Applying a Compositional Authentication Logic to a Protocol Standard

Catherine Meadows
(Joint Work with Dusko Pavlovic)
Feb. 11, 2004

Background and Motivation

- How crypto protocols are designed
  - Start from a standard pattern
  - Add features incrementally
  - Compose with other patterns as needed
- What's needed in cryptographic protocol analysis methods
  - Support for incremental verification
  - Support for reasoning about composition of protocols
- We are working on a logic that supports this
- Wanted to validate by applying to a "real" protocol

Overview of Talk

- Brief overview of logic

- Brief oveview of GDOI protocol, a group key distribution protocol developed by IETF

  - Previously analyzed using NRL Protocol Analyzer

- Derivation of GDOI

- Derivation of attack on GDOI

  - Missed in NPA analysis because of mis-understanding of requirement

- Suggestions for fixing it

The Logic

- Similar to earlier derivational logic of Datta, Derek, Mitchell, and Pavlovic

- Crucial difference: statement couched entirely in terms of partial orders of actions known to an agend
  - More concrete and less prone to error than earlier such logics
  - Smaller syntax and simpler semantics than predecessors

Axioms Describing the Sending and Receiving of Messages

rcv $(t) \Longrightarrow \exists a.\ a = \langle t \rangle \wedge a < (t)$

new $(\nu m)_M \Longrightarrow \forall a_A. \Big(m \in FV(a) \Rightarrow a > (\nu m)\Big) \wedge$

$A \neq M \Rightarrow (\nu m)_M < \langle\langle m \rangle\rangle_M < ((m))_A \leq a_A$

- Also assume that principals, even dishonest ones, don't reveal longterm keys
  - This is not a hard and fast assumption, and could change

Challenge Response Axiom

cr $A : (\nu m)_A\Big(\langle\langle c^{AB}m\rangle\rangle_A < ((r^{AB}m))_A$
$\Longrightarrow \langle\langle c^{AB}m\rangle\rangle_A < ((c^{AB}m))_B < \langle\langle r^{AB}m\rangle\rangle_{B<} <$
$((r^{AB}m))_A\Big)$

- c^{AB} and r^{AB} can be instantiated by
  - plaintext and keyed hash
  - plaintext and digital signature
  - public key encryption and plaintext
  - etc.

- Other axioms describe conclusions that can be derived from composing and refining protocols

The GDOI Protocol

- Group key distribution protocol being developed by IETF

- Two sub-protocols, one for joining group and one for distributing keys to group
  - We will be interested in the group joining (GROUPKEY-PULL) protocol

- GROUPKEY-PULL protocol describes member joining group managed by GCKS

- Conversation encrypted and authenticated by key shared between member and GCKS distributed by IKE Phase 1 protocol

Message Flows in GROUP-KEY PULL Protocol

1. $A \rightarrow B : H^{AB}(m, id), m, ID$

2. $B \rightarrow A : H^{BA}(n, m, sa), n, sa$

3. $A \rightarrow B : H^{AB}(n, m, C^{A'}, S^{A'}(n, m)), C^{A'}, S^{A'}(n, m)$.

4. $B \rightarrow A : H^{BA}(n, m, C^{B'}, sq, k, S^{B'}(n, m)), sq, k,$
   $S^{B'}(n, m)$

Note: Assume all messages encrypted by longterm shared key

What is Proof of Possession?

- Used to piggy-back new identity into protocol

- Member presents certificate $C_{A'}$ containing new identity A'in group

- Proves that she owns new identity by using private key to sign two nonces $S^{A'}(n, m)$.

