Decidability of Security for “Unambiguous” Protocols

Joshua D. Guttman
F. Javier Thayer

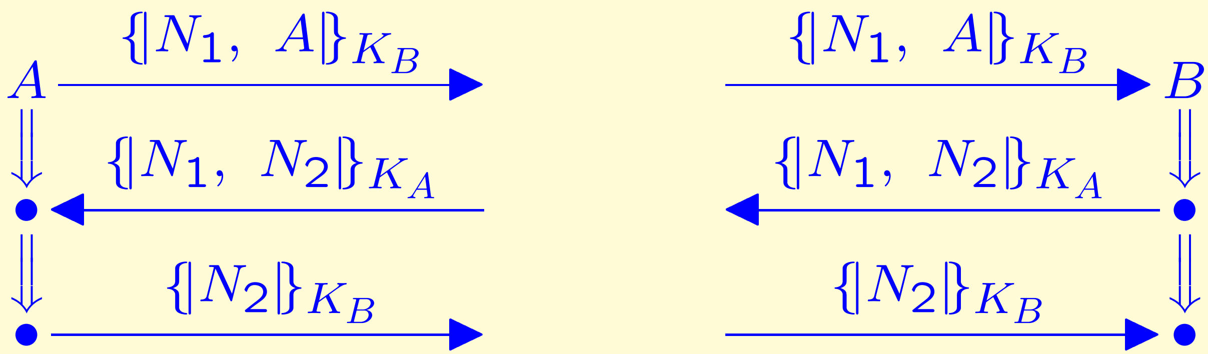
June 2003

Supported by the National Security Agency
and the MITRE-Sponsored Research program

Background

- Secrecy undecidable for cryptographic protocols, broadly understood
  - Proved in Multiset Rewriting Framework (CDLMS, 1999; DLMS, 19
  - A fortiori, authentication undecidable
- But is there a good alternate to this broad definition?
  - Are there narrower classes such that
    - Large majority of protocols belong to narrower class
    - Authentication, secrecy decidable for this class?
- Answer: Yes
  - Ramanujam and Suresh, WITS '03
  - Blanchet and Podelski, FOSSACS '03
  - Essentially, identify same class of protocols
  - Class of "unambiguous" protocols
- Goals of this Talk
  - Define set of unambiguous protocols
  - Sketch proof in strand space framework

An Unambiguous Protocol



Idea: Two nodes have unifiable encrypted parts only if intended to communicate directly

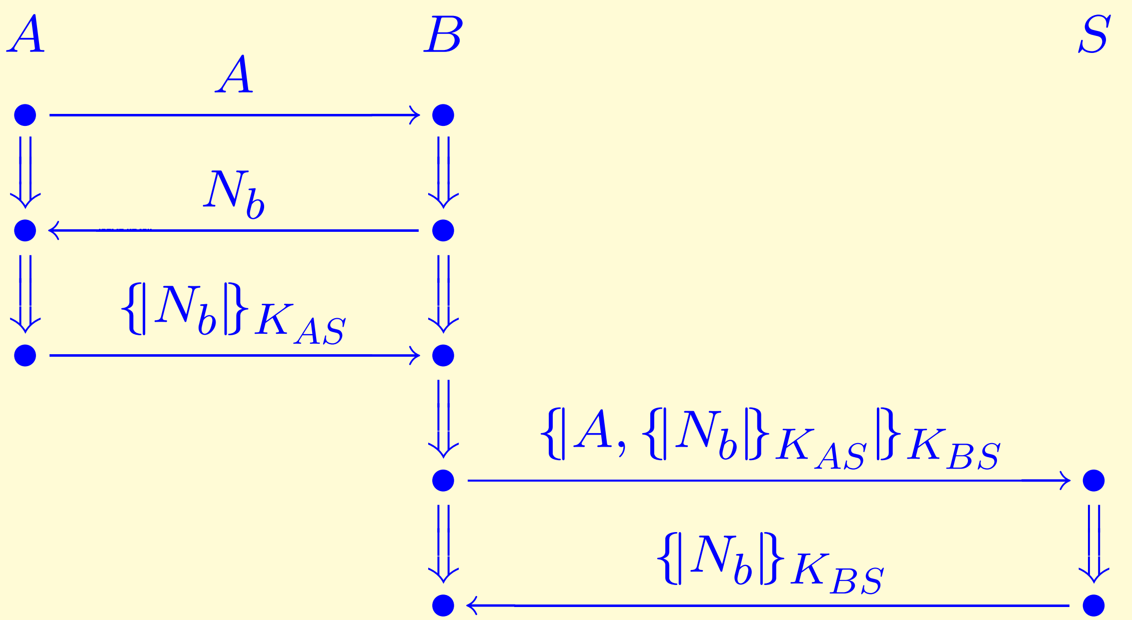
Never any ambiguity in what message an encrypted unit should belong to

