Broadcast-Optimal Two Round MPC with Asynchronous Peer-to-Peer Channels

Ivan Damgård\textsuperscript{1}, Divya Ravi\textsuperscript{1,2}, Luisa Siniscalchi\textsuperscript{3}, Sophia Yakoubov\textsuperscript{1}

eprint.iacr.org/2023/1187

\textsuperscript{1}Aarhus University, \textsuperscript{2}University of Amsterdam, \textsuperscript{3}DTU
Broadcast-Optimal Two Round MPC
Broadcast-Optimal Two Round MPC
Broadcast-Optimal Two Round MPC
Broadcast-Optimal Two Round MPC

\[ y = f(x_A, x_B, x_G) \]
Broadcast-Optimal Two Round MPC

Should we read "Harry Potter" or "Alchemist" for book club?
Broadcast-Optimal Two Round MPC

\[ y = f(x_A, x_B, x_G) \]

should we read [image] or [image] for book club?
Broadcast-Optimal Two Round MPC

\[ y = f(x_A, x_B, x_G) \]

y = should we read or for book club?
Broadcast-Optimal Two Round MPC

\[ y = f(x_A, x_B, x_G) \]

- Privacy: \( t \) corrupt parties learn no additional information about honest parties’ inputs

\[ y = \text{should we read } \] or \[ \text{or } \] for book club?
Broadcast-Optimal Two Round MPC

y = should we read Harry Potter or Chips for book club?

- Privacy: t corrupt parties learn no additional information about honest parties’ inputs
- Correctness
Broadcast-Optimal Two Round MPC

- Privacy: $t$ corrupt parties learn no additional information about honest parties’ inputs
- Correctness

$y = f(x_A, x_B, x_G)$

$y = \text{should we read } \text{or } \text{for book club?}$

Stronger
Broadcast-Optimal Two Round MPC

- Privacy: $t$ corrupt parties learn no additional information about honest parties’ inputs
- Correctness
  - Selective Abort

$y = \text{should we read }$ or $\text{for book club?}$
Broadcast-Optimal Two Round MPC

- Privacy: $t$ corrupt parties learn no additional information about honest parties’ inputs
- Correctness
  - Selective Abort
  - Unanimous Abort

$y = \text{should we read }$ [Image] or [Image] for book club?
Broadcast-Optimal Two Round MPC

- Privacy: $t$ corrupt parties learn no additional information about honest parties’ inputs
- Correctness:
  - Selective Abort
  - Unanimous Abort
  - Identifiable Abort

\[ y = \text{should we read } \text{ or } \text{ for book club?} \]

Bruce did it!
Broadcast-Optimal Two Round MPC

- Privacy: $t$ corrupt parties learn no additional information about honest parties’ inputs
- Correctness:
  - Selective Abort
  - Unanimous Abort
  - Identifiable Abort
  - Guaranteed Output Delivery

$y = \text{should we read } \textit{Harry Potter} \text{ or } \textit{The Help} \text{ for book club?}$

Grace  
Bruce  
Alan  

Stronger
Broadcast-Optimal Two Round MPC
Broadcast-Optimal Two Round MPC
Broadcast-Optimal Two Round MPC
Broadcast-Optimal Two Round MPC

- Rounds are expensive!
  - At least two rounds needed for MPC
Broadcast-Optimal Two Round MPC

• Rounds are expensive!
  • At least two rounds needed for MPC
• Broadcast is expensive!
  • Takes many rounds, or
  • Uses expensive resources
Broadcast-Optimal Two Round MPC

• Rounds are expensive!
  • At least two rounds needed for MPC

• Broadcast is expensive!
  • Takes many rounds, or
  • Uses expensive resources

• Most two-round MPC:
  • Does not use broadcast *(gets weaker guarantees - e.g. selective abort)*
Broadcast-Optimal Two Round MPC

• Rounds are expensive!
  • At least two rounds needed for MPC

• Broadcast is expensive!
  • Takes many rounds, or
  • Uses expensive resources

• Most two-round MPC:
  • Does not use broadcast (gets weaker guarantees - e.g. selective abort)
  • Uses broadcast in both rounds (expensive)
broadcast-optimal two round MPC

which of the two rounds do we really need broadcast in?
Broadcast-Optimal Two Round MPC

which of the two rounds do we *really* need broadcast in?

