# Metareasoning about Security Protocols using Distributed Temporal Logic

**Carlos Caleiro**

Dep. Mathematics, IST, TU Lisbon, Portugal

**Luca Viganò** **David Basin**

Dep. Computer Science, ETH Zurich, Switzerland

**ARSPA WS at IJCAR'04, Cork, Ireland**

**July 4, 2004**

## Motivation

- **Formal methods for security protocol analysis**
- **Most problems due to communication and distribution, rather than cryptography**
- **Many models, many simplifications, many assumptions**

## Motivation

- **Formal methods for security protocol analysis**
- **Most problems due to communication and distribution, rather than cryptography**
- **Many models, many simplifications, many assumptions**

## Goal

- **Use a protocol independent distributed temporal logic**
- **Formalize different models, protocols and security goals**
- **Prove the correctness of modeling and reasoning simplification techniques**

# Plan

- Overview of distributed temporal logic
- A simple network model
- Protocol modeling and security goals
- Metareasoning examples
  - Secrecy lemma
  - One intruder is enough
  - The predatory intruder

# Distributed temporal logic

K. Lodaya, R. Parikh, R. Ramanujam, and P.S. Thiagarajan.
A logical study of distributed transition systems. *Information and Computation*, 119(1):91-118, 1995.

H.-D. Ehrich, C. Caleiro, A. Sernadas, and G. Denker.
Logics for specifying concurrent information systems. In *Logic for Databases and Information Systems*, pages 167–198. Kluwer, 1998.

H.-D. Ehrich and C. Caleiro.
Specifying communication in distributed information systems. *Acta Informatica*, 36:591-616, 2000.

# Distributed temporal logic


K. Lodaya, R. Parikh, R. Ramanujam, and P.S. Thiagarajan.
A logical study of distributed transition systems. *Information and Computation*, 119(1):91-118, 1995.

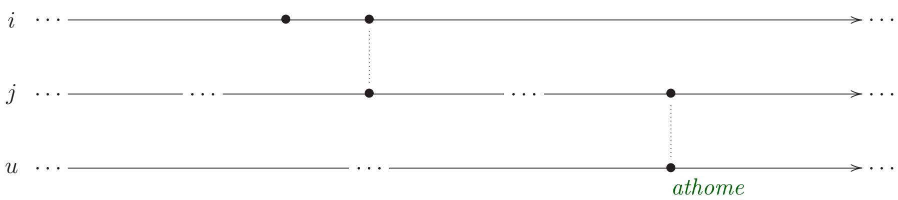
H.-D. Ehrich, C. Caleiro, A. Sernadas, and G. Denker.
Logics for specifying concurrent information systems. In *Logic for Databases and Information Systems*, pages 167–198. Kluwer, 1998.

H.-D. Ehrich and C. Caleiro.
Specifying communication in distributed information systems. *Acta Informatica*, 36:591-616, 2000.


$$@_i[\,\mathsf{X}\ @_j[\,\mathsf{F}\ @_u[\,athome\,]]]$$

"I will next call Jean and tell her to call you later, when you are at home"

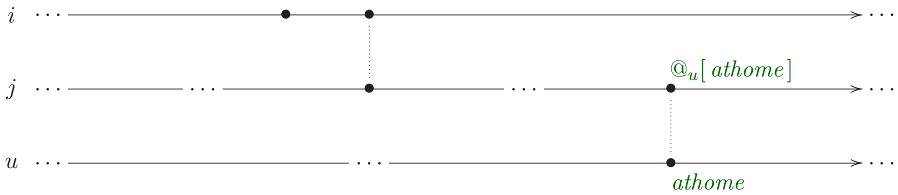
# Distributed temporal logic




$$@_i[\,\mathsf{X}\ @_j[\,\mathsf{F}\ @_u[\,athome\,]]]$$

"I will next call Jean and tell her to call you later, when you are at home"

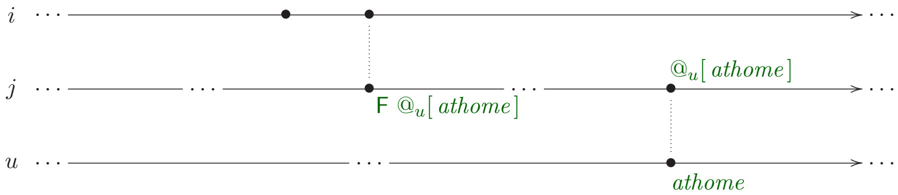
# Distributed temporal logic




$$@_i[\,\mathsf{X}\ @_j[\,\mathsf{F}\ @_u[\,athome\,]]]$$

"I will next call Jean and tell her to call you later, when you are at home"

