Protocol Derivation Assistant

Dusko Pavlovic

and Matthias Anlauff

Kestrel Institute, Palo Alto CA

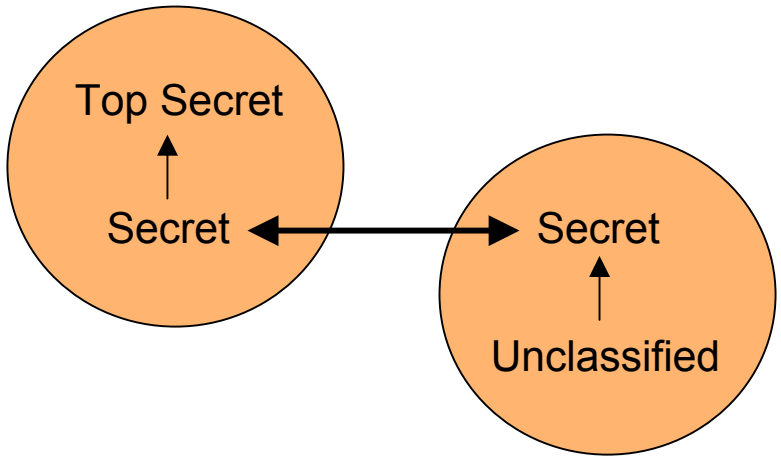
Problem

- networks are complex
  - regulated by protocols
- protocols are complex
  - require incremental approach

Problem

… but

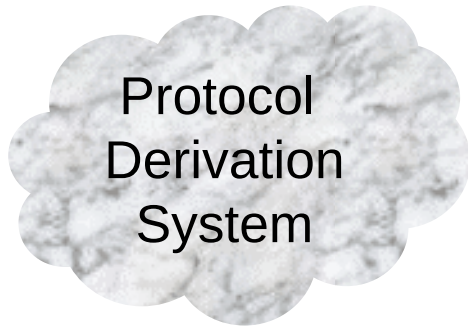
- security is not preserved under
  - refinement
  - composition



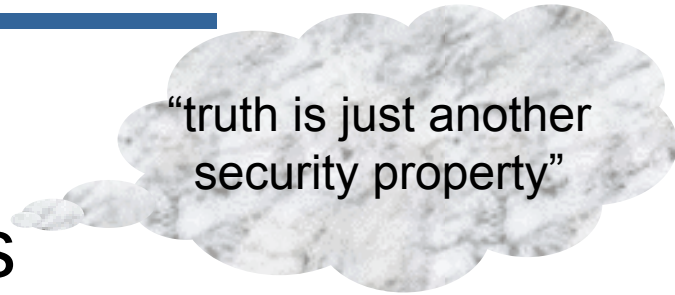
Solution

- annotate processes by properties
  - “distributed hoare logic”
- develop
  - processes and
  - properties

  in parallel



Protocol Derivation System



Protocols

- components
- refinements
- transformations

Proofs

- axioms
- proof rules
- proof transformations

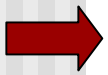
- **derivation patterns**

Protocol Derivation Assistant

- protocol development
- instance checking
- code generation
- property specification
- distributed reasoning
- certificate generation

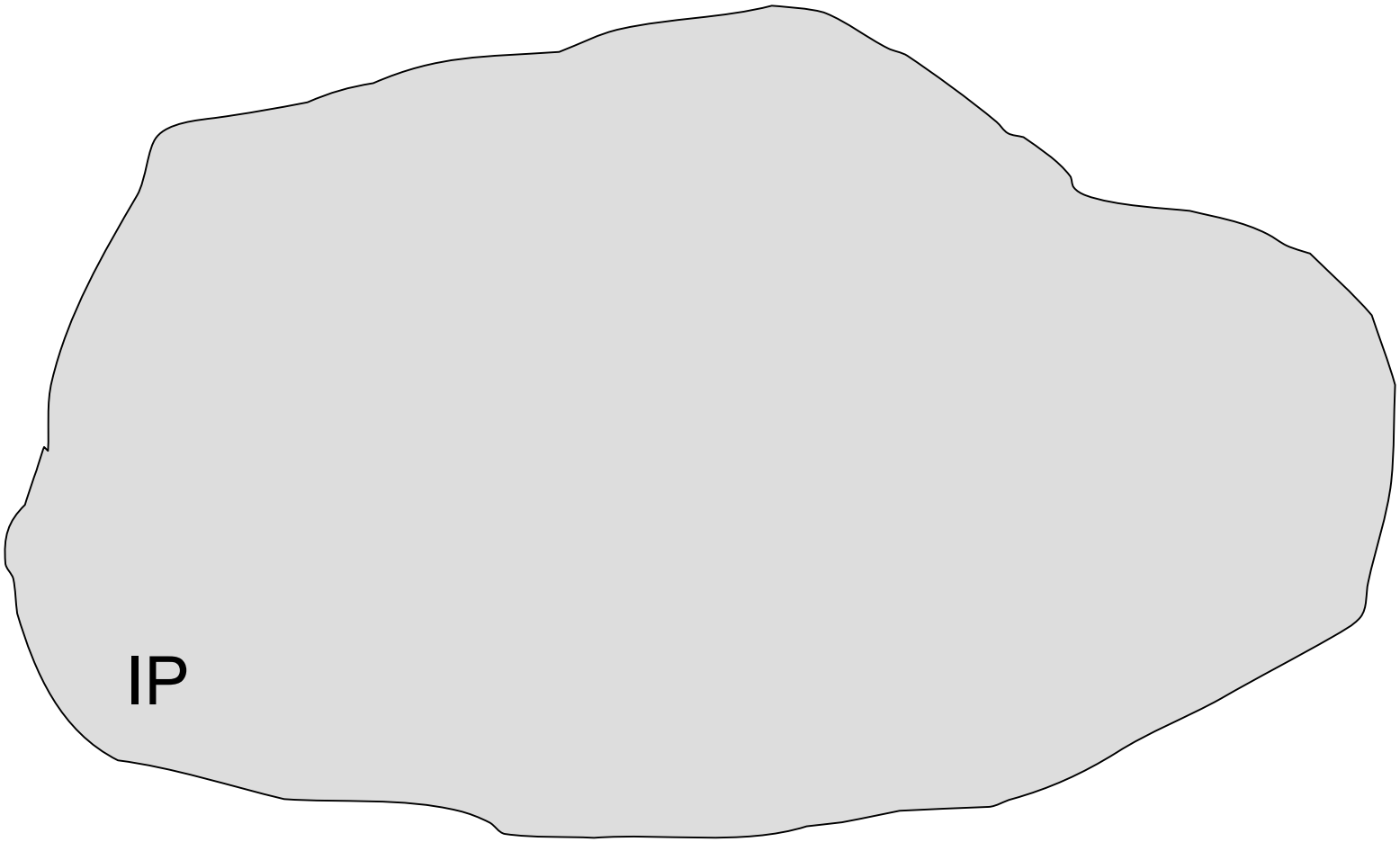
- **library, taxonomy**
- **peer-to-peer exchange**

