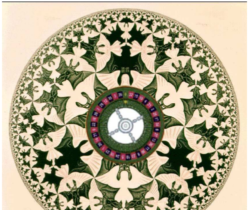
# ProNoBis

# Probability and Nodeterminism, 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:**

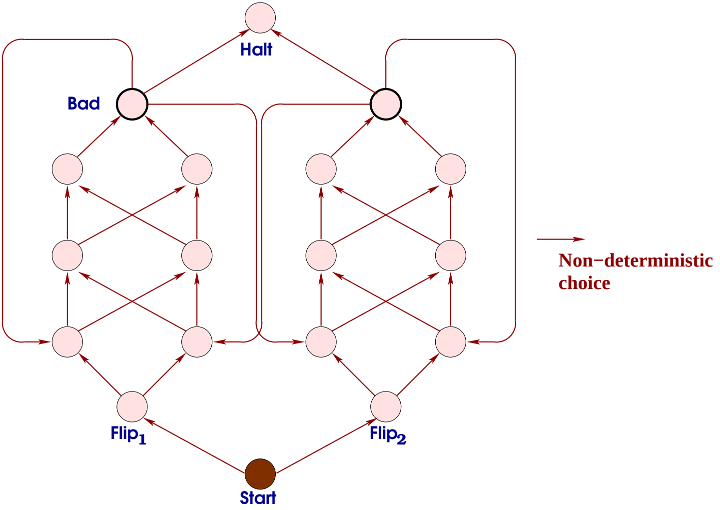
| | |
|---|---|
| **INRIA Futurs** | **projet SECSI**<br>**projet Comete** |
| **ENS Cachan** | **LSV** |
| **EPITA** | **LRDE** |
| **Queen Mary U., London** | **Dept. of Comp. Science** |
| **U. Paris VII Denis Diderot** | **Equipe de logique**<br>**PPS** |
| **U. di Verona** | **Dip. di Informatica**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

Postdoc: Angelo TROINA, shared between Comète and SECSI (01 sep. 2006–31 aug. 2007).

