On the Exact Round Complexity of Secure Three-Party Computation

Arpita Patra, Divya Ravi
Indian Institute of Science

CRYPTO 2018

Our Objective

What is the *exact round complexity* of *3-party* protocols with *honest majority* under the following security notions?

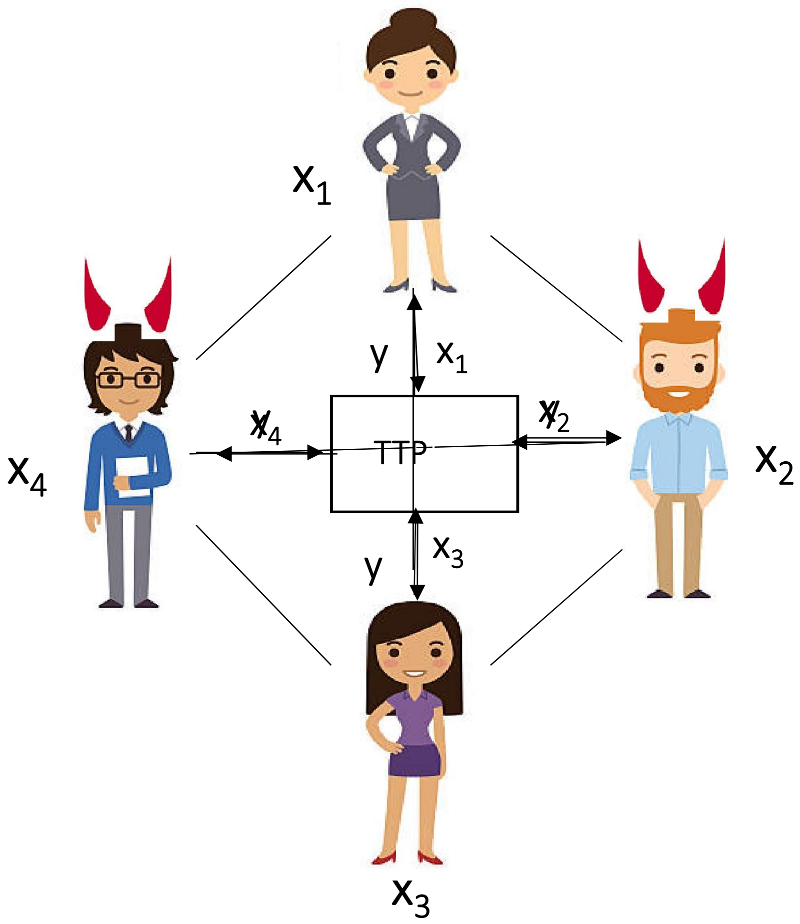
- ❑ **G**uaranteed **o**utput **d**elivery (**god**)
- ❑ Fairness (**fn**)
- ❑ Security with **u**nanimous **a**bort (**ua**)
- ❑ Security with **s**elective **a**bort (**sa**)

Goal: Complete the picture for

- point-to-point channels
- above + broadcast

Lower bounds extend for generic honest majority

MPC



Setup:

- n parties $P_1, \ldots, P_n$; t are corrupted by a centralized adv
- P_i has **private** input x_i
- A common n-input function $f(x_1, x_2, ..x_n)$

Goals:

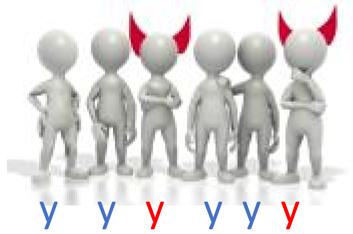
- Correctness: Compute $f(x_1, x_2, ..x_n)$
- Privacy: Nothing more than function output should be revealed

MPC: protocol that emulates TTP

Security Notions: Degree of Robustness

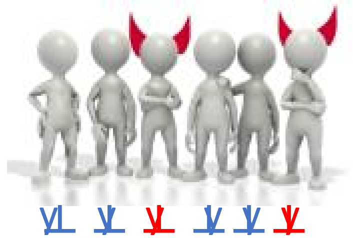
- **Guaranteed output delivery (god)** - Strongest

