18734: Foundations of Privacy

Privacy as Restrictions on Personal Information Flow

Anupam Datta

CMU

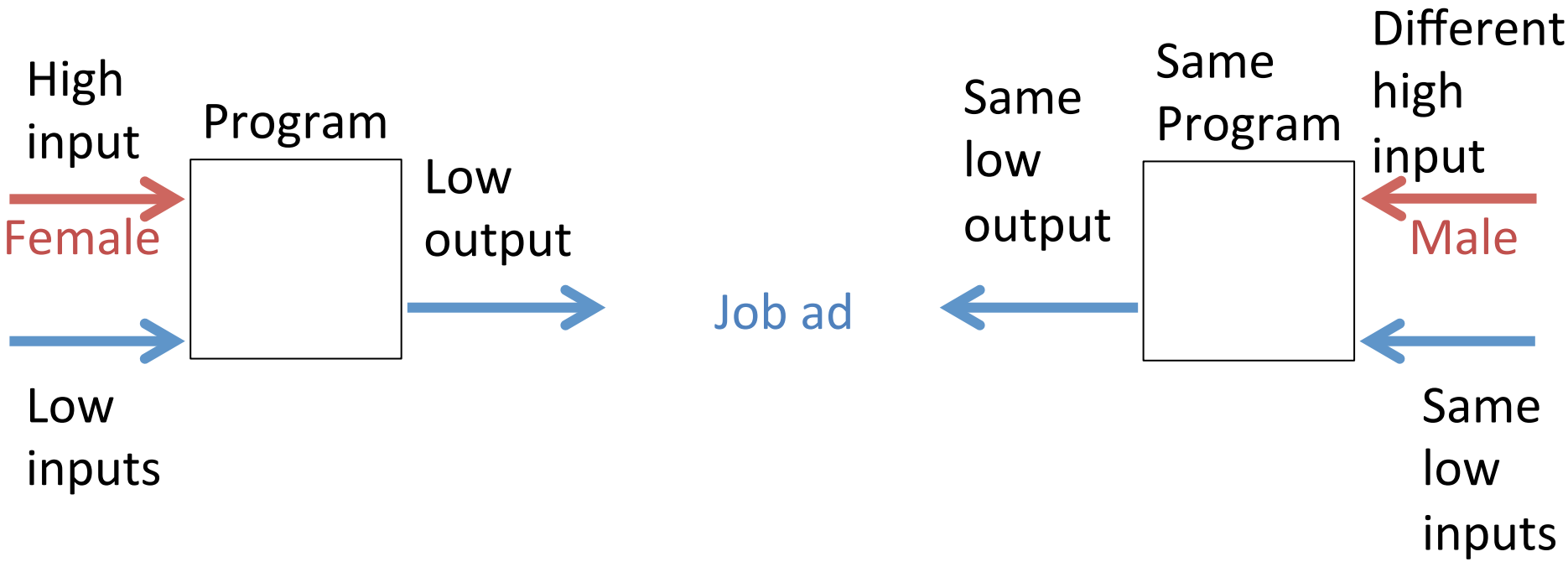
Fall 2015

Organizing Viewpoint

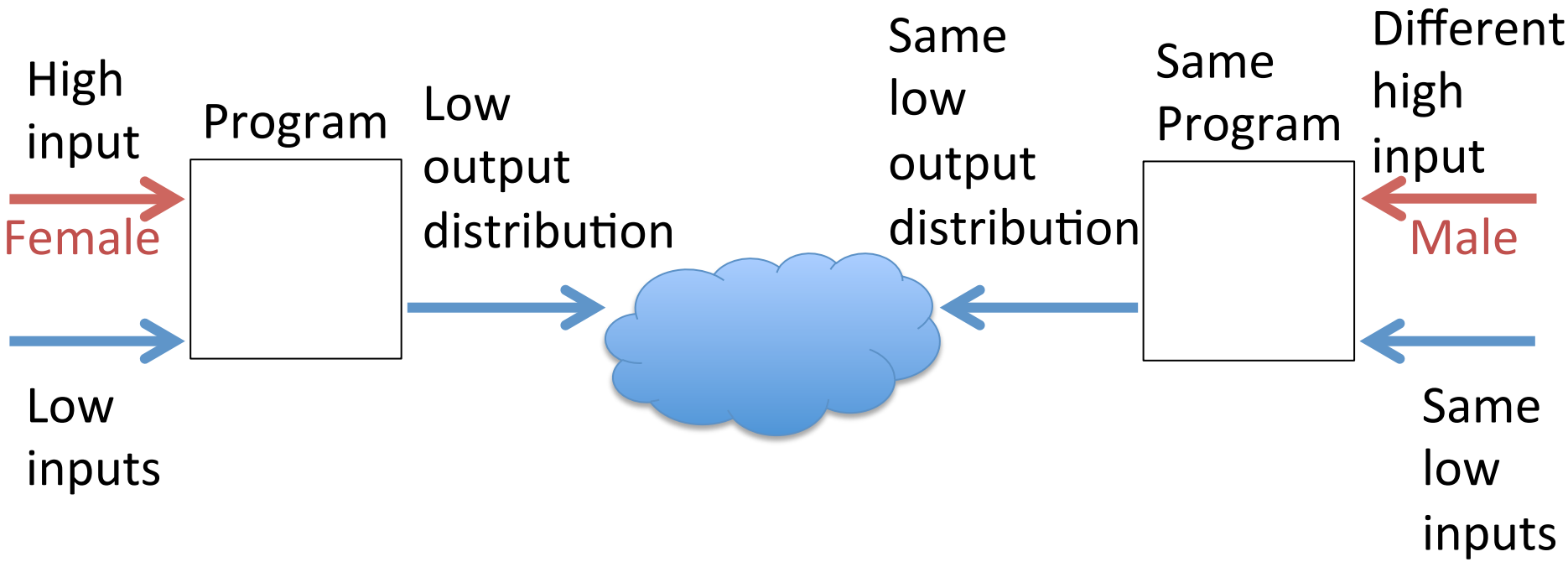
Privacy as a right to restrictions on personal information flow

