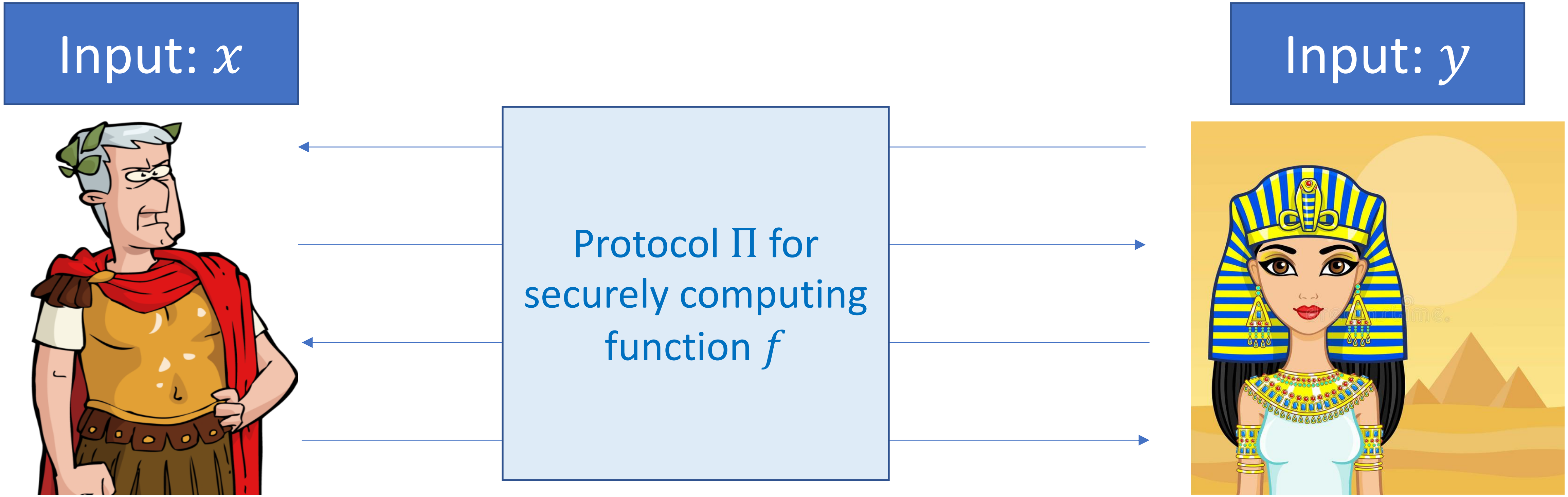
Statistical Security in Two-Party Computation Revisited

Pratik Sarkar (Boston University)

Joint work with

Saikrishna Badrinarayanan (Snap)
Sikhar Patranabis (IBM Research India)

Secure Two-Party Computation (2-PC)



