On The Round Complexity Landscape of Secure Computation

Arpita Patra
Joint work with Divya Ravi and Swati Singla

Indian Institute of Science

TPMPC 2019
Roadmap

Plain (no setup)

Honest Majority
- guaranteed output delivery (god)
- fairness (fn)

Best-of-Both-World
- god | ua
- fn | ua

P2P + BC Channel

Dishonest Majority
- unanimous abort (ua)
- selective abort (sa)

Private (CRS + PKI)

Public (CRS)
MPC

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

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

Corruption Threshold:
- Honest Majority
- Dishonest Majority
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
Best-of-Both-World (BoBW) MPC

**M1:** Protocols of one type break down in the other setting.
- A HM protocol is no longer private and correct in DM setting
- A DM protocol cannot achieve god/fn even when a single party is corrupt

**M2:** Do not care about how the adversary is going to strike. Sleep well.

**M3:** Important applications (voting, federated learning)
- Privacy violation is complete no at any cost
- Yet, guaranteed output computation is called for (as much as theoretically possible)

**Ideal Feasibility:** \( n, t, s: t < n/2 \) and \( s < n \)

- **F1:** (god | ua) \([IKLP06,K07,IKKLP11]\): \( n,t,s: t < n/2, s + t < n \) (else no polynomial time protocol exists)
  + Honest presence is stronger

- **F2:** fn | ua \([LRM10]\)

- **F3:** god | ua (s+1 residual) \([IKLP06]\)

- **F4:** god | ua (1/p security) \([K07,IKKLP11]\)

- **F5:** god | ua (semi-honest) \([IKLP06,PR19]\)
The Round Complexity Landscape

**Best-of-Both-World**

<table>
<thead>
<tr>
<th>god</th>
<th>ua</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>fn</td>
<td>ua</td>
<td>3</td>
</tr>
<tr>
<td>fn</td>
<td>ua</td>
<td>3</td>
</tr>
</tbody>
</table>

**P2P + BC Channel**

**Dishonest Majority (s < n)**

<table>
<thead>
<tr>
<th></th>
<th>Private</th>
<th>Public</th>
<th>Plain</th>
</tr>
</thead>
<tbody>
<tr>
<td>un abort (ua)</td>
<td>2</td>
<td>2</td>
<td>4*</td>
</tr>
<tr>
<td>se abort (sa)</td>
<td>2</td>
<td>2</td>
<td>4*</td>
</tr>
</tbody>
</table>

**Honest Majority (t < n/2)**

<table>
<thead>
<tr>
<th></th>
<th>Private</th>
<th>Public</th>
<th>Plain</th>
</tr>
</thead>
<tbody>
<tr>
<td>Guaranteed (god)</td>
<td>2</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>fairness (fn)</td>
<td>2</td>
<td>3</td>
<td>3</td>
</tr>
</tbody>
</table>

**LB:** r-round (fn|ua)-BoBW protocol reduces to (r-1)-round OT.

**UB:** r round ua dishonest majority implies (r+1)-round (fn|ua)-BoBW + [HH+18,BG+18]: sa → ua

[GIKR02,PR18, JLS15] [HLP12, GS18,BL18] [GMPP16, HH+18, BG+18]
The Round Complexity Landscape

**LB:** Public + 3 rounds

A) $s \leq t$: Degenerates to $n/3 \leq t \leq n/2$; [PR18]

B) $s > t$: **New LB**

### Honest Majority ($t < n/2$)

<table>
<thead>
<tr>
<th></th>
<th>Private</th>
<th>Public</th>
<th>Plain</th>
</tr>
</thead>
<tbody>
<tr>
<td>god</td>
<td>2</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>fairness</td>
<td>fn</td>
<td>2</td>
<td>3</td>
</tr>
</tbody>
</table>

