Rump Session 2016

Fair Secure Computation (or how can I gain strategic advantage by breaking fairness)

Alptekin Küpçü

Koç University

Fair Secure Computation

ALPTEKİN KÜPÇÜ

Assistant Professor of Computer Science and Engineering

KOÇ UNIVERSITY

Secure Multi-Party Computation

X_1 

 X_2

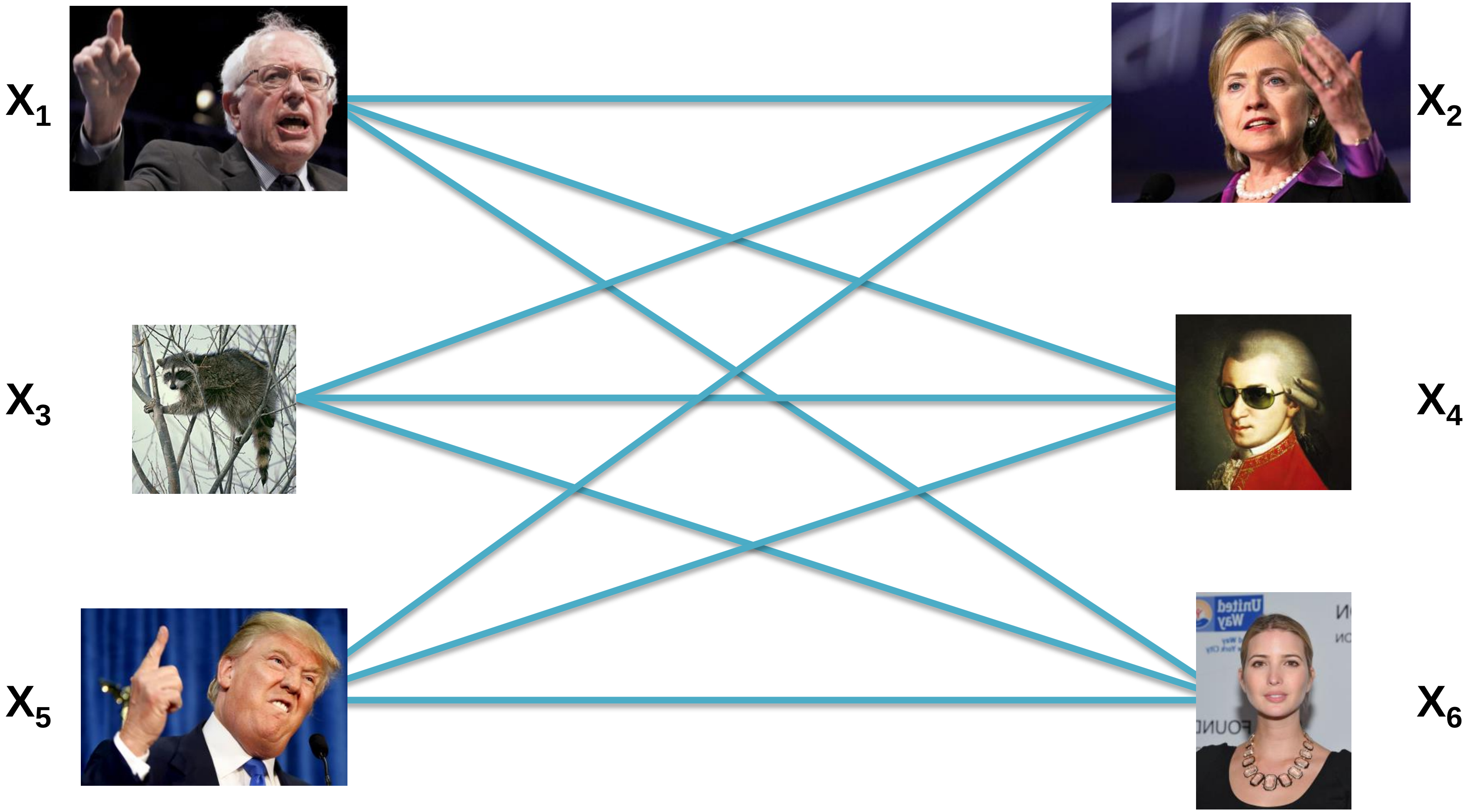
X_3 

 X_4

X_5 

