Strand Spaces
Proving Protocols Corr

Jonathan Herzog

6 April 2001

Introduction

- Second part of talk given early last month
  - Introduced class of cryptographic protocols
  - Modeled at high level of abstraction
  - Imposed strong assumptions
  - Showed that flaws can exist independent of u cryptography
  - Discussed one approach to analysis (model ch
- This talk: Strand Spaces
  - Pencil & paper proof technique
  - Joint work with Guttman, Thayer

Overview of talk

- Brief review of problem
  - Running example: Otway-Rees protocols
- Strand Space formalization
  - Standard assumptions
  - “Regular” participants, penetrator (adversary)
  - Model protocol executions
    - Global view from local views
  - Definitions and machinery
  - Proofs of security conditions
    - Discovery of previously unpublished flaw

Protocols

- Sequence of messages between small number (2 o
cipals
  - No conditionals (except to abort)
- Abstract cryptographic primitives (encryption, sig
- Achieve authentication and/or key transmission

Otway-Rees Protocol

1. $A \longrightarrow B$: $M\ A\ B\ \{|N_a\ M\ A\ B|\}_{K_{as}}$

2. $B \longrightarrow S$: $M\ A\ B\ \{|N_a\ M\ A\ B|\}_{K_{as}}\ \{|N_b\ M\ A\ B|\}_{K_{bs}}$

3. $S \longrightarrow B$: $\{|N_a\ K_{ab}|\}_{K_{as}}\ \{|N_b\ K_{ab}|\}_{K_{bs}}$

4. $B \longrightarrow A$: $\{|N_a\ K_{ab}|\}_{K_{as}}$

- M: **Public, unique session ID**
- N_a, N_b: **"fresh" nonces**
- K_{as}, K_{bs}: **secret keys shared with distinguished se**
- K_{ab}: **fresh session key**
- **Designed to provide mutual authentication and s** K_{ab}
  - **Formalized later in terms of strands**

Message Algebra

- **Messages are elements of an "algebra"** $\mathcal{A}$
- **2 disjoint sets of atomic messages:**
  - **Texts** ($\mathcal{T}$)
  - **Keys** ($\mathcal{K}$)
- **2 operators:**
  - **enc** $: \mathcal{K} \times \mathcal{A} \rightarrow \mathcal{A}$ (**Range:** $\mathcal{E}$)
  - **pair** $: \mathcal{A} \times \mathcal{A} \rightarrow \mathcal{A}$ (**Range:** $\mathcal{C}$)
- **Often distinguish** $\mathcal{T}_{Names} \subseteq \mathcal{T}$, $\mathcal{T}_{Nonces} \subseteq \mathcal{T}$
  - $\mathcal{T}_{Names} \cap \mathcal{T}_{Nonces} = \emptyset$

+

Message Algebra (continued)

- **Message algebra is "free"**
  - **Unique representation of terms**
  - *Exactly* **one way to build elements from aton ations**
  - **Formulas, rather than bit-strings**
- $\mathcal{K}$, $\mathcal{T}$, $\mathcal{E}$, $\mathcal{C}$ **mutually disjoint**
- **For all** M_1, M_2, M_3, $M_4 \in \mathcal{A}$, k_1, $k_2 \in \mathcal{K}$, $T \in \mathcal{T}$
  - $M_1 M_2 \neq M_3 M_4$, **unless** $M_1 = M_3$, $M_2 = M_4$
  - $\{|M_1|\}_{k_1} \neq \{|M_2|\}_{k_2}$ **unless** $M_1 = M_2$, $k_1 = k_2$

+

Message Algebra Structure

- **There is structure in the message algebra to explo**
- **Define the** *subterm* **relation as the smallest rela that for all** a**,** g **and** h**:**
  - $a \sqsubset a$,
  - $a \sqsubset g \Rightarrow a \sqsubset \{\!|g|\!\}_k$
  - $a \sqsubset g \Rightarrow a \sqsubset g\,h \wedge a \sqsubset h\,g$

Strands

- **Two types of actions:** *transmissions* **and** *recepti*
  - **Written** $+M$ **and** $-M$ **(sign omitted when irr**
  - **Assumed to have unsecured sender, recipient**
    - **Ignored in this framework**
- *Trace*: **sequence of actions**
- *Strand*: **trace + unique identifier**
  - **Particular execution of a trace**
  - **Two different strands may have the same trac**
    - **Represent two different executions**
  - **Actions on strands called** *nodes*

$$\langle -A, +B, -C, +D \rangle$$

Regular Participants

- *Regular* **participants: All non-adversary agents**
- **Protocol defines all possible regular traces**
- **Regular participants represented by strands conta sible traces**
- **Internal actions, knowledge not modeled**

