Round-Optimal Black-Box Protocol Compilers

Yuval Ishai (Technion)
Dakshita Khurana (UIUC)
Amit Sahai (UCLA)
Akshayaram Srinivasan (TIFR)

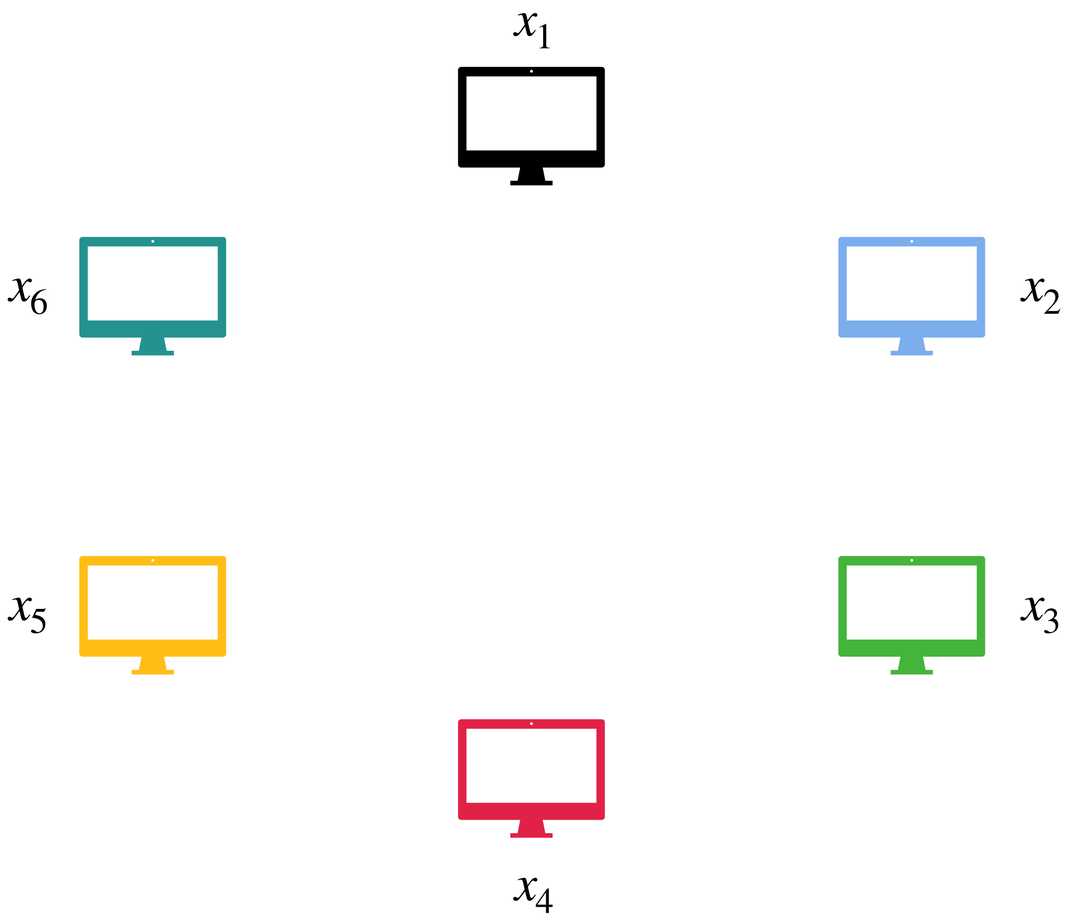
Eurocrypt 2022

Secure Multiparty Computation

[Yao 86, Goldreich-Micali-Wigderson 87]

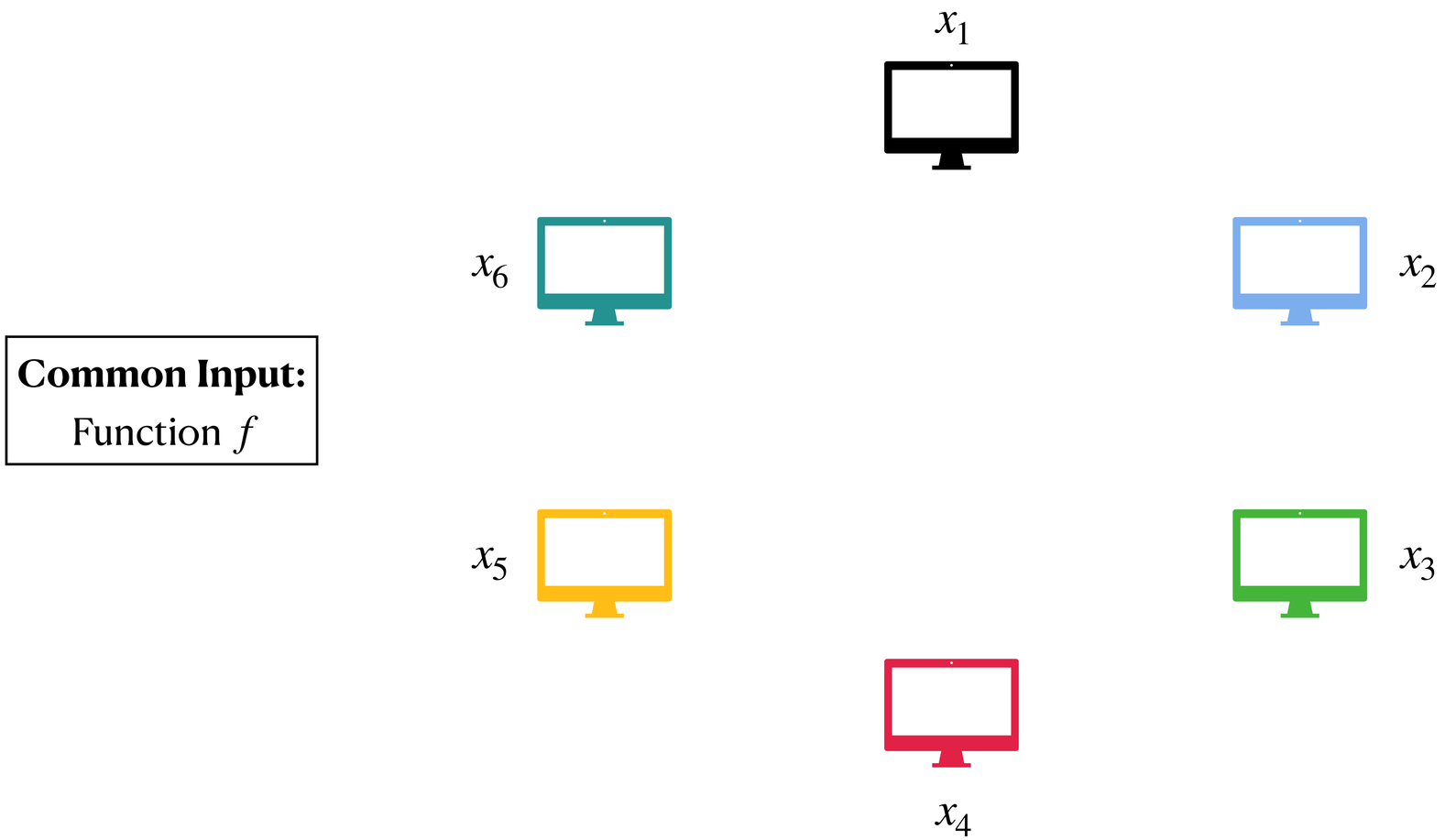
Secure Multiparty Computation

[Yao 86, Goldreich-Micali-Wigderson 87]



Secure Multiparty Computation

[Yao 86, Goldreich-Micali-Wigderson 87]

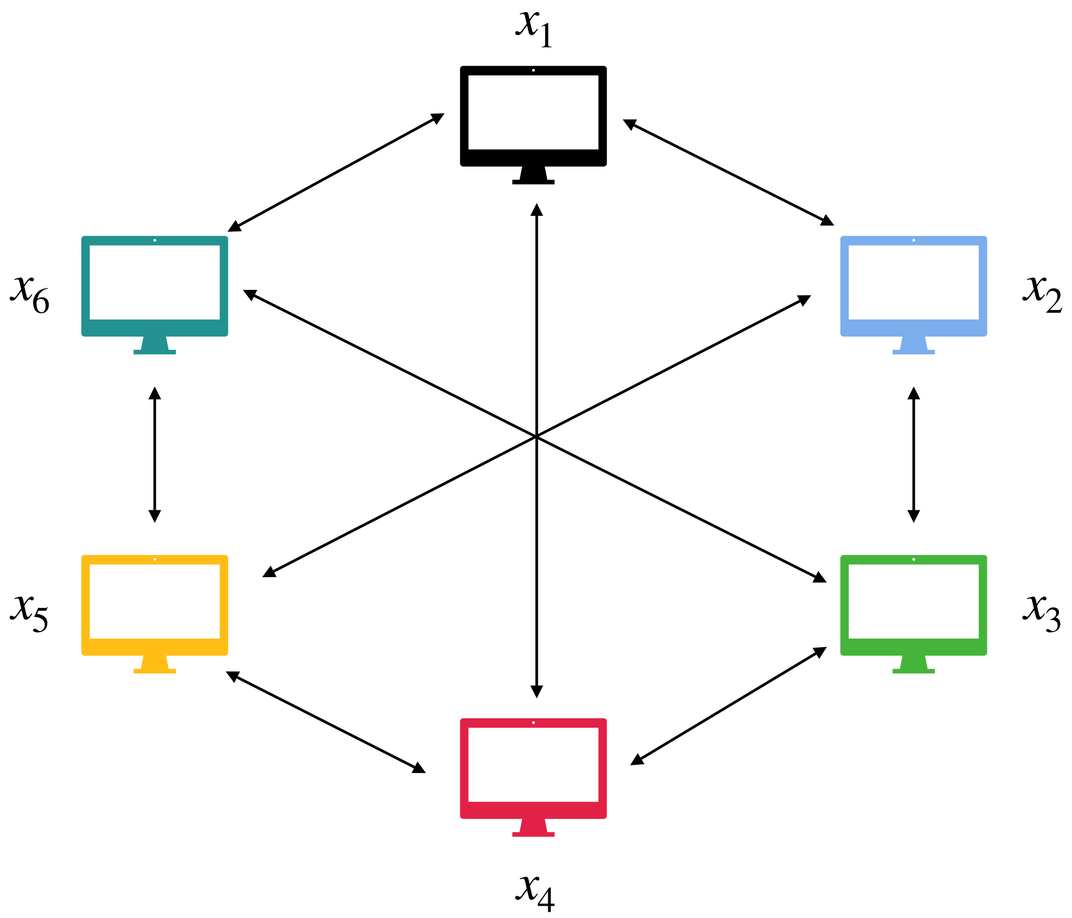


Common Input:
Function f

Secure Multiparty Computation

[Yao 86, Goldreich-Micali-Wigderson 87]

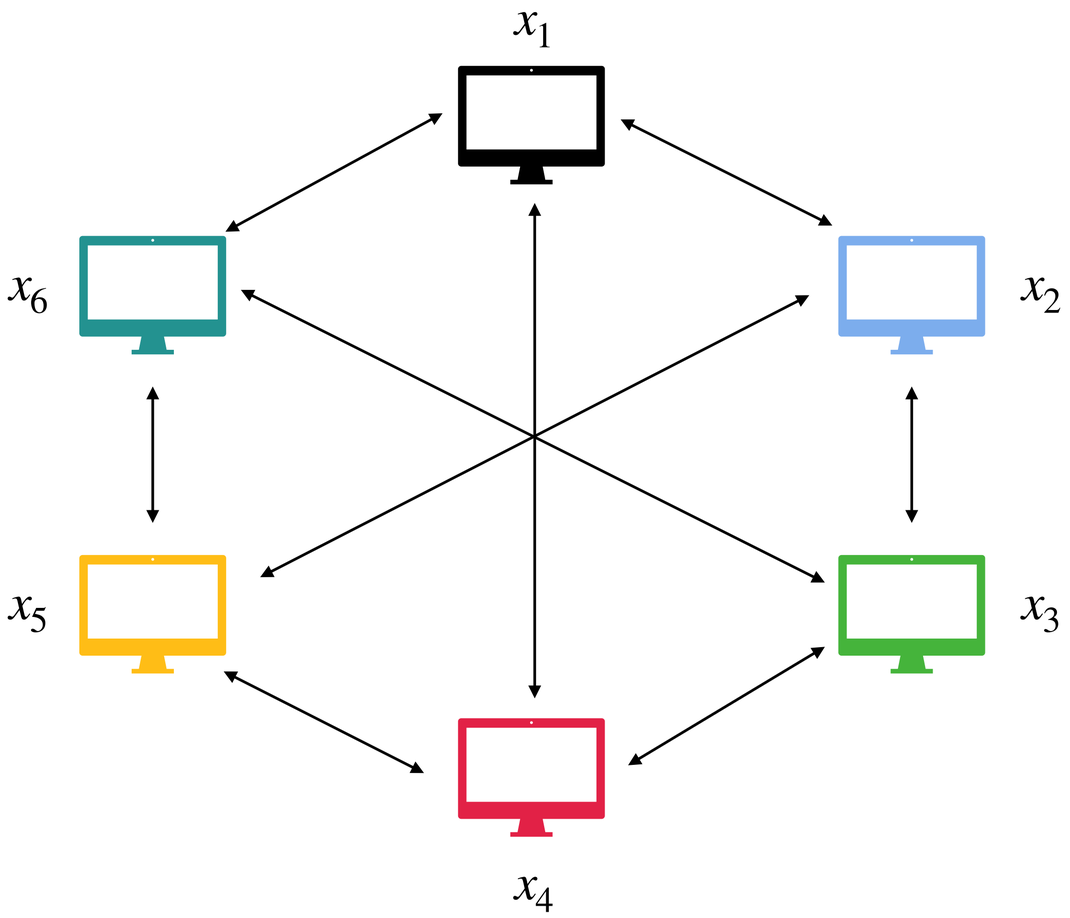
Common Input:
Function f



Secure Multiparty Computation

[Yao 86, Goldreich-Micali-Wigderson 87]

Common Input:
Function f

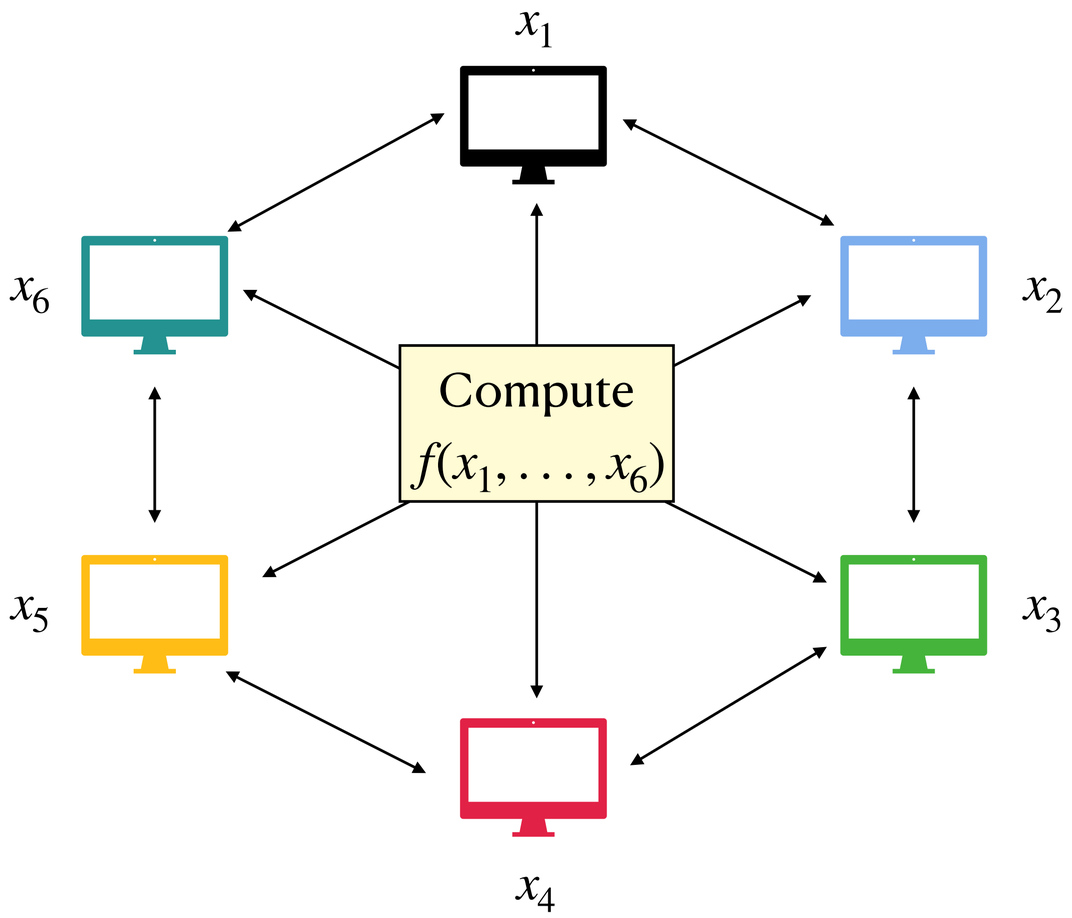


Correctness

Secure Multiparty Computation

[Yao 86, Goldreich-Micali-Wigderson 87]

