Blockchains & Cryptocurrencies

Applications of Blockchains – IV
&
(Distributed) Oracles for Smart Contracts

Instructor: Abhishek Jain
Johns Hopkins University: Spring 2021

Today

1. (Yet) Another application of Blockchains
   - Witness Encryption + Blockchains: Powerful combination

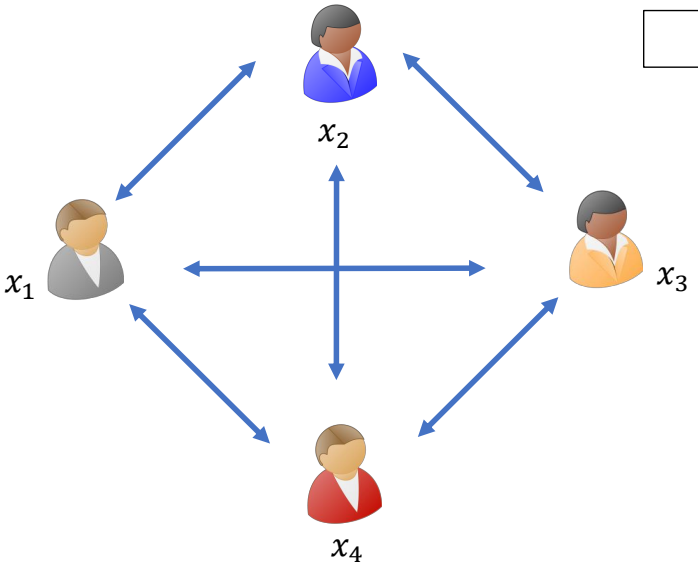
2. Oracles for Smart Contracts
   - Distributing Trust
   - Long-Term Challenges

I. Fair Multiparty Computation from Public Bulletin Boards

Arka Rai Choudhuri - Matthew Green - Abhishek Jain - Gabriel Kaptchuk - Ian Miers

