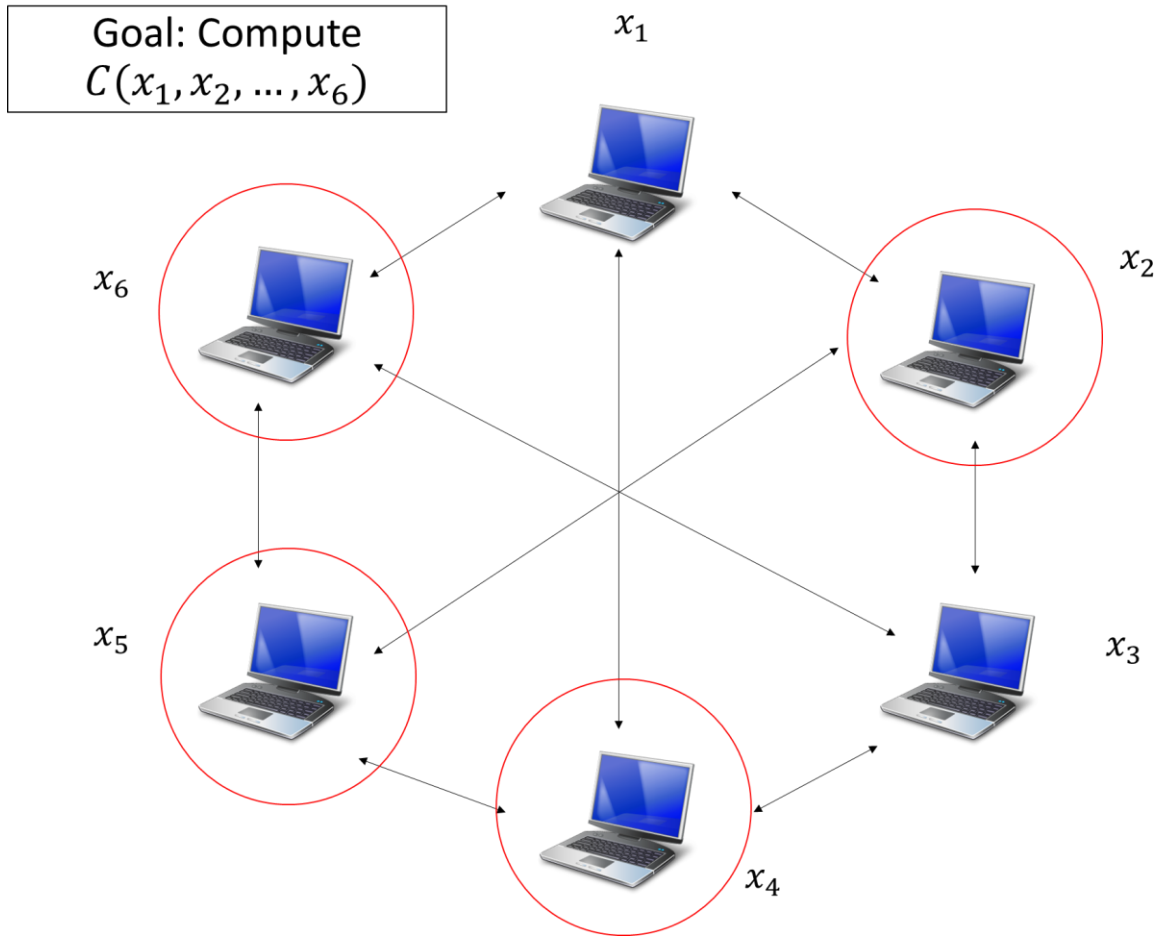
Round-Optimal Black-Box Secure Computation from Two-Round Malicious OT

