The Goals of Protocols

Joshua D. Guttman
Worcester Polytechnic Institute
The MITRE Corporation

March 2013
Bertinoro International Spring School

Thanks to the US National Science Foundation, under grant 1116557

guttman@wpi.edu

Small semantic theory

For crypto protocols

- Skeletons $\mathbb{A}$:
  - Fragmentary parts of executions
  - Some skeletons are non-fragmentary: realized

Small semantic theory

For crypto protocols

- Skeletons $\mathbb{A}$:
  - Fragmentary parts of executions
  - Some skeletons are non-fragmentary: realized
- Homomorphisms H:
  Structure-preserving maps

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

Small semantic theory

For crypto protocols

- Skeletons $\mathbb{A}$:
  - Fragmentary parts of executions
  - Some skeletons are non-fragmentary: realized
- Homomorphisms H:
  Structure-preserving maps

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

- Test-solving transition relation with test λ:

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

Small semantic theory

For crypto protocols

- Skeletons $\mathbb{A}$:
  - Fragmentary parts of executions
  - Some skeletons are non-fragmentary: realized
- Homomorphisms H:
  Structure-preserving maps

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

- Test-solving transition relation with test λ:

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

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

The key facts

- $\mathbb{A} \rightsquigarrow \mathbb{B}$ implies, for some H, $\quad H \colon \mathbb{A} \rightarrowtail \mathbb{B}$

The key facts

- $\mathbb{A} \rightsquigarrow \mathbb{B}$ implies, for some H, $\quad H \colon \mathbb{A} \rightarrowtail \mathbb{B}$

- CPSA computes from $\mathbb{A}_0$ a set S such that
  1. $\mathbb{A}_1 \in S$ implies $\mathbb{A}_1$ is realized
  2. $\mathbb{A}_1 \in S$ implies $\mathbb{A}_0 \rightsquigarrow^{*} \mathbb{A}_1$
  3. If $\mathbb{A}_0 \rightarrowtail \mathbb{B}$ and $\mathbb{B}$ is realized, then for some $\mathbb{A}_1 \in S$ $\mathbb{A}_1 \rightarrowtail \mathbb{B}$

The key facts

- $\mathbb{A} \rightsquigarrow \mathbb{B}$ implies, for some H, $\quad H \colon \mathbb{A} \rightarrowtail \mathbb{B}$
- CPSA computes from $\mathbb{A}_0$ a set S such that
  1. $\mathbb{A}_1 \in S$ implies $\mathbb{A}_1$ is realized
  2. $\mathbb{A}_1 \in S$ implies $\mathbb{A}_0 \rightsquigarrow^* \mathbb{A}_1$
  3. If $\mathbb{A}_0 \rightarrowtail \mathbb{B}$ and $\mathbb{B}$ is realized, then for some $\mathbb{A}_1 \in S$ $\mathbb{A}_1 \rightarrowtail \mathbb{B}$

S: set of realized, accessible skeletons
that separates $\mathbb{A}_0$ from other realized skeletons

Shapes

- CPSA computes a set of shapes for $\mathbb{A}_0$
  1. $\mathbb{A}_1 \in S$ implies $\mathbb{A}_1$ is realized
  2. $\mathbb{A}_1 \in S$ implies $\mathbb{A}_0 \rightsquigarrow^* \mathbb{A}_1$
  3. If $\mathbb{A}_0 \hookrightarrow \mathbb{B}$ and $\mathbb{B}$ is realized, then for some $\mathbb{A}_1 \in S$ $\mathbb{A}_1 \hookrightarrow \mathbb{B}$
  4. $A_1 \hookrightarrow A_2$ implies $A_1 \simeq A_2$ for $A_1, A_2 \in S$

Shapes

- CPSA computes a set of shapes for $\mathbb{A}_0$
  1. $\mathbb{A}_1 \in S$ implies $\mathbb{A}_1$ is realized
  2. $\mathbb{A}_1 \in S$ implies $\mathbb{A}_0 \rightsquigarrow^* \mathbb{A}_1$
  3. If $\mathbb{A}_0 \hookrightarrow \mathbb{B}$ and $\mathbb{B}$ is realized, then for some $\mathbb{A}_1 \in S$ $\mathbb{A}_1 \hookrightarrow \mathbb{B}$
  4. $A_1 \hookrightarrow A_2$ implies $A_1 \simeq A_2$ for $A_1, A_2 \in S$

