Cryptoprotocol transformations that preserve goals

Joshua D. Guttman

Worcester Polytechnic Institute

Dedicated to Bob Dylan
on his 70th birthday

Thanks to: National Science Foundation
(Grant CNS-0952287).

8 Mar 2013
BiSS

A Protocol Design Problem

- Protocol designers

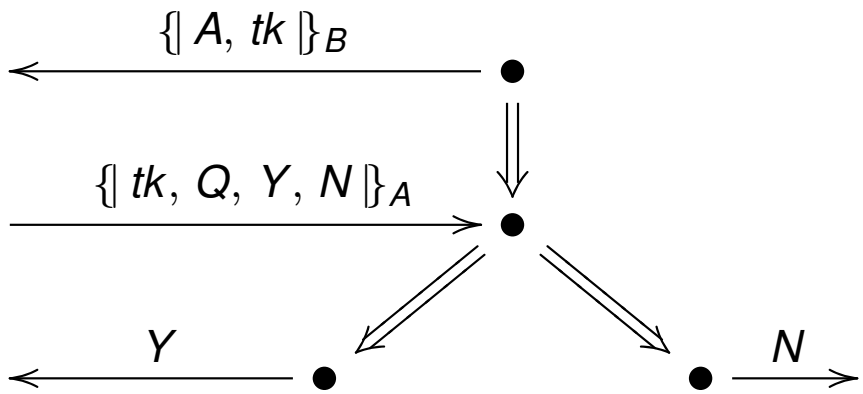
  reuse, adapt, combine

  existing protocols
- Want to achieve additional

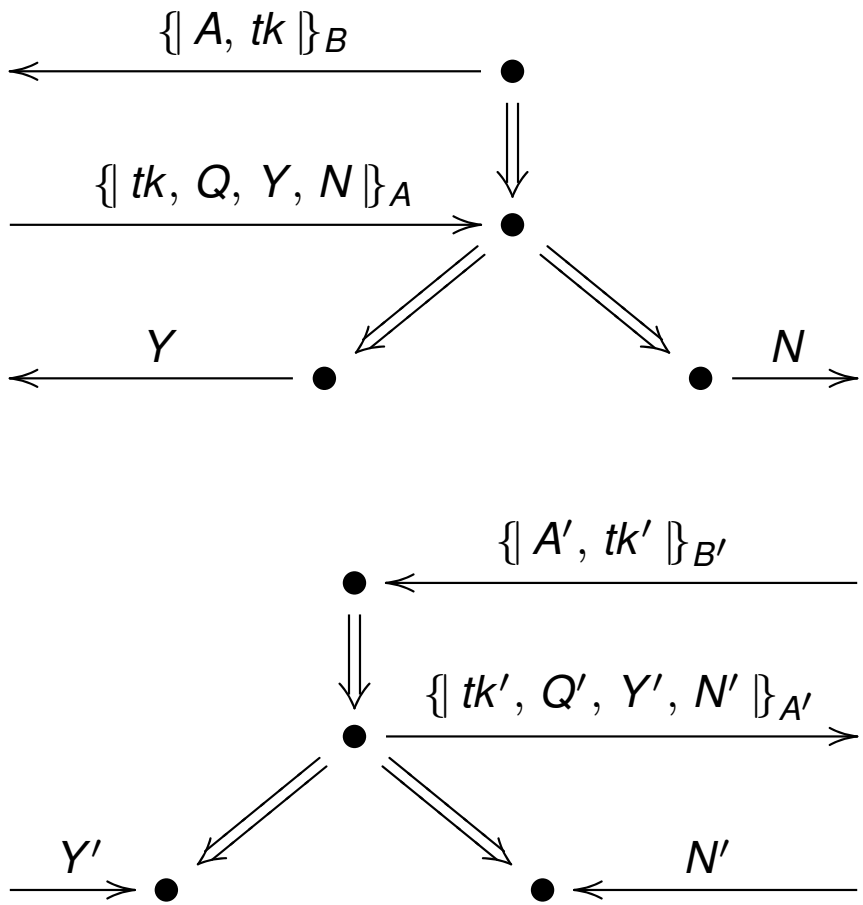
  authentication and confidentiality goals
- Under what conditions are

  source protocol goals preserved?