 X_6

Secure Multi-Party Computation



Secure Multi-Party Computation

Y_1 

 Y_2

Y_3 

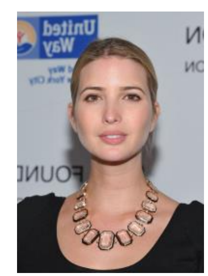
 Y_4

Y_5 

 Y_6

Secure Multi-Party Computation

Y_3

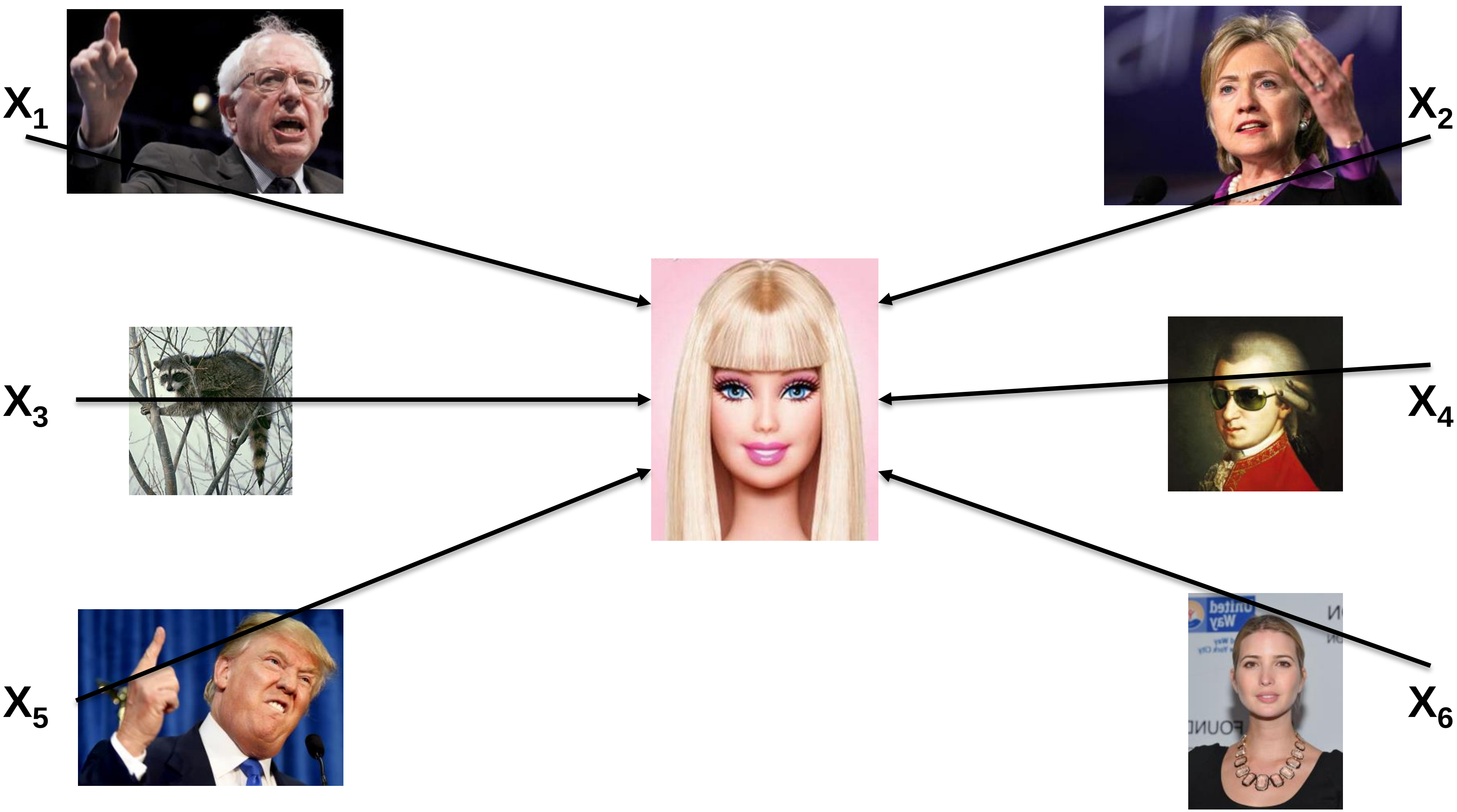


SMPC in a Corporate Setting

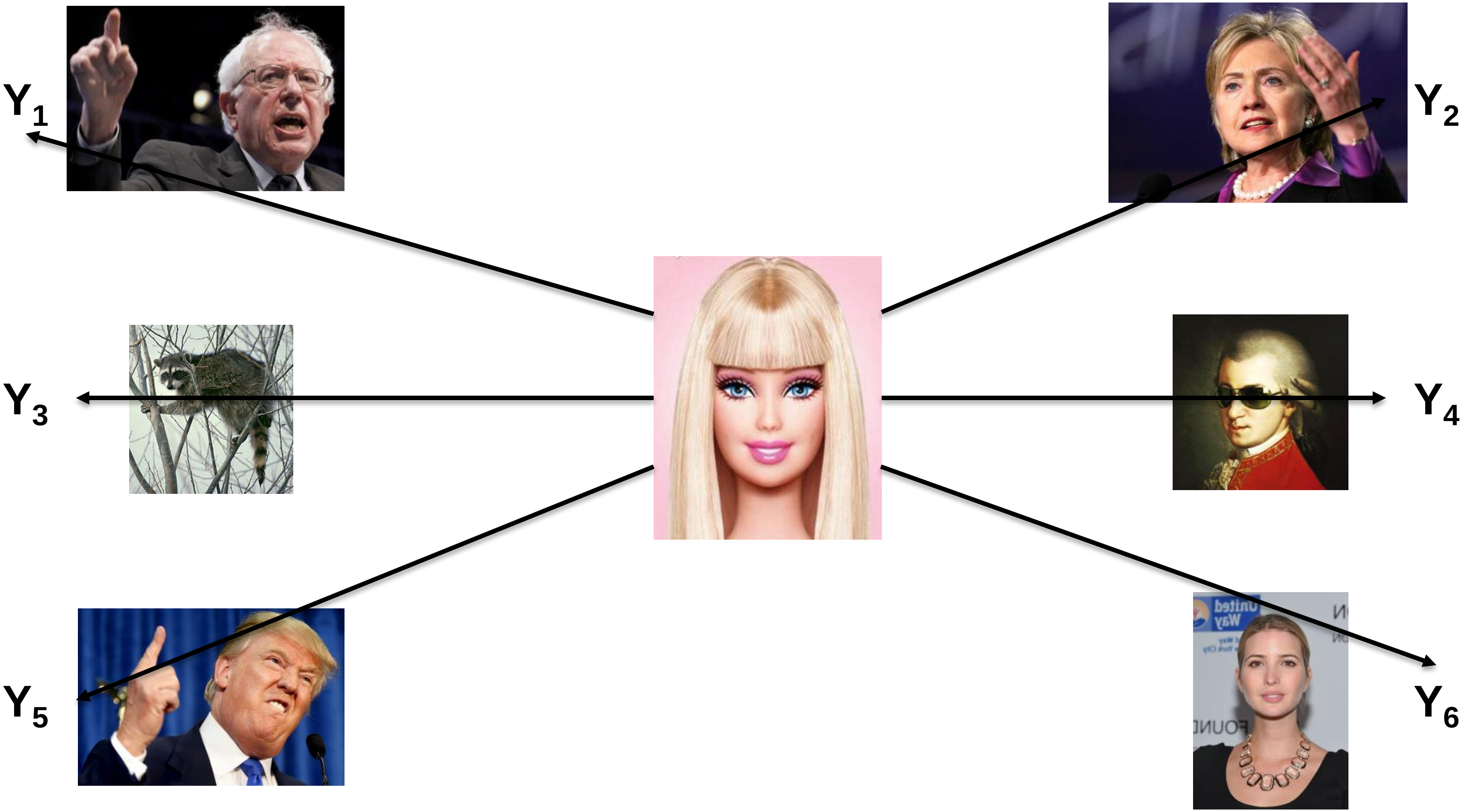
I OWN YOU

Y_3

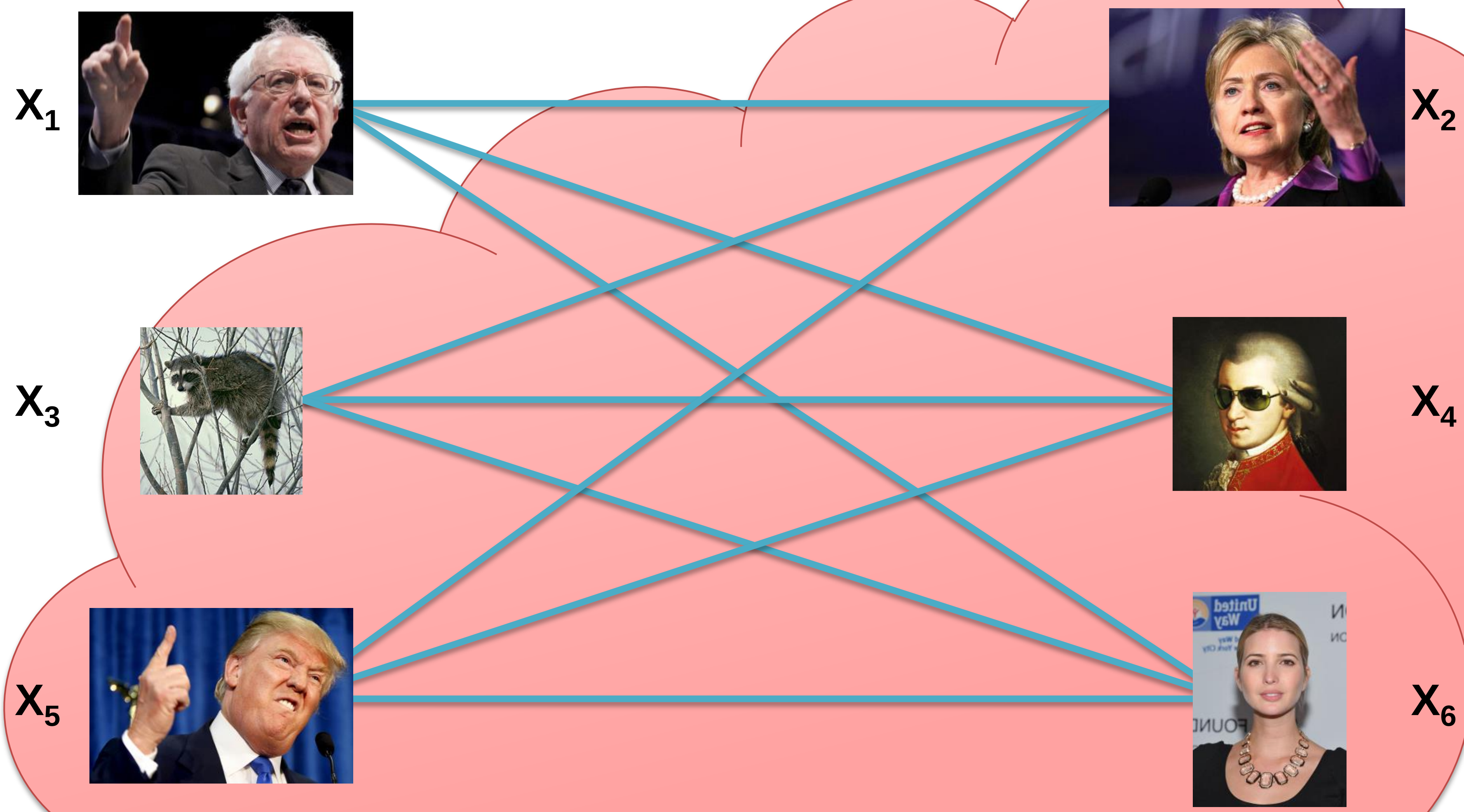
