Interpreting Strands and Multiset Rewriting in Linear Logic

Nancy Durgin

Iliano Cervesato, Max Kanovich, Andre Scedrov

Overview

- Motivations
- MSR $\rightarrow$ LL
- Strands $\rightarrow$ LL
- Comparison

Representing Security Protocols

Strand Spaces $\Leftrightarrow$ Multiset Rewriting (with existentials)

[Guttman et al.] [*CSFW '99*]

- Bisimulation for Reachability (= Basic Secrecy) [*CSFW '00*]
- But parameters and nonces treated differently!
- Are these differences important for other security properties?

Investigate using Linear Logic!

- Refinement of traditional logic
  - Natural accounting of states & resources
- Known connection to Multiset Rewriting (MSR)
  - extension with:
    - first-order parameters
    - existentials
- Express Strands in Linear Logic
  - Build on Dynamic Strands model

Comparing Strands to MSR

$$\begin{tikzcd}[column sep=huge, row sep=huge]
\text{MSR} \arrow[rr, leftrightarrow, "\text{bisimulation}", "\text{(CSFW 00)}"'] \arrow[d, leftrightarrow] & & \text{Strands} \arrow[d, leftrightarrow] \\
\text{Linear logic} \arrow[rr, leftrightarrow, dashed, "?"] & & \text{Linear logic}
\end{tikzcd}$$

Running Example

Needham-Schroeder Protocol

$$A \rightarrow B: \{N_A, A\}_{KB}$$

$$B \rightarrow A: \{N_A, N_B\}_{KA}$$

$$A \rightarrow B: \{N_B\}_{KB}$$

MSR Protocol Notation

- Non-deterministic *infinite*-state systems
- Facts

$$F ::= P(t_1, \ldots, t_n)$$
$$t ::= x \mid c \mid f(t_1, \ldots, t_n)$$

- States $\{ F_1, \ldots, F_n \}$
  - Multiset of facts
    - Includes network messages, private state
    - Intruder will see messages, not private state
    - ***Multi***set allows duplicated messages, states

State Transitions in MSR

- Transition rule
  - $F_1, \ldots, F_k \longrightarrow \exists x_1 \ldots \exists x_m.\ G_1, \ldots, G_n$
- What this means
  - If $F_1, \ldots, F_k$ in state σ, then a next state σ' has
    - Facts $F_1, \ldots, F_k$ removed
    - $G_1, \ldots, G_n$ added, with $x_1 \ldots x_m$ replaced by new symbols
    - Other facts in state σ carry over to σ'
  - Free variables in rule universally quantified

MSR predicates

- N(m) Network messages
- I(m) Intruder info.
- $A_i(t_1,\ldots,t_{ni})$ Role states
- *Pr*, *PrvK*, *PubK*, … Persistent info.

NS: MSR rules for *Alice*

$$\pi_{A0}(A) \rightarrow A_0(A), \pi_{A0}(A)$$

$$A_0(A), \pi_{A1}(B) \rightarrow \exists N_A.\ A_1(A,B,N_A), N(\{N_A,A\}_{KB}), \pi_{A1}(B)$$

$$A_1(A,B, N_A), N(\{N_A,N_B\}_{KA}) \rightarrow A_2(A,B,N_A,N_B)$$

$$A_2(A,B,N_A,N_B) \rightarrow A_3(A,B,N_A,N_B), N(\{N_B\}_{KB})$$

where $\pi_{A0}(A) = Pr(A), PrvK(A,K_A^{-1})$

$\pi_{A1}(B) = Pr(B), PubK(B,K_B)$

Linear Logic Basics

- Fragment of Linear Logic
  - "resource management"
- Multiplicative Conjunction (tensor): $X \otimes Y$
  - Resources X and Y are both available
- Linear Implication: $X \multimap Y$
  - Consume X and replace it with Y
- $\exists$ and $\forall$

From MSR to LL

$$F_1, \ldots, F_k \longrightarrow \exists x_1 \ldots \exists x_m.\ \ G_1, \ldots , G_n$$

$$, \quad \dashrightarrow \quad \otimes$$

$$\longrightarrow \quad \dashrightarrow \quad \multimap$$

$$\exists \quad \dashrightarrow \quad \exists$$

$$\forall \underline{y}.(F_1 \otimes \ldots \otimes F_k \multimap \exists x_1 \ldots \exists x_m (G_1 \otimes \ldots \otimes G_n))$$

