Cryptographic Protocol Design via the Authentication Tests

Joshua Guttman

The MITRE Corporation

Thanks to the MITRE-Sponsored Research program

Protocol Exchange
January 2008

Elaborating protocols

- Protocols constructed by superimposing germ protocols

Elaborating protocols

- Protocols constructed by superimposing germ protocols
  - Superimpose: map roles of germs into elaborated roles
  - Soundness: map shapes of germs into elaborated shapes
  - Preserve authentication and secrecy goals

Elaborating protocols

- Protocols constructed by superimposing germ protocols
  - Superimpose: map roles of germs into elaborated roles
  - Soundness: map shapes of germs into elaborated shapes
  - Preserve authentication and secrecy goals
- Analysis-preserving maps
  - Analysis: authentication tests leading to shapes

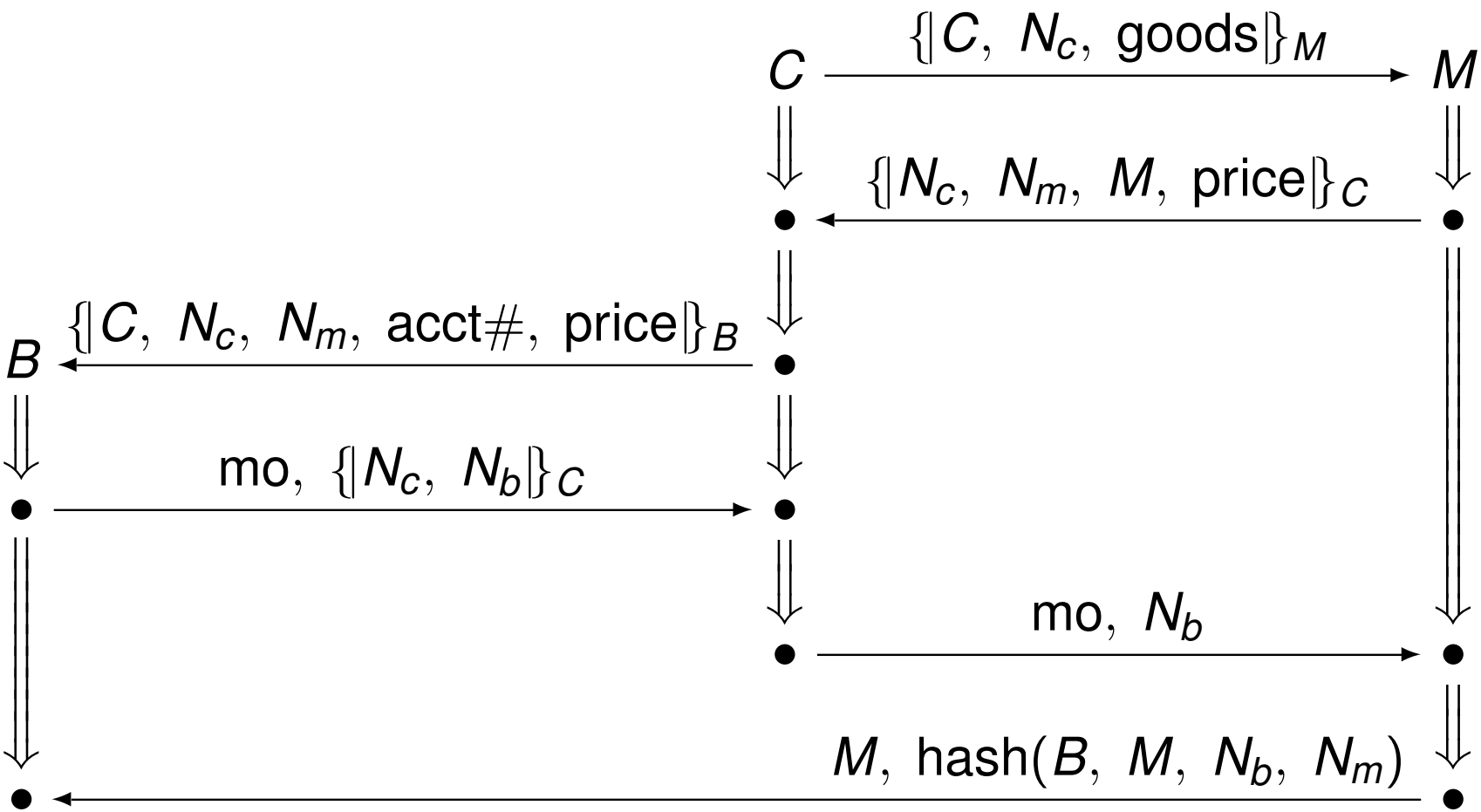
Elaborating protocols

- Protocols constructed by superimposing germ protocols
  - Superimpose: map roles of germs into elaborated roles
  - Soundness: map shapes of germs into elaborated shapes
  - Preserve authentication and secrecy goals
- Analysis-preserving maps
  - Analysis: authentication tests leading to shapes
  - Represent analysis as LTS
    - ★ Nodes: Skeletons $\mathbb{A}$
    - ★ Labeled transitions: $\mathbb{A}_0 \overset{\ell}{\rightsquigarrow} \mathbb{A}_1$ means test ℓ is
      (1) unsolved in $\mathbb{A}_0$,
      (2) solved in $\mathbb{A}_1$,
      (3) in some most general way

Elaborating protocols

- Protocols constructed by superimposing germ protocols
  - Superimpose: map roles of germs into elaborated roles
  - Soundness: map shapes of germs into elaborated shapes
  - Preserve authentication and secrecy goals
- Analysis-preserving maps
  - Analysis: authentication tests leading to shapes
  - Represent analysis as LTS
    - ★ Nodes: Skeletons $\mathbb{A}$
    - ★ Labeled transitions: $\mathbb{A}_0 \overset{\ell}{\rightsquigarrow} \mathbb{A}_1$ means test ℓ is
      (1) unsolved in $\mathbb{A}_0$,
      (2) solved in $\mathbb{A}_1$,
      (3) in some most general way
  - Analysis-preserving map: Weak bisimulation