- GCKS can also perform Proof of Possession

- We attempted to use logic to show composition of Proof of Possesion (PoP) with core GDOI achieved its goals

Deriving Core GDOI: Basic Challenge-Response

Use keyed hash, axiomatized by

hash1: $H^{AB}s = H^{AB}t \Longrightarrow \quad s = t$

hash2: $\langle\langle H^{AB}t\rangle\rangle_{X<} \Longrightarrow \quad X = A \vee X = B$

hash3: $H^{AB}t \;\neq \quad H^{BA}t$

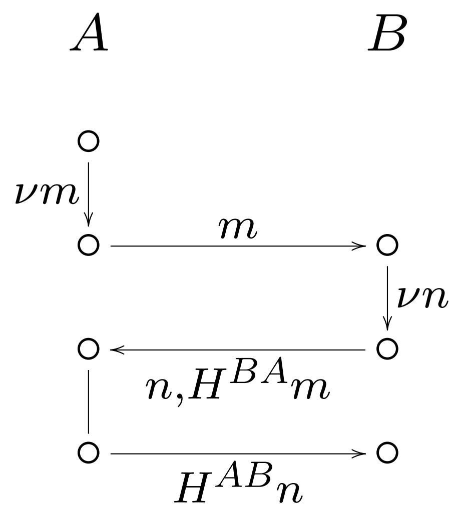
Enough to ensure keyed H^{AB} and H^{BA} instantiate c^{AB} and r^{BA}

Yields Following Derivations

$$\begin{tikzcd}
A & & B \\
\circ \arrow[d, "\nu m"'] & & \\
\circ \arrow[rr, "m"] & & \circ \arrow[d, dash] \\
\circ & & \circ \arrow[ll, "H^{BA}m"]
\end{tikzcd}$$

$$\begin{array}{ll}
A \text{ sees :} & (\nu m)_A < \langle m \rangle_A < (H^{BA}m)_A \\
\quad \text{knows (crh) :} & (\nu m)_A \Big(\langle\langle m \rangle\rangle_A < ((H^{BA}m))_A \\
& \qquad \Longrightarrow \langle\langle m \rangle\rangle_A < \\
& \qquad ((m))_B < \langle\langle H^{BA}m \rangle\rangle_{B<} < \\
& \qquad ((H^{BA}m))_A \Big) \\
\hline
\quad \text{concludes :} & (\nu m)_A < \langle m \rangle_A < \\
& ((m))_B < \langle\langle H^{BA}m \rangle\rangle_{B<} < \\
& (H^{BA}m)_A
\end{array}$$

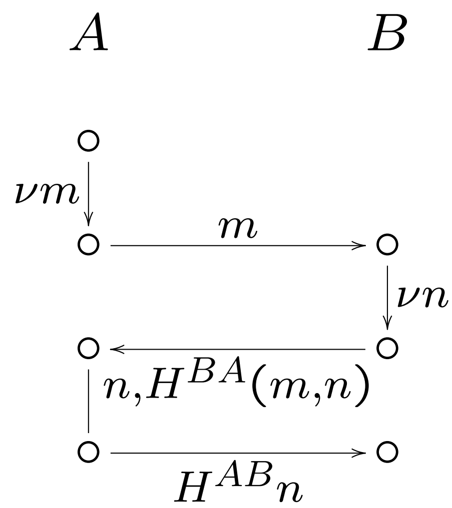
Composing A's and B's C-R Sequentially



$$
\begin{array}{ll}
A \text{ sees :} & (\nu m)_A < \langle m \rangle_A < (n, Hm)_A < \langle Hn \rangle_A \\
\text{(crh)} & (\nu m)_A \Big(\langle\langle m \rangle\rangle_A < ((Hm))_A \\
& \quad \Longrightarrow \langle\langle m \rangle\rangle_A < \\
& \qquad ((m))_B < \langle\langle Hm \rangle\rangle_{B<} < \\
& \qquad ((Hm))_A \Big) \\
\text{(rcv)} & (t) \implies \exists a.\ a = \langle t \rangle \wedge a < (t)
\end{array}
$$

$$
\begin{array}{ll}
A \quad : & (\nu m)_A < \langle m \rangle_A < \\
& ((m))_B < \langle\langle Hm \rangle\rangle_{B<} < \\
& (n, Hm)_A < \langle Hn \rangle_A \ \wedge \\
& \exists Y.\ \langle\langle n | B \to A \rangle\rangle_Y < (n, Hm | B \to A)_A
\end{array}
$$