Outline

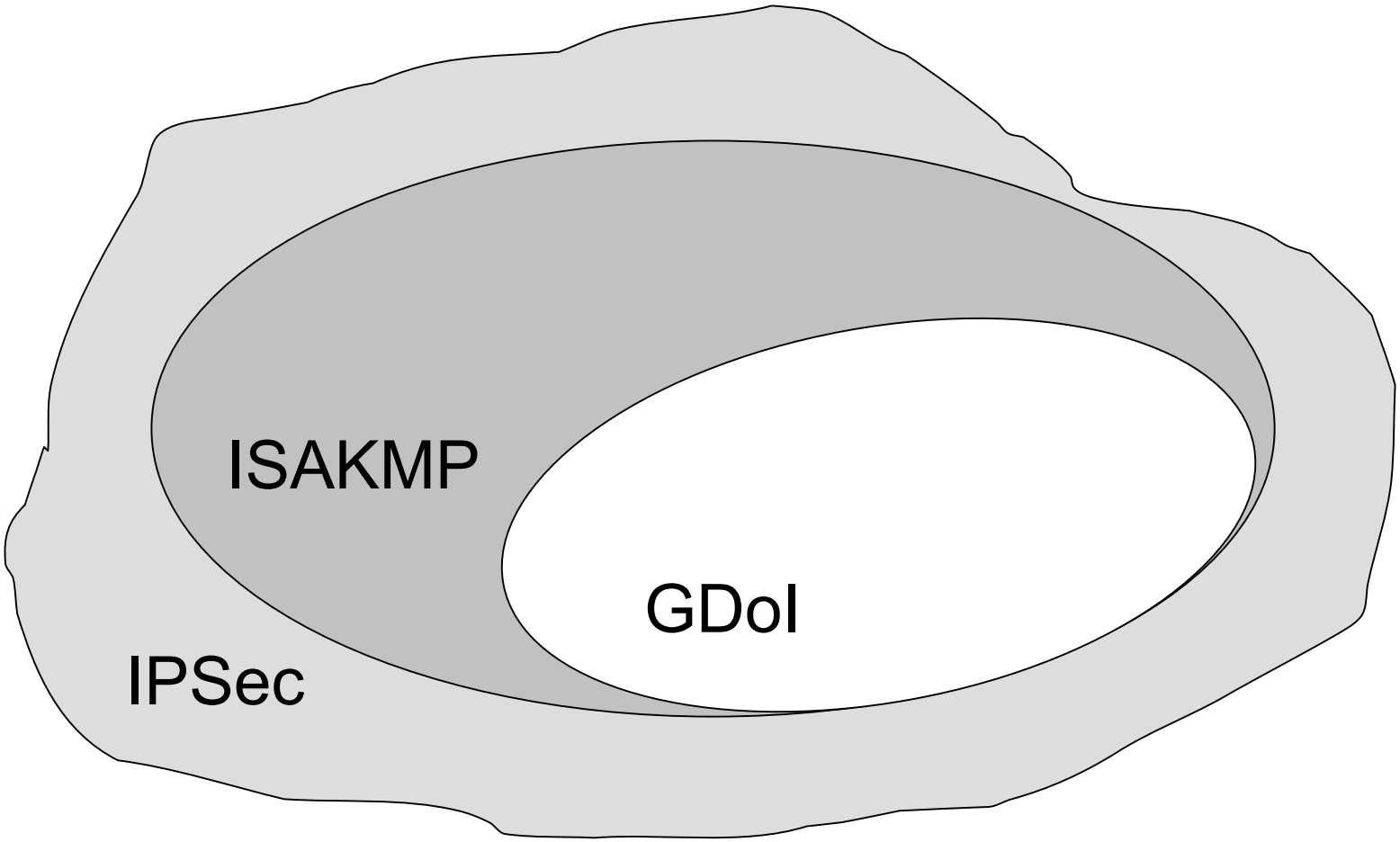


1. Protocols
2. Protocol Derivations
3. Protocol Derivation Assistant

Running example: GDoI



Running example: GDoI



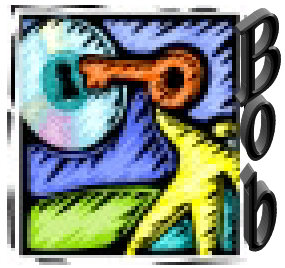
analyzed in joint work with Cathy Meadows

Running example: GDoI

- IPSec [IETF RFC 2400-2410]
  - charter: http://www.ietf.org/html.charters/ipsec-charter.html
- ISAKMP [IETF RFC 2408]
  - documents: http://web.mit.edu/tytso/www/ipsec/
  - distributions: http://web.mit.edu/network/isakmp/
  - implementations: DoD, Cisco
- GDoI [IETF RFC 3547, July 2003]
  - doc.: http://www.networksorcery.com/enp/protocol/gdoi.htm
  - carefully designed: seven internet drafts
  - formally verified and corrected

Group Domain of Interpretation

Group Domain of Interpretation



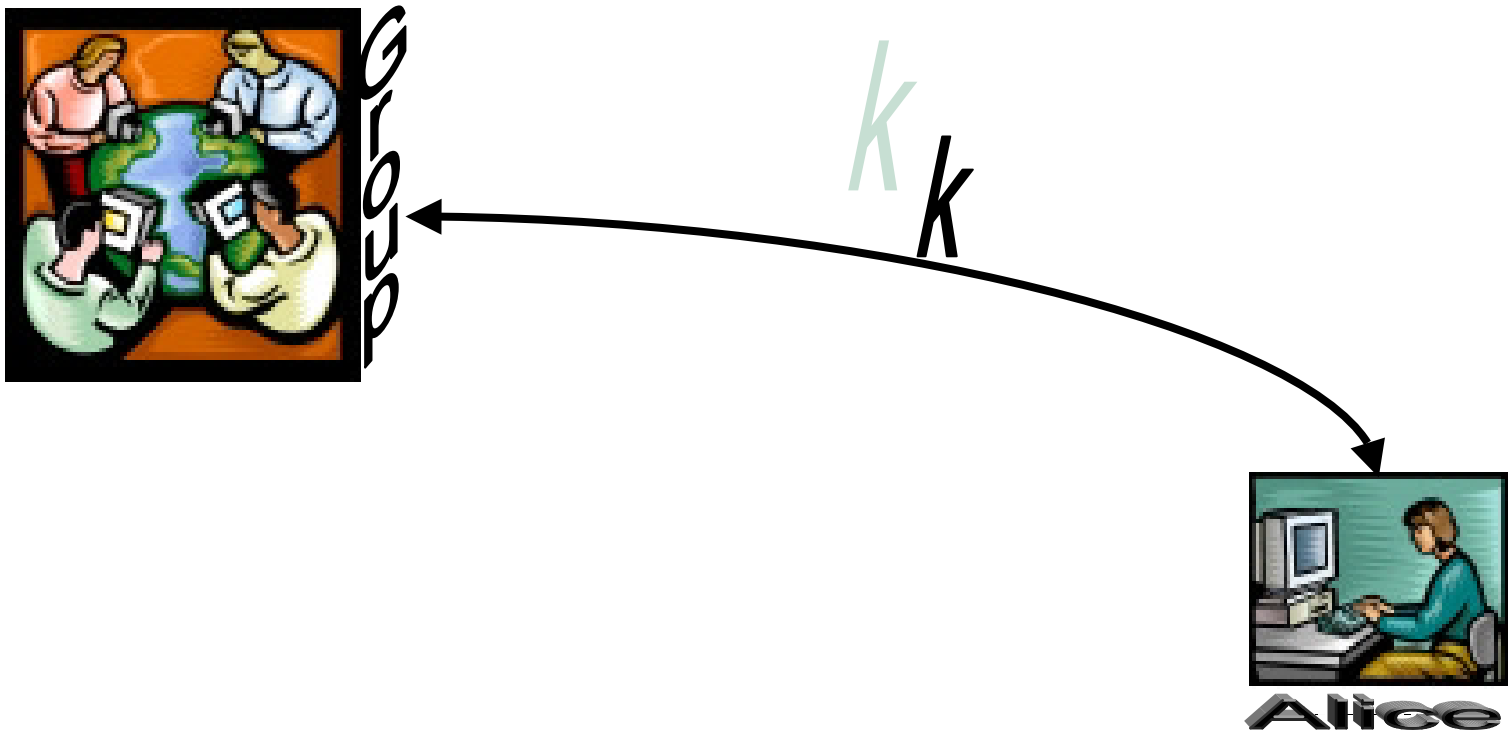
chal[A,B]

resp[A,B], chal[B,A]

