ProNoBis
Probability and Nondeterminism, Bisimulations and Security

Journée des ARCS — 01 octobre 2007
Outline

1 Introduction.
   - Non-Deterministic Choice Only
   - Probabilistic Choice Only
   - Both
   - Cryptographic Protocols

2 Results
   - Infinite (topological) state spaces
   - A Probabilistic Applied $\pi$-Calculus
   - Anonymity

3 Conclusion
Consortium

**Teams:**
- INRIA Futurs
- ENS Cachan
- EPITA
- Queen Mary U., London
- U. Paris VII Denis Diderot
- U. di Verona
- U. of Birmingham
- projet SECSI
- projet Comete
- LSV
- LRDE
- Dept. of Comp. Science
- Equipe de logique
- PPS
- Dip. di Informatica
- School of Comp. Science

Non-Deterministic Choice Only

Outline

1. Introduction.
   - Non-Deterministic Choice Only
   - Probabilistic Choice Only
   - Both
   - Cryptographic Protocols

2. Results
   - Infinite (topological) state spaces
   - A Probabilistic Applied π-Calculus
   - Anonymity

3. Conclusion
Non-Deterministic Choice: Semantics

Non-deterministic choice

Start → Flip_1 → Flip_2 → Halt

Bad
Non-Deterministic Choice: Semantics

Non-deterministic choice

Start

Flip₁

Flip₂

Halt

Bad

Non-deterministic choice
Non-Deterministic Choice: Semantics
Non-Deterministic Choice: Semantics

Non-deterministic choice

Bad

Flip_1

Flip_2

Start

Halt

Non-deterministic choice
Non-Deterministic Choice: Semantics

Non-deterministic choice

Start

Flip₁

Flip₂

Bad

Halt

Non-deterministic choice
Outline

1. Introduction.
   - Non-Deterministic Choice Only
   - Probabilistic Choice Only
   - Both
   - Cryptographic Protocols

2. Results
   - Infinite (topological) state spaces
   - A Probabilistic Applied $\pi$-Calculus
   - Anonymity

3. Conclusion
A (Finite) Markov Chain

Probabilistic choice
Probabilistic Choice Only

Start

Probabilistic choice
Probabilistic Choice Only

Flip a Coin

Start

Flip 1

Flip 2

Biased

Good

Halt

Probabilistic choice
Probabilistic Choice Only

Advance

Probabilistic choice

Probability: 0.5
Probabilistic Choice Only

Flip a Coin

Probabilistic choice
Introduction.

Probabilistic Choice Only

Advance

Probabilistic choice

Probability: 0.5x0.5 = 0.25
Probabilistic choice

Advance

Probability: 0.25 x 0.3 = 0.075
Outline

1. Introduction.
   - Non-Deterministic Choice Only
   - Probabilistic Choice Only
   - Both
   - Cryptographic Protocols

2. Results
   - Infinite (topological) state spaces
   - A Probabilistic Applied $\pi$-Calculus
   - Anonymity

3. Conclusion
A Stochastic Game (Demonic Case)

Both

Non-deterministic (demonic) choice (by adversary)

Probabilistic choice (by program)
Both

Start

Non-deterministic (demonic) choice (by adversary)

Probabilistic choice (by program)
C’s Turn: Malevolently Chooses Biased Side

- Non-deterministic (demonic) choice (by adversary)
- Probabilistic choice (by program)

Diagram showing a decision tree with probabilities for biased and good outcomes, starting from Flip1 and Flip2, leading to Halt or Good.
P’s Turn: Flipping a Coin

Both

Non-deterministic (demonic) choice (by adversary)

Probabilistic choice (by program)
P’s Turn: Advancing

Non-deterministic (demonic) choice (by adversary)

Probabilistic choice (by program)
C’s Turn: Picking Most Biased Side

Non-deterministic (demonic) choice (by adversary)

Probabilistic choice (by program)
P’s Turn

Non-deterministic (demonic) choice (by adversary)

Probabilistic choice (by program)
Introduction

1. Introduction.
   - Non-Deterministic Choice Only
   - Probabilistic Choice Only
   - Both
   - Cryptographic Protocols

2. Results
   - Infinite (topological) state spaces
   - A Probabilistic Applied $\pi$-Calculus
   - Anonymity

3. Conclusion
Anonymity

**Goal:** C should not be able to link agent to her actions.

≠ secret!