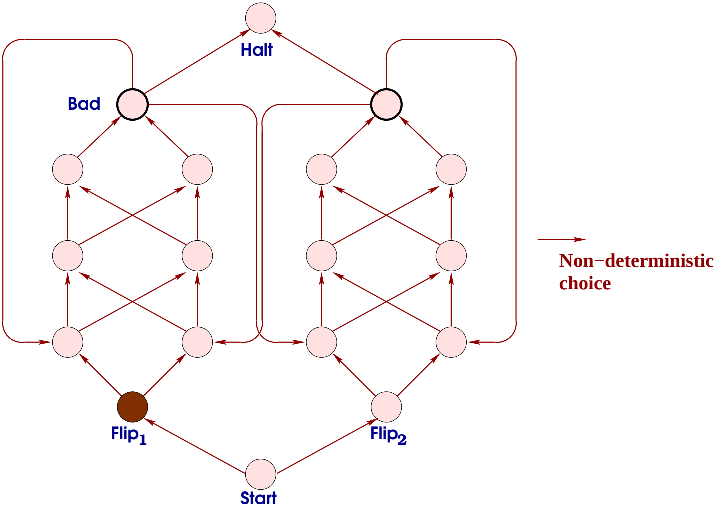
# Outline

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

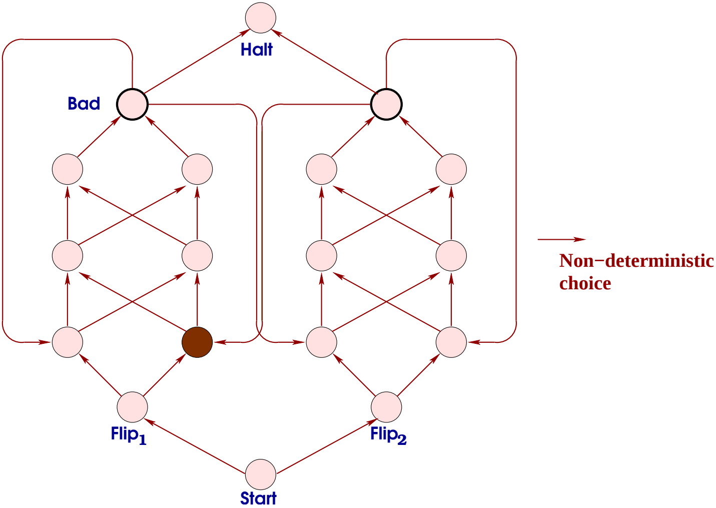
# Non-Deterministic Choice: Semantics



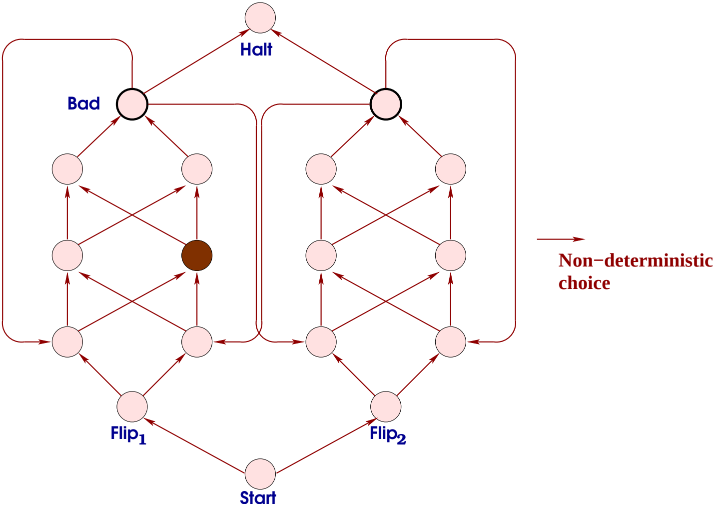
# Non-Deterministic Choice: Semantics



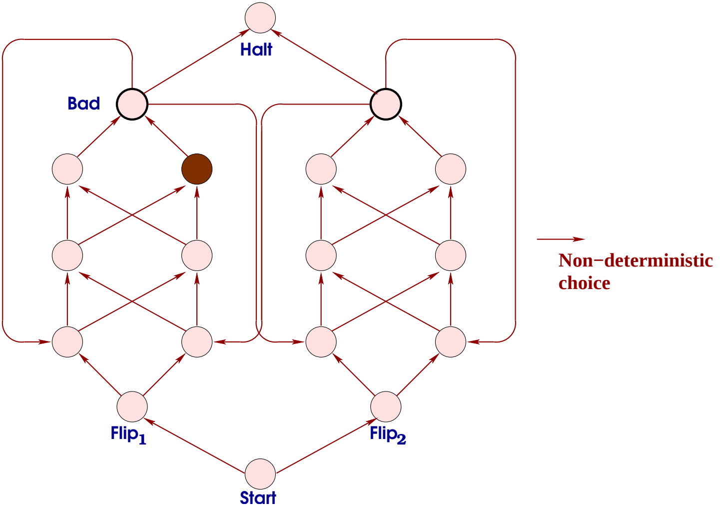
# Non-Deterministic Choice: Semantics



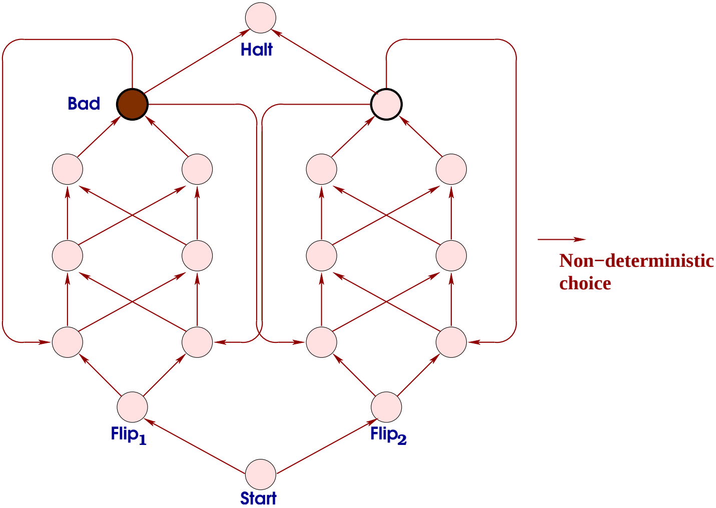
# Non-Deterministic Choice: Semantics



# Non-Deterministic Choice: Semantics



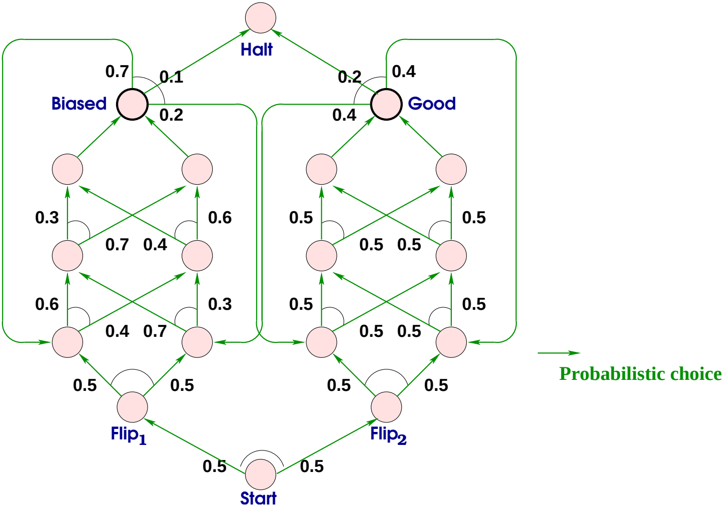