Common Input:
Function f

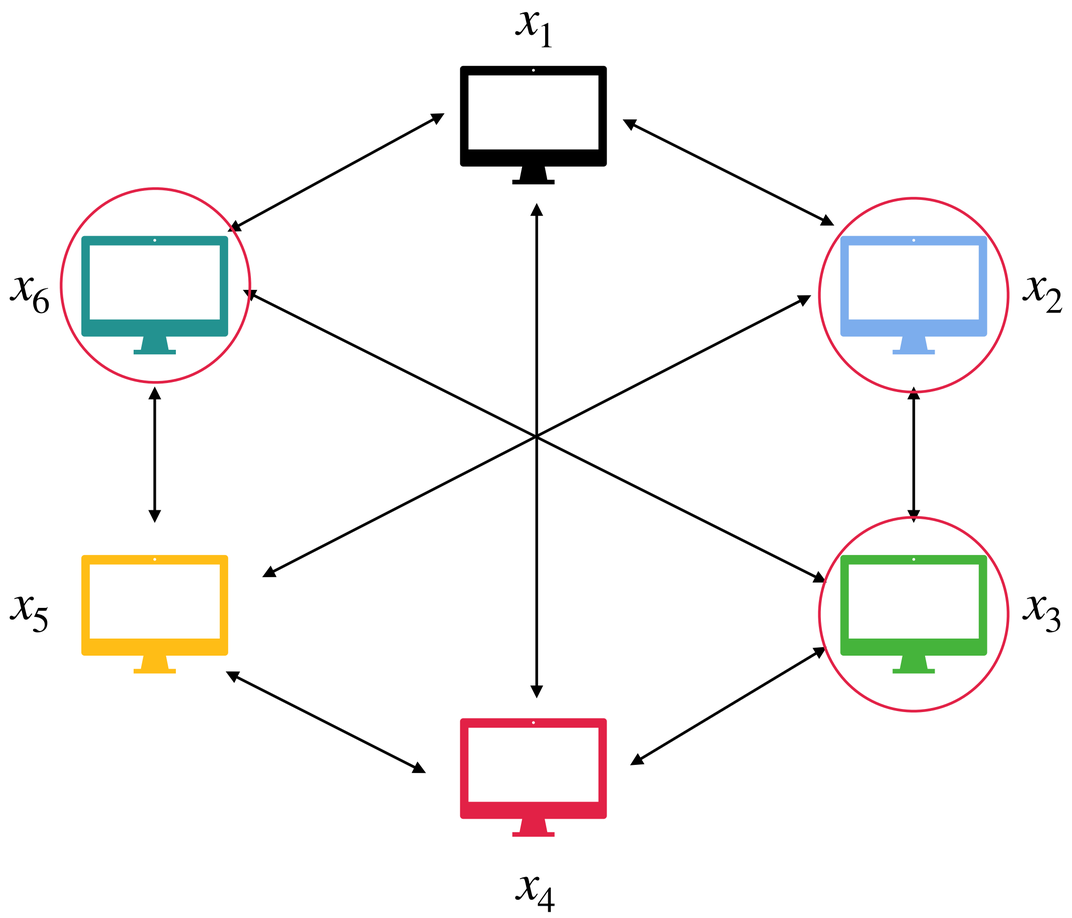


Correctness

Secure Multiparty Computation

[Yao 86, Goldreich-Micali-Wigderson 87]

Common Input:
Function f

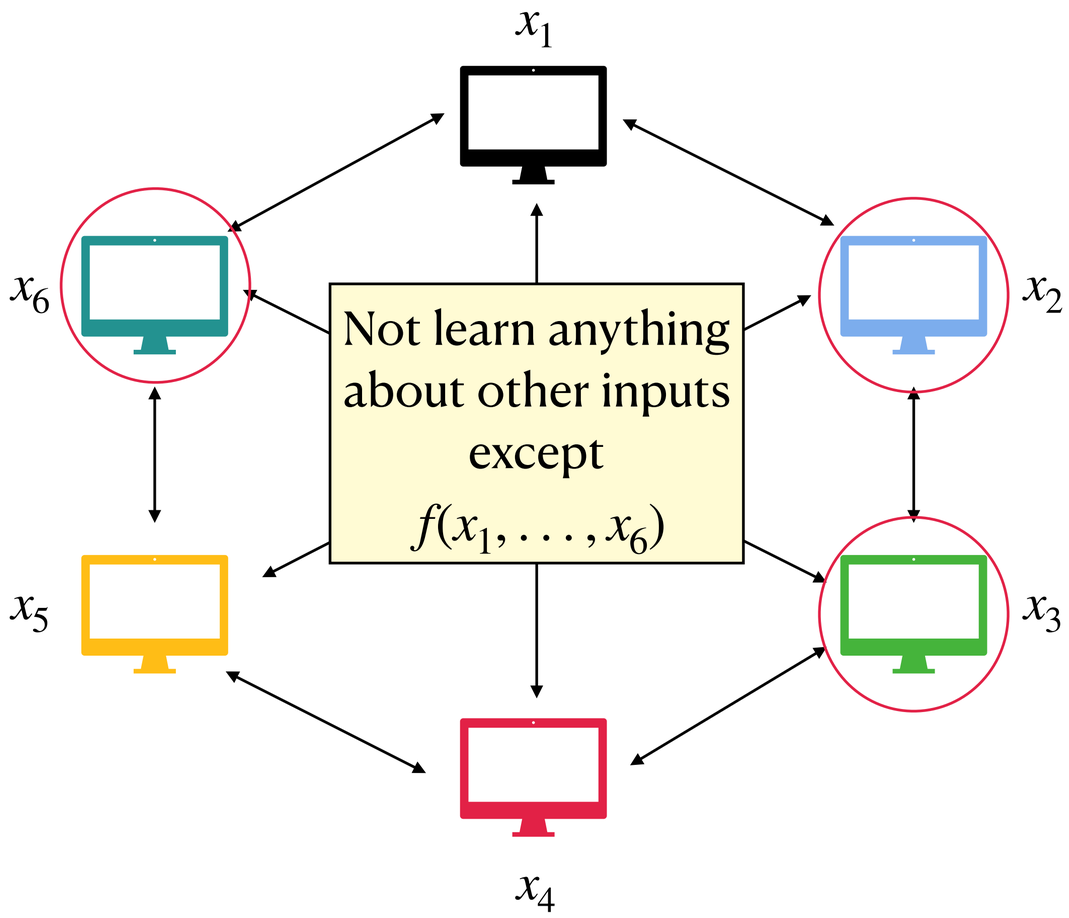


Security

Secure Multiparty Computation

[Yao 86, Goldreich-Micali-Wigderson 87]

Common Input:
Function f



Security

Types of Adversary

Types of Adversary

Semi-Honest Adversary

Types of Adversary

- Follow the protocol specification but try to learn additional information.

Semi-Honest Adversary

Types of Adversary

- Follow the protocol specification but try to learn additional information.
- Easier to protect against.

Semi-Honest Adversary

Types of Adversary

- Follow the protocol specification but try to learn additional information.
- Easier to protect against.

Semi-Honest Adversary

Malicious Adversary

Types of Adversary

- Follow the protocol specification but try to learn additional information.
- Easier to protect against.

Semi-Honest Adversary

- Could deviate from the protocol specification and break security.

Malicious Adversary

Types of Adversary

- Follow the protocol specification but try to learn additional information.
- Easier to protect against.

Semi-Honest Adversary

- Could deviate from the protocol specification and break security.
- Harder to protect against.

Malicious Adversary

Protocol Compilers

Protocol Compilers

Protocol for computing f' with security against Semi-Honest Adversary

Protocol Compiler

Protocol for computing f with security against Malicious adversary

Protocol Compilers

For every f, $\exists f'$.

Protocol Compiler

Protocol for computing f' with security against Semi-Honest Adversary

Protocol for computing f with security against Malicious adversary

Protocol Compilers

For every f, $\exists f'$.

Protocol for computing f' with security against Semi-Honest Adversary

Protocol Compiler

Protocol for computing f with security against Malicious adversary

Goal: Construct "**efficient**" Protocol Compilers.

How to measure efficiency?

How to measure efficiency?

- **Preserve round complexity**

How to measure efficiency?

- **Preserve round complexity**
  - The compiled protocol has the same number of rounds as the initial protocol.

How to measure efficiency?

- **Preserve round complexity**
  - The compiled protocol has the same number of rounds as the initial protocol.
- **Black-Box use**

How to measure efficiency?

- **Preserve round complexity**
  - The compiled protocol has the same number of rounds as the initial protocol.
- **Black-Box use**
  - The compiled protocol makes black-box use of the initial protocol.

How to measure efficiency?

- **Preserve round complexity**
  - The compiled protocol has the same number of rounds as the initial protocol.
- **Black-Box use**
  - The compiled protocol makes black-box use of the initial protocol.
- **Making use of simple tools**

How to measure efficiency?

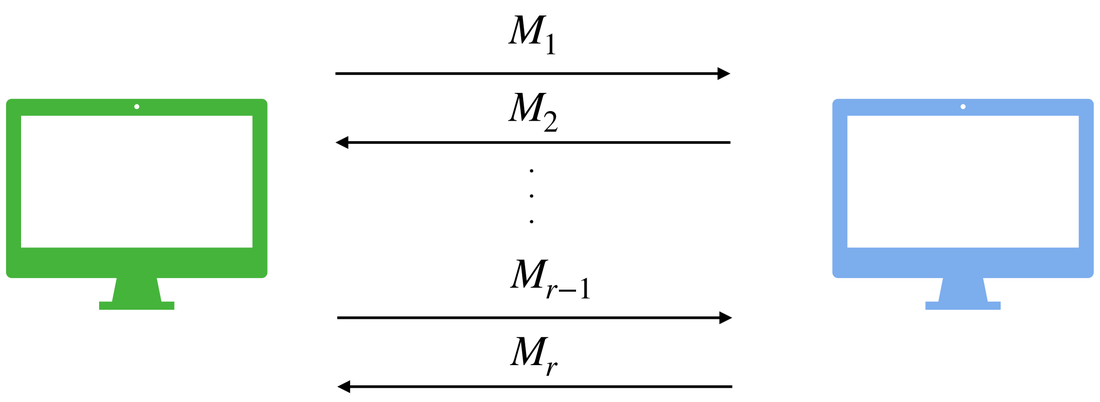
- **Preserve round complexity**
  - The compiled protocol has the same number of rounds as the initial protocol.
- **Black-Box use**
  - The compiled protocol makes black-box use of the initial protocol.
- **Making use of simple tools**
  - The compiler avoids sophisticated and less efficient cryptographic tools.

Prior Approaches

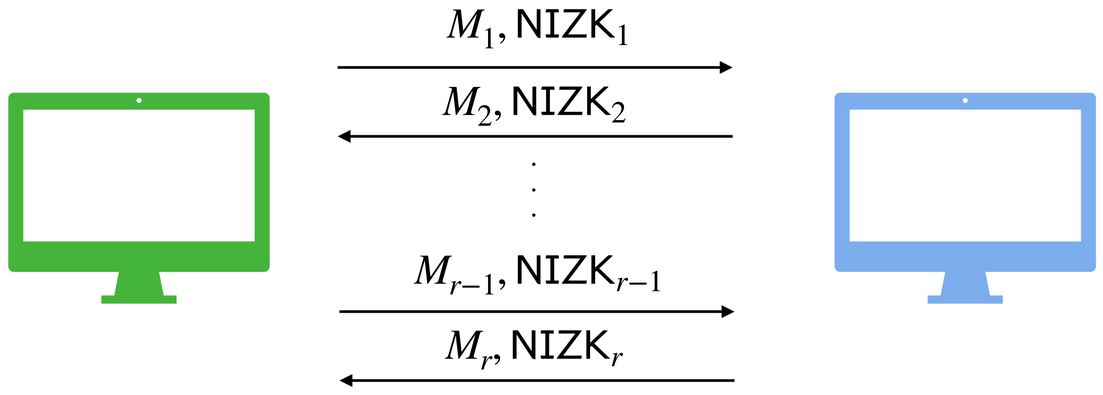
GMW Compiler

Prior Approaches

GMW Compiler



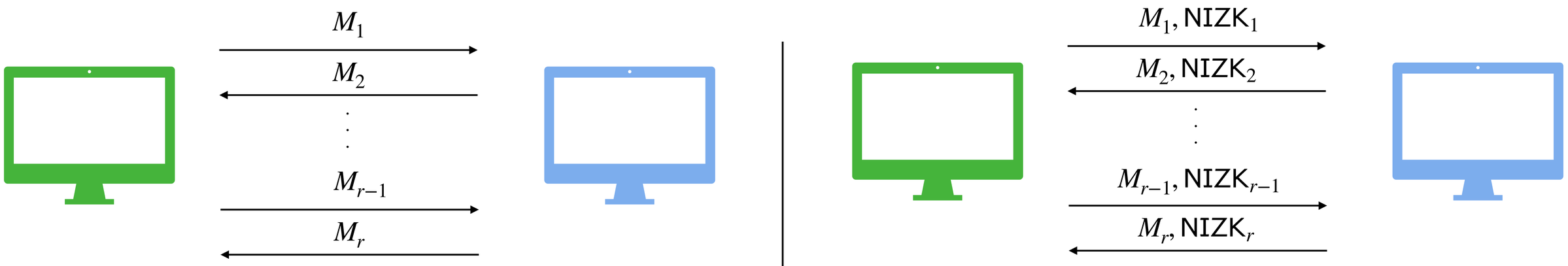
Semi-Honest Secure Protocol



Malicious Secure Protocol

Prior Approaches

GMW Compiler



Semi-Honest Secure Protocol

Malicious Secure Protocol

Non-Black-Box use

Prior Approaches

IPS Compiler

Prior Approaches

IPS Compiler

- A black-box protocol compiler.

Prior Approaches

IPS Compiler

- A black-box protocol compiler.
- Resulted in an increase in round-complexity.

Prior Approaches

IPS Compiler

- A black-box protocol compiler.
- Resulted in an increase in round-complexity.
- Required stronger cryptographic tools such as malicious secure oblivious transfer.

Prior Approaches

IPS Compiler

- A black-box protocol compiler.
- Resulted in an increase in round-complexity.
- Required stronger cryptographic tools such as malicious secure oblivious transfer.
- Required the semi-honest secure protocol to satisfy stronger security property, namely, adaptive security with erasures.

Our Results

Our Results

- A protocol compiler that is:

Our Results

- A protocol compiler that is:
  - Round-Optimal, i.e., transforms round-optimal semi-honest secure protocol to round-optimal malicious secure protocol.

Our Results

- A protocol compiler that is:
  - Round-Optimal, i.e., transforms round-optimal semi-honest secure protocol to round-optimal malicious secure protocol.
  - Black-Box.

Our Results

- A protocol compiler that is:
  - Round-Optimal, i.e., transforms round-optimal semi-honest secure protocol to round-optimal malicious secure protocol.
  - Black-Box.
  - Makes use of simple cryptographic tools/setup: ROM/1-out-2 OT correlations.