**Applications:**

- **e-voting:** voter identities are public, candidate names are public. . . but C should not be able to tell who voted for whom.
- Secret sharing, file sharing (Freenet), auctions, etc.
Cryptographic Protocols

Anonymization

Implementations: Crowds ([ReiterRubin98], sender anonymity), Onion Routing ([SyversonGoldschlagReed97], communication anonymity), Freenet ([Clarke et al.01], anonymous data storage/retrieval).

Our focus: verifying anonymity properties.

Previous models are either:

- purely non-deterministic (CSP [SchneiderSidiropoulos96],
  epistemic logic [SyversonStubblebine99], views
  [HughesShmatikov04]);
- or purely probabilistic (epistemic logic [HalpernONEill04])

... to the exception of [CanettiCheungKaynarLiskovLynchPereiraSegala’06],
where non-determinism is heavily constrained ("task-structured").
Cryptographic Protocols

Our Canonical Example: Chaum’s Dining Cryptographers [1988]

**Problem:**
- $N \geq 3$ cryptographers share a meal;
- The meal is paid either by the organization (master) or one of them. The master decides who pays.
- Each cryptographer is informed by the master whether he has to pay or not.

**Goal:**
- The cryptographers would like to decide whether one of them or the master paid.
- The master cannot be involved.
- If one of the cryptographers paid, he should remain anonymous.
Dining Cryptographers ($N = 3$)
Chaum’s Solution

- Cryptographers are organized in a ring;
- Two adjacent cryptographers share a coin, which they flip secretly;
- Each cryptographer $A$ examines the two coins he shares with his neighbors:
  - If $A$ is paying, $A$ announces “agree” if the two coins agree, “disagree” otherwise.
  - If $A$ is not paying, $A$ says the opposite.

**Fact**: One of the cryptographers is paying $\iff$ the number of “disagree” announced is odd.

(Think in $\mathbb{Z}/2\mathbb{Z}$.)
Modelling the Dining Cryptographers \((N = 3)\)
Cryptographic Protocols

Modeling Dining Cryptographers in the Probabilistic $\pi$-Calculus

\[ \text{Master} = \sum_{i=0}^{2} \tau \cdot m_i \cdot p \cdot m_{i1} \cdot m_{i2} \cdot 0 + \tau \cdot m_0 \cdot m_1 \cdot m_2 \cdot 0 \]

\[ \text{Crypt}_i = m_i(x) \cdot c_{i1}(y) \cdot c_{i1}(z) \cdot \]

if \( x = p \)

then \( \text{pay}_i \) if \( y = z \)

then \( \text{out}_i \) disagree

else \( \text{out}_i \) agree

else if \( y = z \)

then \( \text{out}_i \) agree

else \( \text{out}_i \) disagree

\[ \text{Coin}_i = p_i \cdot \text{Head}_i + p_i \cdot \text{Tail}_i \]

\[ \text{Head}_i = c_{i1}(\text{head} \cdot c_{i1}(\text{head}) \cdot 0 \]

\[ \text{Tail}_i = c_{i1}(\text{tail} \cdot c_{i1}(\text{tail}) \cdot 0 \]

\[ \text{DCP} = (\nu m)(\text{Master} \]

Non-deterministic choice

Anonymous actions

Observables

Probabilistic choice
Chaum’s dining cryptographers is finite-state (“easy case”).

Hence the probabilistic $\pi$-calculus is enough here.

However we need models/process algebras for the case of infinitely many states (see next example).
1-Out-Of-2 Oblivious Transfer

Introduced in [Rabin81, EvenGoldreichLempel85]. Used in e-contract signing, in secure multi-party computation.