Binding A's and B's C-R Sequences



$$
\begin{array}{ll}
A \text{ sees :} & (\nu m)_A < \langle m \rangle_A < (n, H(m,n))_A < \langle Hn \rangle_A \\
\text{(crh)} & (\nu m)_A \Big(\langle\langle m \rangle\rangle_A < ((H\overline{m}))_A \Longrightarrow \\
 & \quad \langle\langle m \rangle\rangle_A < ((m))_B < \langle\langle H\overline{m} \rangle\rangle_{B<} < \\
 & \quad ((H\overline{m}))_A \Big) \\
\text{(rcv)} & (t) \Longrightarrow \exists a.\ a = \langle t \rangle \wedge a < (t) \\
A \ : & B \text{ honest } \Longleftrightarrow (x)_B < (\nu y)_B < \\
 & \qquad \langle y, H(x,y) \rangle_B < (Hy)_B
\end{array}
$$

Conclusion is

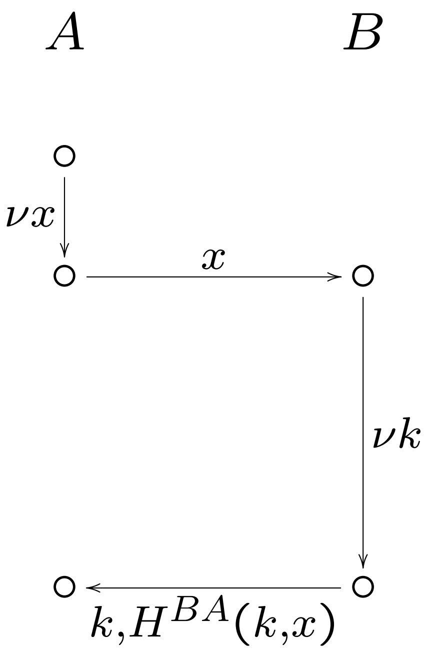
$$
\begin{array}{ll}
A \ : & B \text{ honest } \Longrightarrow (\nu m)_A < \langle m \rangle_A < \\
 & (m)_B < (\nu n)_B < \langle n, H^{BA}(m,n) \rangle_B < \\
 & (n, H^{BA}(m,n))_A < \langle H^{AB} n \rangle_A
\end{array}
$$

