Cryptographic Protocol Composition via the Authentication Tests

Joshua Guttman

The MITRE Corporation
Thanks to the MITRE-Sponsored Research program
and the National Security Agency.

Protocol Exchange
2 Oct 2008

Protocol Composition Problem

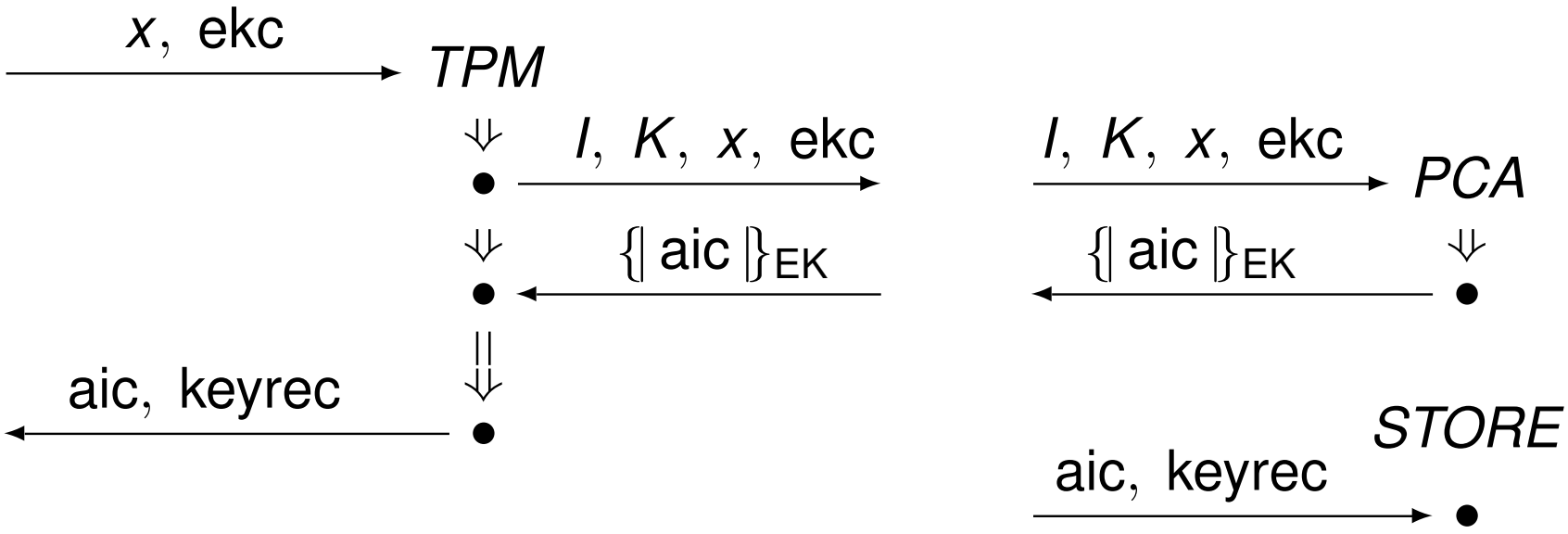
- Protocols analyzed in isolation,
  but used in combinations
  - If Π_1 meets goal G in isolation,
    does it still in combination with Π_2?
  - Motivations:
    - ★ Ease verification burden
    - ★ Provide guidance for compositional protocol design
  - Main result: More inclusive sufficient criterion

Protocol Composition Problem

- Protocols analyzed in isolation,
  but used in combinations
  - If Π_1 meets goal G in isolation,
    does it still in combination with Π_2?
  - Motivations:
    - ★ Ease verification burden
    - ★ Provide guidance for compositional protocol design
  - Main result: More inclusive sufficient criterion
- Method: Model-theoretic approach
  - Syntactic class of formulas
  - Preserved under certain homomorphisms of models

Modified Anonymous Identity Protocol

A Certificate Distribution Protocol



$$\text{ekc} = [\![\, \text{ekctag MFG}, \text{EK} \,]\!]_{\text{MFG}}$$

$$\text{aic} = [\![\, \text{aictag } I, K, x \,]\!]_{\text{PCA}}$$

$$\text{keyrec} = \{|\, \text{aikrectag } K, K^{-1} \,|\}_{\text{srk}}$$

Protocol Goals of MAIP

Whenever

- STORE gets msg for I, K, x, PCA
- privk(MFG), privk(PCA) non-originating
- K, K^{-1} uniquely originating