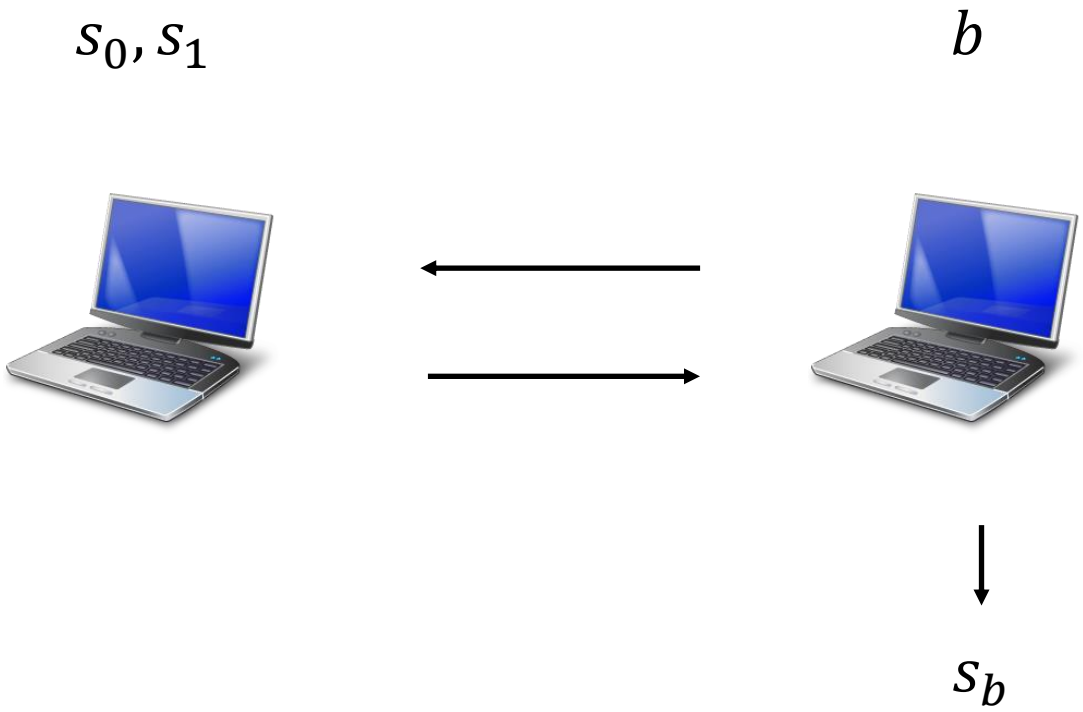
Yuval Ishai, Dakshita Khurana, Amit Sahai, Akshayaram Srinivasan

Technion UIUC UCLA TIFR

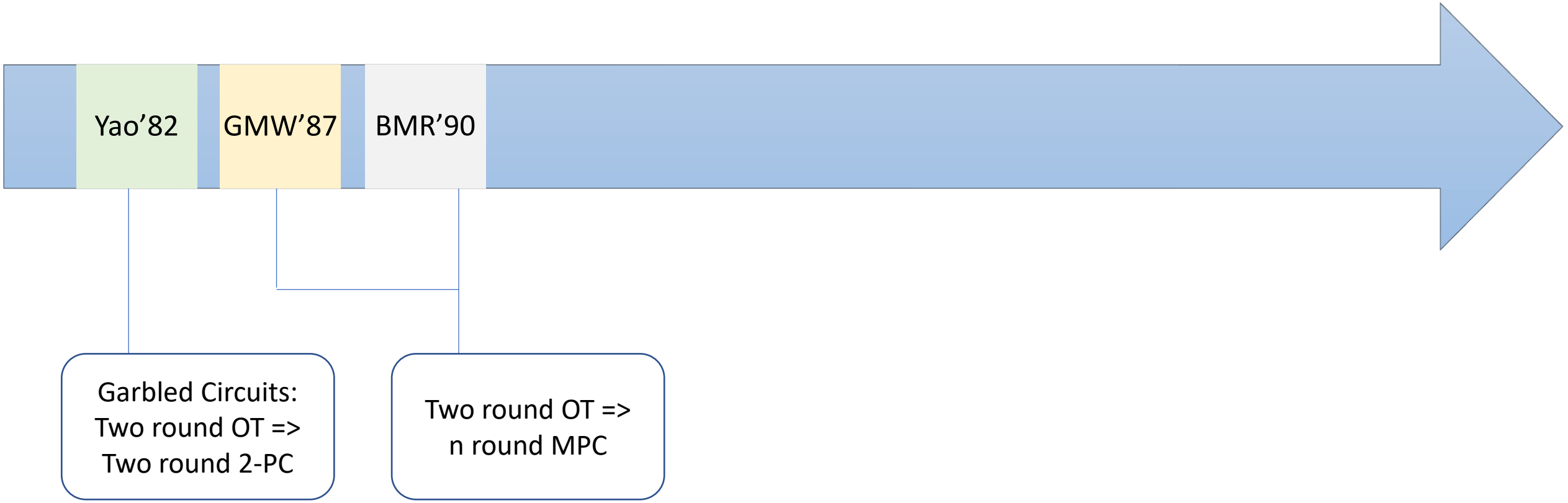
Multiparty Computation (MPC)