- S has two secrets $M_0$ and $M_1$ ($M_0 \neq M_1$);
- R will choose $i \in \{0, 1\}$: wishes to receive $M_i$ from S;

Constraints:
1-Out-Of-2 Oblivious Transfer

Introduced in [Rabin81, EvenGoldreichLempel85]. Used in e-contract signing, in secure multi-party computation.

- S has two secrets $M_0$ and $M_1$ ($M_0 \neq M_1$);
- R will choose $i \in \{0, 1\}$: wishes to receive $M_i$ from S;

**Constraints:**

- R should not receive the other message $M_{1-i}$;
- R should receive $M_i$ with probability $\geq 1/2$;
- S should not be able to tell which

(i.e., to tell the value of $i$)
Cryptographic Protocols

1-Out-Of-2 Oblivious Transfer

**Use:**
- An asymmetric encryption scheme \((\text{enc}(\_ , K), \text{dec}(\_ , K^{-1}))\);
  (e.g., the RSA scheme, with modulus \(N\).)
- Two operations \(\boxplus, \boxminus\) (e.g., \(x \boxplus y = x + y \mod N\).)

**Protocol:**
- **S → R:** fresh public key \(K\), and fresh tokens \(m_0, m_1\);
- **R → S:** \(\text{Req} \triangleq \text{enc}(\text{fresh} \, \ell, K) \boxplus m_i\);
  \((i \in \{0, 1\} \text{ chosen by R.})\)
- **S → R:** \(A_0 \triangleq M_0 \boxplus \text{dec}(\text{Req} \boxminus m_j, K^{-1})\),
  \(A_1 \triangleq M_1 \boxplus \text{dec}(\text{Req} \boxminus m_{1-j}, K^{-1})\),  \(j\);
  \((j \in \{0, 1\} \text{ flipped at random, uniformly.})\)
- **R emits** \(A_i \boxminus \ell\) if \(j = 0\), \(A_{1-i} \boxminus \ell\) if \(j = 1\).
  (Works as expected when \(j = i\).)
Outline

1 Introduction.
   - Non-Deterministic Choice Only
   - Probabilistic Choice Only
   - Both
   - Cryptographic Protocols

2 Results
   - Infinite (topological) state spaces
   - A Probabilistic Applied $\pi$-Calculus
   - Anonymity

3 Conclusion
Results (until now)

- Models for **non-determinism** + **probabilistic** choice in the case of **infinite** state spaces (topological spaces, cpos).
- New process calculi: **PAPi**.
- Modeling **anonymity**, and its many pitfalls.

**Bisimulations** are defined in each case which imply observational equivalence, hence security.
Infinite (topological) state spaces

Outline

1. Introduction.
   - Non-Deterministic Choice Only
   - Probabilistic Choice Only
   - Both
   - Cryptographic Protocols

2. Results
   - Infinite (topological) state spaces
   - A Probabilistic Applied $\pi$-Calculus
   - Anonymity

3. Conclusion
Relax the axioms defining probabilities:

Belief functions:

are strict, monotonic set functions \( \nu : \Omega(X) \to \mathbb{R}^+ \) satisfying a relaxed inclusion-exclusion principle:

\[
\nu \left( \bigcup_{i=1}^{n} U_i \right) \geq \sum_{l \subseteq \{1, \ldots, n\}, l \neq \emptyset} (-1)^{|l|+1} \nu \left( \bigcap_{i \in l} U_i \right)
\]
Relax the axioms defining probabilities:

\[ \nu \left( \bigcup_{i=1}^{n} U_i \right) \geq \sum_{I \subseteq \{1, \ldots, n\}, I \neq \emptyset} (-1)^{|I|+1} \nu \left( \bigcap_{i \in I} U_i \right) \]

Semantic models

A simple notion that allows one to give semantic models of both (demonic) non-determinism and probabilistic choice

- Applies to playful transition systems, where the “set of next states” function is replaced by a belief-function “distribution” of next states.
- Notion of strong (bi)simulation [ICALP’07], even for 2\(\frac{1}{2}\)-player games on topological spaces.
Previsions

- Belief functions only model one **probabilistic** step followed by one **non-deterministic** step;
- But... No transitivity (composition);
Belief functions only model one probabilistic step followed by one non-deterministic step;

But... No transitivity (composition);

Continuous previsions solve the problem [CSL’07]...
Previsions

- Belief functions only model one probabilistic step followed by one non-deterministic step;
- But... No transitivity (composition);
- **Continuous previsions** solve the problem [CSL’07]...
- and also give a sound and complete semantics for higher-order functional languages with non-deterministic and probabilistic choice.
In Continuation Passing Style, you evaluate a program $M$ in a continuation $h$:

- $h$ takes the value of $M$,
- proceeds along... 
- and eventually returns an answer.