<table>
<thead>
<tr>
<th></th>
<th>Dishonest majority</th>
<th>Honest majority</th>
</tr>
</thead>
<tbody>
<tr>
<td>PKI</td>
<td>[CGZ20]</td>
<td>[DMRSY21]</td>
</tr>
<tr>
<td>No PKI</td>
<td></td>
<td>[DRSY23]</td>
</tr>
</tbody>
</table>

PKI: public key infrastructure
Broadcast-Optimal Two Round MPC

which of the two rounds do we *really* need broadcast in?

<table>
<thead>
<tr>
<th></th>
<th>Dishonest majority</th>
<th>Honest majority</th>
</tr>
</thead>
<tbody>
<tr>
<td>PKI</td>
<td>[CG7201]</td>
<td>[DRSY23]</td>
</tr>
<tr>
<td>No PKI</td>
<td></td>
<td><em>Assumes Synchronous Channels</em></td>
</tr>
</tbody>
</table>

PKI: public key infrastructure
Synchronous communication
Synchronous communication

Guaranteed to be delivered within one round
Synchronous communication

Guaranteed to be delivered within one round

Asynchronous communication
Synchronous communication

Asynchronous communication

Guaranteed to be delivered within one round

Arbitrarily delayed by adversary
Synchronous communication

Asynchronous communication

Guaranteed to be delivered within one round

Arbitrarily delayed by adversary
Honest parties never know whether...
- message was never sent, or
- it was delayed
Broadcast-Optimal Two Round MPC with Asynchronous Peer-to-Peer Rounds

<table>
<thead>
<tr>
<th>First round</th>
<th>Second round</th>
</tr>
</thead>
<tbody>
<tr>
<td>asynchronous P2P</td>
<td>asynchronous P2P</td>
</tr>
<tr>
<td>BC</td>
<td>BC</td>
</tr>
</tbody>
</table>

impossible with standard definitions of security

well-studied
### Broadcast-Optimal Two Round MPC with Asynchronous Peer-to-Peer Rounds

<table>
<thead>
<tr>
<th>First round</th>
<th>Second round</th>
</tr>
</thead>
<tbody>
<tr>
<td>asynchronous P2P</td>
<td>asynchronous P2P</td>
</tr>
<tr>
<td></td>
<td>impossible with standard definitions of security</td>
</tr>
<tr>
<td>BC</td>
<td>BC</td>
</tr>
<tr>
<td></td>
<td>Impossible for $n \leq 2t$ (under some conditions)</td>
</tr>
<tr>
<td></td>
<td>well-studied</td>
</tr>
</tbody>
</table>
### Broadcast-Optimal Two Round MPC

**with Asynchronous Peer-to-Peer Rounds**

<table>
<thead>
<tr>
<th>First round</th>
<th>Second round</th>
</tr>
</thead>
<tbody>
<tr>
<td>asynchronous P2P</td>
<td>asynchronous P2P</td>
</tr>
</tbody>
</table>
| **impossible with standard definitions of security** | **Impossible with classical notion of asynchrony**  
We introduce a new variant! |
| BC | **Impossible for n <= 2t**  
Possible otherwise (under some conditions) | **well-studied** |
Broadcast-Optimal Two Round MPC with Asynchronous Peer-to-Peer Rounds

