Probabilistic Methods in Concurrency

Lecture 9

Other uses of randomization: a randomized protocol for anonymity

Catuscia Palamidessi
catuscia@lix.polytechnique.fr
www.lix.polytechnique.fr/~catuscia

Page of the course:
www.lix.polytechnique.fr/~catuscia/teaching/Pisa/

Anonymity

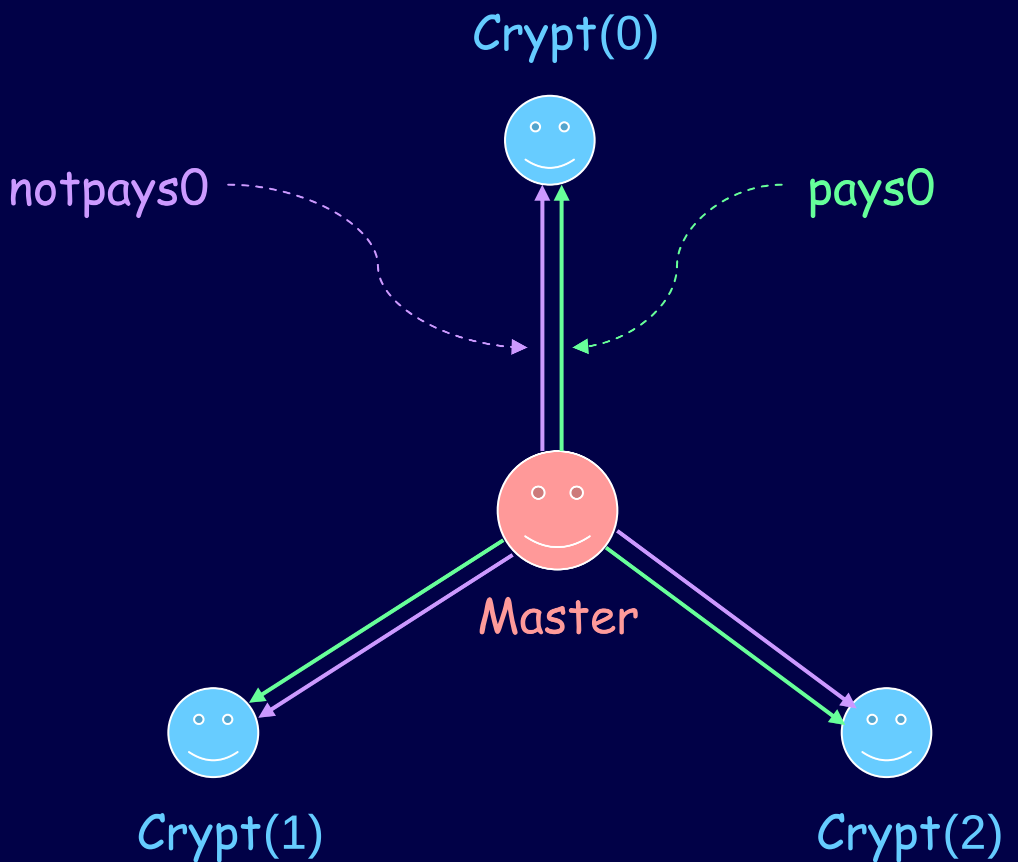
- **Idea:**
  - (In general) To ensure that a certain part of an information becomes public while another part of it remains secret.
  - Typically, what we want to maintain secret is the identity of the agent involved
- Examples:
  - Electronic elections
  - Delation
- We will consider the case of in which the information to make public is whether or not a certain event has taken place, and the information to hide is the identity of the agent performing that event

The dining cryptographers

- **The Problem:**
  - Three cryptographers share a meal
  - The meal is paid either by the organization (master) or by one of them. The master decides who pays
  - Each of the cryptographers is informed by the master whether or not he is paying

- ***GOAL***:
  - The cryptographers would like to know whether the meal is being paid by the master or by one of them, but without knowing who among them, if any, is paying. They cannot involve the master