### Dishonest Majority ($s < n$)

<table>
<thead>
<tr>
<th></th>
<th>Private</th>
<th>Public</th>
<th>Plain</th>
</tr>
</thead>
<tbody>
<tr>
<td>un abort</td>
<td>2</td>
<td>2</td>
<td>4</td>
</tr>
<tr>
<td>se abort</td>
<td>2</td>
<td>2</td>
<td>4</td>
</tr>
</tbody>
</table>

- Guaranteed (god)
- fairness (fn)

### Best-of-Both-World

<table>
<thead>
<tr>
<th></th>
<th>Private</th>
<th>Public</th>
<th>Plain</th>
</tr>
</thead>
<tbody>
<tr>
<td>god</td>
<td>2</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>fn</td>
<td>3</td>
<td>3</td>
<td>5</td>
</tr>
</tbody>
</table>

- LB: Public + 3 rounds
- A) $s \leq t$: Degenerates to $n/3 \leq t \leq n/2$; [PR18]
- B) $s > t$: **New LB**

References:
- [GIKR02, PR18]
- [JLS15, HLP12, GS18, BL18]
- [GMPP16, HH+18, BG+18]
The Round Complexity Landscape

**Best-of-Both-World**

<table>
<thead>
<tr>
<th></th>
<th>Private</th>
<th>Public</th>
<th>Plain</th>
</tr>
</thead>
<tbody>
<tr>
<td>god</td>
<td>2</td>
<td>3</td>
<td>4/5(?)</td>
</tr>
<tr>
<td>fn</td>
<td>3</td>
<td>3</td>
<td>5</td>
</tr>
</tbody>
</table>

**Honest Majority (t < n/2)**

- Guaranteed (god)
- fairness (fn)

<table>
<thead>
<tr>
<th></th>
<th>Private</th>
<th>Public</th>
<th>Plain</th>
</tr>
</thead>
<tbody>
<tr>
<td>god</td>
<td>2</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>fn</td>
<td>2</td>
<td>3</td>
<td>3</td>
</tr>
</tbody>
</table>

**Dishonest Majority (s < n)**

- un abort (ua)
- se abort (sa)

<table>
<thead>
<tr>
<th></th>
<th>Private</th>
<th>Public</th>
<th>Plain</th>
</tr>
</thead>
<tbody>
<tr>
<td>ua</td>
<td>2</td>
<td>2</td>
<td>4</td>
</tr>
<tr>
<td>sa</td>
<td>2</td>
<td>2</td>
<td>4</td>
</tr>
</tbody>
</table>

**UB1,2:** Series of compilers starting from a 2-round ua in DM in the BC-only setting [GS18,BL18].

**UB3:** Non-optimal (possibly) yet most challenging

[GIKR02, PR18, JLS15] [HLP12, GS18, BL18] [GMPP16, HH+18, BG+18]
The Round Complexity Landscape

Best-of-Both-World

<table>
<thead>
<tr>
<th></th>
<th>Private</th>
<th>Public</th>
<th>Plain</th>
</tr>
</thead>
<tbody>
<tr>
<td>god</td>
<td>2</td>
<td>3</td>
<td>4/5</td>
</tr>
<tr>
<td>fn</td>
<td>3</td>
<td>3</td>
<td>5</td>
</tr>
</tbody>
</table>

- Identifiability when abort
- Common random string

BoBW are not demanding $\max\{\text{DM}, \text{HM}\} + (1/0)$

Honest Majority ($t < n/2$)

<table>
<thead>
<tr>
<th></th>
<th>Private</th>
<th>Public</th>
<th>Plain</th>
</tr>
</thead>
<tbody>
<tr>
<td>Guaranteed (god)</td>
<td>2</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>fairness (fn)</td>
<td>2</td>
<td>3</td>
<td>3</td>
</tr>
</tbody>
</table>

Dishonest Majority ($s < n$)

