Two-Round MPC without Round Collapsing Revisited

Towards Efficient Malicious Protocols

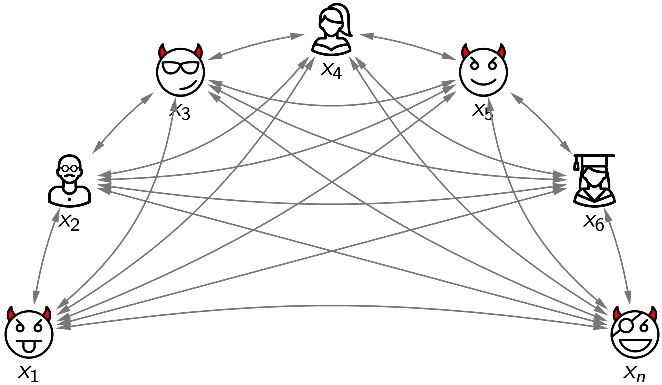
Rachel (Huijia) Lin[1] Tianren Liu[2]

[1]University of Washington, Seattle

[2]Peking University, Beijing

CRYPTO 2022

Multi-Party Computation



Everyone learns $f(x_1, \ldots, x_n)$

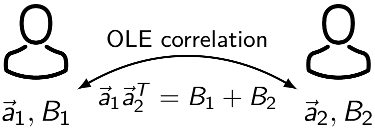
The adversary learns nothing else

Bottleneck

- Bandwidth - Communication complexity
- Latency - The number of round ≥ 2
- Runtime - Computation complexity

This Work	Previous Works

- **2-round communication**
- security w/ unanimous abort
- up to $n-1$ static corruptions
- GOAL: simplicity and efficiency
- **black-box** use of assumptions/field
- in correlated randomness model



widely used & $\exists$ PseudorandomCG

- assume PRG, RO and broadcast channel

NIZK + semi-malicious 2-round MPC

Round collapsing

[GGHR14,GP15,CGP15]
assume iO

[BL18,GS18,GIS18,BLPV18]
malicious 2-round OT

MPC in the head [IKSS21]

Expansive assumptions $\Longrightarrow$ inefficiency

Non-black-box use of the underlying assumptions $\Longrightarrow$ inefficiency

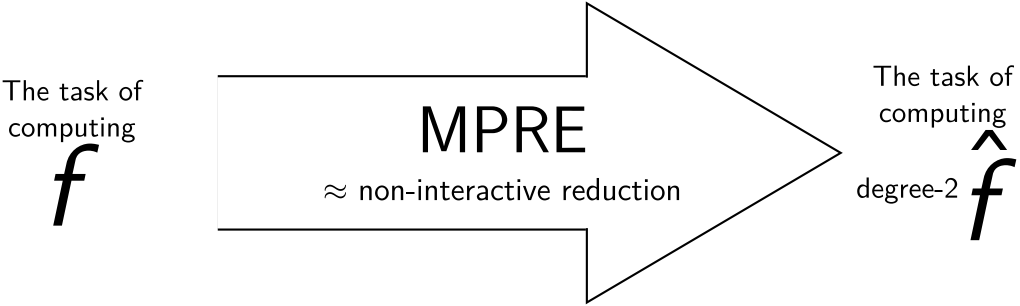
[GIS18,IKSS21] Expansive techniques $\Longrightarrow$ inefficiency