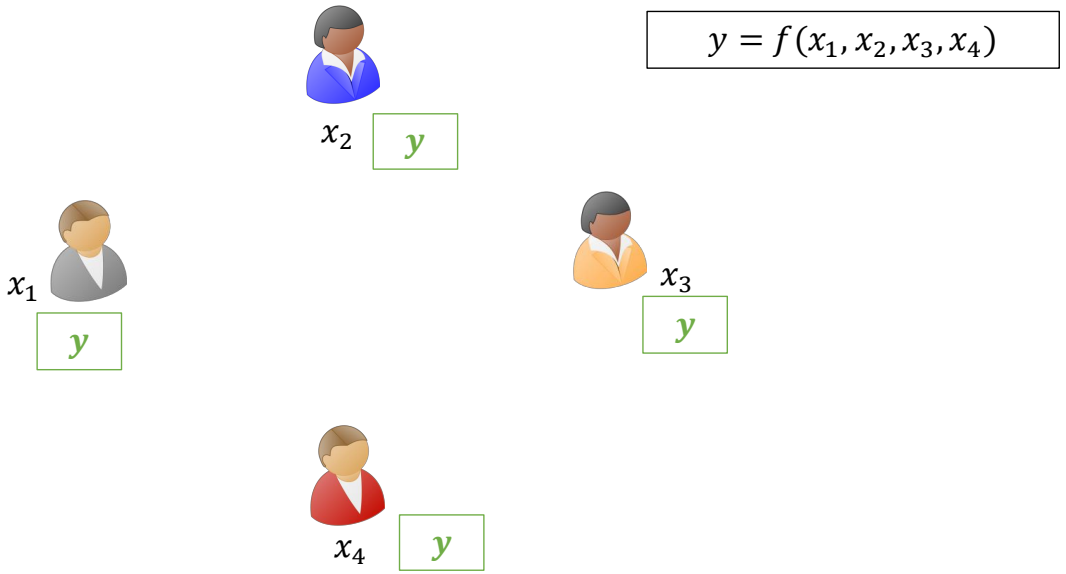
ACM CCS'17

Multi-Party Computation

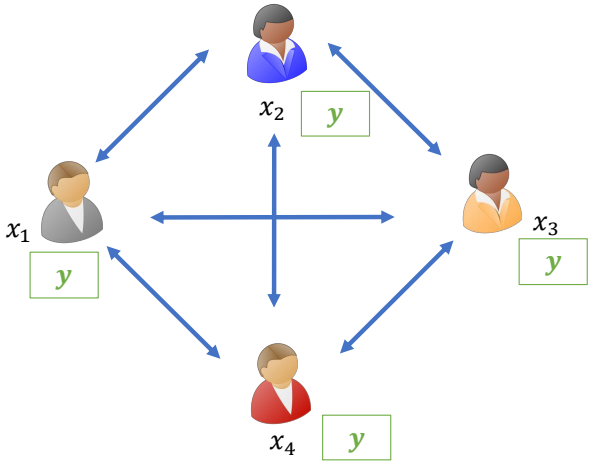


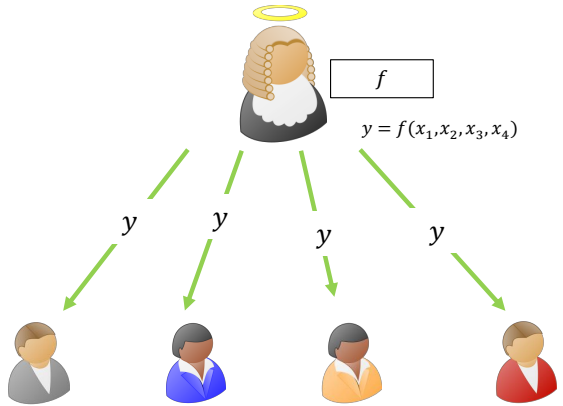
$$y = f(x_1, x_2, x_3, x_4)$$

Multi-Party Computation

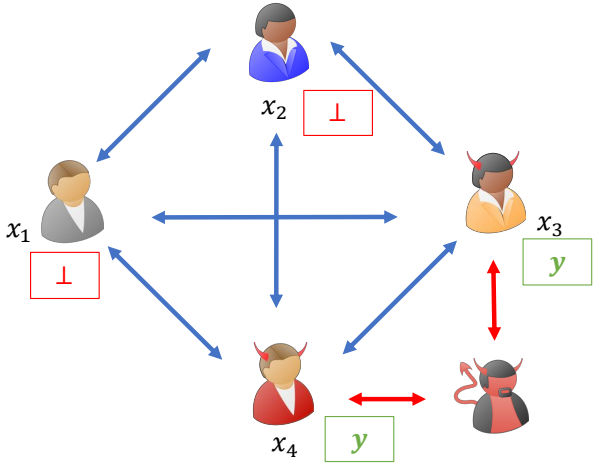


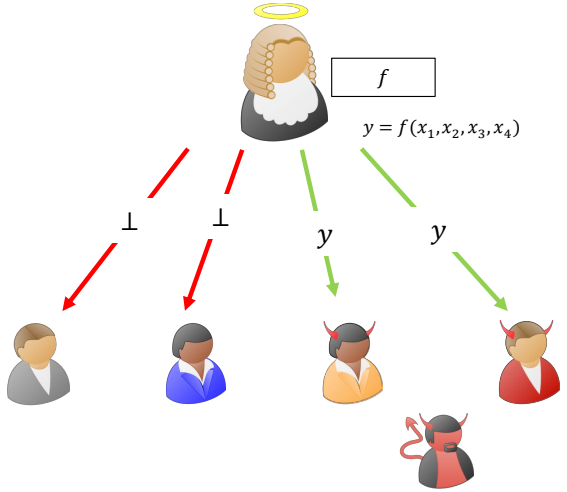
Multi-Party Computation



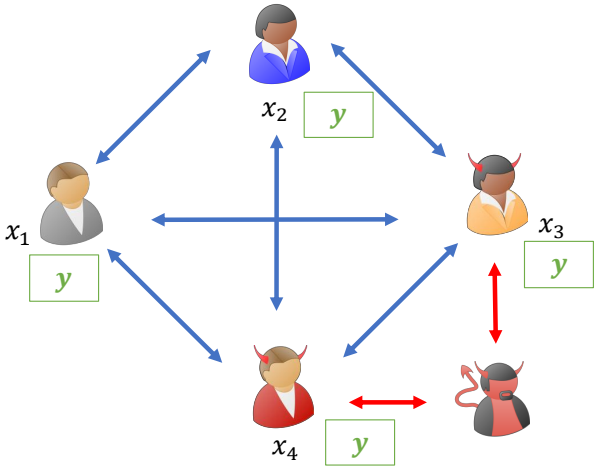


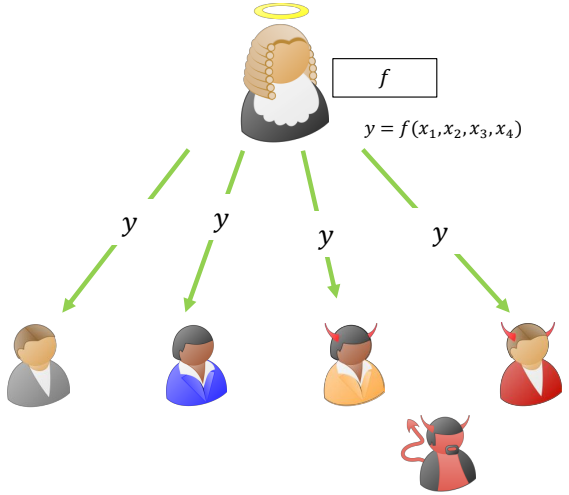
Multi-Party Computation