Then, for some EK,

- A run of the PCA with I, K, x, PCA, EK has reached step 2
- A run of TPM with I, K, x, PCA, EK has reached step 3
- K^{-1} will never be recvd, unprotected

Logical representation

$\forall m, n_0, I, K, x, \mathrm{PCA}, \mathrm{MFG},$

$\quad \mathrm{Store1}(m, I, K, x, \mathrm{PCA})$

$\quad \wedge\ \mathrm{Non}(\mathrm{privk}(\mathrm{MFG})) \wedge \mathrm{Non}(\mathrm{privk}(\mathrm{PCA}))$

$\quad \wedge\ \mathrm{Unq}(K) \wedge \mathrm{Unq}(\mathrm{inv}(K))$

implies

$\exists n_1, n_2, \mathrm{EK},$

$\quad \mathrm{Pca2}(n_1, I, K, x, \mathrm{PCA}, \mathrm{EK})$

$\quad \wedge\ \mathrm{Tpm3}(n_2, I, K, x, \mathrm{PCA}, \mathrm{EK})$

$\quad \wedge\ \neg\mathrm{Lsn1}(n_0, \mathrm{inv}(K))$

Logical Language $\mathcal{L}(\Pi)$

For a protocol Π

Variables	over nodes and order-sorted atoms and msgs
Fn symbols	for fns on atoms: $\mathsf{inv}(\cdot), \mathsf{privk}(\cdot)$, etc.
Predicates	$u = v \quad \mathsf{false}()$
	$\mathsf{Non}(v) \quad \mathsf{Unq}(v) \quad \mathsf{UnqAt}(n, v)$
	$\mathsf{DblArrw}(m, n) \quad \mathsf{Prec}(m, n)$
	Role predicates for each node of a role of Π

What's not in $\mathcal{L}(\Pi)$

Fn symbols $\mathsf{cat}(x, y)$ $\mathsf{enc}(x, y)$

Predicate $\mathsf{MsgAt}(n, x)$

Security Goals

sec. hyp. atomic formula Φ of $\mathcal{L}(\Pi)$

sec. conc. conjunction Ψ of atomic formulas of $\mathcal{L}(\Pi)$

sec. goal $\forall \vec{x} \,.\, (\Phi_1 \wedge \ldots \wedge \Phi_j \quad \supset \quad \exists \vec{y} \,.\, \Psi_1 \vee \ldots \vee \Psi_k)$

Security Goals

sec. hyp. atomic formula Φ of $\mathcal{L}(\Pi)$

sec. conc. conjunction Ψ of atomic formulas of $\mathcal{L}(\Pi)$

sec. goal $\forall \vec{x} \,.\, (\Phi_1 \wedge \ldots \wedge \Phi_j \quad \supset \quad \exists \vec{y} \,.\, \Psi_1 \vee \ldots \vee \Psi_k)$

where

node vars n among $\vec{x}$

appear in role predicates in Φ^s

Security Goal 1

$\forall m, l, K, x, \mathrm{PCA}, \mathrm{MFG},$

$\quad \mathrm{Store1}(m, l, K, x, \mathrm{PCA})$

$\quad \wedge\ \mathrm{Non}(\mathrm{privk}(\mathrm{MFG})) \wedge \mathrm{Non}(\mathrm{privk}(\mathrm{PCA}))$

$\quad \wedge\ \mathrm{Unq}(K) \wedge \mathrm{Unq}(\mathrm{inv}(K))$

implies $\exists n_1, \mathrm{EK}$.

$\quad \mathrm{Pca2}(n_1, l, K, x, \mathrm{PCA}, \mathrm{EK})$

Security Goal 2

$\forall m, l, K, x, \mathrm{PCA}, \mathrm{MFG},$

$\quad \mathrm{Store1}(m, l, K, x, \mathrm{PCA})$

$\quad \wedge\ \mathrm{Non}(\mathrm{privk}(\mathrm{MFG})) \wedge \mathrm{Non}(\mathrm{privk}(\mathrm{PCA}))$

$\quad \wedge\ \mathrm{Unq}(K) \wedge \mathrm{Unq}(\mathrm{inv}(K))$

implies $\exists n_2, \mathrm{EK}$.