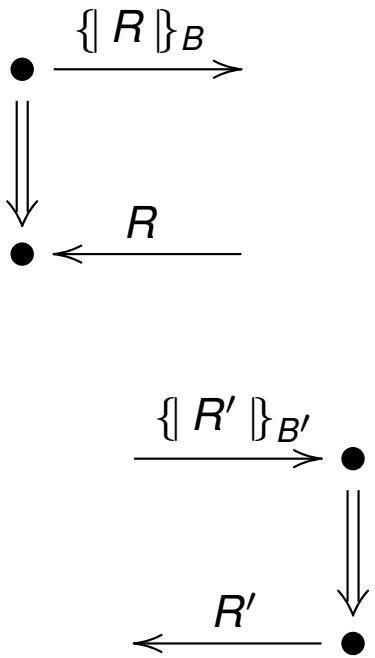
Example: Q & A



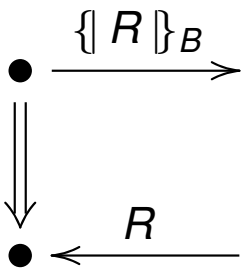
Example: Q & A

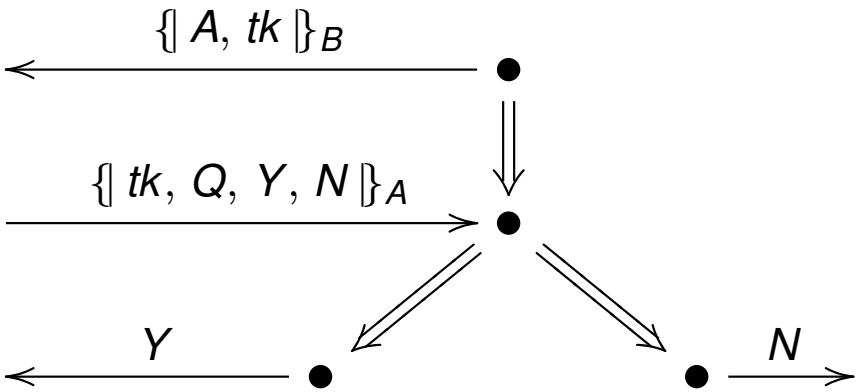


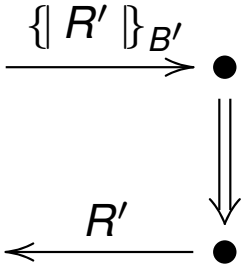
HD: A simple protocol

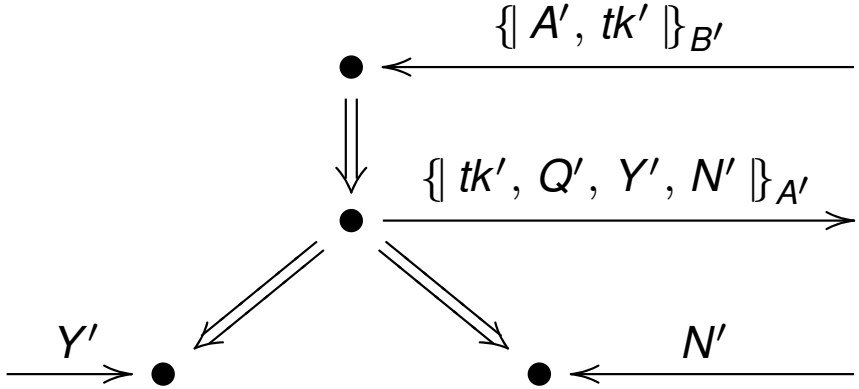


Q & A uses the HD idea

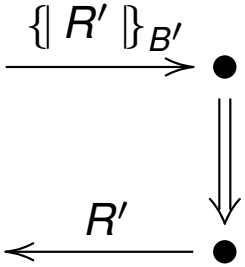


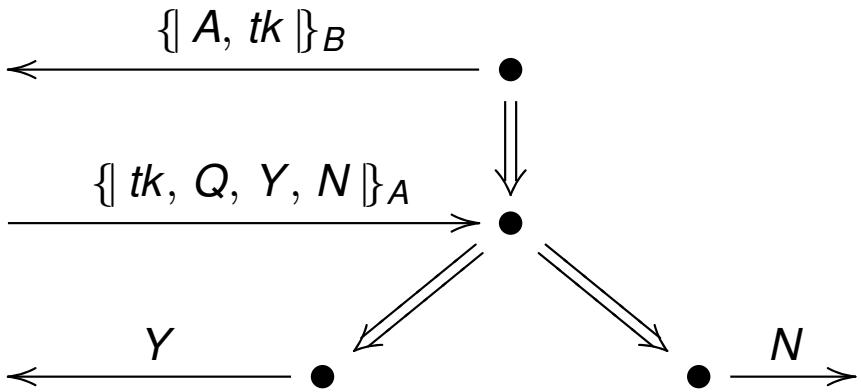


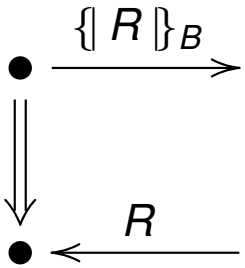


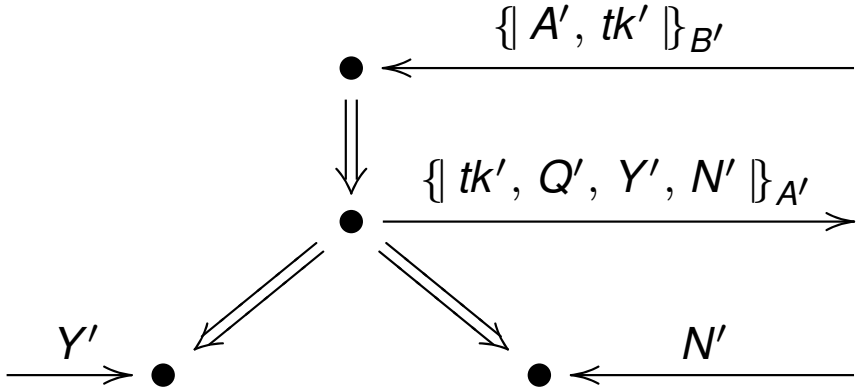


Q & A uses the HD idea repeatedly









Protocol Transformations

- Illustrated several protocol transformations

$$F : \mathrm{HD} \rightarrow \mathrm{Q\ \&\ A}$$

- Each F maps
  - transmissions to transmissions
  - receptions to receptions

  preserving order etc.

Protocol Design Problem

- Protocol designers transform existing protocols
- Want to achieve additional

  authentication and confidentiality goals
- When do transformations preserve security goals?
- Key idea:

  Don't focus on syntactic similarity;
  Focus on similarity in the analysis process

Protocol analysis as scenario-finding

- Protocol analysis activity
  - Start with a partial execution
  - Enrich it, seeking a full execution
  - Branch when alternate enrichments possible

Protocol analysis as scenario-finding

- Protocol analysis activity
  - Start with a partial execution
  - Enrich it, seeking a full execution
  - Branch when alternate enrichments possible
- Scenario-finding in protocol Π is a labeled transition system

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

Protocol analysis as scenario-finding

Preserving goals means preserving analysis

- Protocol analysis activity
  - Start with a partial execution
  - Enrich it, seeking a full execution
  - Branch when alternate enrichments possible
- Scenario-finding in protocol Π is a labeled transition system

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

- Π_2 preserves goals of Π_1 if (roughly)

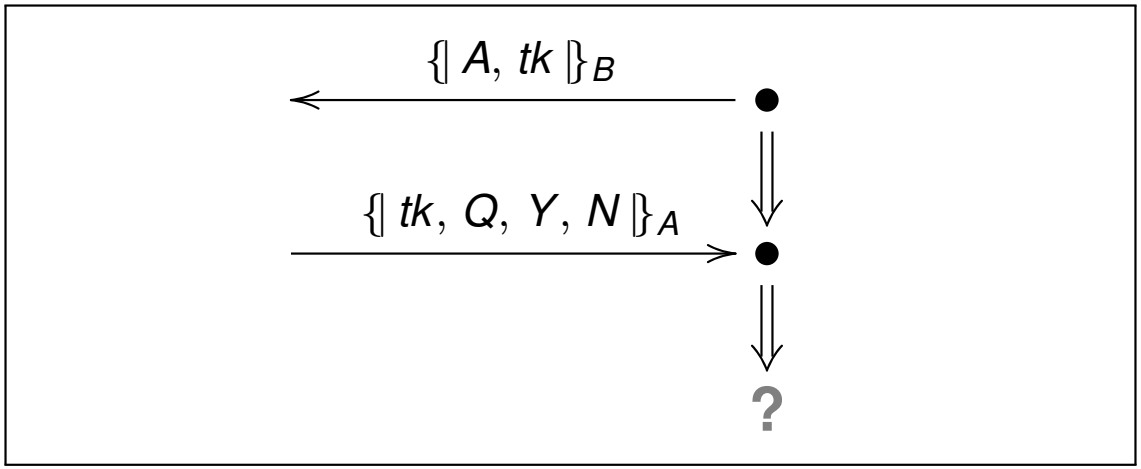
  scenario-finding in Π_1 $\rightsquigarrow_1$ *simulates*
  scenario-finding in Π_2 $\rightsquigarrow_2$