Standard Bundle

$$
\begin{tikzcd}
A \arrow[rrr, "\{\!|N_1,\ A|\!\}_{K_B}"] \arrow[d, Rightarrow] & & & B \arrow[d, Rightarrow] \\
\bullet \arrow[d, Rightarrow] & & & \bullet \arrow[lll, "\{\!|N_1,\ N_2|\!\}_{K_A}"'] \arrow[d, Rightarrow] \\
\bullet \arrow[rrr, "\{\!|N_2|\!\}_{K_B}"] & & & \bullet
\end{tikzcd}
$$

- $n \to n'$ whenever
  - n positive, n' negative
  - $\{\!|h|\!\}_K \sqsubset \mathsf{term}(n)$ and $\{\!|h'|\!\}_{K'} \sqsubset \mathsf{term}(n')$
  - h, h' unifiable
- Protocol is unambiguous if
  its standard bundle has this property

An Ambiguous Protocol (due to Woo-Lam)



Unifiable encrypted subterms on non-communicating nodes

The Claim

The following problem is decidable:

- Let P be an unambiguous protocol
- Let G be a security goal
- Does P achieve G?

Need to define "security goal"

Quick Intro to Strand Spaces

- A strand is a sequence of send*, receive† events ("nodes")
  - Regular strands: a principal's protocol behavior in one local session
  - Adversary strands: a single deduction
  - Bundle: a finite, acyclic graph‡ $\mathcal{B}$ of nodes where
    - $n_0 \Rightarrow n_1$§ and $n_1 \in \mathcal{B}$ implies $n_0 \in \mathcal{B}$
    - $n_1 \in \mathcal{B}$ negative implies exists a unique $n_0 \rightarrow n_1$¶ in $\mathcal{B}$
- Subterms: $\sqsubset$ is smallest reflexive, transitive relation‖ s.t.

$$g \sqsubset g,\ \ h \qquad \text{and} \qquad h \sqsubset g,\ \ h \qquad \text{and} \qquad h \sqsubset \{|h|\}_K$$

- t originates on node n_1 if

*positive
$+$

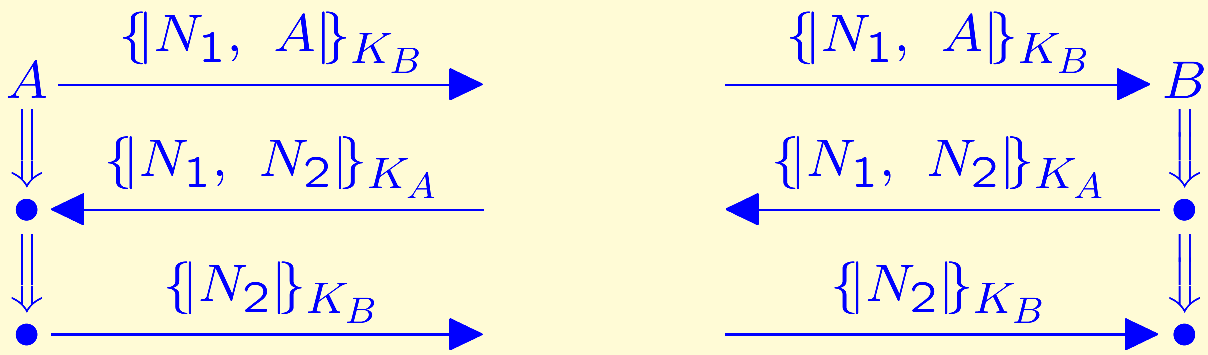
†negative
$-$

‖$K \sqsubset \{|h|\}_K$
only if $K \sqsubset h$

n_1 is positive, $\quad t \sqsubset \mathsf{term}(n_1)$, $\quad n_0 \Rightarrow^+ n_1$ implies $t \not\sqsubset \mathsf{term}(n_0)$

- t originates uniquely in S if $\exists! n \in S$ such that t originates on n
- t is non-originating in S if $\nexists n \in S$ such that t originates on n
  - Non-originating values may still be used as keys