<table>
<thead>
<tr>
<th></th>
<th>Private</th>
<th>Public</th>
<th>Plain</th>
</tr>
</thead>
<tbody>
<tr>
<td>un abort (ua)</td>
<td>2</td>
<td>2</td>
<td>4</td>
</tr>
<tr>
<td>se abort (sa)</td>
<td>2</td>
<td>2</td>
<td>4</td>
</tr>
</tbody>
</table>

[HLP12, JLS15] [GIKR02, PR18, JLS15] [GIKR02, PR18, AC+15] [HLP12, GS18, BL18] [HLP12, GS18, BL18] [GMPP16, HH+18, BG+18]
Lower Bounds for \((fn|ua)\)-BoBW MPC

Assume 4-round \((fn|ua)\) with 3 parties

\((HM)\) \(t = 1: fn\) \hspace{1cm} \((DM)\) \(s = 2: ua\)

\[
f((m_0, m_1), (c, r_2), r_3) = ((m_c + r_2 + r_3), m_c, m_c)
\]

Any \(r\)-round \((fn|ua)\)-BoBW implies \((r-1)\)-round OT

3-round OT between 2-parties

\[
f_{OT}((m_0, m_1), c) = (\bot, m_c)
\]
Lower Bounds for \( (\text{fn} | \text{ua}) - \text{BoBW} \) MPC

Assume 4-round \( (\text{fn} | \text{ua}) \) with 3 parties

\[ f((m_0, m_1), (c, r_2), r_3) = ((m_c + r_2 + r_3), m_c, m_c) \]

(HM) \( t = 1: \text{fn} \) \quad (DM) \( s = 2: \text{ua} \)

3-round OT between 2-parties

\[ f_{\text{OT}}((m_0, m_1), c) = (\bot, m_c) \]

Any \( r \)-round \( (\text{fn} | \text{ua}) - \text{BoBW} \) implies \( (r - 1) \)-round OT

C1: View\( \{P_2, P_3\} = \text{output by R3} \)

\( \Sigma_1 \)

A. Correctness: C1
B. Corrupt \( P_R: \) Case \( s = 2 \)
C. Corrupt \( P_S: \) Case \( t = 1 \)
Lower Bounds for $(fn\mid ua)$-BoBW MPC

Any $r$-round $(fn\mid ua)$-BoBW implies $(r-1)$-round OT

3-round simultaneous-message OT

3-round alternating OT

Rescheduling messages

$(m_0, m_1)$

Tolerant to rushing: An honest parties message does not depend on corrupt parties in the same round.

$P_S$ does not need output and therefore last round message of $P_R$
Upper Bounds for (fn|ua)-BoBW

Any r round ua dishonest-majority implies (i.t) (r+1)-round (fn|ua)-BoBW

Authenticated t-sharing

\[ P_1 \quad y_1 \quad M_{12} \quad M_{13} \quad M_{14} \quad M_{15} = ay_1 + b \]

r-round ua DM protocol

\[ K_{12} \quad P_2 \quad y_2 \]
\[ K_{13} \quad P_3 \quad y_3 \]
\[ K_{14} \quad P_4 \quad y_4 \]
\[ K_{15} \quad P_5 \quad y_5 \]

\( (a,b) \)
Upper Bounds for (fn|ua)-BoBW

Any r round ua dishonest-majority implies (i.t) (r+1)-round (fn|ua)-BoBW

Authenticated 2-sharing

n-party r-round ua DM protocol

Broadcast & Verify

A. (HM) t=2: fn
Upper Bounds for (fn|ua)-BoBW

Any r round ua dishonest-majority implies (i.t) (r+1)-round (fn|ua)-BoBW

Authenticated 2-sharing

Broadcast & Verify

A. (HM) t=2: fn
Upper Bounds for \((fn|ua)-BoBW\)

- **r rounds**
  - **Authenticated 2-sharing**
  - **Broadcast & Verify**

- **1 round**
  - Any r round \(ua\) dishonest-majority implies (i.t) \((r+1)\)-round \((fn|ua)-BoBW\)