  and

  When $\rightsquigarrow_1$ *can progress, so can* $\rightsquigarrow_2$

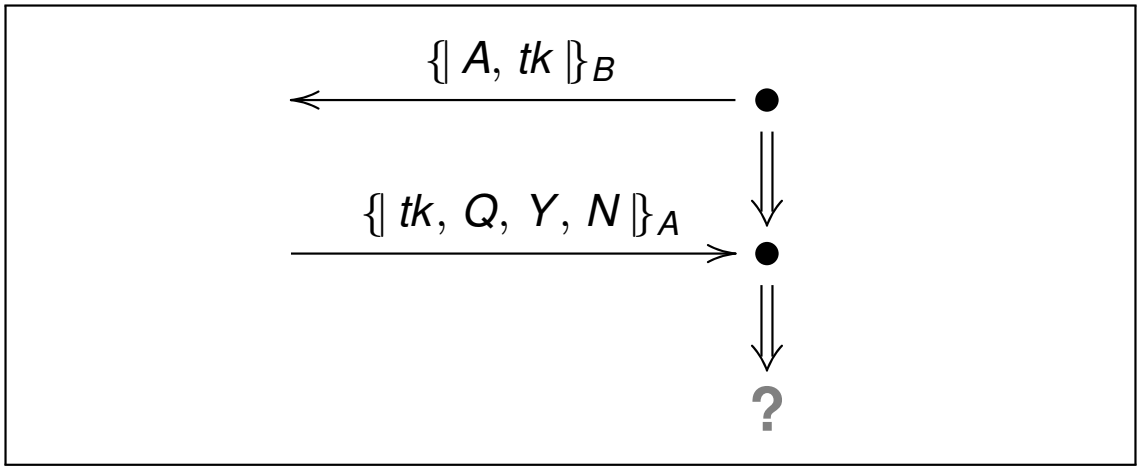
Protocol Analysis for Q & A

One scenario



Protocol Analysis for Q & A

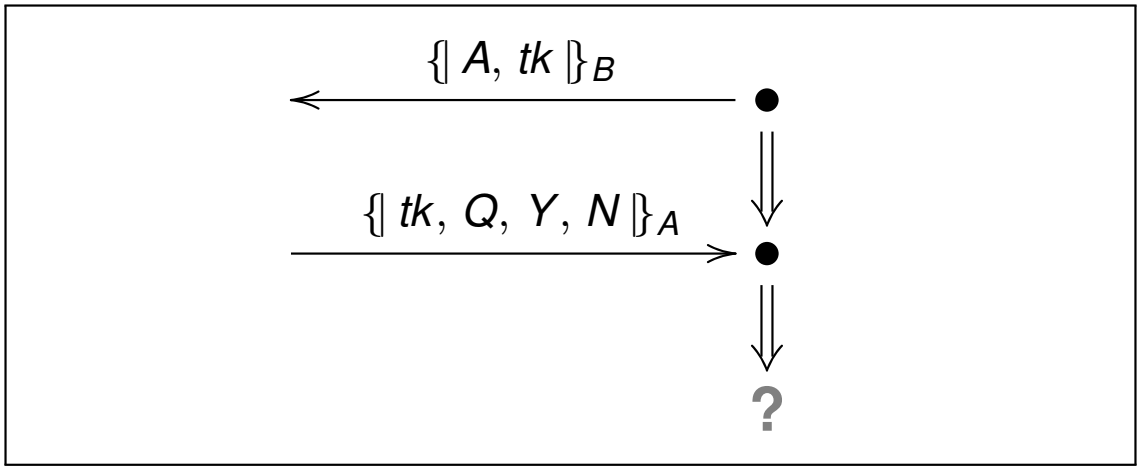
One scenario



What must be true if the Answerer offers a token and gets a query?

Protocol Analysis for Q & A

One scenario



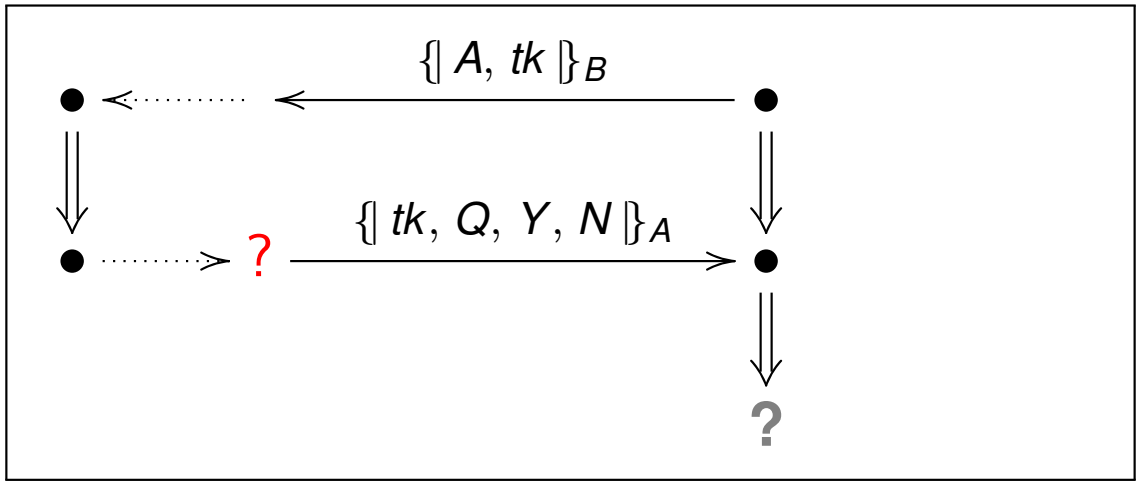
What must be true if the Answerer offers a token and gets a query?

It depends on the assumptions. Assume:

tk freshly chosen
privk(B) uncompromised

Protocol Analysis for Q & A

One scenario



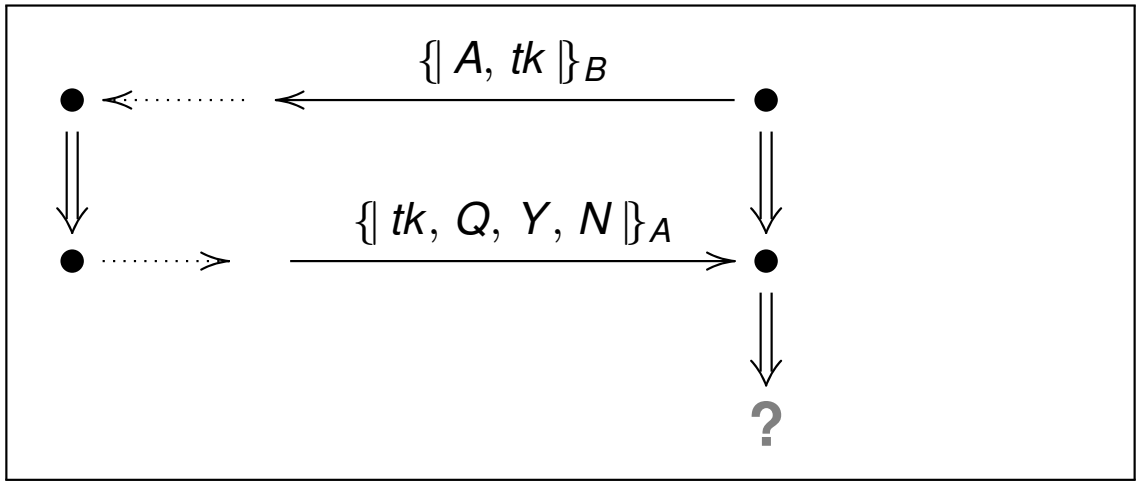
What must be true if the Answerer offers a token and gets a query?

It depends on the assumptions. Assume:

tk freshly chosen
privk(B) uncompromised

Protocol Analysis for Q & A

One scenario



What must be true if the Answerer offers a token and gets a query?