Formally:

$$\llbracket \text{val } M \rrbracket \rho(h) = h(\llbracket M \rrbracket \rho)$$

$$\llbracket \text{let val } x = M \text{ in } N \rrbracket \rho(h) = \llbracket M \rrbracket \rho(\lambda v \cdot \llbracket N \rrbracket (\rho[x := v])(h))$$

$$\llbracket \text{case} \rrbracket \rho(b, v_0, v_1) = \begin{cases} v_0 & \text{if } b = \text{false} \\ v_1 & \text{if } b = \text{true} \end{cases}$$

(Er, in fact, our calculus is direct-style except for the monadic part, which is in CPS, as above.)
Infinite (topological) state spaces

Payoffs, in the Purely Probabilistic Case

Now imagine answers are money. ("utility" to economists).
Now imagine answers are money. ("utility" to economists). I.e., evaluating a term $M$ in continuation $h$ gives you some amount of money $⟦M⟧\rho(h)$.
Payoffs, in the Purely Probabilistic Case

Now imagine answers are money. (“utility” to economists).

I.e., evaluating a term $M$ in continuation $h$ gives you some amount of money $\llbracket M \rrbracket \rho(h)$.

Flipping a boolean value $b$ at random (uniformly) is:

- If $b = \text{false}$, then you get $h(\text{false})$ dollars;
- If $b = \text{true}$, then you get $h(\text{true})$ dollars.

The average payoff is

$$\frac{1}{2} h(\text{false}) + \frac{1}{2} h(\text{true})$$
Now imagine answers are money. ("utility" to economists). I.e., evaluating a term $M$ in continuation $h$ gives you some amount of money $\llbracket M \rrbracket \rho(h)$.

Flipping a boolean value $b$ at random (uniformly) is:

- If $b = \text{false}$, then you get $h(\text{false})$ dollars;
- If $b = \text{true}$, then you get $h(\text{true})$ dollars.

The average payoff is

$$\frac{1}{2} h(\text{false}) + \frac{1}{2} h(\text{true})$$

In other words, drawing at random = taking a mean = integrating.
In an environment $\rho$, with continuation $h : [\tau] \to \mathbb{R}^+$,

$$
[\text{val } M] \rho(h) = h([M] \rho) \\
[\text{let val } x = M \text{ in } N] \rho(h) = [M] \rho(\lambda v \cdot [N] (\rho[x := v])(h)) \\
[\text{case}] \rho(b, v_0, v_1) = \begin{cases} 
  v_0 & \text{if } b = \text{false} \\
  v_1 & \text{if } b = \text{true}
\end{cases}
$$
Infinite (topological) state spaces

A Continuation Semantics... With Choice(s)

In an environment $\rho$, with continuation $h : [\tau] \rightarrow \mathbb{R}^+$,

$$[\text{val } M] \rho(h) = h([M] \rho)$$

$$[\text{let val } x = M \text{ in } N] \rho(h) = [M] \rho(\lambda v \cdot [N] (\rho[x := v])(h))$$

$$[\text{case}] \rho(b, v_0, v_1) = \begin{cases} v_0 & \text{if } b = \text{false} \\ v_1 & \text{if } b = \text{true} \end{cases}$$

$$[\text{flip}: \text{Tbool}] \rho(h) = \frac{1}{2} h(\text{false}) + \frac{1}{2} h(\text{true}) \text{ (mean payoff)}$$
In an environment $\rho$, with continuation $h : \llbracket \tau \rrbracket \rightarrow \mathbb{R}^+$,