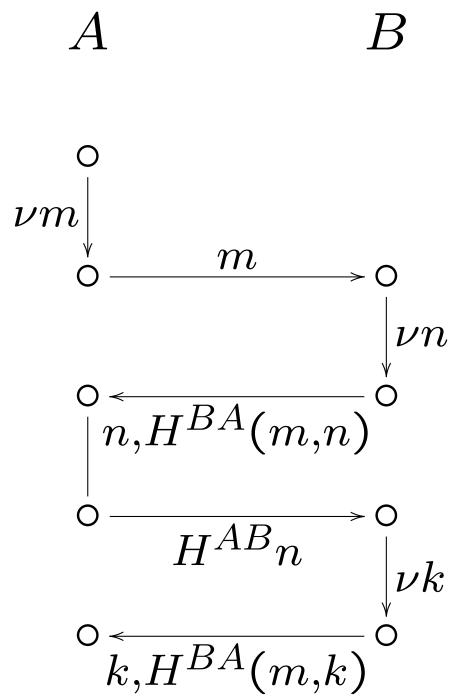
What we Learn from This

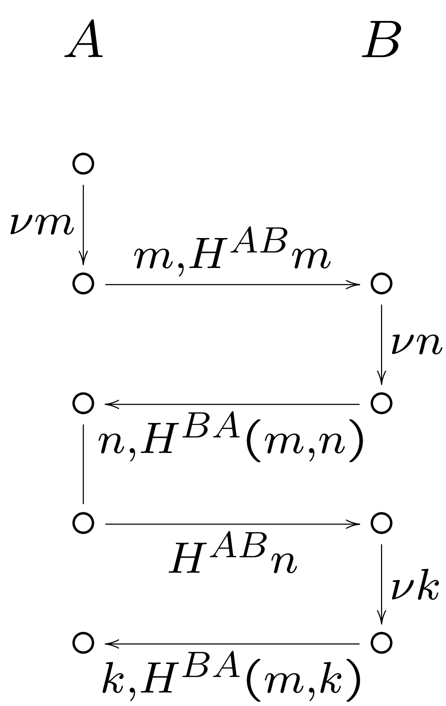
- Protocol satisfies *matching histories*
  - A and B have the same picture of the messages sent

- Using similar reasoning, can also show protocol satisfies *agreement* (Lowe)
  - A and B also know messages were intended for each other

Adding Key Distribution







Axiomatization of Signature

sig1 $S^A t = S^A u \Longrightarrow \quad t = u$

sig2 $\langle\langle S^A t \rangle\rangle_{X<} \Longrightarrow \quad X = A$

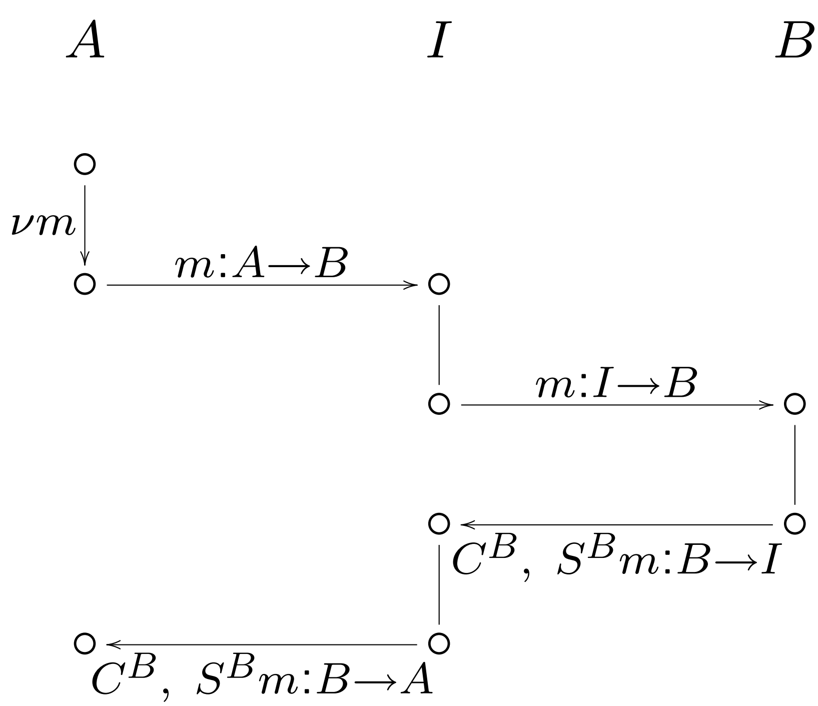
sig3 $V^A(y, t) \quad \Longleftrightarrow \quad y = S^A t$

Proof of Possession (Signature Based Challenge and Response)

