Broadcast-Optimal 2-Round MPC

Ran Cohen Juan Garay Vassilis Zikas

Secure Multiparty Computation

Correctness

Privacy

~~Fairness~~

~~Guaranteed output delivery~~

Impossible in general for $t \geq n/2$ [Cleve'86]

This work: $t < n$

Security with Abort

Identifiable abort

All honest parties
either get output
or abort & identify corrupted parties

Unanimous abort

All honest parties
either get output or abort

Selective abort

Each honest party
either gets output or aborts

How many rounds needed for MPC?

1 round isn't enough:

Residual-function attacks [Halevi-Lindell-Pinkas'11]

2 broadcast rounds suffice:

[Asharov-Jain-LópezAlt-Tromer-Vaikuntanathan-Wichs'12]
[Garg-Gentry-Halevi-Raykova'14] [Gordon-Liu-Shi'15] [Mukherjee-Wichs'16]

Even from minimal assumptions (2-round OT):

[Garg-Srinivasan'18] [Benhamouda-Lin'18]

Optimal ???

Broadcast

+

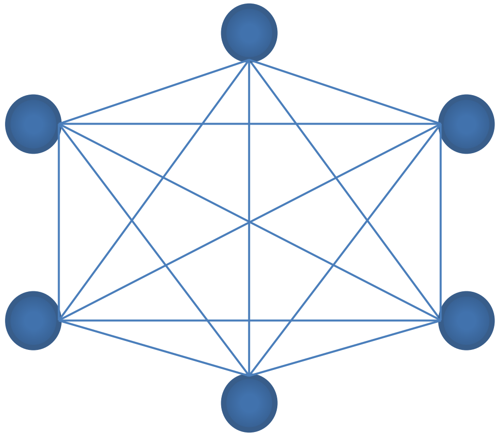
Crypto tools

Optimal !!!

Main Question

Broadcast is an expensive resource

Do we really need it??



2-Round MPC w/o Broadcast

- Lower bound in plain model (no setup):
  2-round MPC with unanimous abort $\Longrightarrow$ 2nd round must be broadcast
  For $n = 3, t = 1$ [Patra-Ravi'18]

- OWF $\Longrightarrow$ 2-round MPC with selective abort over **P2P**
  For $t < n/3$ [Ishai-Kushilevitz-Paskin'10]
  For $t < n/2$ [Ananth-Choudhuri-Goel-Jain'19] [Applebaum-Brakerski-Tsabary'19]

Our Results ($t < n$)

1st round	2nd round	Selective abort	Unanimous abort	Identifiable abort
BC	BC	✓	✓	✓
P2P	BC	✓	✓	✗
BC	P2P	✓	✗	✗
P2P	P2P	✓	✗	✗

LB: any correlated randomness
UB: 2-round OT + CRS

Part 1: Impossibility Results

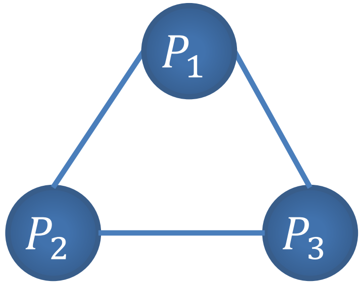
Our Results: Lower Bounds

Given any correlated randomness:

- MPC with identifiable abort $\Longrightarrow$ Both rounds BC
- MPC with unanimous abort $\Longrightarrow$ 2^{nd} round is BC

The function for the lower bound

$x_1 = (x_{1,1}, x_{1,2}) \in \{0,1\} \times \{0,1\}$



$x_2 \in \{0,1\}$

$x_3 = (x_{3,1}, x_{3,2}) \in \{0,1\}^\kappa \times \{0,1\}^\kappa$

Consider the function

$$f(x_1, x_2, x_3) = \begin{cases} (x_{1,1} \oplus x_2)^\kappa \oplus x_{3,1} & \text{if } x_{1,2} = x_2 \\ (x_{1,1} \oplus x_2)^\kappa \oplus x_{3,2} & \text{if } x_{1,2} \neq x_2 \end{cases}$$

In ideal computation of f:

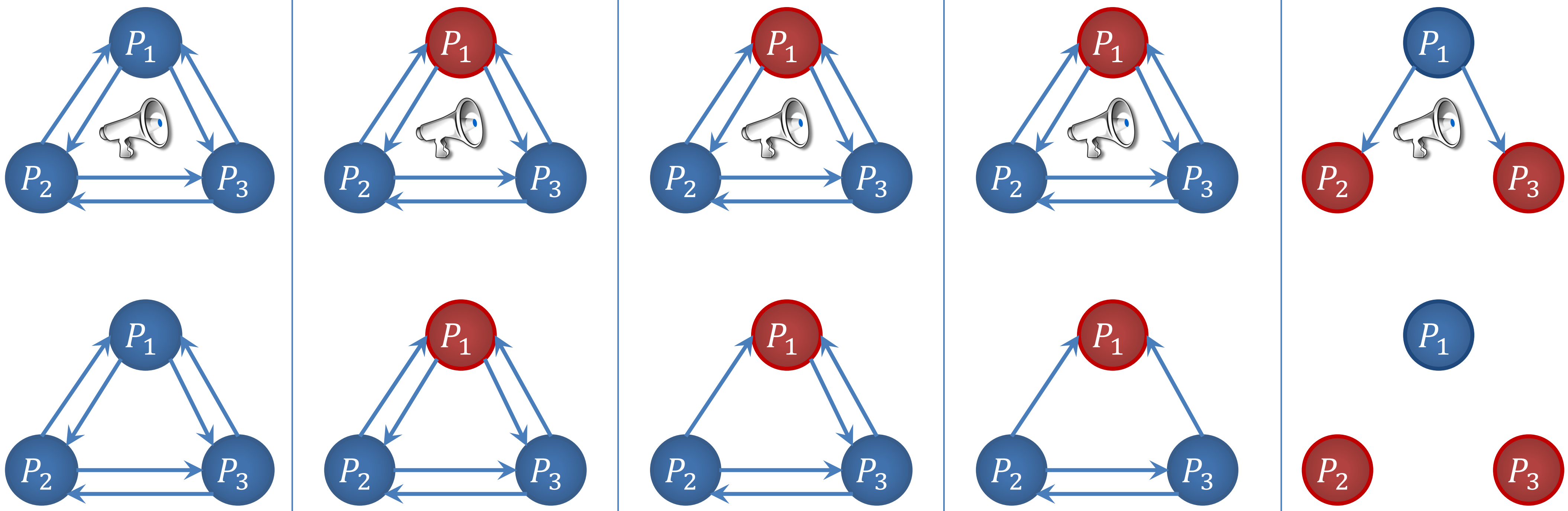
Property 1: Cheating P_2 and P_3 cannot force the output to be 0^κ

