IIITB - MPHASIS RISE 2023

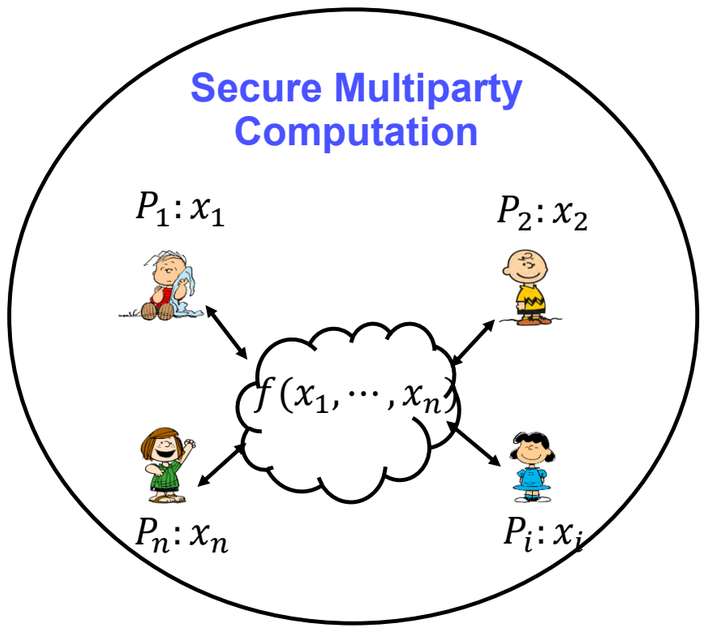
Secure Multi-Party Computation Against Passive Adversaries

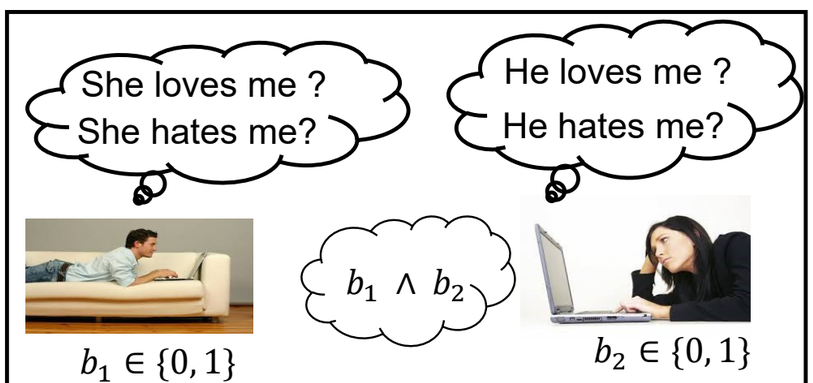
Ashish Choudhury.
Associate Professor@IIITB

Arpita Patra
Associate Professor@IISc

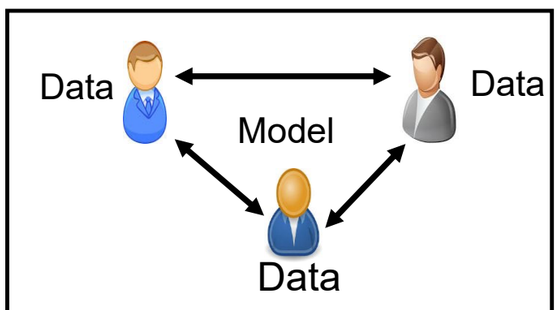
Secure Multiparty Computation (MPC)

Privacy-preserving Data Mining





Secure Online Dating



Privacy-Preserving ML

Secure MPC: A very fundamental problem in modern cryptography

About the Book

- Focus **only** on MPC protocols in the **passive corruption** model
  - Achieving security against such a benign form of adversary itself is non-trivial and demands sophisticated and highly advanced techniques
  - Can be taught as a 4-credit advanced elective course
  - Starting point of MPC protocols against malicious/active/Byzantine corruption
    - Includes detailed security proofs for seminal protocols and state-of-the-art efficiency improvement techniques
    - Presents protocols against **computationally bounded** as well as **computationally unbounded** adversaries
    - Extensive worked out examples and pictorial illustrations
    - Companion free video lectures/NPTEL MOOC