S sometimes surprisingly small, e.g. singleton

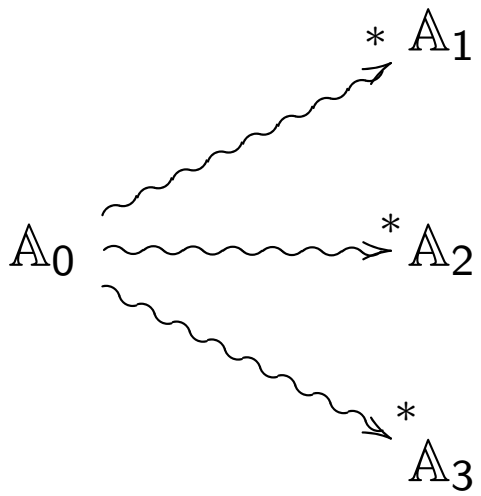
Shapes

- CPSA computes a set of shapes for $\mathbb{A}_0$
  1. $\mathbb{A}_1 \in S$ implies $\mathbb{A}_1$ is realized
  2. $\mathbb{A}_1 \in S$ implies $\mathbb{A}_0 \rightsquigarrow^* \mathbb{A}_1$
  3. If $\mathbb{A}_0 \hookrightarrow \mathbb{B}$ and $\mathbb{B}$ is realized, then for some $\mathbb{A}_1 \in S$ $\mathbb{A}_1 \hookrightarrow \mathbb{B}$
  4. $A_1 \hookrightarrow_{ni} A_2$ implies $A_1 \simeq A_2$ for $A_1, A_2 \in S$

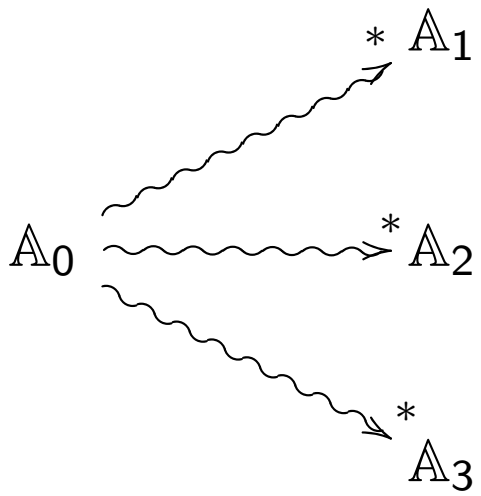
S sometimes surprisingly small, e.g. singleton

"Node-injective" maps

What security goals can CPSA validate?



What security goals can CPSA validate?

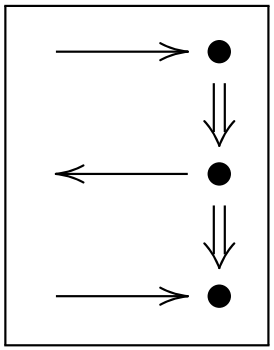


$$\mathbb{A}_0 \rightsquigarrow / \rightsquigarrow^* \cdot$$

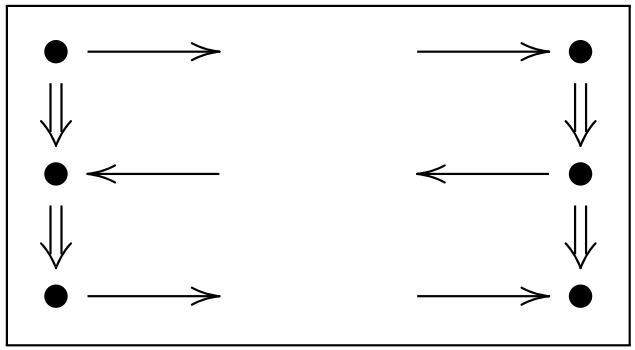
These are authentication and confidentiality goals resp. although allowing great variety

NS Weak Authentication

From responder's point of view



$\xrightarrow{H}$



$\mathrm{Resp}[A, B, N_a, N_b]$

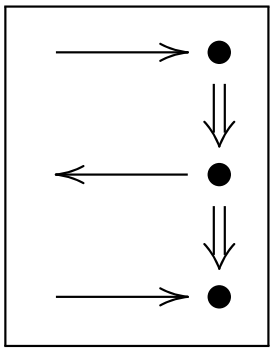
$N_b \in \mathsf{unique}, \quad \mathsf{pubk}(A)^{-1} \in \mathsf{non}$