EPMO Protocol

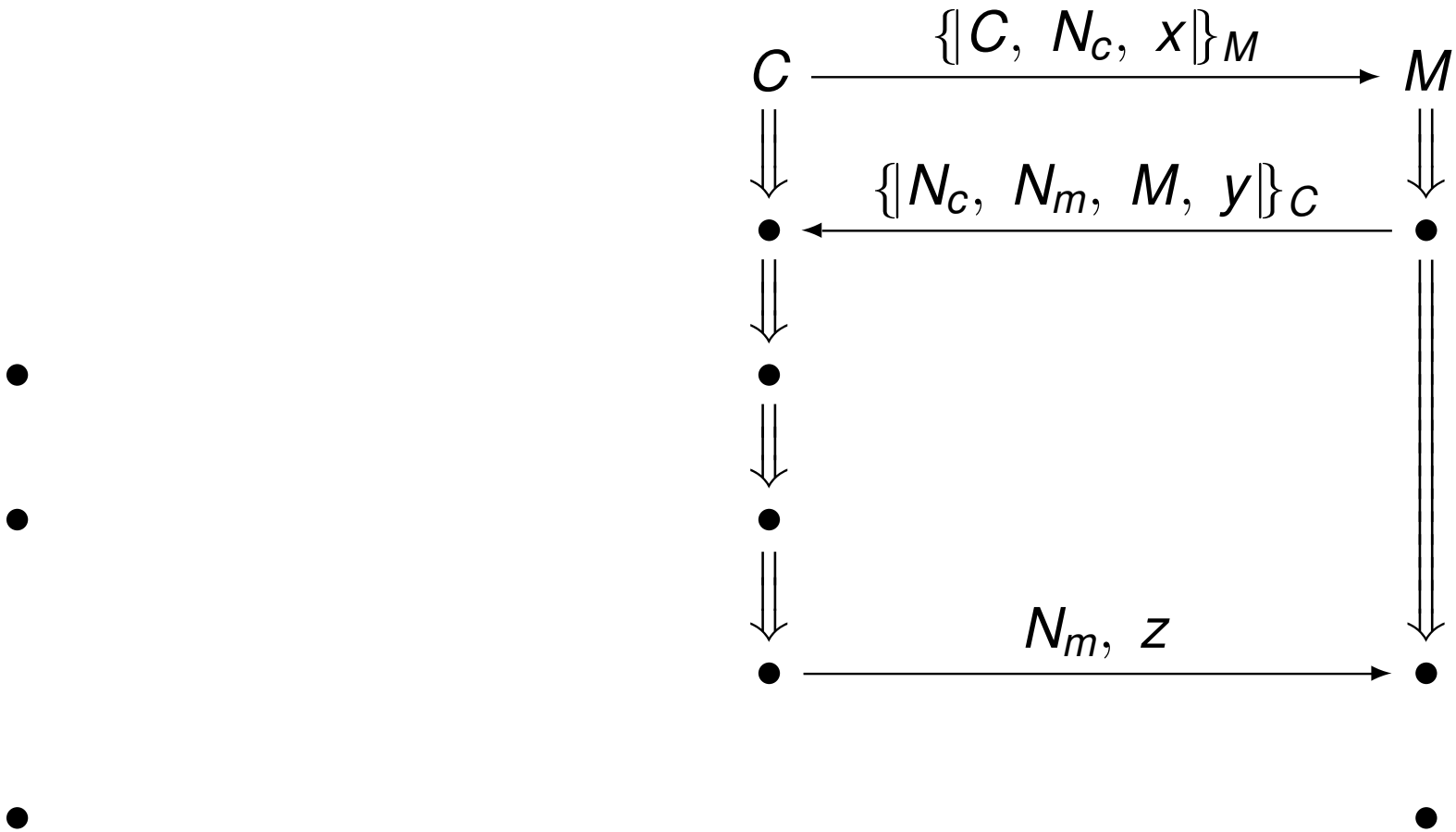


$$\text{mo} = [\![\, \text{hash}(C,\ N_c,\ N_b,\ N_m,\ \text{price}) \,]\!]_B$$

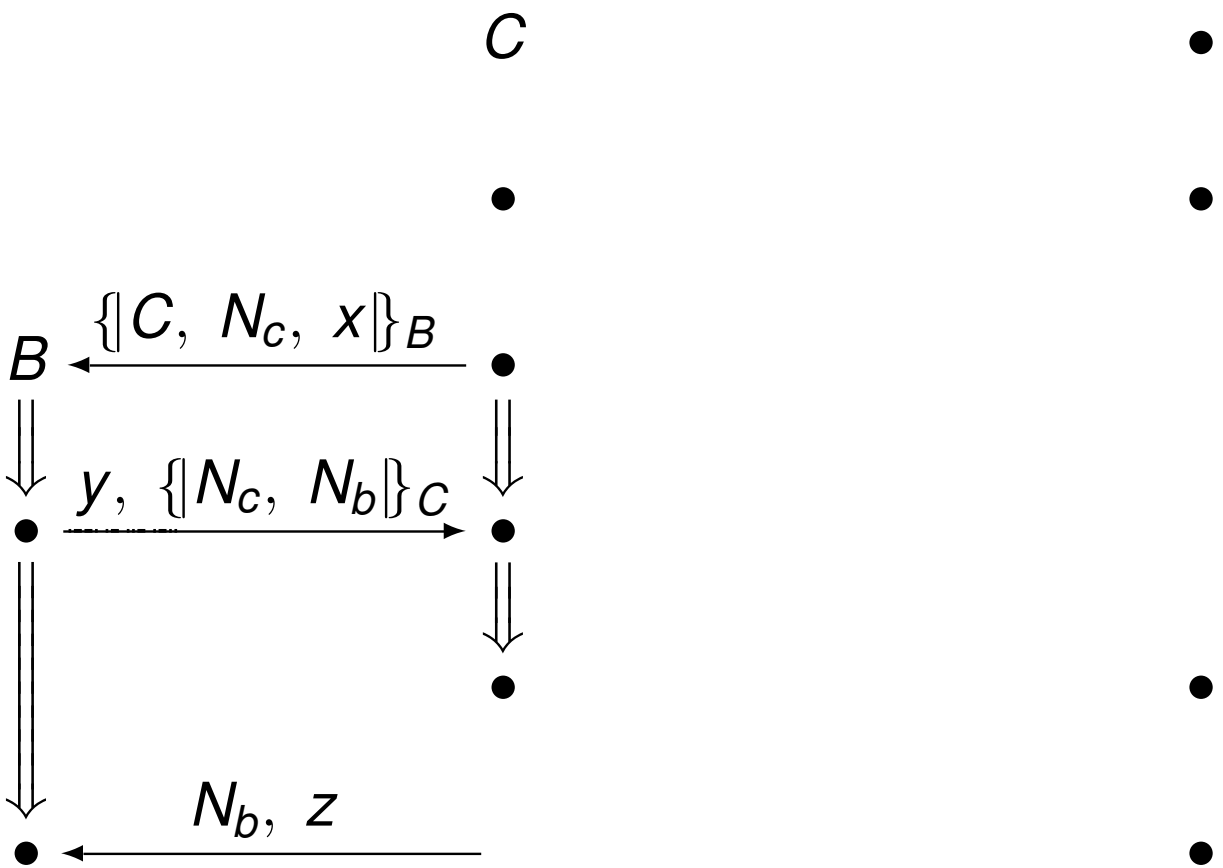
EPMO Goals

- Agree on values:
  - C, M, B agree on each other's identities and price
  - C, M agree on goods; C, B agree on account number
- Preserve confidentiality: Protect
  - C's account number from M, outsiders
  - goods from B, outsiders
  - price from outsiders
  - M's identity from B, unless C decides to complete
  - Occurrence of transaction from outsiders
- Allow decision-making:
  - C decides to spend price for goods from M
  - M decides to sell goods to C for price
  - B decides to transfer price
- Cause state change:
  - B transfers funds
  - M issues shipping order