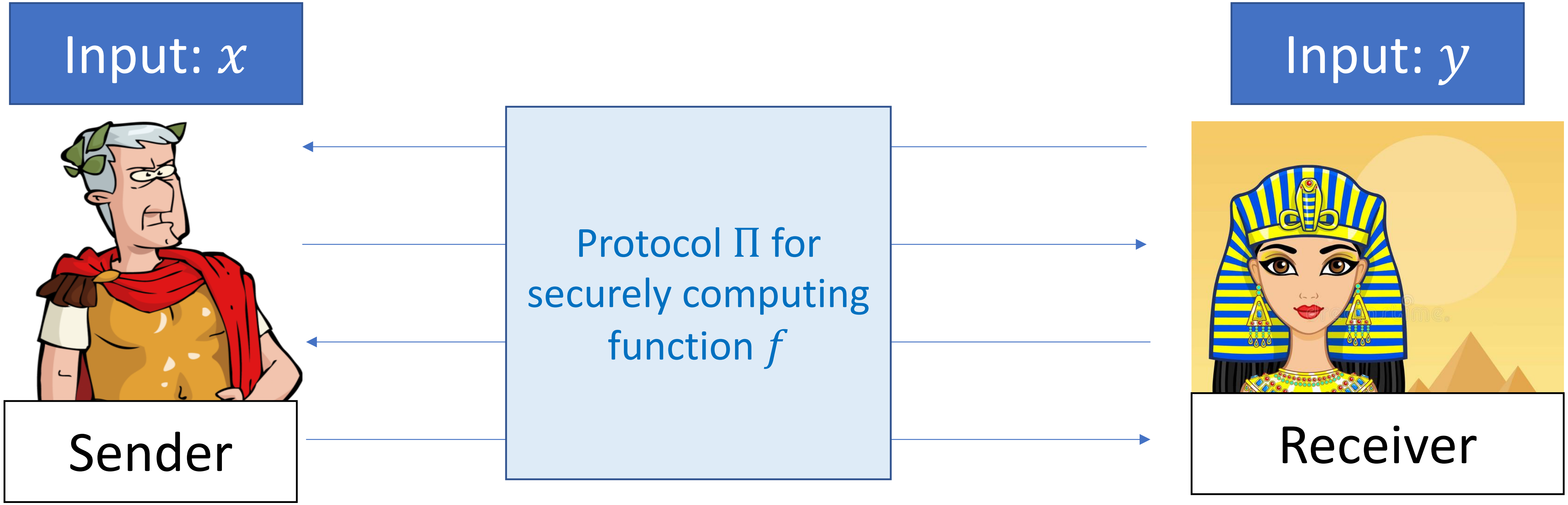
Input: x

Protocol Π for securely computing function f

Input: y

- Correctness: $\Pi(x, y) = f(x, y)$
- Security: Π leaks no information about x and y beyond $\Pi(x, y)$

Secure Two-Party Computation (2-PC)



Input: x

Sender

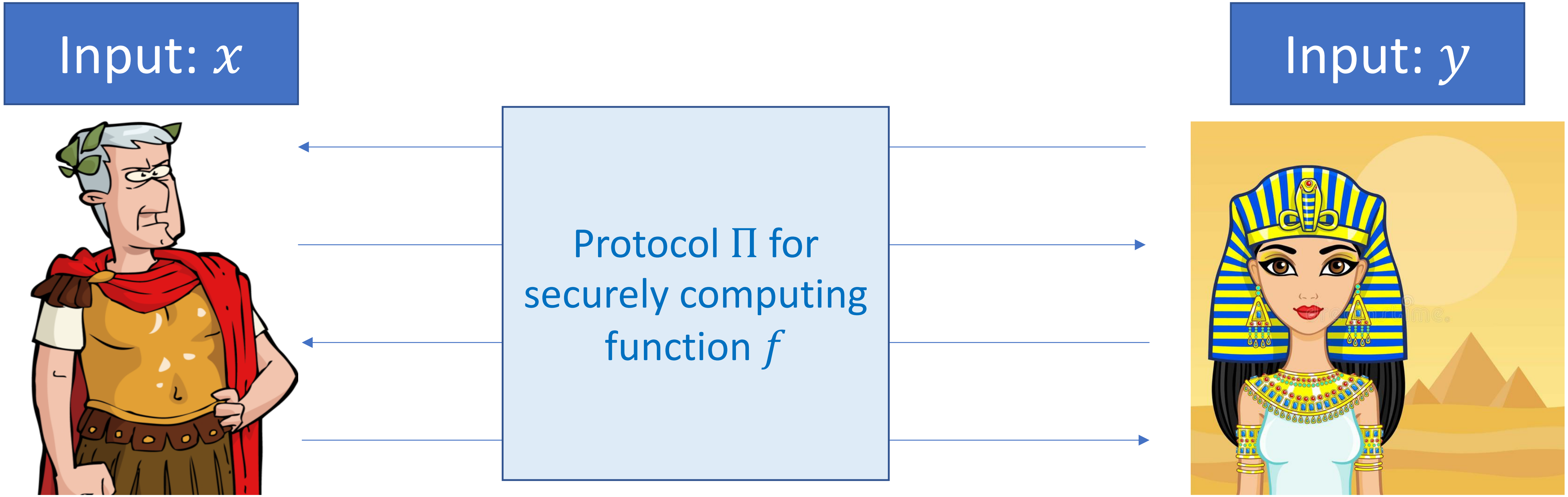
Protocol Π for securely computing function f