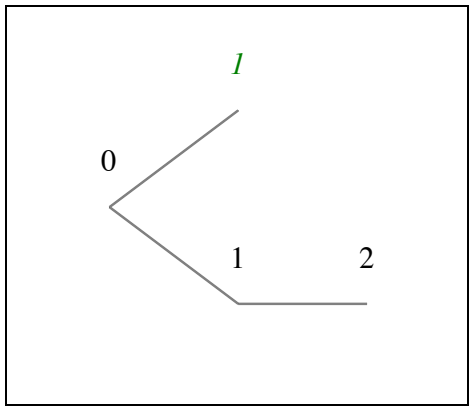
It depends on the assumptions. Assume:

tk freshly chosen
privk(B) uncompromised
privk(A) uncompromised

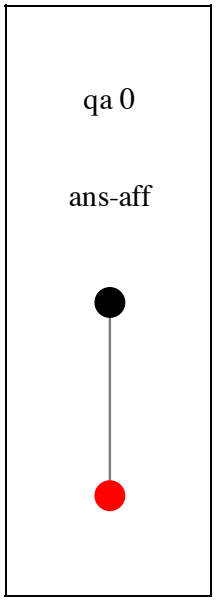
Q & A: Scenario in CPSA

tk fresh, privk(*A*), privk(*B*) uncompromised

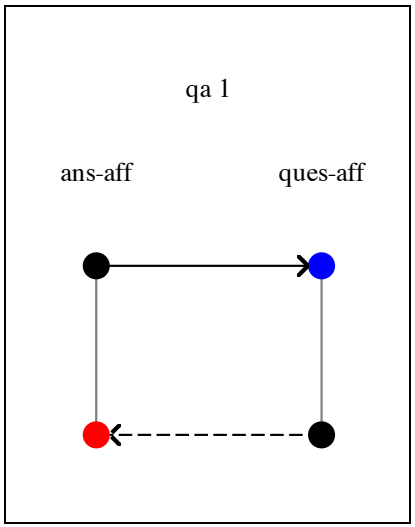
Tree 0.



Item 0, Child: 1, Seen Child: 1.

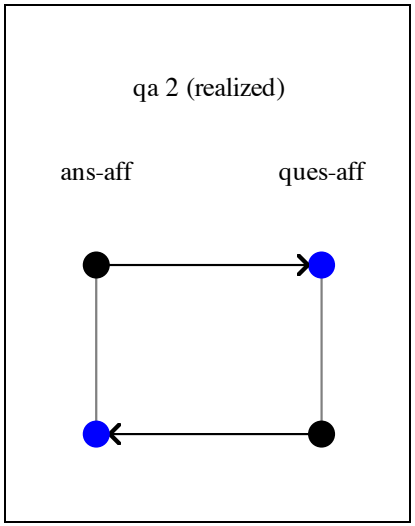


Item 1, Parent: 0, Child: 2.




```
(defstrand ans-aff 2  q tk y n a b)
(defstrand ques-aff 2 q-0 tk y-0 n-0 a b)
```

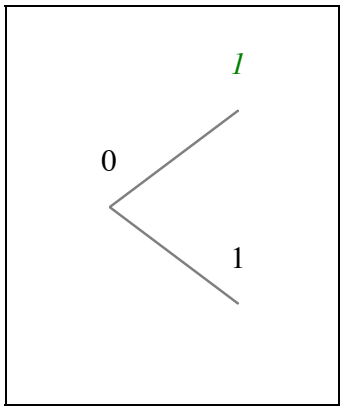
Item 2, Parent: 1.



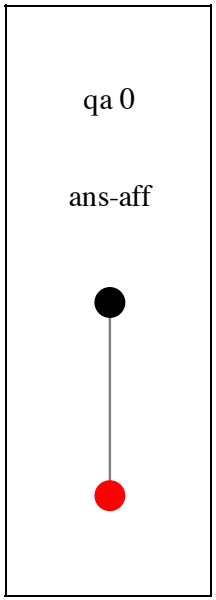
Q & A: Weakened Scenario in CPSA

tk fresh, privk(*B*) uncompromised

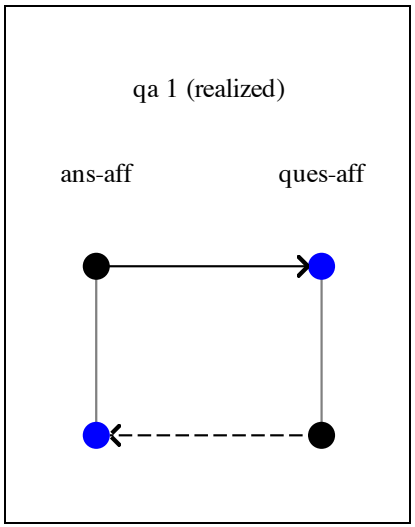
Tree 0.



Item 0, Child: 1, Seen Child: 1.



Item 1, Parent: 0.

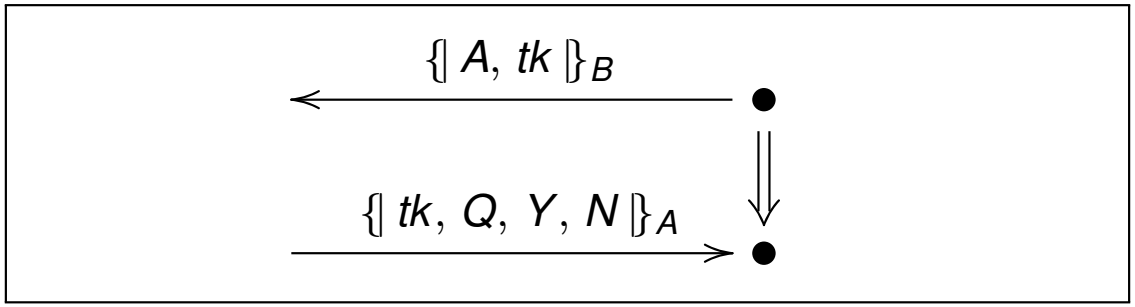


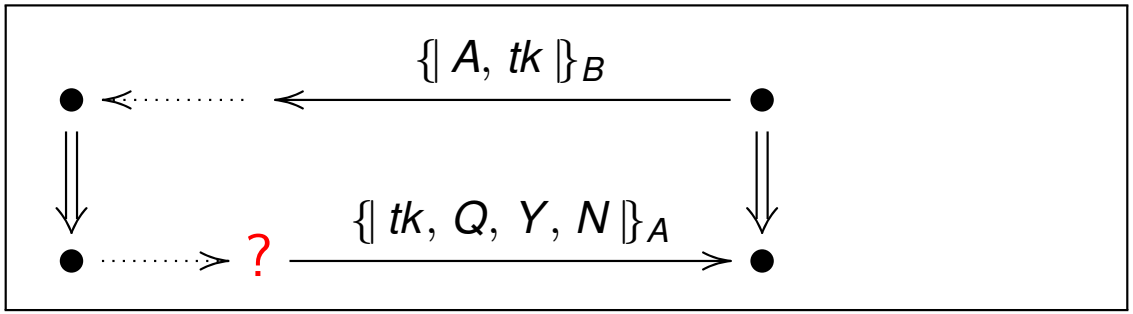

```
(defstrand ans-aff 2 q tk y n a b)
(defstrand ques-aff 2 q-0 tk y-0 n-0 a b)
```

“Skeletons”