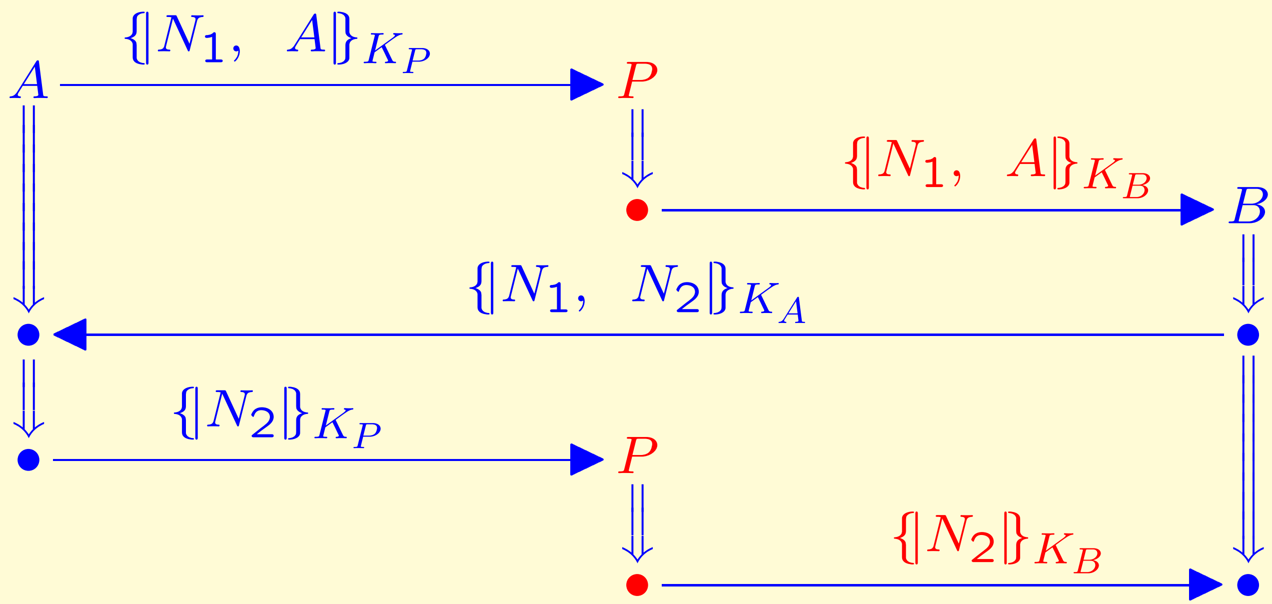
Regular Strands (Example)



NSInit$[A, B, N_1, N_2]$

NSResp$[A, B, N_1, N_2]$

A Bundle



Security Goals: An Example

NS Authentication (Responder's guarantee)

- Suppose:
  - Bundle $\mathcal{B}$ contains a strand Resp$[A, B, N_a, N_b]$
  - K_A^{-1} non-originating in $\mathcal{B}$
  - N_b originates uniquely in $\mathcal{B}$
- Then:
  - There is a strand Init$[A, B, N_a, N_b]$ in $\mathcal{B}$

Authentication: correspondence assertions (of form $\forall\exists$)
This is false for NS (only Init$[A, X, N_a, N_b]$ holds)

General Form of Authentication

- Suppose:
  - Bundle $\mathcal{B}$ contains j_1 nodes of $\mathsf{Strand}_1[\vec{X}]$, . . . , and j_ℓ nodes of $\mathsf{Strand}_\ell[\vec{Y}]$
  - $K, \ldots K'$ non-originating in $\mathcal{B}$
  - $N, \ldots, N'$ originates uniquely in $\mathcal{B}$
- Then $\mathcal{B}$ contains j_0 nodes of some strand $\mathsf{Strand}_0[\vec{Z}]$