Input: y

Receiver

- We designate parties as **sender** and **receiver**
- If **only one** party gets the output, then that party is the **receiver**
- If **both** parties get the output, then the party that gets the output **earlier** is the **receiver**

Secure Two-Party Computation (2-PC)



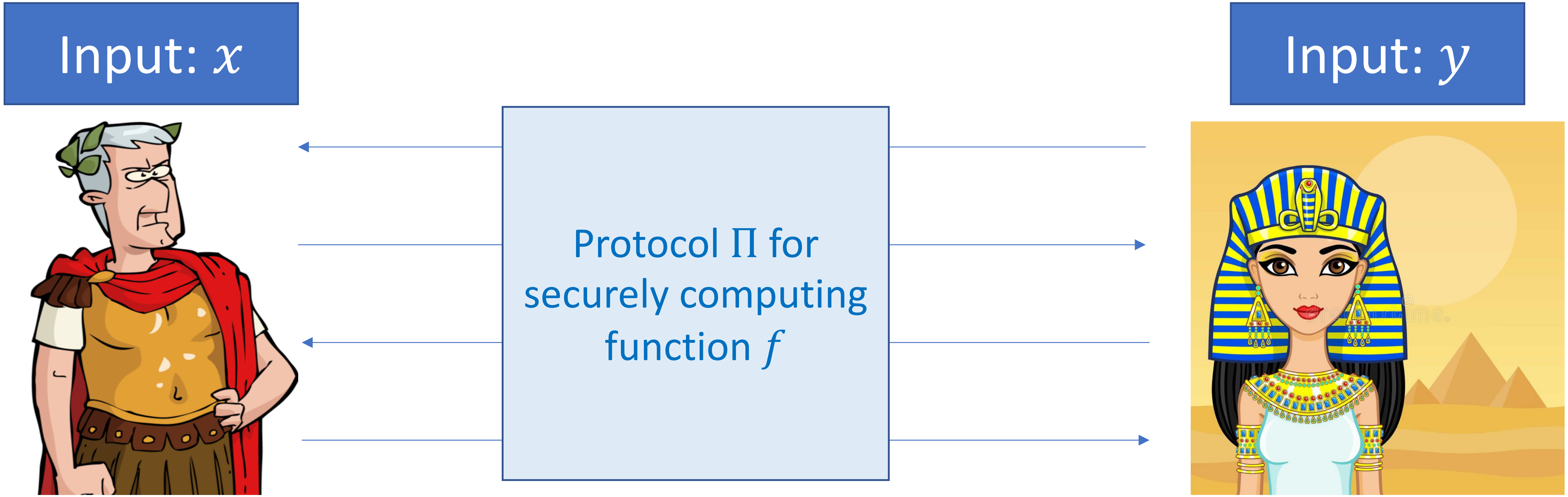
Input: x

Input: y

Protocol Π for securely computing function f

Focus of this talk: secure 2-PC in the plain model (no setup assumptions)

Secure Two-Party Computation (2-PC)



Input: x

Input: y

Protocol Π for securely computing function f

Message Exchange model: a round is a single message from one party to another (simultaneous messaging is **not** allowed)

This Talk

Our Focus

- Construct **round-optimal** 2-PC protocols (in the plain model):
    - with **one** of the two parties being **computationally unbounded**