$$\llbracket \text{val } M \rrbracket \rho(h) = h(\llbracket M \rrbracket \rho)$$

$$\llbracket \text{let } \text{val } x = M \text{ in } N \rrbracket \rho(h) = \llbracket M \rrbracket \rho(\lambda v \cdot \llbracket N \rrbracket (\rho[x := v])(h))$$

$$\llbracket \text{case } \rho(b, v_0, v_1) = \begin{cases} v_0 & \text{if } b = \text{false} \\ v_1 & \text{if } b = \text{true} \end{cases}$$

$$\llbracket \text{flip} : T\text{bool} \rrbracket \rho(h) = \frac{1}{2} h(\text{false}) + \frac{1}{2} h(\text{true}) \text{ (mean payoff)}$$

$$\llbracket \text{amb} : T\text{bool} \rrbracket \rho(h) = \text{inf}(h(\text{false}), h(\text{true})) \text{ (min payoff)}$$

(This is for demonic non-det.; take sup for angelic non-determinism.)
Introduction.

Results

Conclusion

Infinite (topological) state spaces

A Continuation Semantics... With Choice(s)

In an environment $\rho$, with continuation $h : [\tau] \rightarrow \mathbb{R}^+$,

$$
[val \; M] \; \rho(h) = h([M] \; \rho)
$$

$$
[let \; val \; x = M \; in \; N] \; \rho(h) = [M] \; \rho(\lambda v \cdot [N] (\rho[x := v])(h))
$$

$$
[case] \; \rho(b, v_0, v_1) = \begin{cases} 
  v_0 & \text{if } b = \text{false} \\
  v_1 & \text{if } b = \text{true}
\end{cases}
$$

$$
[\text{flip} : \text{Tbool}] \; \rho(h) = \frac{1}{2} h(\text{false}) + \frac{1}{2} h(\text{true}) \ (\text{mean payoff})
$$

$$
[\text{amb} : \text{Tbool}] \; \rho(h) = \inf(h(\text{false}), h(\text{true})) \ (\text{min payoff})
$$

(This is for demonic non-det.; take sup for angelic non-determinism.)

Oh well, but then $[M] \; \rho$ is no longer linear as a functional... we characterize which properties they should have [CSL’07].
Outline

1. Introduction.
   - Non-Deterministic Choice Only
   - Probabilistic Choice Only
   - Both
   - Cryptographic Protocols

2. Results
   - Infinite (topological) state spaces
   - A Probabilistic Applied $\pi$-Calculus
   - Anonymity

3. Conclusion
A Probabilistic Applied $\pi$-Calculus

**PAPi: A Calculus for Cryptographic Systems**

- **Expressive power**
  - PAPi [ProNoBis07]
  - applied pi-calculus [AbadiFournet00]  
    - add equational theories (more versatility)
  - probabilistic pi-calculus [HerescuPalamidessi00]
  - spi-calculus [AbadiGordon97]  
    - add message passing, encryption.
  - pi-calculus [Milner]  
    - add probabilistic choice
  - CCS  
    - add mobility (channel passing)
PAPi: Syntax

Terms ($\equiv$ values $\cong$ messages):

\[ M, N ::= a, b, c, \ldots \mid x, y, z, \ldots \mid f(M_1, \ldots, M_l) \]

...interpreted modulo an equational theory $E$
PAPi: Syntax

Terms (\(\simeq\) values \(\simeq\) messages):

\[M, N ::= a, b, c, \ldots \mid x, y, z, \ldots \mid f(M_1, \ldots, M_l)\]

\[\ldots\text{interpreted modulo an equational theory } E\]

Processes (\(\simeq\) programs \(\simeq\) systems):

\[P, Q ::= 0 \mid u\langle M\rangle.P \mid u(x).P \mid P + Q \mid P \oplus_p Q \mid P | Q \mid !P \mid \nu n.P \mid \text{if } M = N \text{ then } P \text{ else } Q\]

Extended processes (\(\simeq\) programs-in-context):

\[A, B ::= P \mid \nu n.A \mid \nu x.A \mid A | B \mid \{M/x\}\]

**Note:** Active substitutions (\(\simeq\) adversarial knowledge \(\simeq\) contexts):

special case where \(P = 0\).
Use *schedulers* to resolve non-determinism.