Asymptotic Complexity

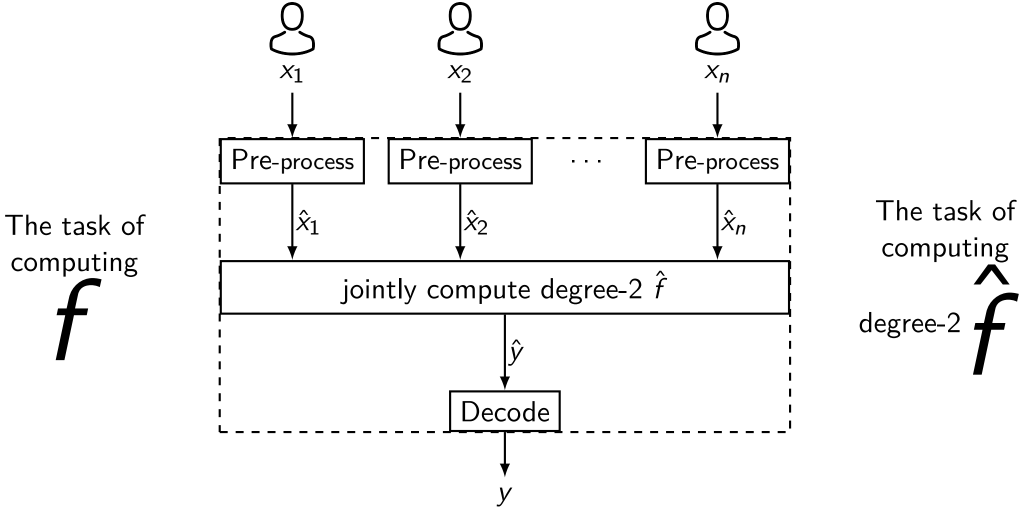
	communication complexity	assumption
[GIS18,IKSS21]	$\lvert C\rvert \cdot \text{poly}(\lambda, n)$	2-round OT
This work	$O(\lvert C\rvert \cdot \lambda \cdot n^3)$	2-party correlated randomness
Constant-round [WRK17]	$O(\lvert C\rvert \cdot \lambda \cdot n^2)$	2-party correlated randomness
Many-round [SPDZ]	$O(\lvert C\rvert \cdot \lambda \cdot n)$	n-party correlated randomness

Main Ideas

Multi-Party Randomized Encoding [Applebaum-Brakerski-Tsabary]



Multi-Party Randomized Encoding [Applebaum-Brakerski-Tsabary]



Multi-Party Randomized Encoding [Applebaum-Brakerski-Tsabary]

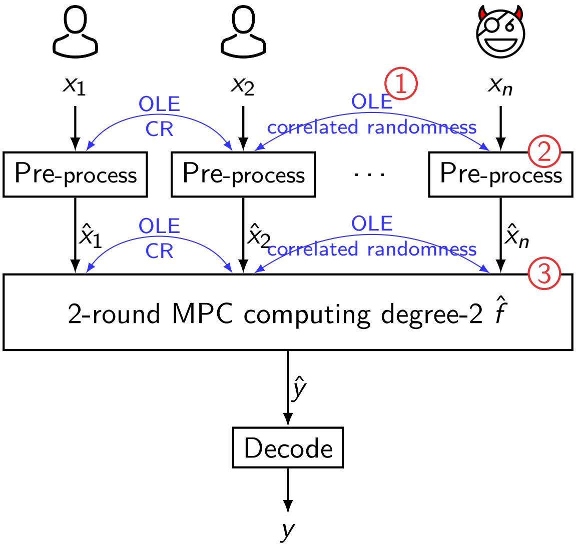
The task of computing f $=$ The task of constructing MPRE for f $+$ The task of computing degree-2 $\hat{f}$

ABT18	ABT19	LLW20	This work
semi-honest	**malicious**	**semi-honest**	**malicious**
honest-majority	**honest-majority**	**honest-minority**	**honest-minority**

ABT18
semi-honest
honest-majority

LLW20
semi-honest
honest-minority

This work
malicious
honest-minority



3 vulnerabilities:

1. correlated randomness

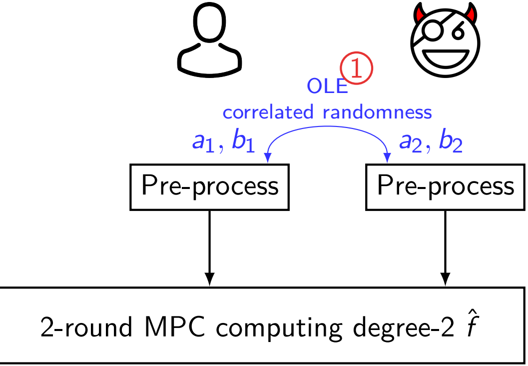
2. preprocessing

3. MPC for $\hat{f}$

Challenge:
Fix vulnerabilities w/ $O(1)$ blow-up

c.c. $= O(|C| \cdot \lambda \cdot n^3)$

Fix 1: enforce using right correlated randomness



~~To ensure $a_1 a_2 = b_1 + b_2$~~

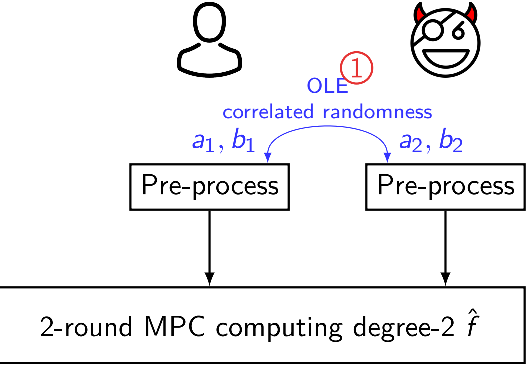
To hide info when $a_1 a_2 \neq b_1 + b_2$

First attempt:

if want to hide info when $a_1 a_2 \neq b_1 + b_2$

- samples random r
- let $\hat{f}$ output $\underbrace{r(a_1 a_2}_{\text{degree-3, cannot computed by } \hat{f}} - b_1 - b_2) + \text{info}$

Fix 1: enforce using right correlated randomness



~~To ensure $a_1 a_2 = b_1 + b_2$~~

To hide info when $a_1 a_2 \neq b_1 + b_2$

Second attempt:

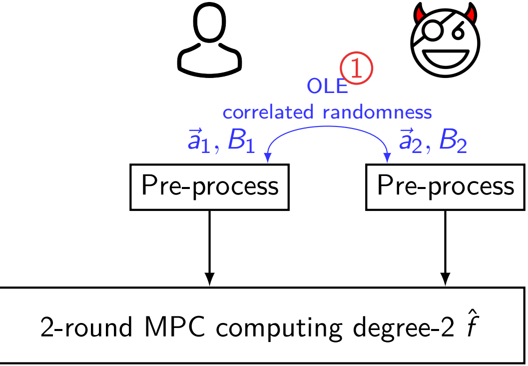
if want to hide info when $a_1 a_2 \neq b_1 + b_2$

- samples random r_1, r_2

- let $\hat{f}$ output $\begin{bmatrix} a_1 & b_1 + b_2 \\ 1 & a_2 \end{bmatrix} \begin{bmatrix} r_1 \\ r_2 \end{bmatrix} + \begin{bmatrix} info \\ 0 \end{bmatrix}$

leak a_1, a_2 if is corrupted

Fix 1: enforce using right correlated randomness



Replace scalar OLE CR by matrix OLE CR

$\vec{a}_1 \cdot \vec{a}_2^T = B_1 + B_2$

if  want to hide info when $\vec{a}_1 \cdot \vec{a}_2^T = B_1 + B_2$

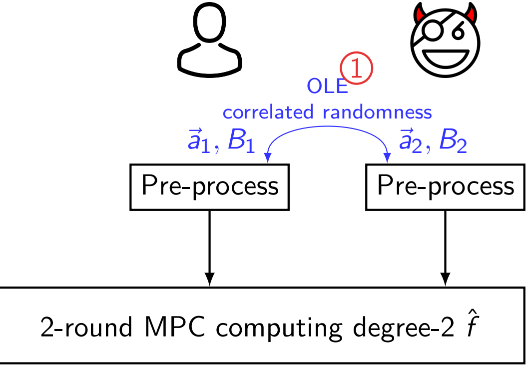
-  samples random $\vec{v}_1, \vec{v}_2$

$$\vec{a}_1 \cdot \vec{a}_2^T \neq B_1 + B_2$$

$$\overset{\text{w.h.p.}}{\Longleftrightarrow} \vec{v}_1^T \vec{a}_1 \cdot \vec{a}_2^T \vec{v}_2 \neq \vec{v}_1^T (B_1 + B_2) \vec{v}_2$$

$$\Longleftrightarrow \begin{bmatrix} \vec{v}_1^T \vec{a}_1 & \vec{v}_1^T (B_1 + B_2) \vec{v}_2 \\ 1 & \vec{a}_2^T \vec{v}_2 \end{bmatrix} \text{ full-rank}$$