# Non-Deterministic Choice: Semantics



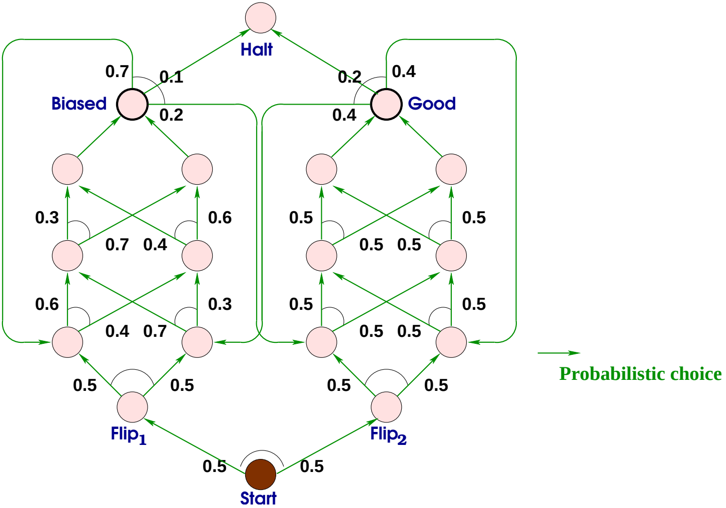
# Outline

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

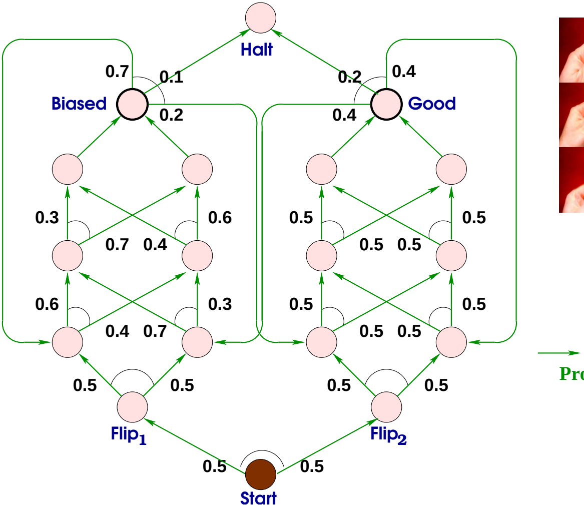
# A (Finite) Markov Chain



# Start

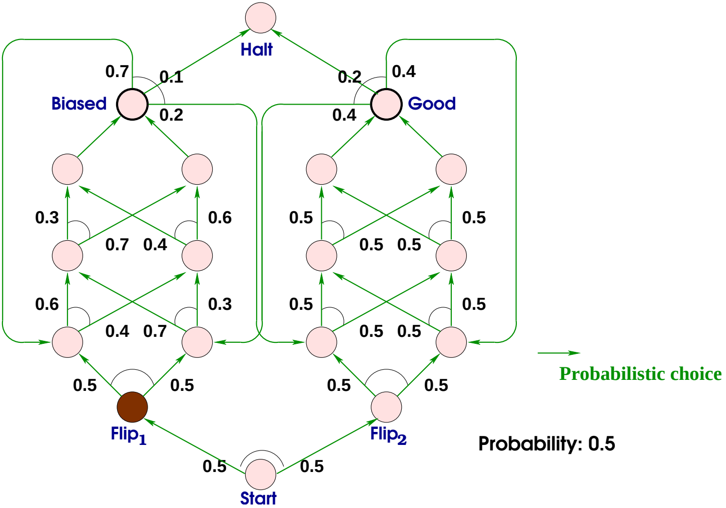

Halt
0.7
0.1
0.2
0.4
Biased
0.2
0.4
Good
0.3
0.6
0.7
0.4
0.6
0.3
0.4
0.7
0.5
0.5
0.5
0.5
0.5
0.5
0.5
0.5
0.5
0.5
0.5
0.5
0.5
0.5
0.5
0.5
$\text{Flip}_1$
$\text{Flip}_2$
0.5
0.5
Start
Probabilistic choice

