Two-Round MPC without Round Collapsing
Towards Efficient Malicious Protocols

Rachel (Huijia) Lin¹ Tianren Liu²

¹University of Washington, Seattle
²Peking 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 rounds $\geq 2$
- Runtime - Computation complexity
This Work

- 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

\\[ \vec{a}_1, B_1 \xrightarrow{\text{OLE correlation}} \vec{a}_1 \vec{a}_2^T = B_1 + B_2 \xrightarrow{\text{OLE correlation}} \vec{a}_2, B_2 \\\]

Previous Works

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 \( \implies \) inefficiency
Non-black-box use of the underlying assumptions \( \implies \) inefficiency
- [GIS18, IKSS21] Expansive techniques \( \implies \) inefficiency
## Asymptotic Complexity

<table>
<thead>
<tr>
<th></th>
<th>communication complexity</th>
<th>assumption</th>
</tr>
</thead>
<tbody>
<tr>
<td>[GIS18,IKSS21]</td>
<td>$</td>
<td>C</td>
</tr>
<tr>
<td>This work</td>
<td>$O(</td>
<td>C</td>
</tr>
<tr>
<td>Constant-round [WRK17]</td>
<td>$O(</td>
<td>C</td>
</tr>
<tr>
<td>Many-round [SPDZ]</td>
<td>$O(</td>
<td>C</td>
</tr>
</tbody>
</table>
Main Ideas
Multi-Party Randomized Encoding [Applebaum-Brakerski-Tsabary]

The task of computing $f$ $\approx$ non-interactive reduction $\approx$ The task of computing degree-2 $\hat{f}$

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

The task of computing $f$ involves the following steps:

1. Each participant $i = 1, 2, \ldots, n$ sends their input $x_i$ to the system.
2. The inputs are preprocessed to obtain estimates $\hat{x}_1, \hat{x}_2, \ldots, \hat{x}_n$.
3. The estimates are then joint-aggregated to compute a degree-2 estimate $\hat{\hat{f}}$.
4. The aggregated estimate is then decoded to produce the final output $\hat{y}$.
5. The output $\hat{y}$ is interpreted as the result of the computation $\hat{f}$. 

The flowchart illustrates these steps, with $x_i$ as inputs, $\hat{x}_i$ as pre-processed estimates, $\hat{f}$ as the joint-aggregated estimate, and $\hat{y}$ as the final output.
The task of computing $f$ is equal to the task of constructing MPRE for $f$ plus the task of computing degree-2 hat $f$.

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

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

Pre-process $a_1, b_1$ → OLE $a_1 a_2$ and $b_1 + b_2$ → Pre-process $a_2, b_2$ → 2-round MPC computing degree-2 $\hat{f}$

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 $\hat{f}$ want to hide info when $a_1 a_2 \neq b_1 + b_2$
- samples random $r$
- let $\hat{f}$ output $r(a_1 a_2 - b_1 - b_2) + \text{info}$

degree-3, cannot computed by $\hat{f}$
Fix 1: enforce using right correlated randomness

To ensure $a_1a_2 = b_1 + b_2$
To hide info when $a_1a_2 \neq b_1 + b_2$

Second attempt:
if want to hide info when $a_1a_2 \neq b_1 + b_2$
- 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

Pre-process $\vec{a}_1, B_1$ \rightarrow \text{OLE correlated randomness} \rightarrow \text{Pre-process} $\vec{a}_2, B_2$

2-round MPC computing degree-2 $\hat{f}$

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 $\vec{v}_1, \vec{v}_2$
  $\vec{a}_1 \cdot \vec{a}_2^T \neq B_1 + B_2$
  \[ \overset{\text{w.h.p.}}{\iff} \vec{v}_1^T \vec{a}_1 \cdot \vec{a}_2^T \vec{v}_2 \neq \vec{v}_1^T (B_1 + B_2) \vec{v}_2 \]
  \[ \iff \begin{bmatrix} \vec{v}_1^T \vec{a}_1 & \vec{v}_1^T (B_1 + B_2) \vec{v}_2 \\ 1 & \vec{a}_2^T \vec{v}_2 \end{bmatrix} \text{ full-rank} \]
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 \( \vec{a}_1 \cdot \vec{a}_2^T = B_1 + B_2 \)
- \( \vec{v}_1, \vec{v}_2 \) samples random
- \( r_1, r_2 \) samples random
- let \( \hat{f} \) output

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

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

leak \( \langle \vec{a}_1, \vec{v}_1 \rangle, \langle \vec{a}_2, \vec{v}_2 \rangle \) if \( \vec{v}_2 \) is corrupted
Fix 2: enforce honest preprocessing

2-round MPC computing degree-2 $\hat{f}$ & enforcing input well-formedness

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. $\hat{f} = x_1 x_2 + z_1 + z_2$