$\quad \mathrm{Tpm3}(n_2, l, K, x, \mathrm{PCA}, \mathrm{EK})$

Security Goal 3

$\forall m, n_0, I, K, x, \mathrm{PCA}, \mathrm{MFG},$

$\quad \mathrm{Store1}(m, I, K, x, \mathrm{PCA})$

$\quad \wedge\ \mathrm{Non}(\mathrm{privk}(\mathrm{MFG})) \wedge \mathrm{Non}(\mathrm{privk}(\mathrm{PCA}))$

$\quad \wedge\ \mathrm{Unq}(K) \wedge \mathrm{Unq}(\mathrm{inv}(K))$

$\quad \wedge\ \mathrm{Lsn1}(n_0, \mathrm{inv}(K))$

implies

$\quad \mathrm{false}()$

Protocol independence

Suppose $\Pi_1 \subseteq \Pi$

Π_1 is independent of the rest of Π if

> *For every security goal $G_1 \in \mathcal{L}(\Pi_1)$,*
> *if G_1 is satisfied in every execution of Π_1,*
> *then G_1 is satisfied in every execution of Π*

Protocol independence

Suppose $\Pi_1 \subseteq \Pi$

Π_1 is independent of the rest of Π if

> *For every security goal $G_1 \in \mathcal{L}(\Pi_1)$,*
> *if G_1 is satisfied in every execution of Π_1,*
> *then G_1 is satisfied in every execution of Π*

Execution means realized skeleton

Skeleton $\mathbb{A}$

1. $\text{nodes}(\mathbb{A})$, finite set of regular nodes
   If $n \Rightarrow^* n'$ and $n' \in \text{nodes}(\mathbb{A})$,
   then $n \in \text{nodes}(\mathbb{A})$ and $n \preceq_{\mathbb{A}} n'$
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)

Partial description of regular behavior in some set of executions

Realized skeletons

Skeleton $\mathbb{A}$ is realized if
for each reception node n,
adversary can derive
msg(n) using

- $\{\text{msg}(m) : m \text{ is a transmission node and } m \preceq_{\mathbb{A}} n\}$
- Atoms other than
  - $\text{non}_{\mathbb{A}}$
  - $\text{unique}_{\mathbb{A}}$ values that originate in $\mathbb{A}$

and normal Dolev-Yao rules

Satisfaction

σ : Var $\rightarrow$ nodes($\mathbb{A}$) $\cup$ msgs

$\mathbb{A}, \sigma \models \Phi$

- $\mathbb{A}, \sigma \models \mathsf{Non}(v)$ iff $\sigma(v) \in \mathsf{non}_{\mathbb{A}}$
- $\mathbb{A}, \sigma \models \mathsf{Unq}(v)$ iff $\sigma(v) \in \mathsf{unique}_{\mathbb{A}}$
- $\mathbb{A}, \sigma \models \mathsf{UnqAt}(m, v)$ iff $\sigma(m) \in \mathsf{nodes}(\mathbb{A})$, and $\sigma(v) \in \mathsf{unique}_{\mathbb{A}}$, and $\sigma(v)$ originates at node $\sigma(m)$
- $\mathbb{A}, \sigma \models \mathsf{RoleRhoJ}(m, v_1, \ldots, v_k)$ iff $\sigma(m) \in \mathsf{nodes}(\mathbb{A})$ and $\sigma(m)$ an instance of the j^{th} node of role ρ with parameters

$$\sigma(v_1), \ldots, \sigma(v_k)$$

etc.

Satisfaction

σ : Var $\to$ nodes($\mathbb{A}$) $\cup$ msgs

$\mathbb{A}, \sigma \models \Phi$

- $\mathbb{A}, \sigma \models \mathsf{Non}(v)$ iff $\sigma(v) \in \mathsf{non}_{\mathbb{A}}$
- $\mathbb{A}, \sigma \models \mathsf{Unq}(v)$ iff $\sigma(v) \in \mathsf{unique}_{\mathbb{A}}$
- $\mathbb{A}, \sigma \models \mathsf{UnqAt}(m, v)$ iff $\sigma(m) \in \mathsf{nodes}(\mathbb{A})$, and $\sigma(v) \in \mathsf{unique}_{\mathbb{A}}$, and $\sigma(v)$ originates at node $\sigma(m)$
- $\mathbb{A}, \sigma \models \mathsf{RoleRhoJ}(m, v_1, \ldots, v_k)$ iff $\sigma(m) \in \mathsf{nodes}(\mathbb{A})$ and $\sigma(m)$ an instance of the j^{th} node of role ρ with parameters

$$\sigma(v_1), \ldots, \sigma(v_k)$$

etc.