Regular Participants (continued)

- **Strand patterns for regular participants (Otway-Re**
  - **Initiator (A)**

$$\langle \quad + \quad M\,A\,C\,\{\!|N_a\,M\,A\,C|\!\}_{K_{as}}$$
$$- \quad \{\!|N_a\,K_{ac}|\!\}_{K_{as}}\rangle$$

  - **Responder: (B)**

$$\langle \quad - \quad M\,D\,B\,\{\!|g|\!\}_k$$
$$+ \quad M\,D\,B\,\{\!|g|\!\}_k\,\{\!|N_b\,M\,D\,B|\!\}_{K_{bs}}$$
$$- \quad \{\!|h|\!\}_k\,\{\!|N_b\,K_{db}|\!\}_{K_{bs}}$$
$$+ \quad \{\!|h|\!\}_k\rangle$$

  - **Server: (S)**

$$\langle \quad - \quad M\,A\,B\,\{\!|N_a\,M\,A\,B|\!\}_{K_{bs}}\,\{\!|N_b\,M\,A\,B$$
$$+ \quad \{\!|N_a\,K_{ab}|\!\}_{K_{as}}\,\{\!|N_b\,K_{ab}|\!\}_{K_{bs}}\rangle$$

Regular Participants (continued)

- Strands "refuse" to receive any messages other expected ones
  - Implicit abort/fail operation in such cases
- Regular strands completely defined by values
  - No variables
  - These are different strands:

$$\left\langle +M\ A\ B\ \{\!|N_a\ M\ A\ B|\!\}_{K_{as}}, -\{\!|N_a\ K_{ab}|\!\}_{K\right.$$

$$\left\langle +M\ A\ B\ \{\!|N_a\ M\ A\ B|\!\}_{K_{as}}, -\{\!|N_a\ K'_{ab}|\!\}_{K\right.$$

Regular Participants (continued)

- **Often convenient to define sets of strands with sin**

Init-Strands$[A, B, M, N_a, k_{ab}] =$
$\Big\{s$: s **has trace** $\Big\langle M\ A\ B\ \{\!|N_a\ M\ A\ B|\!\}_{K_{as}}, -\{\!|N_a\ I$

(Empty if parameters of wrong types)

- **Build larger sets from these:**

$$\text{Init-Strands}[*, B, M, *, k_{ab}] = \bigcup_{\substack{A \in \mathcal{T}_{Names},\\ N_a \in \mathcal{T}_{Nonces}}} \text{Init-Strands}[A, B, M, N_a, k$$

Penetrator (Adversary)

- Represented in terms of atomic (abstract) actions
  - More complex actions can be built from these
- Unbounded number of strands of the forms:
  - **[C]:** $\langle -g, -h, +gh \rangle$
  - **[S]:** $\langle -gh, +g, +h \rangle$
  - **[E]:** $\langle -g, -k, +\{\!|g|\!\}_k \rangle$
  - **[D]:** $\left\langle -\{\!|g|\!\}_k, -k^{-1}, +g \right\rangle$
  - **[M]:** $\langle +g \rangle$, if $g \in \mathcal{T}_\mathcal{P} \subseteq \mathcal{T}$
  - **[K]:** $\langle +k \rangle$, if $k \in \mathcal{K}_\mathcal{P} \subseteq \mathcal{K}$

  (Often assume limits on $\mathcal{T}_\mathcal{P}$, $\mathcal{K}_\mathcal{P}$)
- Communication channels double as penetrator wo
- Model penetrator control over network later