[Goguen and Meseguer, 1982]

Noninterference

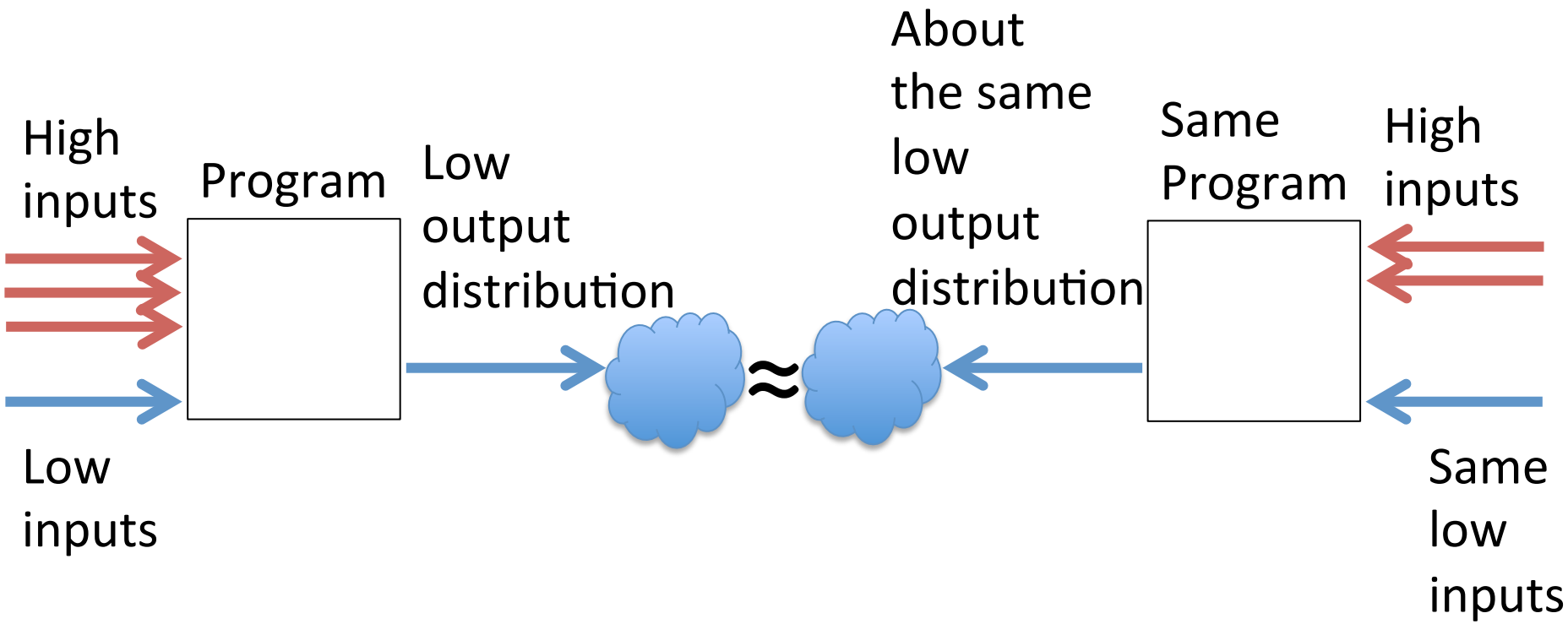


Probabilistic Noninterference



[Dwork, McSherry, Nissim & Smith, 2006]

Differential Privacy



Example from HIPAA Privacy Rule

A covered entity may disclose an individual's protected health information (phi) to law-enforcement officials for the purpose of identifying an individual if the individual made a statement admitting participating in a violent crime that the covered entity believes may have caused serious physical harm to the victim

- Concepts in privacy policies
  - **Actions:** send(p1, p2, m)
  - **Roles:** inrole(p2, law-enforcement)
  - **Data attributes:** attr_in(prescription, phi)
  - **Temporal constraints:** in-the-past(state(q, m))
  - **Purposes:** purp_in(u, id-criminal))
  - **Beliefs:** believes-crime-caused-serious-harm(p, q, m)

Black-and-white concepts

Grey concepts

Privacy as Restrictions on Personal Information Flow