<table>
<thead>
<tr>
<th>First round</th>
<th>Second round</th>
</tr>
</thead>
<tbody>
<tr>
<td>asynchronous P2P</td>
<td>asynchronous P2P</td>
</tr>
<tr>
<td></td>
<td>impossible with standard definitions of security</td>
</tr>
<tr>
<td></td>
<td>Impossible with classical notion of asynchrony</td>
</tr>
<tr>
<td></td>
<td>We introduce a new variant!</td>
</tr>
<tr>
<td>BC</td>
<td>BC</td>
</tr>
<tr>
<td></td>
<td>Impossible for $n \leq 2t$</td>
</tr>
<tr>
<td></td>
<td>Possible otherwise (under some conditions)</td>
</tr>
<tr>
<td></td>
<td>well-studied</td>
</tr>
</tbody>
</table>
Impossibility of asyncP2P, BC
Impossibility of asyncP2P, BC
Impossibility of asyncP2P, BC
Impossibility of asyncP2P, BC

round 1: asyncP2P
round 2: BC
Impossibility of asyncP2P, BC

round 1: asyncP2P
round 2: BC
Impossibility of asyncP2P, BC

round 1: asyncP2P
round 2: BC

- Nothing $H$ says depends on $X_B$
Impossibility of asyncP2P, BC

round 1: asyncP2P

round 2: BC

- Nothing H says depends on $X_B$
- ... so B can swap out $X_B$ after the computation!
Impossibility of asyncP2P, BC

- Nothing H says depends on $X_B$
- ... so B can swap out $X_B$ after the computation!

**Round 1: asyncP2P**

$H(X_H)$

**Round 2: BC**

- $f(X_H, X_B)$
- $f(H(X_H), X_B')$
- residual function attack!
$(t_d, t_m)$-asynchrony
$(t_d, t_m)$-asynchrony

- Deafness threshold
- Muteness threshold
(t_d, t_m)-asynchrony
(t_d, t_m) - asynchrony

- t_d = 2

deafness threshold
muteness threshold
$(t_d, t_m)$-asynchrony

- $t_d = 2$

deafness threshold  
muteness threshold
(td, tm)-asynchrony

defauness threshold    muteness threshold

• td = 2
• tm = 1
(t_d, t_m)-asynchrony

- t_d = 2
- t_m = 1
$(t_d, t_m)$-asyncP2P, BC

with PKI

round 1: $(t_d, t_m)$-asyncP2P

round 2: BC

residual function attack!
(td,tm)-asyncP2P, BC

with PKI

round 1: (td,tm)-asyncP2P
round 2: BC

Possible as long as
 tm >= n-1,
 td >= 1

residual function attack!
(t_d,t_m)-asyncP2P, BC
with PKI

round 1: (t_d,t_m)-asyncP2P
round 2: BC

Possible as long as t_m >= n-1,
  t_d >= 1

residual function attack!
\((t_d, t_m)\)-asyncP2P, BC
with PKI

round 1: \((t_d, t_m)\)-asyncP2P
round 2: BC

Possible as long as
\(t_m \geq n-1,\) \(t_d \geq 1\)

residual function attack!
\((t_d,t_m)\)-asyncP2P, BC

with PKI

round 1: \((t_d,t_m)\)-asyncP2P

round 2: BC

Possible as long as \(t_m \geq n-t\), \(t_d \geq 1\)

residual function attack!
(t_d, t_m)-asyncP2P, BC with PKI

round 1: (t_d, t_m)-asyncP2P
round 2: BC

Possible as long as:
- t_m >= n-t, t_d >= 1

Possible as long as:
- t_m >= n-t, t_d >= 1

residual function attack!
$(t_d,t_m)$-asyncP2P, BC
with private channels

round 1: $(t_d,t_m)$-asyncP2P
round 2: BC
(t_d, t_m)-asyncP2P, BC
with private channels

round 1: (t_d, t_m)-asyncP2P
round 2: BC

f(X_{H_1}, X_{H_2}, X_C)
C(X_C)