Ideal World



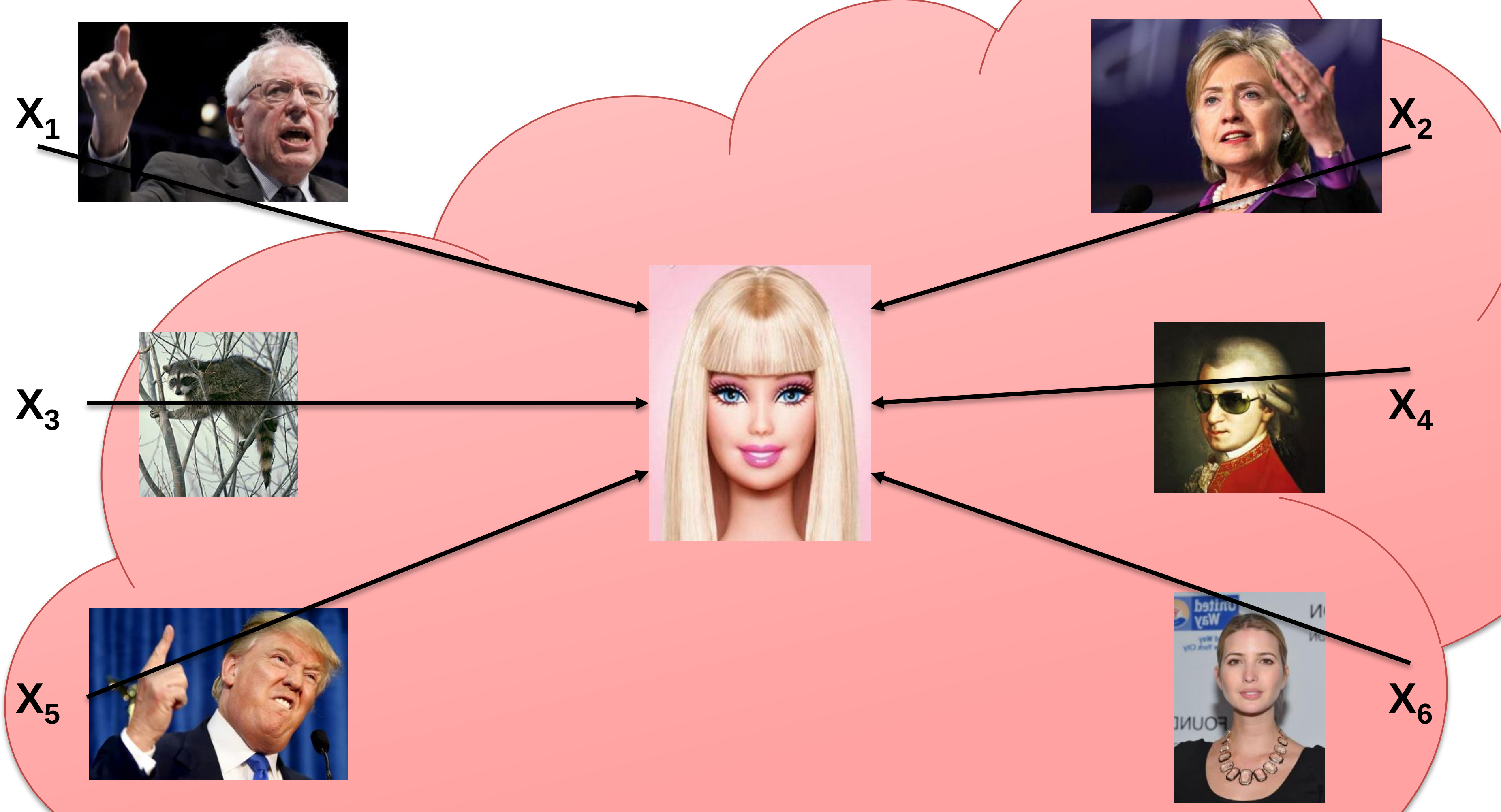
Ideal World



Real World



Simulator



Fairness Impossible in General

- Assume a trusted Arbiter is available
  - Only trusted for fairness, not security
    - May collude with players
    - Should not learn input/output
  - Optimistically employed
  - Must be efficient (otherwise bottleneck)