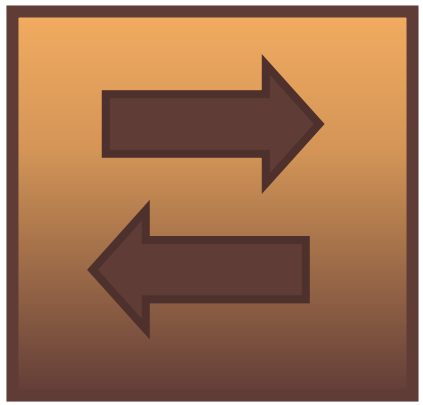
resp[B,A]

k

Group Domain of Interpretation

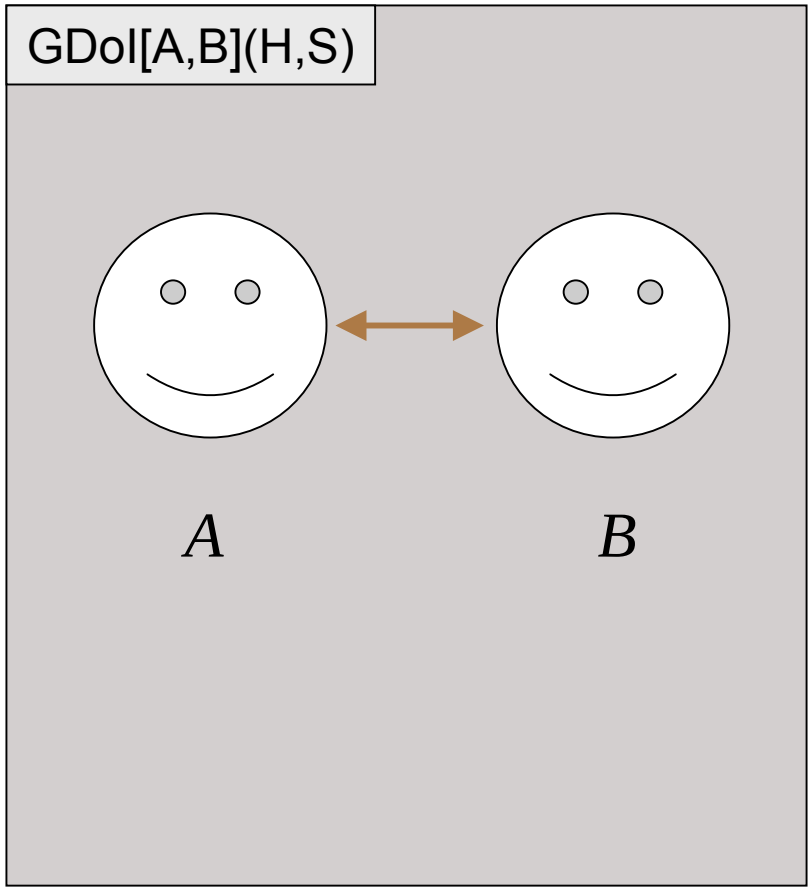


Group Domain of Interpretation

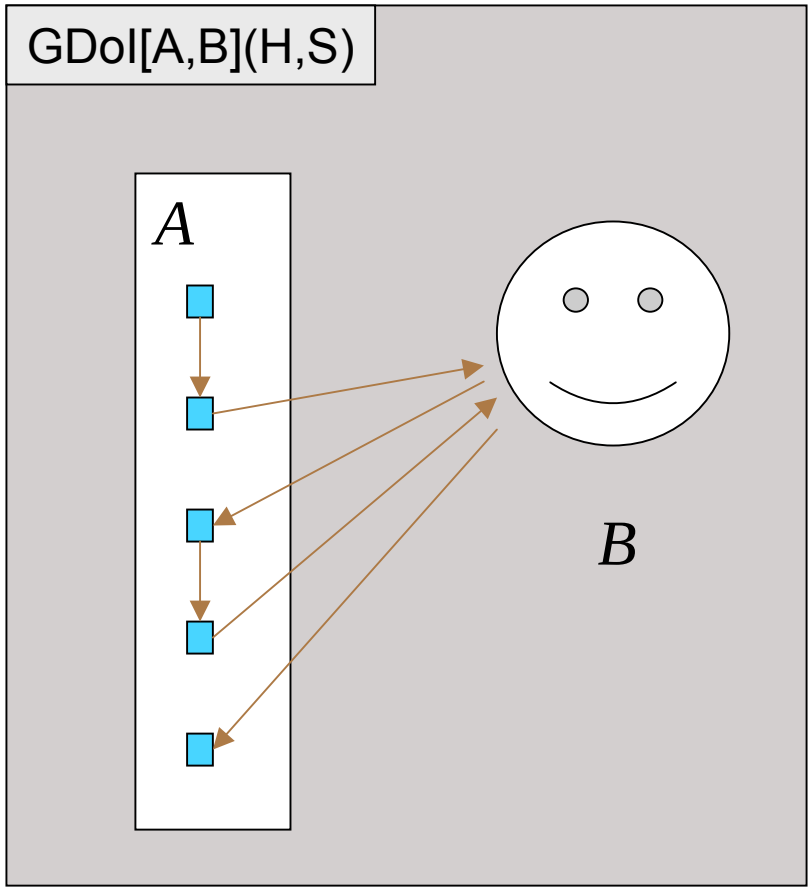


GDoI[A,B](H,S)