Applications

2PC

Applications

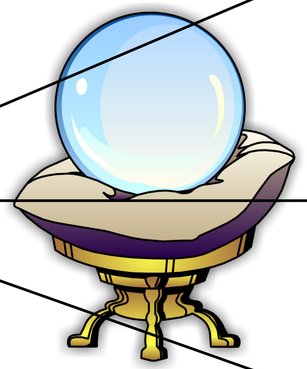
2PC

Two-round
Semi-Honest
2PC

Applications

2PC

Two-round Semi-Honest 2PC



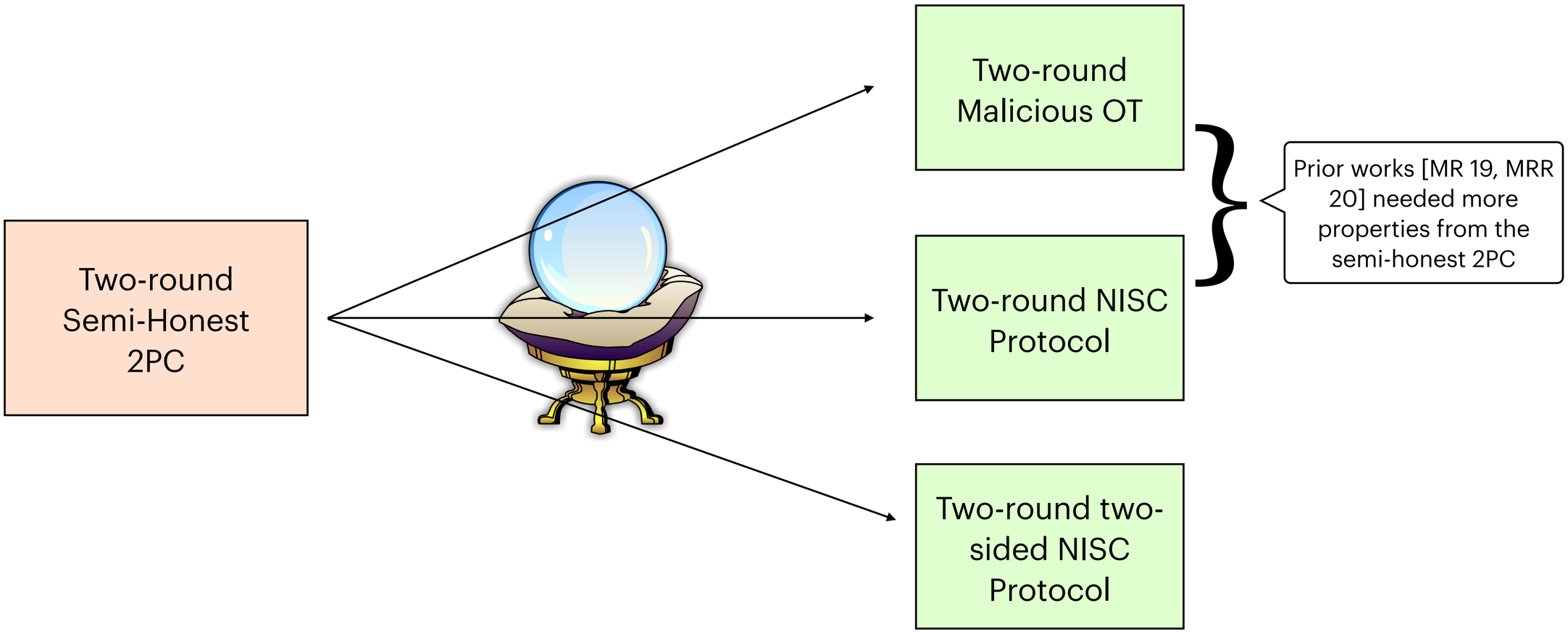
Two-round Malicious OT

Two-round NISC Protocol

Two-round two-sided NISC Protocol

Applications

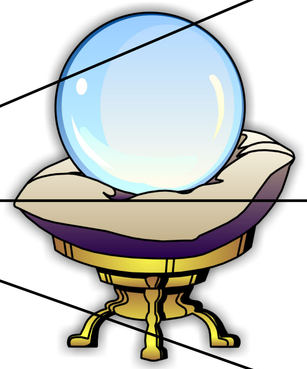
2PC



Applications

2PC

Two-round Semi-Honest 2PC



Two-round Malicious OT

Two-round NISC Protocol

Two-round two-sided NISC Protocol

Prior works [MR 19, MRR 20] needed more properties from the semi-honest 2PC

ROM can be replaced with fixed poly sized OT correlations if we start with semi-malicious 2PC

Applications

MPC

Applications

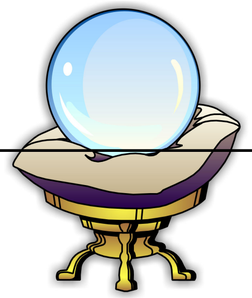
MPC

Two-round
Semi-Honest
OT

Applications

MPC

Two-round Semi-Honest OT

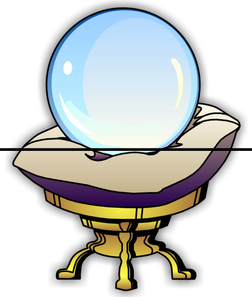


Three-round malicious MPC

Applications

MPC

Two-round Semi-Honest OT



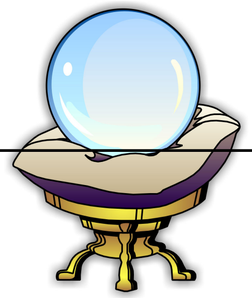
Three-round malicious MPC

Round-Optimality follows from [ABGIS 20]

Applications

MPC

Two-round Semi-Honest OT



Three-round malicious MPC

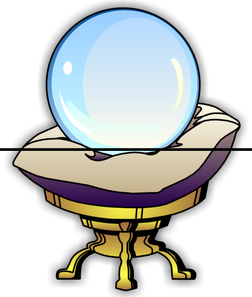
Round-Optimality follows from [ABGIS 20]

Two-round Semi-Malicious* MPC

Applications

MPC

Two-round Semi-Honest OT



Three-round malicious MPC

Round-Optimality follows from [ABGIS 20]

Two-round Semi-Malicious* MPC

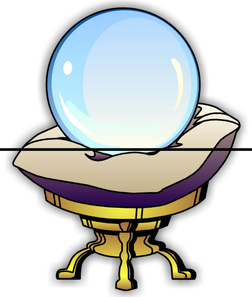
OT Correlations

Two-round malicious MPC

Applications

MPC

Two-round Semi-Honest OT



Three-round malicious MPC

Round-Optimality follows from [ABGIS 20]

Two-round Semi-Malicious* MPC

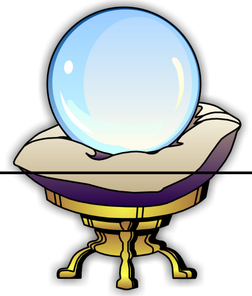
OT Correlations

Two-round malicious MPC

Prior work [IKSS 21] required complex multiparty correlations.

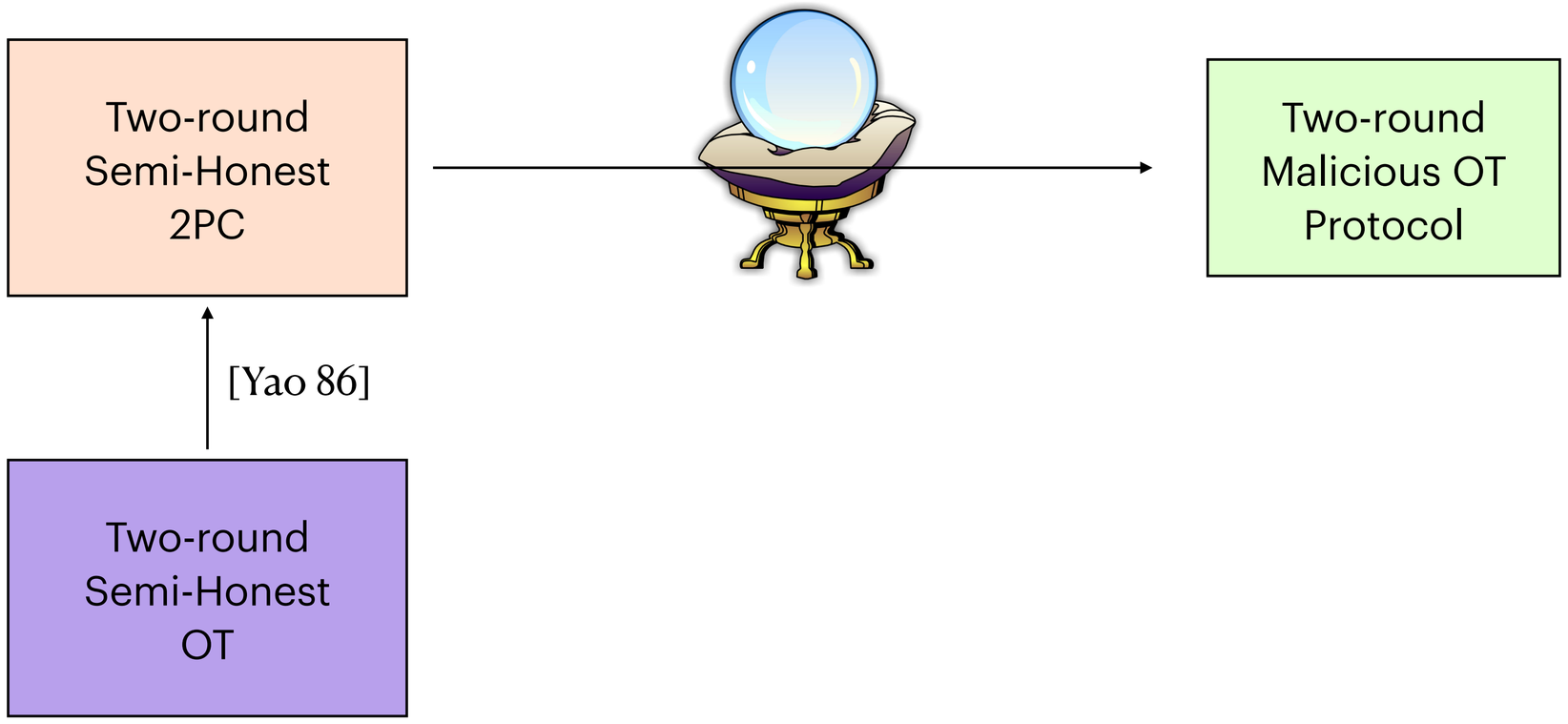
In this talk

Two-round
Semi-Honest
2PC



Two-round
Malicious OT
Protocol

In this talk

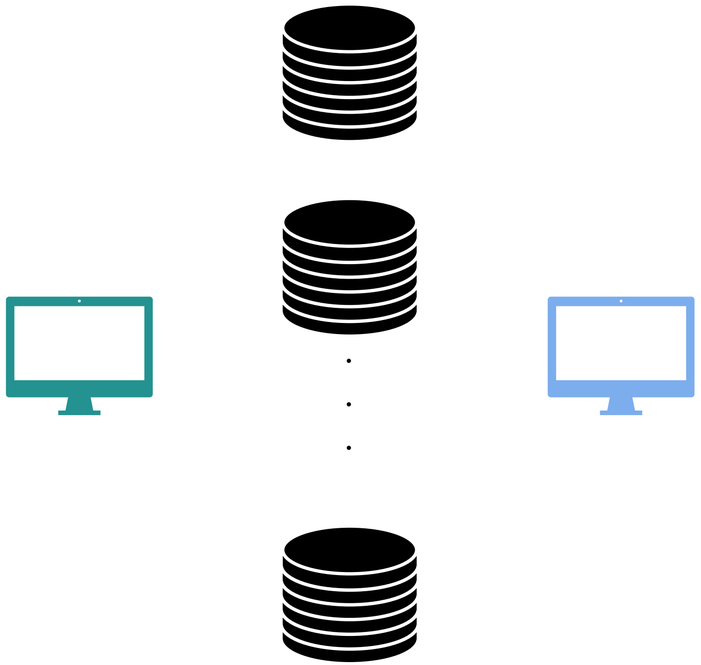

Two-round
Semi-Honest
2PC
Two-round
Malicious OT
Protocol
[Yao 86]
Two-round
Semi-Honest
OT

Brief Recap of IPS Compiler

[Ishai-Prabhakaran-Sahai 08]

Brief Recap of IPS Compiler

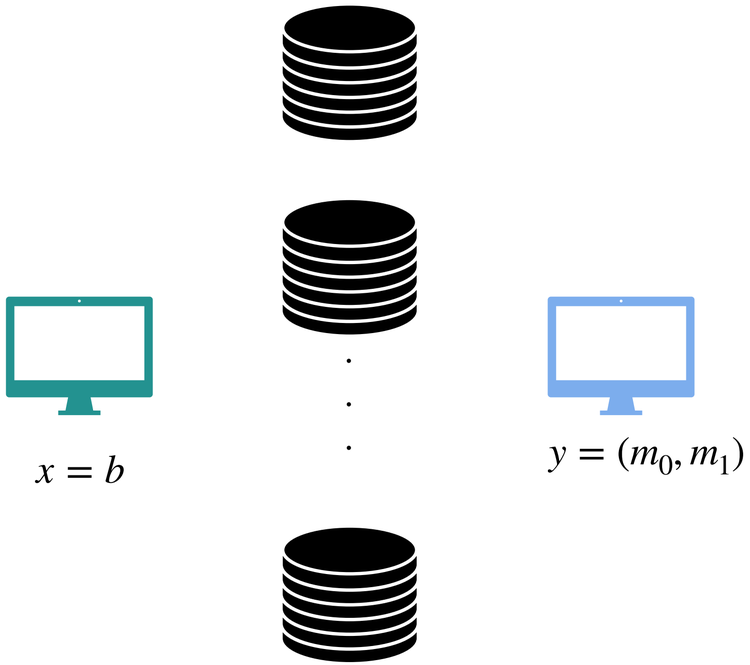
[Ishai-Prabhakaran-Sahai 08]



Outer Protocol

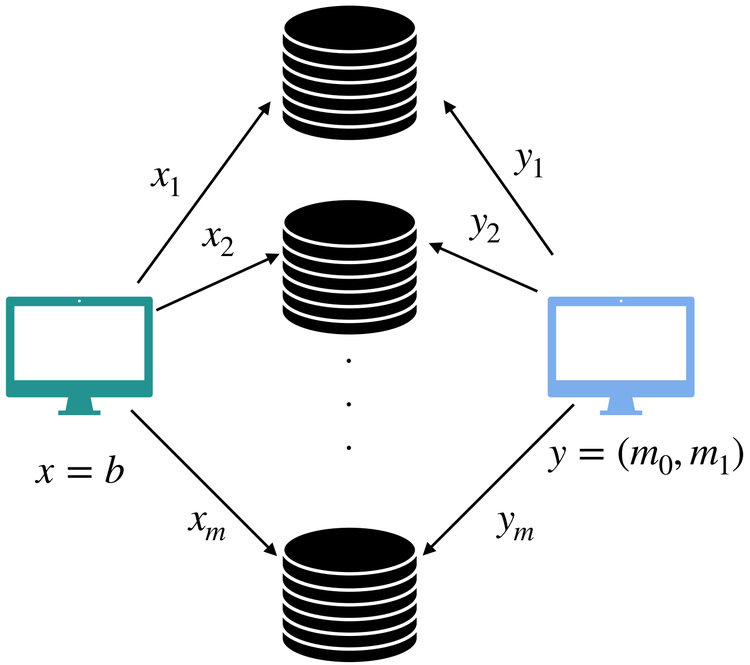
Brief Recap of IPS Compiler

[Ishai-Prabhakaran-Sahai 08]



Brief Recap of IPS Compiler

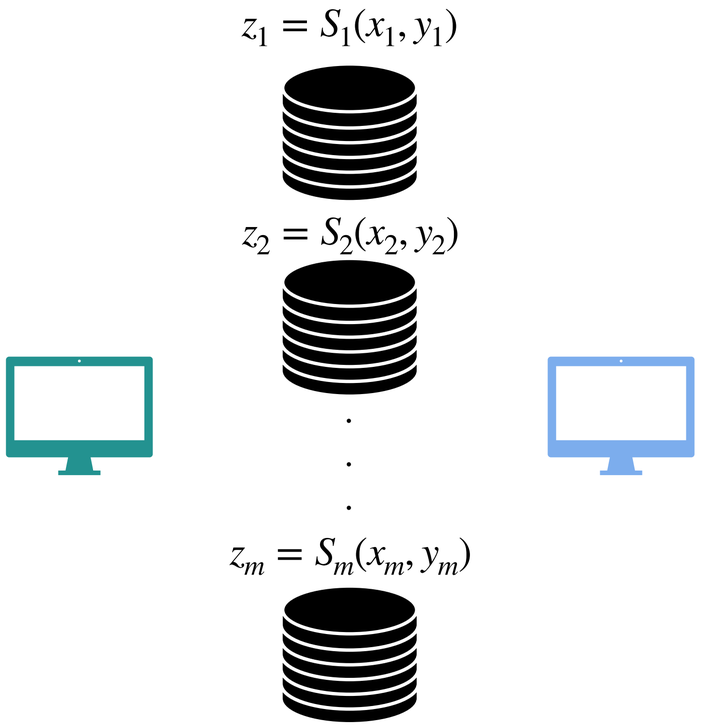
[Ishai-Prabhakaran-Sahai 08]



Outer Protocol

Brief Recap of IPS Compiler

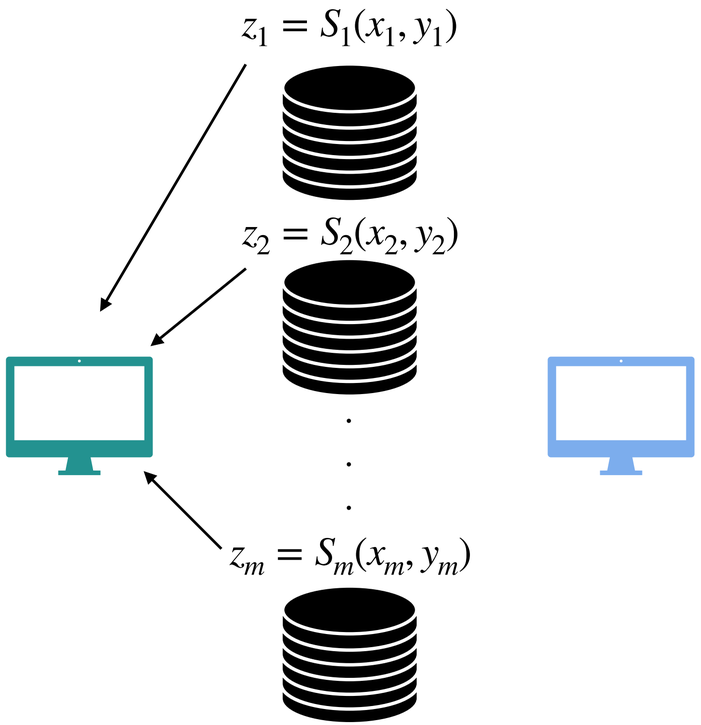
[Ishai-Prabhakaran-Sahai 08]



