# Lecture 3: Simulation, Indistinguishability, and the Necessity of PKI

(Lecture Series on Foundations of Blockchains)

# An Impossibility Result

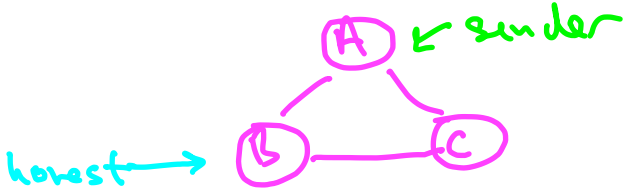
**Theorem:** [PSL80, FLM85] if $f \geq \frac{n}{3}$, no deterministic protocol for Byzantine broadcast satisfies both agreement + validity in the synchronous model.

[doesn't this contradict positive result for Dolev-Strong? - hold that thought]

**Will show:** special case of $n = 3$, $f = 1$.

(general case reduces to this case - a good HW problem)

# Some Vague Intuition



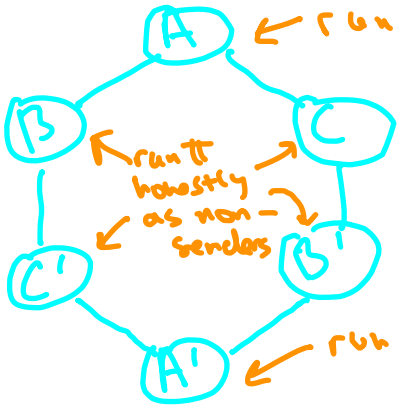

- A could be Byzantine and tell B & C conflicting things
- B & C can compare notes, but one may be Byzantine and trying to frame A
- honest node B can't distinguish which of A, C responsible for conflict

# Proof: A Thought Experiment

$n \geq 3$, $f = 1$

→ theme: simulation, indistinguishability

Let $\Pi$ be a deterministic BB protocol (satisfying validity + agreement).

