Modelling and Analysing of Security Protocol: Lecture 12

Probabilistic Modelling Checking of Anonymous Systems

Tom Chothia
CWI

Today

- Model Checking for finite systems
- Specifying properties in CTL
- Dining Philosophers

BREAK
- Probabilistic finite systems
- Specifying probabilistic properties in PCTL
- Dining Cryptographers

PCTL

Probabilistic Model Checking

Dinning Cryptographers

- Nodes form a ring
- Each adjacent pair picks a random number
- Each node broadcasts the sum (xor) of the adjacent numbers
- The user who wants to send a message also adds the message
- The total sum (xor) is:
  \[ r_1 + r_2 + r_5 + r_3 + r_5 + r_1 + m = m \]
Results of the Model Checking

Results of the Model Checking

Result of $P(\text{Tails})=0.25$

Result of $P(\text{Tails})=0.25$

Result of $P(\text{Tails})=0.21132$

Today

- Model Checking for finite systems
- Specifying properties in CTL
- Dinning Philosophers example
  - BREAK
  - Probabilistic finite systems
  - Specifying probabilistic properties in PCTL
  - Dinning Cryptographers