Fairness Impossible in General

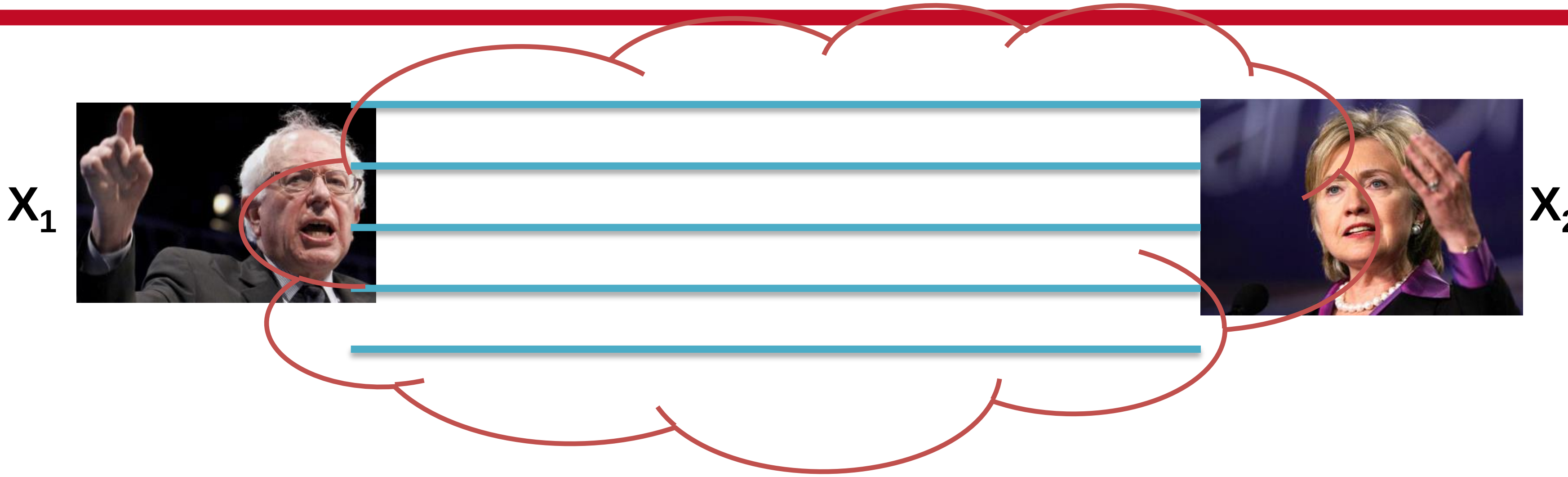
- Assume a trusted Arbiter is available
  - Only trusted for fairness, not security
    - May collude with players
    - Should not learn input/output
  - Optimistically employed
  - Must be efficient (otherwise bottleneck)
- Ideal TTP