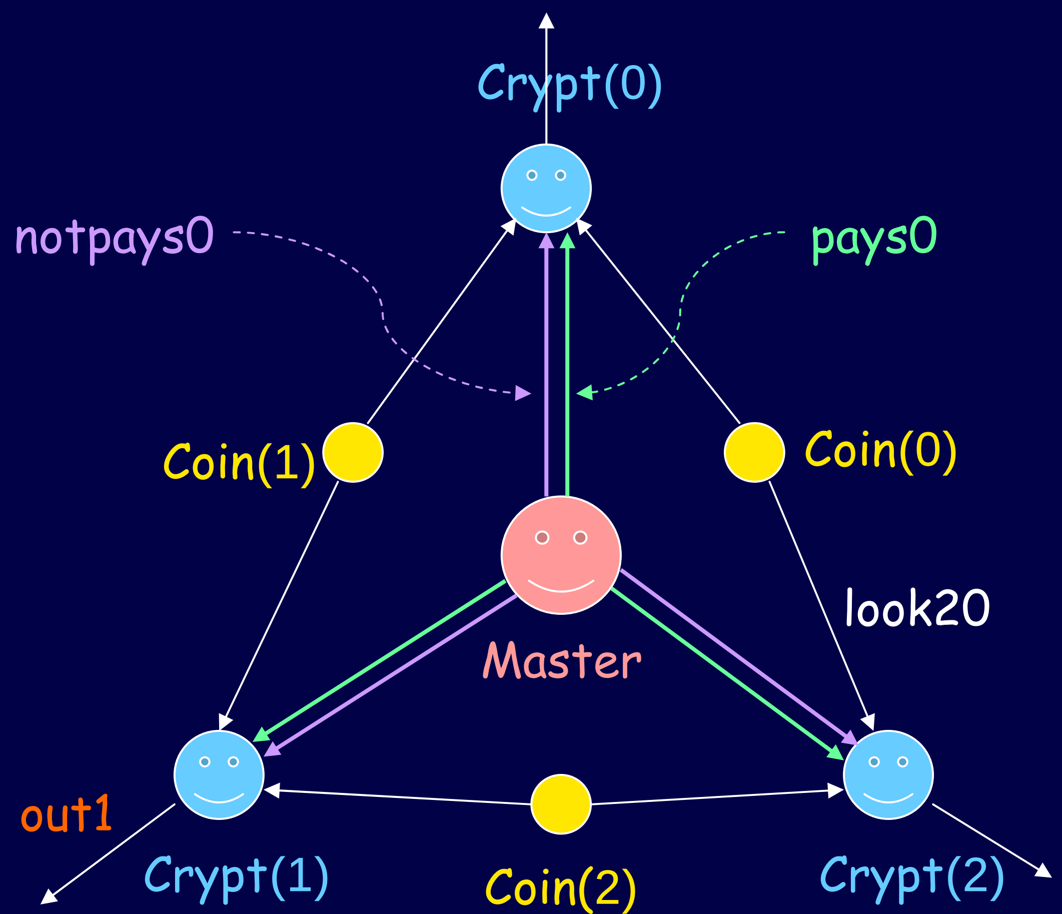
Example: The dining cryptographers



The dining cryptographers: A solution

- Each cryptographer tosses a coin (probabilistic choice). Each coin is in between two cryptographers.
- The result of each coin-tossing is visible to the adjacent cryptographers, and only to them.
- Each cryptographer examines the two adjacent coins
  - If he is paying, he announces "agree" if the results are the same, and "disagree" otherwise.
  - If he is not paying, he says the opposite

The dining cryptographers: A solution



Properties of the solution

Proposition 1 (Public information): if the number of "disagree" is even, then the master is paying. Otherwise, one of them is paying.

Proposition 2 (Anonymity): In the latter case, if the coin is fair then the non paying cryptographers and the external observers will not be able to deduce whom exactly is paying

Anonymity: formal definition

- We will model events as consisting of two components: the event itself, x, and the identity of the agent performing the event, a