Outer Protocol

Brief Recap of IPS Compiler

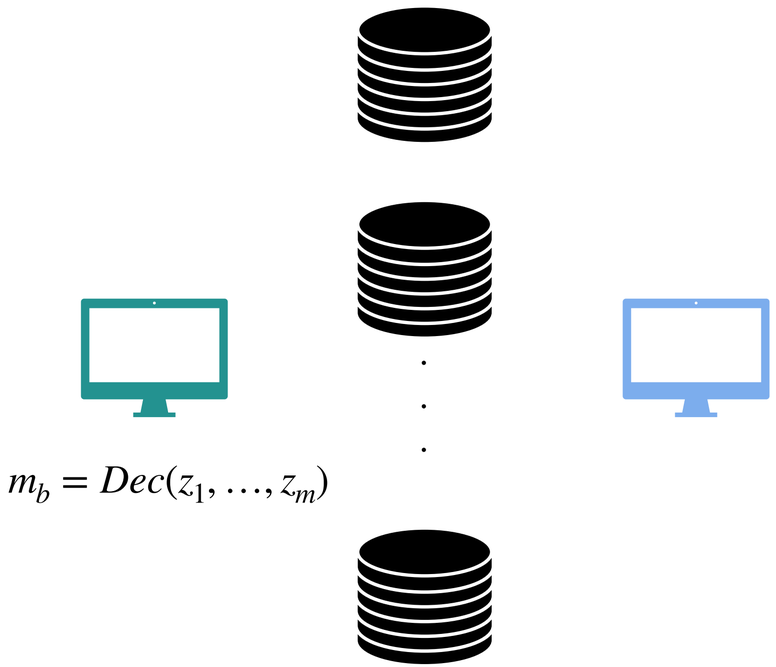
[Ishai-Prabhakaran-Sahai 08]



Outer Protocol

Brief Recap of IPS Compiler

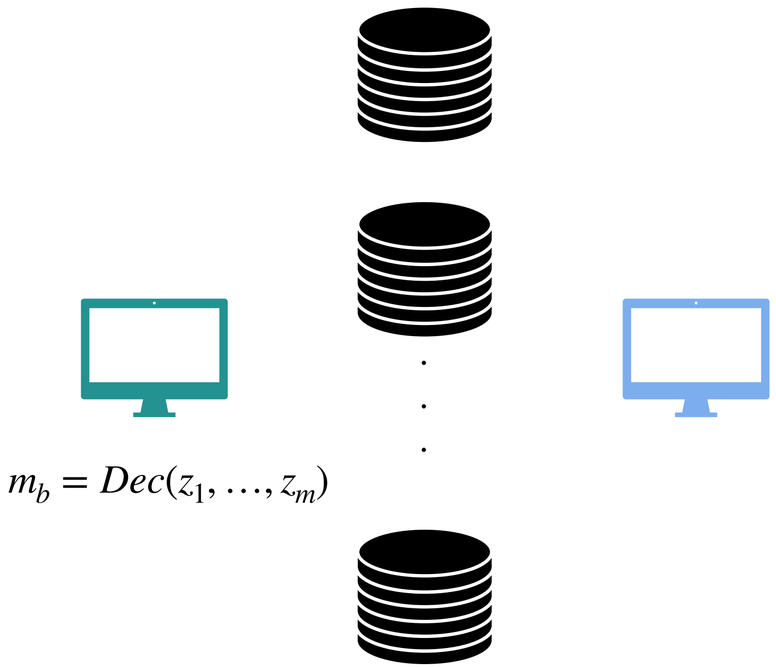
[Ishai-Prabhakaran-Sahai 08]



Brief Recap of IPS Compiler

[Ishai-Prabhakaran-Sahai 08]

Malicious security against any $\mathscr{A}$ that corrupts one of the clients and a constant fraction of servers [IKP 10].

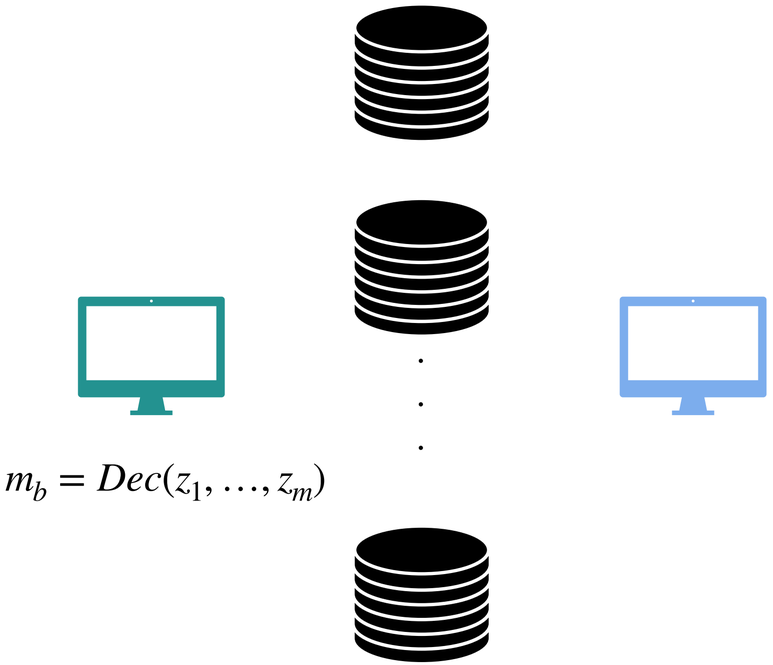


Outer Protocol

Brief Recap of IPS Compiler

[Ishai-Prabhakaran-Sahai 08]

Malicious security against any $\mathscr{A}$ that corrupts one of the clients and a constant fraction of servers [IKP 10].



Outer Protocol

Two-round Semi-Honest* 2PC for $S_1(\cdot, \cdot)$

Two-round Semi-Honest* 2PC for $S_2(\cdot, \cdot)$

.
.
.

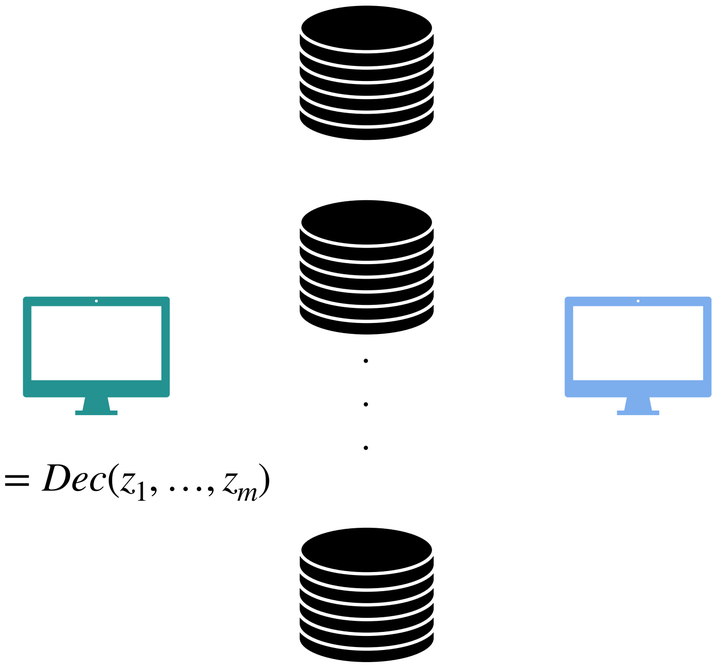
Two-round Semi-Honest* 2PC for $S_m(\cdot, \cdot)$

Inner Protocol

Brief Recap of IPS Compiler

[Ishai-Prabhakaran-Sahai 08]

Malicious security against any $\mathscr{A}$ that corrupts one of the clients and a constant fraction of servers [IKP 10].



$m_b = Dec(z_1, \ldots, z_m)$

Outer Protocol

Two-round Semi-Honest* 2PC for $S_1(\cdot, \cdot)$

Two-round Semi-Honest* 2PC for $S_2(\cdot, \cdot)$

.
.
.