# Flip a Coin



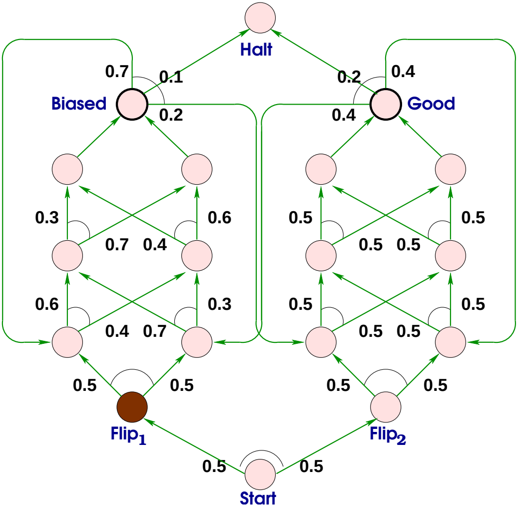

**Probabilistic choice**

# Advance



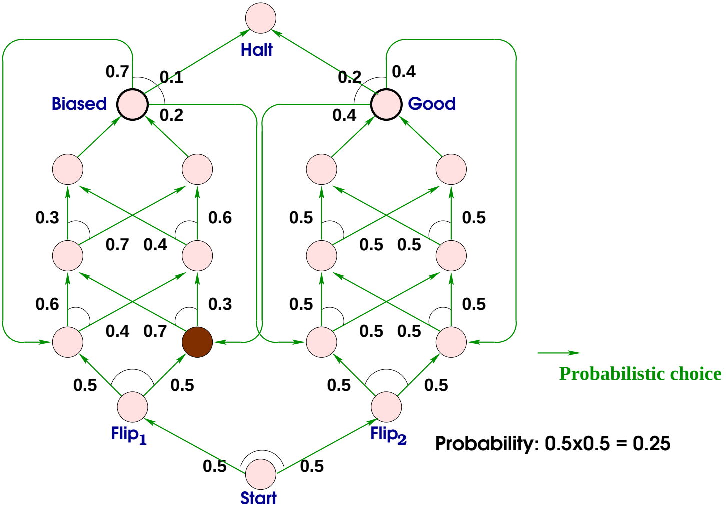

**Probability: 0.5**

# Flip a Coin



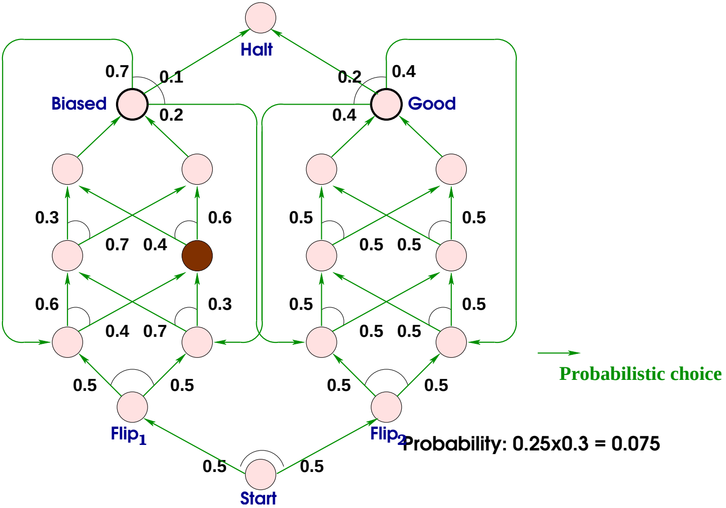

Probabilistic choice

# Advance




Probability: 0.5x0.5 = 0.25

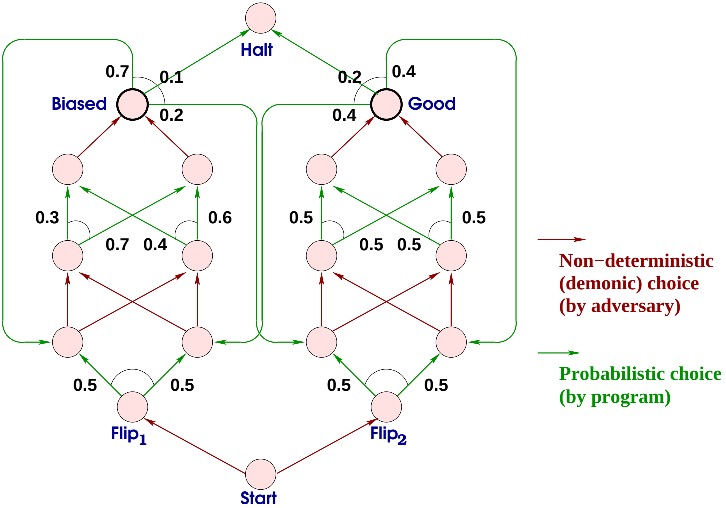
# Advance



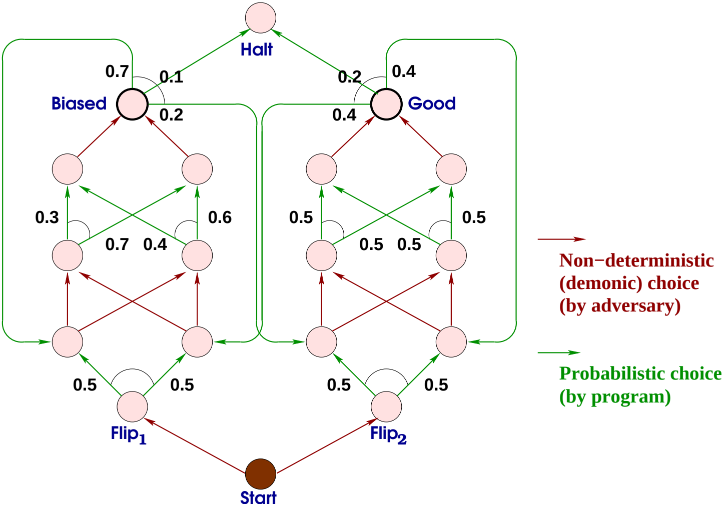

Probability: 0.25x0.3 = 0.075

# Outline

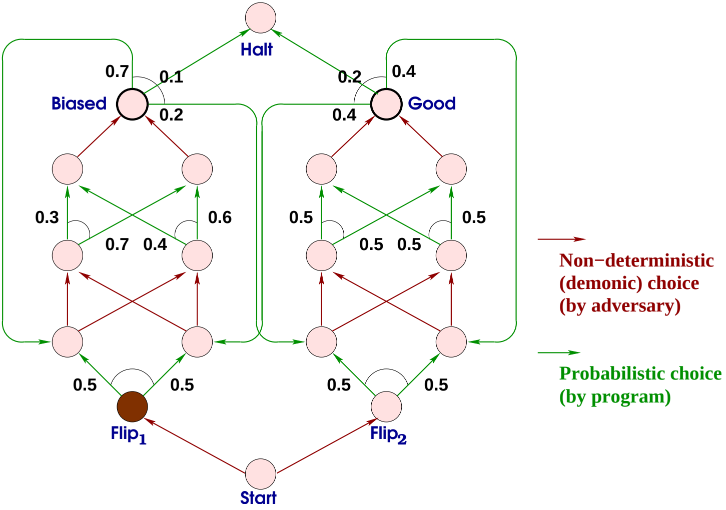