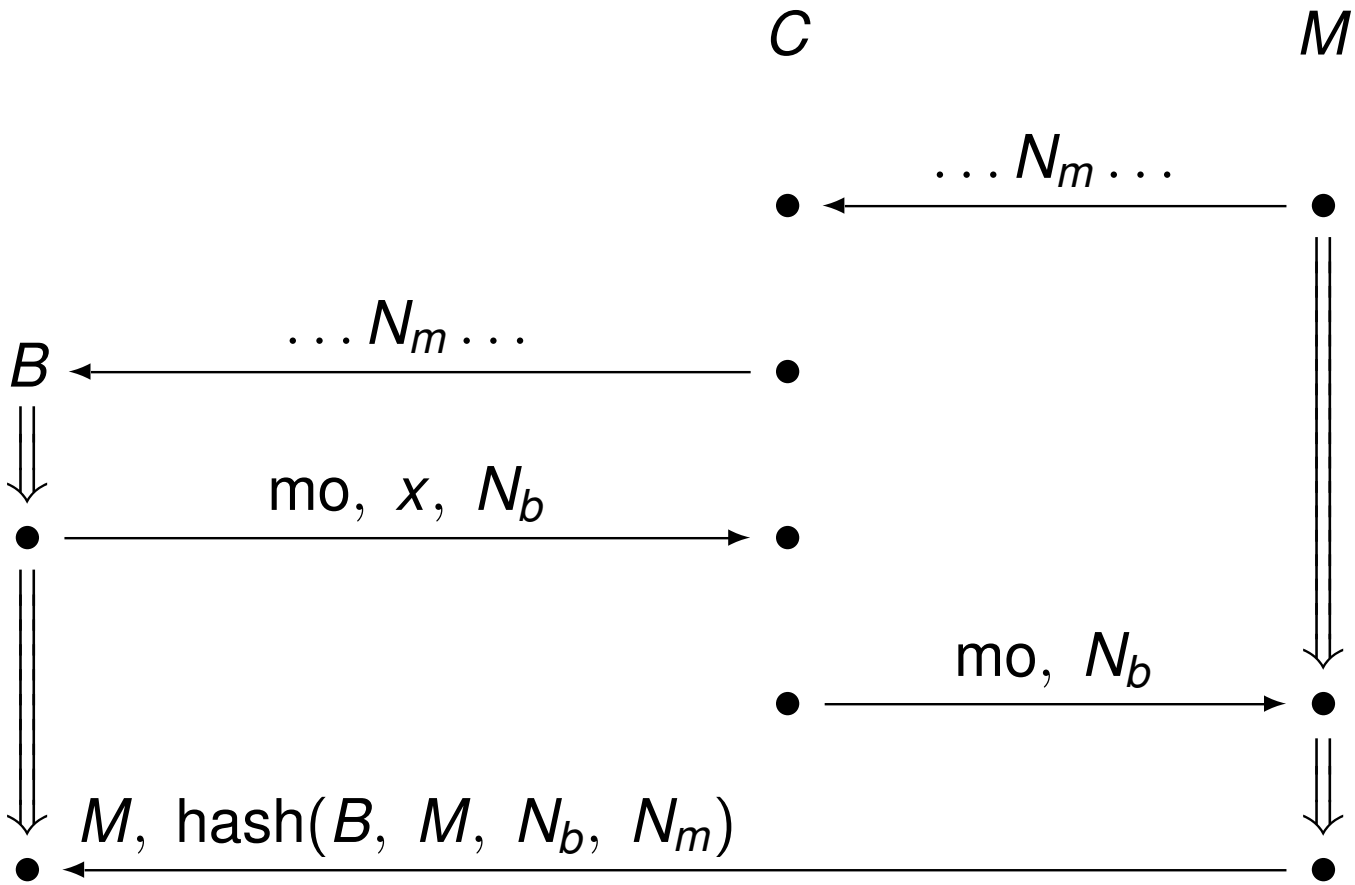
EPMO Germ 1: C/M



EPMO Germ 2: C/B

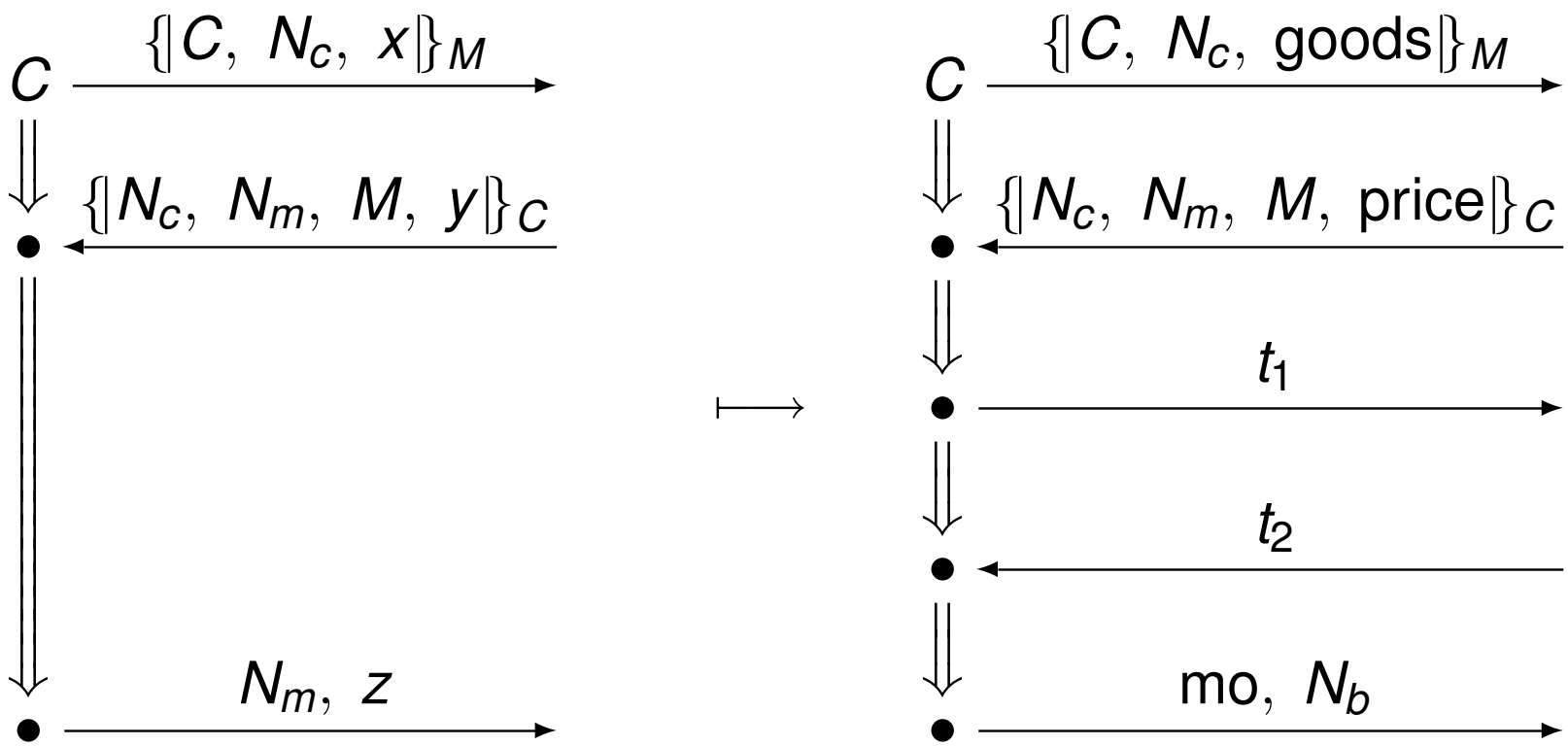


EPMO Germ 3: M/B

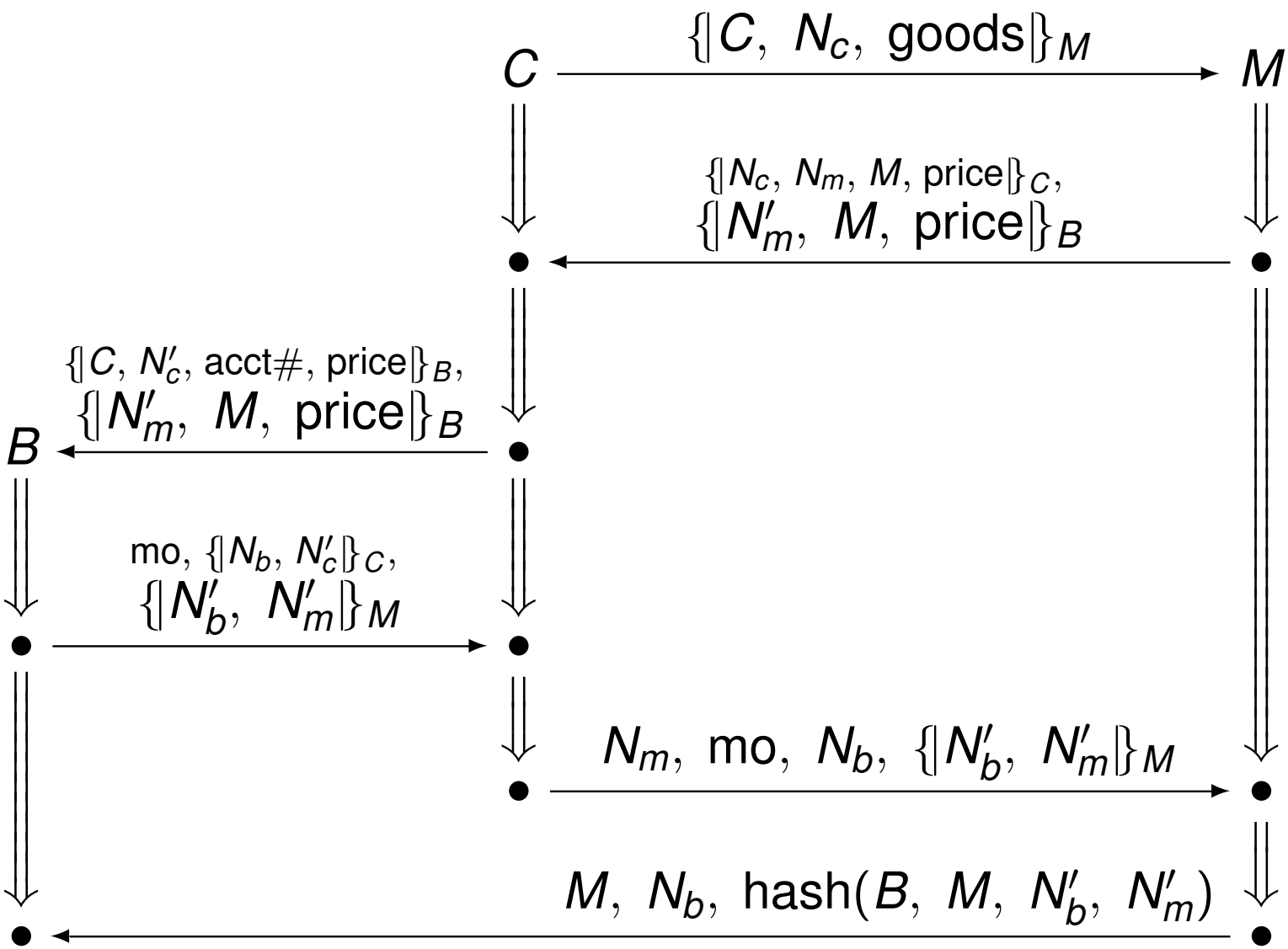


$$\text{mo} = [\![\, \text{hash}(y,\ N_b,\ N_m,\ z) \,]\!]_B$$

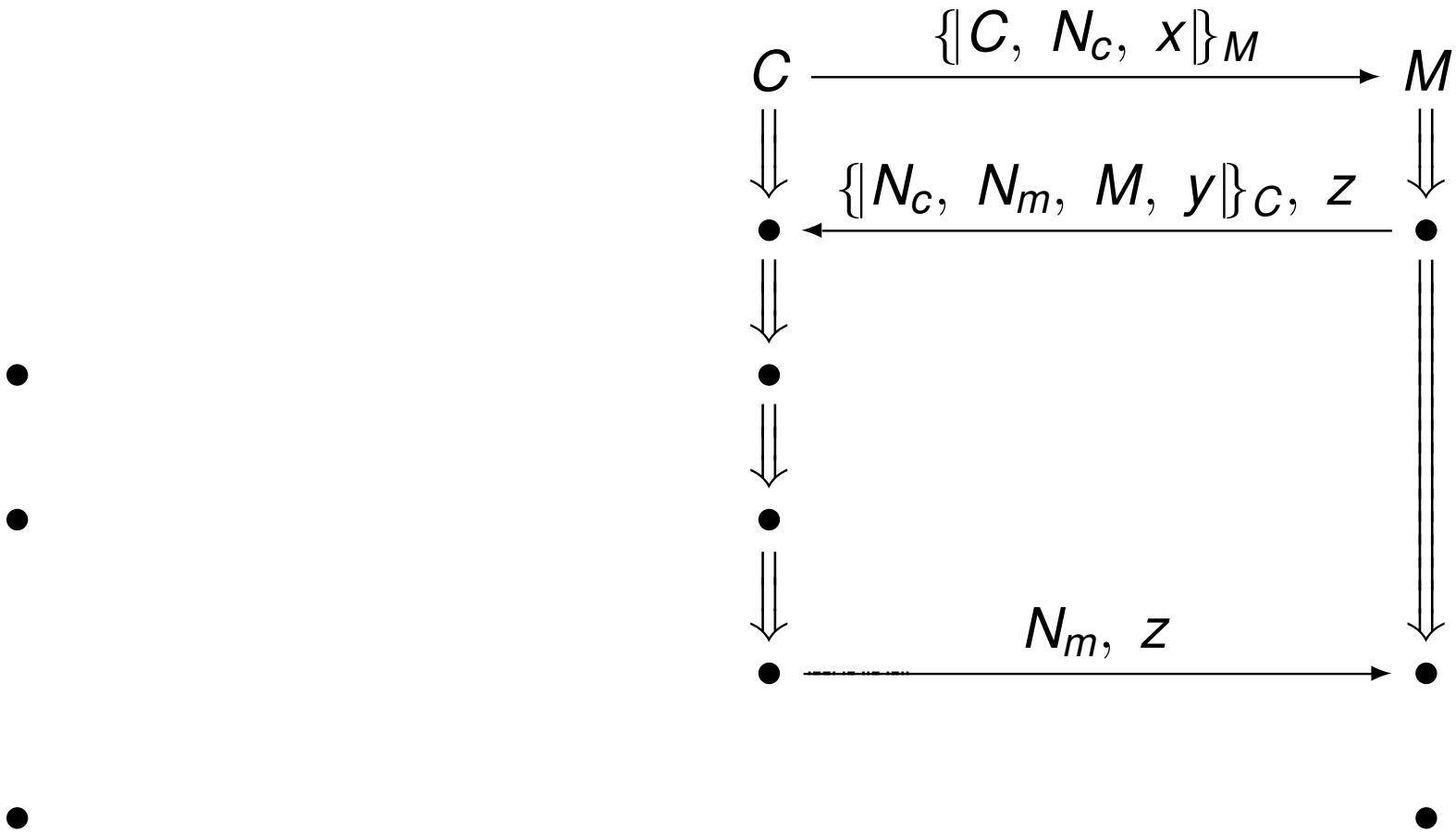
Map germ 1 C role to elaborated role



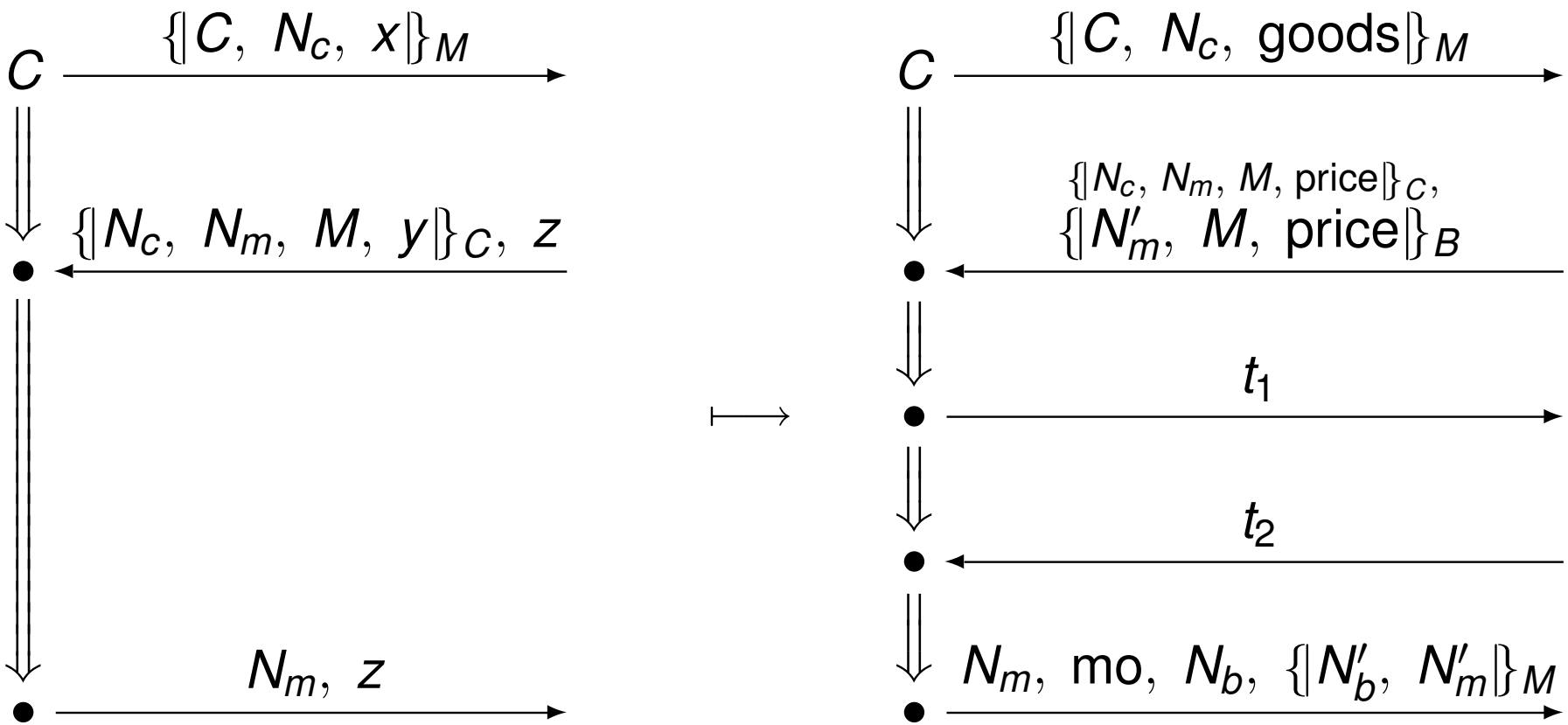
EPMOa $\quad mo = \llbracket \mathrm{hash}(C,\ N'_b,\ N'_m,\ \mathrm{price}) \rrbracket_B$



EPMOa Germ 1: C/M



Map germ 1 C role to elaborated role



Role translation

Simple role mapping notion

$g = (\sigma, f)$ is a role translation from ρ_1 to ρ_2 iff

1. $(\rho_1 \downarrow k) \cdot \sigma = \rho_2 \downarrow f(k)$ for each $k \in [1, \text{len}(\rho_1)]$
2. $\text{non}(\rho_1) \cdot \sigma \subseteq \text{non}(\rho_2)$
3. $\text{unique}(\rho_1) \cdot \sigma \subseteq \text{unique}(\rho_2)$

where σ is a substitution
and f is order-preserving

Protocol elaboration

$G = \langle (\sigma_i, f_i) \rangle_{i \in I}$ is a protocol elaboration from Π_1 to Π_2 iff

G is a vector of role translations,