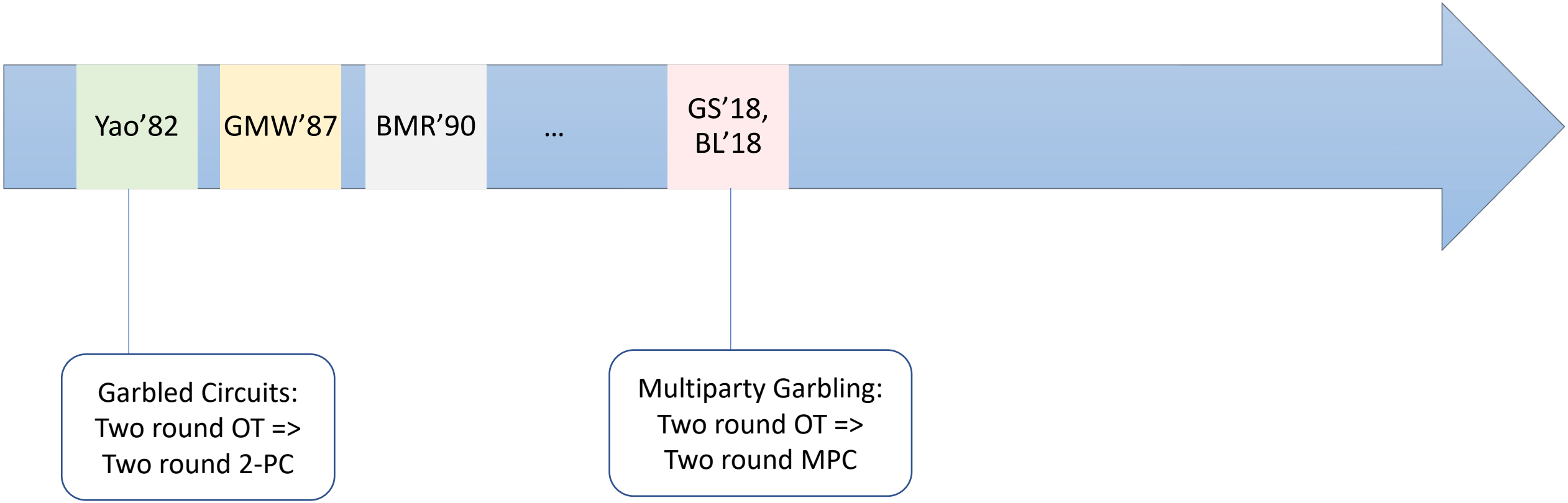
Building Block: Oblivious Transfer



Progress in Understanding MPC

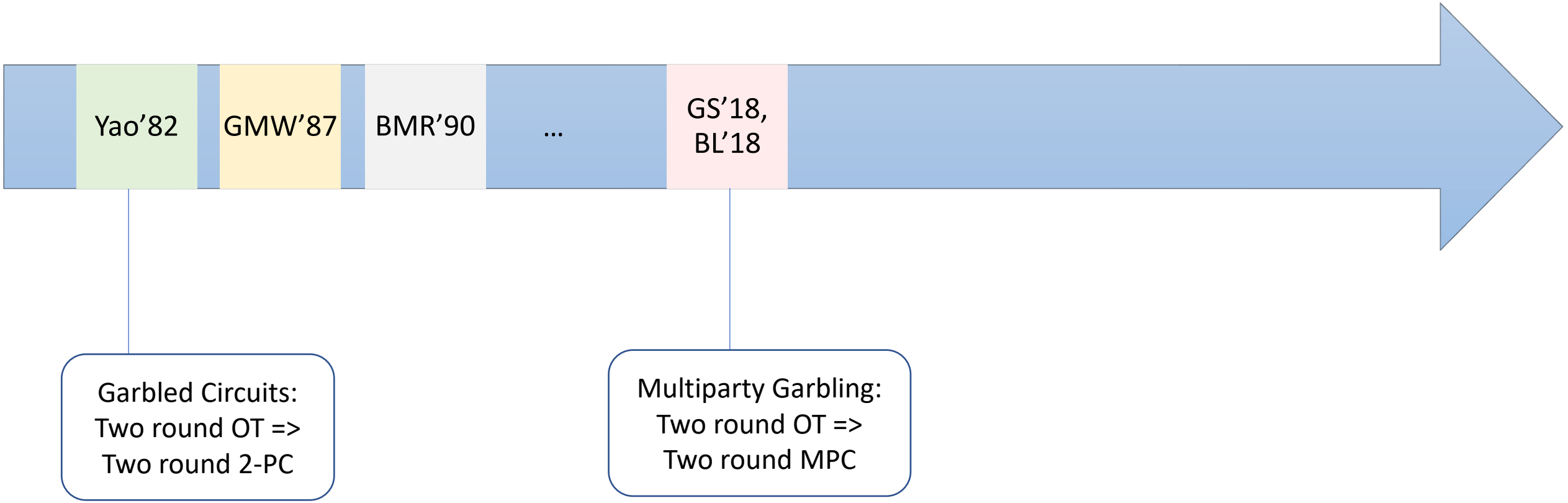


Progress in Understanding MPC



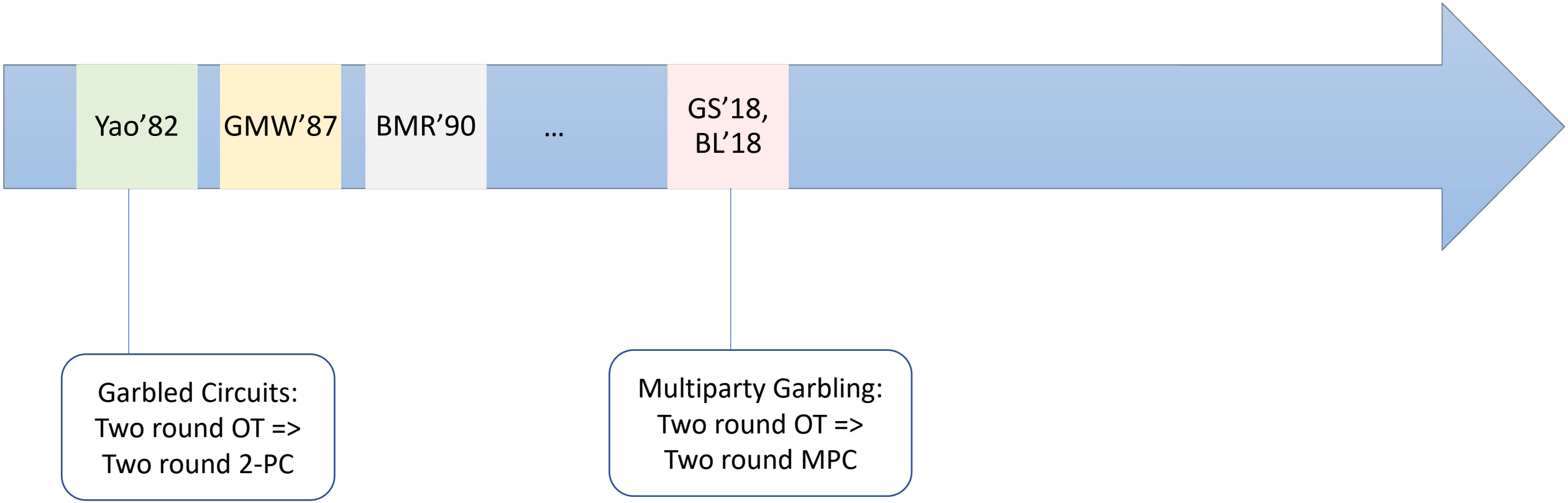
Progress in Understanding MPC

Malicious Security in the CRS Model



Progress in Understanding MPC

Malicious Security in the CRS Model



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 *adaptive* OT =>
Three round MPC

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 *adaptive* OT =>