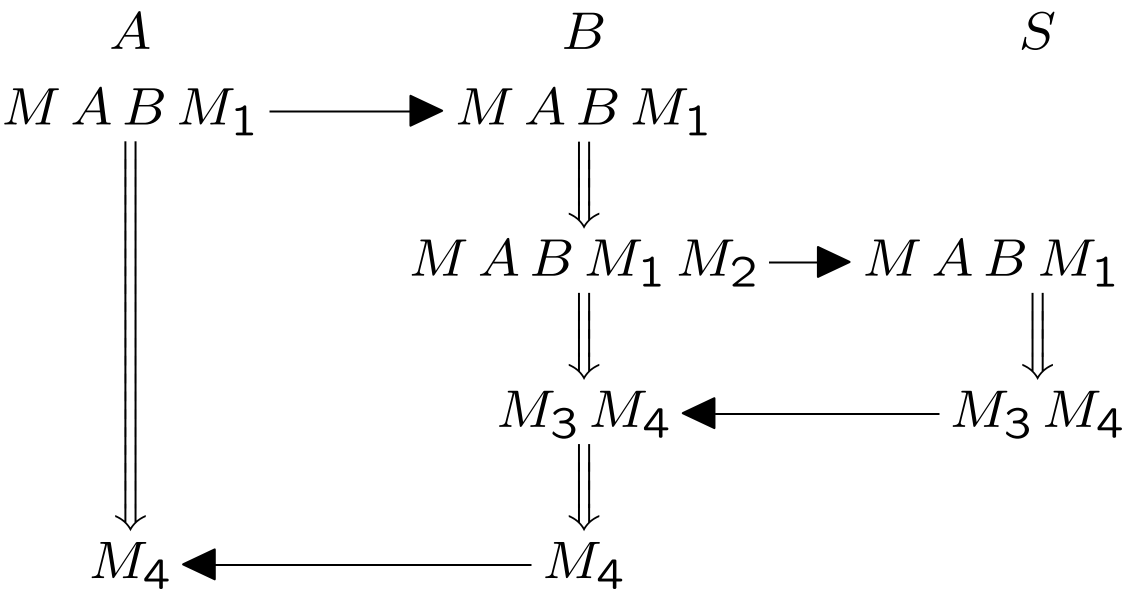
+

Bundles

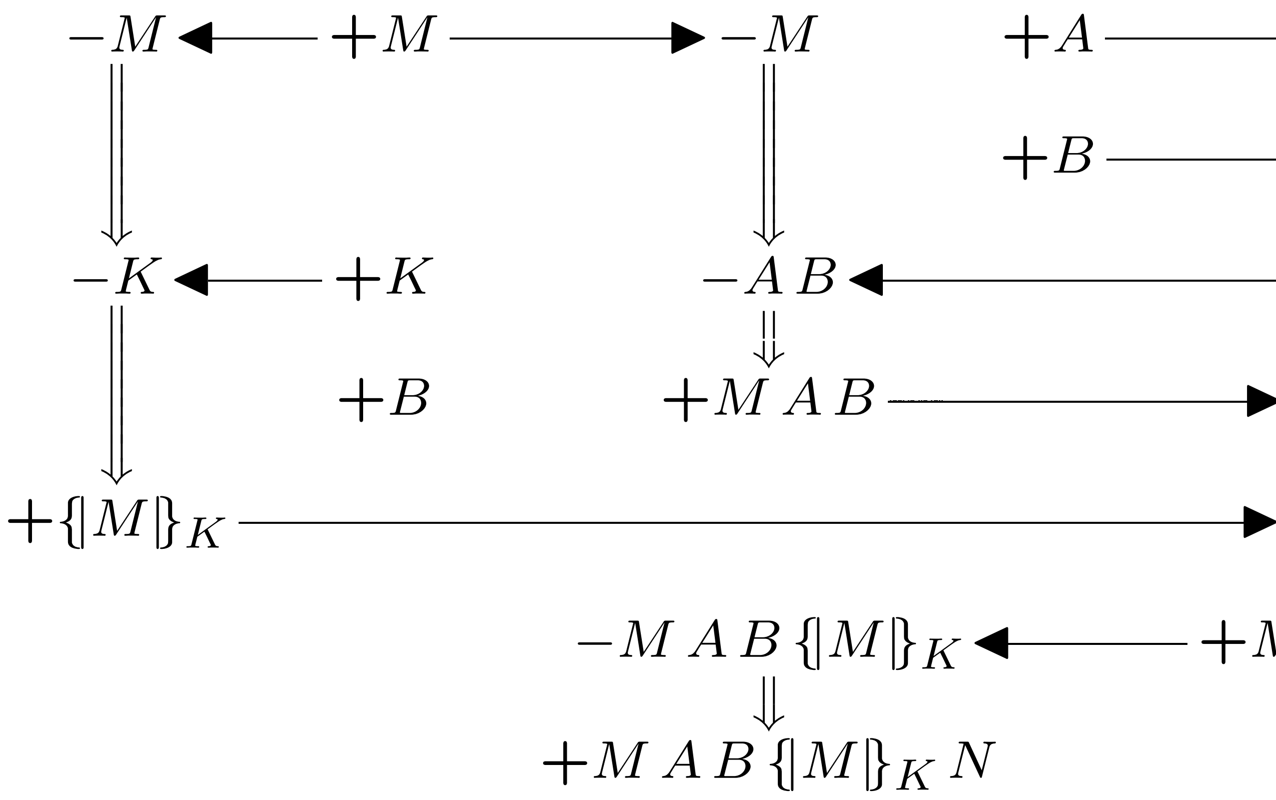
- Consider graphs where
  - Nodes are actions on regular, penetrator stran
  - Two types of edges:
    - We write $+g \rightarrow -g$ (transmission/receptio
    - We write $g \Rightarrow h$ if (g, h) are consecutive s strand
- A *bundle* is such a graph $\mathcal{C}$ (finite) where
  - If $-n$ is a node of $\mathcal{C}$, then there exists a un $+n$ of $\mathcal{C}$ such that $+n \rightarrow -n$ is an edge of $\mathcal{C}$
  - If n_1 is a node of $\mathcal{C}$, and $n_0 \Rightarrow n_1$, then n_0 is C and $n_0 \Rightarrow n_1$ is an edge of $\mathcal{C}$
  - $\mathcal{C}$ is acyclic
- Models concepts of causality