Two-round Semi-Honest* 2PC for $S_m(\cdot, \cdot)$

Inner Protocol

Watchlist Protocol

The IPS Compiled Protocol

The IPS Compiled Protocol

$x = b$

$y = (m_0, m_1)$

The IPS Compiled Protocol

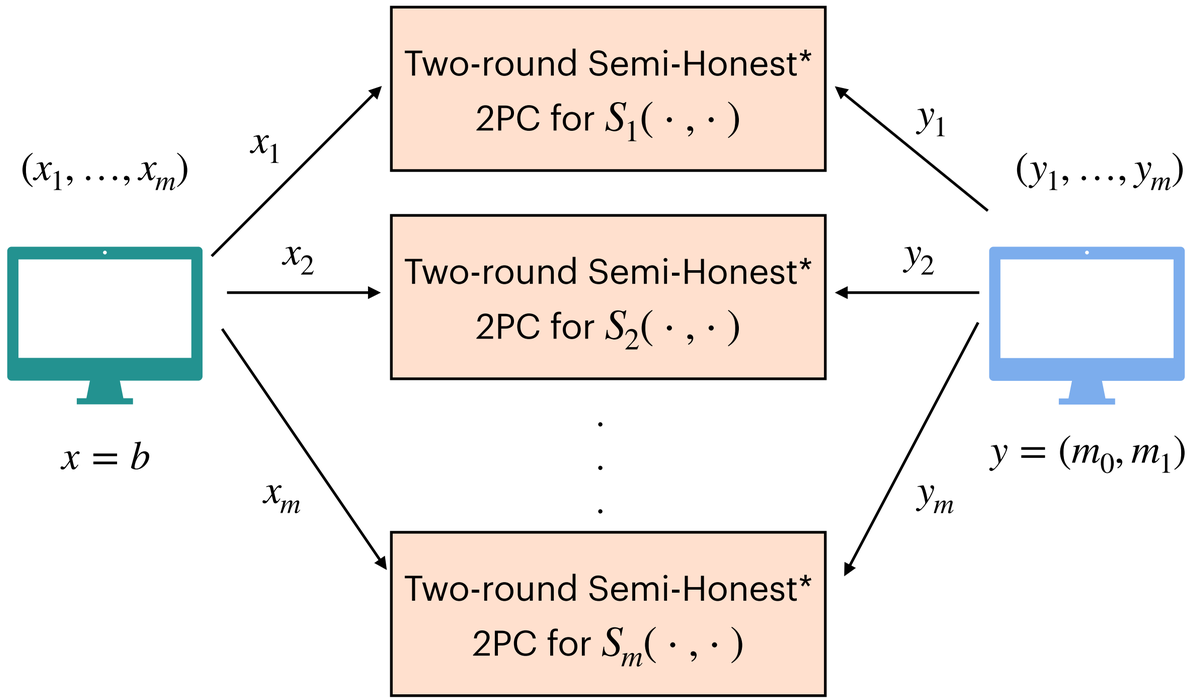
$(x_1, \ldots, x_m)$

$x = b$

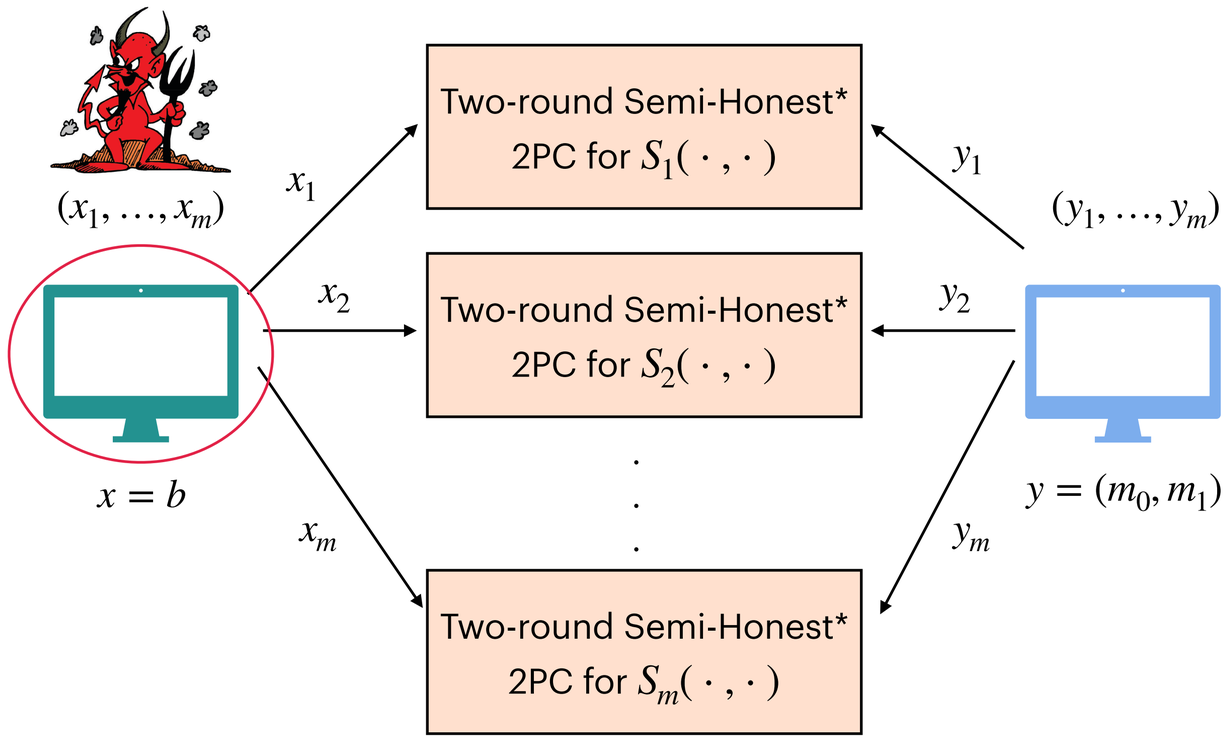
$(y_1, \ldots, y_m)$

$y = (m_0, m_1)$

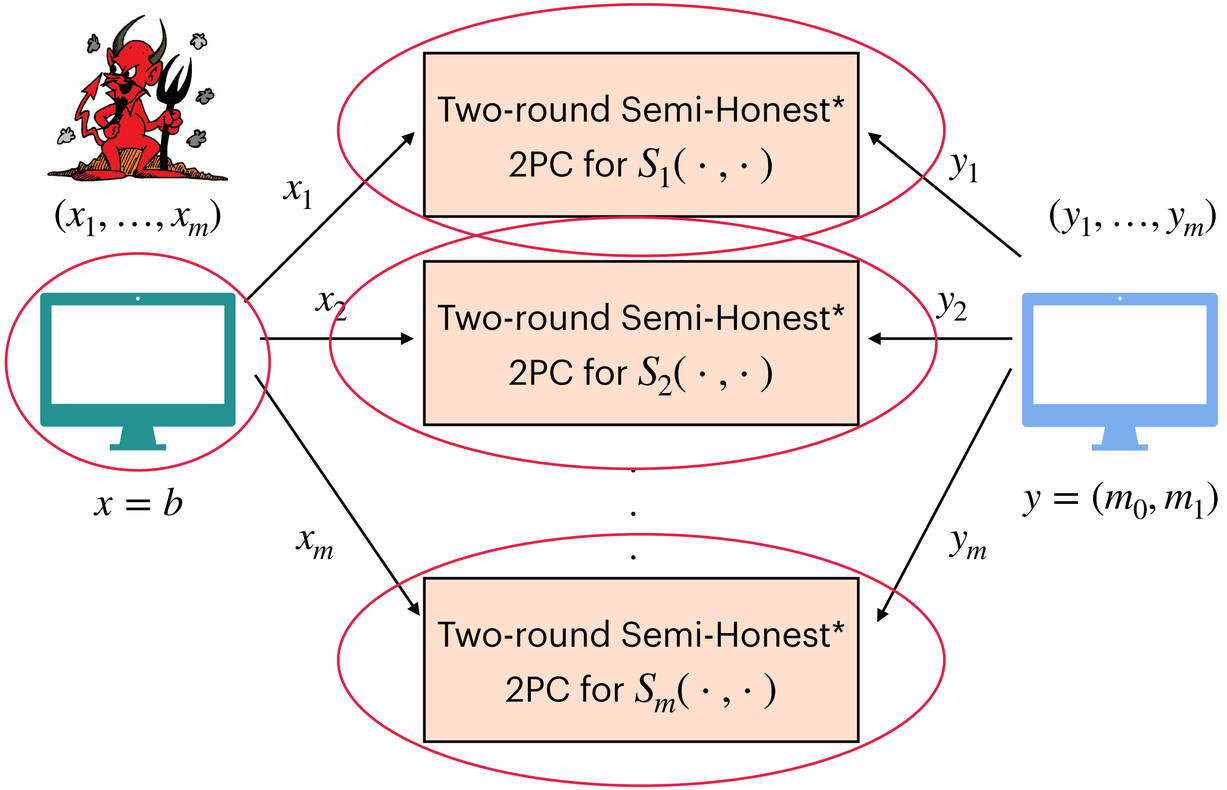
The IPS Compiled Protocol



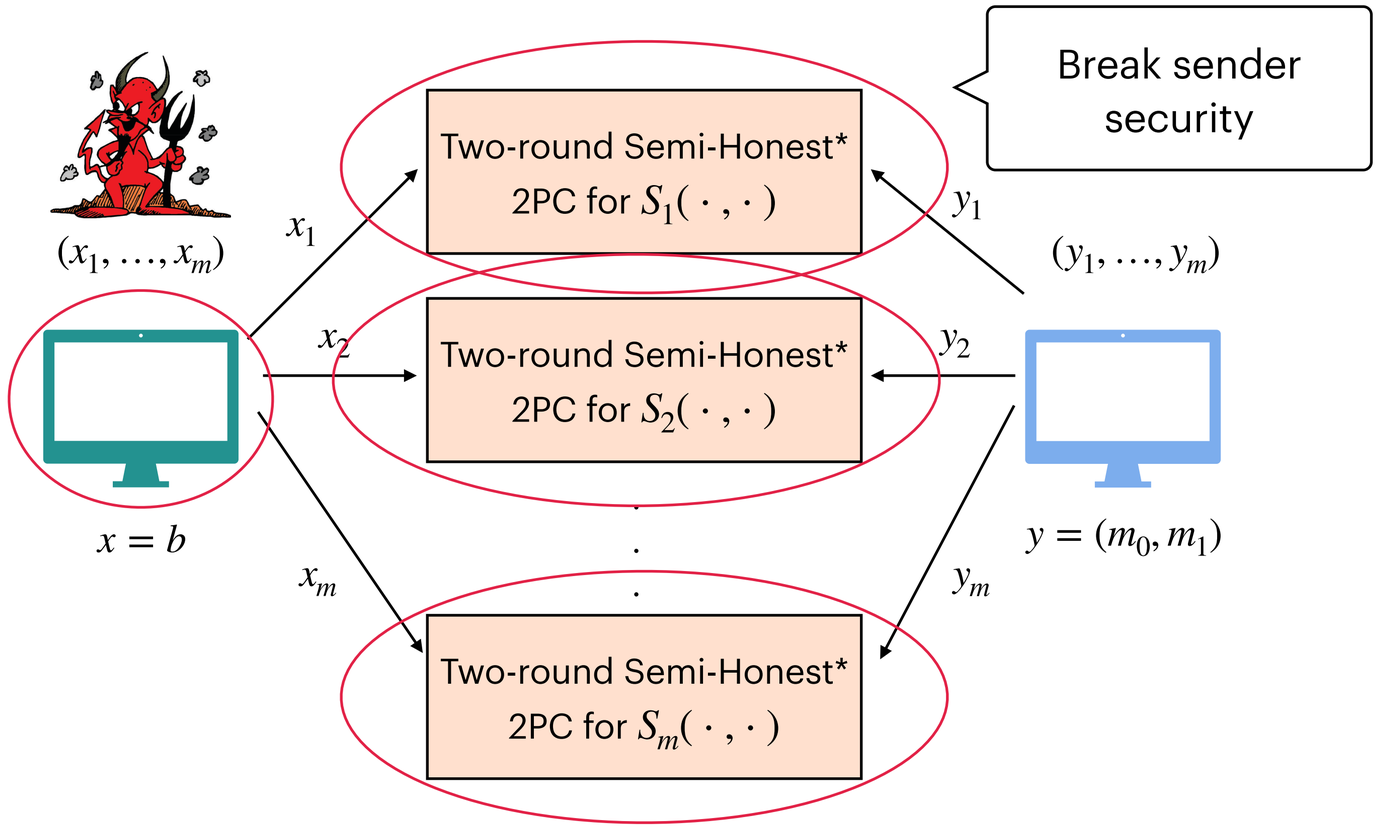
The IPS Compiled Protocol



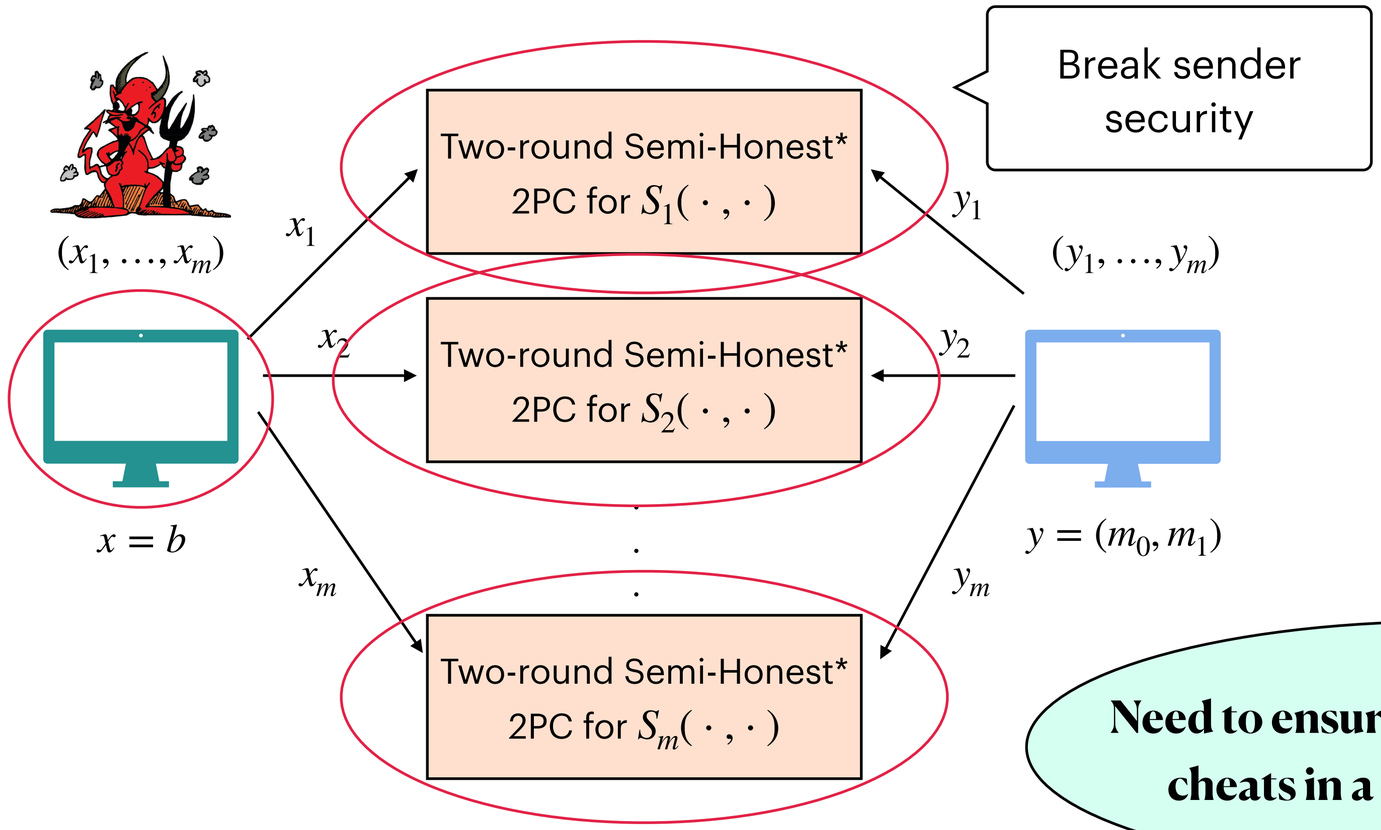
The IPS Compiled Protocol



The IPS Compiled Protocol

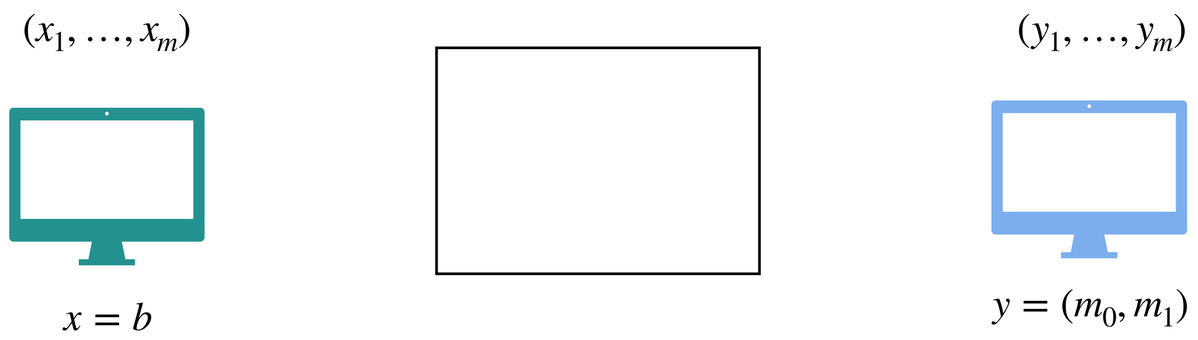


The IPS Compiled Protocol

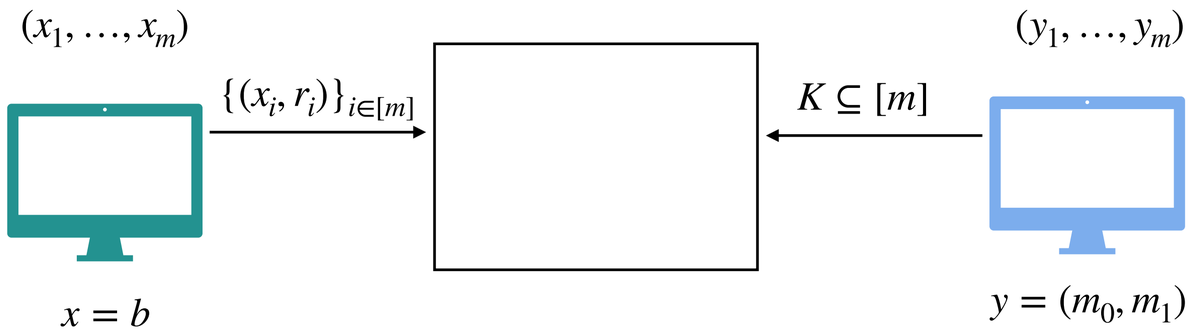


Need to ensure that adversary only cheats in a constant fraction

Role of Watchlist Protocol

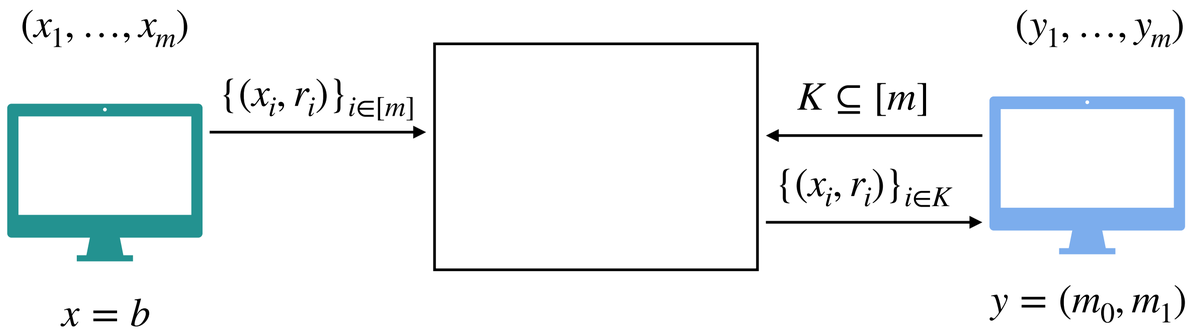


Role of Watchlist Protocol



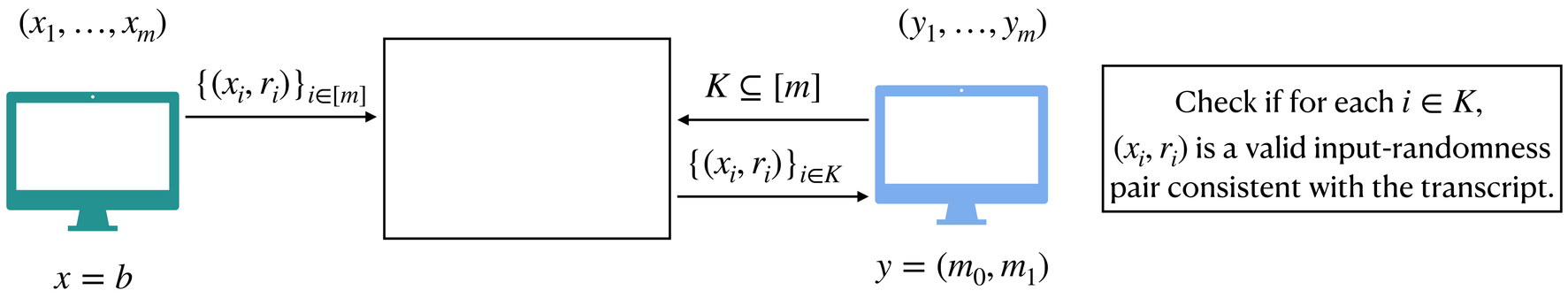
Watchlist Protocol

Role of Watchlist Protocol



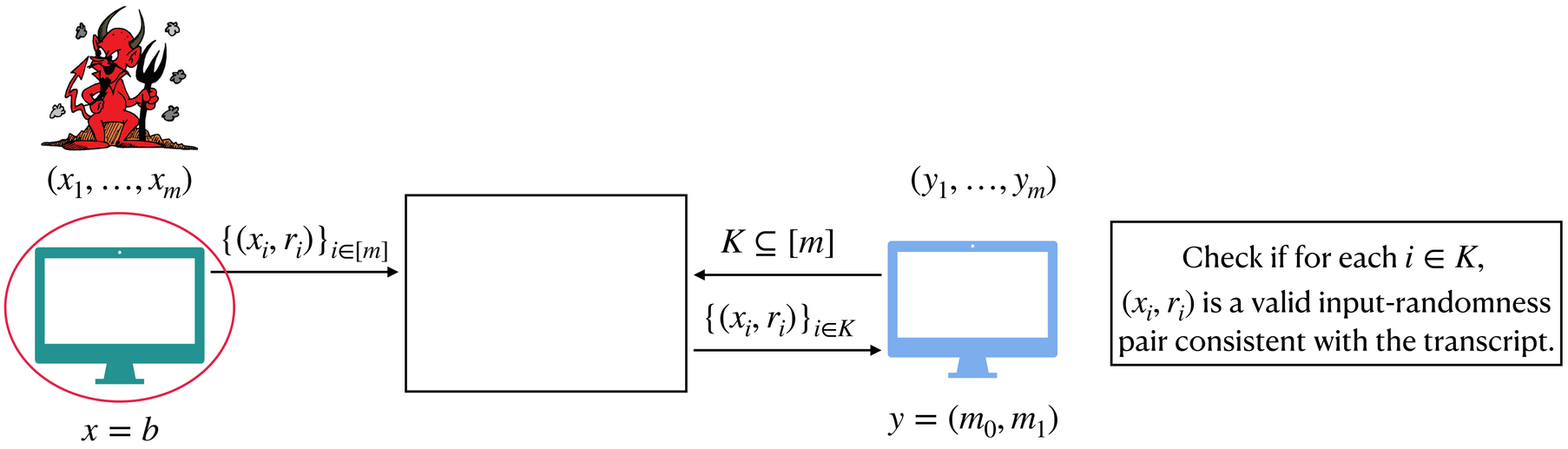
Watchlist Protocol

Role of Watchlist Protocol



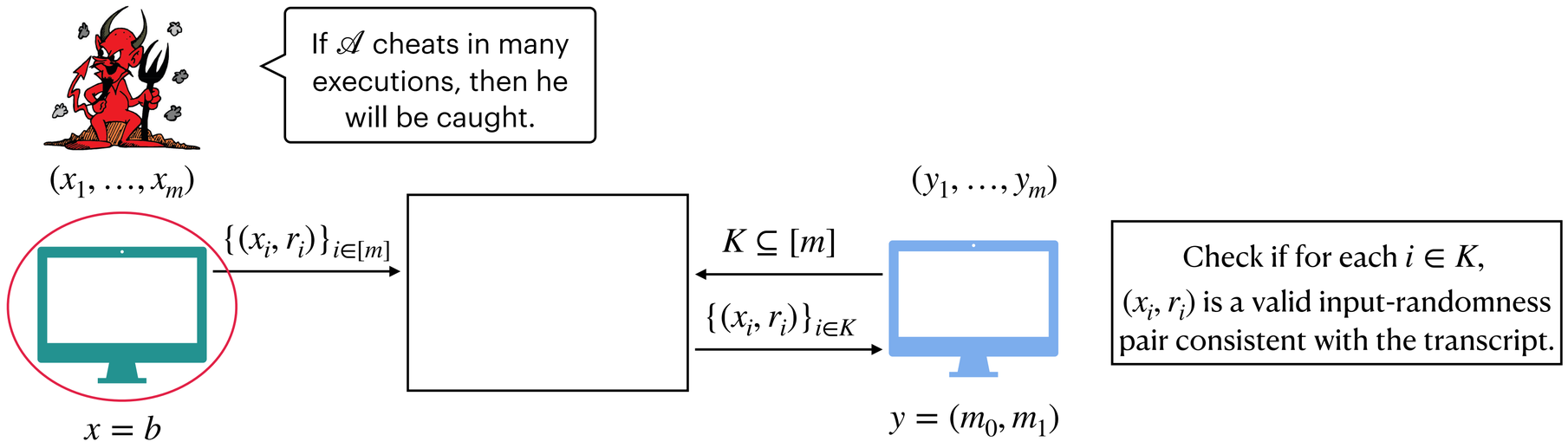
Watchlist Protocol

Role of Watchlist Protocol



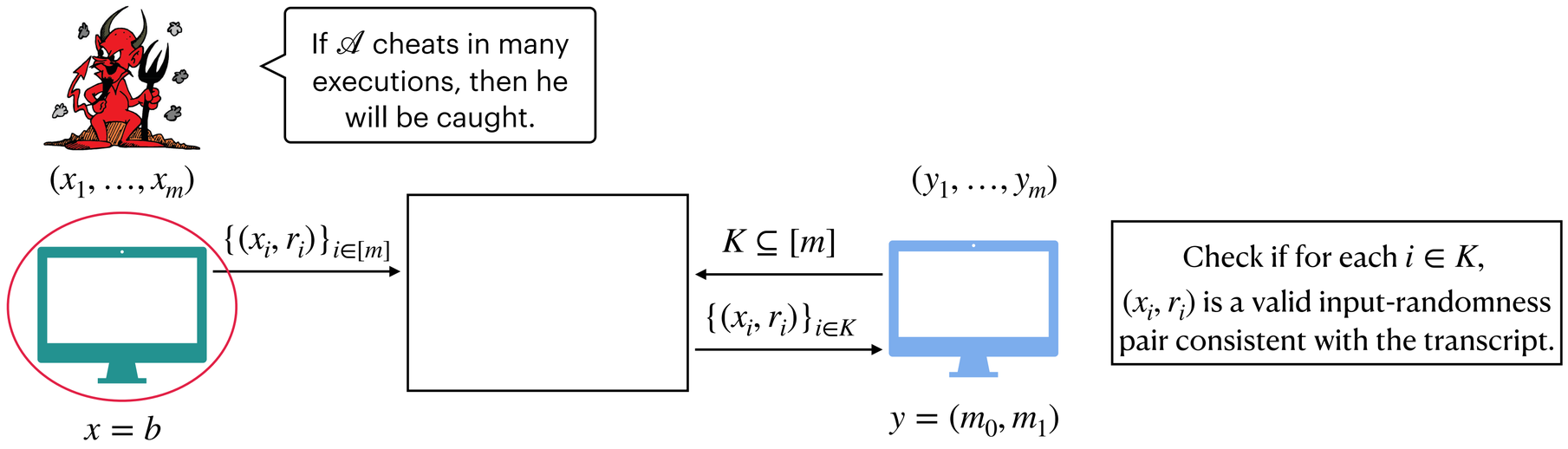
Watchlist Protocol

Role of Watchlist Protocol



Watchlist Protocol

Role of Watchlist Protocol



Watchlist Protocol

Construction of watchlist protocol requires malicious OT

Our Solution

K need not be kept secret but needs to be randomly chosen after the receiver message.