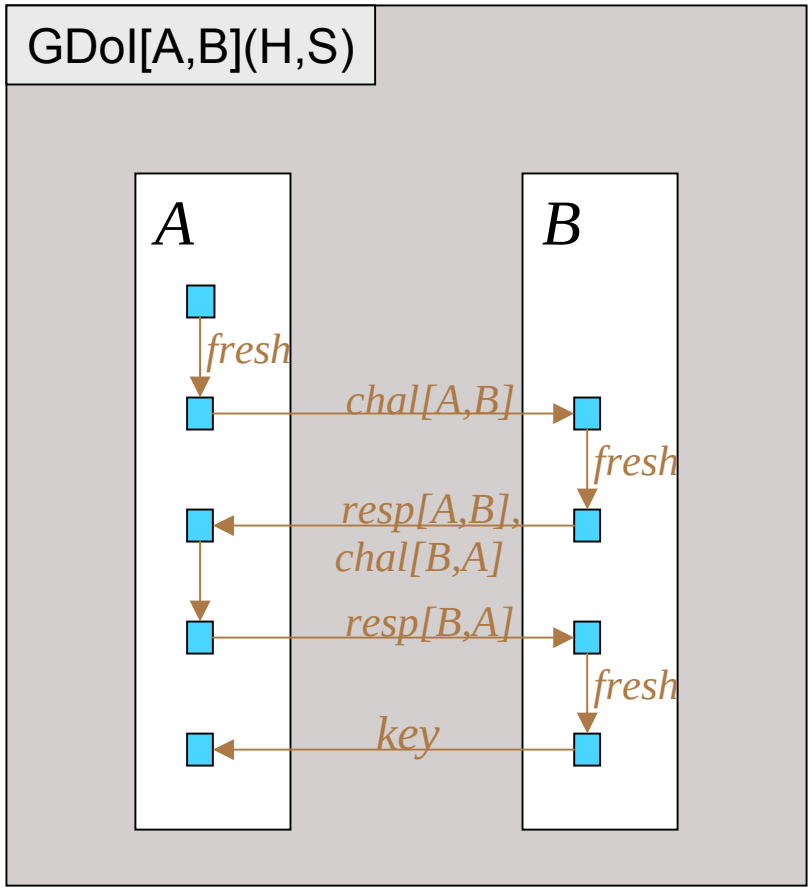
Group Domain of Interpretation



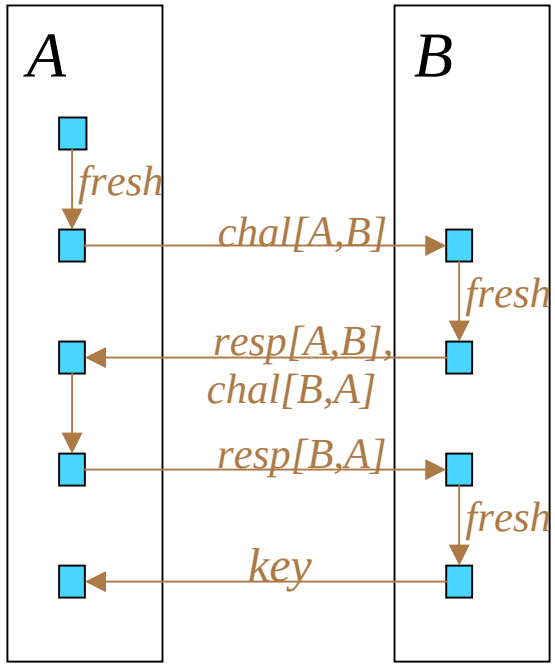
Group Domain of Interpretation



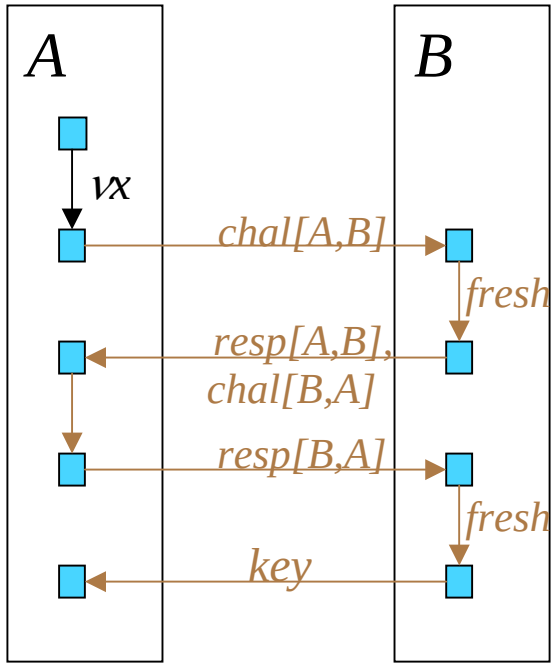
Group Domain of Interpretation



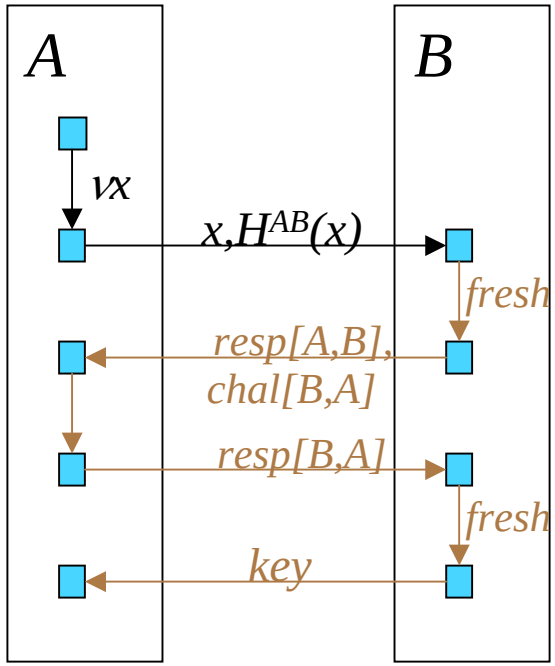
Group Domain of Interpretation



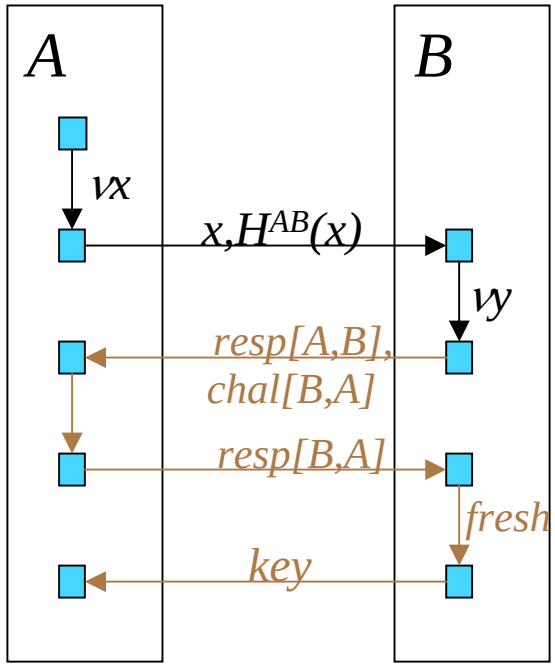
Group Domain of Interpretation



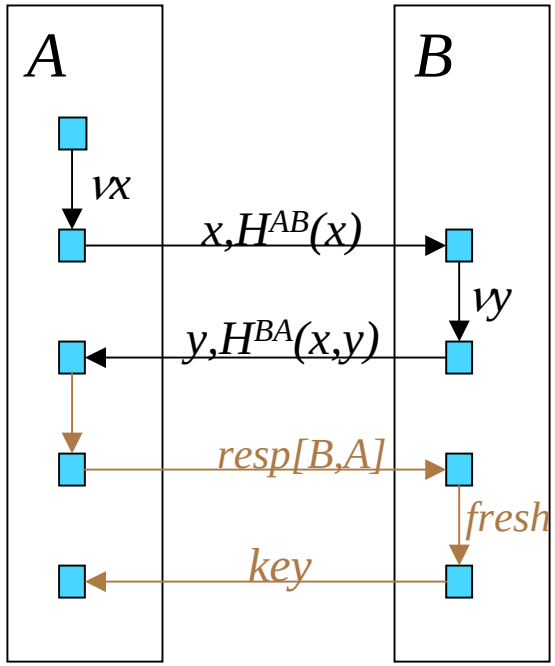
Group Domain of Interpretation



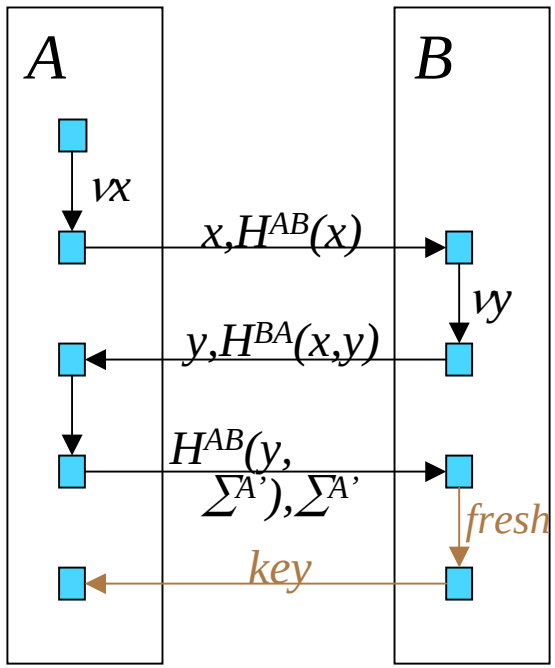
Group Domain of Interpretation



Group Domain of Interpretation

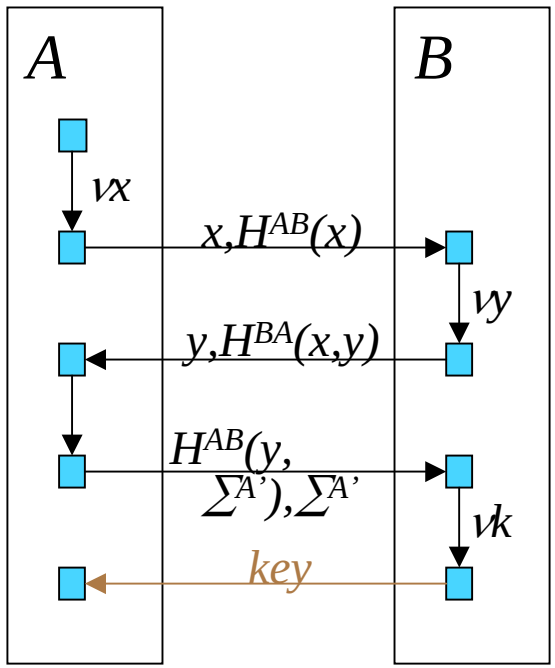


Group Domain of Interpretation



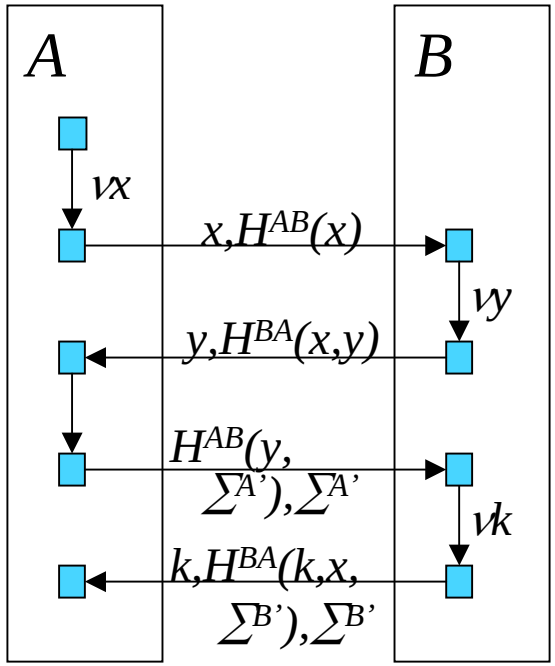
$$\Sigma^Z = C^Z, S^Z(x,y)$$

Group Domain of Interpretation



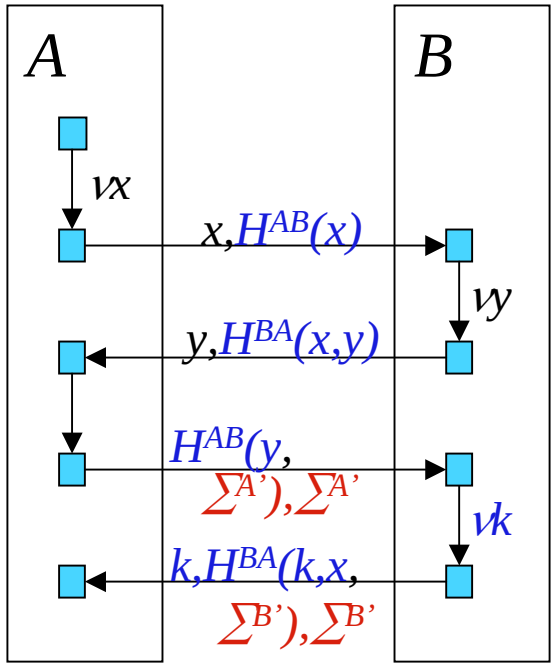