Assume:

tk freshly chosen
privk(B) uncompromised

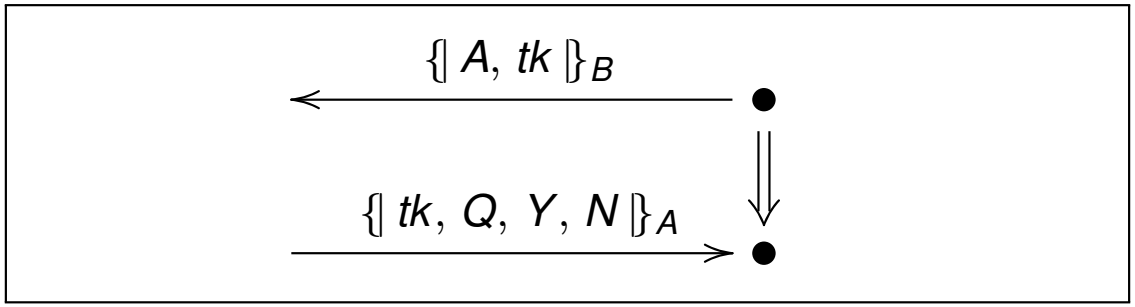


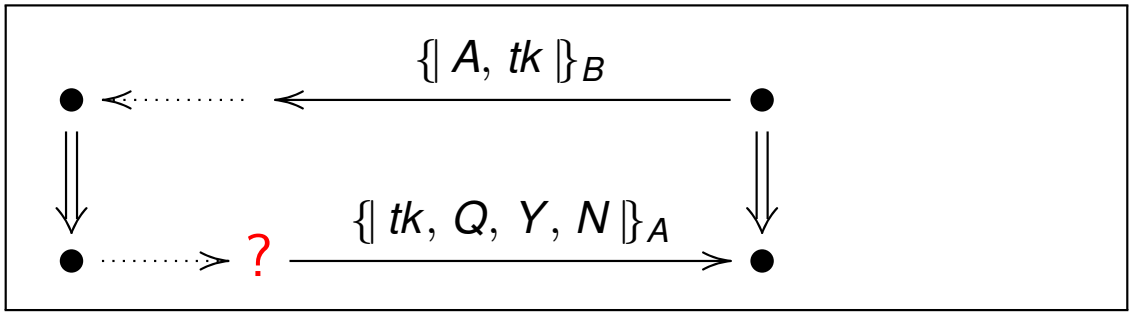


"Skeletons"

Assume:

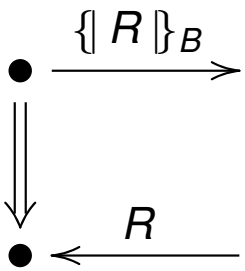
tk freshly chosen
privk(B) uncompromised

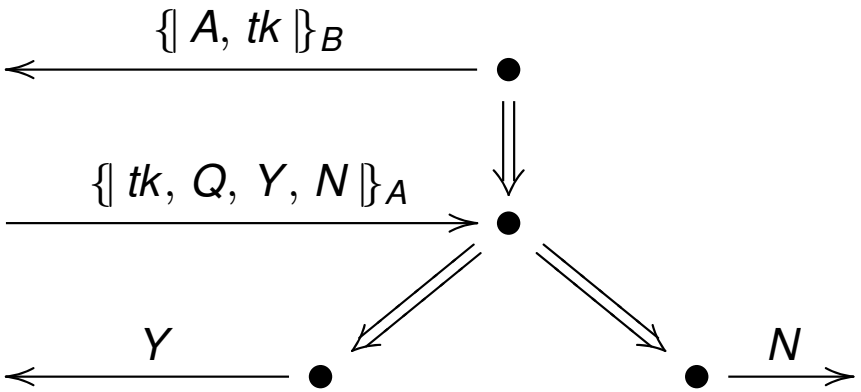


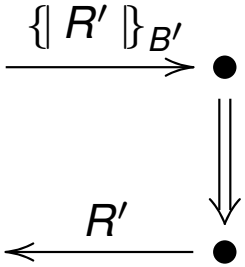


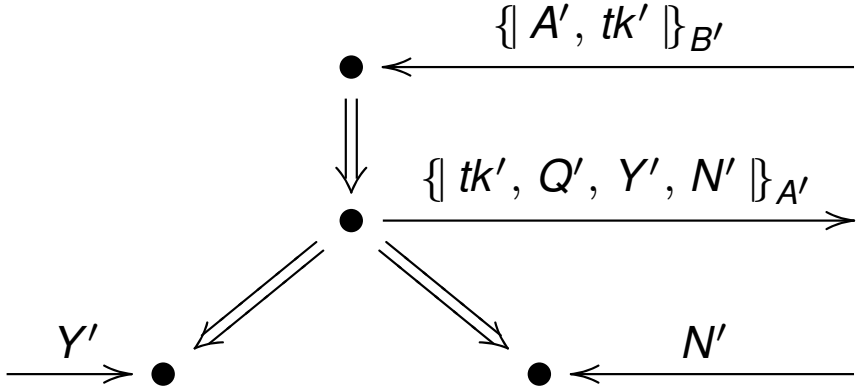
Skeleton $\mathbb{A}$ is realized if possible execution

Q & A uses the HD idea

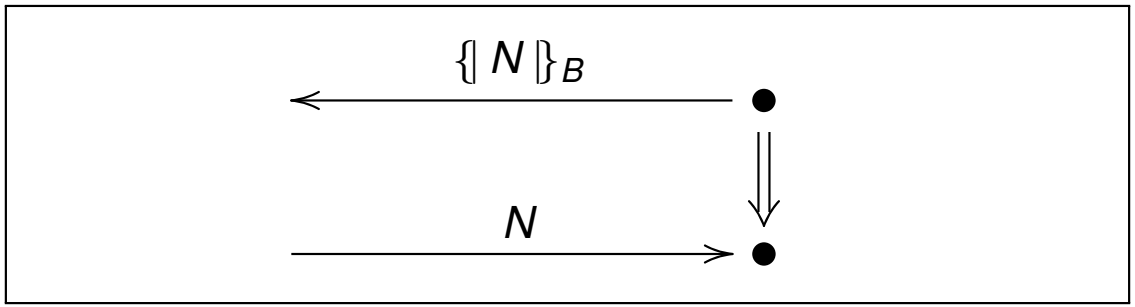




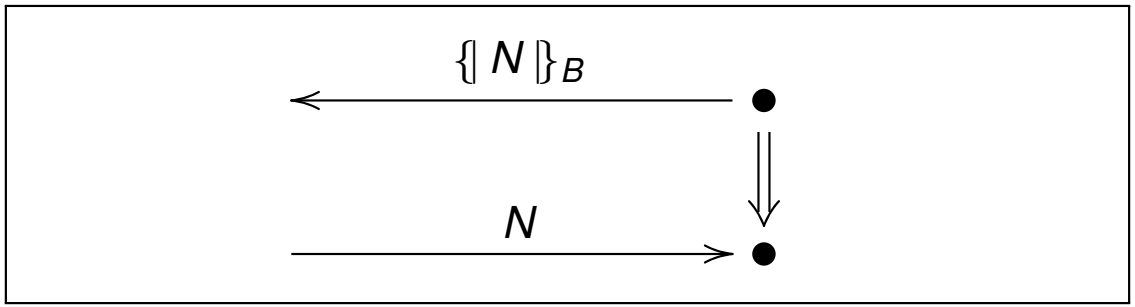




Protocol Analysis for HD

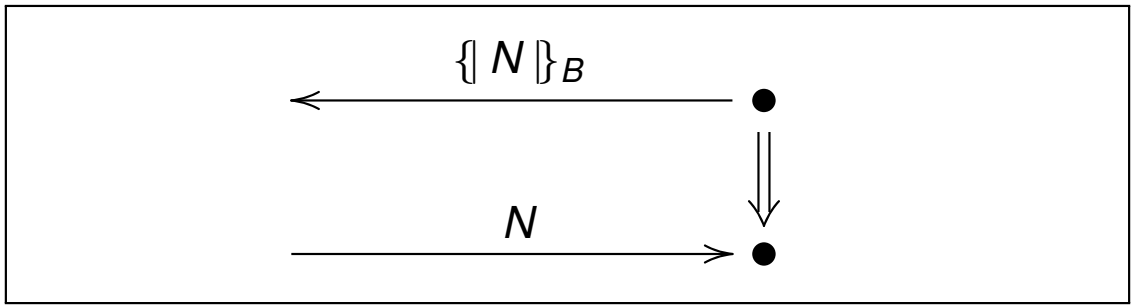


Protocol Analysis for HD



What must be true if the Answerer offers a token and gets a query?