where each G_i is a role translation mapping
role ρ_i of Π_1 to some role ρ_j of Π_2

Protocol elaboration

$G = \langle (\sigma_i, f_i) \rangle_{i \in I}$ is a protocol elaboration from Π_1 to Π_2 iff

G is a vector of role translations,
where each G_i is a role translation mapping
role ρ_i of Π_1 to some role ρ_j of Π_2

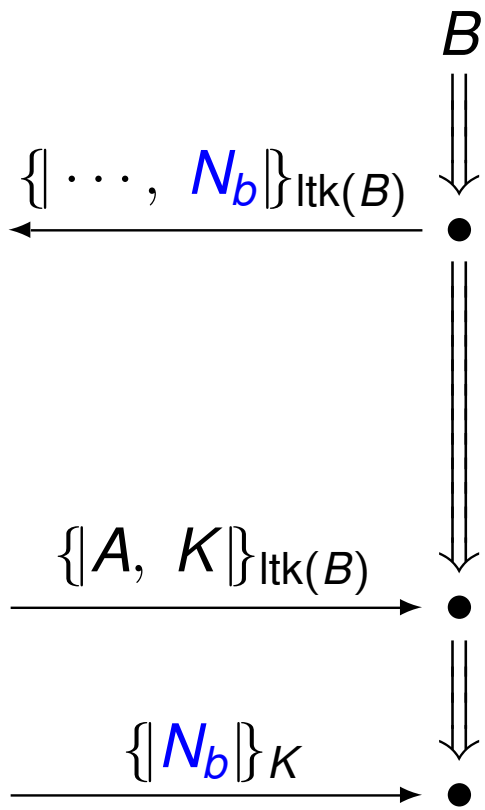
When does a protocol elaboration
preserve security goals?

Elaborating protocols

- Protocols constructed by superimposing germ protocols
  - Superimpose: map roles of germs into elaborated roles
  - Soundness: map shapes of germs into elaborated shapes
  - Preserve authentication and secrecy goals
- Analysis-preserving maps
  - Analysis: authentication tests leading to shapes
  - Represent analysis as LTS
    - ★ Nodes: Skeletons $\mathbb{A}$
    - ★ Labeled transitions: $\mathbb{A}_0 \overset{\ell}{\rightsquigarrow} \mathbb{A}_1$ means test ℓ is
      (1) unsolved in $\mathbb{A}_0$,
      (2) solved in $\mathbb{A}_1$,
      (3) in some most general way
  - Analysis-preserving map: Weak bisimulation