+

Example Bundle



Example Bundle



(Where $N = \{|N_b\, M\ A\ B|\}_{K_{bs}}$**)**

+

Bundle Properties

- **Bundles are partial orders**
  - **Any non-empty set has minimal elements**

- **Important Definition 1:**
  - **A value v *originates* on a node n if**
    - n **is a positive node (transmission)**
    - $v \sqsubset n$**,**
    - **If $n' \Rightarrow \ldots \Rightarrow n$, then $v \not\sqsubset n$**
  - **Origination points are where values spontane pear**
  - **Minimal elements of $\{n|v \sqsubset n\}$ are origination**
  - **We model the freshness of a value by saying t a unique origination point in the bundle**

+

+

Bundle Properties (continued)

- **Important Definition 2:**
  - **A set $H \subseteq \mathcal{A}$ is *honest*, with respect to a se[t] trator strands, if**
    - **For all bundles $\mathcal{C}$, minimal elements of**

$$\{n \in nodes(\mathcal{C}) | term(n) \in H\}$$

      are not on penetrator nodes.
  - **Important tool for proving security conditions**
  - **Example of honest set will come later**

+

Secrecy Conditions

- Intuitively, a value v is secret if no penetrator can
  v from the messages of regular participants
- A value v is *secret*, with respect to a set of assun
  if no bundle that satisfies $\mathcal{A}$ contains a node of the
- One proof technique:
  - Show that v is in an honest set H
  - Fix an arbitrary bundle that satisfies $\mathcal{A}$.
  - Through case analysis, show that H has no m
    ements on regular strands
  - Because H is honest, no minimal elements on p
    strands
  - Hence, no nodes in bundle in H

Authentication Conditions

- **Example: "If a bundle contains all of a given initiat then it must also contain a given responder stranc**
- **Formalized as inference: If a bundle contains a str α, then the bundle also contains a strand from a s β**
- **One proof technique:**
  - **Suppose the bundle contains a strand $s \in \alpha$**
  - **Find a honest set H_s so that s contains a noc**
  - **Since the bundle has a node in H_s, it must ha imal element**
  - **Minimal elements must be on regular strands**
  - **Show that those strands must be in β**

Ideals

- Honest sets only useful if they exist
- Let $\mathrm{k} \subseteq \mathcal{K}$. Then a k-ideal I is a set such that
  - $g \in I \Rightarrow g\,h \in I$, $h\,g \in I$
  - $g \in I$, $k \in \mathbf{k} \Rightarrow \{\!|g|\!\}_k \in I$
- Let S be a set of messages.
  - Then $I_{\mathrm{k}}[S]$ is the smallest k-ideal that contai
- Big theorem: If
  - $S \subseteq \mathcal{T} \cup \mathcal{K}$,
  - $S \cap (\mathcal{T}_{\mathcal{P}} \cup \mathcal{K}_{\mathcal{P}}) = \emptyset$,
  - $\mathbf{k} = (\mathcal{K} \setminus S)^{-1}$, and

  Then $I_{\mathrm{k}}[S]$ is honest

Ideals Intuition

- **Typically,**
  - S **is a set of secrets**
  - **Since** $\mathrm{k} = (\mathcal{K} \setminus S)^{-1}$**,** k **contains (inverse of) e**
    key
- $I_{\mathrm{k}}[S]$ **contains every term in which a secret is encry**
  with non-secret keys
- **Theorem: penetrator can only produce one of thes**
  ing one first