General Form of Secrecy

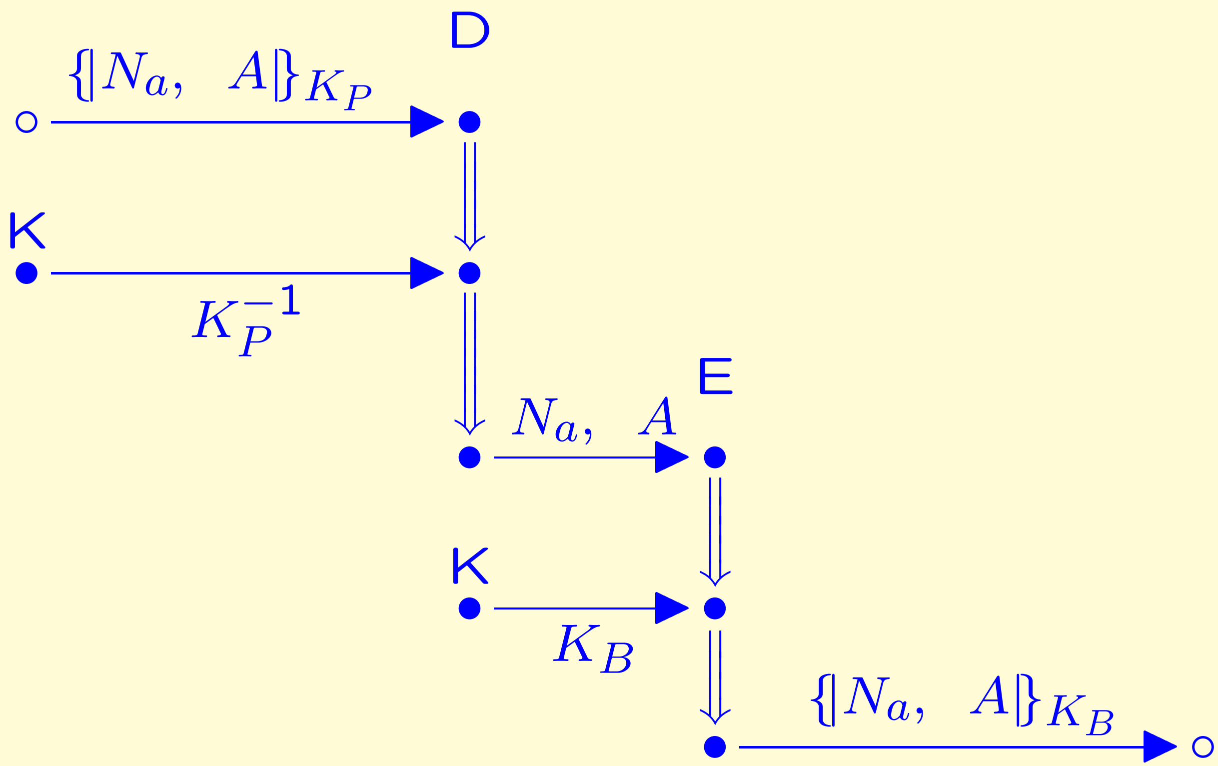
Secrecy for a value v

- Suppose:
  - Bundle $\mathcal{B}$ contains j_1 nodes of Strand1[$\vec{X}$], . . . , and j_ℓ nodes of Strand$_\ell$[$\vec{Y}$]
  - $K, \ldots K'$ non-originating in $\mathcal{B}$
  - $N, \ldots, N'$ originates uniquely in $\mathcal{B}$
- Then $\mathcal{B}$ contains no node n with term$(n) = v$

The Claim

- The following problem is decidable:
  - Let P be an unambiguous protocol
  - Let G be a security goal
  - Does P achieve G?
- Proof strategy:
  - For given P, G, if there's any counterexample bundle, then there's a bundle of size $< k_{P,G}$
  - Measure size by number of regular strands
  - Given any counterexample bundle, construct a "small" sub-bundle
- Must consider both adversary activity and regular activity