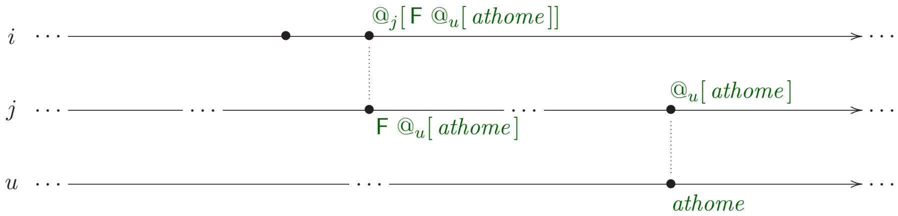
# Distributed temporal logic




$$@_i[\,\mathsf{X}\ @_j[\,\mathsf{F}\ @_u[\,athome\,]]]$$

"I will next call Jean and tell her to call you later, when you are at home"

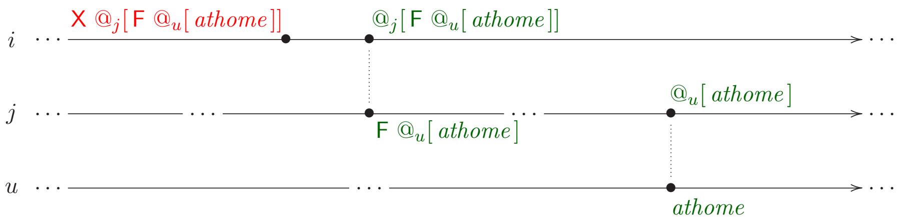
# Distributed temporal logic




$$@_i[\,\mathsf{X}\ @_j[\,\mathsf{F}\ @_u[\,athome\,]]]$$

"I will next call Jean and tell her to call you later, when you are at home"

# Distributed temporal logic




$$@_i[\,\mathsf{X}\ @_j[\,\mathsf{F}\ @_u[\,athome\,]]]$$

"I will next call Jean and tell her to call you later, when you are at home"

# Syntax

**Distributed signature** $\Sigma = \langle Id, \{Act_i\}_{i \in Id}, \{Prop_i\}_{i \in Id} \rangle$

$Id$ finite set of **agent identifiers**
each $Act_i$ is a set of **local action symbols**
each $Prop_i$ is a set of **local state propositions**

$$\mathcal{L} ::= @_i[\mathcal{L}_i] \mid \perp \mid \mathcal{L} \Rightarrow \mathcal{L}$$

$$\mathcal{L}_i ::= Act_i \mid Prop_i \mid \perp \mid \mathcal{L}_i \Rightarrow \mathcal{L}_i \mid \mathcal{L}_i \,\mathsf{U}\, \mathcal{L}_i \mid \mathcal{L}_i \,\mathsf{S}\, \mathcal{L}_i \mid @_j[\mathcal{L}_j]$$

# Models

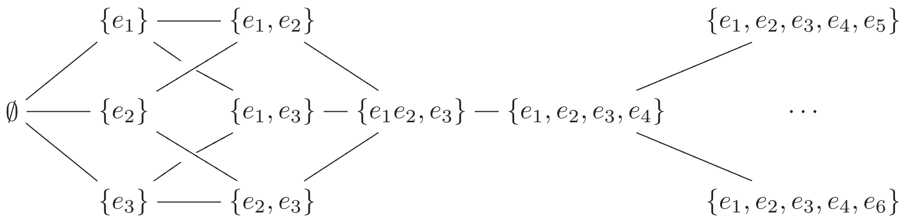
$\mu = \langle \lambda, \alpha, \pi \rangle$

$$\lambda \quad \left\{ \begin{tikzcd} i & e_1 \arrow[r] & e_4 \arrow[r] \arrow[d, dotted, no head] & e_5 \arrow[rr] & & e_8 \arrow[r] \arrow[d, dotted, no head] & \cdots \\ j & e_2 \arrow[r] & e_4 \arrow[rr] \arrow[d, dotted, no head] & & e_7 \arrow[r] \arrow[d, dotted, no head] & e_8 \arrow[r] & \cdots \\ k & e_3 \arrow[r] & e_4 \arrow[r] & e_6 \arrow[r] & e_7 \arrow[r] & e_9 \arrow[r] & \cdots \end{tikzcd} \right.$$