Real Arbiter

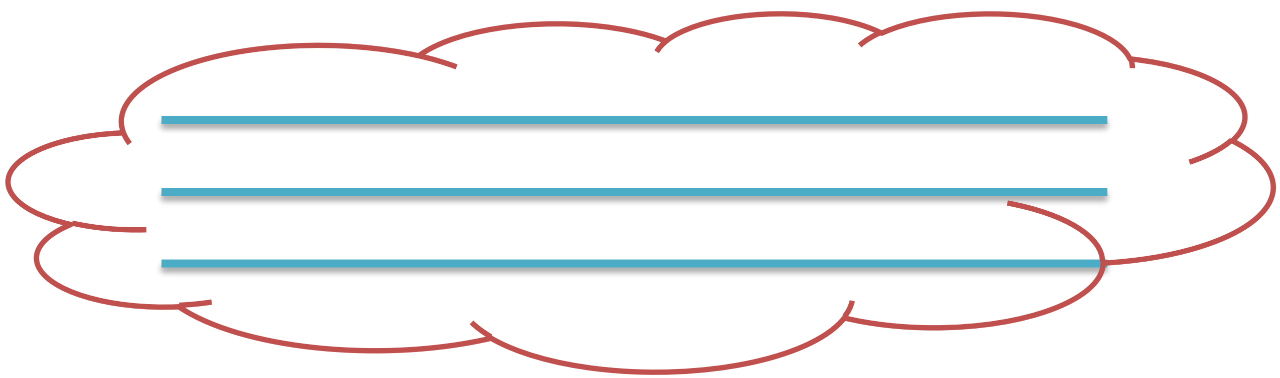
Fair and Secure Computation

- **Fairness extentions and Arbiter resolutions must be simulated**

Simulating Fairness

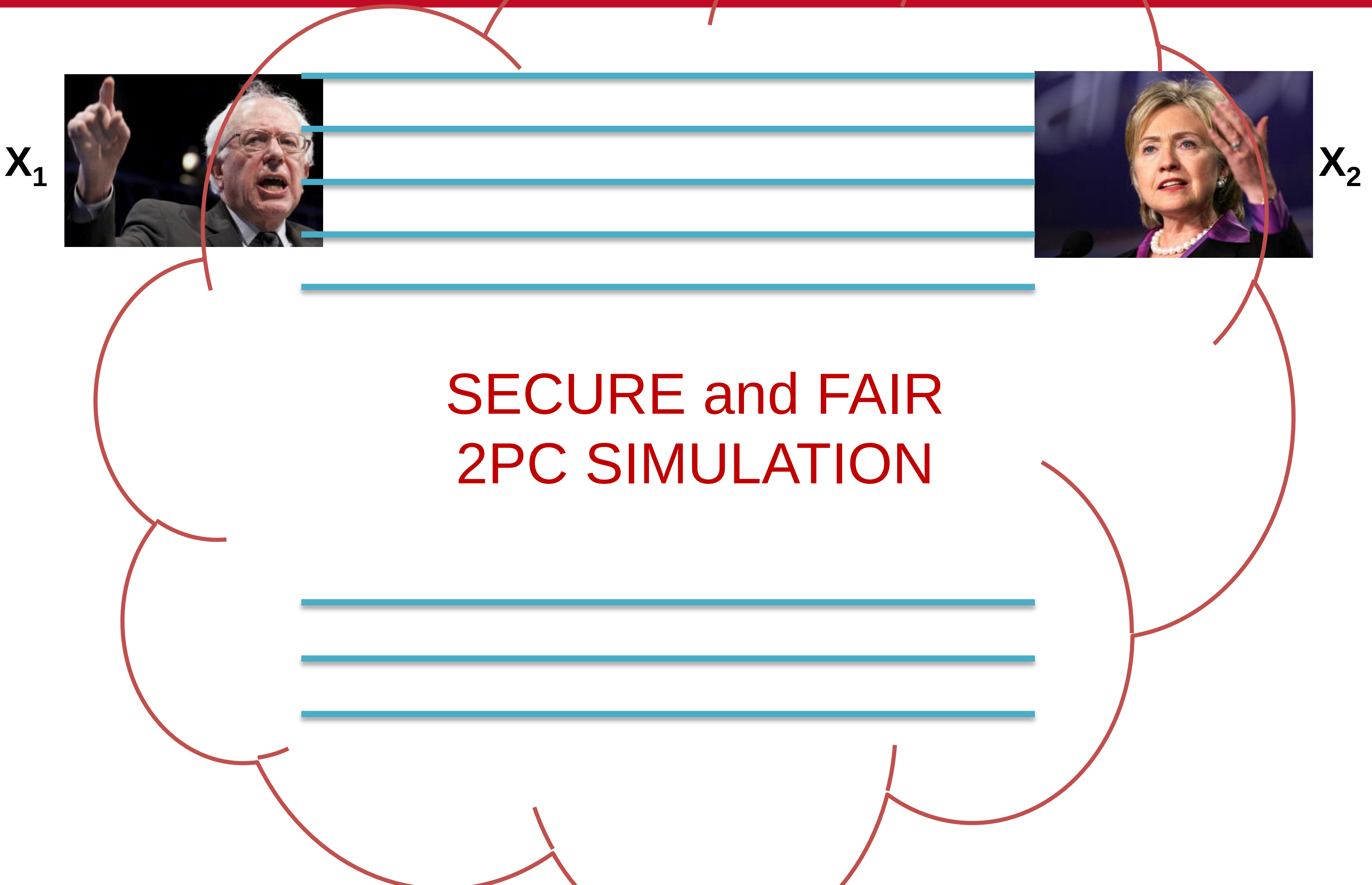


SECURE 2PC SIMULATION