$$\Sigma^Z = C^Z, S^Z(x,y)$$

Group Domain of Interpretation



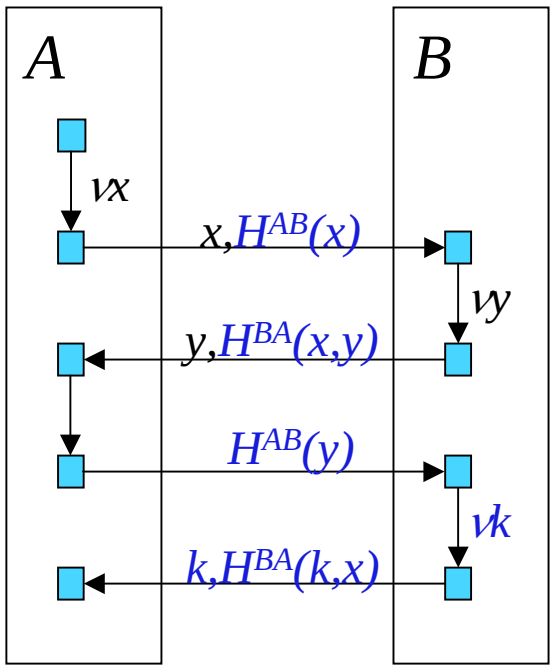
$$\sum^{Z} = C^{Z},S^{Z}(x,y)$$

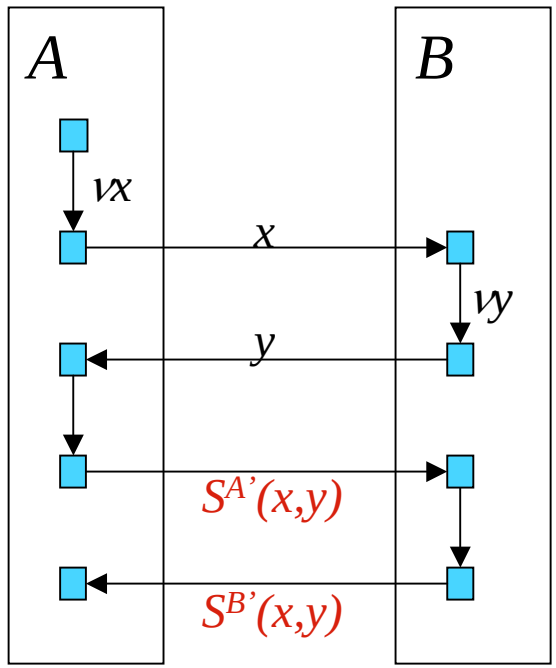
Group Domain of Interpretation



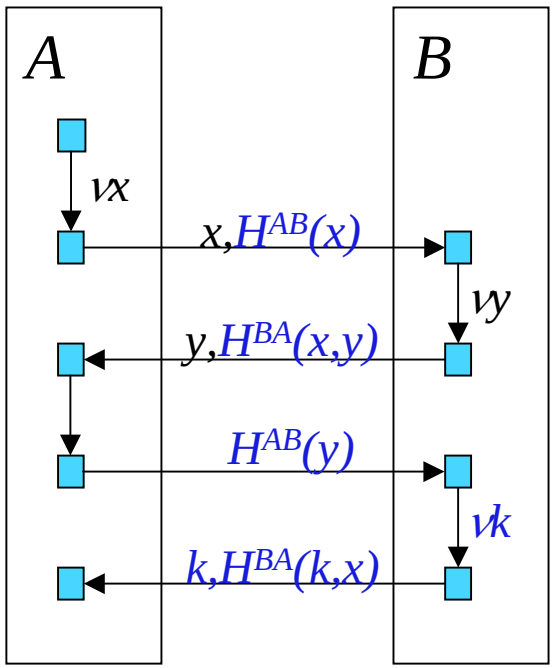
$$\sum^{Z} = C^{Z}, S^{Z}(x,y)$$

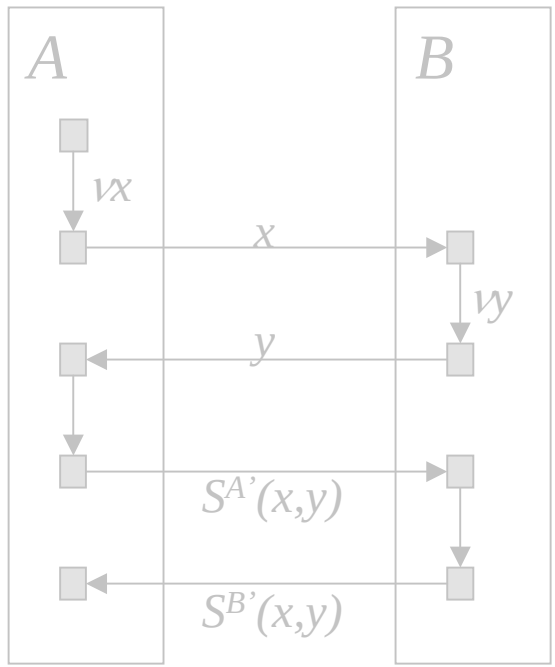
Group Domain of Interpretation



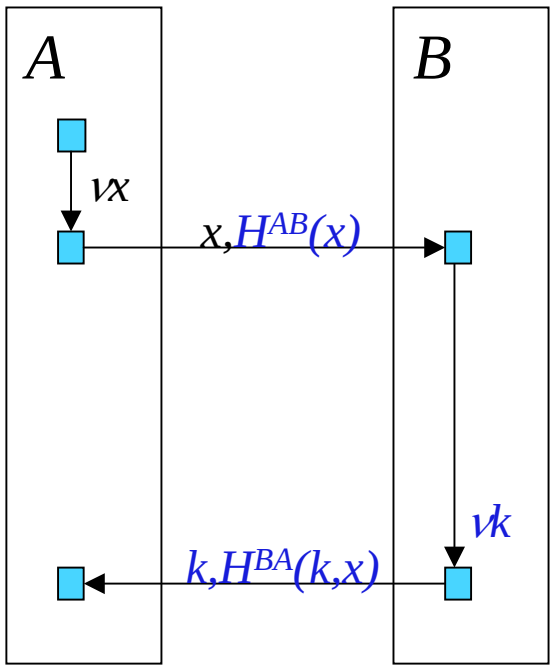


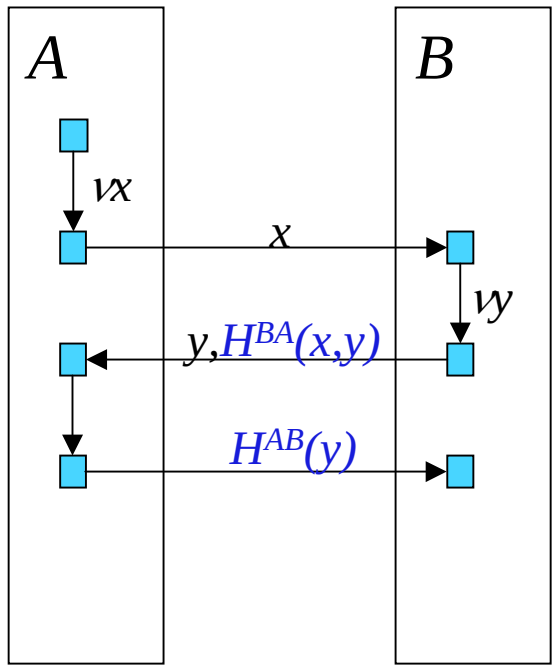
Group Domain of Interpretation



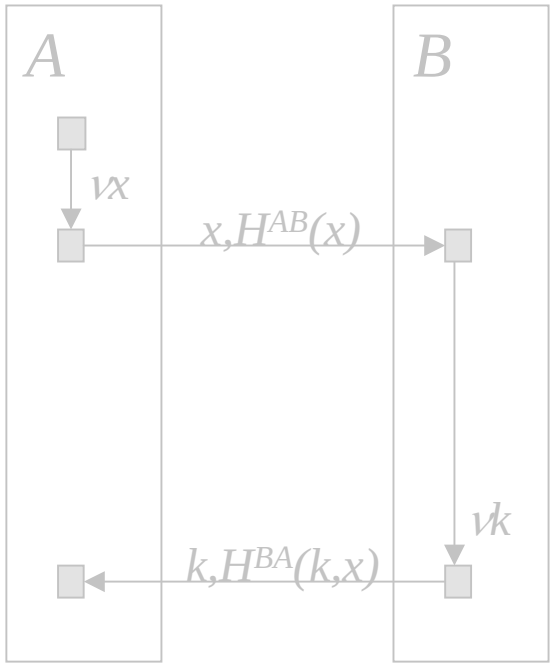


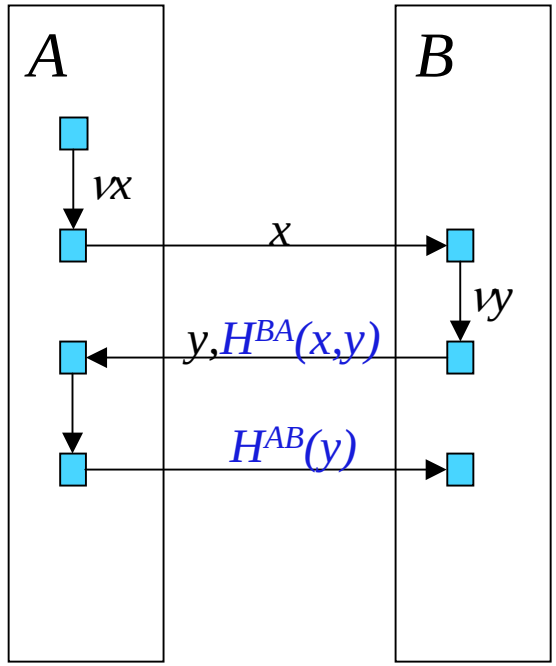
Group Domain of Interpretation



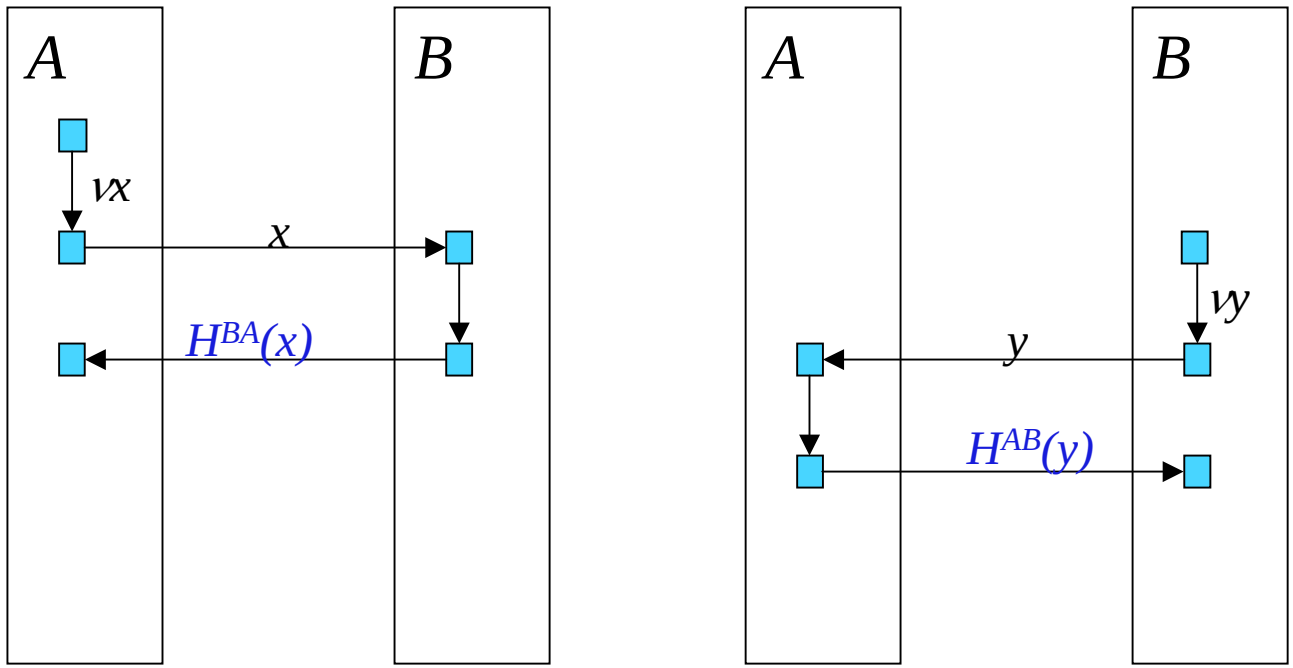


Group Domain of Interpretation

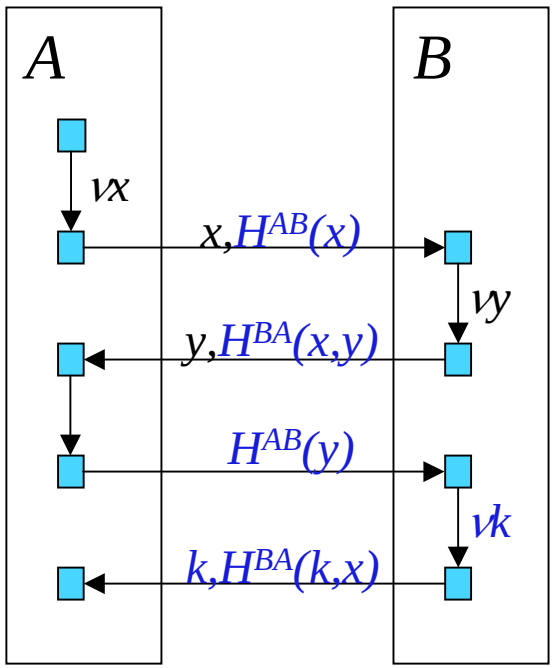


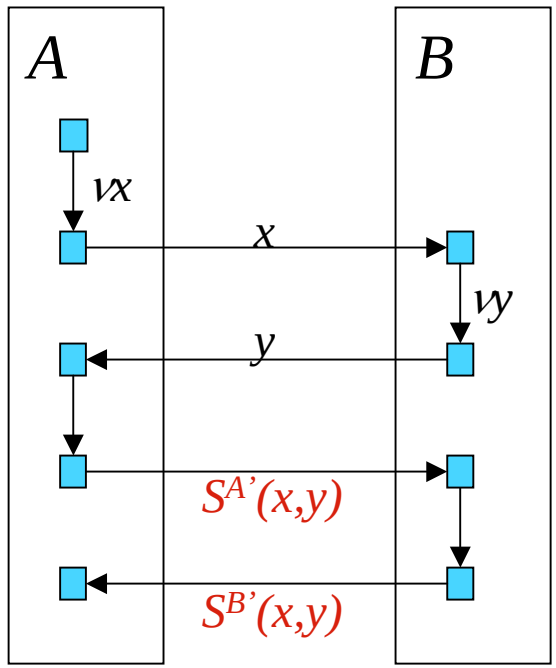