**Authenticated 2-sharing**

- \(n\)-party r-round \(ua\) DM protocol

**Broadcast & Verify**

- A. (HM) \(t=2\): \(fn\)
- B. (DM) \(s=3\): \(ua?\)
Upper Bounds for \((fn|ua)\)-BoBW

Any r round \(ua\) dishonest-majority implies \((i.t) (r+1)\)-round \((fn|ua)\)-BoBW

Authenticated 2-sharing

- **P_1**
  - \(y_1\)
  - \(P_2, P_3, P_4, P_5\)

- **P_2**
  - \(y_2\)
  - \(P_1, P_3, P_4, P_5\)

- **P_3**
  - \(y_3\)
  - \(P_1, P_2, P_4, P_5\)

- **P_4**
  - \(y_4\)
  - \(P_1, P_2, P_3, P_5\)

- **P_5**
  - \(y_5\)
  - \(P_1, P_2, P_3, P_4\)

Broadcast & Verify

<table>
<thead>
<tr>
<th>y_1</th>
<th>y_2</th>
<th>y_3</th>
<th>y_4</th>
<th>y_5</th>
</tr>
</thead>
<tbody>
<tr>
<td>P_2, P_3, P_4, P_5</td>
<td>P_1, P_3, P_4, P_5</td>
<td>P_1, P_2, P_4, P_5</td>
<td>P_1, P_2, P_3, P_5</td>
<td>P_4, P_5, P_3, P_4</td>
</tr>
</tbody>
</table>

A. (HM) \(t=1\): \(fn\)

B. (DM) \(s=2\): \(ua\)?
Upper Bounds for \((fn|ua)\)-BoBW

- **n-party r-round ua DM protocol**
- **Authenticated 2-sharing**
  - \(P_1\) \(y_1\)
  - \(P_2\) \(y_2\)
  - \(P_3\) \(y_3\)
  - \(P_4\) \(y_4\)
  - \(P_5\) \(y_5\)

- **Broadcast & Verify**
  - \(y_1\)
  - \(y_2\)
  - \(y_3\)
  - \(y_4\)
  - \(y_5\)

Any r round \(ua\) dishonest-majority implies \((i.t)\) \((r+1)\)-round \((fn|ua)\)-BoBW

A. (HM) \(t=1\): \(fn\)

B. (DM) \(s=2\): \(ua?\)
Upper Bounds for \((fn|ua)\)-BoBW

Any r round \(ua\) dishonest-majority implies \((i.t)\) \((r+1)\)-round \((fn|ua)\)-BoBW

Authenticated 2-sharing [P10]

n-party r-round \(ua\) DM protocol

\[
\begin{align*}
\text{P}_1 & \quad y_1 & K_1, a_5(K_1) \\
K_{12} & \quad \text{P}_2 & y_2 & K_2, a_5(K_2) \\
K_{13} & \quad \text{P}_3 & y_3 \\
K_{14} & \quad \text{P}_4 & y_4 \\
\text{P}_5 & \quad y_5 & a_5(x), a_5(0) = y_5
\end{align*}
\]
(god|ua)-BoBW: Overview (3-round + CRS | 2-round PKI)

* Semi-malicious: Between semi-honest and malicious
  - for every round r there is an input and random coins that explains its behaviour until round r
  - Can abort
(god|ua)-BoBW: Overview (5-round + Plain)

3-round (god|ua)-BoBW
Semi-malicious
Broadcast-only

3-round (god|ua)-BoBW
Delayed-semi-malicious
Broadcast-only

BL18-like compiler

5-round (god|ua)-BoBW
Malicious
Broadcast-only

The proof was extremely challenging
Conclusion

We almost settled the exact round complexity of two (actually three) important classes of BoBW protocols.

?) 4-round (god | ua)-BoBw in Plain model?

??) Round complexity of the other class of BoBW protocols?
ברוך