NS Attack: Adversary Activity



Destructive

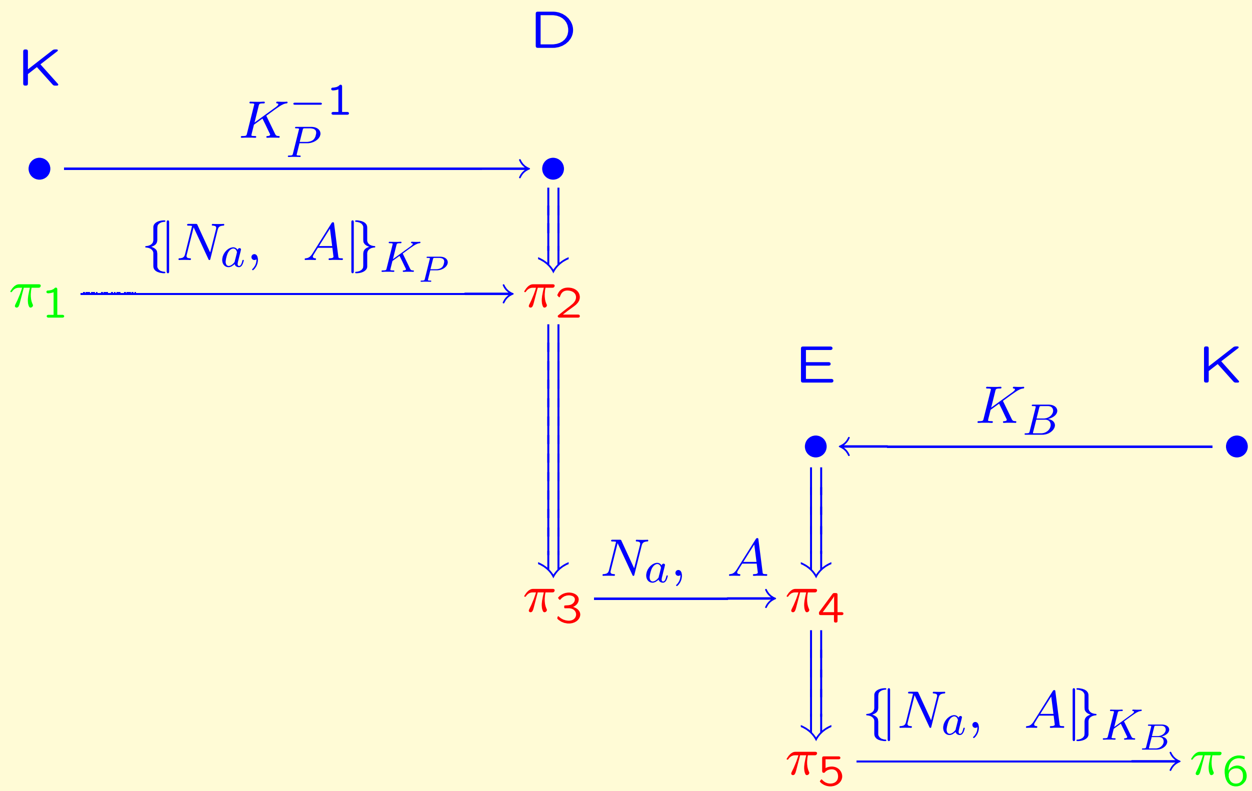
Constructive

May assume destruction precedes construction

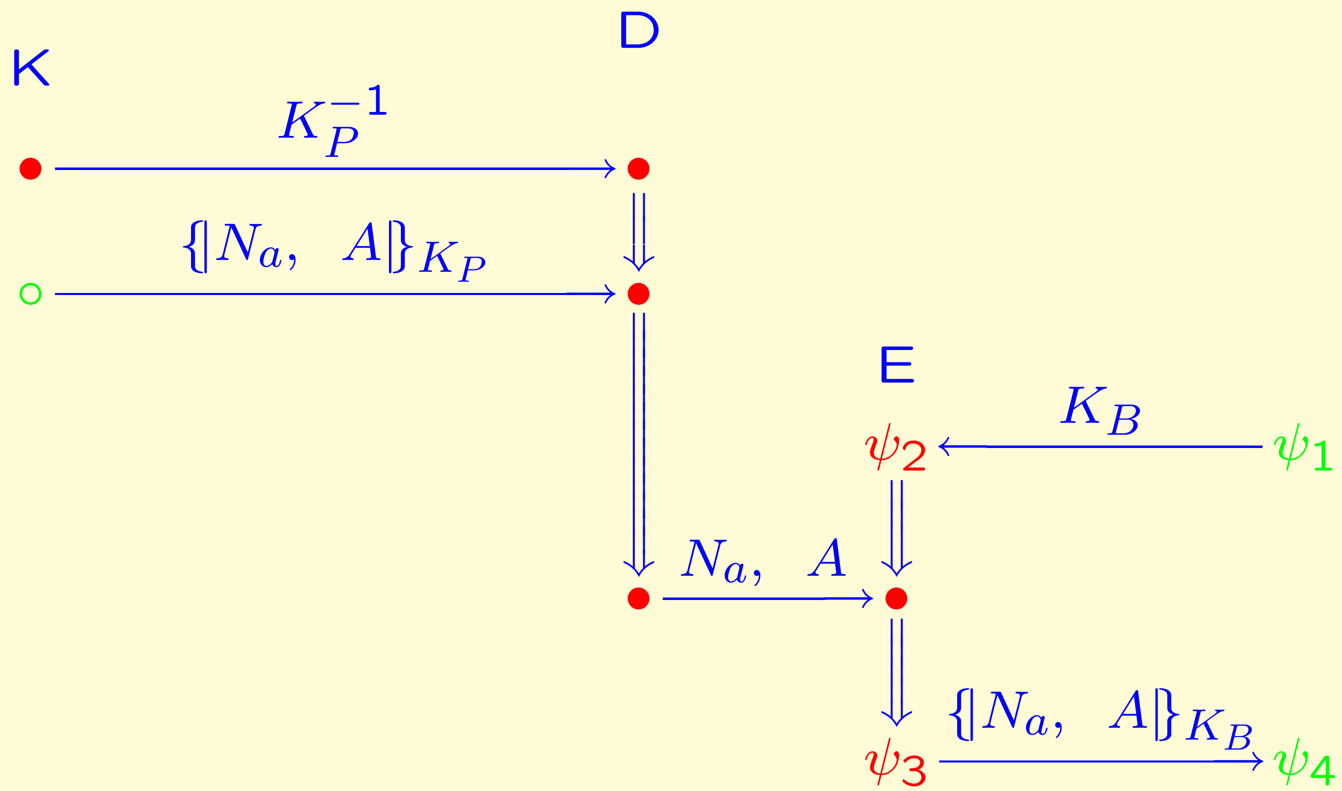
Paths

- $m \Rightarrow^{+} n$ means n occurs after m on the same strand
- $m \longmapsto n$ means either 1 or 2:
  1. $m \rightarrow n$
  2. $m \Rightarrow^{+} n$ where
     term(m) negative and
     term(n) positive
- Path p through $\mathcal{C}$: sequence
  $p_1 \longmapsto p_2 \longmapsto \cdots \longmapsto p_k$
  - Typically assume p_1 positive node, p_k negative node
  - Notation: $|p| = k$, $\ell(p) = p_k$
- Penetrator path: p_j penetrator node, except possibly $j = 1$ or $j = k$

A Penetrator Path



Another Penetrator Path



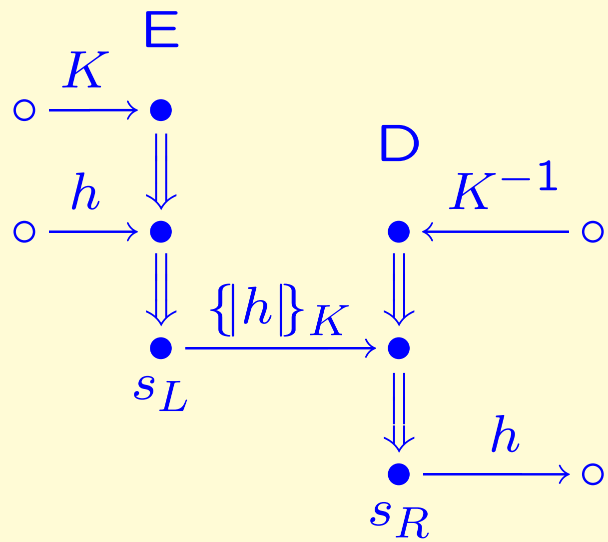
Equivalence and Normality