f(X_{H_1}, X_{H_2}, X_C)
$(t_d, t_m)$-asyncP2P, BC
with private channels

round 1: $(t_d, t_m)$-asyncP2P
round 2: BC

Possible as long as
$t_m \geq (n-t)/2, \quad t_d \geq (n-t)/2$
(t_d, t_m)-asyncP2P, BC
with private channels

round 1: (t_d, t_m)-asyncP2P
round 2: BC

Possible as long as
\[ t_m \geq (n-t)/2, \quad t_d \geq (n-t)/2 \]
(t_d, t_m)-asyncP2P, BC
with private channels

round 1: (t_d, t_m)-asyncP2P
round 2: BC

Possible as long as t_m >= (n-t)/2, t_d >= (n-t)/2

residual function attack!
(t_d, t_m)-asyncP2P, BC
with private channels

round 1: (t_d, t_m)-asyncP2P
round 2: BC

Possible as long as
\( t_m \geq (n-t)/2 \),
\( t_d \geq (n-t)/2 \)

residual function attack!
\((t_d,t_m)\)-asyncP2P, BC

round 1: \((t_d,t_m)\)-asyncP2P
round 2: BC

Possible as long as
\[ t_m \geq (n-t)/2, \]
\[ t_d \geq (n-t)/2 \]
(td,tm)-asyncP2P, BC

round 1: (td,tm)-asyncP2P
round 2: BC

Possible as long as

\[ t_m \geq \frac{(n-t)}{2}, \quad t_d \geq \frac{(n-t)}{2} \]

residual function attack!
(t_d, t_m)-asyncP2P, BC

Possible as long as

round 1: (t_d, t_m)-asyncP2P
round 2: BC

Possible as long as

residual function attack!
(t_d, t_m)-asyncP2P, BC

round 1: (t_d, t_m)-asyncP2P
round 2: BC

Possible as long as $t_m + t_d \geq n-t$

residual function attack!
\((t_d, t_m)\)-asyncP2P, BC

- with PKI
- with private channels
- no PKI or private channels
\[(t_d, t_m)\text{-asyncP2P, BC}\]

- **With PKI:**
  - \(t_m\) and \(n-t\) segments.
  - \(t_d\) time period.

- **With private channels:**
  - \(t_m\), \((n-t)/2\), and \(t_d\) segments.

- **No PKI or private channels:**
  - \(t_m\), \(n-t\), and \(t_d\) segments.
$(t_d, t_m)$-asyncP2P, BC

- with PKI
- with private channels
- no PKI or private channels

- with unanimous abort (UA)
- with identifiable abort (IA)
\((t_d, t_m)\text{-asyncP2P, BC}\)

- **With unanimous abort (UA)**
  - \(n-t\) time units
  - \(n-2t\) time units
  - \(n-3t\) time units
  - With PKI

- **With identifiable abort (IA)**
  - \(n-t\) time units
  - \((n-t)/2\) time units
  - \(n-3t\) time units
  - With private channels

- **No PKI or private channels**
  - \(n-3t\) time units
  - \(n-t\) time units
  - With private channels
$(t_d, t_m)$-asyncP2P, BC

- $t_m$
  - $n-t$
    - with unanimous abort (UA)
  - $n-2t$
    - with identifiable abort (IA)

- $t_d$
  - $n-3t$
    - with PKI

- $(n-t)/2$
  - with private channels

- $n-t$
  - no PKI or private channels
(t_d,t_m)-asyncP2P, BC: Constructions

- Using tools from previous papers
  - Variants of one-or-nothing secret sharing
    - Do not support all values of t_d,t_m
- New constructions from indistinguishability obfuscation
  - New primitive: puncturable sender-public key encryption
  - Inefficient / unrealistic building blocks
Summary

• Our contributions:
  • New notion of \((t_d,t_m)\)-asynchrony
  • Impossibility results
  • Constructions