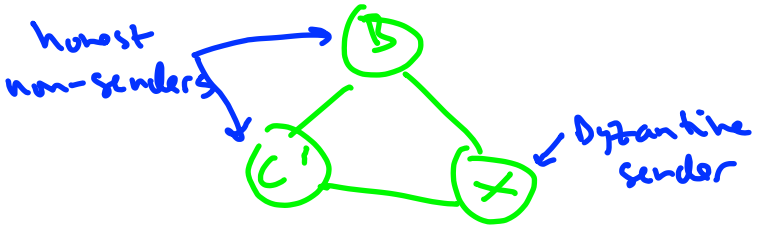


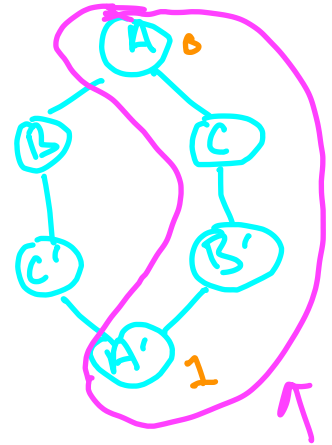

← run $\Pi$ honestly as sender, input = 0

run $\Pi$ honestly as sender, input = 1 →

**Note:** well defined. All 6 nodes eventually output 0 or 1.
(since $\Pi$ satisfies termination)

# Proof: Scenario #1



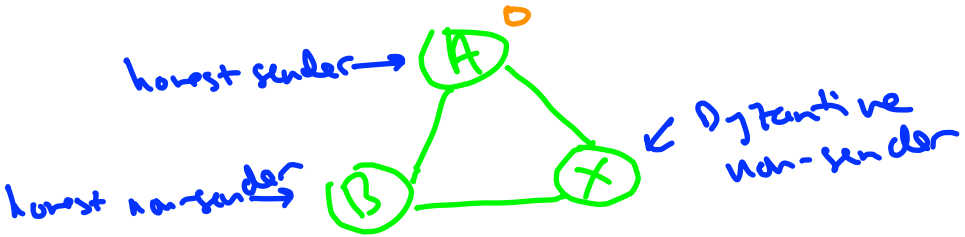

**Strategy for X:** Simulates all of A(0) — C — B' — A'(1)

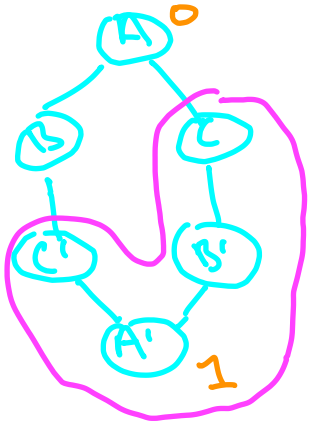
- i.e., interacts with B as A would, with C' as A' would
- Because $\Pi$ satisfies agreement, **B, C' output the same bit**

⇒ must do so also in the thought experiment

(B, C' operate identically in both cases, by construction of X's strategy)

# Proof: Scenario #2




X simulate all of these

**Strategy for X**: simulate $C' - A' - B' - C$

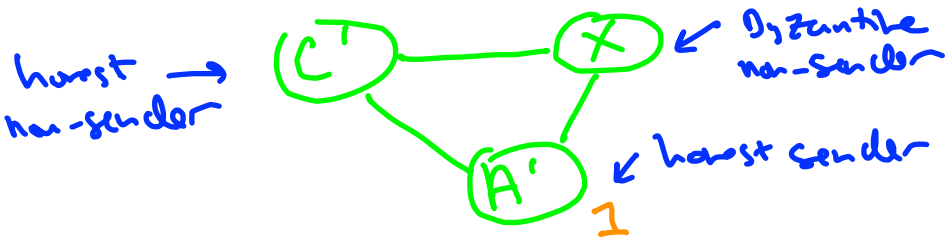
(interacts with B as if were C', with A as if were C)

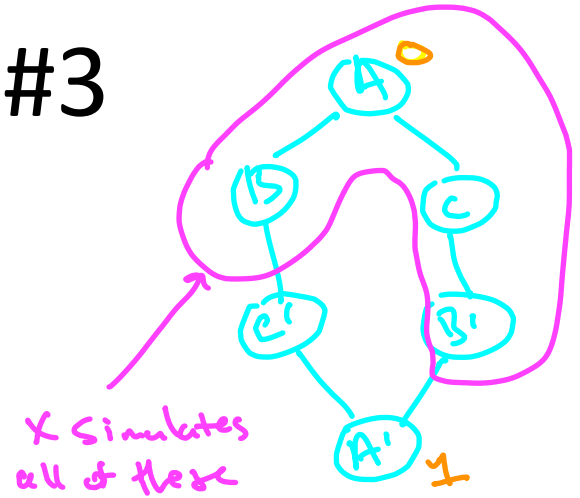
- because $\Pi$ satisfies validity, A & B both output 0

=> must do so also in the thought experiment

(A & B operate identically in both cases, by construction of X's strategy)

# Proof: Scenario #3




**Strategy for X**: Simulate B–A–C–B'

(interacts with C' as it was B in thought experiment, with A' as it were B')

- because $\Pi$ satisfies validity, A', C' both output 1.

=> must do also in the thought experiment

(by construction of X's simulation strategy)

**Note**: the 3 boxed constraints => thought experiment can't be well defined (but it is, a contradiction => $\Pi$ can't exist). BCD

# Discussion

Upshot: (crypto matters!)
PKI => get BB for all f
no PKI => get BB only if f < n/3

**Question:** why doesn't the Dolev-Strong protocol contradict this impossibility result?

**Recall:** for Dolev-Strong, assumed PKI (public key infrastructure).

**Note:** proof of impossibility results breaks down with PKI. Issues:

1. how to define thought experiment?
   => share keys between the two copies of a node
2. PKI + ideal signatures makes simulation impossible.