$\mathrm{Init}[A, B', N_a, N_b] \quad \mathrm{Resp}[A, B, N_a, N_b]$

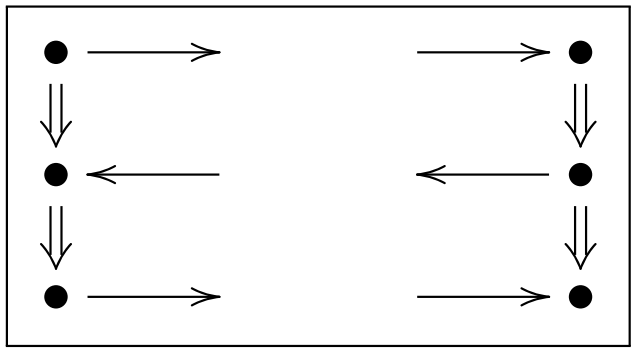
$N_b \in \mathsf{unique}, \quad \mathsf{pubk}(A)^{-1} \in \mathsf{non}$

Stronger Authentication

From responder's point of view



$\xrightarrow{H}$



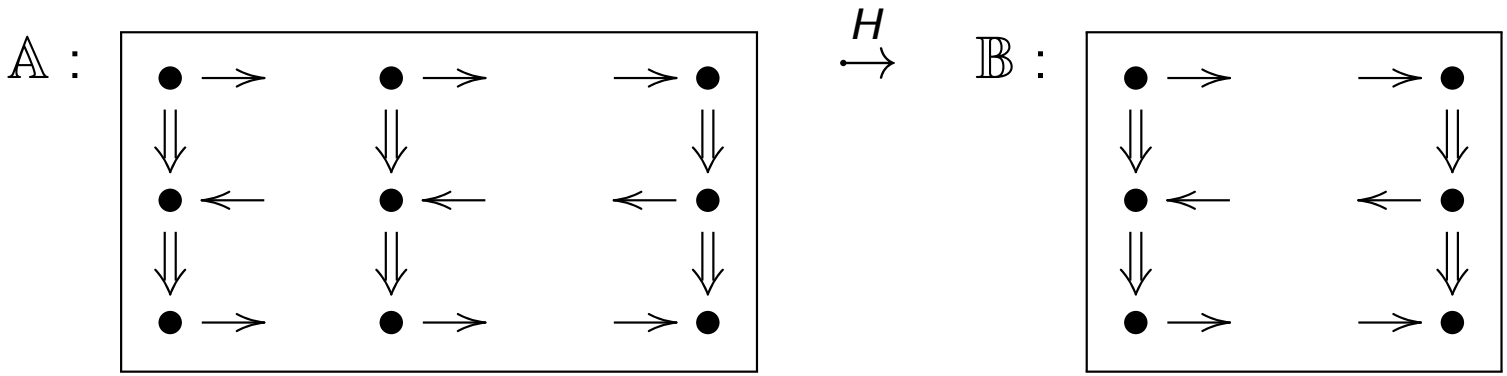
$\mathrm{Resp}[A, B, N_a, N_b]$

$N_b \in \mathsf{unique}, \quad \mathsf{pubk}(A)^{-1} \in \mathsf{non}$

$\mathrm{Init}[A, B, N_a, N_b] \quad \mathrm{Resp}[A, B, N_a, N_b]$

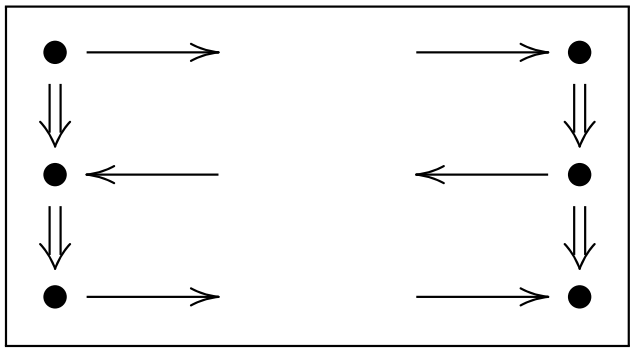
$N_b \in \mathsf{unique}, \quad \mathsf{pubk}(A)^{-1} \in \mathsf{non}$