# Models

$\mu = \langle \lambda, \alpha, \pi \rangle$

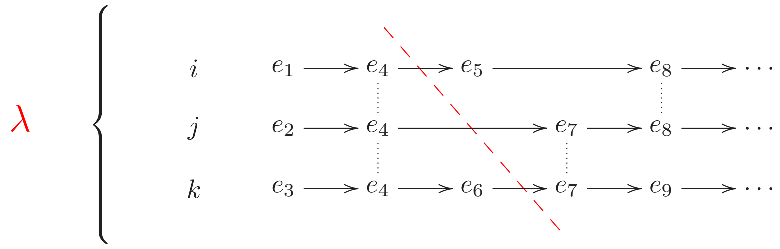
$$\lambda \quad \left\{ \begin{array}{lllllll} i & e_1 \longrightarrow & e_4 \longrightarrow & e_5 \longrightarrow & & e_8 \longrightarrow & \cdots \\ j & e_2 \longrightarrow & e_4 \longrightarrow & & e_7 \longrightarrow & e_8 \longrightarrow & \cdots \\ k & e_3 \longrightarrow & e_4 \longrightarrow & e_6 \longrightarrow & e_7 \longrightarrow & e_9 \longrightarrow & \cdots \end{array} \right.$$

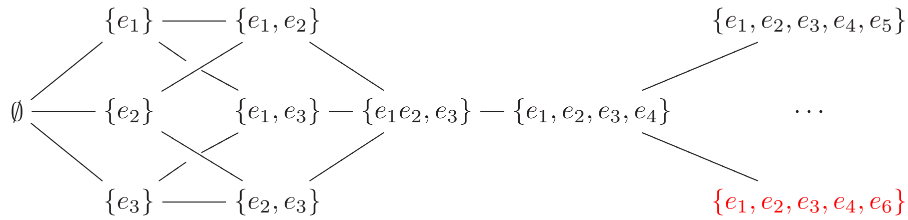



Global configurations $\Xi$

# Models

$\mu = \langle \lambda, \alpha, \pi \rangle$




Global configurations $\Xi$

# Models

$\mu = \langle \lambda, \alpha, \pi \rangle$

$$\lambda \quad \left\{ \begin{array}{llllllll} i & \Downarrow & e_1 \longrightarrow & e_4 \longrightarrow & e_5 \longrightarrow & \longrightarrow & e_8 \longrightarrow & \cdots \\ j & & e_2 \longrightarrow & e_4 \longrightarrow & \longrightarrow & e_7 \longrightarrow & e_8 \longrightarrow & \cdots \\ k & & e_3 \longrightarrow & e_4 \longrightarrow & e_6 \longrightarrow & e_7 \longrightarrow & e_9 \longrightarrow & \cdots \end{array} \right.$$

$\emptyset$

Local configurations $\Xi_i$

# Models

$\mu = \langle \lambda, \alpha, \pi \rangle$

$$\lambda \quad \left\{ \begin{tikzcd} i & e_1 \arrow[r, "\Downarrow"] & e_4 \arrow[r] \arrow[d, dotted, no head] & e_5 \arrow[rr] & & e_8 \arrow[r] \arrow[d, dotted, no head] & \cdots \\ j & e_2 \arrow[r] & e_4 \arrow[rr] \arrow[d, dotted, no head] & & e_7 \arrow[r] \arrow[d, dotted, no head] & e_8 \arrow[r] & \cdots \\ k & e_3 \arrow[r] & e_4 \arrow[r] & e_6 \arrow[r] & e_7 \arrow[r] & e_9 \arrow[r] & \cdots \end{tikzcd} \right.$$

$$\begin{tikzcd} \emptyset \arrow[r, no head] & \{e_1\} \end{tikzcd}$$

Local configurations $\Xi_i$

# Models

$\mu = \langle \lambda, \alpha, \pi \rangle$

$$\lambda \quad \left\{ \begin{array}{ll} i & e_1 \longrightarrow e_4 \xrightarrow{\Downarrow} e_5 \longrightarrow e_8 \longrightarrow \cdots \\ j & e_2 \longrightarrow e_4 \longrightarrow e_7 \longrightarrow e_8 \longrightarrow \cdots \\ k & e_3 \longrightarrow e_4 \longrightarrow e_6 \longrightarrow e_7 \longrightarrow e_9 \longrightarrow \cdots \end{array} \right.$$

$$\emptyset \;\text{———}\; \{e_1\} \;\text{———}\; \{e_1, e_4\}$$

Local configurations $\Xi_i$

# Models

$\mu = \langle \lambda, \alpha, \pi \rangle$

$$\lambda \quad \left\{ \begin{array}{llllllll} i & e_1 & \longrightarrow e_4 & \longrightarrow e_5 & \xrightarrow{\quad\Downarrow\quad} & e_8 & \longrightarrow \cdots & \\ j & e_2 & \longrightarrow e_4 & \xrightarrow{\qquad\qquad} & e_7 & \longrightarrow e_8 & \longrightarrow \cdots & \\ k & e_3 & \longrightarrow e_4 & \longrightarrow e_6 & \longrightarrow e_7 & \longrightarrow e_9 & \longrightarrow \cdots & \end{array} \right.$$

$$\emptyset \;\text{——}\; \{e_1\} \;\text{——}\; \{e_1, e_4\} \;\text{——}\; \{e_1, e_4, e_5\}$$