FAIRNESS ARGUMENT

Simulating Fairness



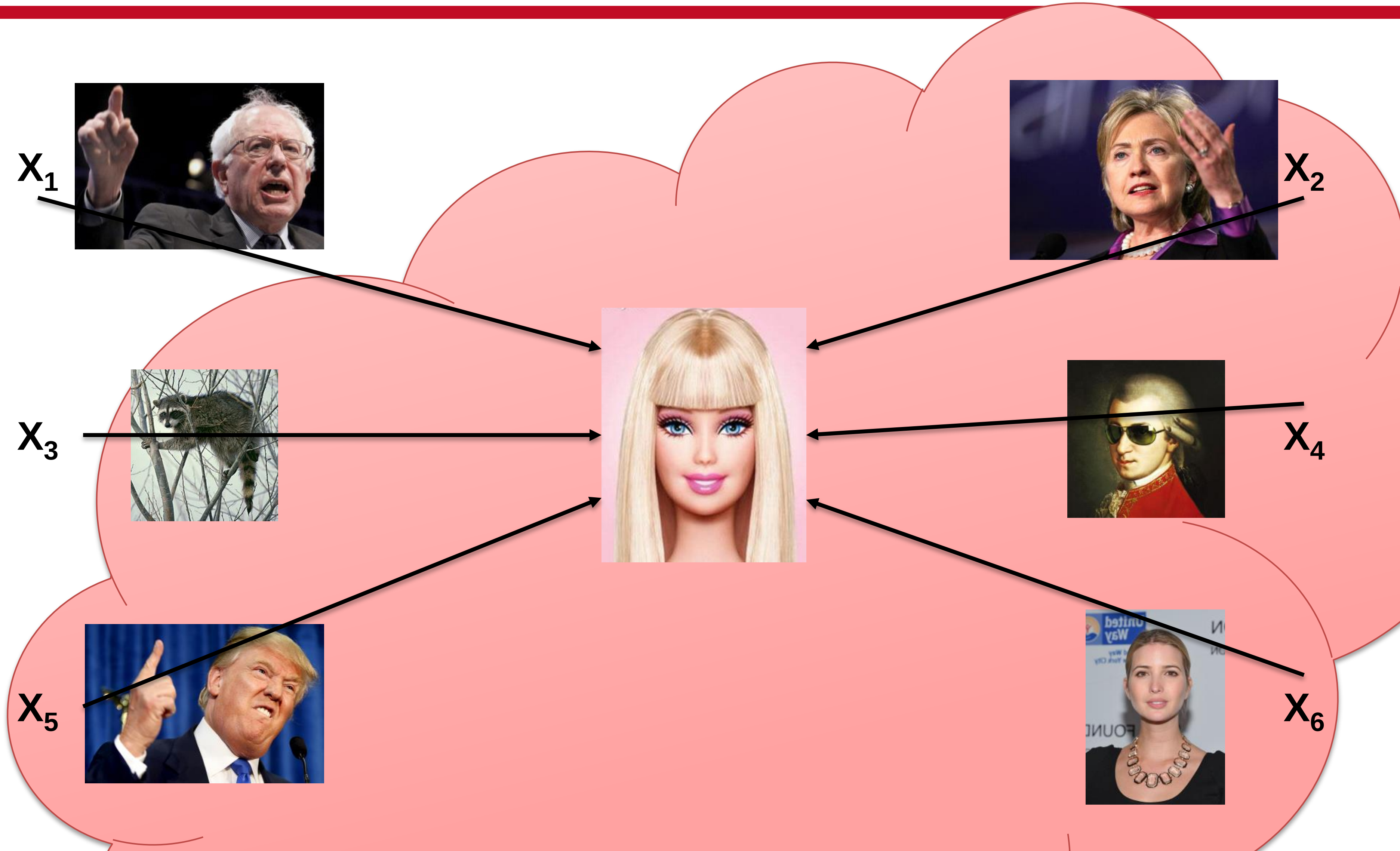
Fair and Secure Computation

- Fairness extentions and Arbiter resolutions must be simulated
  - Otherwise the protocol may be insecure!