- $\mathcal{B} \equiv \mathcal{B}'$ if
  - Same regular nodes
  - Same uniquely originating values
  - Same non-originating values
- Bundle $\mathcal{B}$ normal if

  No penetrator path p has constructive $\Rightarrow$ edge before destructive $\Rightarrow$ edge

- Any bundle is equivalent to a normal one
  - Eliminate redundancies
  - No other constructive/destructive pairs by freeness

E-D Redundancies

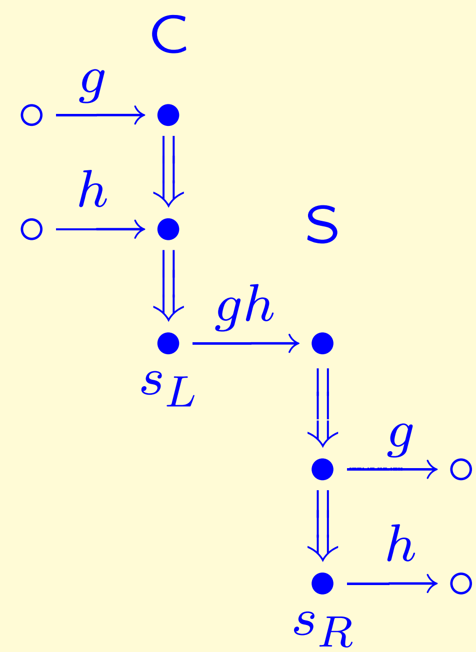


E-D Redundancy Elimination

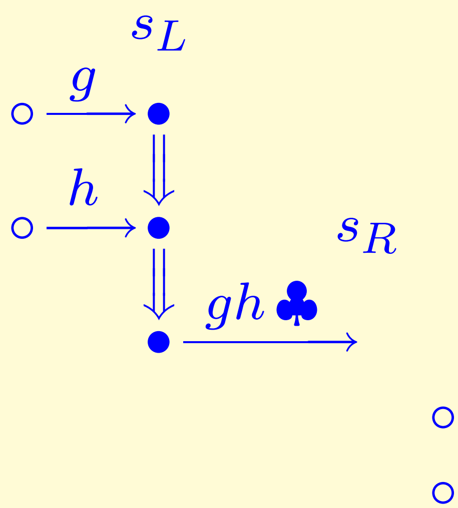
$$
\begin{tikzcd}
\circ \arrow[r, "K"] & \bullet \arrow[d, Rightarrow] & & \\
\circ \arrow[r, "h"] & \bullet \arrow[d, Rightarrow] & {} & \circ \arrow[l, "K^{-1}\ \clubsuit"'] \\
& \bullet \arrow[r, "\{|h|\}_K\ \clubsuit"] & {} & \\
& & & \circ
\end{tikzcd}
$$