Group Domain of Interpretation

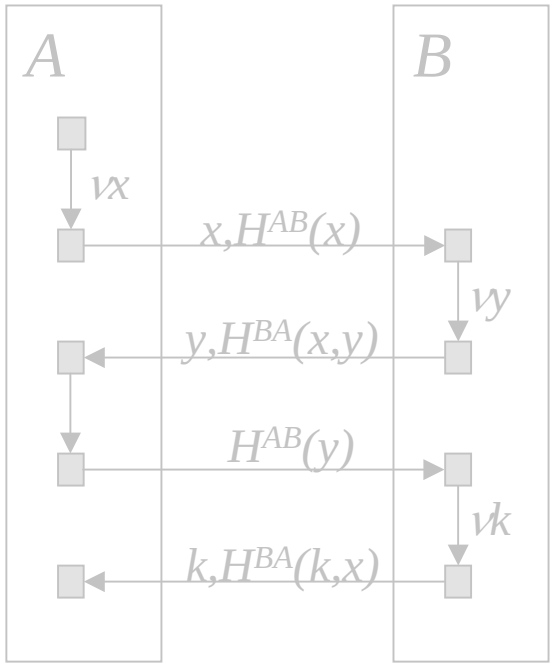


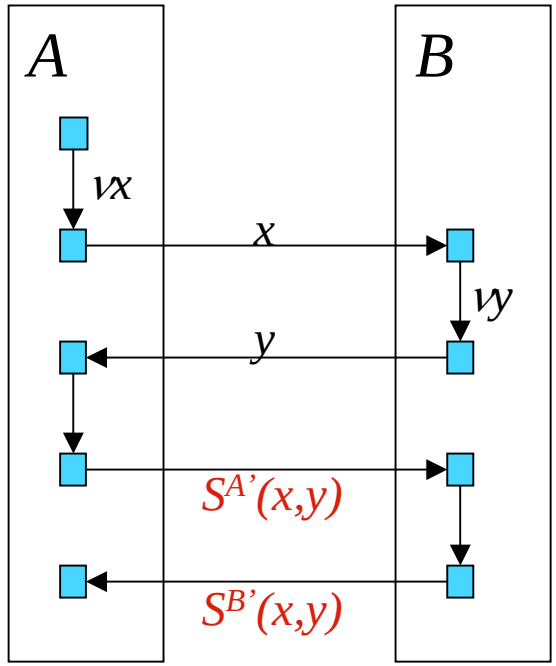
Group Domain of Interpretation



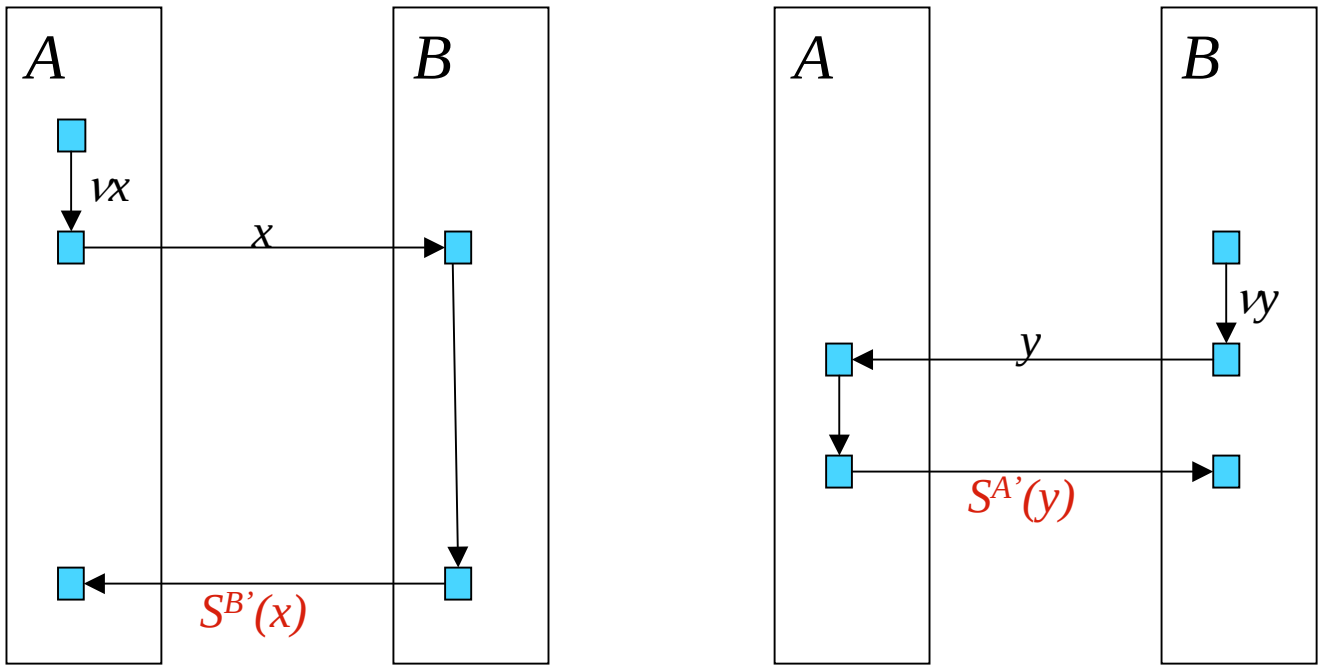


Group Domain of Interpretation





Group Domain of Interpretation



Outline

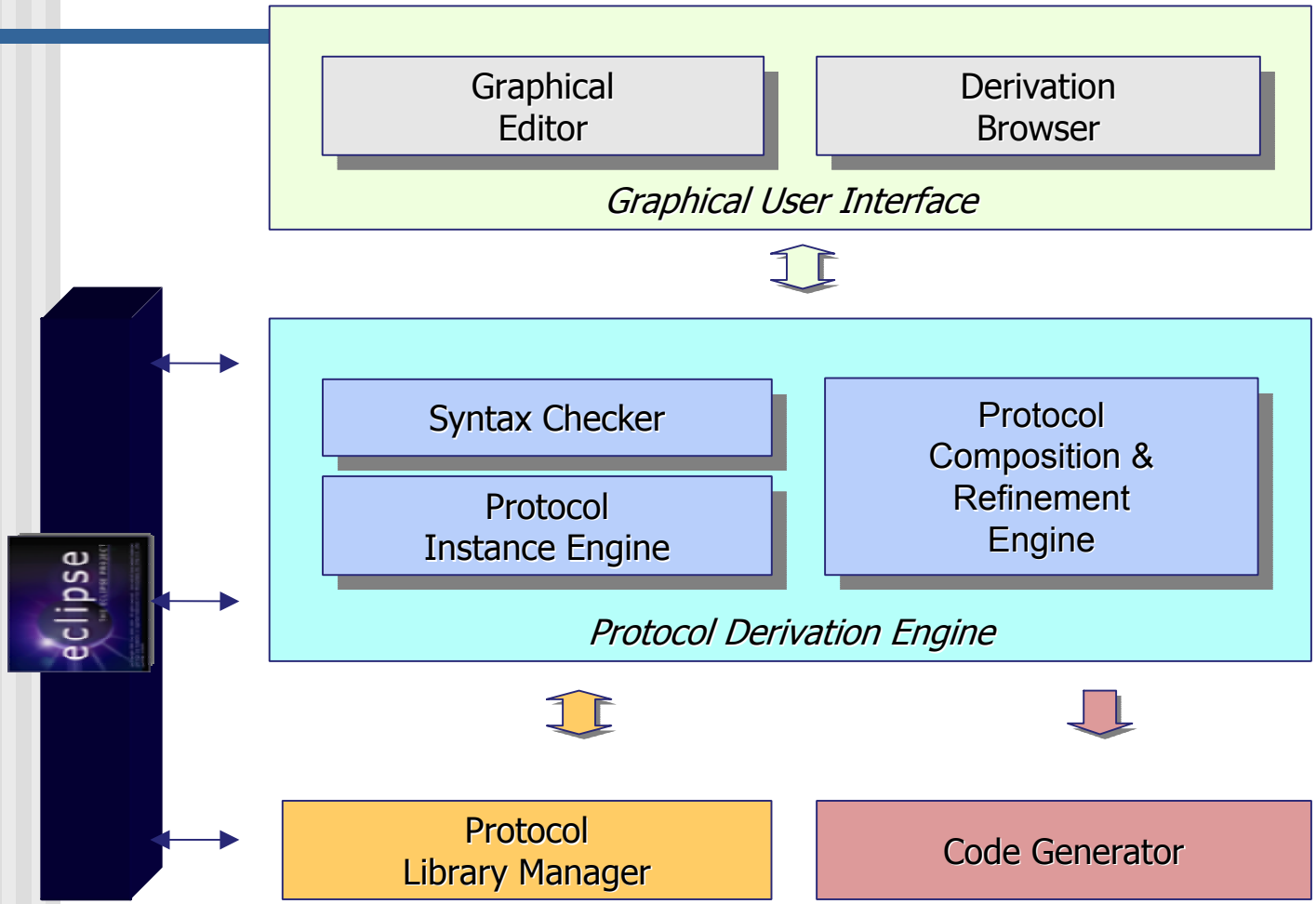
1. Protocols
2. Protocol Derivations
3. Protocol Derivation Assistant

but for derivations we need…

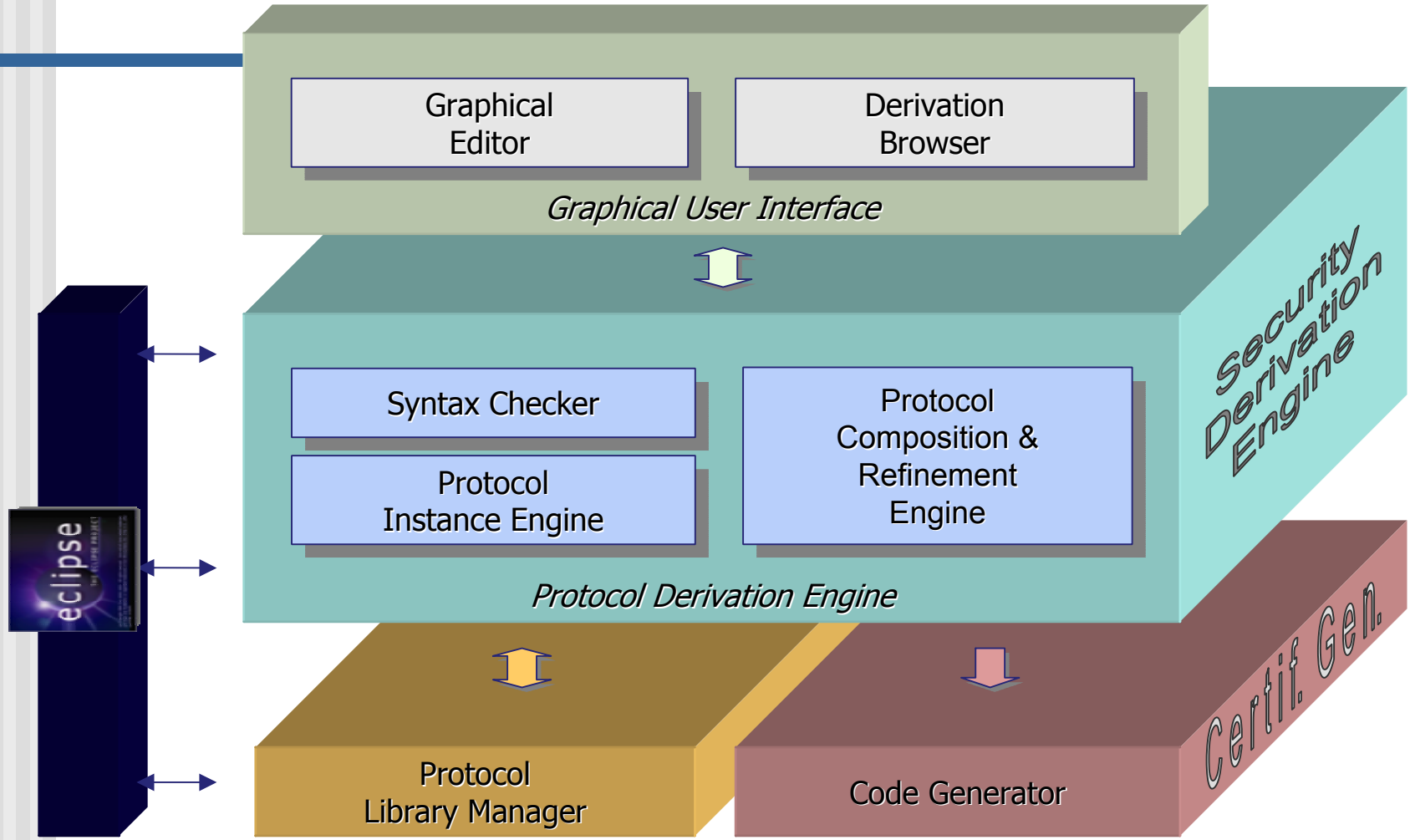
Outline

1. Protocols
2. Protocol Derivations
3. Protocol Derivation Assistant

PDA Architecture



PDA Architecture



Outline

1. Protocols
2. Protocol Derivations
3. Protocol Derivation Assistant

PDA DEMO

Deriving attacks on GDoI.

GDoIv2 proposal.

Summary

- PDA supports:
  - protocol specifications
    - process representations
    - property axioms
    - distributed reasoning
  - composition and refinement of distributed processes
  - evolving taxonomies of protocols and properties
  - rudimentary code generation
- to do:
  - automate property derivations
  - code and certificate generation
  - integrate other tools
  - add crypto

Papers

- An encapsulated authentication logic for reasoning about key distribution protocols
  - with I. Cervesato and C. Meadows, *submitted*
- Deriving, attacking and defending GDOI
  - with C. Meadows, *Proceedings of ESORICS 2004* (Springer LNCS)
- A derivational system and compositional logic for security protocols
  - with A. Datta, A. Derek and J. Mitchell, *J. of Comp. Security* 2004
- Abstraction and refinement in protocol derivation
  - with A. Datta, A. Derek and J. Mitchell, *Proceedings of CSFW 2004* (IEEE)

Papers

- Secure protocol composition
  - with A. Datta and A. Derek and J. Mitchell, *Proceedings of MFPS 2003* (ELNCS); ext. abstract in *FMCS 2003* (ACM)
- Derivation system for security protocols and its logical formalization
  - with A. Datta, A. Derek and J. Mitchell, *Proceedings of CSFW 2003* (IEEE)
- Compositional logic for protocol correctness
  - with N. Durgin and J. Mitchell, *J. of Comp. Security* 2003; eariler version in *CSFW 2001* (IEEE)
- Composition and refinement of behavioral specifications
  - with D. Smith, *ASE 2002* (IEEE)

www.kestrel.edu/users/pavlovic/

PDA web site

www.kestrel.edu/software/pda/