# A Stochastic Game (Demonic Case)



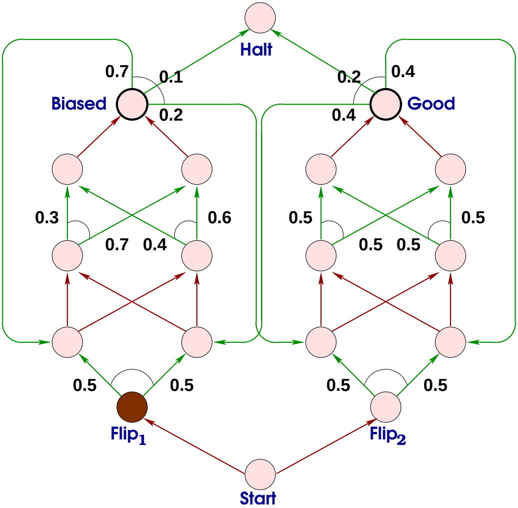
# Start


Halt
0.7
0.1
0.2
0.4
Biased
0.2
0.4
Good
0.3
0.6
0.7 0.4
0.5
0.5
0.5 0.5
0.5 0.5
0.5 0.5
Flip$_1$
Flip$_2$
Start
Non−deterministic
(demonic) choice
(by adversary)
Probabilistic choice
(by program)

# C's Turn: Malevolently Chooses Biased Side



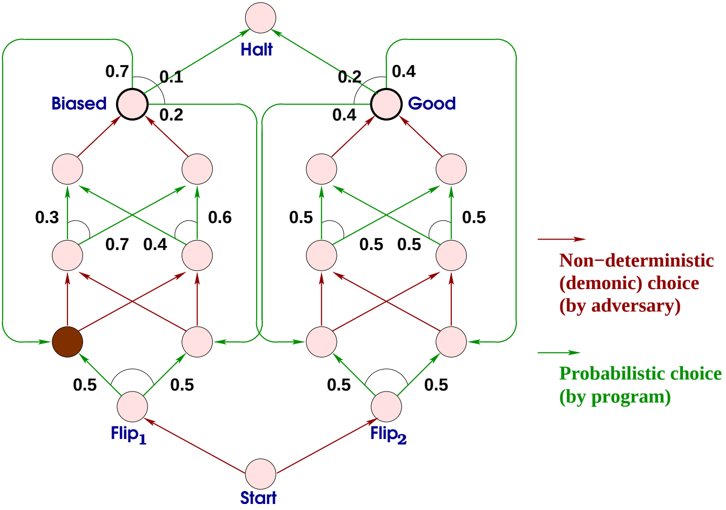
# P's Turn: Flipping a Coin



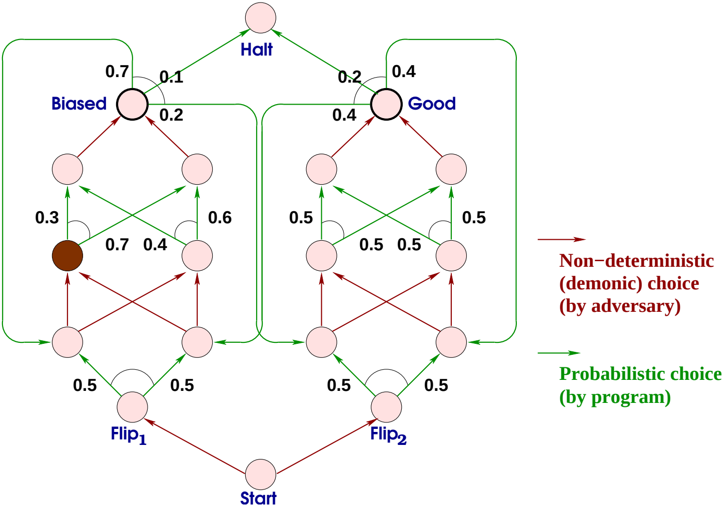

Non−deterministic (demonic) choice (by adversary)