Otway-Rees Secrecy

- **Wish to show secrecy of K_{ab}:**
  - **Suppose K_{ab} is uniquely originating**
  - **Suppose K_{as}, $K_{bs} \notin \mathcal{K}_{\mathcal{P}}$**
  - **Suppose the bundle $\mathcal{C}$ contains a strand in** Serv-Strands$[A, B, M, N_a, N_b, K_{ab}]$
  - **Let $S = \{K_{as}, K_{bs}, K_{ab}\}$, $\mathbf{k} = \mathcal{K} \setminus S$**
  - **Then no node in $\mathcal{C}$ is in $I_{\mathbf{k}}[S]$**
- **Proof:**
  - **S, $\mathbf{k}$ meet criteria of big theorem**
  - **Case analysis: no regular node are minimal el** $I_{\mathbf{k}}[S]$
  - **Hence, no nodes in bundle in $I_{\mathbf{k}}[S]$**

Corollary to Big Theorem

- **Suppose**
  - $S \subseteq \mathcal{T} \cup \mathcal{K}$, $(\mathcal{K} \setminus S)^{-1} = \mathbf{k}$, **and** $S \cap (\mathcal{T}_{\mathcal{P}} \cup \mathcal{K}_{\mathcal{P}}$
  - **No regular node is a minimal element of** $I_{\mathbf{k}}[S$

Then any message of the form $\{|g|\}_k$ **for** $k \in S$ **originated on a regular node.**

+

Otway-Rees Authentication

- **Suppose** $\mathcal{C}$ **contains a strand in** Init-Strands$[A, B,$
- **If:**
  - $A \neq B$,
  - N_a **is uniquely originating,**
  - **All keys that originate on server strands** *uniq*
    nate on server strands
  - K_{as}, $K_{bs} \notin \mathcal{K}_{\mathcal{P}}$,
- **Then for some** N_b, $\mathcal{C}$ **contains strands in**

$$\text{Serv-Strands}[A, B, M, N_a, N_b, K_{ab}]\text{, and}$$

$$\text{Resp-Strands}[A, B, M, N_b, *]$$

+

Otway-Rees Authentication: Proof

- **Proof: Messy**
- **Let** $S = \{K_{as}\}$**,** $\mathbf{k} = \mathcal{K} \setminus S$**.**
- **Show no regular nodes are minimal elements** $I_{\mathbf{k}}[S$
- **Apply Corollary: Any term of the form** $\{|g|\}_{K_{as}}$ **ori regular node**
- **Hence,** $\{|N_a\, K_{ab}|\}_{K_{as}}$ **originates on regular node**
  - **Case analysis: strand in** Serv-Strands$[A, B, M, N_a, N_b, K_{ab}]$ **(for some**
- **Apply previous result: No minimal elements of** $I_{\mathbf{k}'}$ $S' = \{K_{as}, K_{bs}, K_{ab}\}$**,** $\mathbf{k}' = \mathcal{K} \setminus S'$
- **Hence** $\{|M\, N_b\, A\, B|\}_{K_{bs}}$ **originates on regular stran**
  - **Case analysis:** Resp-Strands$[A, B, M, N_b, *]$

Otway-Rees Authentication (continued)

- **Similar result for Responder: suppose**
  - $\mathcal{C}$ **contains a strand in**

    $$\textsf{Resp-Strands}[A, B, M, N_a, K_{ab}]$$

  - $A \neq B$**,**
  - N_b **is uniquely originating,**
  - **All keys that originate on server strands** *uniq*
    nate on server strands
  - K_{as}, $K_{bs} \notin \mathcal{K}_{\mathcal{P}}$**,**
- **Then** $\mathcal{C}$ **contains strands in** $\textsf{Serv-Strands}[A, B, M,$
  and $\textsf{Init-Strands}[A, B, M, *, *]$
- **Note: Cannot show that initiator, responder agree**
  key

Closing Remarks

- Further developments:
  - Protocol composition
  - Automated protocol analysis
    - Athena (Song)
  - Simpler results
    - Authentication tests
- Open questions
  - Non-free algebras (Xor, Diffie–Hellman)
  - Reconciliation with computational viewpoint