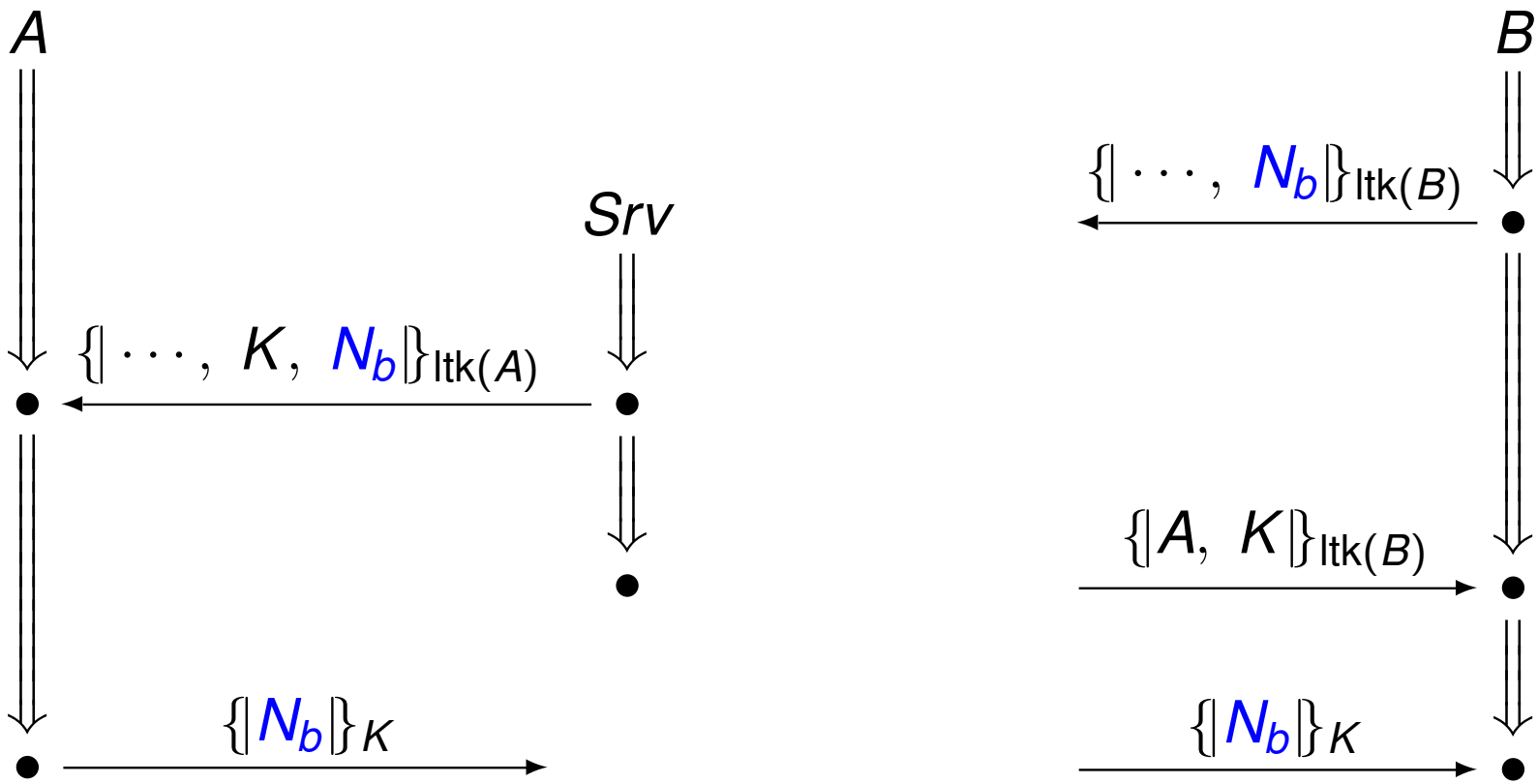
Transforming challenge to response

Example: Yahalom



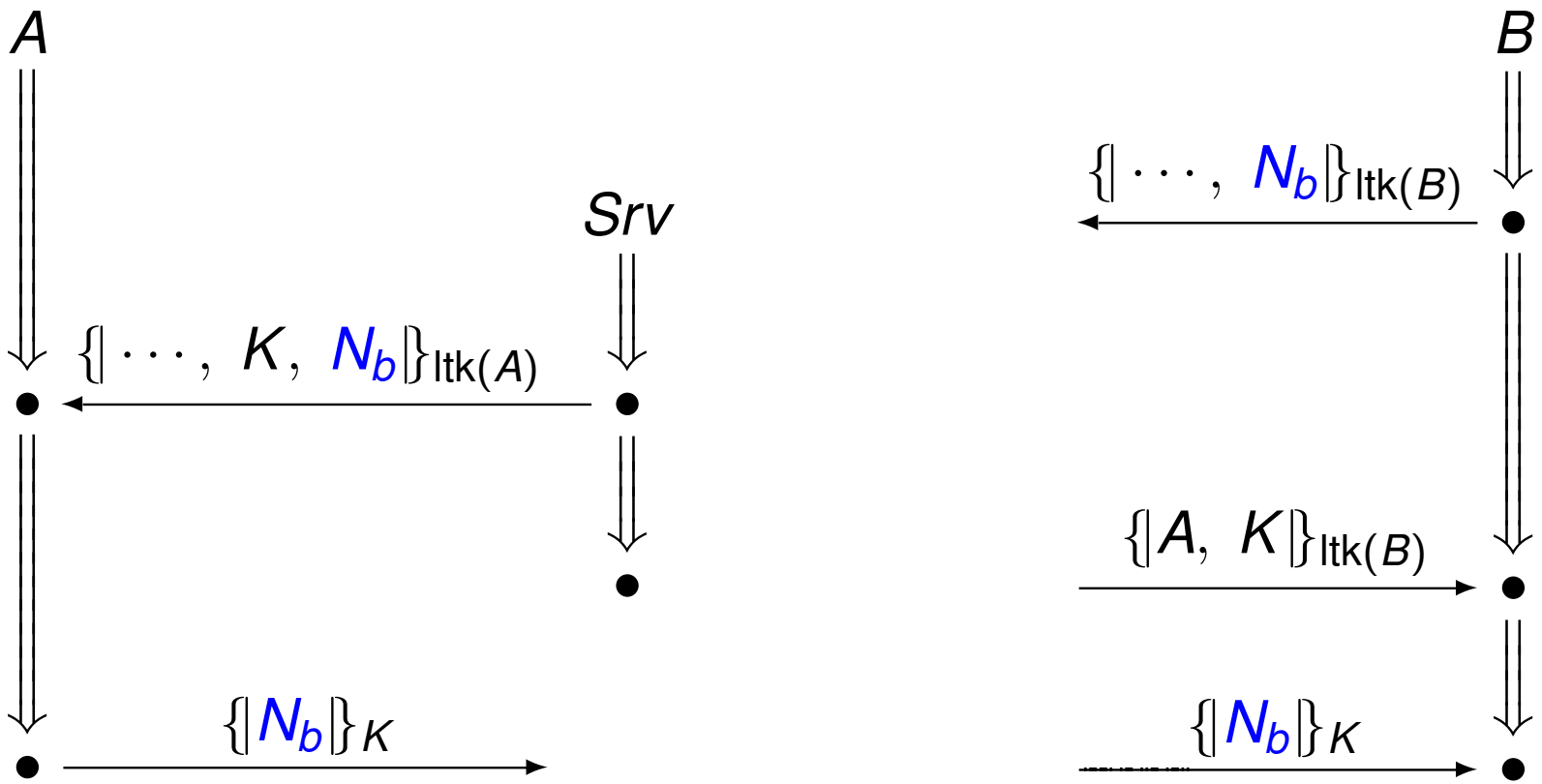
Transforming challenge to response

Example: Yahalom



Secrecy of N_b

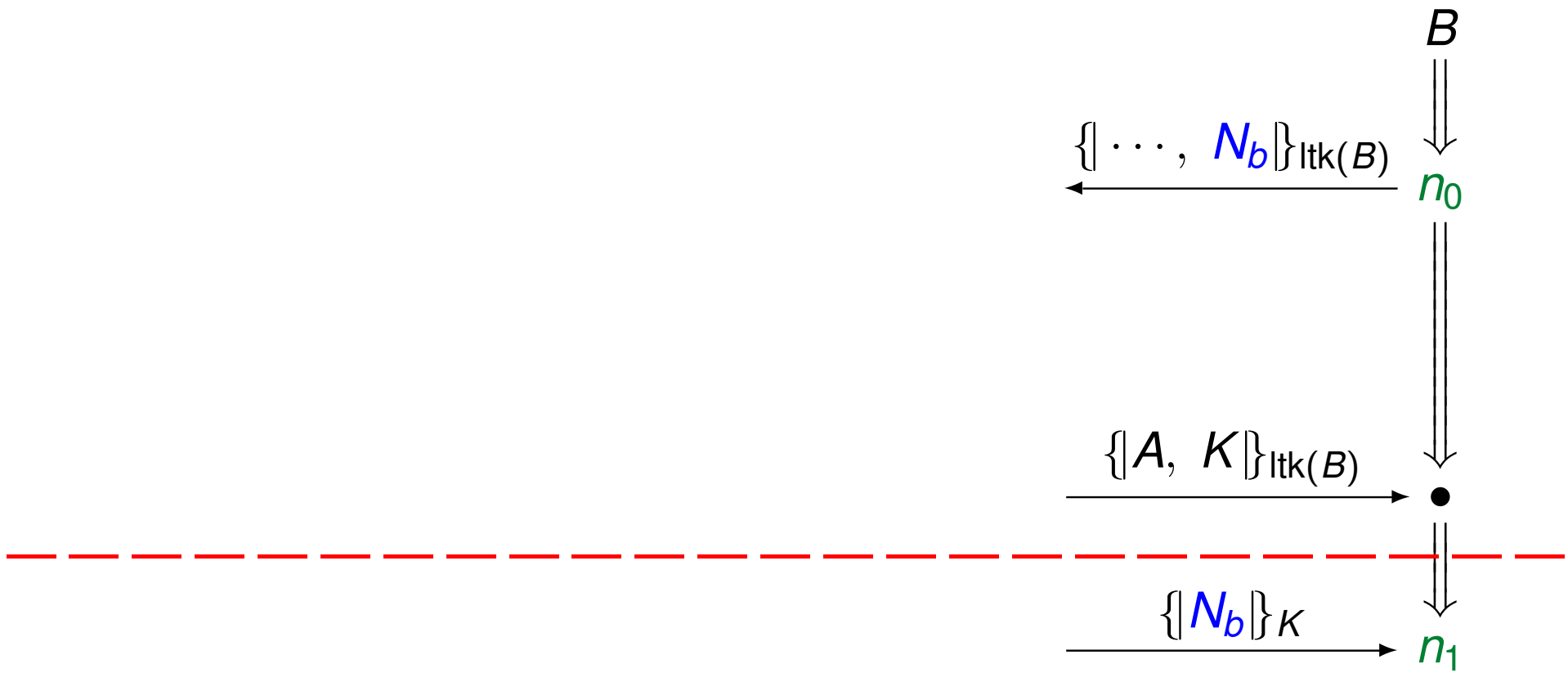
Example: Yahalom



N_b confined to $\{|\cdots, N_b|\}_{ltk(B)}$, $\{|\cdots, K, N_b|\}_{ltk(A)}$, $\{|N_b|\}_K$