Our Solution

K need not be kept secret but needs to be randomly chosen after the receiver message.

$(x_1, \ldots, x_m)$

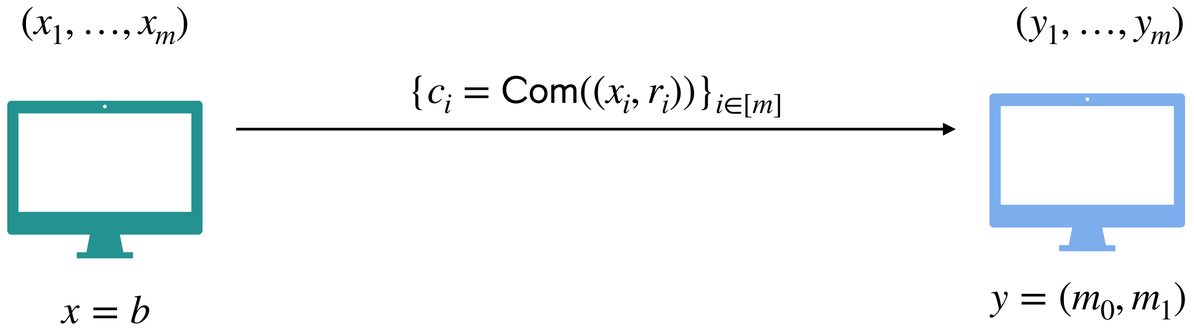
$x = b$

$(y_1, \ldots, y_m)$

$y = (m_0, m_1)$

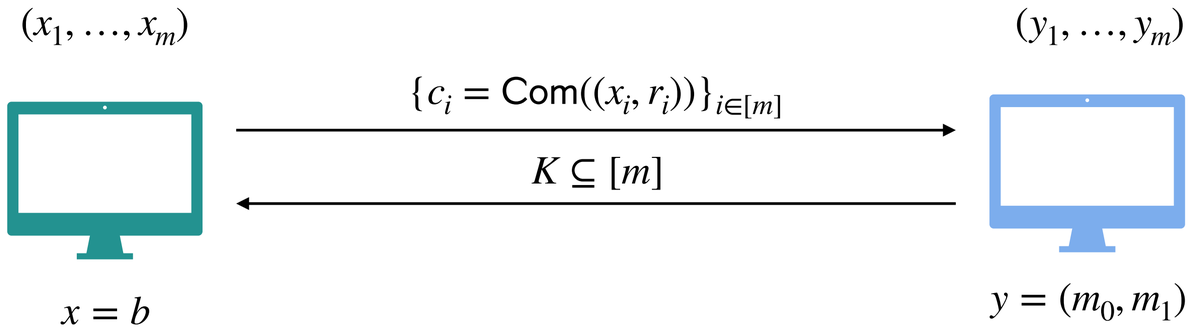
Our Solution

K need not be kept secret but needs to be randomly chosen after the receiver message.



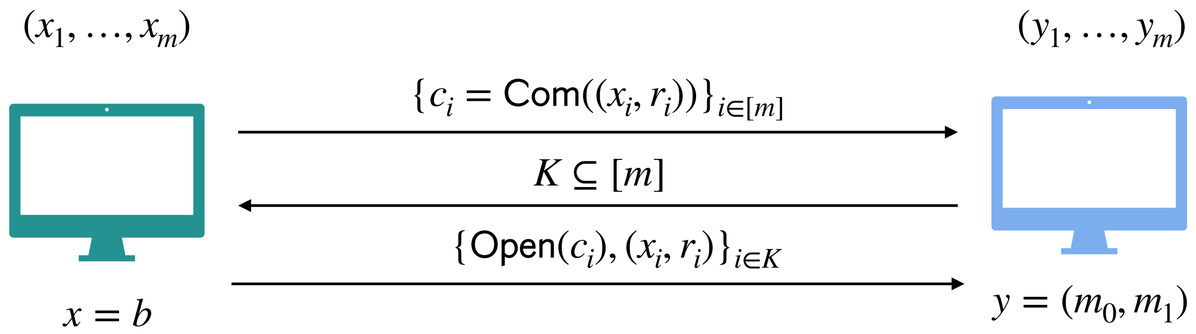
Our Solution

K need not be kept secret but needs to be randomly chosen after the receiver message.



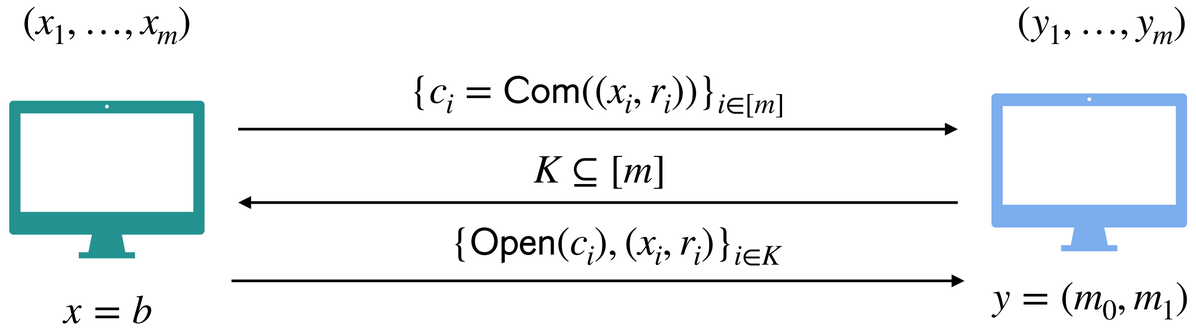
Our Solution

K need not be kept secret but needs to be randomly chosen after the receiver message.



Our Solution

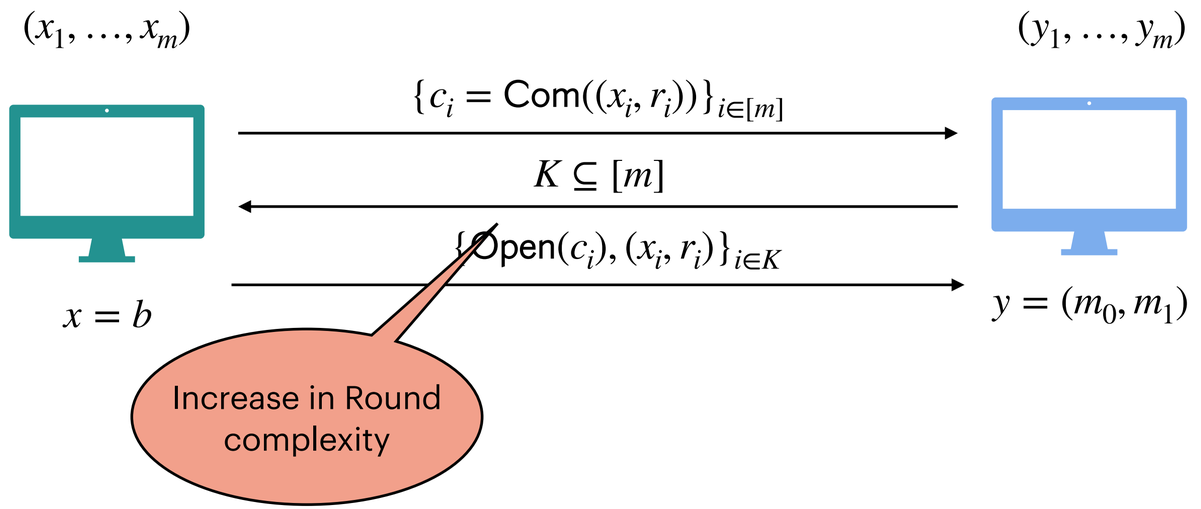
K need not be kept secret but needs to be randomly chosen after the receiver message.



Check if for each $i \in K$, (x_i, r_i) is a valid input-randomness pair consistent with the transcript.

Our Solution

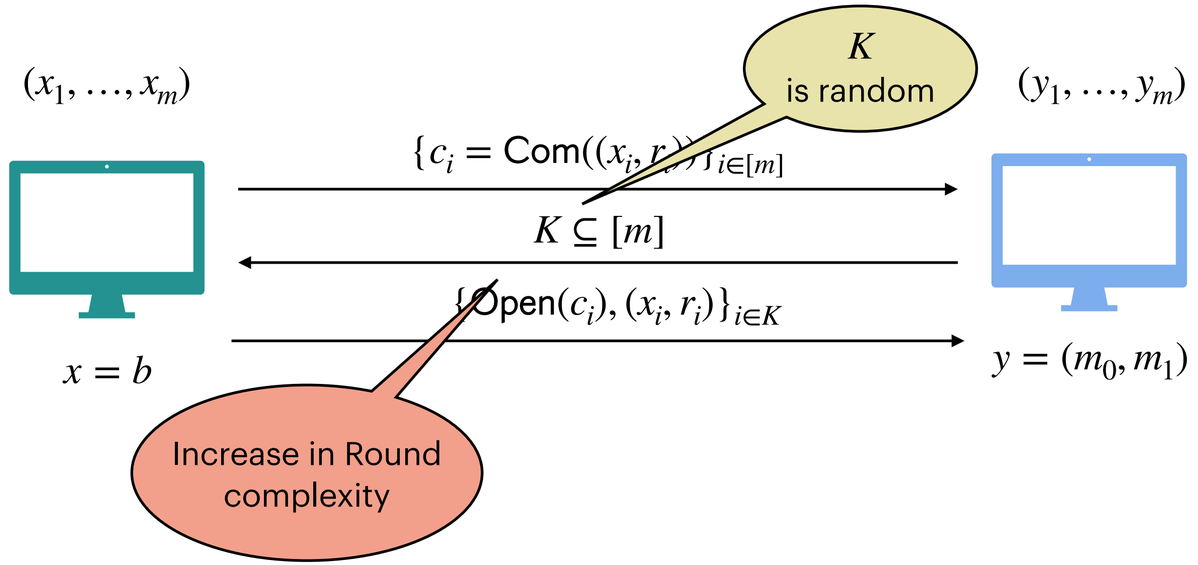
K need not be kept secret but needs to be randomly chosen after the receiver message.



Check if for each $i \in K$, (x_i, r_i) is a valid input-randomness pair consistent with the transcript.

Our Solution

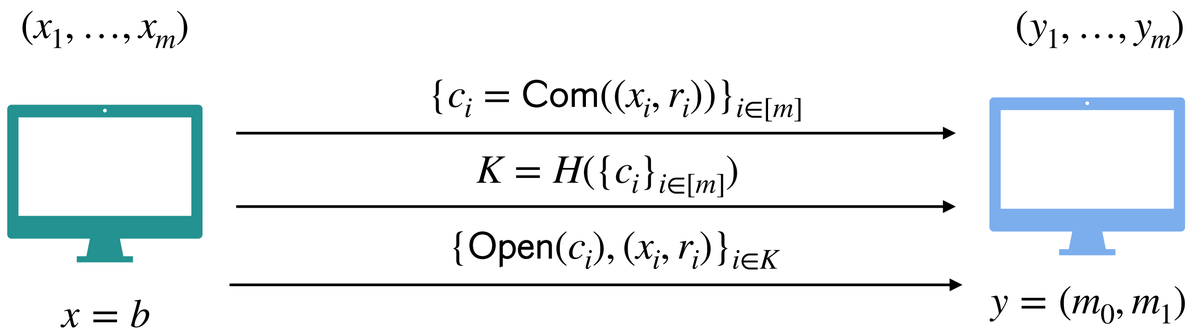
K need not be kept secret but needs to be randomly chosen after the receiver message.



Check if for each $i \in K$, (x_i, r_i) is a valid input-randomness pair consistent with the transcript.