Fix 1: enforce using right correlated randomness



Replace scalar OLE CR by matrix OLE CR
$\vec{a}_1 \cdot \vec{a}_2^T = B_1 + B_2$

if want to hide info when $\vec{a}_1 \cdot \vec{a}_2^T = B_1 + B_2$

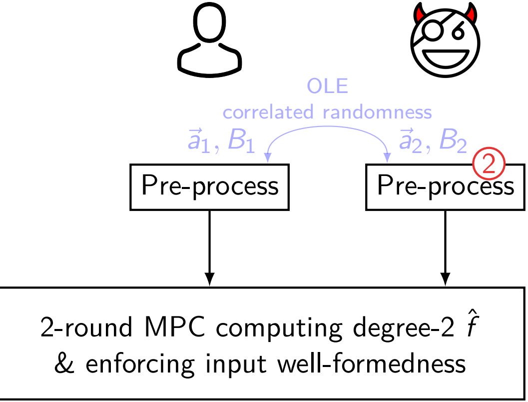
- samples random $\vec{v}_1, \vec{v}_2$
- samples random r_1, r_2
- let $\hat{f}$ output

$$\begin{bmatrix} \langle \vec{a}_1, \vec{v}_1 \rangle & \vec{v}_1^T (B_1 + B_2) \vec{v}_2 \\ 1 & \langle \vec{a}_1, \vec{v}_1 \rangle \end{bmatrix} \begin{bmatrix} r_1 \\ r_2 \end{bmatrix} + \begin{bmatrix} info \\ 0 \end{bmatrix}$$

$\vec{v}_1^T (B_1 + B_2) \vec{v}_2 r_2$ is "degree-2"
because knows $\vec{v}_1, \vec{v}_2, r_2$

leak $\langle \vec{a}_1, \vec{v}_1 \rangle, \langle \vec{a}_2, \vec{v}_2 \rangle$ if is corrupted

Fix 2: enforce honest preprocessing

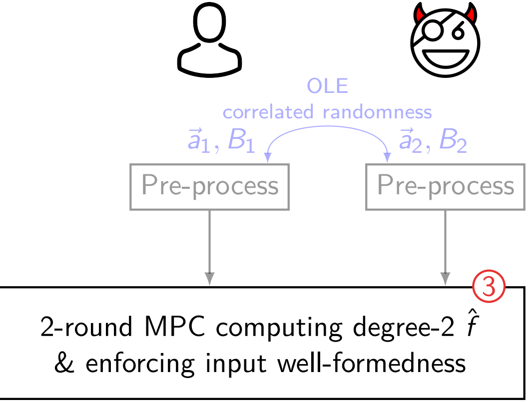


To enforce honestly preprocess . . .

. . . shirk the duty to the next slide.

Our MPRE is "semi-malicious"

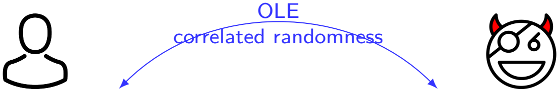
Fix 3: malicious MPC for degree-2 $\hat{f}$



Observation:
The 2-round MPC for degree-2 $\hat{f}$ in [LLW20] is "somewhat" maliciously secure.

Fix 3: malicious MPC for degree-2 $\hat{f}$

In semi-honest setting, assume w.l.o.g. $\hat{f} = x_1 x_2 + z_1 + z_2$



x_1, z_1 a_1, b_1 a_2, b_2 x_2, z_2

round 1	broadcast $c_1 = a_1 + x_1$	broadcast $c_2 = a_2 + x_2$
round 2	broadcast $m_1 = x_1 c_2 + b_1 + z_1$	broadcast $m_2 = x_2 c_1 + b_2 + z_2$
output	$m_1 + m_2 - c_1 c_2$ (which equals $x_1 x_2 + z_1 + z_2$)	