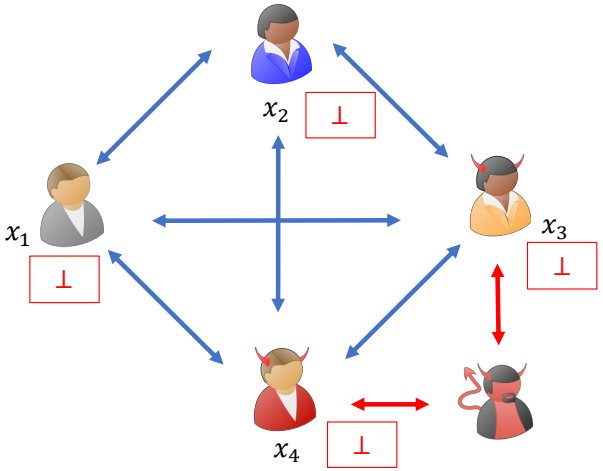


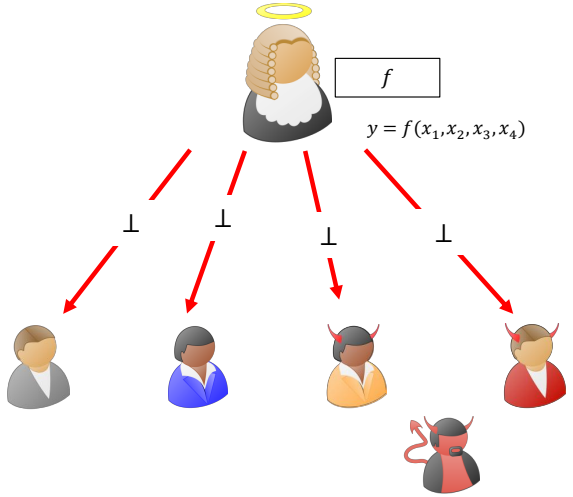
Fair Multi-Party Computation





Fair Multi-Party Computation

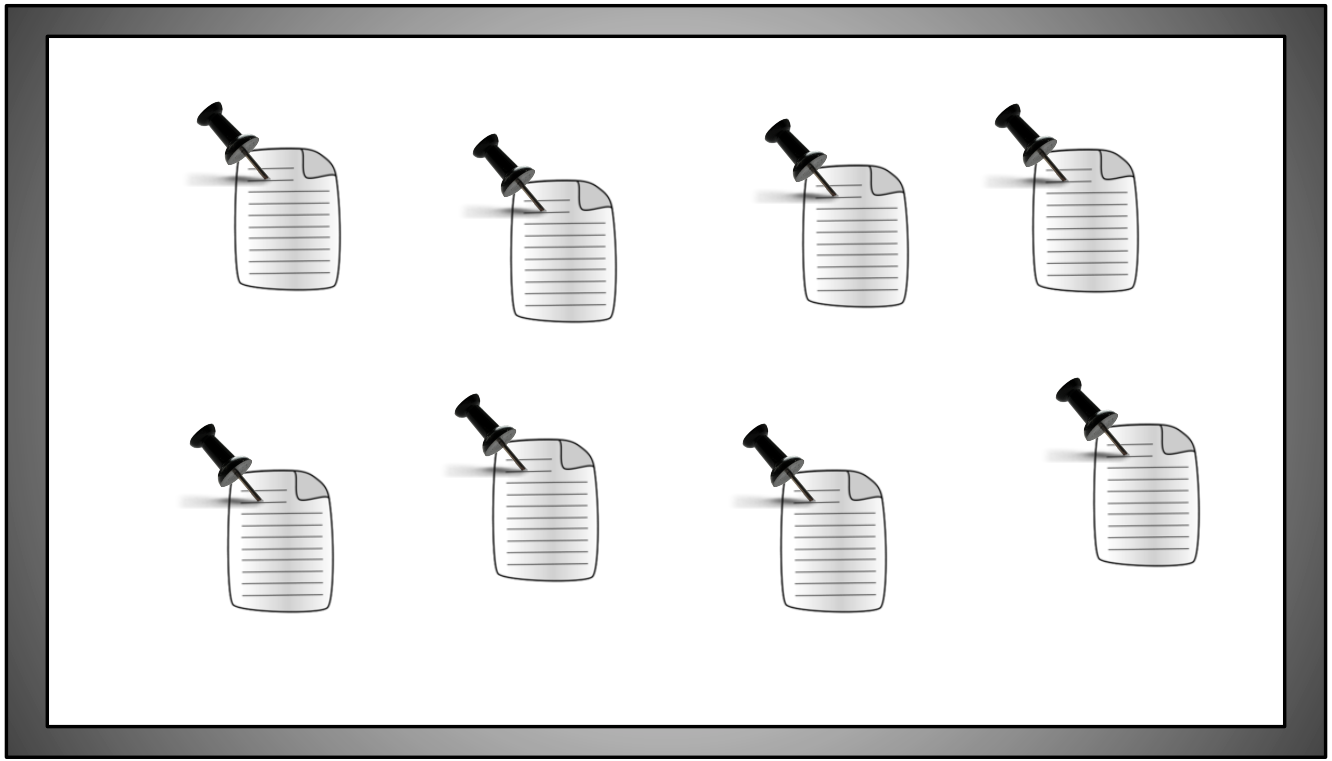




Attempts to Achieve Fairness

- General Fairness is impossible without an honest majority [Cleve 86]
- Gradual Release Mechanisms [BeaGol89, BonNao00, GarJak02]
- Restricted Class of functions [GHKL08,…]
- Fairness with Penalties [BenKum14, ADMM14] (Two Lectures Ago)
- Δ-T fairness with Trusted Hardware [PST16]

Public Bulletin Boards



Public Bulletin Boards

1. **Public:** Messages are visible to all parties

2. **Available:** Messages are permanently available (cannot be modified or deleted)

3. **Unforgeable:** No adversary can produce a “valid looking” state of the bulletin board which is different from the real state. (Can think of the bulletin board providing an unforgeable signature for every post)

Why Bulletin Boards?