Three round MPC

Two round OT =>
Three round MPC in RO model,
Two round MPC in OT correlations model

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]

BLACK-BOX

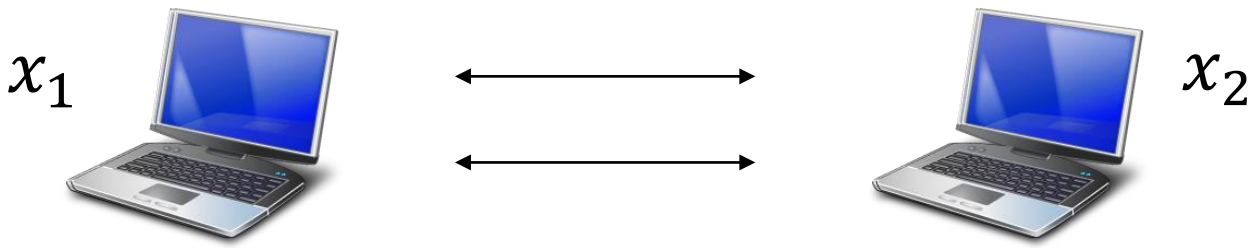
Our Results

In the common reference string (CRS) model,

- 2 round maliciously secure OT ➔ 3 round maliciously secure MPC

- 2 round maliciously secure OT ➔ 2 round 2-sided NISC

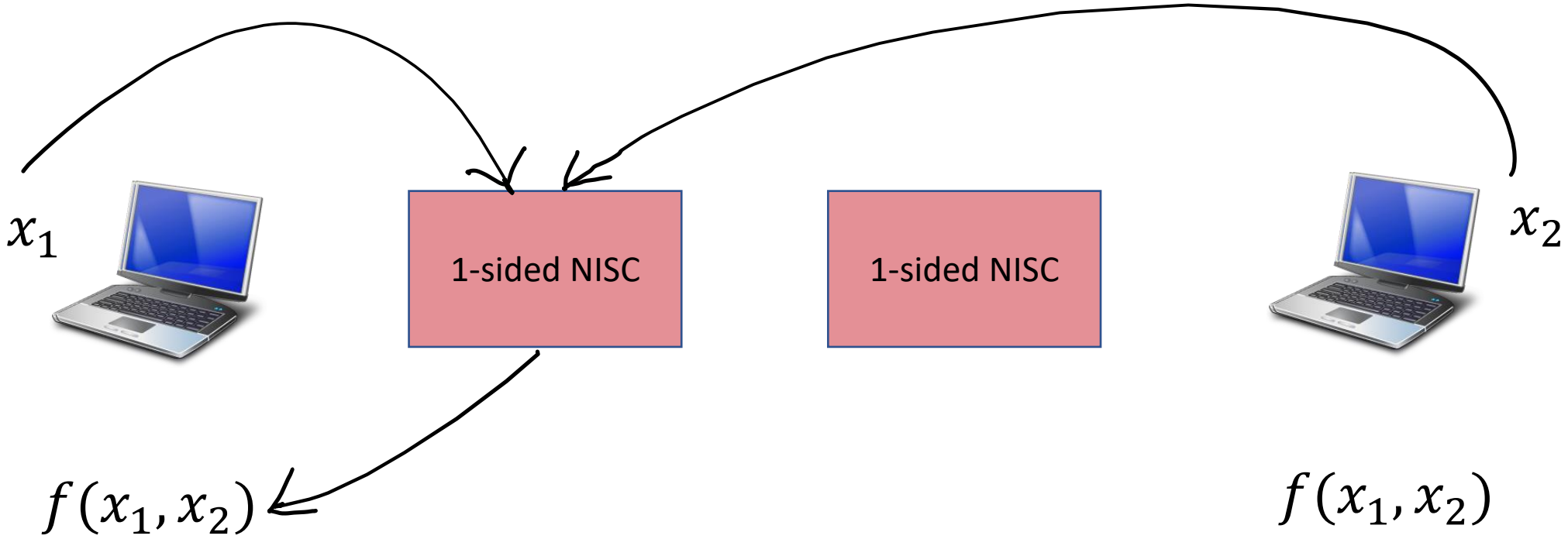
Two-Sided Non-Interactive Secure Computation (NISC)