Local configurations $\Xi_i$

# Models

$\mu = \langle \lambda, \alpha, \pi \rangle$

$$\lambda \quad \left\{ \begin{array}{ll} i & e_1 \longrightarrow e_4 \longrightarrow e_5 \longrightarrow e_8 \xrightarrow{\Downarrow} \cdots \\ j & e_2 \longrightarrow e_4 \longrightarrow e_7 \longrightarrow e_8 \longrightarrow \cdots \\ k & e_3 \longrightarrow e_4 \longrightarrow e_6 \longrightarrow e_7 \longrightarrow e_9 \longrightarrow \cdots \end{array} \right.$$

$$\emptyset \;\text{———}\; \{e_1\} \;\text{———}\; \{e_1, e_4\} \;\text{———}\; \{e_1, e_4, e_5\} \;\text{———}\; \{e_1, e_4, e_5, e_8\} \;\text{———}\; \cdots$$

Local configurations $\Xi_i$

# Models

$\mu = \langle \lambda, \alpha, \pi \rangle$

$$\lambda \quad \left\{ \begin{tikzcd}[column sep=small] i & e_1 \arrow[r] & e_4 \arrow[r] \arrow[d, dash, dotted] & e_5 \arrow[rr] & & e_8 \arrow[r] \arrow[d, dash, dotted] & \cdots \\ j & e_2 \arrow[r] & e_4 \arrow[rr] \arrow[d, dash, dotted] & & e_7 \arrow[r] \arrow[d, dash, dotted] & e_8 \arrow[r] & \cdots \\ k & e_3 \arrow[r] & e_4 \arrow[r] & e_6 \arrow[r] & e_7 \arrow[r] & e_9 \arrow[r] & \cdots \end{tikzcd} \right.$$

$\alpha = \{\alpha_i\}_{i \in Id}$, each $\alpha_i : Ev_i \longrightarrow Act_i$

$\pi = \{\pi_i\}_{i \in Id}$, each $\pi_i : \Xi_i \longrightarrow 2^{Prop_i}$

$$\pi_i(\emptyset) \xrightarrow{\alpha_i(e_1)} \pi_i(\{e_1\}) \xrightarrow{\alpha_i(e_4)} \pi_i(\{e_1, e_4\}) \xrightarrow{\alpha_i(e_5)} \pi_i(\{e_1, e_4, e_5\}) \xrightarrow{\alpha_i(e_8)} \cdots$$

# Satisfaction

The global satisfaction relation at a given global configuration $\xi$ of $\mu$ is:

- $\mu, \xi \Vdash @_i[\varphi]$ if $\mu, \xi|_i \Vdash_i \varphi$;
- $\mu, \xi \nVdash \bot$; and $\mu, \xi \Vdash \gamma \Rightarrow \delta$ if $\mu, \xi \nVdash \gamma$ or $\mu, \xi \Vdash \delta$, where

the local satisfaction relations at given local configurations are:

- $\mu, \xi_i \Vdash_i \mathit{act}$ if $\xi_i \neq \emptyset$ and $\alpha_i(\mathit{last}(\xi_i)) = \mathit{act}$;
- $\mu, \xi_i \Vdash_i p$ if $p \in \sigma_i(\xi_i)$;
- $\mu, \xi_i \nVdash_i \bot$; and $\mu, \xi_i \Vdash_i \varphi \Rightarrow \psi$ if $\mu, \xi_i \nVdash_i \varphi$ or $\mu, \xi_i \Vdash_i \psi$;
- $\mu, \xi_i \Vdash_i \varphi \mathsf{U} \psi$ if there exists $\xi_i'' \in \Xi_i$ with $\xi_i \subsetneq \xi_i''$ such that $\mu, \xi_i'' \Vdash_i \psi$, and $\mu, \xi_i' \Vdash_i \varphi$ for every $\xi_i' \in \Xi_i$ with $\xi_i \subsetneq \xi_i' \subsetneq \xi_i''$;
- $\mu, \xi_i \Vdash_i \varphi \mathsf{S} \psi$ if there exists $\xi_i'' \in \Xi_i$ with $\xi_i'' \subsetneq \xi_i$ such that $\mu, \xi_i'' \Vdash_i \psi$, and $\mu, \xi_i' \Vdash_i \varphi$ for every $\xi_i' \in \Xi_i$ with $\xi_i'' \subsetneq \xi_i' \subsetneq \xi_i$; and
- $\mu, \xi_i \Vdash_i @_j[\varphi]$ if $\xi_i \neq \emptyset$, $\mathit{last}(\xi_i) \in Ev_j$ and $\mu, (\mathit{last}(\xi_i) \downarrow)|_j \Vdash_j \varphi$.