$\clubsuit$ Discarded message

C-S **Redundancies**



C-S Redundancy Elimination



♣ Discarded message

Paths that Avoid Key Edges

- If p is destructive and p never traverses D-key edge then p is falling

$$\mathsf{term}(\ell(p)) \sqsubset \mathsf{term}(p_1)$$

- If p is constructive and p never traverses E-key edge then p is rising

$$\mathsf{term}(p_1) \sqsubset \mathsf{term}(\ell(p))$$

- If bundle normal and p avoids key edges

$$p = q \;\rightarrow\; q' \qquad\qquad q \text{ falling} \qquad\qquad q' \text{ rising}$$

- $\mathsf{term}(\ell(q)) = \mathsf{term}(q'_1) = \mathsf{pbt}(p)$ called "path bridge term"

$$\mathsf{pbt}(p) \sqsubset p_1 \qquad\qquad \mathsf{pbt}(p) \sqsubset \ell(p)$$

- Unambiguous protocols: If p connects mismatched nodes, $\mathsf{pbt}(p)$ is unencrypted

An Inefficient Bundle

$$
\begin{tikzcd}
m \arrow[r, "\{\!|N_a,\ \ A|\!\}_{K_P}"] \arrow[dd, Rightarrow] & P \arrow[d, Rightarrow] & \\
& \bullet \arrow[r, "\{\!|N_a,\ \ A|\!\}_{K_B}"] & B \arrow[d, Rightarrow] \\
\bullet \arrow[d, Rightarrow] & & \bullet \arrow[ll, "\{\!|N_a,\ \ N_b|\!\}_{K_A}"'] \arrow[dd, Rightarrow] \\
m' \arrow[r, "\clubsuit\quad \{\!|N_a,\ \ A|\!\}_{K_P}"] & n \arrow[d, Rightarrow] & \\
& \bullet \arrow[r, "\{\!|N_a,\ \ A|\!\}_{K_B}"] & \bullet
\end{tikzcd}
$$

Note: This protocol is fictitious!

An Efficient Bundle

$$
\begin{tikzcd}
m \arrow[rr, "\{\!|N_a,\ A|\!\}_{K_P}"] \arrow[dd, Rightarrow] & & P \arrow[d, Rightarrow] & \\
& & \bullet \arrow[r, "\{\!|N_a,\ A|\!\}_{K_B}"] & B \arrow[d, Rightarrow] \\
\bullet \arrow[d, Rightarrow] & & & \bullet \arrow[lll, "\{\!|N_a,\ N_b|\!\}_{K_A}"'] \arrow[dd, Rightarrow] \\
m' & \clubsuit & n \arrow[d, Rightarrow] & \\
& & \bullet \arrow[r, "\{\!|N_a,\ A|\!\}_{K_B}"] & \bullet
\end{tikzcd}
$$

Efficient: $m \prec m' \prec n$ and m' regular implies term$(m) \neq$ term(n)

Every bundle equivalent to a normal, efficient bundle

The Claim

- The following problem is decidable:
  - Let P be an unambiguous protocol
  - Let G be a security goal
  - Does P achieve G?
- Proof strategy:
  - For given P, G, if there's any counterexample bundle, then there's a bundle of size $< k_{P,G}$
  - Measure size by number of regular strands
  - Given any counterexample bundle $\mathcal{B}$, construct a "small" sub-bundle
  - May assume $\mathcal{B}$ normal, efficient
- Form of G:

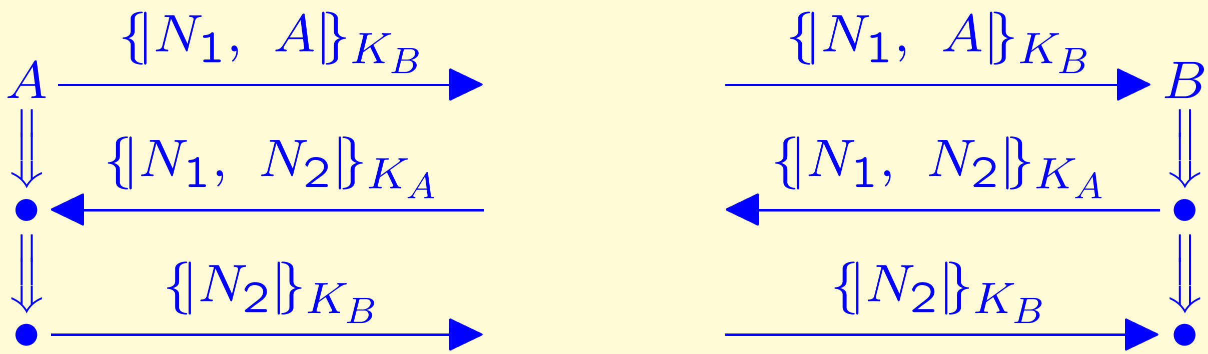
If	certain regular nodes* in $\mathcal{B}$
	certain values† uniquely originating, non-originating
Then	certain other regular nodes in $\mathcal{B}$