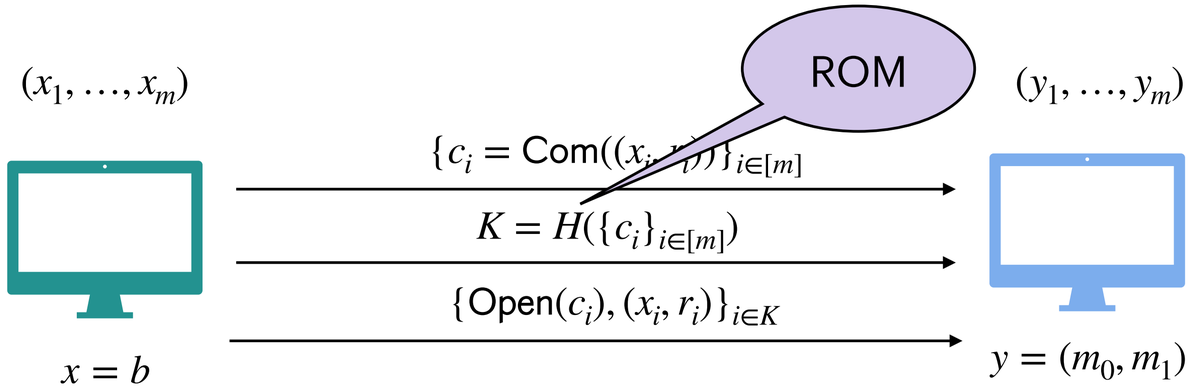
Our Solution

Fiat-Shamir paradigm

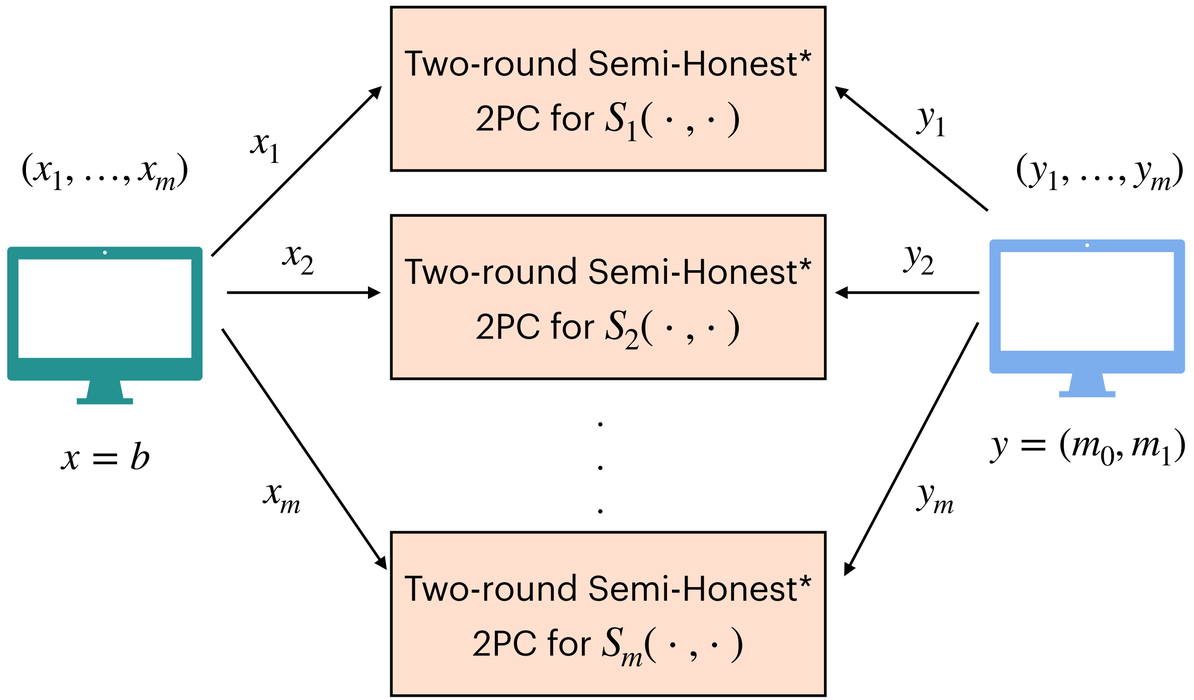


Our Solution

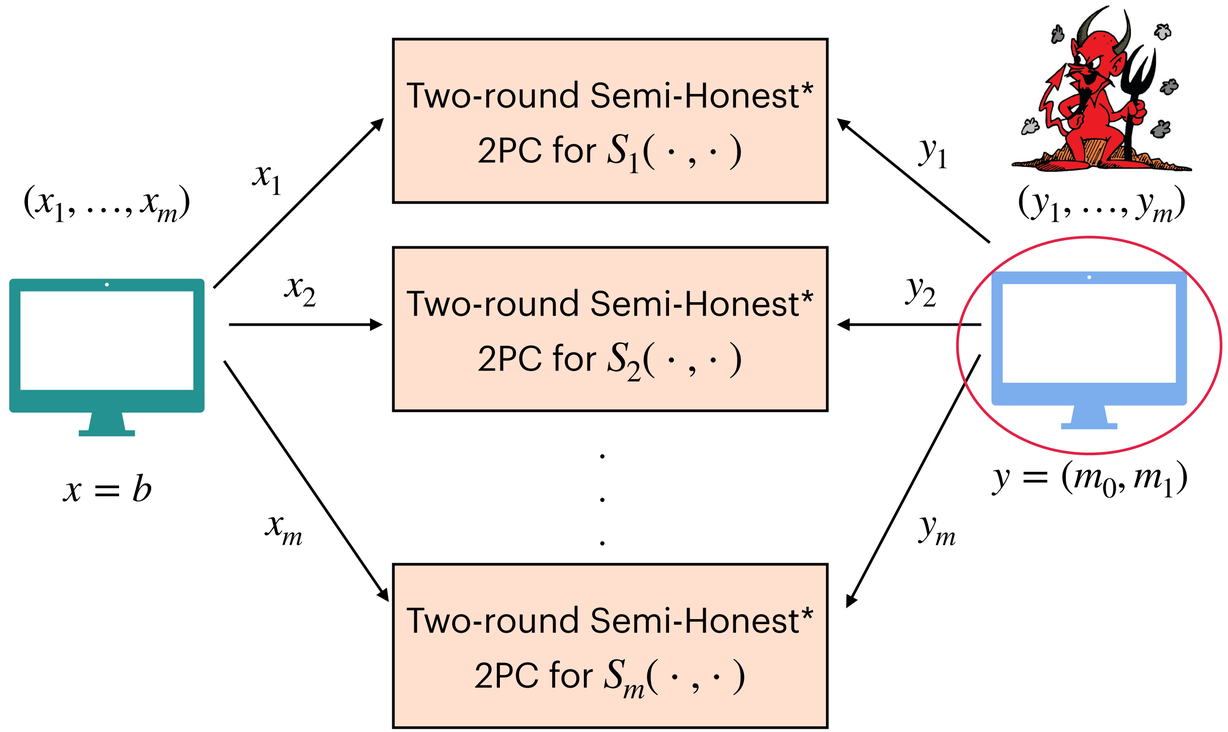
Fiat-Shamir paradigm



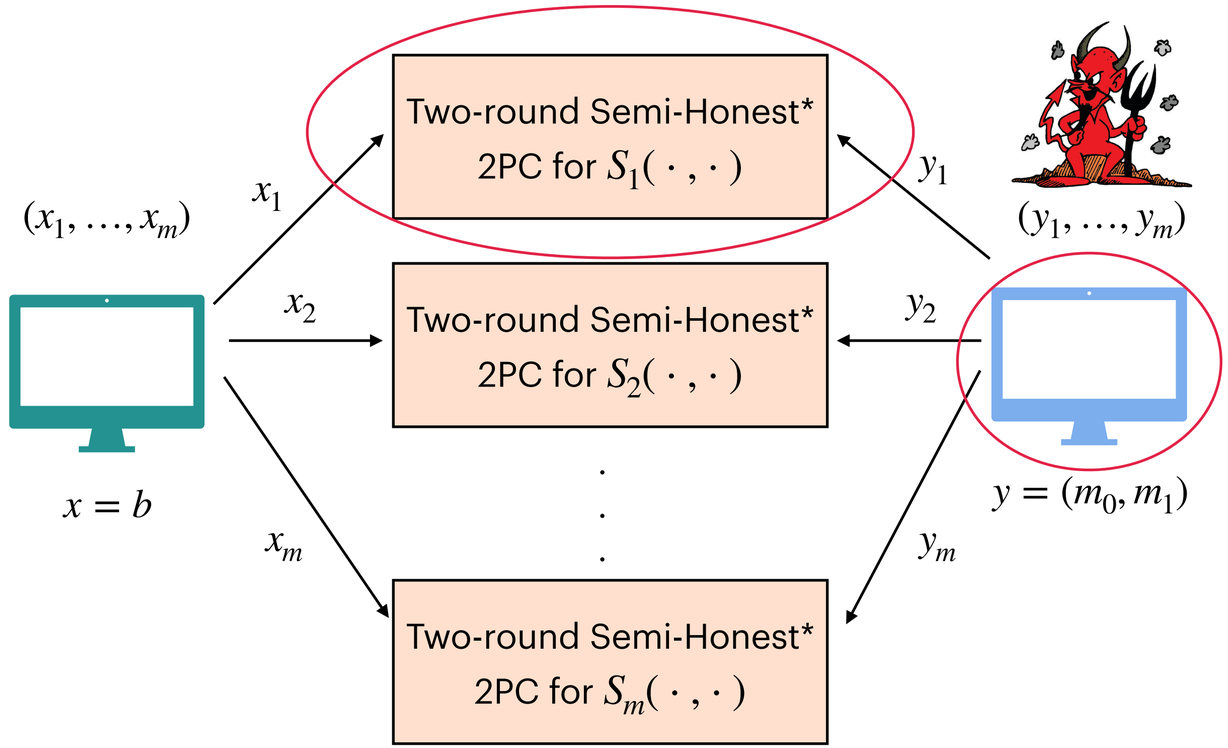
Dealing with Adaptive Security with Erasures



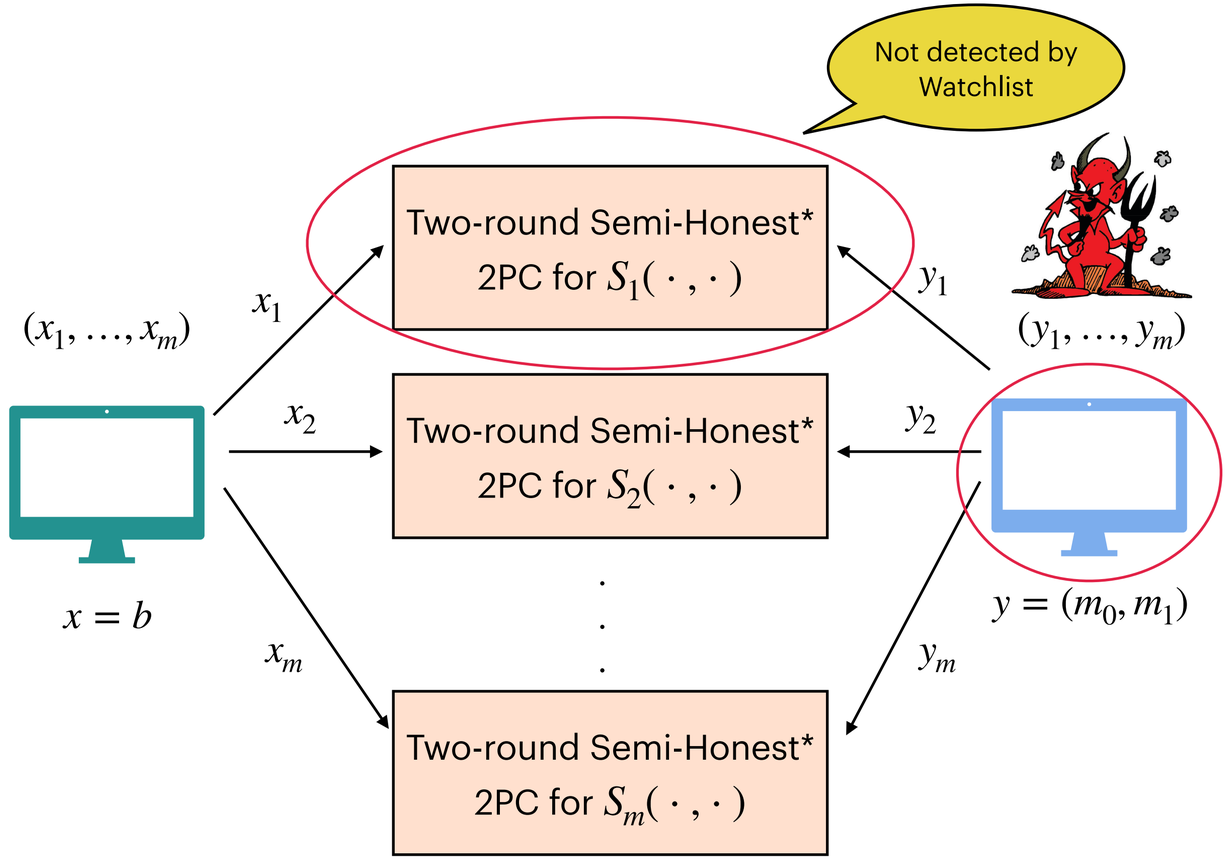
Dealing with Adaptive Security with Erasures



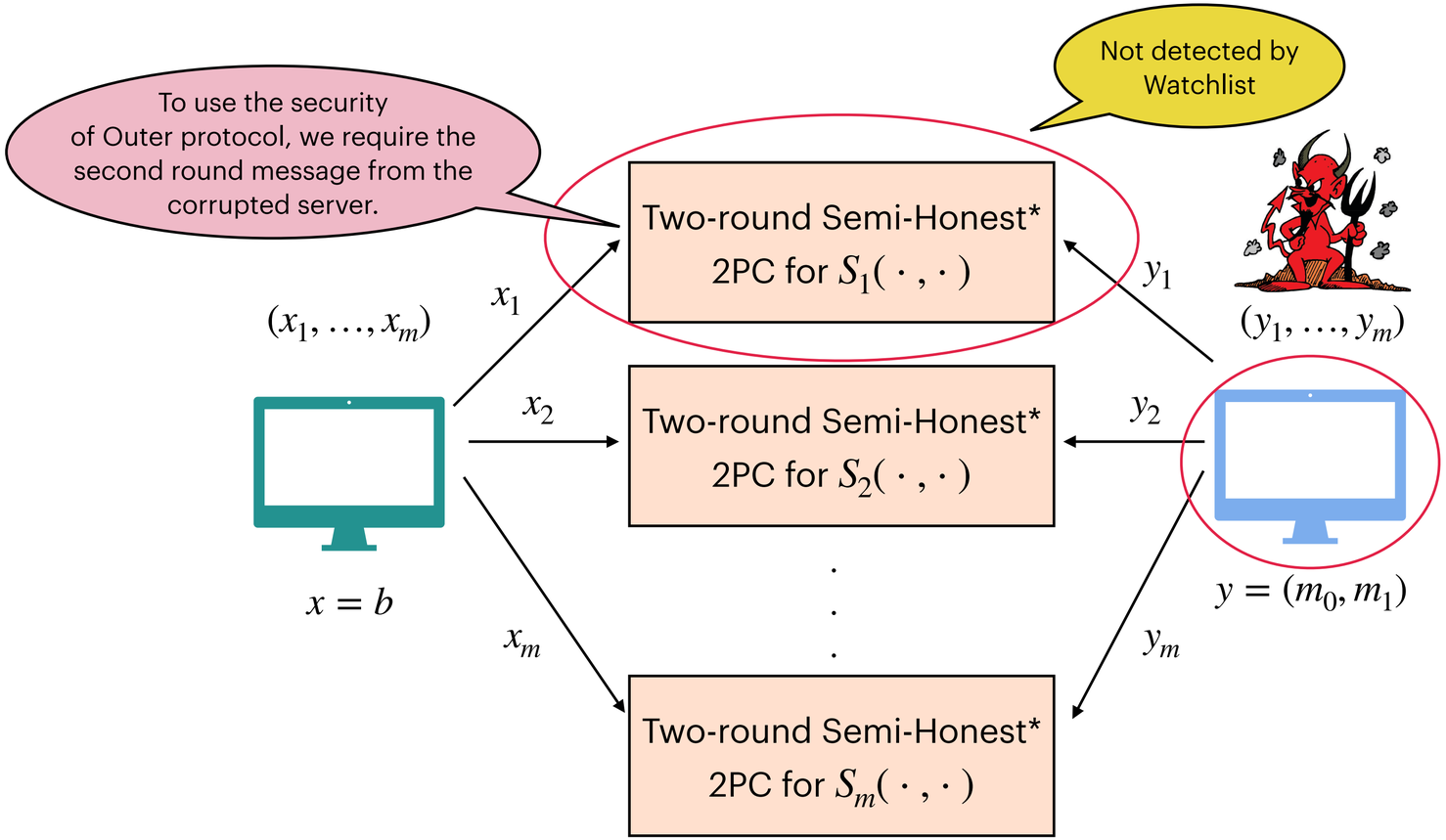
Dealing with Adaptive Security with Erasures



