

AC-Framework for Privacy-Preserving Collaboration

Wei Jiang & Chris Clifton

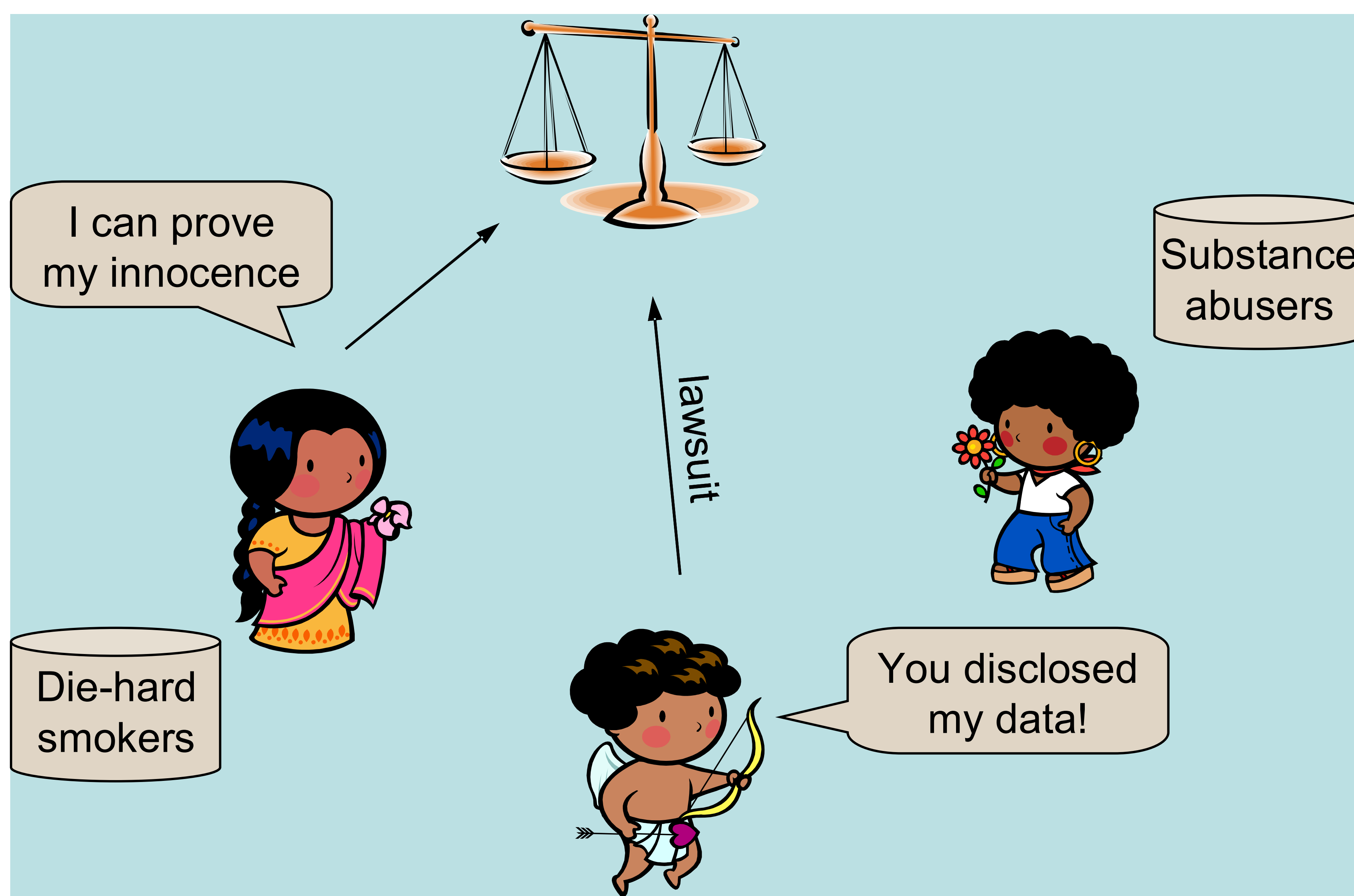
Definitions

- The **Accountable Computing**-framework
 - Collaborative Computation Framework
 - Parties are obligated to accept responsibility to participate correctly
- Privacy-preserving collaboration
 - Distributed data analysis without sharing sensitive info
 - Distributed data mining without sharing data directly
- *Objective: cheating can be detected after the fact*

Advantages

- Proving innocence
 - Alice vs. Bob
- Building trust
 - Collaboration among companies
- Spot checking
 - Regulating an industry
- Incentive driven
 - Incentive for honest behaviors

A motivating example



The story

- Alice conducted a regression analysis on her and Bob's data
- Alice was allowed to see Bob's confidential data but chose not to do so
- A year later, Carl found his personal data published on a website
- Carl came to Bob, but Bob blamed this disclosure on Alice
- Carl filed a lawsuit against Alice
- *Under the AC-framework, Alice was able to prove her innocence to the court*

Solutions developed: a protocol identifying beneficial collaborations among transportation companies; a protocol computing cardinality of set intersection
Planned work: a generic protocol based on secure circuit evaluation (SMC)