As usual $\mu \Vdash \gamma$ if $\mu, \xi \Vdash \gamma$ for every global configuration $\xi$.

# A simple network model

$Princ$ set of principals
$Name = \{Name_A\}_{A \in Princ}$ pairwise disjoint sets of names
$Id = Princ \uplus \{Ch\}$

$Msg$ build by composition and encryption, from $Name$, $Nonce$ and $Key$

For $A \in Princ$
$Act_A$ : *send*$(M, B')$, *rec*$(M)$, *spy*$(M)$, and *nonce*$(N)$
$Prop_A$ : *knows*$(M)$

For the channel
$Act_{Ch}$ : *in*$(M, A')$, *out*$(M, A')$, and *leak*
$Prop_{Ch}$ : none

# Network axioms

## Knowledge axioms for principals

**(K1)** $@_A[\mathit{knows}(M_1; M_2) \Leftrightarrow (\mathit{knows}(M_1) \wedge \mathit{knows}(M_2))]$;

**(K2)** $@_A[(\mathit{knows}(M) \wedge \mathit{knows}(K)) \Rightarrow \mathit{knows}(\{M\}_K)]$;

**(K3)** $@_A[(\mathit{knows}(\{M\}_K) \wedge \mathit{knows}(K^{-1})) \Rightarrow \mathit{knows}(M)]$;

**(K4)** $@_A[\mathit{knows}(M) \Rightarrow \mathsf{G}_\circ\, \mathit{knows}(M)]$;

**(K5)** $@_A[\mathit{rec}(M) \Rightarrow \mathit{knows}(M)]$;

**(K6)** $@_A[\mathit{spy}(M) \Rightarrow \mathit{knows}(M)]$; and

**(K7)** $@_A[\mathit{nonce}(N) \Rightarrow \mathit{knows}(N)]$.

## Fresh nonce generation

**(N1)** $@_A[\mathit{nonce}(N) \Rightarrow \mathsf{Y} \neg\, \mathit{knows}(M_N)]$; and

**(N2)** $@_A[\mathit{nonce}(N)] \Rightarrow \bigwedge_{B \in Princ \setminus \{A\}} @_B[\neg\, \mathit{knows}(M_N)]$.

# Network axioms

## Behaviour and communication axioms for the channel

**(C1)** $@_{Ch}[\mathit{in}(M, A') \Rightarrow \bigvee_{B \in Princ} @_B[\mathit{send}(M, A')]]$;

**(C2)** $@_{Ch}[\mathit{out}(M, A') \Rightarrow \mathsf{P}\ \mathit{in}(M, A')]]$; and

**(C3)** $@_{Ch}[\mathit{out}(M, A') \Rightarrow @_A[\mathit{rec}(M)]]$.

## Behaviour and communication axioms for principals

**(P1)** $@_A[\mathit{send}(M, B') \Rightarrow \mathsf{Y}(\mathit{knows}(M) \wedge \mathit{knows}(B'))]$;

**(P2)** $@_A[\mathit{send}(M, B') \Rightarrow @_{Ch}[\mathit{in}(M, B')]]$;

**(P3)** $@_A[\mathit{rec}(M) \Rightarrow @_{Ch}[\bigvee_{A' \in Name_A} \mathit{out}(M, A')]]$;

**(P4)** $@_A[\mathit{spy}(M) \Rightarrow @_{Ch}[leak \wedge \mathsf{P} \bigvee_{B' \in Name} \mathit{in}(M, B')]]$;

**(P5)** $@_A[\bigwedge_{B \in Princ \setminus \{A\}} \neg @_B[\top]]$; and

**(P6)** $@_A[\mathit{nonce}(N) \Rightarrow \neg\, @_{Ch}[\top]]$.

# Protocol modeling

Protocols described as a series of steps of the form

$$(\mathrm{step}_q) \quad x_s \to x_r \;:\; (n_{q_1}, \ldots, n_{q_t}).\ M$$

Hon - honest principals follow the rules of the protocol and use only one name
Intr - dishonest principals are potential "intruders"

Given a protocol with $j$ distinct roles, and an instantiation with names $A'_1, \ldots, A'_j$ of principals $A_1, \ldots, A_j$

$$\mathrm{step}_q^i = \begin{cases} \langle \mathit{nonce}(N_{q_1}) \ldots \mathit{nonce}(N_{q_t}).\mathit{send}(M, A'_r)\rangle & \text{if } i = s \\ \langle \mathit{rec}(M)\rangle & \text{if } i = r \\ \langle\rangle & \text{otherwise} \end{cases}$$