Protocol Analysis for HD

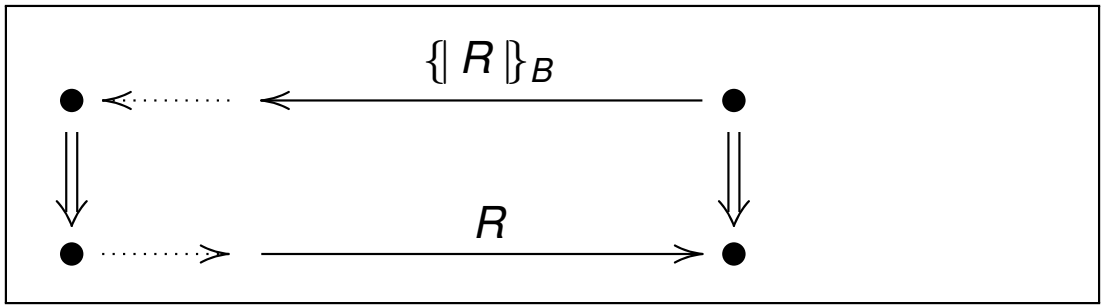


What must be true if the Answerer offers a token and gets a query?

It depends on the assumptions. Assume:

R freshly chosen
privk(B) uncompromised

Protocol Analysis for HD



What must be true if the Answerer offers a token and gets a query?

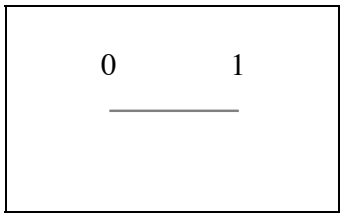
It depends on the assumptions. Assume:

R freshly chosen
privk(B) uncompromised

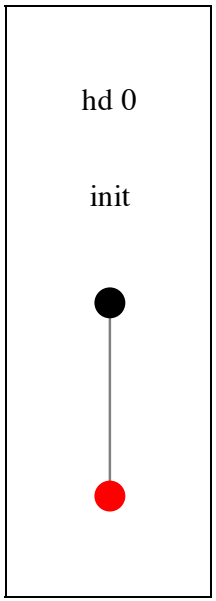
HD example in CPSA

r fresh, privk(*B*) uncompromised

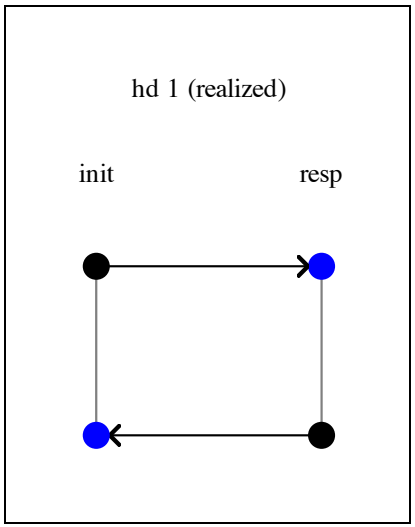
Tree 0.



Item 0, Child: 1.



Item 1, Parent: 0.

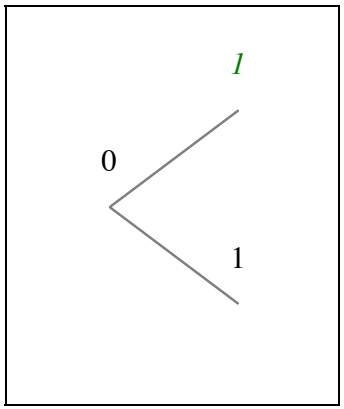



```
(defstrand init 2 r b)
(defstrand resp 2 r b)
```

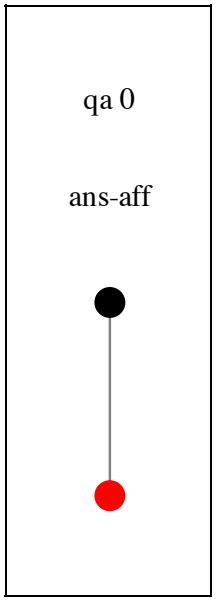
Q & A: Weakened Scenario in CPSA

tk fresh, privk(*B*) uncompromised

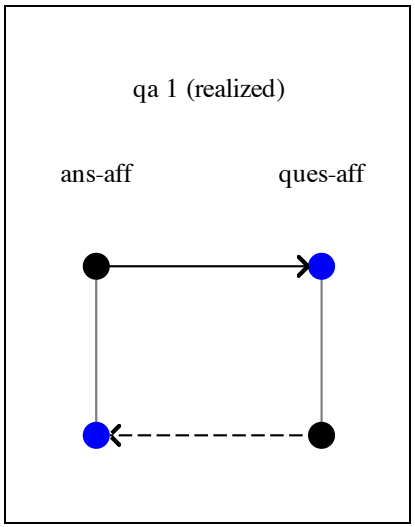
Tree 0.



Item 0, Child: 1, Seen Child: 1.



Item 1, Parent: 0.




```
(defstrand ans-aff 2 q tk y n a b)
(defstrand ques-aff 2 q-0 tk y-0 n-0 a b)
```

Comparing HD and Q & A Analyses

Weakened Q & A Scenario

- Start with corresponding scenarios (skeletons)
- HD analysis can always take step to a skeleton $\mathbb{A}$ when Q & A analysis can take step to corresponding $\mathbb{B}$

- If HD analysis takes step from a skeleton $\mathbb{A}$ then Q & A analysis takes step from corresponding $\mathbb{B}$

Comparing HD and Q & A Analyses

Weakened Q & A Scenario

- Start with corresponding scenarios (skeletons)
- HD analysis can always take step to a skeleton $\mathbb{A}$ when Q & A analysis can take step to corresponding $\mathbb{B}$

$$\rightsquigarrow_1 \textit{ simulates } \rightsquigarrow_2$$

- If HD analysis takes step from a skeleton $\mathbb{A}$ then Q & A analysis takes step from corresponding $\mathbb{B}$

$$\rightsquigarrow_2 \textit{ live when } \rightsquigarrow_1 \text{ is}$$

Comparing HD and Q & A Analyses

Weakened Q & A Scenario

- Start with corresponding scenarios (skeletons)
- HD analysis can always take step to a skeleton $\mathbb{A}$
  when Q & A analysis can take step to corresponding $\mathbb{B}$

  $\rightsquigarrow_1$ *simulates* $\rightsquigarrow_2$
- If HD analysis takes step from a skeleton $\mathbb{A}$
  then Q & A analysis takes step from corresponding $\mathbb{B}$