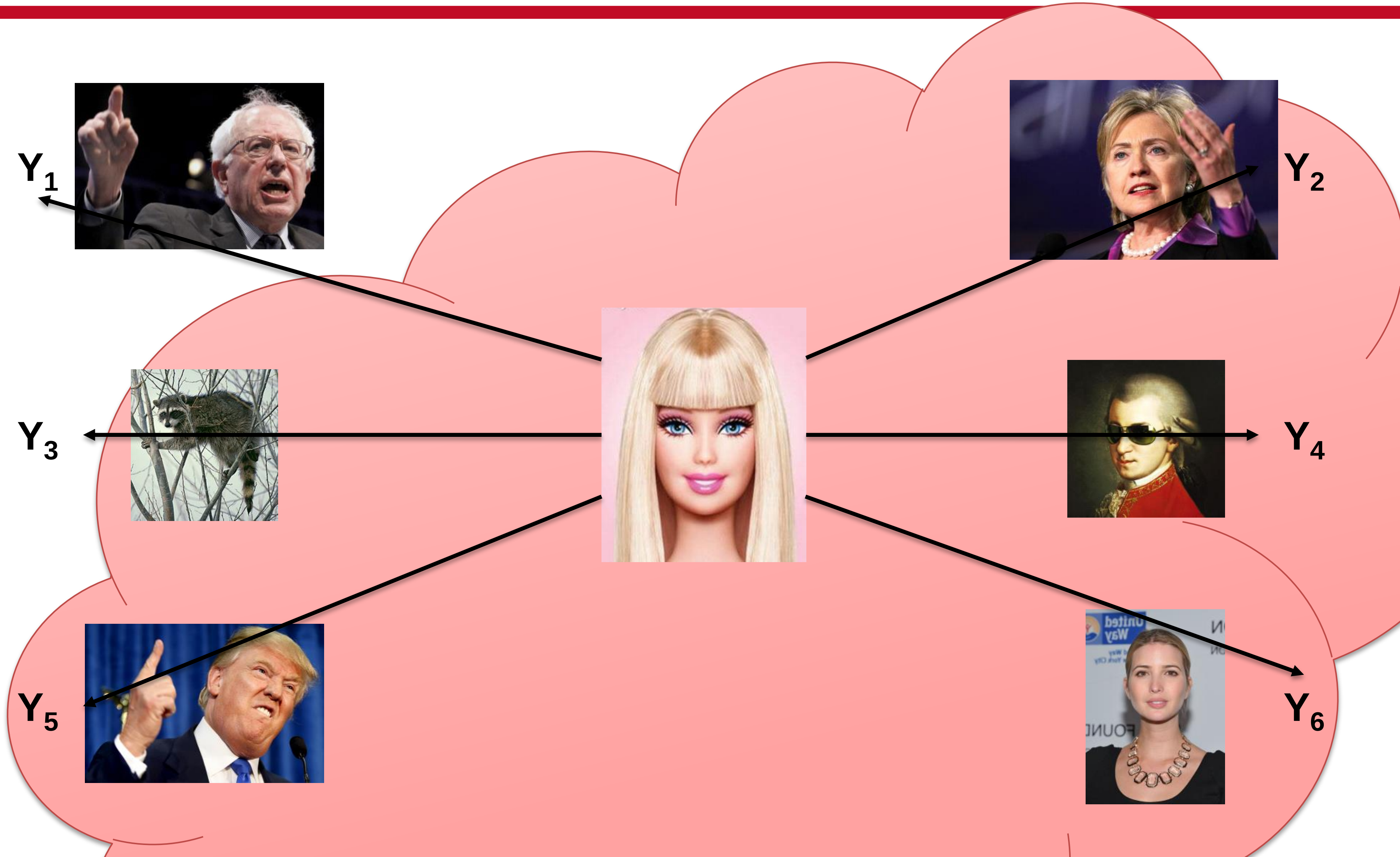
Fair and Secure Computation

- Fairness extentions and Arbiter resolutions must be simulated
  - Otherwise the protocol may be insecure!
- Simulator may contact  only when fairness is guaranteed