Sound and Complete

NS: Linear Logic rules for *Alice*

$$\pi_{A0}(A) \multimap A_0(A) \otimes \pi_{A0}(A)$$

$$A_0(A) \otimes \pi_{A1}(B) \multimap$$
$$\exists N_A.\ A_1(A,B,N_A) \otimes N(\{N_A,A\}_{KB}) \otimes \pi_{A1}(B)$$

$$A_1(A,B,\ N_A) \otimes N(\{N_A,N_B\}_{KA}) \multimap A_2(A,B,N_A,N_B)$$

$$A_2(A,B,N_A,N_B) \multimap A_3(A,B,N_A,N_B) \otimes N(\{N_B\}_{KB})$$

where $\pi_{A0}(A) = Pr(A),\ PrvK(A,K_A^{-1})$

$\pi_{A1}(B) = Pr(B),\ PubK(B,K_B)$

Strands [*Guttman et al.*]

- Graphical representation
  - causal interactions
- Designed for after-the-fact analysis
- Events
  - message sent, message received
- Strands
  - finite sequences of events

  $s_1 \Rightarrow s_2 \Rightarrow \ldots \Rightarrow s_k$, each s_j an event

NS: A Bundle

$$
\begin{tikzcd}
\{N_A, A\}_{KB} \arrow[r] \arrow[d, Rightarrow] & \{N_A, A\}_{KB} \arrow[d, Rightarrow] \\
\{N_A, N_B\}_{KA} \arrow[d, Rightarrow] & \{N_A, N_B\}_{KA} \arrow[l] \\
\{N_B\}_{KB} \arrow[r] & {}
\end{tikzcd}
$$

Dynamic Strands [*CSFW '00*]

- Support executable specifications
- Specification language
  - Decorated strands
- Execution capabilities
  - Configurations
  - Transitions

Parametric strands

- Strands are <u>instances</u> of *roles*
- Parameters: instantiable information
- Constraints:
  - Fresh variables (Nonces)
  - Persistent info.

NS: Parametric Strand for *Alice*

Alice (A, B, N_A, N_B) :

