Round-Optimal Black-Box Secure Computation from Two-Round Malicious OT

Yuval Ishai, Dakshita Khurana, Amit Sahai, Akshayaram Srinivasan

Technion     UIUC     UCLA     TIFR
Multiparty Computation (MPC)

Goal: Compute $C(x_1, x_2, ..., x_6)$
Building Block: Oblivious Transfer

\[ s_0, s_1 \quad b \quad s_b \]
Progress in Understanding MPC

- Yao’82
- GMW’87
- BMR’90

Garbled Circuits:
Two round OT => Two round 2-PC

Two round OT => n round MPC
Progress in Understanding MPC

Garbled Circuits:
Two round OT =>
Two round 2-PC

Multiparty Garbling:
Two round OT =>
Two round MPC
Progress in Understanding MPC

Malicious Security in the CRS Model

Yao’82  GMW’87  BMR’90  ...  GS’18, BL’18

Garbled Circuits:
Two round OT => Two round 2-PC

Multiparty Garbling:
Two round OT => Two round MPC
Progress in Understanding MPC

Malicious Security in the CRS Model

Yao’82  GMW’87  BMR’90  ...  GS’18, BL’18

Garbled Circuits:
Two round OT =>
Two round 2-PC

Multiparty Garbling:
Two round OT =>
Two round MPC

BLACK-BOX: [IKOPS’11]  NON-BLACK-BOX
Progress in Understanding MPC

Malicious Security in the CRS Model

Garbled Circuits: Two round OT => Two round 2-PC

Two round adaptive OT => Three round MPC

BLACK-BOX: [IKOPS’11]
Progress in Understanding MPC

Malicious Security in the CRS Model

- Two round OT => Three round MPC
- Two round adaptive OT => Three round MPC

BLACK-BOX: [IKOPS’11]

BLACK-BOX
Progress in Understanding MPC

**Malicious Security in the CRS Model**

- **Garbled Circuits:**
  - Two round OT => Two round 2-PC

**BLACK-BOX:** [IKOPS’11]

- **Two round OT => Three round MPC in CRS model**
  - Matches known lower bound [ABGIS’20]
Our Results

In the common reference string (CRS) model,

- 2 round maliciously secure OT $\Rightarrow$ 3 round maliciously secure MPC
- 2 round maliciously secure OT $\Rightarrow$ 2 round 2-sided NISC
Two-Sided Non-Interactive Secure Computation (NISC)

Known result: Two-round One-sided NISC from black-box use of two-round OT [IKOPS’11]
Two-Sided Non-Interactive Secure Computation (NISC)

Known result: Two-round One-sided NISC from black-box use of two-round OT [IKOPS’11]
Two-Sided Non-Interactive Secure Computation (NISC)

\[ f(x_1, x_2) \]

1-sided NISC

1-sided NISC

\[ f(x_1, x_2) \]
Two-Sided Non-Interactive Secure Computation (NISC)

\[ f(x_1, x_2) \]

Key Technical Challenge: Ensure input consistency across executions

Use MPC-in-the-head techniques [IPS’08] to check input consistency
Quick Recap of the IPS Compiler

Outer Protocol
Quick Recap of the IPS Compiler

Malicious security against corruption of one of the clients and a constant fraction of servers [IKP 10].
Quick Recap of the IPS Compiler

\[ z_1 = S_1(x_1, y_1) \]
Semi-honest 2PC for \( S_1 \)

\[ z_2 = S_2(x_2, y_2) \]
Semi-honest 2PC for \( S_2 \)

\[ z_m = S_m(x_m, y_m) \]
Semi-honest 2PC for \( S_m \)

\[ \text{Inner Protocols} \]

\[ \text{Dec}(z_1, \ldots, z_m) \]

\[ \text{Dec}(z_1, \ldots, z_m) \]
Quick Recap of the IPS Compiler

Need to ensure that adversary only cheats in a constant fraction
Quick Recap of the IPS Compiler

\[ z_1 = S_1(x_1, y_1) \]

\[ z_2 = S_2(x_2, y_2) \]

\[ z_m = S_m(x_m, y_m) \]

\[ x \]

\[ y \]

Dec (z₁, ..., zₘ)

Dec (z₁, ..., zₘ)

Semi-honest 2PC for S₁

Semi-honest 2PC for S₂

Semi-honest 2PC for Sₘ

Inner Protocols

WATCHLISTS:
Cut-and-choose checks on a random subset of inner protocols

Need to ensure that adversary only cheats in a constant fraction
Specific choice of inner protocol and watchlists

• Inner Protocol should satisfy an additional output equivocality property
  • Two-sided NISC: Any one-sided NISC (which can be based on OT [IKOPS’11]) Alternatively Garbled circuits + OT
  • MPC: Robust MPC building on [PS’21]
Specific choice of inner protocol and watchlists

• Inner Protocol should satisfy an additional output equivocality property
  • Two-sided NISC: Any one-sided NISC (which can be based on OT [IKOPS’11]) Alternatively Garbled circuits + OT
  • MPC: Robust MPC building on [PS’21]

• Watchlist mechanism should allow the simulator to decide and program which executions will be watched by malicious parties
  • Build this using ideas from [IKOPS’11]
Another Perspective

• Start with simple round-optimal realizations that BB use *semi-honest OT*
  *semi-honest 2-sided NISC* (Garbled circuits + OT)
  *semi-honest MPC* [PS’21]
Another Perspective

• Start with simple round-optimal realizations that BB use *semi-honest OT*
  *semi-honest 2-sided NISC* (Garbled circuits + OT)
  *semi-honest MPC* [PS’21]

• Plug in maliciously secure OT

• The result is an inner protocol, which is bootstrapped to full malicious security via the IPS compiler
Open Questions

• Obtain our results from BB use of two-round semi-honest OT

• Base 3 round MPC on 3 round maliciously secure OT

• Can similar results be obtained in the OT-hybrid model?