CSE 5095-007: Blockchain Technology

Lecture 15

On the Use of the Blockchain Model

Ghada Almashaqbeh

UConn - Fall 2021

Outline

- An application of the blockchain model.
    - Circumventing impossibility results.
        - Fair multiparty computation.

Motivation

- Beside the payment service that cryptocurrencies provide, their blockchains provide a useful computation model.
  - A public bulletin board.
- This allowed:
  - Building new cryptographic primitives and improve existing ones.
    - Monetary incentivised time lock puzzles.
  - Circumventing known impossibility results.
    - ***Fair MPC.***
  - Replacing strong security assumptions.
    - Used in NIZK to replace the trusted setup.

Fair Multiparty Computation

Background

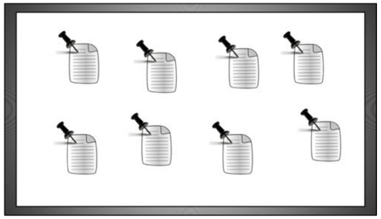
- Secure multiparty computation (SMC or MPC) allows mutually distrusted parties to compute a function on their private input while preserving the privacy of this input.
- Informally, a secure MPC protocol must achieve three security properties:
  - **Correctness:** output computed by a MPC protocol should be identical to the function output evaluated over the parties’ input in the clear.
  - **Privacy:** nothing will be revealed about a partie’s input to the other beyond what could be inferred from the output.
  - **Fairness:** either all parties obtain the output value or no one does.

Fair MPC

- Fairness in the standard model is impossible if a majority of the parties is dishonest.
- Blockchains can provide a tool to go around this impossibility.
    - Financial notion of fairness.
        - Penalty deposit, a party that aborts loses the deposit to honest parties.
    - Work in the public bulletin board model to achieve complete fairness.
        - We will explore [Choudhuri et al., 2017]
        - * slides are based on the author’s talk in CCS 2017

Complete Fairness in MPC

- Work in the public bulletin board model to achieve complete fairness.
    - All get the output or none will get it.
- A public bulletin board is:
    - Public.
    - Available (messages are permanently available).
    - Unforgeable (like it provides an unforgeable signature for every post).
- A blockchain can be used as a bulletin board.

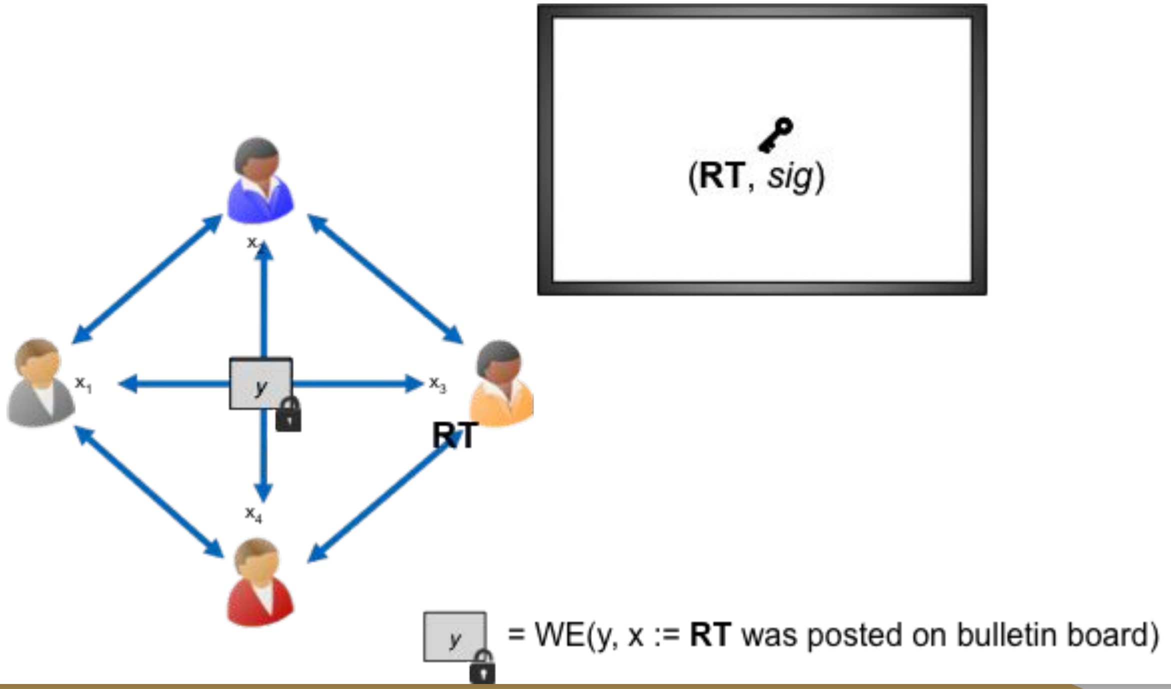


The Big Picture

- Use an unfair MPC protocol to produce a ciphertext of the function output.
- Decrypting this ciphertext needs a witness that some string, called a release token RT, has been posted on the bulletin board.
    - Reduces the problem to fair decryption.
- Since the bulletin board is public, everyone will have access to this witness and will be able to decrypt and obtain the output.
    - That is, if a corrupted party (i.e., an adversary) aborts the computation early, all what it obtains is a ciphertext of the output, not the output itself.

The Proposed Scheme I

- Use witness encryption to achieve the previous goal.
  - Instead of encrypting with a key, the output y is encrypted using a statement x.
  - The ciphertext can be only decrypted using a witness of x (which is RT together with the signature in our case).



= WE(y, x := **RT** was posted on bulletin board)

The Proposed Scheme II

- RT is posted only after finishing the unfair MPC protocol.
    - So if the adversary aborts this protocol, it will not be able to decrypt the output (and no one will).
    - If it aborts in the exchange of RT phase, it does not matter. The adversary has to post RT on the public bulletin board to decrypt the output.
- Several technical issues:
    - Security of the scheme should be based on extractable witness encryption because the statement x is always true.
    - A more efficient construction can be obtained by using trusted hardware to emulate witness encryption.

References

- [Choudhuri et al., 2017] Choudhuri, Arka Rai, Matthew Green, Abhishek Jain, Gabriel Kaptchuk, and Ian Miers. "Fairness in an unfair world: Fair multiparty computation from public bulletin boards." In CCS 2017.