$\boxed{N_A \text{ Fresh}, \pi_A(A,B)}$

$\{N_A, A\}_{KB} \longrightarrow$

$\Downarrow$

$\{N_A, N_B\}_{KA} \longleftarrow$

$\Downarrow$

$\{N_B\}_{KB} \longrightarrow$

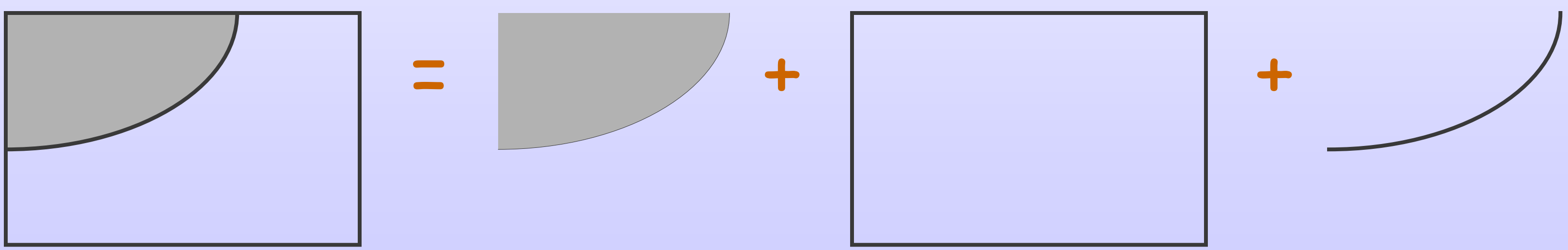
where

$\pi(A,B) = \ Pr(A), PrvK(A, K_A^{-1}),$
$\qquad\qquad\ Pr(B), PubK(B, K_B)$

Configurations

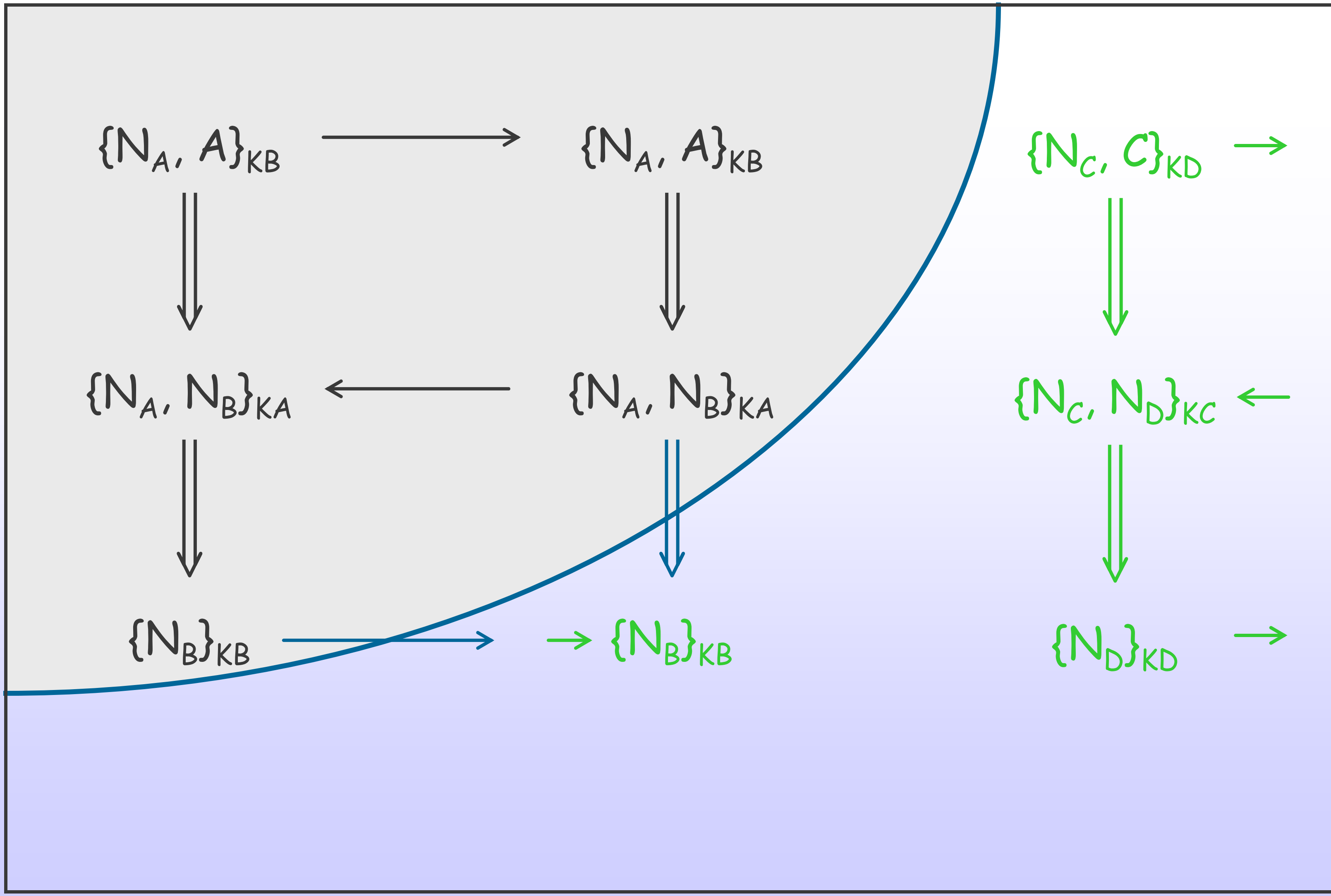
? Capture possible next actions

- Extension : bundle + remaining actions
- Configuration : bundle + extension
- Fringe : crossing arrows