Each $\mathrm{run}_A^i = \langle \mathit{act}_1 \ldots \mathit{act}_n \rangle$ is characterized by

$$\mathrm{role}_A^i = \mathit{act}_n \wedge \mathsf{P}(\mathit{act}_{n-1} \wedge \mathsf{P}(\ldots \wedge \mathsf{P}\, \mathit{act}_1) \ldots)\,.$$

# Security goals

$$\mathrm{secr}_S(A_1,\ldots,A_j)$$

secrecy goal for $S$ among honest participants $A_1,\ldots,A_j$

$$\bigwedge_{i=1}^{j} @_{A_i}[\mathsf{P}_\circ\ \mathrm{role}^i_{A_i}] \Rightarrow \bigwedge_{B\in Princ\setminus\{A_1,\ldots,A_j\}} \ \bigwedge_{M\in S} @_B[\neg\ \textit{knows}(M)]$$

---

$$\mathrm{auth}^{i,j,q}_{A,B}$$

authentication goal for honest $A$ in role $i$ wrt some $B$ in role $j$

$$@_A[\mathrm{role}^i_A] \Rightarrow @_B[\mathsf{P}_\circ\ \textit{send}(M,A)],\ \text{if } B \text{ is honest}$$

$$@_A[\mathrm{role}^i_A] \Rightarrow \bigvee_{C\in Intr} @_C[\mathsf{P}_\circ\ \textit{send}(M,A)],\ \text{if } B \text{ is dishonest}$$

assuming that $\mathrm{step}_q$ requires $x_j$ to send message $M$ to $x_i$

# Metareasoning: secret data lemma

Given $S \subseteq Msg$, $Msg_S$ are the $S$-secure messages, that is, messages where items from $S$ can only appear under the scope of an encryption with a key whose inverse is also in $S$

## Protocol independent secret data lemma

$G \subseteq Princ$, $\mu$ network model such that

$\mu \Vdash \bigwedge_{A \in G} @_A[\neg\, \mathit{send}(M, C')]$ for every $M \notin Msg_S$ and every name $C'$, and

$\mu \Vdash \bigvee_{A \in G} @_A[* \Rightarrow \mathsf{F}\, \mathit{nonce}(N)]$ for every nonce $N \in S$.

If it is the case that

- $\mu, \xi \Vdash \bigwedge_{B \in Princ \setminus G} @_B[\neg\, \mathit{knows}(M)]$ for every $M \notin Msg_S$,

then also

- $\mu, \xi \Vdash \bigwedge_{B \in Princ \setminus G} @_B[\mathsf{G}_\circ\, \neg\, \mathit{knows}(M)]$ for every $M \notin Msg_S$.

# Metareasoning: secrecy lemma

$$\mathrm{secr}_F = \bigwedge_{i=1}^{j} @_{A_i}[\mathsf{P}_\circ\ \mathrm{role}^i_{A_i}] \Rightarrow \bigwedge_{B \in Princ \setminus \{A_1,\ldots,A_j\}} \bigwedge_{M \in F} @_B[\neg\, \textsf{\textit{knows}}(M)].$$

## Secrecy lemma

A protocol guarantees $\mathrm{secr}_F$ for a protocol instantiation with honest participants $A_1, \ldots, A_j$, provided that all the messages ever sent by $A_1, \ldots, A_j$ in any protocol run are $(\{K^{-1}_{A_1}, \ldots, K^{-1}_{A_j}\} \cup F)$-secure.

# Metareasoning: secrecy lemma

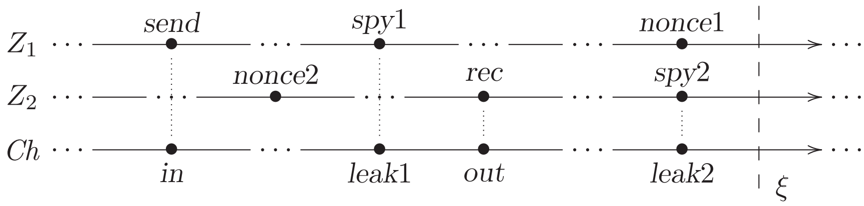
$$\mathrm{secr}_F = \bigwedge_{i=1}^{j} @_{A_i}[\mathsf{P}_\circ\ \mathrm{role}^i_{A_i}] \Rightarrow \bigwedge_{B \in Princ \setminus \{A_1,\ldots,A_j\}} \bigwedge_{M \in F} @_B[\neg\, \mathit{knows}(M)].$$