An Injectiveness Property

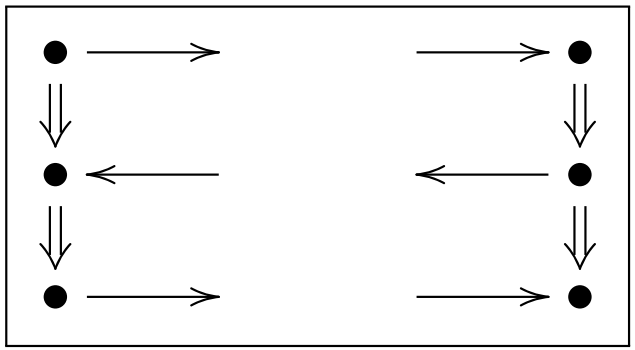


$$N_a, N_b \in \text{unique}, \quad \text{pubk}(A)^{-1} \in \text{non}$$

An Implicit Authentication Property



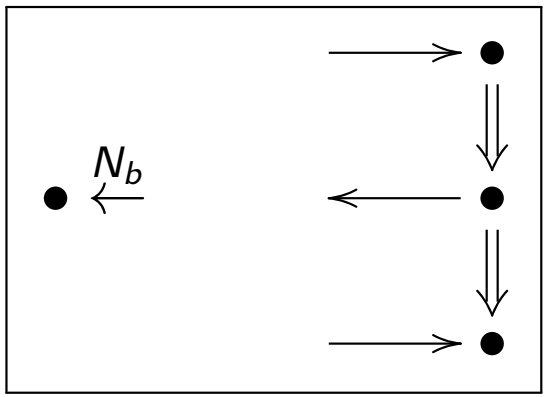
$\xrightarrow{H}$



$\text{Init}[X, Y, N_a, N_b]$ $\text{Resp}[A, B, N_a, N_b]$ $\text{Init}[A, B, N_a, N_b]$ $\text{Resp}[A, B, N_a, N_b]$

A Confidentiality Property

$\mathbb{A}$:

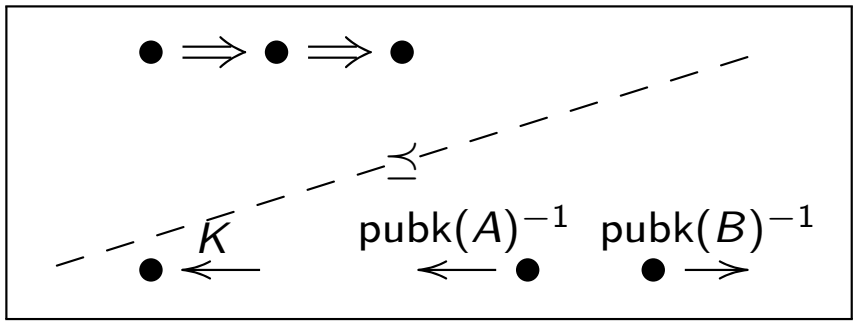


$\not\to$.

$\mathrm{Resp}[A, B, N_a, N_b]$

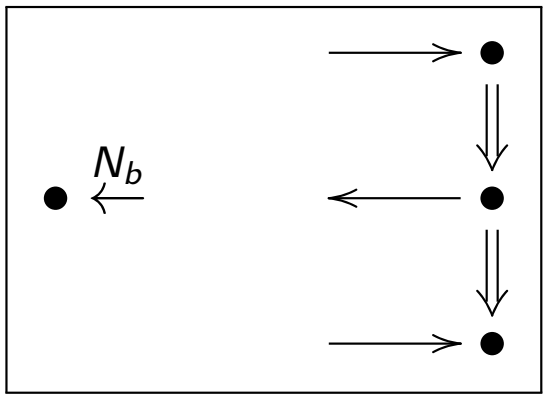
$N_b \in \mathsf{unique}, \quad \mathsf{pubk}(A)^{-1} \in \mathsf{non}$

Forward Secrecy



A Confidentiality Property

$\mathbb{A}$:



$\not\to$.