- May assume $m \in \mathcal{B}$ implies $m \preceq n$ for some node of interest n

Proof

- Consider maximal paths p leading to a node of interest
- Bound number of regular strands traversed on p
- Bound "branching factor" for paths
- Only finite number of bundles of given size exist

Regular Strands Traversed on Path



- u_P: Number of successive edges in standard bundle for P (3 in this example)
- At most u_P successive matches along p
  - Each mismatch consumes a protected value $a \in v_P$
  - Efficiency implies no repetitions
- Bound: $u_P \cdot |v_P|$

Branching Factor

- Let h_P be maximum height* of a regular term in P
- Consider $p_0 = p_1\ p_2$, where
  - p_1, p_2 begin with regular node;
  - p_1 has no other regular node
- Length$(p_1) \leq 2 \cdot h_P$
- Number of such $p_1 \leq 2^{2 \cdot h_P}$

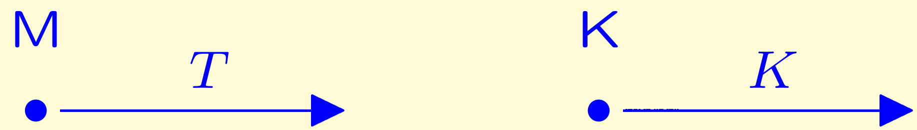
Number of regular strands below node of interest $p \leq (2^{2 \cdot h_P})^{u_P \cdot |v_P|}$

*Maximum length of
branch in abstract syntax tree
of term

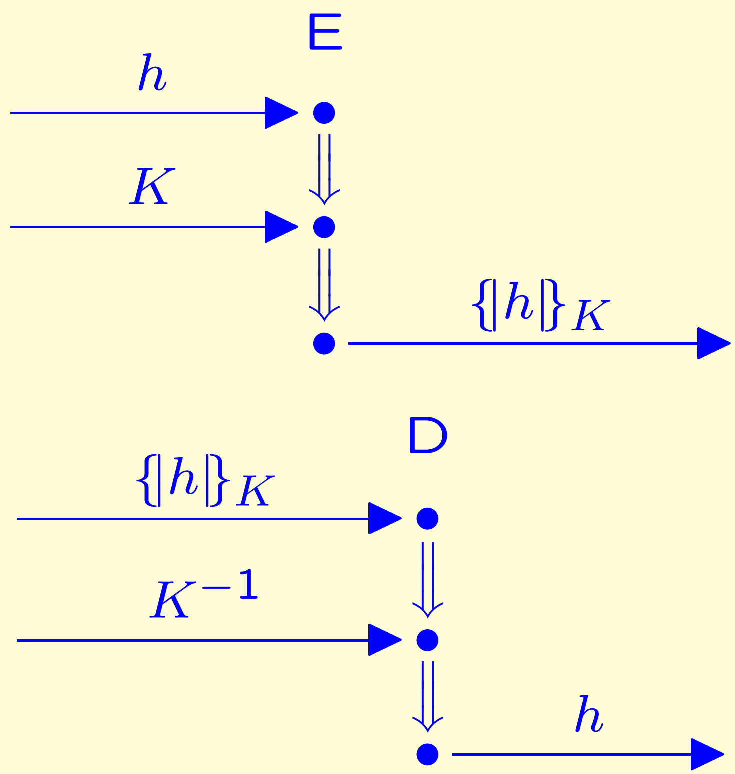
Summary

- Defined “unambiguous” protocols
  - Following Ramanujam, Suresh and Blanchet and Podelski
- Considered special forms of bundles
  - Normal bundles
  - Efficient bundles
- Limited number of regular strands below any node of interest
  - Smallest counterexample has only these regular strands

Adversary Strands, I: Initiating Values



Adversary Strands, II: Encrypt, Decrypt



Formalizes notion of ideal cryptography

Adversary Strands, III: Concatenate, Separate