Satisfaction

σ : Var $\rightarrow$ nodes($\mathbb{A}$) $\cup$ msgs

$\mathbb{A}, \sigma \models \Phi$

- $\mathbb{A}, \sigma \models \mathsf{Non}(v)$ iff $\sigma(v) \in \mathsf{non}_{\mathbb{A}}$
- $\mathbb{A}, \sigma \models \mathsf{Unq}(v)$ iff $\sigma(v) \in \mathsf{unique}_{\mathbb{A}}$
- $\mathbb{A}, \sigma \models \mathsf{UnqAt}(m, v)$ iff $\sigma(m) \in \mathsf{nodes}(\mathbb{A})$, and $\sigma(v) \in \mathsf{unique}_{\mathbb{A}}$, and $\sigma(v)$ originates at node $\sigma(m)$
- $\mathbb{A}, \sigma \models \mathsf{RoleRhoJ}(m, v_1, \ldots, v_k)$ iff $\sigma(m) \in \mathsf{nodes}(\mathbb{A})$ and $\sigma(m)$ an instance of the j^{th} node of role ρ with parameters

$$\sigma(v_1), \ldots, \sigma(v_k)$$

etc.

Satisfaction

σ : Var $\rightarrow$ nodes($\mathbb{A}$) $\cup$ msgs

$\mathbb{A}, \sigma \models \Phi$

- $\mathbb{A}, \sigma \models \mathsf{Non}(v)$ iff $\sigma(v) \in \mathsf{non}_{\mathbb{A}}$
- $\mathbb{A}, \sigma \models \mathsf{Unq}(v)$ iff $\sigma(v) \in \mathsf{unique}_{\mathbb{A}}$
- $\mathbb{A}, \sigma \models \mathsf{UnqAt}(m, v)$ iff $\sigma(m) \in \mathsf{nodes}(\mathbb{A})$, and $\sigma(v) \in \mathsf{unique}_{\mathbb{A}}$, and $\sigma(v)$ originates at node $\sigma(m)$
- $\mathbb{A}, \sigma \models \mathsf{RoleRhoJ}(m, v_1, \ldots, v_k)$ iff $\sigma(m) \in \mathsf{nodes}(\mathbb{A})$ and $\sigma(m)$ an instance of the j^{th} node of role ρ with parameters

$$\sigma(v_1), \ldots, \sigma(v_k)$$

etc.

Satisfaction

σ : Var $\rightarrow$ nodes($\mathbb{A}$) $\cup$ msgs

$\mathbb{A}, \sigma \models \Phi$

- $\mathbb{A}, \sigma \models \mathrm{Non}(v)$ iff $\sigma(v) \in \mathrm{non}_{\mathbb{A}}$
- $\mathbb{A}, \sigma \models \mathrm{Unq}(v)$ iff $\sigma(v) \in \mathrm{unique}_{\mathbb{A}}$
- $\mathbb{A}, \sigma \models \mathrm{UnqAt}(m, v)$ iff $\sigma(m) \in \mathrm{nodes}(\mathbb{A})$, and $\sigma(v) \in \mathrm{unique}_{\mathbb{A}}$, and $\sigma(v)$ originates at node $\sigma(m)$
- $\mathbb{A}, \sigma \models \mathrm{RoleRhoJ}(m, v_1, \ldots, v_k)$ iff $\sigma(m) \in \mathrm{nodes}(\mathbb{A})$ and $\sigma(m)$ an instance of the j^{th} node of role ρ with parameters

$$\sigma(v_1), \ldots, \sigma(v_k)$$

etc.

Counterexamples to goals

$\mathbb{A}$ is a counterexample to a goal G iff

- $\mathbb{A}$ is realized
- $\mathbb{A} \models \neg G$

Strong disjointness

Π, Π_1 has *strongly disjoint encryption* (s.d.e.) iff

it has neither encryption creation conflicts nor extraction conflicts

Encryption creation conflict

One condition to avoid

"Encryption creation conflict" means:

- n_1 lies on $\rho_1 \in \Pi_1$
- $e_1 \sqsubseteq \mathrm{msg}(n_1)$
- any $\alpha(e_1)$ originates at a non-primary node n_2

$$E(\Pi_1) = \{\alpha(e_1) : e_1 \sqsubseteq \mathrm{msg}(n_1) \wedge n_1 \text{ lies on some } \rho_1 \in \Pi_1\}$$