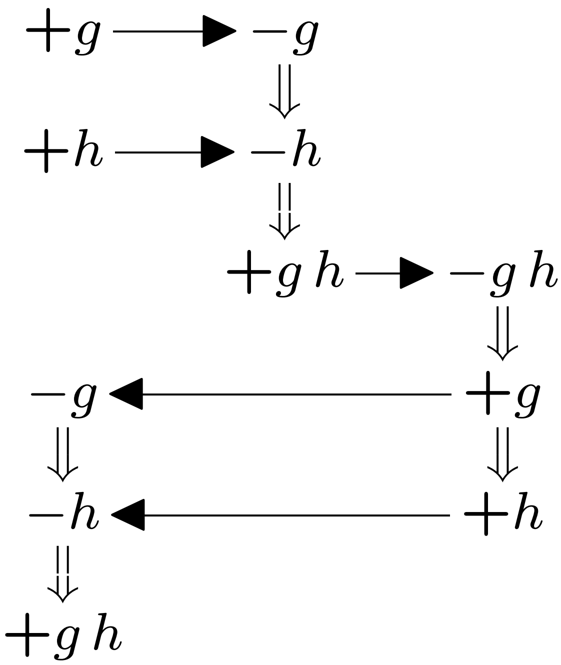
What Good are Proofs?

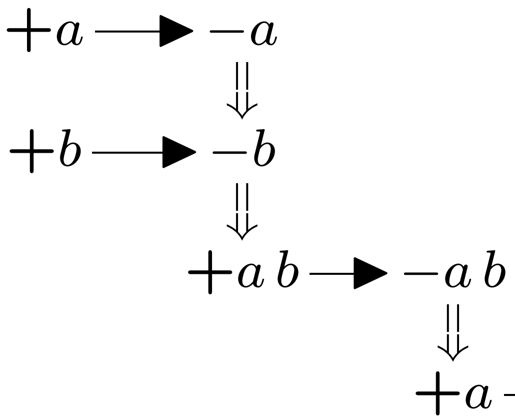
- Strands: proof technique
  - Uses (standard) strong assumptions
  - Proves (at present) protocol-specific statemen
- Proof fails:
  - Find cryptography-independent flaw
- Proof works:
  - What have you shown?
  - Strong motivation for justifying assumptions
  - Goal for further work on cryptographic primiti

Formalization of Security Conditions

- In practice, two types of security conditions to pro
  - Secrecy of values (keys, nonces)
  - Authentication
- State of the art:
  - Competing models, formalizations, intuitions
  - Most methods prove protocol-specific condi pressed in model
  - Why?
    - Still debate over right definitions
    - Protocols seem to satisfy points on con conditions
- No reason Strand Space reasoning would be inva universal definitions

Origination Vs. Minimality





Subterm relation

- **Note that $k \sqsubset \{\!|g|\!\}_k \Rightarrow k \sqsubset g$**
  - **Intuition: $a \sqsubset b$ means that a can be "learned**
  - **To say that $k \not\sqsubset \{\!|g|\!\}_k$ (unless $k \sqsubset g$) prohibits attacks**
  - **Other definitions of subterm possible**
    - **Lead to similar results**

Ideals (continued)

- **Proof of big theorem– case analysis**
- **Example: [D] strand** ($\left\langle -\{|g|\}_k, -k^{-1}, +g \right\rangle$)
  - **If** $+g$ **is a minimal element, then** $k^{-1} \notin I_{\mathbf{k}}[S$
    $k^{-1} \notin S$
  - **Since** $(\mathcal{K} \setminus S)^{-1} = \mathbf{k}$, $k^{-1} \in \mathbf{k}^{-1}$. **Hence,** $k \in$
  - **But since** $g \in I_{\mathbf{k}}[S]$, $\{|g|\}_k \in I_{\mathbf{k}}[S]$

Ideals (continued)

- **More complex example: [E] strand ($\langle -g, -k, +\{\!|g$**
  - **Suppose** $\{\!|g|\!\}_k \in I_k[S]$**, but** $g \notin I_{\mathbf{k}}[S]$
  - **Let** $I' = I_{\mathbf{k}}[S] \setminus \{\{\!|g|\!\}_k\}$**.**
  - I' **still contains** S
    - $S \subseteq \mathcal{T} \cup \mathcal{K}$
  - I' **still closed under join operator**
  - I' **still closed under encryption with keys in** $\mathbf{k}$
    - **If not, because** $g \in I_{\mathbf{k}}[S]$ **and** $k \in \mathbf{k}$
  - **Hence,** I' **a smaller** $\mathbf{k}$**-ideal containing** S**, a con**