## Secrecy lemma

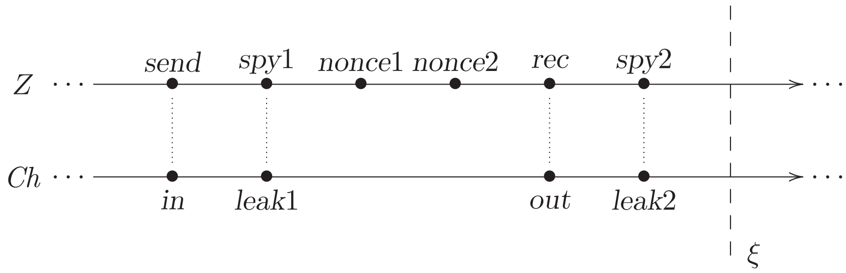
A protocol guarantees $\mathrm{secr}_F$ for a protocol instantiation with honest participants $A_1, \ldots, A_j$, provided that all the messages ever sent by $A_1, \ldots, A_j$ in any protocol run are $(\{K^{-1}_{A_1}, \ldots, K^{-1}_{A_j}\} \cup F)$-secure.

J.Millen, H.Ruess - Protocol independent secrecy, 2000
Discreeteness
Avoiding artificial notions like spells

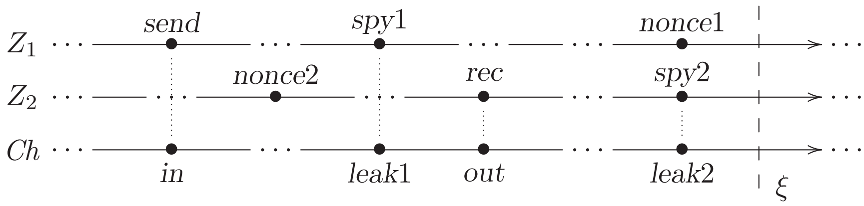
# Metareasoning: one intruder is enough



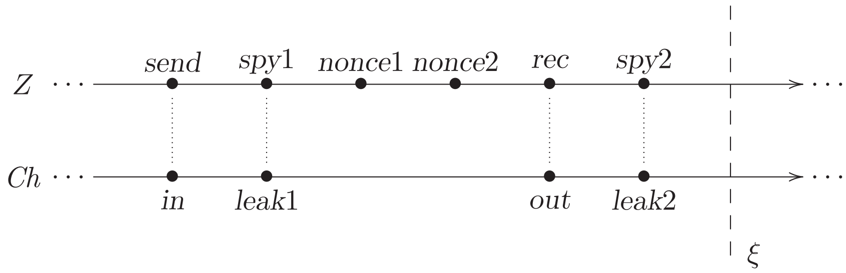

can be reduced to



# Metareasoning: one intruder is enough




can be reduced to

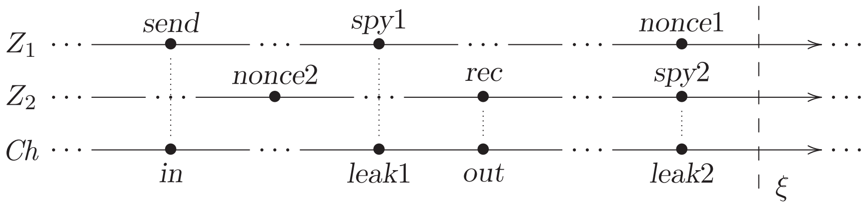



$\mu, \xi \Vdash @_A[\varphi]$ iff $\mu', \xi \Vdash @_A[\varphi]$ for $A \in Hon$, $\varphi \in \mathcal{L}_A$ without @

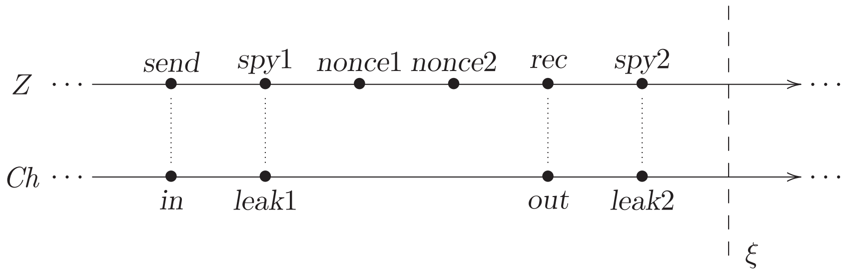
$\mu, \xi \Vdash \bigvee_{A \in Intr} @_A[\mathsf{P}_\circ\ act]$ iff $\mu', \xi \Vdash @_Z[\mathsf{P}_\circ\ act]$

if $\mu, \xi \Vdash \bigvee_{A \in In} @_A[\mathit{knows}(M)]$ then $\mu', \xi \Vdash @_Z[\mathit{knows}(M)]$