Encryption creation conflict

One condition to avoid

"Encryption creation conflict" means:

- n_1 lies on $\rho_1 \in \Pi_1$
- $e_1 \sqsubseteq \mathsf{msg}(n_1)$
- any $\alpha(e_1)$ originates at a non-primary node n_2

$E(\Pi_1) =$

$$\{\alpha(e_1) : e_1 \sqsubseteq \mathsf{msg}(n_1) \wedge n_1 \text{ lies on some } \rho_1 \in \Pi_1\}$$

Extraction conflict

Another condition to avoid

"Extraction conflict" means:

- $t_1 \sqsubseteq e_1 \sqsubseteq \mathrm{msg}(n_2)$ for $e_1 \in E(\Pi_1)$, n_2 non-primary recv
- $n_2 \Rightarrow^+ n_2'$ where n_2 non-primary transmission
- for some $S \subseteq E(\Pi)$:
  - $m \Rightarrow^+ n_2'$ implies $t_1 \odot^S \mathrm{msg}(m)$
  - $t_1 \dagger^S \mathrm{msg}(n_2')$

$t_1 \dagger^S t$: a path in t reaches t_1 and traverses neither

1. a key edge, nor
2. a member of S

$t_1 \odot^S t$ is negation of $t_1 \dagger^S t$

Extraction conflict

Another condition to avoid

"Extraction conflict" means:

- $t_1 \sqsubseteq e_1 \sqsubseteq \mathrm{msg}(n_2)$ for $e_1 \in E(\Pi_1)$, n_2 non-primary recv
- $n_2 \Rightarrow^+ n_2'$ where n_2 non-primary transmission
- for some $S \subseteq E(\Pi)$:
  - $m \Rightarrow^+ n_2'$ implies $t_1 \odot^S \mathrm{msg}(m)$
  - $t_1 \dagger^S \mathrm{msg}(n_2')$

$t_1 \dagger^S t$: a path in t reaches t_1 and traverses neither

1. a key edge, nor
2. a member of S

$t_1 \odot^S t$ is negation of $t_1 \dagger^S t$

Extraction conflict

Another condition to avoid

"Extraction conflict" means:

- $t_1 \sqsubseteq e_1 \sqsubseteq \mathrm{msg}(n_2)$ for $e_1 \in E(\Pi_1)$, n_2 non-primary recv
- $n_2 \Rightarrow^+ n_2'$ where n_2 non-primary transmission
- for some $S \subseteq E(\Pi)$:
  - $m \Rightarrow^+ n_2'$ implies $t_1 \odot^S \mathrm{msg}(m)$
  - $t_1 \dagger^S \mathrm{msg}(n_2')$

$t_1 \dagger^S t$: a path in t reaches t_1 and traverses neither

1. a key edge, nor
2. a member of S

$t_1 \odot^S t$ is negation of $t_1 \dagger^S t$

Occurs only within

t_1 occurs only within S in t

Let S be a set of encryptions; $t_1 \odot^S t$ iff
every path through a.s.t. of t that reaches t_1 traverses either

- a key edge linking $\{\!|\, x \,|\!\}_y$ to y, or
- some $e \in S$ prior to t_1

Cuts

Cut: a partition L, U of nodes($\mathbb{A}$) s.t.

- U is non-empty
- $m \in L$ and $n \in U$ implies $n \not\preceq_{\mathbb{A}} m$

Cut($c, S, \mathbb{A}$): the cut L, U (if any exists) where $U =$

$$\{n \in \text{nodes}(\mathbb{A}) : \exists m \,.\, m \preceq_{\mathbb{A}} n \wedge c \dagger^{S} \text{msg}(m)\}$$

where c is either

- an atom $c \in \text{unique}_{\mathbb{A}}$ originating in $\mathbb{A}$
- an encryption

Cuts

Cut: a partition L, U of nodes($\mathbb{A}$) s.t.