Probabilistic choice (by program)

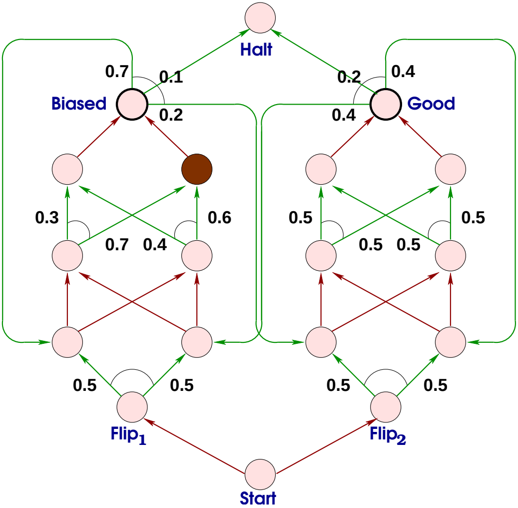
# P's Turn: Advancing



# C's Turn: Picking Most Biased Side



# P's Turn




Non−deterministic (demonic) choice (by adversary)

Probabilistic choice (by program)

# 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

# Anonymity

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

$\neq$ 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.

# 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 constrainted ("task-structured").

# Our Canonical Example: Chaum's Dining Cryptographers [1988]

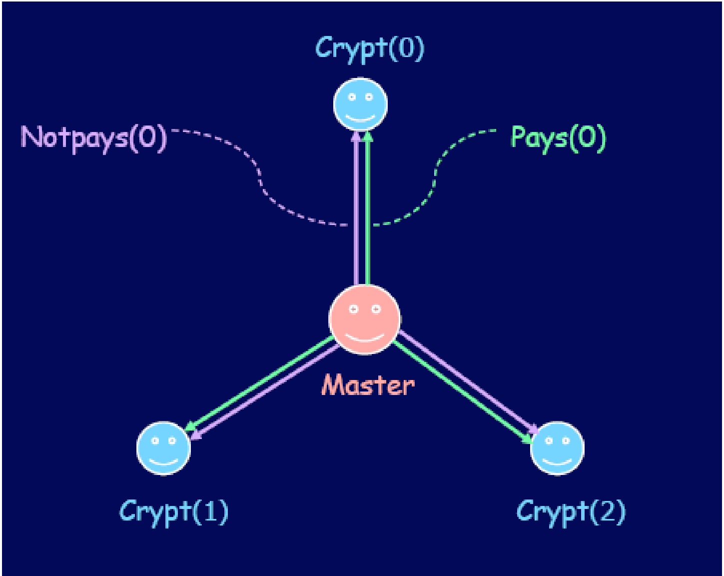
**Problem**:

- $N \geq 3$ 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 $\Leftrightarrow$ the number of "disagree" announced is *odd*.

(Think in $\mathbb{Z}/2\mathbb{Z}$.)

# Modelling the Dining Cryptographers ($N = 3$)

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

$$
\boxed{\begin{aligned} \mathit{Master} = {} & \textstyle\sum_{i=0}^{2} \tau \,.\, \overline{m_i}\mathsf{p} \,.\, \overline{m_{i\oplus 1}}\mathsf{n} \,.\, \overline{m_{i\oplus 2}}\mathsf{n} \,.\, 0 \\ & + \quad \tau . \overline{m_0}\mathsf{n} \,.\, \overline{m_1}\mathsf{n} \,.\, \overline{m_2}\mathsf{n} \,.\, 0 \end{aligned}}
$$

Nondeterministic choice

$$
\begin{aligned}
\mathit{Crypt}_i = {} & m_i(x) \,.\, c_{i,i}(y) \,.\, c_{i,i\oplus 1}(z) \,. \\
& \quad \text{if } x = \mathsf{p} \\
& \quad\quad \text{then } \overline{\mathit{pay}_i} \,.\, \text{if } y = z \\
& \quad\quad\quad \text{then } \overline{\mathit{out}_i}\,\mathit{disagree} \\
& \quad\quad\quad \text{else } \overline{\mathit{out}_i}\,\mathit{agree} \\
& \quad\quad \text{else if } y = z \\
& \quad\quad\quad \text{then } \overline{\mathit{out}_i}\,\mathit{agree} \\
& \quad\quad\quad \text{else } \overline{\mathit{out}_i}\,\mathit{disagree}
\end{aligned}
$$