  Adversary cannot prevent honest parties from getting output



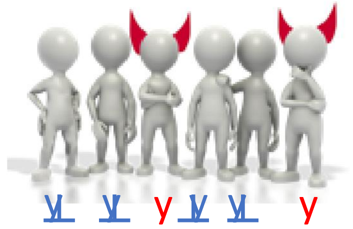
- **Fairness (fn)**

  If adversary gets output, all get the output



- **Security with unanimous abort (ua)**

  Either all or none of the honest parties get output (may be unfair)



- **Security with selective abort (sa)** - weakest

  Adversary selectively deprives some honest parties of the output

3PC with One Corruption: Why?

- **Popular setting for MPC in practice:** First Large-Scale Deployment of Danish Sugar Beet Auction, ShareMind, Secure ML

- **Strong security goals:** god and fairness only achievable in honest majority setting [Cleve86]

- **Leveraging one corruption to circumvent lower bounds:**
  + 2-round 4PC of [IKKP15] circumvents the lower-bound 3 rounds for fair MPC with $t > 1$ [GIKR02]!
  + VSS with one corruption is possible in one round!

- **Weak assumptions:** possible from OWF/P shunning PK primitives such as OT altogether

- **Lightweight constructions and better round guarantee:**

  + No cut-and-choose + 2 vs 4 in plain model with point-to-point channels

[Cleve86] Richard Cleve. Limits on the security of coin flips when half the processors are faulty (extended abstract). In ACM STOC, 1986.
[IKKP15] Yuval Ishai, Ranjit Kumaresan, Eyal Kushilevitz, and Anat Paskin-Cherniavsky. Secure computation with minimal interaction, revisited. CRYPTO, 2015.
[GIKR02] Rosario Gennaro, Yuval Ishai, Eyal Kushilevitz, and Tal Rabin. On 2-round secure multiparty computation. In CRYPTO, 2002.

The Exact Round Complexity of 3PC

	- Broadcast			+ Broadcast		
		Lower	Upper		Lower	Upper
selective abort (**sa**)	2	[HLP11]	[IKKP15]	2	[HLP11]	[IKKP15]
unanimous abort (**ua**)	3	Our Work	Our Work	2	[HLP11]	Our Work
fairness (**fn**)	3	Our Work	Our Work	3	Our Work	Our Work
Guaranteed (**god**)	Impossible	[CHOR16]	--	3	Our Work	Our Work

L1: 3 rounds are necessary for **ua** in [- broadcast]

- Implies optimality of 3PC with **sa** in terms of security

U1: 3 rounds are sufficient for **fn** in [- broadcast]

Lower bounds can be extended for any n, t with 3t > n > 2t

Upper bounds rely on (injective) OWF (garbled circuits)

L2: 3-rounds are necessary for **fn** in [+ broadcast]

- Broadcast does **not** improve round complexity
- Complements a result that fairness requires 3 rounds for t>1 and any n;

U2: 2-rounds are sufficient for **ua** in [+ broadcast]