$$\mathrm{Resp}[A, B, N_a, N_b]$$

$N_b \in \mathsf{unique}, \quad \mathsf{pubk}(A)^{-1} \in \mathsf{non}$

Characterizing $\mathbb{A}$ by a formula

$$\begin{aligned}
&\mathtt{RespThd}(n) \wedge \mathtt{RespScd}(m) \wedge \mathtt{Coll}(m, n) \wedge \mathtt{Lsn}(\ell) \wedge \\
&\mathtt{Hear}(\ell, k) \wedge \mathtt{Peer}(m, a) \wedge \mathtt{Self}(m, b) \\
&\wedge \mathtt{MyNonce}(m, c) \wedge \mathtt{YourNonce}(m, d) \\
&\wedge \mathtt{Non}(\mathtt{inv}(\mathtt{pk}(a))) \wedge \mathtt{UnqAt}(m, c).
\end{aligned} \tag{1}$$

Characterizing $\mathbb{A}$ by a formula

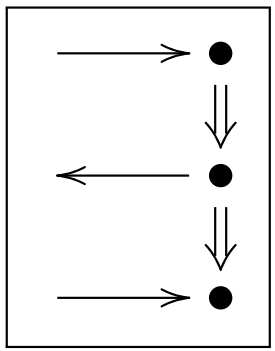
$$\begin{aligned}&\mathtt{RespThd}(n) \wedge \mathtt{RespScd}(m) \wedge \mathtt{Coll}(m,n) \wedge \mathtt{Lsn}(\ell) \wedge \\ &\mathtt{Hear}(\ell,k) \wedge \mathtt{Peer}(m,a) \wedge \mathtt{Self}(m,b) \\ &\wedge \mathtt{MyNonce}(m,c) \wedge \mathtt{YourNonce}(m,d) \\ &\wedge \mathtt{Non}(\mathtt{inv}(\mathtt{pk}(a))) \wedge \mathtt{UnqAt}(m,c).\end{aligned} \tag{1}$$

Goal formula: (1) implies falsehood

Stronger Authentication

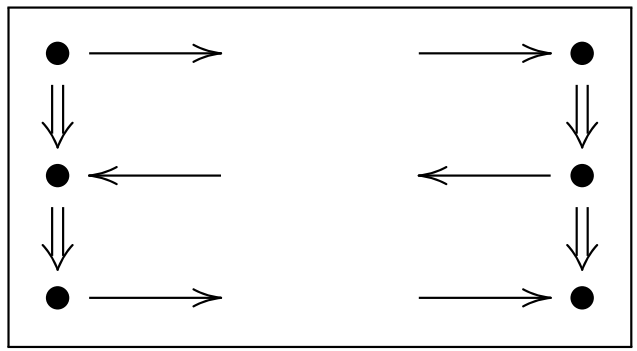
From responder's point of view

$\mathbb{A}'$:



$\xrightarrow{H}$

$\mathbb{B}$:



$\mathrm{Resp}[A, B, N_a, N_b]$

$N_b \in \mathsf{unique}, \quad \mathsf{pubk}(A)^{-1} \in \mathsf{non}$

$\mathrm{Init}[A, B, N_a, N_b] \quad \mathrm{Resp}[A, B, N_a, N_b]$

$N_b \in \mathsf{unique}, \quad \mathsf{pubk}(A)^{-1} \in \mathsf{non}$

Characterizing $\mathbb{A}'$ by a formula

$$\begin{aligned} &\texttt{RespThd}(n) \wedge \texttt{RespScd}(m) \wedge \texttt{Coll}(m, n) \wedge \\ &\texttt{Peer}(m, a) \wedge \texttt{Self}(m, b) \\ &\wedge \texttt{MyNonce}(m, c) \wedge \texttt{YourNonce}(m, d) \\ &\wedge \texttt{Non}(\texttt{inv}(\texttt{pk}(a))) \wedge \texttt{UnqAt}(m, c). \end{aligned} \tag{2}$$

Characterizing $\mathbb{B}$ by a formula

$$
\begin{aligned}
&(2) \wedge \texttt{InitThd}(n') \wedge \\
&\texttt{Self}(n', a) \wedge \texttt{Peer}(n', b) \wedge \\
&\texttt{YourNonce}(n', c) \wedge \texttt{MyNonce}(n', d)
\end{aligned}
\tag{3}
$$

Characterizing $\mathbb{B}$ by a formula

$$\begin{aligned} &(2) \wedge \texttt{InitThd}(n') \wedge \\ &\texttt{Self}(n', a) \wedge \texttt{Peer}(n', b) \wedge \\ &\texttt{YourNonce}(n', c) \wedge \texttt{MyNonce}(n', d) \end{aligned} \tag{3}$$

Goal formula: (2) implies $\exists n'$. (3)