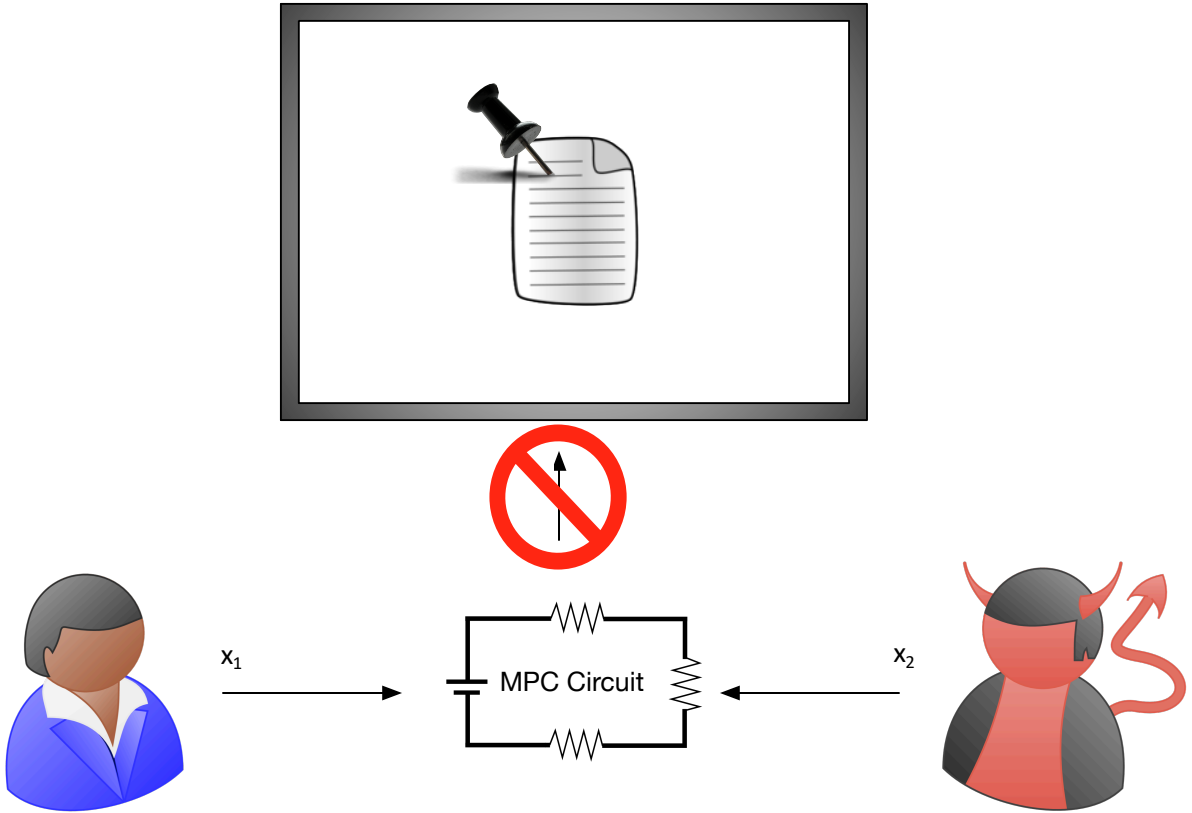
- Existing technologies can be used as bulletin boards

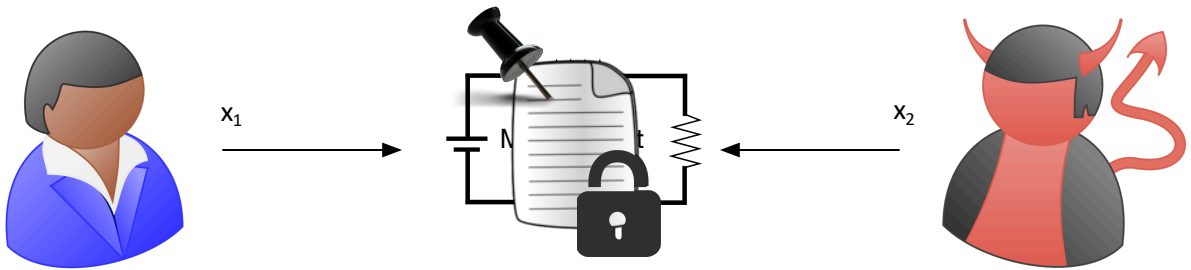
I. Proof-of-Stake based Blockchains

- Blockchain records are public and available.
- Proof-of-stake based blockchains satisfy unforgeability [Goyal-Goyal'17]

II. Google Certificate Transparency

- Can be used as an append-only public log
- Certificates present in the log can be verified by root signature.


x_1
MPC Circuit
x_2



How to Decrypt?