$f(x_1, x_2)$ $f(x_1, x_2)$

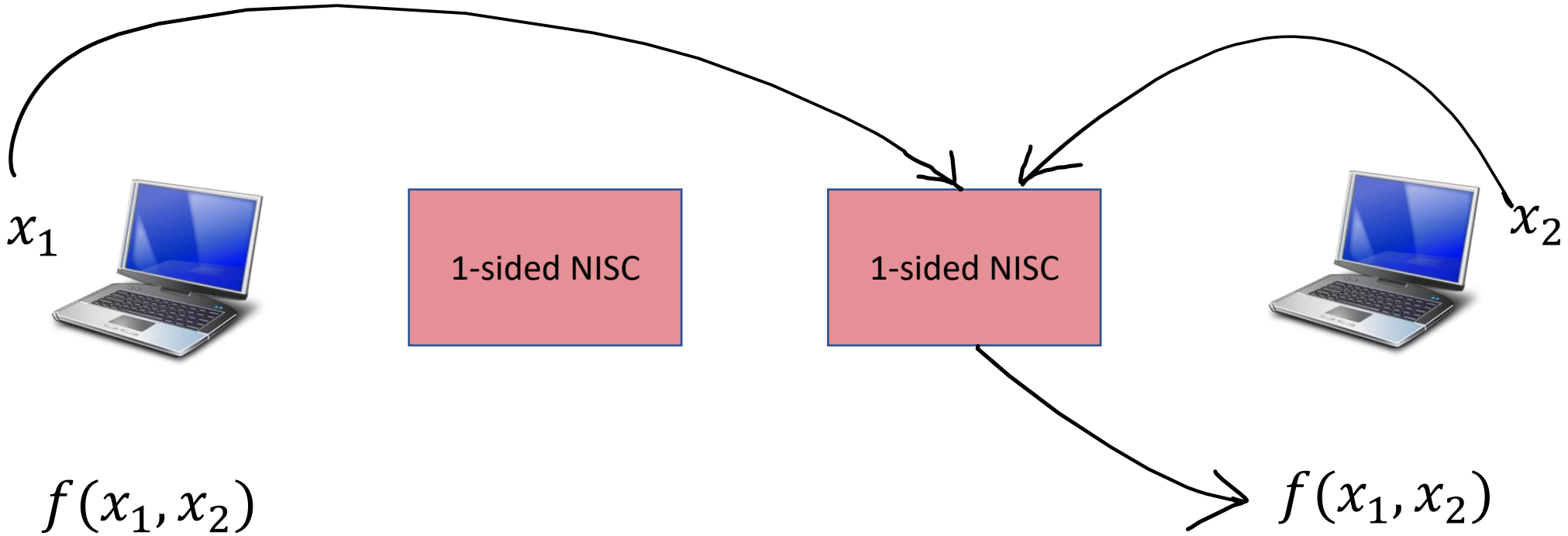
Known result: Two-round One-sided NISC from black-box use of two-round OT [IKOPS'11]

Two-Sided Non-Interactive Secure Computation (NISC)