- Similar proofs for as for hash based challenge and response

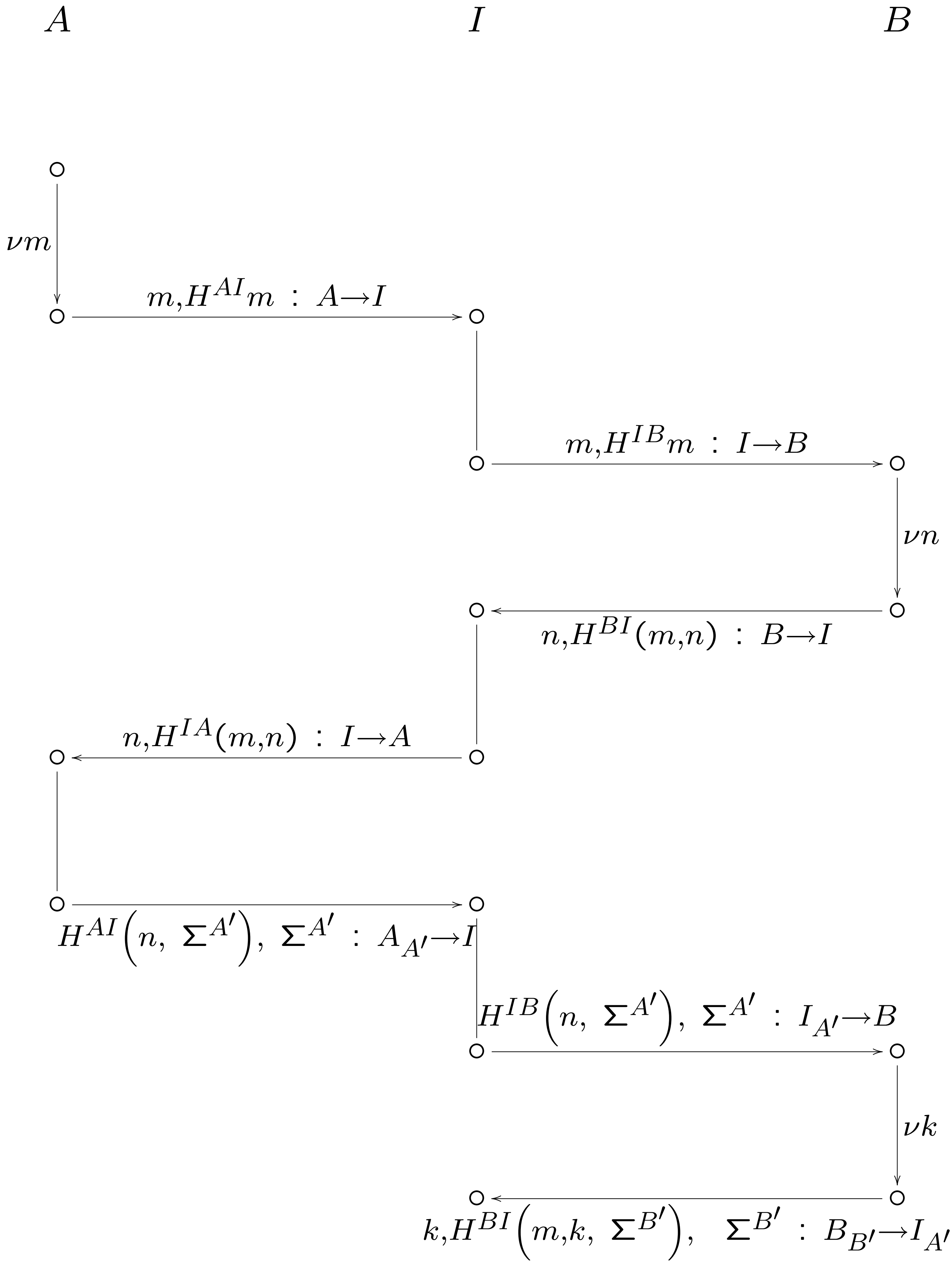
- Main difference: only matching histories, not agreement