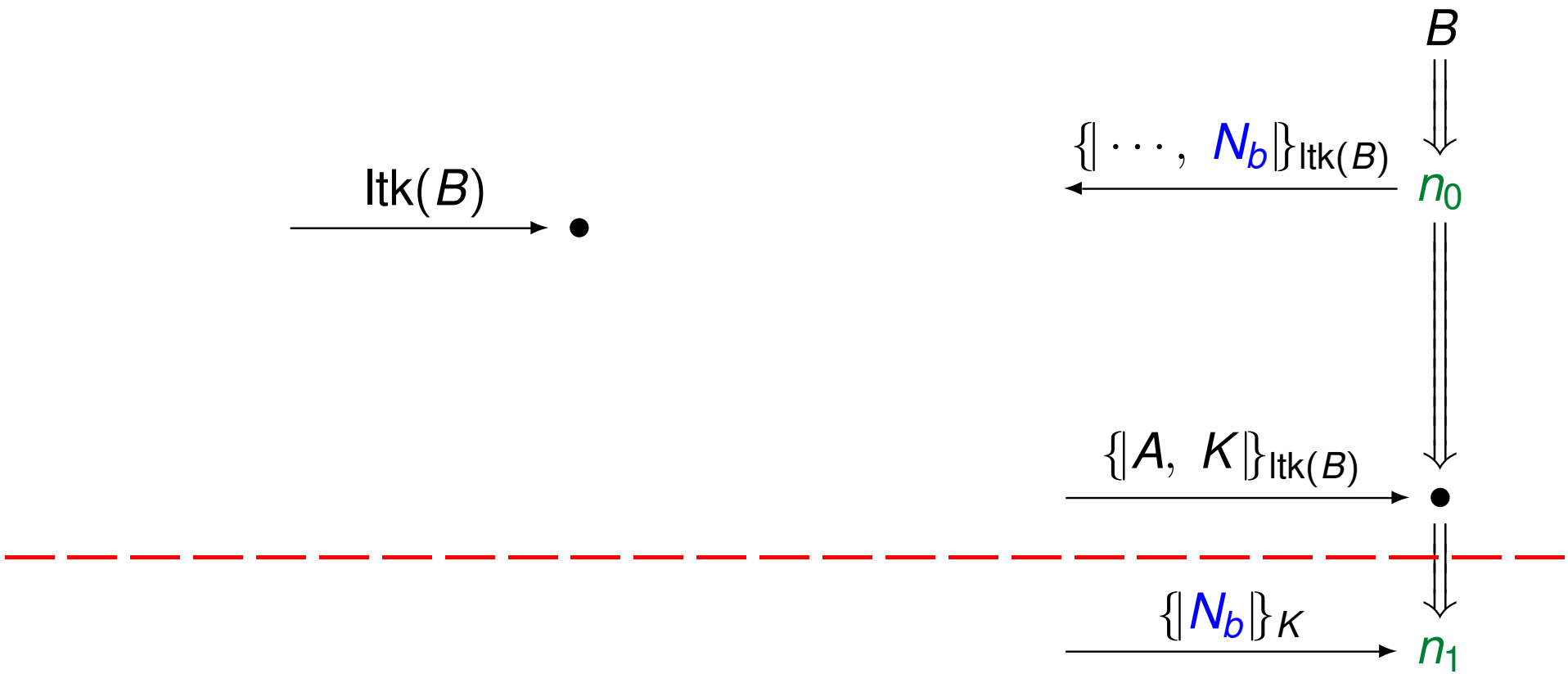
N_b escapes $\{|\cdots, N_b|\}_{\mathrm{ltk}(B)}$ and $\{|\cdots, K, N_b|\}_{\mathrm{ltk}(A)}$

The test from n_0 to n_1



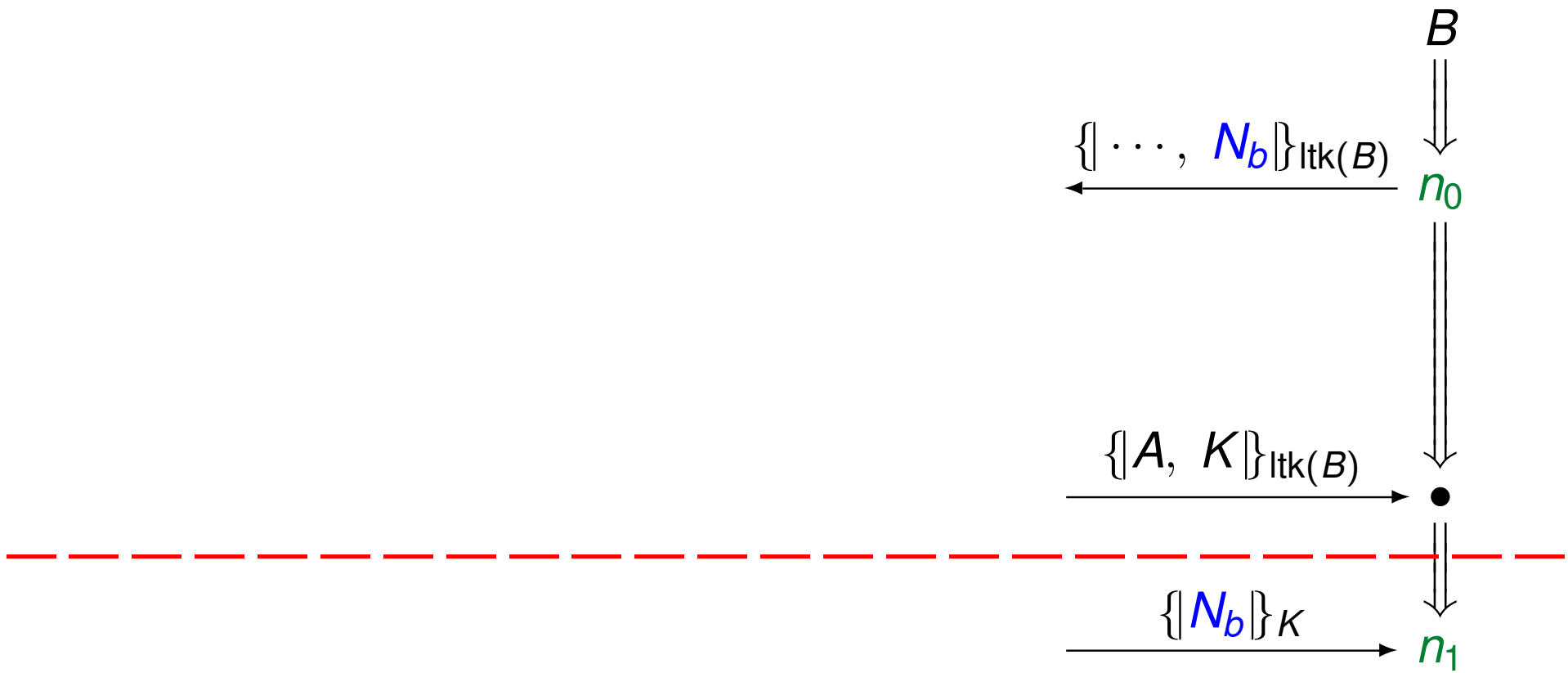
N_b escapes $\{|\cdots, N_b|\}_{\mathrm{ltk}(B)}$ and $\{|\cdots, K, N_b|\}_{\mathrm{ltk}(A)}$

One solution



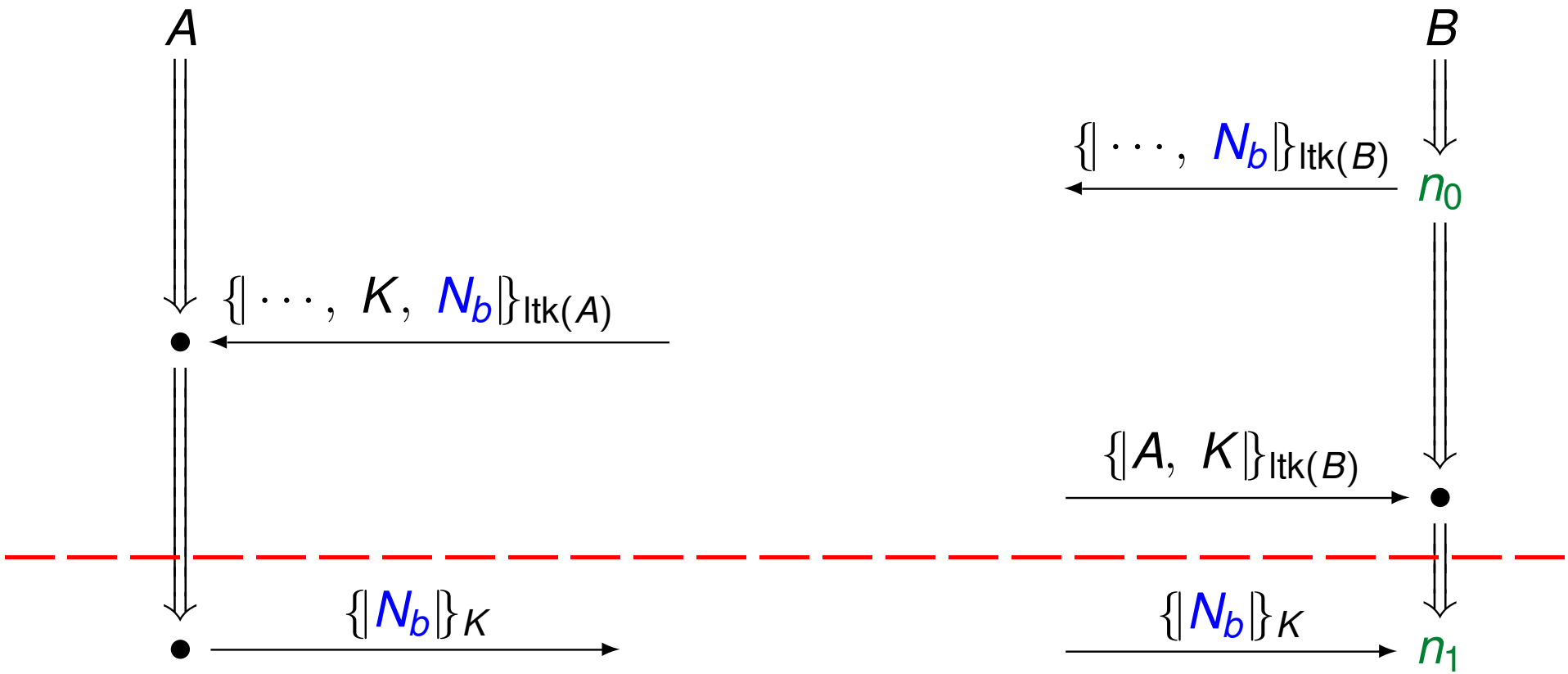
N_b escapes $\{|\cdots, N_b|\}_{\mathrm{ltk}(B)}$ and $\{|\cdots, K, N_b|\}_{\mathrm{ltk}(A)}$