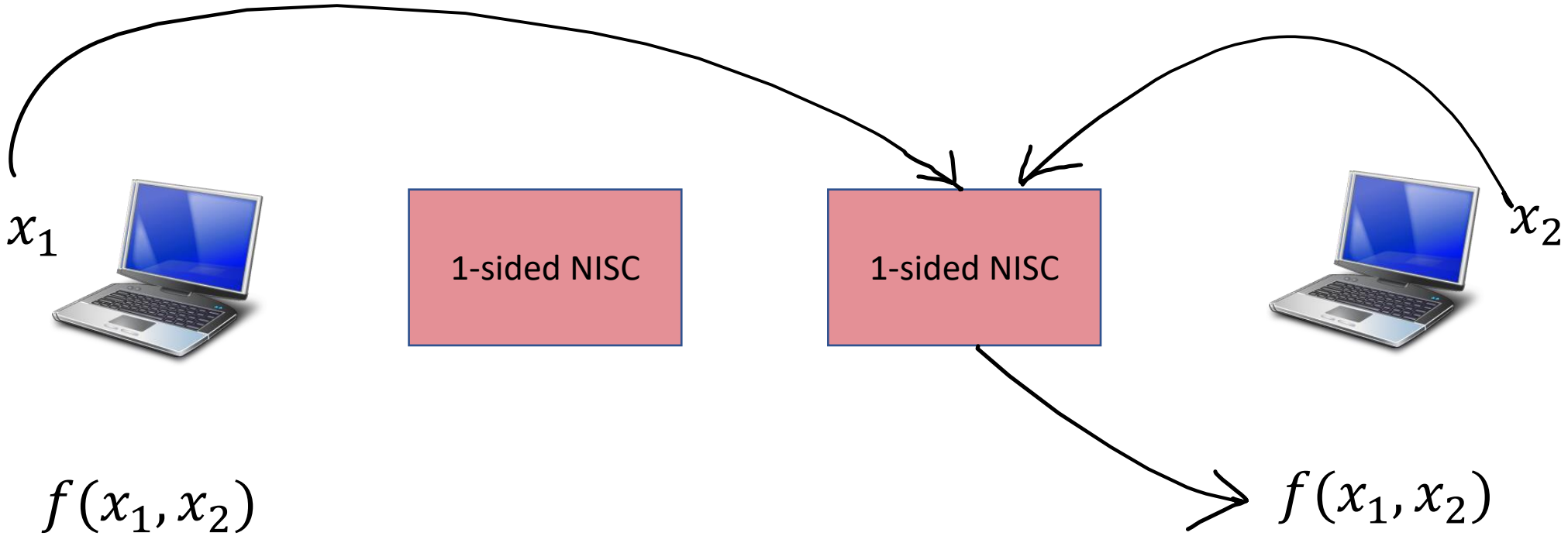


Known result: Two-round One-sided NISC from black-box use of two-round OT [IKOPS'11]

Two-Sided Non-Interactive Secure Computation (NISC)



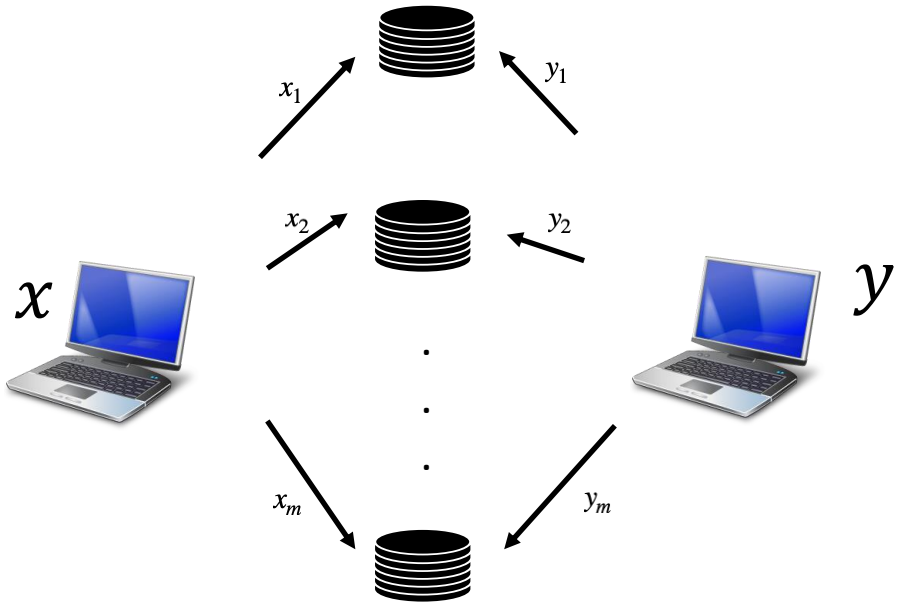
Two-Sided Non-Interactive Secure Computation (NISC)