- Here's an attack against agreement



Attempt to Prove Proof of Possession

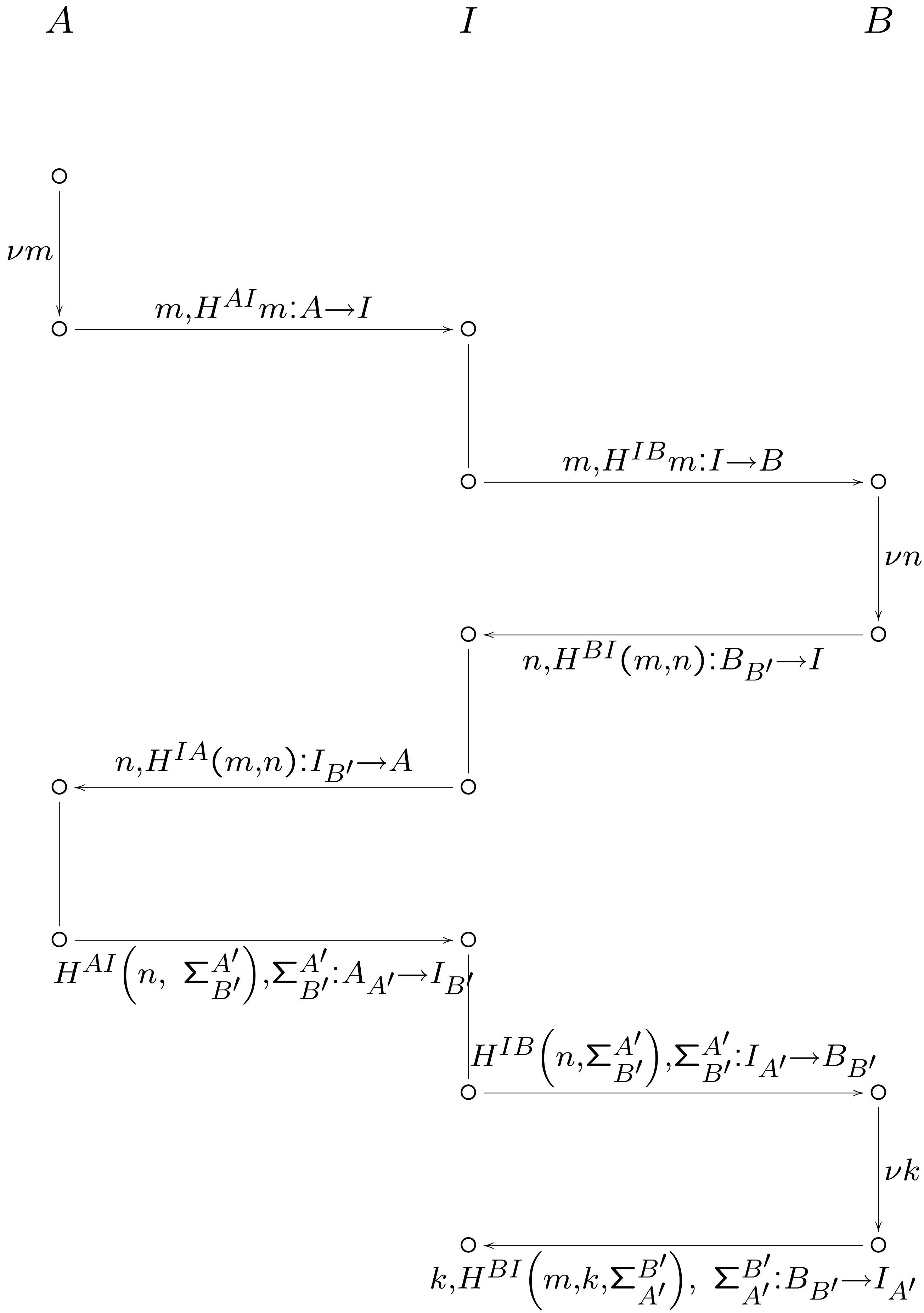
- PoP can be thought of as composition of Hash-based challenge-response and signature-based challenger-response
  - but with different identities
- Failed to come up with proof of PoP
  - Could not find any way to link the two different sets of identities
  - Began to look for ways to attack it
- Found we could find attack by composing hash-based challenge-response with attack on signature-based challenge response
- Note: $\Sigma^{A'} = S^{A'}(m, n)$