- U is non-empty
- $m \in L$ and $n \in U$ implies $n \not\preceq_{\mathbb{A}} m$

Cut($c, S, \mathbb{A}$): the cut L, U (if any exists) where $U =$

$$\{n \in \text{nodes}(\mathbb{A}) : \exists m \,.\, m \preceq_{\mathbb{A}} n \wedge c \dagger^{S} \text{msg}(m)\}$$

where c is either

- an atom $c \in \text{unique}_{\mathbb{A}}$ originating in $\mathbb{A}$
- an encryption

Solved cut

$L, U = \mathrm{Cut}(c, S, \mathbb{A})$ is solved iff
for every $\preceq_{\mathbb{A}}$-minimal $n_1 \in U$, either:

- n_1 is a transmission node, or
- for some $m = \mathrm{Lsn}[t]$ with $m \prec_{\mathbb{A}} n_1$, either
  - $c = \{\!|\, t_0 \,|\!\}_t$ or else
  - $t = t_1^{-1}$ where $\{\!|\, t_0 \,|\!\}_{t_1} \in S$

Authentication tests
Theorem

- If $\mathbb{A}$ is realized, there exists $\mathbb{A}'$ s.t.
  - $\mathbb{A}'$ adds only listener nodes to $\mathbb{A}$
  - every well-defined Cut$(c, S, \mathbb{A}')$ is solved
- If every well-defined Cut$(c, S, \mathbb{A})$ is solved, then $\mathbb{A}$ is realized

S.D.E. vs. Independence

Π, Π_1 s.d.e.

For goal $G_1 \in \mathcal{L}(\Pi_1)$ and Π-skeleton $\mathbb{A}$ with

$$\mathbb{A} \models \neg G_1$$

Can we squeeze out a Π_1-skeleton $\mathbb{A}_1$ from $\mathbb{A}$ s.t.

$$\mathbb{A}_1 \models \neg G_1 \quad ?$$

Steps for independence

Π, Π_1 s.d.e., Primary goal G_1

- Step 1: Restrict $\mathbb{A}$ to Π_1
  - Discard non-primary nodes
  - $\mathbb{A} \models \neg G_1$ implies $(\mathbb{A} \restriction \Pi_1) \models \neg G_1$
  - But $(\mathbb{A} \restriction \Pi_1)$ possibly not realized
- May need to "generalize" $(\mathbb{A} \restriction \Pi_1)$
  - Un-replace non-primary encryptions with indeterminates
  - A "removal" is the operation of doing so

Removals

- Homomorphism $\alpha = [x_i \mapsto e_i]_{i \in I}$ for
  - Family $\{x_i\}_{i \in I}$ of distinct indeterminates
  - Family $\{e_i\}_{i \in I}$ of distinct non-primary encryptions
- Result of a removal $\alpha = [x_i \mapsto e_i]_{i \in I}$ on t_1 (used backward):
  - Find topmost occurrences of e_i^s
  - Plug in resp. x_i^s

  Always choose $\{x_i\}_{i \in I}$ not appearing in t_1
- Result of a removal on a primary node is primary

Result of a removal on a skeleton

Removal $\alpha = [x_i \mapsto e_i]_{i \in I}$

$\mathbb{B} = \alpha(\mathbb{A})$ iff

- ϕ a bijection between nodes($\mathbb{A}$) and nodes($\mathbb{B}$)
- msg($\phi(n)$) $= \alpha$(msg(n)) for all $n \in$ nodes($\mathbb{A}$)
- $\preceq_{\mathbb{B}} = \phi(\preceq_{\mathbb{A}})$, $\quad \text{unique}_{\mathbb{B}} = \phi(\text{unique}_{\mathbb{A}})$, $\quad \text{non}_{\mathbb{B}} = \phi(\text{non}_{\mathbb{A}})$

$\mathbb{A}$ is the result of the removal α on $\alpha(\mathbb{A})$ iff

- $\{x_i\}_{i \in I}$ don't appear in $\alpha(\mathbb{A})$
- $\{e_i\}_{i \in I}$ don't appear in $\mathbb{A}$

Result of a removal on a skeleton

Removal $\alpha = [x_i \mapsto e_i]_{i \in I}$

$\mathbb{B} = \alpha(\mathbb{A})$ iff

- ϕ a bijection between nodes($\mathbb{A}$) and nodes($\mathbb{B}$)
- msg($\phi(n)$) $= \alpha$(msg(n))
  for all $n \in$ nodes($\mathbb{A}$)
- $\preceq_{\mathbb{B}} = \phi(\preceq_{\mathbb{A}})$, $\quad \text{unique}_{\mathbb{B}} = \phi(\text{unique}_{\mathbb{A}})$, $\quad \text{non}_{\mathbb{B}} = \phi(\text{non}_{\mathbb{A}})$