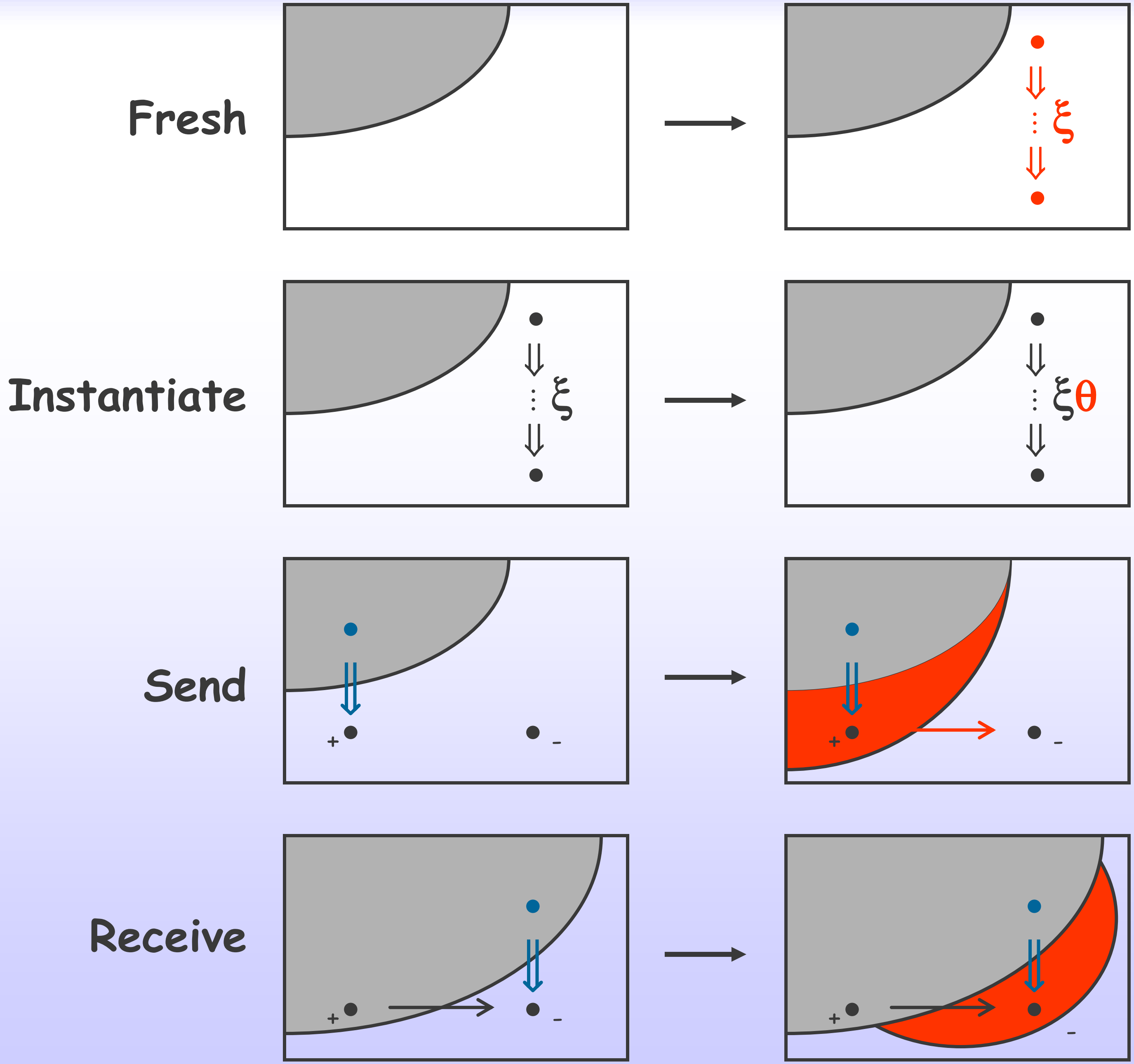


Configuration = bundle + extension + fringe

NS: Configuration



Strand Transitions



Decorated Strands

- Add initial ($\top$) and final node ($\perp$)
- Add labels $Q(q_i)$ to $\Rightarrow$ arrows
- Add label stop to last $\Rightarrow$ arrow

NS: Decorated Strand for *Alice*

Alice (A, B, N_A, N_B) :

$\boxed{N_A \text{ Fresh}, \pi_A(A,B)}$

$$
\begin{array}{cl}
\top & \\
\Downarrow Q(q_0) & \\
\{N_A, A\}_{KB} & \longrightarrow \\
\Downarrow Q(q_1) & \\
\{N_A, N_B\}_{KA} & \longleftarrow \\
\Downarrow Q(q_2) & \\
\{N_B\}_{KB} & \longrightarrow \\
\Downarrow \text{stop} & \\
\bot &
\end{array}
$$

where

$\pi(A,B) =$ $Pr(A)$, $PrvK(A, K_A^{-1})$,
$Pr(B)$, $PubK(B, K_B)$

From Strands to LL

- Encoding of variables
  - Labels (q_i) --> ∃
  - Fresh variables --> ∃
  - Instantiated variables --> ∀
- Encoding of nodes (see paper)