A
I
B
νm
$m, H^{AI} m \ : \ A \to I$
$m, H^{IB} m \ : \ I \to B$
νn
$n, H^{BI}(m,n) \ : \ B \to I$
$n, H^{IA}(m,n) \ : \ I \to A$
$H^{AI}\left(n, \ \Sigma^{A'}\right), \ \Sigma^{A'} \ : \ A_{A'} \to I$
$H^{IB}\left(n, \ \Sigma^{A'}\right), \ \Sigma^{A'} \ : \ I_{A'} \to B$
νk
$k, H^{BI}\left(m,k, \ \Sigma^{B'}\right), \ \ \Sigma^{B'} \ : \ B_{B'} \to I_{A'}$

Can we fix PoP by strengthening Signature-based Challenge-Response?

- Use $\Sigma^{A'}_{B'} = S^{A'}(B', m, n)$ instead of $\Sigma^{A'} = S^{A'}(m, n)$.

- But, still vulnerable to attack
  - Appears to be an emergent(?) attack
  - Obtained by gluing two honest runs of the protocols together in an insecure way


A
I
B
νm
$m, H^{AI} m : A \to I$
$m, H^{IB} m : I \to B$
νn
$n, H^{BI}(m, n) : B_{B'} \to I$
$n, H^{IA}(m, n) : I_{B'} \to A$
$H^{AI}\left(n,\ \Sigma_{B'}^{A'}\right), \Sigma_{B'}^{A'} : A_{A'} \to I_{B'}$
$H^{IB}\left(n, \Sigma_{B'}^{A'}\right), \Sigma_{B'}^{A'} : I_{A'} \to B_{B'}$
νk
$k, H^{BI}\left(m, k, \Sigma_{A'}^{B'}\right),\ \Sigma_{A'}^{B'} : B_{B'} \to I_{A'}$

A Better Solution

- Replace $\Sigma^{A'} = S^{A'}(m, n)$ with $S_{A'}(\sigma^{AB}, m, n)$
  - where σ^{AB} is the authentication key shared between A and B

What Can B Conclude?

- Honest principal playing role of A' will only sign its own σ^{AB}
  - So if A' honest, then $A = A'$.

- Honest principal playing role of A
  - $S^{A'}(\sigma^{AB}, m, n)$ appears in a hash computed by A with σ^{AB}
  - Assuming that A is honest, she will only include a $S^{A'}(\sigma^{AB}, m, n)$ in the hash if she computed it herself using the private key of A'.
  - Therefore, assuming that A is honest, $A = A'$

What Can't B Conclude?

- We can't prove anything about dishonest A colluding with dishonest A'
- This would require new axiom saying that if A' computes $S^{A'}m$ then it must know m.
- Collusion would then require principals to share longterm keys
- But, standard sound implementation of digital signatures violates the proposed axiom

Standard Refinement of Digital Signature

- Replace $S^{A'}x$ with $S^{A'}h(x)$ where h is a one-way hash function

- Prevents leakage of x
  - Very important, for example, where x contains a long-term key

- Thus, $S^{A'}(\sigma^{AB}, m, n)$ is replaced by $S^{A'}(h(\sigma^{AB}, m, n))$

- Dishonest A could pass $h(\sigma^{AB}, m, n)$ to colluding A' without revealing longterm key

Context Binding: An Emerging Problem in Cryptographic Protocol Analysis

- GDOI PoP an example of problem in *context binding* (my terminology)

- A and B established a security association in one context: IKE and IKE identities

- Want to bootstrap this into security association in new context: Group and group identities

- Often done by composing protocol in one context with protocol in another context

- This isn't the only example of such security problems with such a composition

  - IETF Extensible Authentication Protocol has similar problem

Conclusion: What do we have?

- Foundations for an epistemic logic for reasoning about principals' knowledge about sequences of events
  - Supports incremental evaluation and composition
- Even in its early stages, its use has already lead to the discovery of an attack
- Also, have found potential for using logic to find attacks directly, by composing attacks and legitimate protocol runs of component protocols
- Promising for attacking emerging class of problems: context binding