is malicious secure

- a weaker notion of security
- can be lifted to security w/ abort

c_i is a commitment of x_i

- simulate $x_i = c_i - a_i$

Fix 3: malicious MPC for degree-2 $\hat{f}$

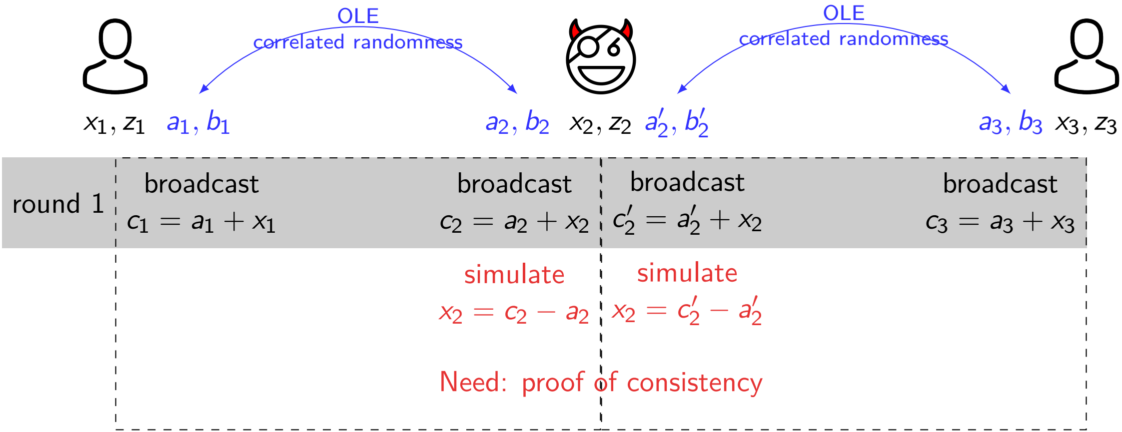
Assume w.l.o.g. every coordinate of $\hat{f}$ looks like $x_1 x_2 + z_1 + z_2$

x_1, z_1 a_1, b_1 a_2, b_2 x_2, z_2 a_2', b_2' a_3, b_3 x_3, z_3

round 1	broadcast $c_1 = a_1 + x_1$	broadcast $c_2 = a_2 + x_2$	broadcast $c_2' = a_2' + x_2$	broadcast $c_3 = a_3 + x_3$
round 2	broadcast $m_1 = x_1 c_2 + b_1 + z_1$	broadcast $m_2 = x_2 c_1 + b_2 + z_2$	broadcast $m_2' = x_2 c_3 + b_2' + z_2$	broadcast $m_3 = x_3 c_2 + b_3 + z_3$
output	$m_1 + m_2 - c_1 c_2$ (which equals $x_1 x_2 + z_1 + z_2$)		$m_2' + m_3 - c_2' c_3$ (which equals $x_2 x_3 + z_2 + z_3$)	

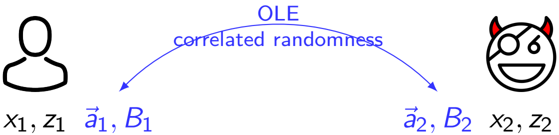
Fix 3: malicious MPC for degree-2 $\hat{f}$

Assume w.l.o.g. every coordinate of $\hat{f}$ looks like $x_1 x_2 + z_1 + z_2$



Fix 3: malicious MPC for degree-2 $\hat{f}$

Assume w.l.o.g. every coordinate of $\hat{f}$ looks like $x_1 x_2 + z_1 + z_2$



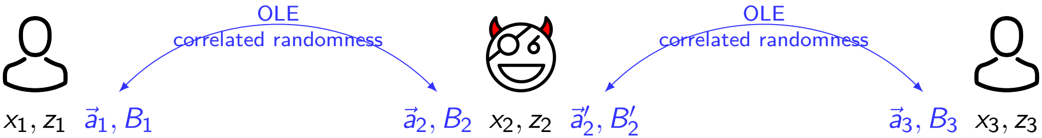
round 1		broadcast $\vec{c}_2 = \vec{a}_2 + (x_2, tail)$
round 2	broadcast random $\vec{q}$	
round 3		open $\langle \vec{q}, (x_2, tail) \rangle$

matrix OLE correlated randomness
$\vec{a}_1 \vec{a}_2^T = B_1 + B_2$

$\vec{c}_2$ allows partial (linear) opening

Fix 3: malicious MPC for degree-2 $\hat{f}$

Assume w.l.o.g. every coordinate of $\hat{f}$ looks like $x_1 x_2 + z_1 + z_2$



round 1	broadcast $\vec{c}_2 = \vec{a}_2 + (x_2, tail)$	broadcast $\vec{c}'_2 = \vec{a}'_2 + (x_2, tail)$
round 2	broadcast random $\vec{q}$	broadcast random $\vec{q}'$
round 3	open $\langle \vec{q}, (x_2, tail) \rangle, \langle \vec{q}', (x_2, tail) \rangle$	open $\langle \vec{q}, (x_2, tail) \rangle, \langle \vec{q}', (x_2, tail) \rangle$