Anonymous actions

Observables

$$
\boxed{\mathit{Coin}_i = p_h \tau \,.\, \mathit{Head}_i + p_t \tau \,.\, \mathit{Tail}_i}
$$

Probabilistic choice

$$
\begin{aligned}
\mathit{Head}_i &= \overline{c}_{i,i}\mathit{head} \,.\, \overline{c}_{i\ominus 1,i}\mathit{head} \,.\, 0 \\
\mathit{Tail}_i &= \overline{c}_{i,i}\mathit{tail} \,.\, \overline{c}_{i\ominus 1,i}\mathit{tail} \,.\, 0 \\
\mathit{DCP} &= (\nu \vec{m})(\mathit{Master}
\end{aligned}
$$

# Remarks

- 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 $i$!)

# 1-Out-Of-2 Oblivious Transfer

Use:

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

Protocol:

- S $\rightarrow$ R: fresh public key $K$, and fresh tokens $m_0$, $m_1$;
- R $\rightarrow$ S: $Req \hat{=} enc(\text{fresh } \ell, K) \boxplus m_i$;
  ($i \in \{0, 1\}$ chosen by R.)
- S $\rightarrow$ R: $A_0 \hat{=} M_0 \boxplus dec(Req \boxminus m_j, K^{-1})$,
  $A_1 \hat{=} M_1 \boxplus dec(Req \boxminus m_{1-j}, K^{-1})$, $j$;
  ($j \in \{0, 1\}$ 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

# 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.

# 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:

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

# Relax the axioms defining probabilities:

## Belief functions:

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

## 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);

# 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]...

# 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 probabilitic choice.

# Previsions = Choice, in Continuation Passing Style

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:

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

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

# Payoffs, in the Purely Probabilistic Case

Now imagine answers are money. ("utility" to economists).

# 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 $[\![M]\!]\,\rho(h)$.

# 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 $[\![M]\!]\,\rho(h)$.
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

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

# 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 $[\![M]\!]\,\rho(h)$.
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.

# A Continuation Semantics. . . With Choice(s)

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

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

# A Continuation Semantics. . . With Choice(s)

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

$$
\begin{aligned}
[\![\mathtt{val}\, M]\!]\,\rho(h) &= h([\![M]\!]\,\rho) \\
[\![\mathtt{let}\,\mathtt{val}\, x = M \;\mathtt{in}\; N]\!]\,\rho(h) &= [\![M]\!]\,\rho(\lambda v \cdot [\![N]\!]\,(\rho[x := v])(h)) \\
[\![\mathtt{case}]\!]\,\rho(b, v_0, v_1) &= \begin{cases} v_0 & \text{if } b = \text{false} \\ v_1 & \text{if } b = \text{true} \end{cases} \\
[\![\mathtt{flip} : \mathtt{Tbool}]\!]\,\rho(h) &= \frac{1}{2}h(\text{false}) + \frac{1}{2}h(\text{true}) \text{ (mean payoff)}
\end{aligned}
$$

# A Continuation Semantics. . . With Choice(s)

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

$$
\begin{array}{rcl}
[\![\mathtt{val}\, M]\!]\,\rho(h) & = & h([\![M]\!]\,\rho) \\
[\![\mathtt{let}\,\mathtt{val}\, x = M \,\mathtt{in}\, N]\!]\,\rho(h) & = & [\![M]\!]\,\rho(\lambda v \cdot [\![N]\!]\,(\rho[x := v])(h)) \\
[\![\mathtt{case}]\!]\,\rho(b, v_0, v_1) & = & \begin{cases} v_0 & \text{if } b = \text{false} \\ v_1 & \text{if } b = \text{true} \end{cases} \\
[\![\mathtt{flip} : \mathtt{Tbool}]\!]\,\rho(h) & = & \frac{1}{2} h(\text{false}) + \frac{1}{2} h(\text{true}) \text{ (mean payoff)} \\
[\![\mathtt{amb} : \mathtt{Tbool}]\!]\,\rho(h) & = & \inf(h(\text{false}), h(\text{true})) \text{ (min payoff)}
\end{array}
$$