Property 2: Cheating P_1 and P_2 cannot learn both $x_{3,1}$ and $x_{3,2}$

1) Unanimous abort $\Longrightarrow$ 2^{nd} round is BC

Round 1

Round 2



Honest run: all get output

P_2, P_3 get output

P_2, P_3 get output

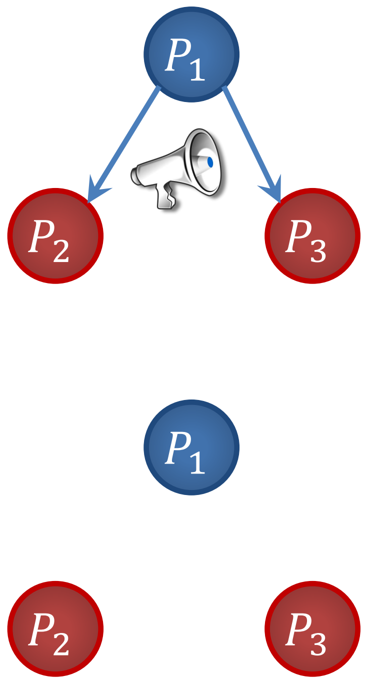
P_2, P_3 get output

1) Unanimous abort $\Longrightarrow$ 2nd round is BC

P_2, P_3 learn output from P_1's 1st message

$\Rightarrow$ P_2, P_3 can choose their input afterwards

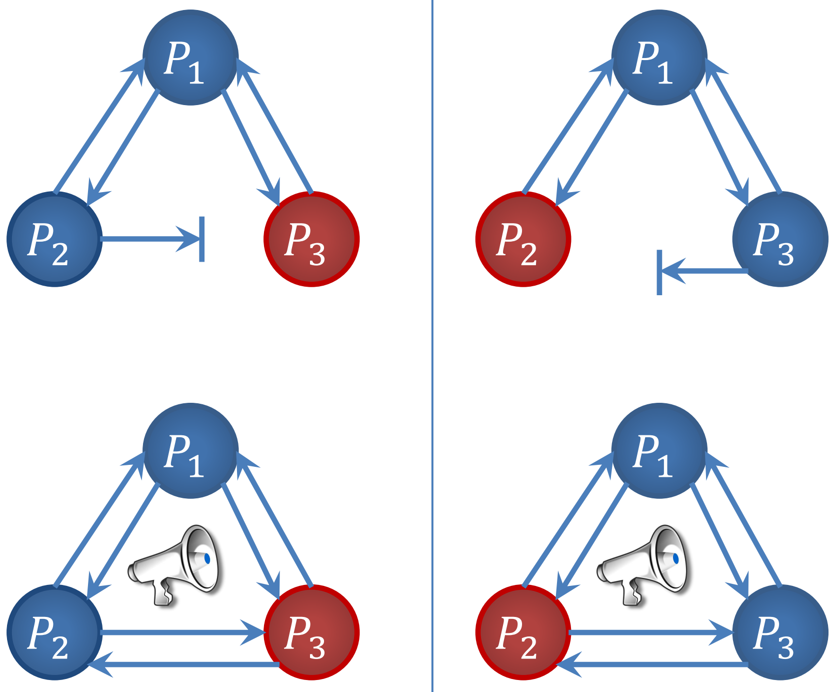
$\Rightarrow$ P_2, P_3 can force P_1's output to 0^κ