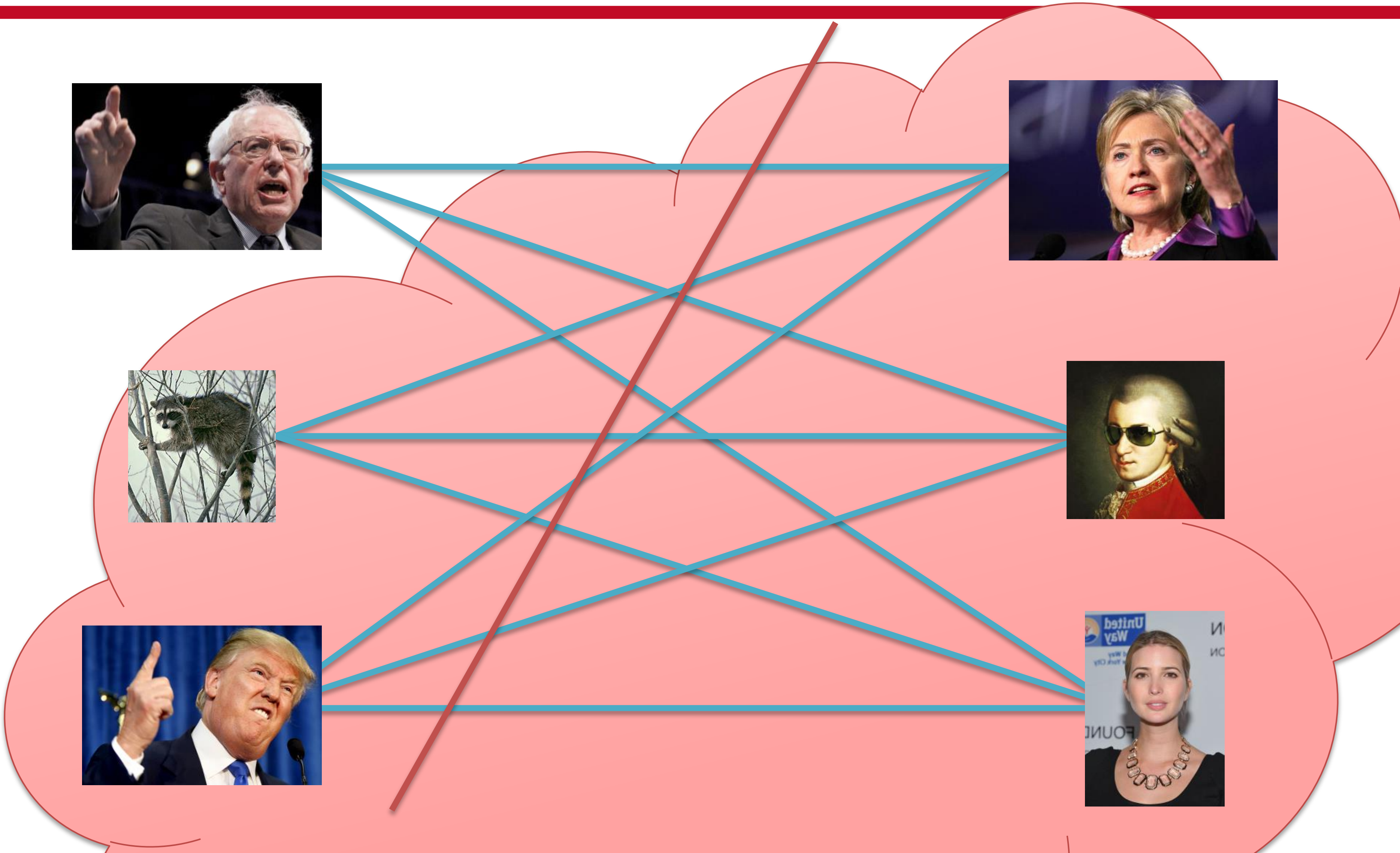
Simulator



Ideal World



Real World



Fair and Secure Computation

- **Fairness extentions and Arbiter resolutions must be simulated**
  - **Otherwise the protocol may be insecure!**
- **Simulator may contact**  **only when fairness is guaranteed**
  - **Otherwise real and ideal world outputs are distinguishable**

Fair and Secure Computation

- Fairness extentions and Arbiter resolutions must be simulated
  - Otherwise the protocol may be insecure!
- Simulator may contact  only when fairness is guaranteed
  - Otherwise real and ideal world outputs are distinguishable
- Arbiter cannot harm security

Our Solutions

# Participants	# Rounds	# Messages
2	O(1)	O(1)
n	O(1)	O(n^2)

- **OPTIMAL asymptotic performance**
- **Cut-and-choose or zero-knowledge**
- **Malicious or covert**
- **2PC or MPC**

Comparison

- Compared to related works, we provide
  - Optimal asymptotic performance
    - Constant round (not gradual release)
    - No broadcast
    - Arbiter load independent of the circuit size
  - Do not require an external payment mechanism
    - In a competitive corporate setting, how can one value some output that is unknown beforehand?
  - Full simulation proofs
  - Arbiter cannot harm security
    - Also proven via simulation
    - Only fairness is lost if Arbiter colludes with malicious parties

Our Papers

- **Reading**
  - **Kılınç and Küpçü, CT-RSA 2015**, ***Optimally Efficient Multi-Party Fair Exchange and Fair Secure Multi-Party Computation***
  - **Kılınç and Küpçü, FC 2016**, ***Efficiently Making Secure Two-Party Computation Fair***
  - **Küpçü and Mohassel, FC 2016**, ***Fast Optimistically Fair Cut-and-Choose 2PC***

- ***Funding Acknowledgements***
  - ***TÜBİTAK, the Scientific and Technological Research Council of TURKEY***
  - ***COST Action IC1306 Cryptoactio***

ALPTEKİN KÜPÇÜ

Assistant Professor of Computer Science and Engineering

http://crypto.ku.edu.tr

KOÇ UNIVERSITY

CRYPTO@KU