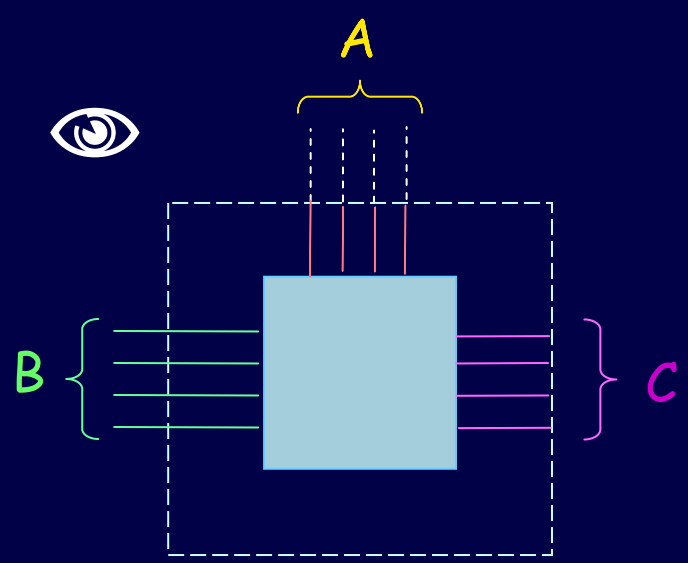
$$ax$$

- AnonyAgs: the agents who want to remain secret
- Given x, define $A = \{ax \mid a \in AnonyAgs\}$

- **Definition:** A protocol described as a system P provides anonymity if an arbitrary permutation of the events in A, applied to an execution of P, does not change the probabilities of the observables

Anonymity

- In general, given P, consider the sets:
  - A = { ax | a ∈ AnonyAgs } : the actions that we want to know only partially (we want to know x but not a)
  - B : the actions that we want to observe (it may include x but not a)
  - C = Actions – (B U A) : The actions we want to hide



The system to consider for the Anonymity analysis: P\C

Definition: The system is anonymous if for every scheduler, for every observations O_1, O_2 in B, and for every action ax ∈ A, we have

$$pb(ax|O_1) = pb(ax|O_2)$$

i.e. the observables do not allow to deduce anything about the identity of the agent

Equivalently: for every O, a and b, we have

$$pb(O|ax) = pb(O|bx) .$$

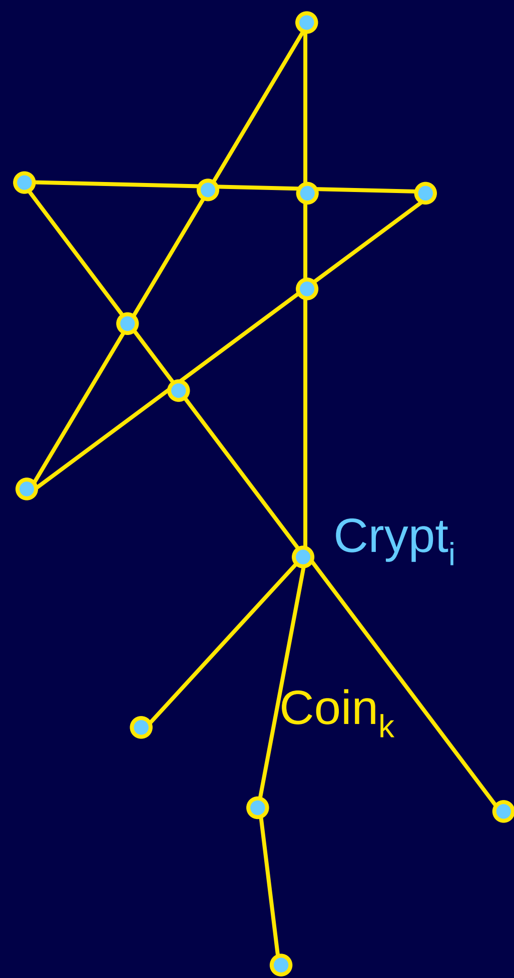
Namely, the probability of an observable does not depend on the identity of the agent

The protocol in the general case

- In general, given an arbitrary graph, where the nodes represent the cryptographers, and the arcs the coins, we can extend the protocol as follows:
  - $b_i = 0$ if cryptographer i does not pay, $b_i = 1$ otherwise
  - $coin_k = 0$ if coin k gives head, $coin_k = 1$ otherwise
  - $crypt_i$ = output of cryptographer i, calculated as follows:

$$crypt_i = \sum_{k \text{ adjacent } i} coin_k + b_i$$

where the sums are binary



The protocol in the general case

- **Proposition:** there is a payer iff

$$\Sigma_i \ crypt_i = 0$$

Proof: just observe that in this sum each $coin_k$ is counted twice. Furthermore there is at most one k s.t. $b_k = 1$. Hence the result is 0 iff there is no k s.t. $b_k = 1$.

- **Proposition:** If all the coins are fair, and the graph is connected, then
  - the system is anonymous for every external observer
  - the system is anonymous for any node j such that, if we remove j and all its adjacent arcs, the rest of the graph is still connected