  $\rightsquigarrow_2$ *live* when $\rightsquigarrow_1$ is

These two properties imply:
Π_2 *preserves all security goals achieved by* Π_1
for this starting point

Security goals

An authentication goal

$$\begin{array}{ccc} \texttt{Init}(s) \wedge & \texttt{AtPos2}(s,m) \wedge & \texttt{Peer}(s,b) \wedge \\ \texttt{Nonce}(s,v) \wedge & \texttt{Uncompr}(\texttt{inv}(\texttt{pk}(b))) \wedge & \texttt{FreshAt}(n,v) \end{array}$$

implies

$$\begin{array}{cccc} \exists s' . & \texttt{Resp}(s') \wedge & \texttt{AtPos2}(s',m') & \texttt{Self}(s',b) \\ & \texttt{Nonce}(s',v) & \texttt{Prec}(n,m') & \texttt{Prec}(m',m) \end{array}$$

Security goals

A (bogus) confidentiality goal

$$\texttt{Init}(s) \wedge \texttt{Nonce}(s, v) \wedge \texttt{AtPos2}(s, m) \wedge \texttt{Uncompr}(\texttt{inv}(\texttt{pk}(b))) \wedge \texttt{Heard}(s', v) \wedge \texttt{Peer}(s, b) \wedge \texttt{FreshAt}(n, v) \wedge$$

implies

$$\texttt{falsehood}$$

Form of a security goal

$$\forall \overline{x} \,.\, (\phi \quad \supset \quad \exists \overline{y} \,.\, \psi_1 \vee \ldots \vee \psi_j)$$

where ϕ and each ψ_i is a conjunction of atomic formulas

Form of a security goal

$$\forall \overline{x} \,.\, (\phi \quad \supset \quad \exists \overline{y} \,.\, \psi_1 \vee \ldots \vee \psi_j)$$

where ϕ and each ψ_i is a conjunction of atomic formulas

Key point:
ϕ and the ψ_i are
preserved under homomorphisms

Skeletons form models for a language $\mathcal{L}(\Pi)$

Some vocabulary shared among all Π

$\texttt{Prec}(m, n)$ $\texttt{Fresh}(v)$ $\texttt{FreshAt}(n, v)$ $\texttt{Uncompr}(v)$

Some vocabulary is Π-specific

	$\texttt{AtPos1}(s, n)$	$\texttt{AtPos2}(s, n)$	
$\texttt{Init}(s)$	$\texttt{Resp}(s)$	$\texttt{Lsn}(s)$	
$\texttt{Peer}(s, b)$	$\texttt{Self}(s, b)$	$\texttt{Nonce}(s, v)$	$\texttt{Heard}(s, v)$

Skeletons form models for a language $\mathcal{L}(\Pi)$

Some vocabulary shared among all Π

$$\texttt{Prec}(m,n) \qquad \texttt{Fresh}(v) \qquad \texttt{FreshAt}(n,v) \qquad \texttt{Uncompr}(v)$$

Some vocabulary is Π-specific

$$\begin{array}{cccc} & \texttt{AtPos1}(s,n) & \texttt{AtPos2}(s,n) & \\ \texttt{Init}(s) & \texttt{Resp}(s) & \texttt{Lsn}(s) & \\ \texttt{Peer}(s,b) & \texttt{Self}(s,b) & \texttt{Nonce}(s,v) & \texttt{Heard}(s,v) \end{array}$$

"Homomorphism" defined in normal way for $\mathcal{L}(\Pi)$-structures $\mathbb{A}$

Characteristic formula, characteristic skeleton

ϕ is a *characteristic formula for* $\mathbb{A}$ *under* η_*:

$$\mathbb{B} \models_\eta \phi \quad \text{iff} \quad \exists H \,.\, H\colon \mathbb{A} \to \mathbb{B} \text{ and } \eta = H \circ \eta_*$$

Characteristic formula, characteristic skeleton

ϕ is a *characteristic formula for* $\mathbb{A}$ *under* η_*:

$$\mathbb{B} \models_\eta \phi \quad \text{iff} \quad \exists H \,.\, H\colon \mathbb{A} \to \mathbb{B} \text{ and } \eta = H \circ \eta_*$$

$\mathbb{A}$ is a *characteristic skeleton for* ϕ *under* η_*:

$$\mathbb{A} \models_{\eta_*} \phi$$

and

$$\mathbb{B} \models_\eta \phi \text{ implies } \exists! H \,.\, H\colon \mathbb{A} \to \mathbb{B} \text{ and } \eta = H \circ \eta_*$$

Form of a security goal

$$\forall \overline{x} \,.\, (\phi \quad \supset \quad \exists \overline{y} \,.\, \psi_1 \vee \ldots \vee \psi_j)$$

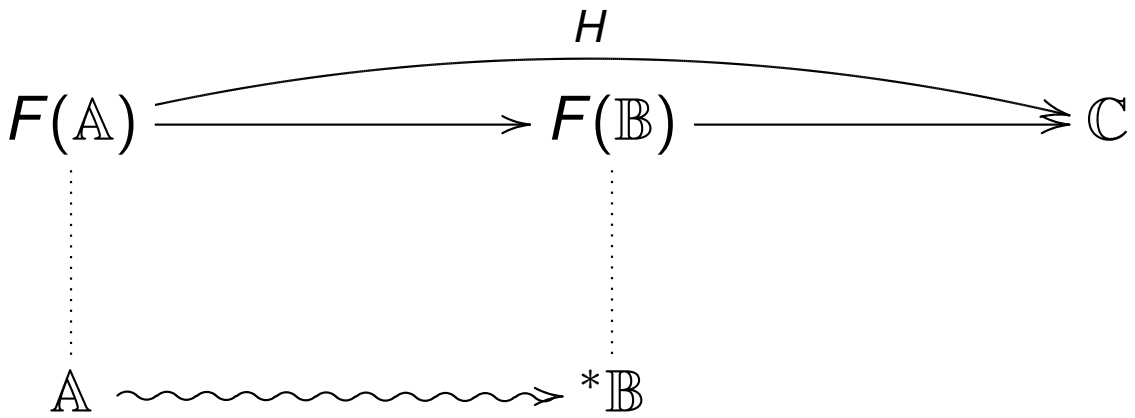
where ϕ and each ψ_i is a conjunction of atomic formulas

Key point:
ϕ and the ψ_i are
preserved under homomorphisms

The *starting point* of a security goal
is the characteristic skeleton of ϕ

What we want

For F to preserve goals



Definition: Analysis LTS (ALTS)

$S \subseteq Skel(\Pi)$

Λ contains dead (no realized images)

Definition: Analysis LTS (ALTS)

$S \subseteq \mathit{Skel}(\Pi)$
Λ contains dead (no realized images)

$\cdot \dot{\rightsquigarrow} \cdot \subseteq S \times \Lambda \times S$ is a ALTS iff

(A) If $\mathbb{A} \in S$, then $\exists \mathbb{B} \,.\, \mathbb{A} \rightsquigarrow \mathbb{B}$ iff $\mathbb{A}$ is not realized;

(B) If $\mathbb{A} \overset{\ell}{\rightsquigarrow} \mathbb{B}$, then:

1. If $\ell =$ dead, then $\rightsquigarrow$ stutters, and $\mathbb{A}$ has no realized images;

Definition: Analysis LTS (ALTS)

$S \subseteq \mathit{Skel}(\Pi)$
Λ contains dead (no realized images)

$\cdot \dot{\rightsquigarrow} \cdot \subseteq S \times \Lambda \times S$ is a ALTS iff

(A) If $\mathbb{A} \in S$, then $\exists \mathbb{B} \,.\, \mathbb{A} \rightsquigarrow \mathbb{B}$ iff $\mathbb{A}$ is not realized;

(B) If $\mathbb{A} \overset{\ell}{\rightsquigarrow} \mathbb{B}$, then:

1. If $\ell = \text{dead}$, then $\rightsquigarrow$ stutters, and $\mathbb{A}$ has no realized images;
2. If $\ell \neq \text{dead}$, then $\mathbb{A} \to \mathbb{B} \not\to \mathbb{A}$;

Definition: Analysis LTS (ALTS)

$S \subseteq \mathit{Skel}(\Pi)$
Λ contains dead (no realized images)

$\cdot \dot{\rightsquigarrow} \cdot \subseteq S \times \Lambda \times S$ is a ALTS iff

(A) If $\mathbb{A} \in S$, then $\exists \mathbb{B} \,.\, \mathbb{A} \rightsquigarrow \mathbb{B}$ iff $\mathbb{A}$ is not realized;

(B) If $\mathbb{A} \overset{\ell}{\rightsquigarrow} \mathbb{B}$, then:

1. If $\ell =$ dead, then $\rightsquigarrow$ stutters, and $\mathbb{A}$ has no realized images;
2. If $\ell \neq$ dead, then $\mathbb{A} \to \mathbb{B} \not\to \mathbb{A}$;
3. If $J \colon \mathbb{A} \to \mathbb{C}$, with realized $\mathbb{C}$, then

   $\exists\, \mathbb{B}'$ s.t. $\mathbb{A} \overset{\ell}{\rightsquigarrow} \mathbb{B}'$ and

   $J = K \circ H$, where $\mathbb{A} \overset{H}{\to} \mathbb{B}' \overset{K}{\to} \mathbb{C}$

Definition: Analysis LTS (ALTS)

$S \subseteq \mathit{Skel}(\Pi)$
Λ contains dead (no realized images)

$\cdot \dot{\rightsquigarrow} \cdot \subseteq S \times \Lambda \times S$ is a ALTS iff

(A) If $\mathbb{A} \in S$, then $\exists \mathbb{B} \,.\, \mathbb{A} \rightsquigarrow \mathbb{B}$ iff $\mathbb{A}$ is not realized;

(B) If $\mathbb{A} \overset{\ell}{\rightsquigarrow} \mathbb{B}$, then:

1. If $\ell = \text{dead}$, then $\rightsquigarrow$ stutters, and $\mathbb{A}$ has no realized images;
2. If $\ell \neq \text{dead}$, then $\mathbb{A} \to \mathbb{B} \not\to \mathbb{A}$;
3. If $J \colon \mathbb{A} \to \mathbb{C}$, with realized $\mathbb{C}$, then

   $\exists\, \mathbb{B}'$ s.t. $\mathbb{A} \overset{\ell}{\rightsquigarrow} \mathbb{B}'$ and

   $J = K \circ H$, where $\mathbb{A} \overset{H}{\to} \mathbb{B}' \overset{K}{\to} \mathbb{C}$

$\{\mathbb{B} \colon \mathbb{A} \overset{\ell}{\rightsquigarrow} \mathbb{B}\}$ called the ℓ-cohort for $\mathbb{A}$

Transformations and ALTS

Assume $F : \Pi_1 \to \Pi_2$ a transformation
$G : \Lambda_1 \to \Lambda_2$ a label map with $G^{-1}(\{\text{dead}\}) = \{\text{dead}\}$
$\rightsquigarrow_1$, $\rightsquigarrow_2$ ALTS for Π_1, Π_2 resp.

F, G preserve progress iff $\mathbb{A} \overset{\ell}{\rightsquigarrow}_1$ implies $F(\mathbb{A}) \overset{G(\ell)}{\rightsquigarrow}_2$

$\rightsquigarrow_1$ simulates $\rightsquigarrow_2$ for F, G iff $F(\mathbb{A}) \overset{G(\ell)}{\rightsquigarrow}_2 \mathbb{B}'$ implies

for some $\mathbb{B}$, $F(\mathbb{B}) = \mathbb{B}'$ and $\mathbb{A} \overset{\ell}{\rightsquigarrow}_1 \mathbb{B}$

Theorem: $\rightsquigarrow_1^*$ witnesses for Π_2 executions

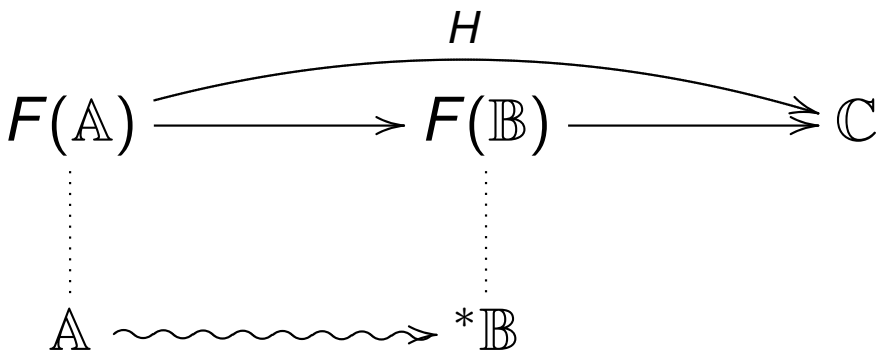
Assume $F : \Pi_1 \to \Pi_2$ a transformation
$G : \Lambda_1 \to \Lambda_2$ a label map with $G^{-1}(\{\text{dead}\}) = \{\text{dead}\}$
$\rightsquigarrow_1$, $\rightsquigarrow_2$ ALTS for Π_1, Π_2 resp.

with

progress and simulation

For every Π_2-realized $\mathbb{C}$, if $H : F(\mathbb{A}) \to \mathbb{C}$

There is a Π_1-realized $\mathbb{B}$ such that $\mathbb{A} \rightsquigarrow_1^* \mathbb{B}$ and:

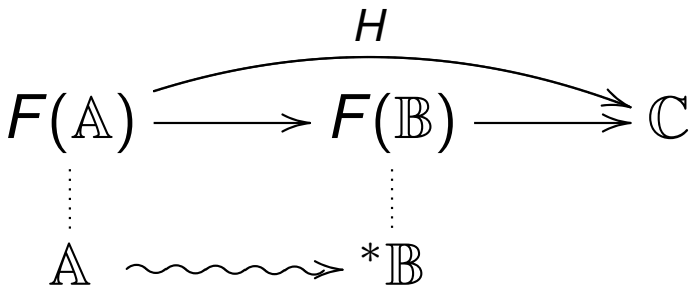


Preserving security goals

If Π_1 achieves goal Ψ

$$\forall \vec{x} \,.\, (\phi_0 \supset \exists \vec{y} \,.\, \phi_1 \vee \ldots \vee \phi_k)$$

and $F : \Pi_1 \to \Pi_2$ satisfies



then Π_2 achieves $Tr_F(\Psi)$