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

$c_i$ is a commitment of $x_i$
- simulate $x_i = c_i - a_i$

<table>
<thead>
<tr>
<th>round 1</th>
<th>broadcast</th>
<th>broadcast</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>$c_1 = a_1 + x_1$</td>
<td>$c_2 = a_2 + x_2$</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>round 2</th>
<th>broadcast</th>
<th>broadcast</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>$m_1 = x_1 c_2 + b_1 + z_1$</td>
<td>$m_2 = x_2 c_1 + b_2 + z_2$</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>output</th>
<th>$m_1 + m_2 - c_1 c_2$</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>(which equals $x_1 x_2 + z_1 + z_2$)</td>
</tr>
</tbody>
</table>
Fix 3: malicious MPC for degree-2 $\hat{f}$

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

<table>
<thead>
<tr>
<th>Round 1</th>
<th>Broadcast</th>
<th>Broadcast</th>
<th>Broadcast</th>
<th>Broadcast</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>$c_1 = a_1 + x_1$</td>
<td>$c_2 = a_2 + x_2$</td>
<td>$c_2' = a_2' + x_2$</td>
<td>$c_3 = a_3 + x_3$</td>
</tr>
<tr>
<td>Round 2</td>
<td>broadcast</td>
<td>broadcast</td>
<td>broadcast</td>
<td>broadcast</td>
</tr>
<tr>
<td></td>
<td>$m_1 = x_1 c_2 + b_1 + z_1$</td>
<td>$m_2 = x_2 c_1 + b_2 + z_2$</td>
<td>$m'_2 = x_2 c_3 + b'_2 + z_2$</td>
<td>$m_3 = x_3 c_2 + b_3 + z_3$</td>
</tr>
<tr>
<td>Output</td>
<td>$m_1 + m_2 - c_1 c_2$</td>
<td>$m'_2 + m_3 - c'_2 c_3$</td>
<td>(which equals $x_1 x_2 + z_1 + z_2$)</td>
<td>(which equals $x_2 x_3 + z_2 + z_3$)</td>
</tr>
</tbody>
</table>
Fix 3: malicious MPC for degree-2 $\hat{f}$

Assume w.l.o.g. every coordinate of $\hat{f}$ looks like $x_1x_2 + z_1 + z_2$

<table>
<thead>
<tr>
<th>Round 1</th>
<th>Broadcast</th>
<th>Broadcast</th>
<th>Broadcast</th>
<th>Broadcast</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>$c_1 = a_1 + x_1$</td>
<td>$c_2 = a_2 + x_2$</td>
<td>$c'_2 = a'_2 + x_2$</td>
<td>$c_3 = a_3 + x_3$</td>
</tr>
<tr>
<td></td>
<td>simulate $x_2 = c_2 - a_2$</td>
<td>simulate $x_2 = c'_2 - a'_2$</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Need: proof of consistency</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Fix 3: malicious MPC for degree-2 $\hat{f}$

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

**Diagram:**

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

**Matrix:**

Matrix $\text{OLE correlated randomness}$

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

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

round 2
- broadcast random $\vec{q}$
- broadcast random $\vec{q}'$

round 3
- open $\langle \vec{q}, (x_2, \text{tail}) \rangle, \langle \vec{q}', (x_2, \text{tail}) \rangle$
- open $\langle \vec{q}, (x_2, \text{tail}) \rangle, \langle \vec{q}', (x_2, \text{tail}) \rangle$
Fix 3: malicious MPC for degree-2 $\hat{f}$

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

\[
\text{round 1 broadcast: } \tilde{c}_2 = \tilde{a}_2 + (x_2, \text{tail}) \quad \text{broadcast: } \tilde{c}'_2 = \tilde{a}'_2 + (x_2, \text{tail})
\]

\[
\text{Fiat-Shamir: } \tilde{q} \leftarrow \text{RO}(\tilde{c}_2, \tilde{c}'_2)
\]

\[
\text{open: } \langle \tilde{q}, (x_2, \text{tail}) \rangle \quad \text{open: } \langle \tilde{q}, (x_2, \text{tail}) \rangle
\]
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
techniques: linear opening, Fiat-Shamir, linear proof
2-round malicious MPC for $f$

Pre-process $\vec{a}_1, B_1$

PRE

Pre-process $\vec{a}_2, B_2$

2-round MPC computing degree-2 $\hat{f}$ & enforcing input well-formedness

OLE

correlated randomness

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

\[
\vec{a}_1, B_1 \quad \rightarrow \quad \vec{a}_1 \vec{a}_2^T = B_1 + B_2 \quad \rightarrow \quad \vec{a}_2, B_2
\]

OLE correlation

Widely used & $\exists$ PseudorandomCG

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!