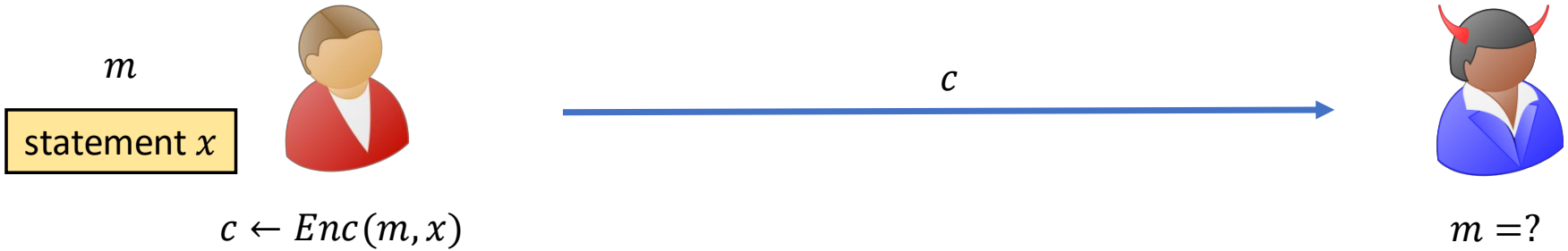
Want: Fair Decryption

- Either both the parties should be able to decrypt, or no one
- Put differently, either both parties can learn decryption key or no one can
- **Idea:** *Decryption key*: = (a release token **RT**, and bulletin board's signature on **RT**)
- But standard encryption schemes do not have such special keys!

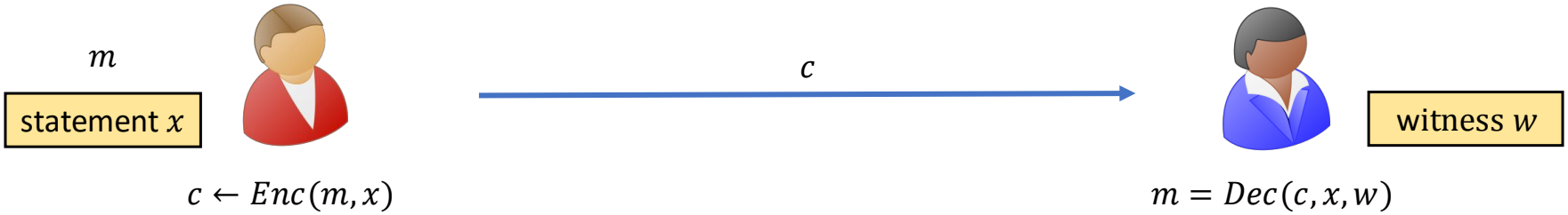
Want: “Conditional Decryption”

- Want: Ciphertexts that can only be decrypted if a certain action was implemented
- Put differently, decryption should only be possible if a statement is true
- **Problem:** Regular encryption/decryption keys are random strings (without such structure)

Witness Encryption [Garg-Gentry-Sahai-Waters'13]



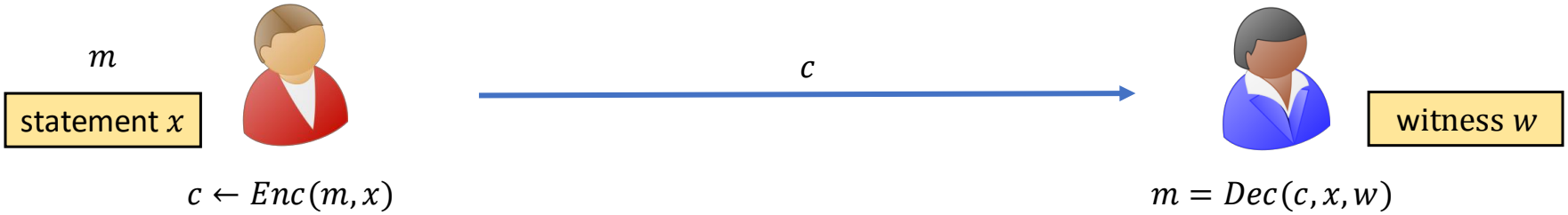
Witness Encryption [Garg-Gentry-Sahai-Waters'13]