Key Technical Challenge: Ensure input consistency across executions

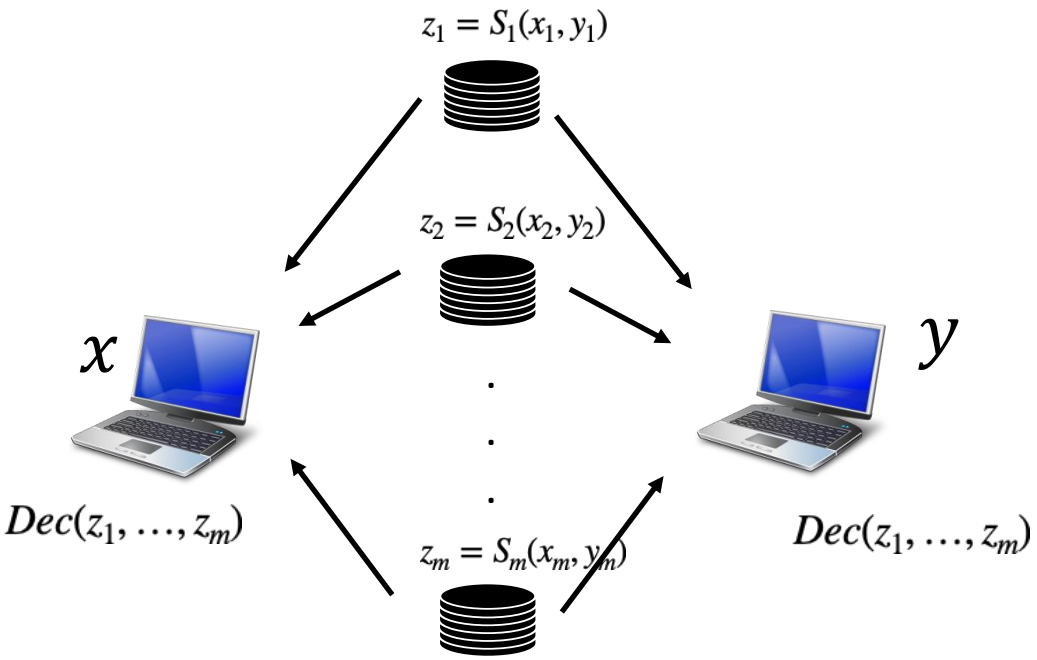
Use MPC-in-the-head techniques [IPS'08] to check input consistency