2) Identifiable abort $\Longrightarrow$ both rounds are BC

Round 1

Round 2



Attack 1

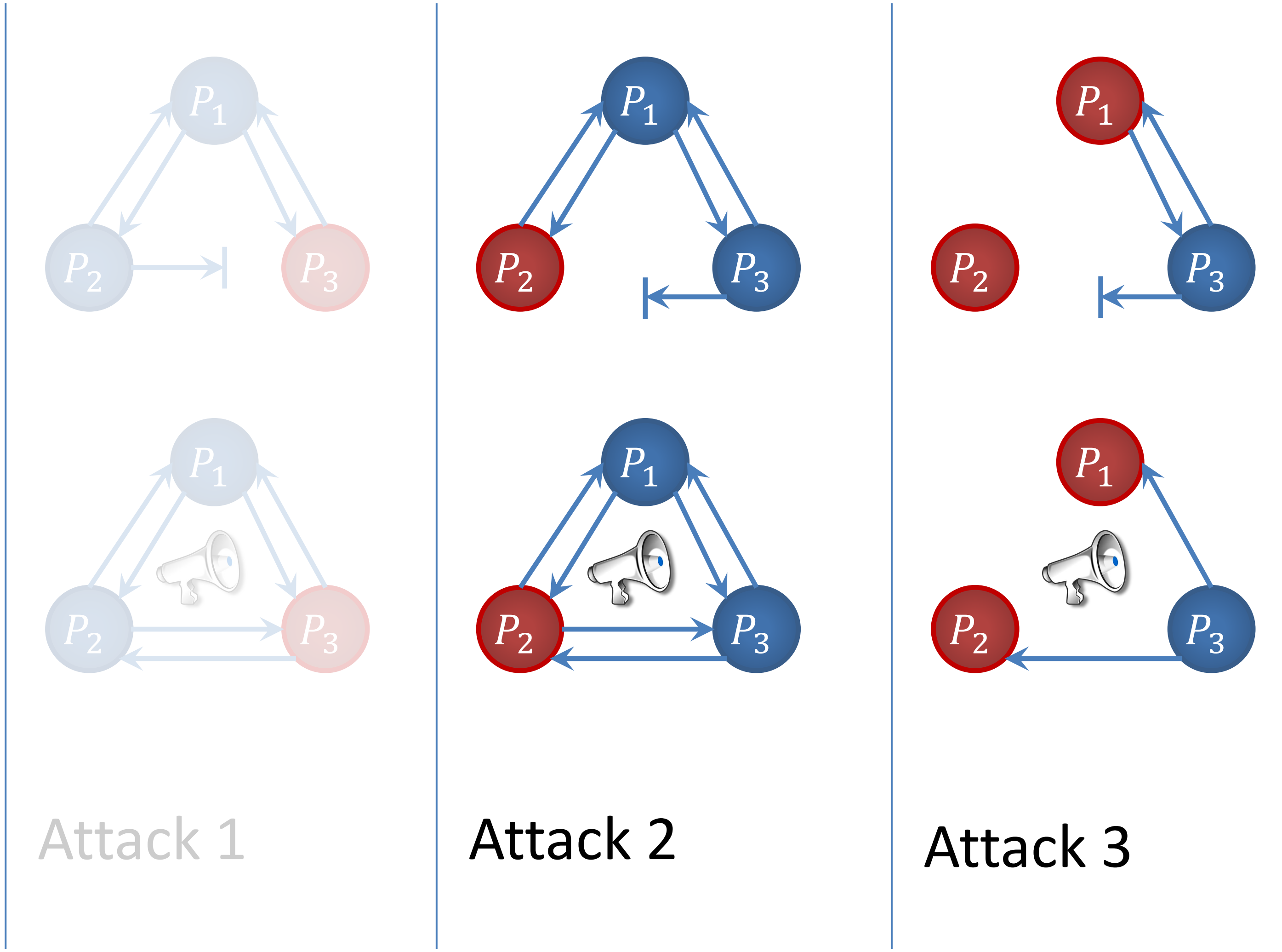
Attack 2

P_1 can't abort $\Longrightarrow$ honest parties get output

2) Identifiable abort $\Longrightarrow$ both rounds are BC

Round 1

Round 2



- Adv gets P_3's messages w/o playing P_2

$\Rightarrow$ Can play P_2 on different inputs

$\Rightarrow$ Can learn both P_3's inputs

(∗) See the paper for many missing details

P_1 can't abort $\Longrightarrow$ honest parties get output

Part 2: Feasibility Results

Our Results: Feasibility

Given 2-round OT (in CRS model):

- Both rounds BC $\Longrightarrow$ MPC with identifiable abort
- 2nd round is BC $\Longrightarrow$ MPC with unanimous abort
- Both rounds P2P $\Longrightarrow$ MPC with selective abort

Structure of 2-round protocols

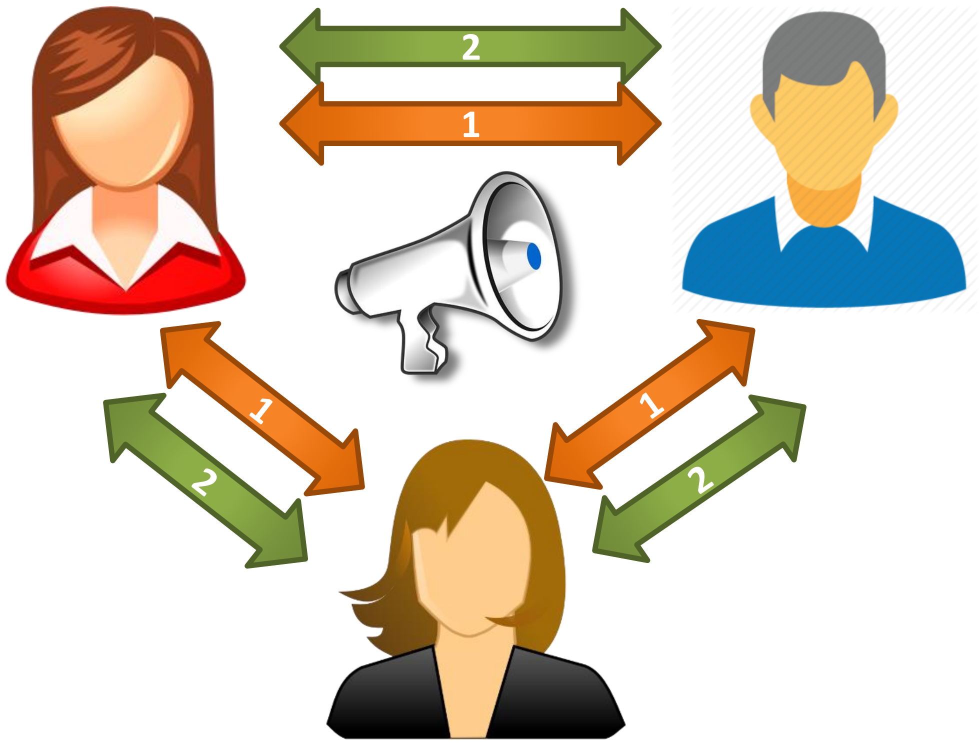
Send $m_i^1 = \text{firstmsg}(x_i, r_i)$