Security: If x is "false", then Enc(m,x) is indistinguishable from Enc(m,x')

“Strong” Witness Encryption

[Goldwasser-Kalai-Popa-Vaikuntanathan-Zeldovich’13]



(Informal) Security: Enc(m,x) is indistinguishable from Enc(m,x’) even for “true” x if no efficient adversary can find a witness for x

(“Strong”) Witness Encryption

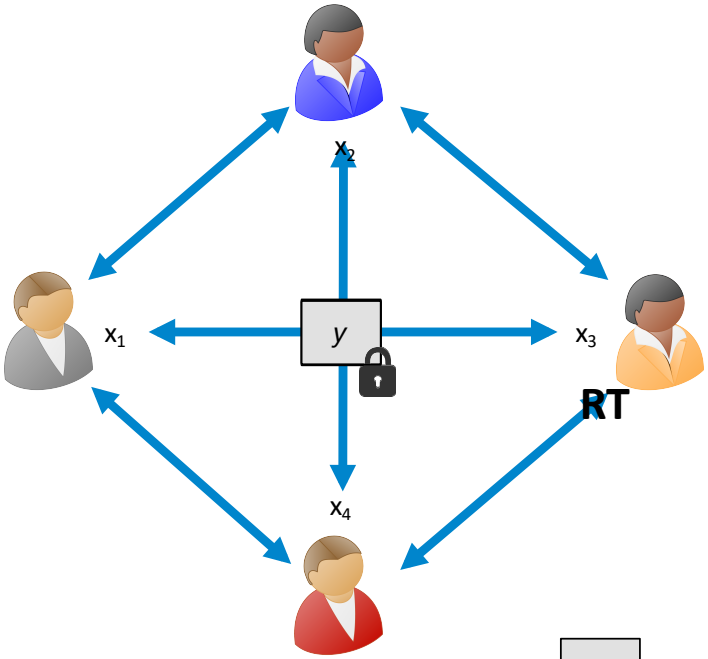
- Candidate constructions known [Garg-Gentry-Sahai-Waters’13, Gentry-Lewko-Waters’14]

- Open problem: Constructing WE from standard crytpographic assumptions

Back to Fair MPC

- **Idea:** Let's use Witness Encryption (WE) to encrypt the output

- After the initial (unfair) MPC, anyone can post a release token **RT** to the bulletin board. Then **RT**, together with signature of the bulletin board can be a "witness" for decryption



(**RT**, *sig*)

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

What is the “release token”?

- The release token **RT** is shared between the parties
- Consider two party case (for simplicity):
  - **RT** := (RT_1, RT_2) where RT_1 is chosen by P_1 and RT_2 is chosen by P_2
  - After initial (unfair) MPC, parties exchange RT_1 and RT_2 with each other
  - Now, if adversary aborts in the initial MPC, RT exchange phase will not happen, so adversary cannot learn the output
  - If adversary aborts in the **RT** exchange phase, that’s ok. In order to recover output, it must post **RT** on bulletin board, which makes it public.

Security

- **Think:** Can we base security on Witness Encryption?

- **Problem:** Statement is always true (signatures on RT "exist", just finding them without posting RT on bulletin board is "hard")

- Therefore, need **"Strong"** Witness Encryption for security (can be avoided in some special cases)

A more efficient solution

- Emulate Witness encryption using Trusted Hardware, e.g., Intel SGX

- In this case, an efficient solution can be obtained if we start from an efficient (unfair) MPC

Takeaways and Questions to ponder on

- Cryptographic Witness Encryption is “expensive” (and still not known from standard assumptions)
- Trusted Hardware is, well, trusted
- Can we simply emulate Witness encryption via a smart-contract on blockchains?
- **Main Problem:** Everything on blockchain is public. How do we store and compute on secrets?
  - In other words: How to implement **“private” smart-contracts**?

II. Chainlink

(A Decentralized Oracle Network)

Steve Ellis – Ari Juels – Sergey Nazarov

On (virtual) whiteboard