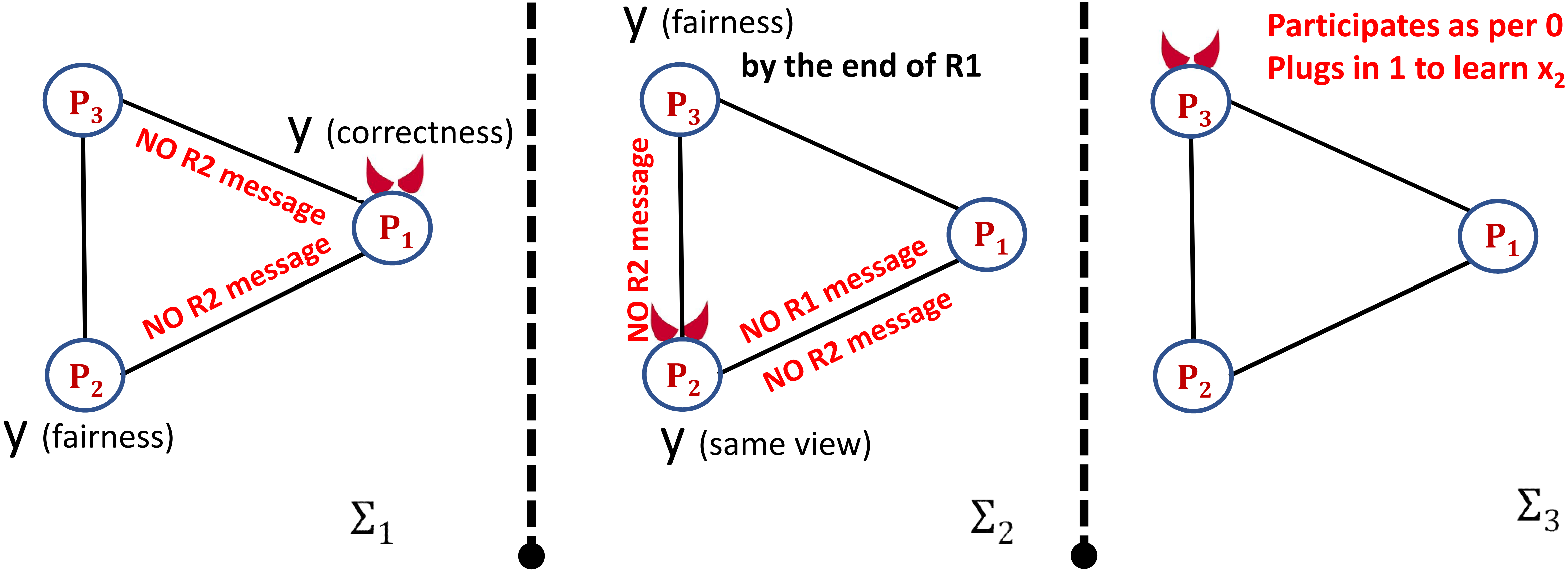
- Broadcast improves round complexity

U3: 3-rounds are sufficient for **god** in [+ broadcast]

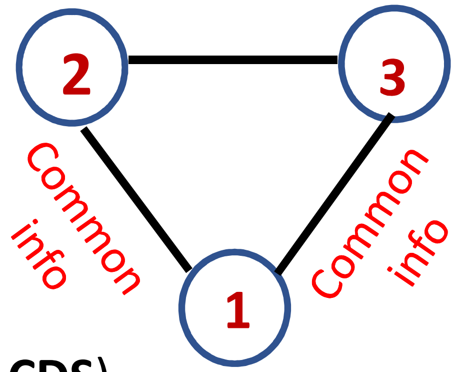
Lower Bounds (3 rounds necessary for **ua [-broadcast]** and for **fn [+broadcast]**)

Pick a special function
Assume 2-round protocol exist → Define a sequence of diff adversarial strategies → No privacy!

$$f(x_1, x_2, x_3) = \begin{cases} 1 & \text{if } x_2 = x_3 = 1 \\ 0 & \text{otherwise} \end{cases}$$



Upper Bounds: Overview and Challenges



3–round Fair protocol [-Broadcast]

- No broadcast : Conflict and confusion
- Novel mechanism : Reward honesty with **certificate** (Dual purpose)
  1) used to unlock output 2) acts as proof
- New primitive : Authenticated conditional disclosure of secret (**Authenticated- CDS**)
  via *privacy-free garbled circuits*

2–round unanimous abort [+Broadcast]

R2 private communication: Soft spot

R1 private (detect early and report in R2)

Two-part release mechanism for encoded inputs of the parties

R2 broadcast (publicly detectable)

3–round Guaranteed Output Delivery [+Broadcast]

Strong identifiability : either get output / identify corrupt by second round

Upper Bounds : Common Challenge

- Input Consistency
  - *Intra-input consistency* (Variant of “proof-of-cheating”)
  - *Inter-input consistency* (new trick with no additional overhead)

Thank You