$\mathbb{A}$ is the result of the removal α on $\alpha(\mathbb{A})$ iff

- $\{x_i\}_{i \in I}$ don't appear in $\alpha(\mathbb{A})$
- $\{e_i\}_{i \in I}$ don't appear in $\mathbb{A}$

Homomorphisms and satisfaction

- If ϕ is an atomic formula, then

$$\mathbb{A}, \sigma \models \phi \quad \text{implies} \quad \alpha(\mathbb{A}), \alpha \circ \sigma \models \phi$$

- If $\alpha(\mathbb{A}), \alpha \circ \sigma \models \phi$ implies $\mathbb{A}, \sigma \models \phi$ when ϕ is:
  - $m = n$, $\mathrm{Pos}(n)$, $\mathrm{Neg}(n)$, $m \prec n$, $m \Rightarrow n$ and m, n variables over nodes
  - $x = y$, $\mathrm{Non}(v)$, $\mathrm{Unq}(v)$, $\mathrm{UnqAt}(m, v)$ and α is injective
  - a role predicate and α is a removal
- For goals $G_1 \in \mathcal{L}(\Pi_1)$ and removals α,

$$\alpha(\mathbb{A}) \models \neg G_1 \quad \text{implies} \quad \mathbb{A} \models \neg G_1$$

Homomorphisms and satisfaction

- If ϕ is an atomic formula, then

$$\mathbb{A}, \sigma \models \phi \quad \text{implies} \quad \alpha(\mathbb{A}), \alpha \circ \sigma \models \phi$$

- If $\alpha(\mathbb{A}), \alpha \circ \sigma \models \phi$ implies $\mathbb{A}, \sigma \models \phi$ when ϕ is:
  - $m = n$, $\mathsf{Pos}(n)$, $\mathsf{Neg}(n)$, $m \prec n$, $m \Rightarrow n$ and m, n variables over nodes
  - $x = y$, $\mathsf{Non}(v)$, $\mathsf{Unq}(v)$, $\mathsf{UnqAt}(m, v)$ and α is injective
  - a role predicate and α is a removal
- For goals $G_1 \in \mathcal{L}(\Pi_1)$ and removals α,

$$\alpha(\mathbb{A}) \models \neg G_1 \quad \text{implies} \quad \mathbb{A} \models \neg G_1$$

Homomorphisms and satisfaction

- If ϕ is an atomic formula, then

$$\mathbb{A}, \sigma \models \phi \quad \text{implies} \quad \alpha(\mathbb{A}), \alpha \circ \sigma \models \phi$$

- If $\alpha(\mathbb{A}), \alpha \circ \sigma \models \phi$ implies $\mathbb{A}, \sigma \models \phi$ when ϕ is:
  - $m = n$, $\mathsf{Pos}(n)$, $\mathsf{Neg}(n)$, $m \prec n$, $m \Rightarrow n$ and m, n variables over nodes
  - $x = y$, $\mathsf{Non}(v)$, $\mathsf{Unq}(v)$, $\mathsf{UnqAt}(m, v)$ and α is injective
  - a role predicate and α is a removal
- For goals $G_1 \in \mathcal{L}(\Pi_1)$ and removals α,

$$\alpha(\mathbb{A}) \models \neg G_1 \quad \text{implies} \quad \mathbb{A} \models \neg G_1$$

Counterexamples are realized

α removes all non-primary encryptions

Realized $\quad \mathbb{B} \models \neg G_1 \qquad \alpha(\mathbb{A}) = \mathbb{B} \restriction \Pi_1$

Is $\mathbb{A}$ realized?

Primary tests

$$\alpha(\mathbb{A}) = \mathbb{B} \restriction \Pi_1$$

- Every test in $\mathbb{A}$ maps to a primary test in $\mathbb{B}$
- Every primary test in $\mathbb{B}$ has a primary solution
- Preimage of this solution is a solution in $\mathbb{A}$

Protocol Composition Problem

- Protocols analyzed in isolation,
  but used in combinations
  - If Π_1 meets goal G in isolation,
    does it still in combination with Π_2?
  - Motivations:
    - ★ Ease verification burden
    - ★ Provide guidance for compositional protocol design
  - Main result: More inclusive sufficient criterion
- Method: Model-theoretic approach
  - Syntactic class of formulas
  - Preserved under certain homomorphisms of models