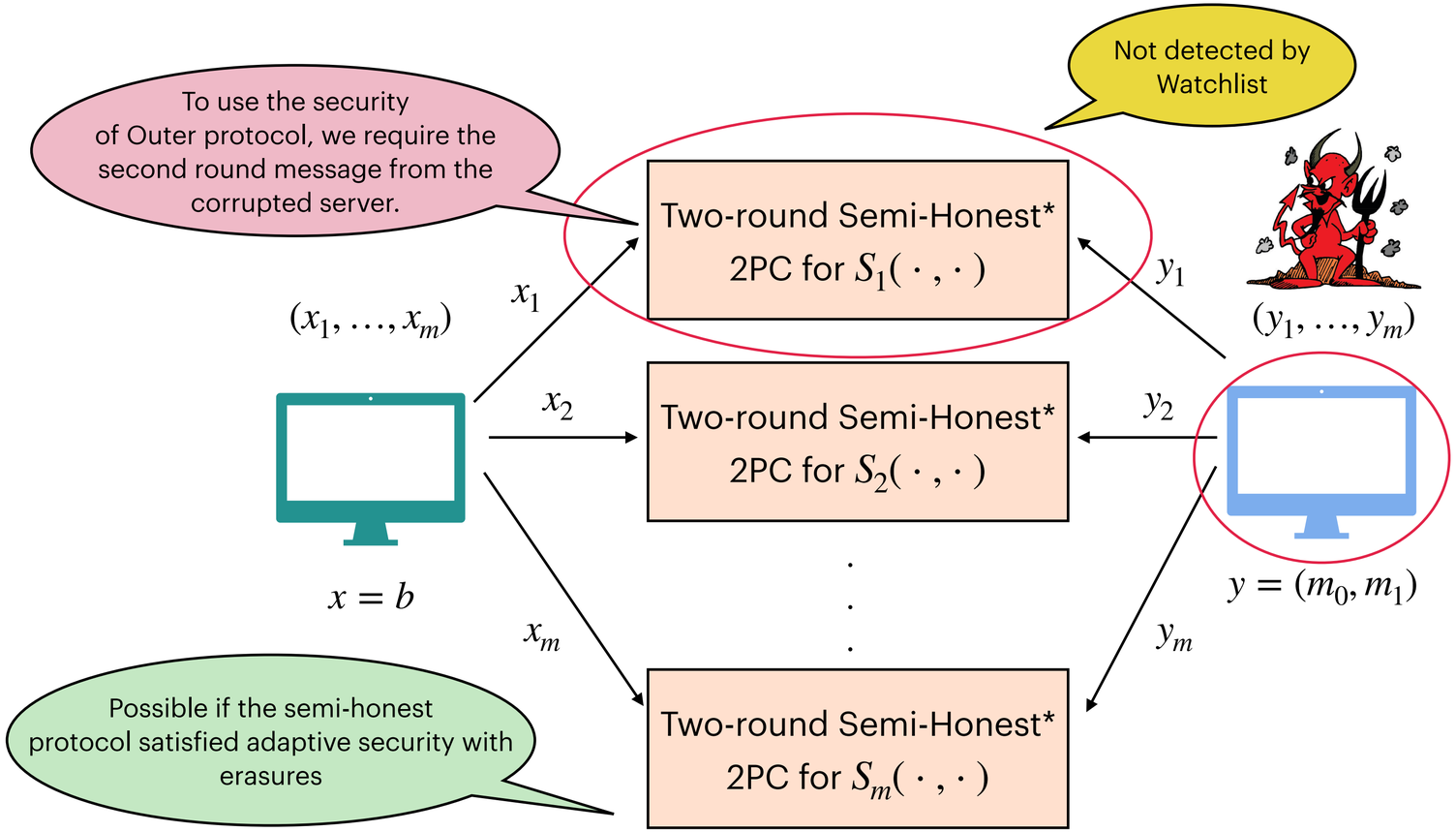
Dealing with Adaptive Security with Erasures



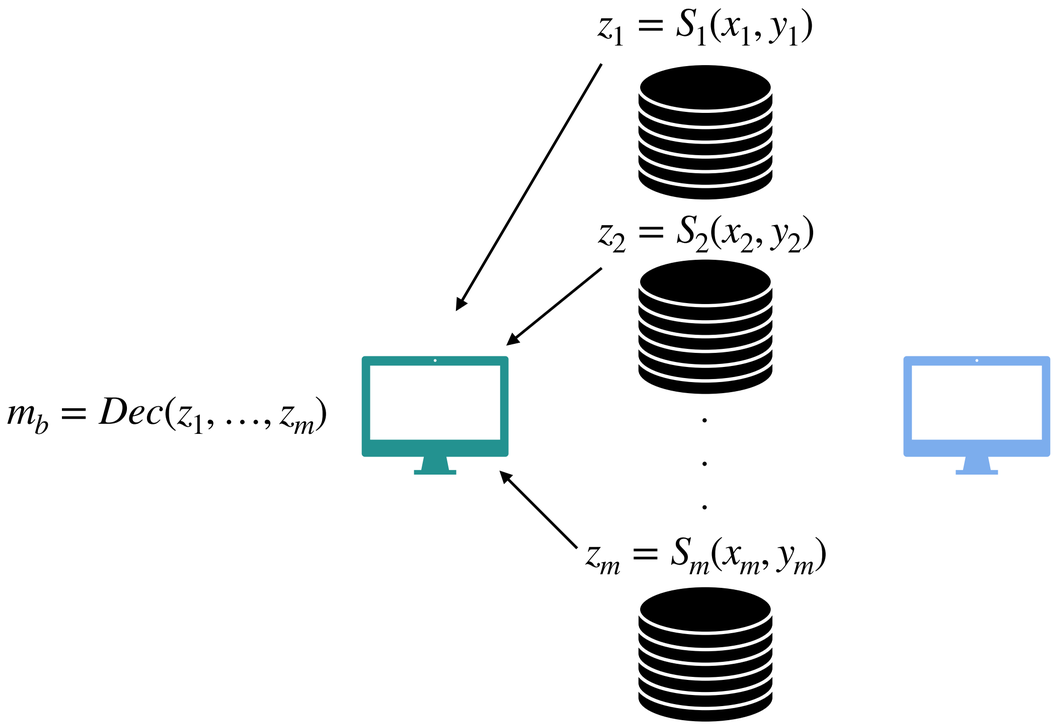
Dealing with Adaptive Security with Erasures



Dealing with Adaptive Security with Erasures

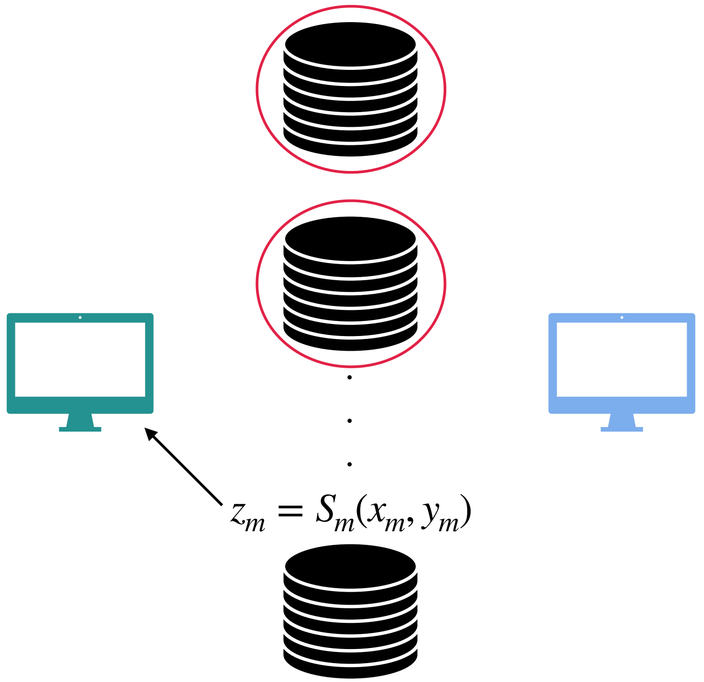


Stronger Outer Protocol



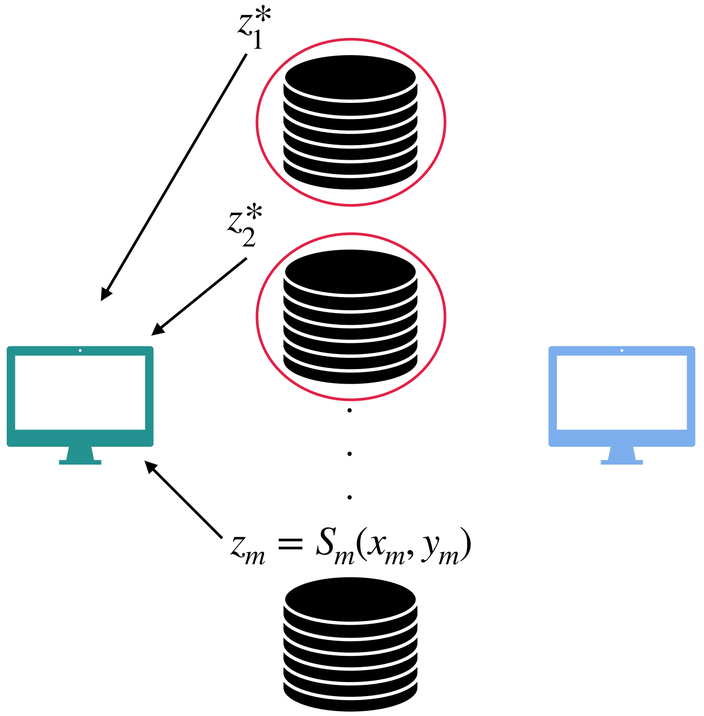
Outer Protocol

Stronger Outer Protocol



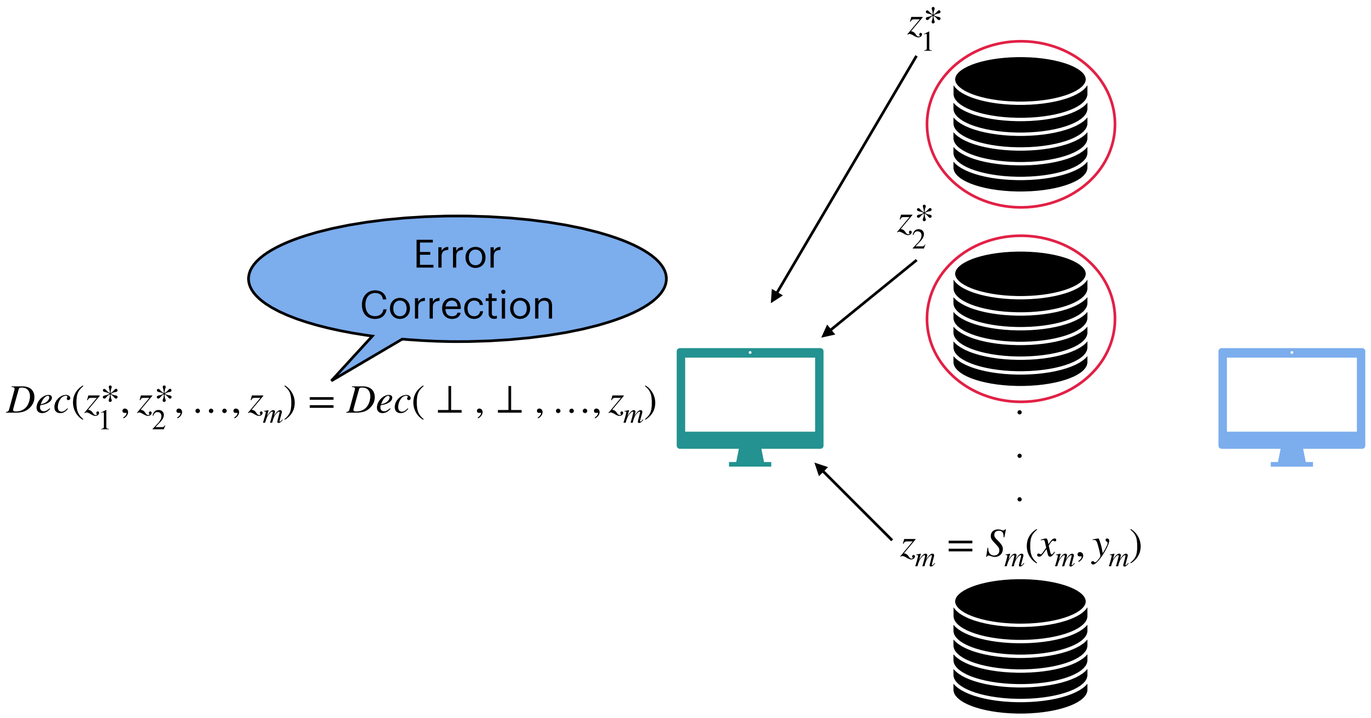
Outer Protocol

Stronger Outer Protocol



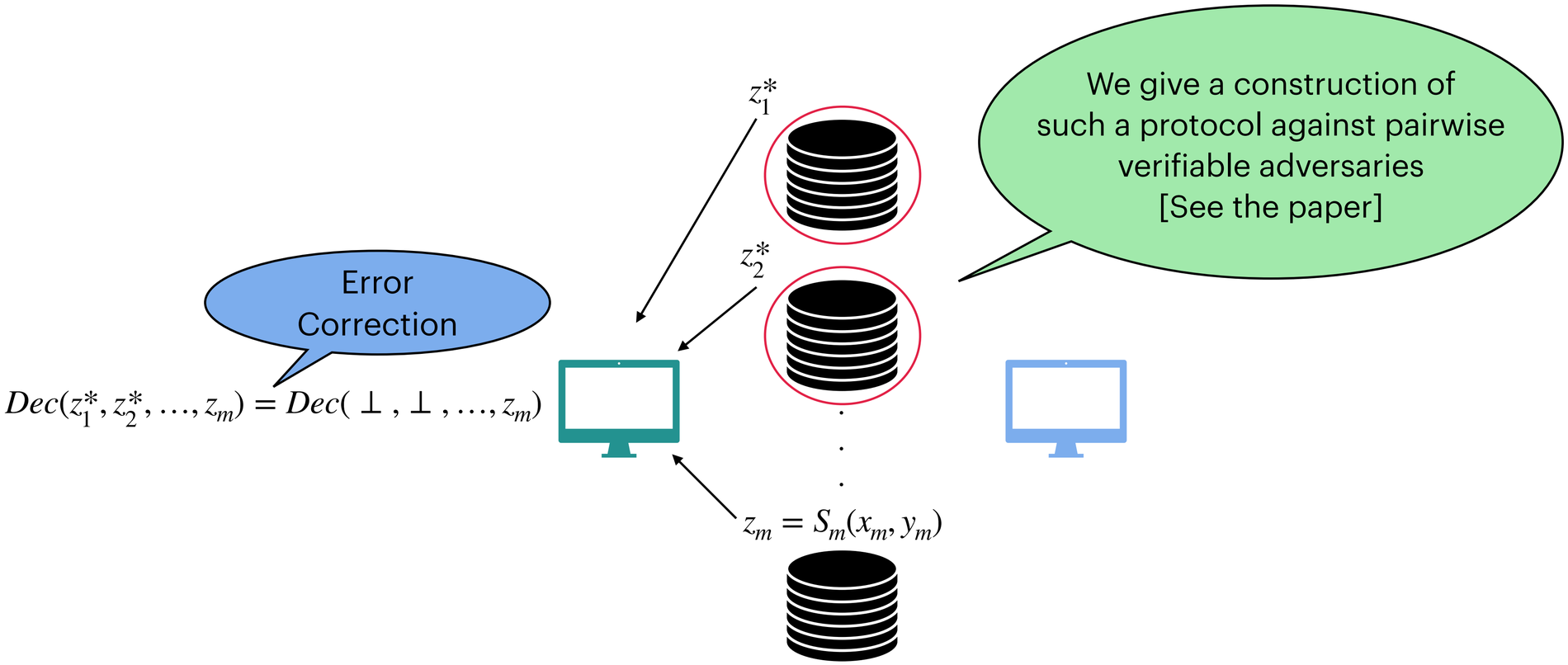
Outer Protocol

Stronger Outer Protocol



Outer Protocol

Stronger Outer Protocol



Outer Protocol

Conclusion

Conclusion

- We gave round-optimal constructions of two-party and multiparty protocols in the ROM (resp. OT correlations) model that made black-box use of Semi-Honest (resp. Semi-Malicious) protocols.

Conclusion

- We gave round-optimal constructions of two-party and multiparty protocols in the ROM (resp. OT correlations) model that made black-box use of Semi-Honest (resp. Semi-Malicious) protocols.
- Our construction can be viewed as a novel twist to the IPS compiler by strengthening the outer protocol to weaken the security of the inner protocol.

Conclusion

- We gave round-optimal constructions of two-party and multiparty protocols in the ROM (resp. OT correlations) model that made black-box use of Semi-Honest (resp. Semi-Malicious) protocols.
- Our construction can be viewed as a novel twist to the IPS compiler by strengthening the outer protocol to weaken the security of the inner protocol.
- **Open Problems:**

Conclusion

- We gave round-optimal constructions of two-party and multiparty protocols in the ROM (resp. OT correlations) model that made black-box use of Semi-Honest (resp. Semi-Malicious) protocols.
- Our construction can be viewed as a novel twist to the IPS compiler by strengthening the outer protocol to weaken the security of the inner protocol.
- **Open Problems:**
  - Remove the need for ROM.

Conclusion

- We gave round-optimal constructions of two-party and multiparty protocols in the ROM (resp. OT correlations) model that made black-box use of Semi-Honest (resp. Semi-Malicious) protocols.
- Our construction can be viewed as a novel twist to the IPS compiler by strengthening the outer protocol to weaken the security of the inner protocol.
- **Open Problems:**
  - Remove the need for ROM.
  - Other applications of the outer protocol?

Conclusion

- We gave round-optimal constructions of two-party and multiparty protocols in the ROM (resp. OT correlations) model that made black-box use of Semi-Honest (resp. Semi-Malicious) protocols.
- Our construction can be viewed as a novel twist to the IPS compiler by strengthening the outer protocol to weaken the security of the inner protocol.
- **Open Problems:**
  - Remove the need for ROM.
  - Other applications of the outer protocol?
  - Finding applications with good concrete efficiency.

Conclusion

- We gave round-optimal constructions of two-party and multiparty protocols in the ROM (resp. OT correlations) model that made black-box use of Semi-Honest (resp. Semi-Malicious) protocols.
- Our construction can be viewed as a novel twist to the IPS compiler by strengthening the outer protocol to weaken the security of the inner protocol.
- **Open Problems:**
  - Remove the need for ROM.
  - Other applications of the outer protocol?
  - Finding applications with good concrete efficiency.

Thank you!