**Weak bisimulation**

The largest symmetric relation $R$ s.t. $A R B$ implies:

1. $A \approx_E B$ (static equivalence);
2. $\forall$ scheduler $F \cdot \exists$ scheduler $F' \cdot \forall$ $R^*$-equivalence class $C$, $\text{Prob}_A^F(C) = \text{Prob}_B^{F'}(C)$;
3. $\forall$ scheduler $F \cdot \exists$ scheduler $F' \cdot \forall \alpha, C \cdot [\ldots] \Rightarrow \text{Prob}_A^F(\alpha, C) = \text{Prob}_B^{F'}(\tau^* \alpha \tau^*, C)$.

- Note: infinite state space (infinitely many terms, to start with).

However, we have not used previsions to this end (yet).
Define **contextual equivalence** \( \equiv \) for two closed extended processes \( A, B \), iff no adversary (context) can tell the difference between \( A \) and \( B \) by interacting with each.

**Theorem**

\[ A \equiv B \text{ iff there is a weak bisimulation } R \text{ such that } A R B. \]

**Application:**

1-out-of-2 Oblivious Transfer with \( R \) picking \( i \) at random \( \approx \)

“\( R \) gets \( M_0 \)” \( \oplus_{0.5} \) “\( R \) gets \( M_1 \).”

(Unfeasible to show directly. Build a weak bisimulation.)
Outline

1 Introduction.
   - Non-Deterministic Choice Only
   - Probabilistic Choice Only
   - Both
   - Cryptographic Protocols

2 Results
   - Infinite (topological) state spaces
   - A Probabilistic Applied $\pi$-Calculus
   - Anonymity

3 Conclusion
Let $S$ be a system (e.g., the prob. $\pi$-calculus implementation of Chaum’s dining cryptographers). An observer $I$ may deduce probabilistic information about the $S$ by interacting with it:

- not captured by any purely non-deterministic model;
- cannot (usually) apply methods from statistics:
  
  Repeating experiments is nonsense. . .
  
  since $I$ may keep track of past experiments and change behaviors (i.e., change distributions).
Early Definitions of Anonymity [ReiterRubin98]

A suspect $X$ is:

- **beyond suspicion**: to $I$, $X$ is not more likely of being the culprit than any other agent;
- **probable innocence**: $X$ is less likely of being the culprit than all the other agents;
- **possible innocence**: $I$ cannot be sure that $X$ is the culprit (purely non-deterministic, weakest notion).

(There are 4 configs when one cryptographer payed; assume the following 3 configurations are seen more often than the 4th, but the 4th still happens. This is a breach of anonymity that possible innocence does not detect.)
Anonymity through Evidence

Through **Evidence**, let:

\[
\text{Evidence}("i \text{ paid", obs}) = \frac{P(\text{obs|"i \text{ paid")}}{\sum_j P(\text{obs|"j \text{ paid")}}
\]

Then S is **strongly anonymous** iff for every observable obs, for every \(i, j\),

\[
\text{Evidence}("i \text{ paid", obs}) = \text{Evidence}("j \text{ paid", obs}
\]

Beautiful connection to **channel capacity** [TGC’06].
For any reasonable (fixed) scheduler, Chaum’s implementation is then strongly anonymous.
Anonymity

Nasty Schedulers

- For any reasonable (fixed) scheduler, Chaum’s implementation is then **strongly anonymous**.
- Note that fixing the scheduler means we are back in the purely **probabilistic** case.
For any reasonable (fixed) scheduler, Chaum’s implementation is then *strongly anonymous*.

Note that fixing the scheduler means we are back in the purely *probabilistic* case.