Same test



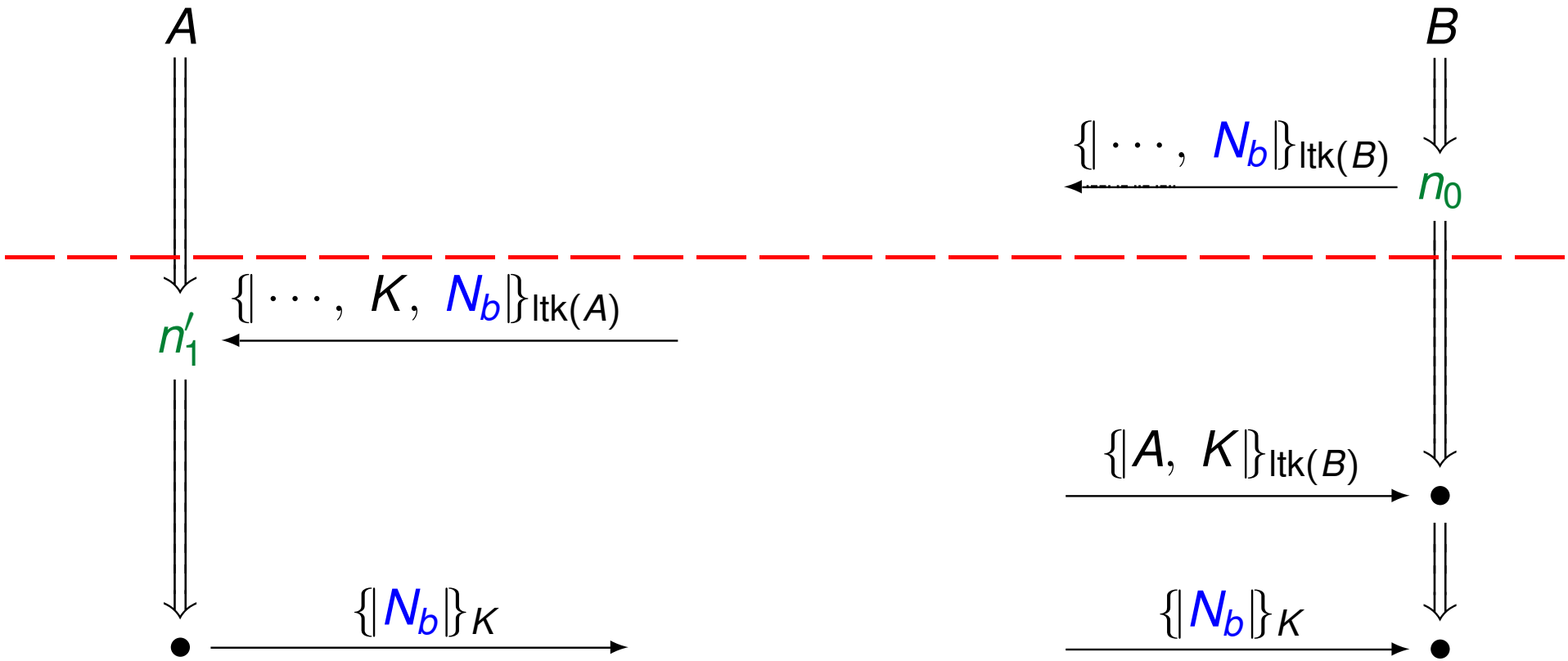
N_b escapes $\{|\cdots, N_b|\}_{\mathrm{ltk}(B)}$ and $\{|\cdots, K, N_b|\}_{\mathrm{ltk}(A)}$

Another solution



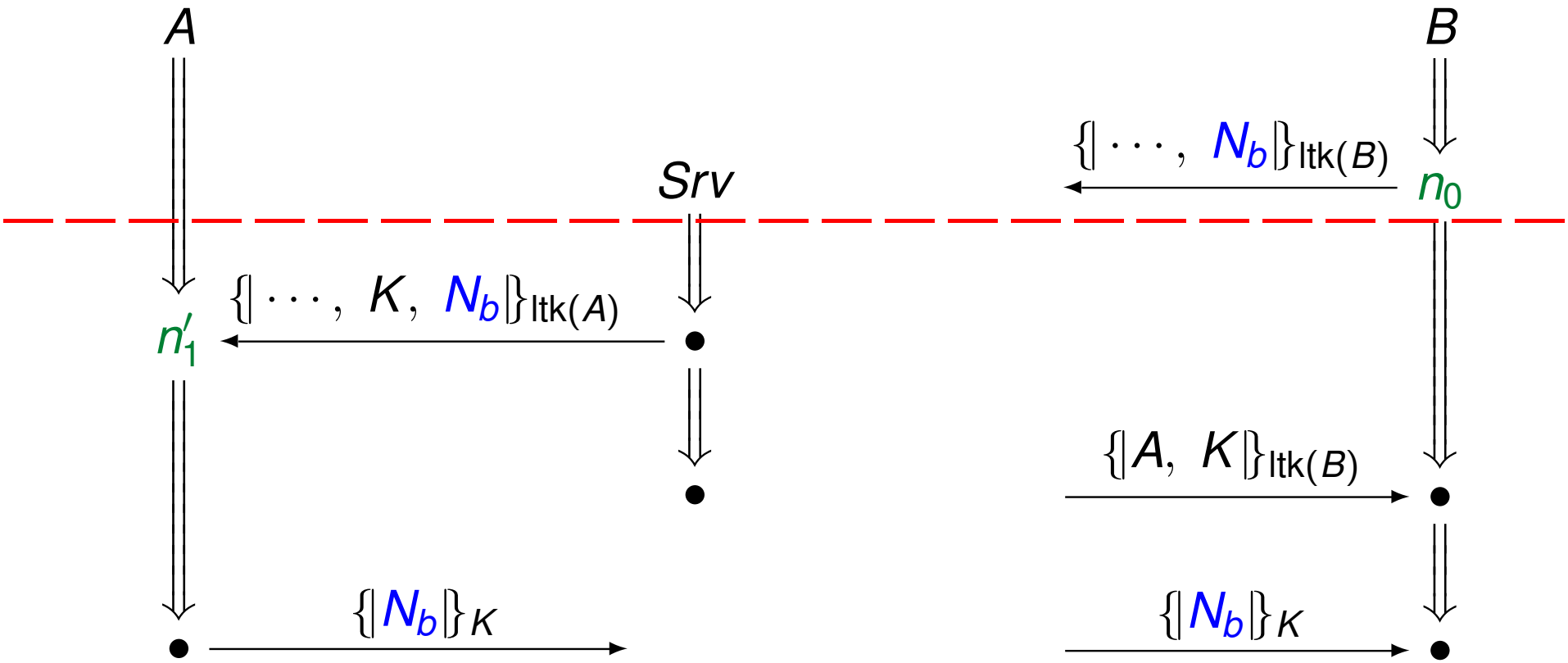
N_b escapes from $\{|\cdots, N_b|\}_{\mathrm{ltk}(B)}$

Another test, from n_0 to n'_1



N_b escapes from $\{\!|\cdots, N_b|\!\}_{\mathrm{ltk}(B)}$

One solution



Form of the authentication test principles

Every test transformation has a solution

Outgoing authentication test

Suppose nonce or session key a originates freshly at event n_0, and

> *a occurs at n_0 only within encryptions* $\{\!|\cdots a \cdots|\!\}_K$

but later at event n_1, a occurs outside those encryptions.

Then either:

> *a regular (honest) participant transforms a*

or else

> *K^{-1}, the decryption key for K, is compromised.*

Outgoing authentication test

Suppose nonce or session key a originates freshly at event n_0, and

> *a occurs at n_0 only within encryptions* $\{\!|\cdots a \cdots|\!\}_K$

but later at event n_1, a occurs outside those encryptions.

