# COMETE

## Activities related to ProNoBiS

# The team

- Catuscia Palamidessi (DR INRIA)
- Frank Valencia (CR CNRS)
- Peng Wu (Postdoc)
- Sardaouna Hamadou (Future postdoc)
- Kostas Chatzikokolakis (PhD student)
- Romain Beauxis (PhD student)
- Purnima Gupta (Intern)
- ? Sylvain Pradalier (future PhD student)
- ? Carlos Olarte (future PhD student)

# The probabilistic pi-calculus

- Asynchronous pi-calculus + a probabilistic input-choice construct
- Originally developed for filling the expressive gap between the pi-calculus and the asynchronous pi-calculus
- Used for specifying probabilistic security protocols
  - The fair exchange (Kostas + Catuscia)
  - Various anonymity protocols (Kostas + Catuscia)
- Model checker based on PRISM being developed in collab with Kwiatkowska's group
  - Dave Parker and Peng Wu

# Anonymity

- Study of a notion of strong probabilistic anonymity (Catuscia and Mohit Bhargava)
  - Combining nondeterminism (anonymous agents)and probability (protocols mechanisms)
    - Theory of evidence
- Probable innocence
  - Satisfied by “real protocols” like Crowds
  - various definitions
    - limit on the probability of detecting the culprit (Rubin)
    - limit on the probability of the agent to be the culprit
  - development of a notion that combines both requirements (Kostas and Catuscia)

# Anonymity: future work

- Other forms of nondeterminism (with Purnima)
- Group anonymity (with Purnima)
- Extension to other paradigms of partial information-hiding (with Sardaouna)
- Relation with information Theory (project PRINTEMPS, with Prakash Panangaden)
- A logic based on conditional probability

# Concurrent Constraint Programming

- Applications to security:
  - Constraints = partial knowledge accumulated by adversary
  - Monotonic evolution of the store = monotonic adversary
    - SPL (Winskel and Crazzolara) , applied spi-calculus
- Advantages: Elegant and simple Denotational semantics based on closure operators
- CCP as a subset of the pi-calculus (Valencia,Saraswat, Victor, Palamidessi)
- Project followed by Valencia. Collaboration with Colombian universities