However, the probabilistic $\pi$-calculus implementation is *not* (even weakly) anonymous...
Anonymity

Nasty Schedulers

- For any reasonable (fixed) scheduler, Chaum’s implementation is then strongly anonymous.
- Note that fixing the scheduler means we are back in the purely probabilistic case.
- However, the probabilistic $\pi$-calculus implementation is not (even weakly) anonymous. . .
- **Problem**: among all schedulers, there is a (non-computable) scheduler that ⭐magically⭐ schedules the cryptographer who paid (if any) first. Then I simply observes who answered first.
Problem was folklore in the cryptographers’ world. 
(… And they always restrict to some hand-crafted, behind-the-scenes scheduler.)

Three different solutions published in 2007, from different groups [ProNoBiS, van Rossum et al., Mullins et al.].
Anonymity

Separating Nasty from Nice Schedulers

- Problem was folklore in the cryptographers’ world.
  (… And they always restrict to some hand-crafted, behind-the-scenes scheduler.)
- Three different solutions published in 2007, from different groups [ProNoBiS, van Rossum et al., Mullins et al.].
- Instrument processes with labeled non-deterministic choice, and make schedulers explicit:

\[
S ::= L.S \mid (L, L).S \mid \text{if } L \text{ then } S \text{ else } S \mid 0
\]

- Some choice labels are private (just like channel names) and model internal non-determinism, which schedulers cannot have control over [CONCUR’07].
  (Done for CCS + probabilities, not yet for PAPI.)
Outline

1 Introduction.
   - Non-Deterministic Choice Only
   - Probabilistic Choice Only
   - Both
   - Cryptographic Protocols

2 Results
   - Infinite (topological) state spaces
   - A Probabilistic Applied $\pi$-Calculus
   - Anonymity

3 Conclusion
Conclusion

www.lsv.ens-cachan.fr/~goubault/ProNobis/index.html

- **Publications:**
  - 7 intl. journals (incl. 5 TCS, 1 SIAM J. Computing);
  - 17 intl. confs (incl. 2 LICS, 2 CONCUR, 1 ICALP, 1 CSL, 1 FOSSACS, 2 CSF, 1 FCC).

- Some negative (unpublishable...) results too: our initial hope of relating theories of evidence to belief function semantics is doomed [HalpernFagin92].

- **More** questions now than we had at the beginning...
Future

- Applying previsions to questions of **numerical accuracy** in reactive programs (with CEA, Dassault Aviation, Hispano-Suiza, Supélec).
Future

- Applying previsions to questions of **numerical accuracy** in reactive programs (with CEA, Dassault Aviation, Hispano-Suiza, Supélec).
- Relating the (strategy-less) approach of previsions with random/deterministic **strategies** (ongoing work with R. Segala).
Future

- Applying previsions to questions of **numerical accuracy** in reactive programs (with CEA, Dassault Aviation, Hispano-Suiza, Supélec).
- Relating the (strategy-less) approach of previsions with random/deterministic strategies (ongoing work with R. Segala).
- (Hemi-)**distances** between probabilistic+non-deterministic systems, and bisimulations **up to some error**.
Future

- Applying previsions to questions of **numerical accuracy** in reactive programs (with CEA, Dassault Aviation, Hispano-Suiza, Supélec).
- Relating the (strategy-less) approach of previsions with random/deterministic strategies (ongoing work with R. Segala).
- (Hemi-)**distances** between probabilistic+non-deterministic systems, and bisimulations **up to some error**.
- Belief function semantics of **CCP** (concurrent constraint programming), and connection to Dolev-Yao-style adversaries.
  
  **Note**: parallel composition=Demps-Shafer combination rule!
Future

- Applying previsions to questions of **numerical accuracy** in reactive programs (with CEA, Dassault Aviation, Hispano-Suiza, Supélec).
- Relating the (strategy-less) approach of previsions with random/deterministic **strategies** (ongoing work with R. Segala).
- (Hemi-)**distances** between probabilistic+non-deterministic systems, and bisimulations up to some error.
- Belief function semantics of **CCP** (concurrent constraint programming), and connection to Dolev-Yao-style adversaries.
  - **Note**: parallel composition=Dempster-Shafer combination rule!
- **Model-checking** (done for probabilistic pi-calculus [QEST’07], a few ideas in [ICALP’07] for general topological case).