chosen, C's decryption key uncompromised



$EPMO_2$: What does the merchant learn?

If N_m freshly chosen, C's decryption key uncompromised



Three key facts

- $\mathbb{A} \rightsquigarrow \mathbb{B}$ implies

$$H\colon \mathbb{A} \mapsto \mathbb{B}$$

for some H

Three key facts

- $\mathbb{A} \rightsquigarrow \mathbb{B}$ implies

$$H\colon \mathbb{A} \mapsto \mathbb{B}$$

  for some H
- $\mathbb{A}$ is realized implies in LTS

$$\mathbb{A} \sim / \rightsquigarrow$$

Three key facts

- $\mathbb{A} \rightsquigarrow \mathbb{B}$ implies

$$H\colon \mathbb{A} \mapsto \mathbb{B}$$

  for some H
- $\mathbb{A}$ is realized implies in LTS

$$\mathbb{A} \sim / \rightsquigarrow$$

- Suppose $\mathbb{A}_0 \mapsto \mathbb{A}$ and $\mathbb{A}$ is realized.
  Then for some realized $\mathbb{A}_1$,

$$\mathbb{A}_0 \rightsquigarrow^* \mathbb{A}_1 \quad \text{and} \quad \mathbb{A}_1 \mapsto \mathbb{A}$$

Application-specific crypto protocols

Three claims

- Central to secure distributed systems
- Analysis uses two basic principles: authentication tests
  - Formalized in a small denotational semantics
  - Analysis tool CPSA
- Authentication tests also suggest systematic protocol design methods