The Goal Language $\mathcal{GL}(\Pi)$ of a Protocol

- Protocol-independent vocabulary

Functions:	$\texttt{pk}(a)$	$\texttt{sk}(a)$	$\texttt{inv}(k)$
	$\texttt{lts}(a, b)$		
Relations:	$\texttt{Preceq}(m, n)$	$\texttt{Coll}(m, n)$	$=$
	$\texttt{Unq}(v)$	$\texttt{UnqAt}(n, v)$	$\texttt{Non}(v)$

The Goal Language $\mathcal{GL}(\Pi)$ of a Protocol

- Protocol-independent vocabulary

Functions:	$\texttt{pk}(a)$	$\texttt{sk}(a)$	$\texttt{inv}(k)$
	$\texttt{lts}(a, b)$		
Relations:	$\texttt{Preceq}(m, n)$	$\texttt{Coll}(m, n)$	$=$
	$\texttt{Unq}(v)$	$\texttt{UnqAt}(n, v)$	$\texttt{Non}(v)$

- Protocol specific vocabulary for Π
  - Role predicates, e.g.

    `RespFst(n)` `RespScd(n)` `RespThd(n)` `Lsn(n)`

  - Parameter predicates, e.g.

    `Self(n,a)` `MyNonce(n,c)` `YourNonce(n,c)`

Security Goals in $\mathcal{GL}(\Pi)$

- Φ is positive existential: built from atomic formulas using

  and or there exists

Security Goals in $\mathcal{GL}(\Pi)$

- Φ is positive existential: built from atomic formulas using

  and or there exists

- "Positive existential" matches "preserved under homomorphisms"

Security Goals in $\mathcal{GL}(\Pi)$

- Φ is positive existential: built from atomic formulas using

  and or there exists

- "Positive existential" matches "preserved under homomorphisms"
- $\Phi \supset \Psi$ is a security goal if

  Φ, Ψ are positive existential in $\mathcal{GL}(\Pi)$

Security Goals in $\mathcal{GL}(\Pi)$

- Φ is positive existential: built from atomic formulas using

  and or there exists

- "Positive existential" matches "preserved under homomorphisms"
- $\Phi \supset \Psi$ is a security goal if

  Φ, Ψ are positive existential in $\mathcal{GL}(\Pi)$

- Every security goal equivalent to a set of formulas

$$\phi \supset \bigvee_{i<k} \exists \vec{y_k} \,.\, \phi_i$$

where ϕ and ϕ_i are conjunctions of atoms

Skeletons are Models, Goals are Implications

- Each skeleton $\mathbb{A}$ is a finite structure
  - Has a "characteristic formula" $\mathsf{cf}(\mathbb{A})$ expressing its content
  - $\mathsf{cf}(\mathbb{A})$ is a conjunction of atomic formulas
  - $\mathbb{A} \rightarrow \mathbb{B}$ if and only if $\mathbb{B} \models_\eta \mathsf{cf}(\mathbb{A})$

Skeletons are Models, Goals are Implications

- Each skeleton $\mathbb{A}$ is a finite structure
  - Has a "characteristic formula" $\mathsf{cf}(\mathbb{A})$ expressing its content
  - $\mathsf{cf}(\mathbb{A})$ is a conjunction of atomic formulas
  - $\mathbb{A} \rightarrow \mathbb{B}$ if and only if $\mathbb{B} \models_\eta \mathsf{cf}(\mathbb{A})$
- What if $\mathbb{A}$ has shape set S in protocol Π?

Skeletons are Models, Goals are Implications

- Each skeleton $\mathbb{A}$ is a finite structure
  - Has a "characteristic formula" $\mathsf{cf}(\mathbb{A})$ expressing its content
  - $\mathsf{cf}(\mathbb{A})$ is a conjunction of atomic formulas
  - $\mathbb{A} \hookrightarrow \mathbb{B}$ if and only if $\mathbb{B} \models_\eta \mathsf{cf}(\mathbb{A})$
- What if $\mathbb{A}$ has shape set S in protocol Π?
- Π bundles then satisfy:

$$\mathsf{cf}(\mathbb{A}) \supset \bigvee_{\mathbb{B} \in S} \exists \vec{y} \,.\, \mathsf{cf}(\mathbb{B})$$

where $\vec{y}$ includes all variables free in $\mathsf{cf}(\mathbb{B})$ but not in $\mathsf{cf}(\mathbb{A})$