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

# A Continuation Semantics. . . With Choice(s)

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

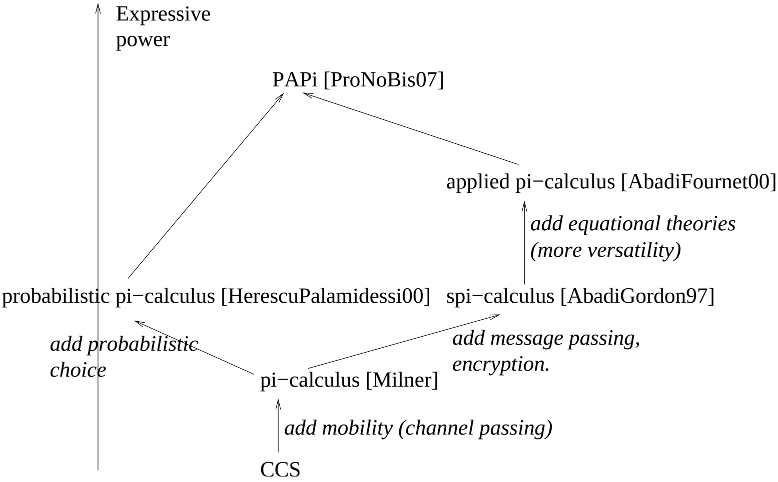
$$\begin{array}{rcl}
[\![\mathtt{val}\, M]\!]\,\rho(h) & = & h([\![M]\!]\,\rho) \\
[\![\mathtt{let}\,\mathtt{val}\, x = M \;\mathtt{in}\; N]\!]\,\rho(h) & = & [\![M]\!]\,\rho(\lambda v \cdot [\![N]\!]\,(\rho[x := v])(h)) \\
[\![\mathtt{case}]\!]\,\rho(b, v_0, v_1) & = & \begin{cases} v_0 & \text{if } b = \text{false} \\ v_1 & \text{if } b = \text{true} \end{cases} \\
[\![\mathtt{flip} : \mathtt{Tbool}]\!]\,\rho(h) & = & \frac{1}{2}h(\text{false}) + \frac{1}{2}h(\text{true}) \text{ (mean payoff)} \\
[\![\mathtt{amb} : \mathtt{Tbool}]\!]\,\rho(h) & = & \inf(h(\text{false}), h(\text{true})) \text{ (min payoff)}
\end{array}$$

(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

# PAPi: A Calculus for Cryptographic Systems



# PAPi: Syntax

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

$$M, N \;::=\; a, b, c, \ldots \;\;\Big|\;\; x, y, z, \ldots \;\;\Big|\;\; f(M_1, \ldots, M_l)$$

...interpreted modulo an equational theory $E$

# PAPi: Syntax

Terms ($\cong$ 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 $E$

Processes ($\cong$ programs $\cong$ systems):

$$\begin{aligned} P, Q \ ::= \ & \mathbf{0} \ \mid \ \overline{u}\langle M\rangle.P \ \mid \ u(x).P \ \mid \ P + Q \ \mid \ P \oplus_p Q \ \mid \\ & P \mid Q \ \mid \ !P \ \mid \ \nu n.P \ \mid \ \text{if } M = N \text{ then } P \text{ else } Q \end{aligned}$$

Extended processes ($\cong$ programs-in-context):

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

**Note**: Active substitutions ($\cong$ adversarial knowledge $\cong$ contexts): special case where $P = \mathbf{0}$.

# PAPi: Weak Bisimulation

Use *schedulers* to resolve non-determinism.

## Weak bisimulation

The largest symmetric relation $\mathcal{R}$ s.t. $A\mathcal{R}B$ implies:

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

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

However, we have not used previsions to this end (yet).

# PAPi: Main Theorem [APLAS'07]

Define contextual equivalence $\approx$ for two closed extended processes $A$, $B$, iff no adversary (context) can tell the difference between $A$ and $B$ by interacting with each.

**Theorem**

*$A \approx B$ iff there is a weak bisimulation $\mathfrak{R}$ such that $A \mathfrak{R} B$.*

**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

# Defining Anonymity

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:

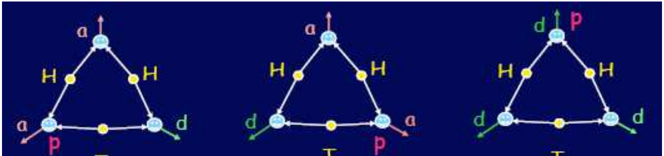
Repeating experiments is nonsense. . .
since *I* may keep track of past experiments
and change behaviors (i.e., change distributions).

# 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:

$$Evidence(\text{“}i\text{ paid”}, obs) = \frac{P(obs|\text{“}i\text{ paid”})}{\sum_j P(obs|\text{“}j\text{ paid”})}$$

- Then S is strongly anonymous iff for every observable *obs*, for every $i, j$,

$$Evidence(\text{“}i\text{ paid”}, obs) = Evidence(\text{“}j\text{ paid”}, obs)$$

Beautiful connection to channel capacity [TGC'06].

# Nasty Schedulers

- For any reasonable (fixed) scheduler, Chaum's implementation is then strongly anonymous.

# 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.

# 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. . .

# 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 $\star$magically$\star$ schedules the cryptographer who paid (if any) first.
  Then *I* simply observes who answered first.

# 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.].

# 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:

$$S \ ::= \ L.S \ \Big| \ (L, L).S \ \Big| \ \text{if } L \text{ then } S \text{ else } S \ \Big| \ \mathbf{0}$$

- 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=Dempster-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).