Fix 3: malicious MPC for degree-2 $\hat{f}$

Assume w.l.o.g. every coordinate of $\hat{f}$ looks like $x_1 x_2 + z_1 + z_2$

OLE
correlated randomness

OLE
correlated randomness

x_1, z_1 $\vec{a}_1, B_1$ $\vec{a}_2, B_2$ x_2, z_2 $\vec{a}'_2, B'_2$ $\vec{a}_3, B_3$ x_3, z_3

round 1

broadcast
$\vec{c}_2 = \vec{a}_2 + (x_2, tail)$

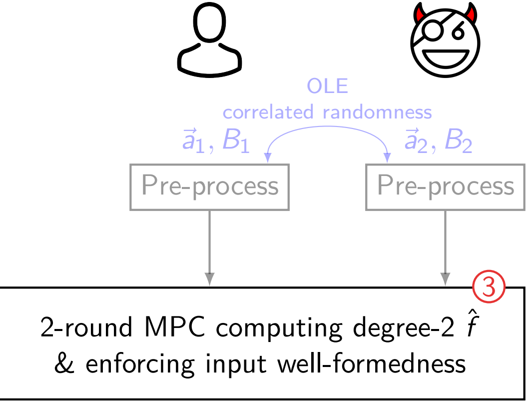
broadcast
$\vec{c}'_2 = \vec{a}'_2 + (x_2, tail)$

Fiat-Shamir
$\vec{q} \leftarrow RO(\vec{c}_2, \vec{c}'_2)$

open
$\langle \vec{q}, (x_2, tail) \rangle$

open
$\langle \vec{q}, (x_2, tail) \rangle$

Fix 3: malicious MPC for degree-2 $\hat{f}$

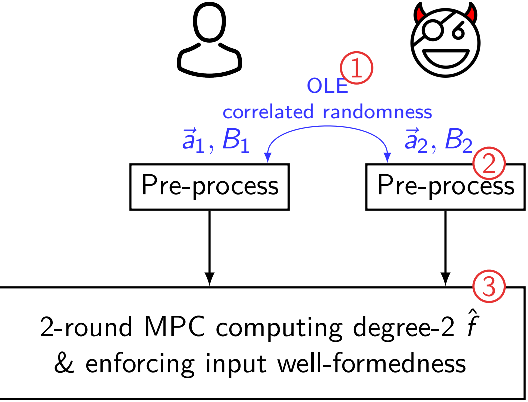


Observation:
The 2-round MPC for degree-2 $\hat{f}$ in [LLW20] is maliciously secure if output dim $= 1$.

Proof of **consistency**
assumptions: matrix OLE CR & RO
tech: linear opening, Fiat-Shamir

Proof of **well-formedness**
assumptions: matrix OLE CR & RO
tech: linear opening, Fiat-Shamir, linear proof

2-round malicious MPC for f



Semi-malicious MPRE for f

+

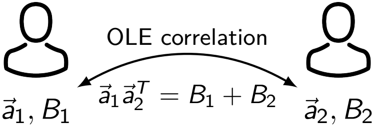
2-round MPC for $\hat{f}$
that checks well-formedness

||

2-round MPC for f

This Work

- **2-round communication**
- security w/ unanimous abort
- up to $n-1$ static corruptions
- GOAL: **simplicity and efficiency**
- **black-box** use of assumptions
- in correlated randomness model



  widely used & $\exists$ PseudorandomCG
- assume PRG, RO and broadcast channel

Towards Concrete Efficiency

- c.c. $O(|C| \cdot \lambda \cdot n^3)$ for circuit
- statistical secure MPC for arithmetic branching program, w/ black-box field access
- computation complexity $\approx$ communication complexity

Thanks for listening!