# Metareasoning: one intruder is enough




can be reduced to




H. Comon-Lundh, V.Cortier - Security properties: two agents are sufficient, 2003

Intruders part of the model

# Metareasoning: the predatory intruder

- $Z$ spies every message sent by an honest principal immediately after it arrives to the channel, and that is all the spying he does

$$@_{Ch}[@_Z[\mathit{spy}(M)] \Leftrightarrow \mathsf{Y} \bigvee_{A \in Hon} @_A[\bigvee_{B' \in Name} send(M, B')]]$$

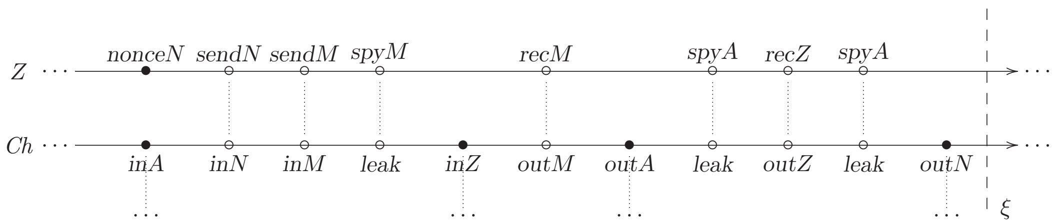
- $Z$ never bothers receiving messages (he has already spied them)

$$@_Z[\neg\, \mathit{rec}(M)]$$

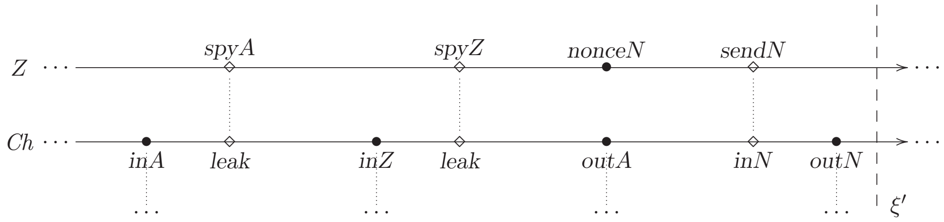
- $Z$ only sends messages to honest principals, and just immediately before the honest principal gets them

$$@_Z[\neg\, \mathit{send}(M, Z')] \quad \text{and} \quad @_Z[\mathit{send}(M, A) \Rightarrow @_{Ch}[\mathsf{X}\ @_A[\mathit{rec}(M)]]]$$

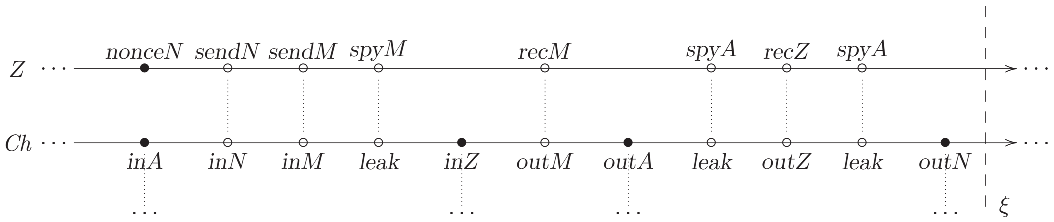
# Metareasoning: the predatory intruder



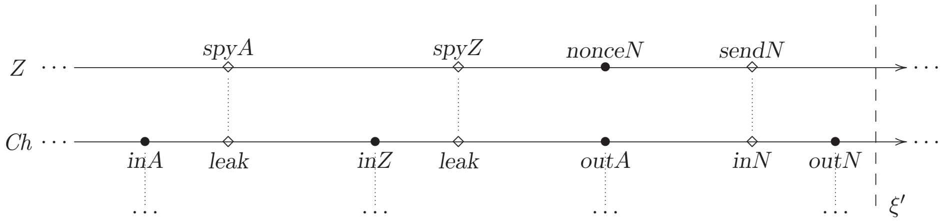

can be reduced to



# Metareasoning: the predatory intruder




can be reduced to




Towards justifiying the linearization of distributed communication in trace models

Corollary: the intruder only needs to send messages according to the protocol

## Conclusion and further work

- **Distributed temporal logic as a tool for security protocol model analysis**
- **A few of its potentialities**
- **Further work**
  - **Other widely used reductions: bounds on the number of honest principals, step compression**
  - **Nicer conditions for secrecy, and its relationship to authentication**
  - **New meaningful partial order reductions**
  - **Protocol compositionality**

# Conclusion and further work

- Distributed temporal logic as a tool for security protocol model analysis
- A few of its potentialities
- Further work
  - Other widely used reductions: bounds on the number of honest principals, step compression
  - Nicer conditions for secrecy, and its relationship to authentication
  - New meaningful partial order reductions
  - Protocol compositionality

**Thank you!**