Quick Recap of the IPS Compiler



Outer Protocol

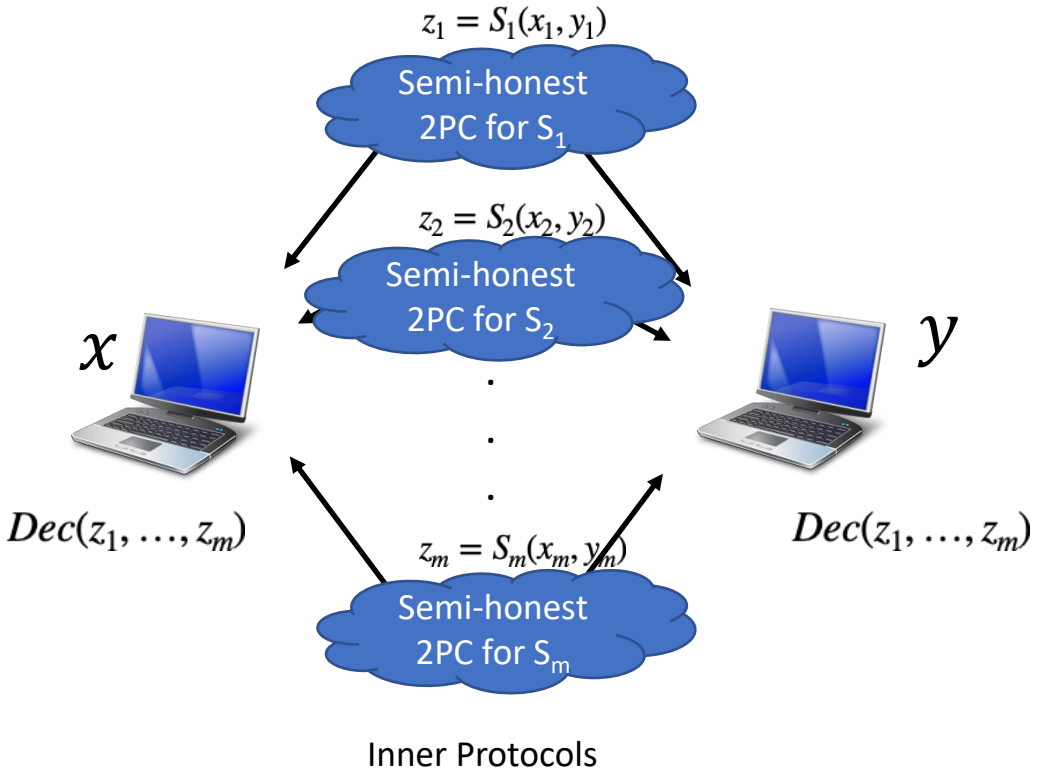
Quick Recap of the IPS Compiler



Outer Protocol

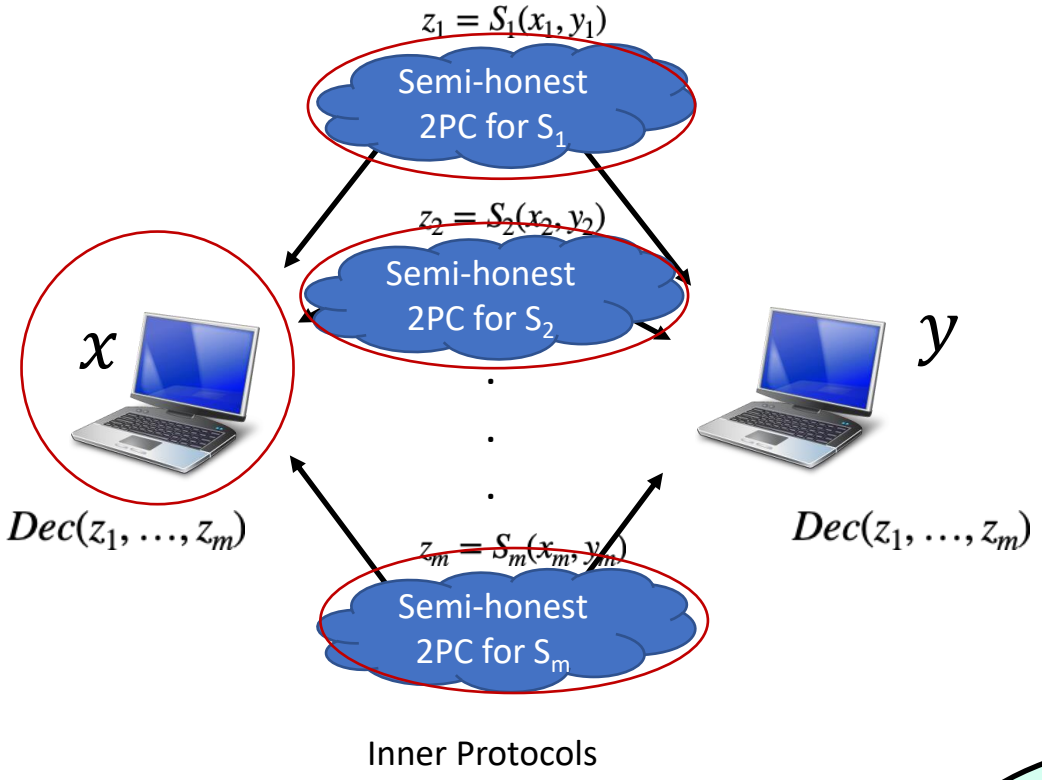
Malicious security against corruption of one of the clients and a constant fraction of servers [IKP 10].

Quick Recap of the IPS Compiler



Inner Protocols

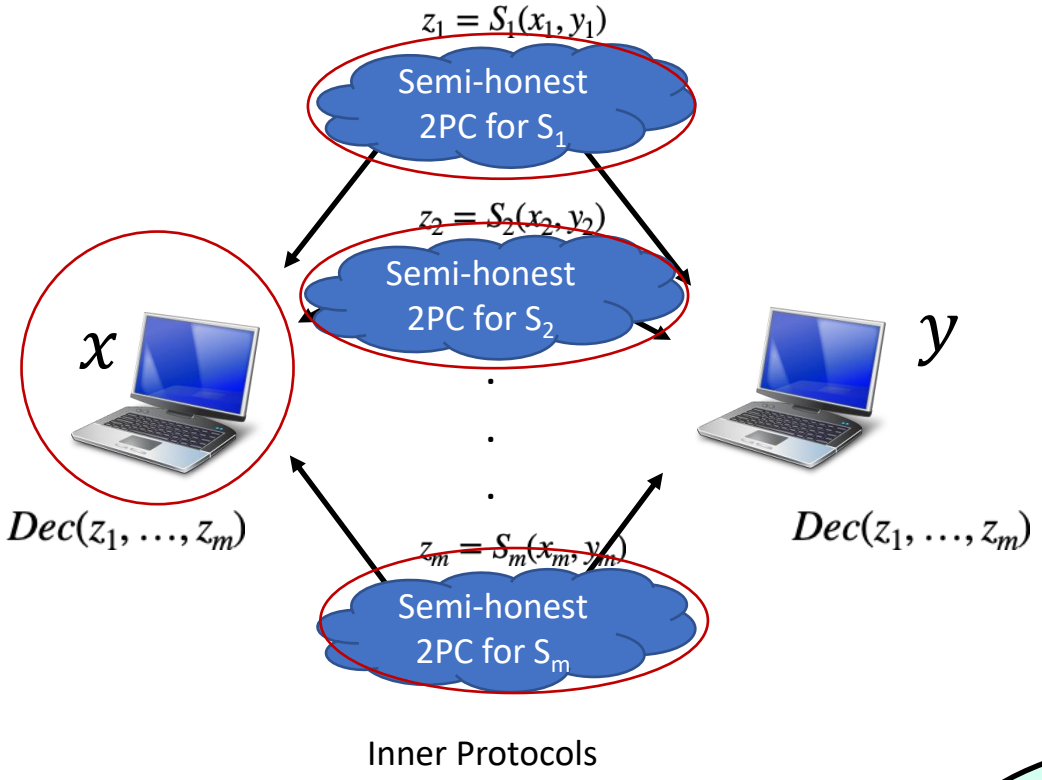
Quick Recap of the IPS Compiler



Inner Protocols

Need to ensure that adversary only cheats in a constant fraction

Quick Recap of the IPS Compiler



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*?