A test transformation from n_0 to n_1

Then either:

> *a regular (honest) participant transforms a*

or else

> *K^{-1}, the decryption key for K, is compromised.*

Solutions: regular transformation or compromise

Preserving the tests and solutions

For soundness, an elaboration G must preserve

- Points of origination for critical values
  - nonces
  - session keys
  - encryptions
- Tests, i.e. nodes that
  receive a critical value in a new form
- Transforming edges, i.e. regular edges that
  transmit a critical value in a new form

A criterion for sound elaboration

$G = \langle (\sigma_i, f_i) \rangle_{i \in I}$ is a *sound elaboration* if

1. Each σ_i is injective on nonces, keys
   Acts only on "indeterminates of translation" $x, y, \ldots$
2. For each nonce or key a,
   or encryption $e = \{\!|t_0|\!\}_K$,
   and set of encryptions S,
   letting $t = a$ or $t = e$,

   if t is carried only within S in $\rho_i \downarrow k$ for each $k < k_1$,
   and t is carried outside S in node $\rho_i \downarrow k_1$,
   then the same is true for $t \cdot \sigma_i$, $S \cdot \sigma_i$,
   and the nodes of the target ρ_j up to $f(k_1)$

   and "conversely"

where (σ_i, f_i) maps $\rho_i \in \Pi_1$ to $\rho_j \in \Pi_2$

Carried only within

Message t_0 is *carried only within* S in t_1 iff
S is a set of encryptions and

- $t_0 \neq t_1$ and either
- $t_1 \in S$

or $t_1 = t_2,\ t_3$ and t_0 is carried only within S in both t_2 and t_3

or $t_1 = \{|t_2|\}_{t_3}$ and t_0 is carried only within S in t_2

or t_1 is an atom or indeterminate

Carried only within

Message t_0 is *carried only within* S in t_1 iff
S is a set of encryptions and

- $t_0 \neq t_1$ and either
- $t_1 \in S$

or $t_1 = t_2,\ t_3$ and t_0 is carried only within S in both t_2 and t_3

or $t_1 = \{|t_2|\}_{t_3}$ and t_0 is carried only within S in t_2

or t_1 is an atom or indeterminate

i.e. every path p through a.s.t. for t_1

traverses a member of S before reaching t_0
if p reaches t_0
and p does not traverse a key used for encryption

Carried outside

Message t_0 is *carried outside* S in t_1 iff
it is not carried only within S in t_1

Carried outside

Message t_0 is *carried outside* S in t_1 iff
it is not carried only within S in t_1

i.e. some path p through a.s.t. for t_1

> *traverses no member of S before reaching* t_0
> *and p does not traverse a key used for encryption*

“Conversely” meaning:

2. For each nonce or key a,
   or encryption $e = \{\!|t_0|\!\}_K$,
   and set of encryptions S,
   letting $t = a$ or $t = e$, if t appears in ρ_i

   if $t \cdot \sigma_i$ is carried only within $S \cdot \sigma_i$ in $\rho_j \downarrow k$ for each $k < k_2$,
   and $t \cdot \sigma_i$ is carried outside $S \cdot \sigma_i$ in $\rho_j \downarrow k_2$,
   then $k_2 = f(k_1)$, where
   t is carried only within S in $\rho_i \downarrow k$ for each $k < k_1$,
   and t is carried outside S in node $\rho_i \downarrow k_1$

Why does this criterion suffice?

If $G\colon \Pi_1 \longrightarrow \Pi_2$ is a sound elaboration,
then G preserves the security goals of Π_1

Why does this criterion suffice?

If $G\colon \Pi_1 \longrightarrow \Pi_2$ is a sound elaboration,
then G preserves the security goals of Π_1

Idea: G preserves Π_1's protocol analysis because:

- Analysis of Π_1: an LTS leading via authentication tests to shapes
- Some skeletons $\mathbb{A}$ for Π_1 related with skeletons $\mathbb{B}$ for Π_2
- Related skeletons have same unsolved Π_1-tests
- Solutions produce related skeletons

Why does this criterion suffice?

If $G\colon \Pi_1 \longrightarrow \Pi_2$ is a sound elaboration,
then G preserves the security goals of Π_1

Idea: G preserves Π_1's protocol analysis because:

- Analysis of Π_1: an LTS leading via authentication tests to shapes
- Some skeletons $\mathbb{A}$ for Π_1 related with skeletons $\mathbb{B}$ for Π_2
- Related skeletons have same unsolved Π_1-tests
- Solutions produce related skeletons

I.e. "related" is a bisimulation;
weak because $\mathbb{B}$ may have tests τ not of form $G(\cdot)$

What is an authentication goal? View 1

An assertion

- Suppose for any realized skeleton $\mathbb{A}$:
  - $\mathbb{A}$ contains a strand Resp$[A, B, N_a, N_b]$
  - $K_A^{-1} \in \text{non}_{\mathbb{A}}$
  - $N_b \in \text{unique}_{\mathbb{A}}$
  - $N_b \neq N_a$
- Then there is a strand Init$[A, B, N_a, N_b]$ in $\mathbb{A}$

Authentication: correspondence assertions (of form $\forall\exists$)
(True for NSL, false for NS)

What is an authentication goal? View 2

A homomorphism $H_g : \mathbb{A}_a \mapsto \mathbb{A}_g$

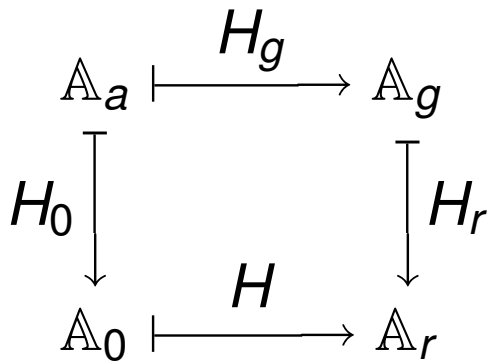
- Assumption skeleton $\mathbb{A}_a$:
  - Nodes of Resp$[A, B, N_a, N_b]$
  - $\{K_A^{-1}\} = \text{non}_{\mathbb{A}}$
  - $\{N_b\} = \text{unique}_{\mathbb{A}}$
- Goal skeleton $\mathbb{A}_g$
  also has nodes of Init$[A, B, N_a, N_b]$

View 2: $H_g : \mathbb{A}_a \mapsto \mathbb{A}_g$

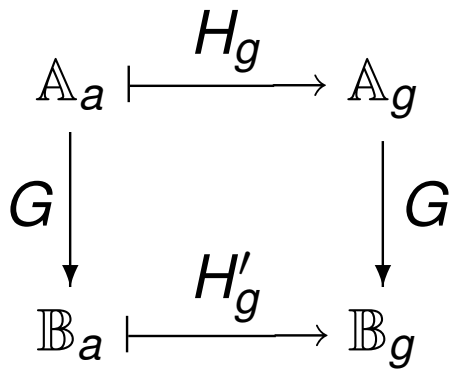
Meaning: Given

- Any $H_0 : \mathbb{A}_a \mapsto \mathbb{A}_0$
- Any $H : \mathbb{A}_0 \mapsto \mathbb{A}_r$ with $\mathbb{A}_r$ realized

There exists $H_r : \mathbb{A}_g \mapsto \mathbb{A}_r$ such that $H \circ H_0 = H_r \circ H_g$



When does G preserve $H_g : \mathbb{A}_a \mapsto \mathbb{A}_g$?



Elaborating protocols

- Protocols constructed by superimposing germ protocols
  - Superimpose: map roles of germs into elaborated roles
  - Soundness: map shapes of germs into elaborated shapes
  - Preserve authentication and secrecy goals
- Analysis-preserving maps
  - Analysis: authentication tests leading to shapes
  - Represent analysis as LTS
    - ★ Nodes: Skeletons $\mathbb{A}$
    - ★ Labeled transitions: $\mathbb{A}_0 \overset{\ell}{\rightsquigarrow} \mathbb{A}_1$ means test ℓ is
      (1) unsolved in $\mathbb{A}_0$,
      (2) solved in $\mathbb{A}_1$,
      (3) in some most general way
  - Analysis-preserving map: Weak bisimulation

Skeleton

1. $\text{nodes}_{\mathbb{A}}$, finite set of regular nodes
2. $\preceq_{\mathbb{A}}$, reflexive partial order on $\text{nodes}_{\mathbb{A}}$ representing causal accessibility
3. $\text{non}_{\mathbb{A}}$, set of keys assumed non-originating (uncompromised, because used but not sent)
4. $\text{unique}_{\mathbb{A}}$, set of atoms assumed uniquely originating (like nonces, session keys)

When $n \Rightarrow^* n'$ and $n' \in \text{nodes}_{\mathbb{A}}$, we require

$$n \in \text{nodes}_{\mathbb{A}} \text{ and } n \preceq_{\mathbb{A}} n'$$

Homomorphism

$H = \phi, \sigma$ where

ϕ: $\text{nodes}_{\mathbb{A}_0} \mapsto \text{nodes}_{\mathbb{A}_1}$
σ maps atoms to atoms[1]

such that

1. ϕ respects strand structure, and

$$\text{term}(n) \cdot \sigma = \text{term}(\phi(n))$$

   for all $n \in \mathbb{A}_0$
2. $m \preceq_{\mathbb{A}_0} n$ implies $\phi(m) \preceq_{\mathbb{A}_1} \phi(n)$
3. $(\text{non}_{\mathbb{A}_0}) \cdot \sigma \subset \text{non}_{\mathbb{A}_1}$
4. $(\text{unique}_{\mathbb{A}_0}) \cdot \sigma \subset \text{unique}_{\mathbb{A}_1}$

[1] $x \cdot \sigma$ means σ applied to all atoms throughout x