Receive $\vec{m}_1 = (m_1^1, \ldots, m_n^1)$

Send $m_i^2 = \text{secondmsg}(x_i, r_i, \vec{m}_1)$

Receive $\vec{m}_2 = (m_1^2, \ldots, m_n^2)$

Output $y = \text{output}(x_i, r_i, \vec{m}_1, \vec{m}_2)$



Inconsistency-detection compiler [ACGJ'19]

Round 1 (over P2P):

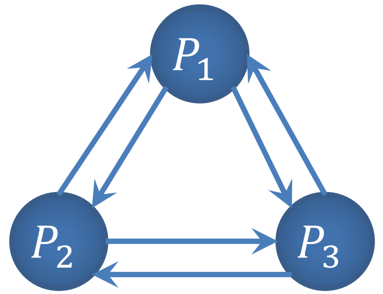
- Party P_i sends $m_i^1 = \mathrm{firstmsg}(x_i, r_i)$ to everyone
- Compute $(GC_i, LBL_i) \leftarrow$ Garble$\left(\mathrm{secondmsg}_{x_i,r_i}(\vec{m}_1)\right)$
- $\forall$ input wire w, share $lbl_i^{w,b} = lbl_{i\to 1}^{w,b} \oplus \cdots \oplus lbl_{i\to n}^{w,b}$
- $\forall$ input wire w, send $lbl_{i\to j}^{w,b}$ to P_j

Round 2 (over BC):

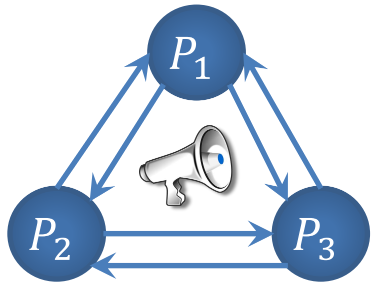
- Party P_i receives $\vec{m}_1 = (m_1^1, \ldots, m_n^1)$
- Broadcast GC_i and shares of labels corresponding to $\vec{m}_1$

Output:

- $\forall j$ party P_i reconstructs labels $LBL_j^{\vec{m}_1}$
- $\forall j$ party P_i evaluates $GC_j\left(LBL_j^{\vec{m}_1}\right)$ to obtain m_j^2
- Output $y = \mathrm{output}(x_i, r_i, \vec{m}_1, \vec{m}_2)$



Round 1



Round 2

Proof idea

- If every P_i sends the same m_i^1 to all parties

$\Longrightarrow$ All parties can reconstruct the same labels for each GC

$\Longrightarrow$ Security reduces to the original protocol

- If some P_i sent different messages $m_i^1 \neq \widetilde{m}_i^1$ to different parties

$\Longrightarrow$ No party can reconstruct the labels for GC_i

$\Longrightarrow$ All parties abort

- Similar compiler used by [ACGJ'19] (for $t < n/2$) and [GIS'18] (for semi-honest)
  Simulation used **specific properties** of the original broadcast-model protocol

- We prove for any broadcast-model protocol (**black-box simulation**)
  New **receiver-specific simulation** technique (see the paper)

- Two P2P rounds $\Longrightarrow$ selective abort

Summary

1st round	2nd round	Selective abort	Unanimous abort	Identifiable abort
BC	BC	✓	✓	✓
P2P	BC	✓	✓	✗
BC	P2P	✓	✗	✗
P2P	P2P	✓	✗	✗

Thank You