NS: *Alice* role in Linear Logic

$$\exists q_0,q_1,q_2.\exists n_A.\forall k_A,k_A^{-1},k_B,n_B.$$

$$\pi_A(k_A,k_A^{-1},k_B) \multimap \pi_A(k_A,k_A^{-1},k_B) \otimes Q(q_0) \quad \otimes\ ($$

$$Q(q_0) \multimap N(\{k_A,n_A\}_{k_B}) \otimes Q(q_1) \quad \otimes\ ($$

$$Q(q_1) \otimes N(\{n_A,n_B\}_{k_A}) \multimap Q(q_2) \quad \otimes\ ($$

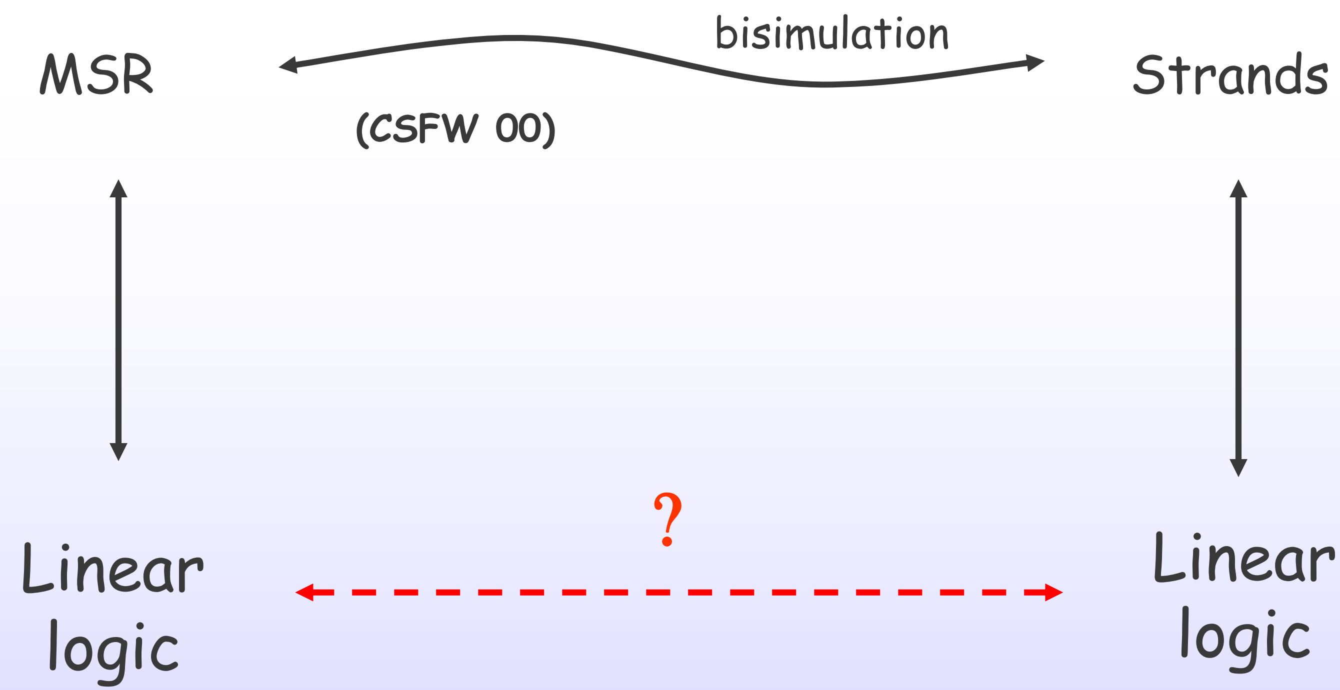
$$Q(q_2) \multimap N(\{n_A\}_{k_B}) \quad \otimes\ stop)))$$

Sound and Complete

MSR and Strands in Linear Logic

- MSR in linear logic
  - $\forall \underline{z}.\ A_i(\ldots) \multimap \exists \underline{y}.\ N_i(\ldots) \otimes A_{i+1}(\ldots)$
- Strands in linear logic
  - $\exists \underline{q}\ \exists \underline{y}\ \forall \underline{z}.\ N_0(\ldots) \multimap N_1(\ldots) \otimes Q(q_1) \quad \otimes\ ($
    $Q(q_1) \multimap N_2(\ldots) \otimes Q(q_2) \quad \otimes\ ($
    $Q(q_2) \multimap \ldots \quad))\ldots)$
- Not logically equivalent!

Conclusions



- Approximate bisimulation
  - Agreement on the secrecy property
- Non-equivalent interpretations in LL
  - Differences on other security properties?

Future Work

- Other security properties?
  - Not reducible to reachability
- Other LL representations
  - Proof-nets
- Use of LL to study other formalisms
  - Spi-calculus