This Talk

Our Focus

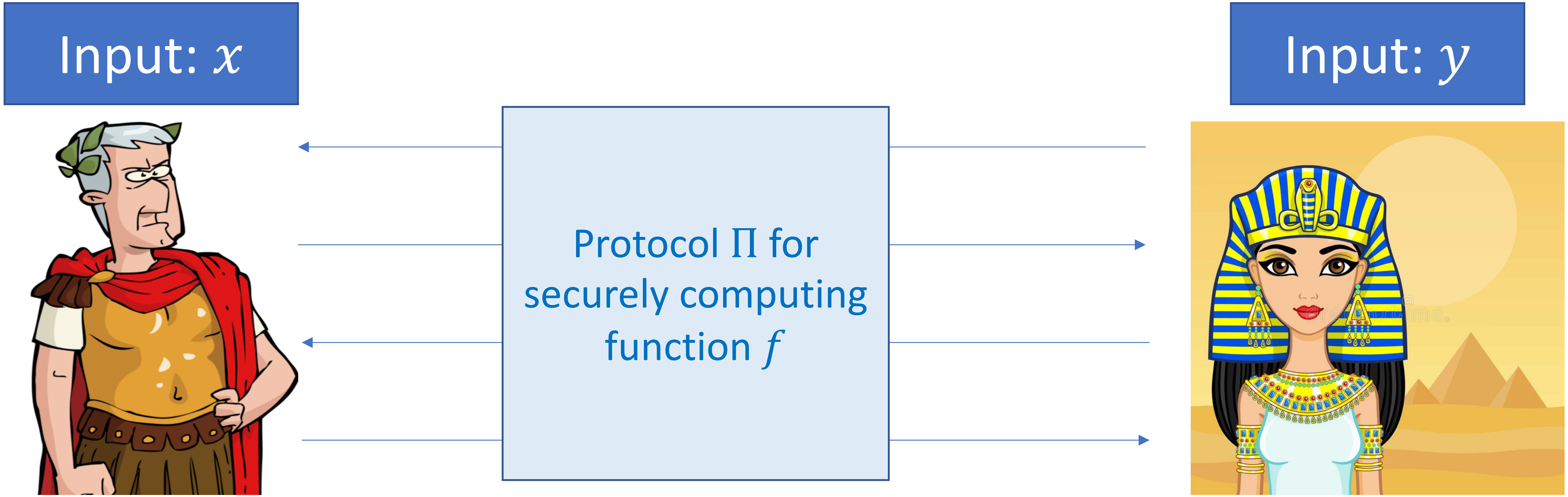
- Construct **round-optimal** 2-PC protocols (in the plain model):
  - with **one** of the two parties being **computationally unbounded**
  - with security against malicious corruptions

This Talk

Our Focus

- Construct **round-optimal** 2-PC protocols (in the plain model):
  - with **one** of the two parties being **computationally unbounded**
  - with security against malicious corruptions
  - with poly-time black-box simulation-based security

Round Complexity of 2-PC



Input: x

Protocol Π for securely computing function f

Input: y

Why care about round complexity?

- Fewer rounds impose less network latency
- Round optimal protocols have useful applications in cryptography

Round Complexity of 2-PC

Lower Bounds: [KatOst04]

- **4 rounds** are necessary if **only one party** wishes to get output
- **5 rounds** are necessary if **both parties** wish to get the output

Round Complexity of 2-PC

What if one of the two parties is **computationally unbounded?**

Lower Bound for ZK Proofs

- **5 rounds** are necessary for computational ZK proofs for NP with black-box simulation [Katz08]

Round Complexity of 2-PC

What if one of the two parties is **computationally unbounded?**

Lower Bound for ZK Proofs

- **5 rounds** are necessary for computational ZK proofs for NP with black-box simulation [Katz08]*

Unbounded Prover is the information-theoretic sender
Computational verifier is the computational receiver

Round Complexity of 2-PC

What if one of the two parties is **computationally unbounded?**

Lower Bound for ZK Proofs

- **5 rounds** are necessary for computational ZK proofs for NP with black-box simulation [Katz08]*

Unbounded Prover is the information-theoretic sender
Computational verifier is the computational receiver

Rules out **4 rounds** protocol when the sender is computationally unbounded

Round Complexity of 2-PC

What if one of the two parties is **computationally unbounded?**

Lower Bound for 2-PC: Summary

- **4 rounds** are necessary when only the receiver learns the output [KatOst04]
- **5 rounds** are necessary when both receiver and sender learn the output [KatOst04]
- **5 rounds** are necessary when the sender is computationally unbounded [Katz08]

Round Complexity of 2-PC

What if one of the two parties is **computationally unbounded?**

Lower Bound for 2-PC: Summary

- **4 rounds** are necessary when only the receiver learns the output [KatOst04]
- **5 rounds** are necessary when both receiver and sender learn the output [KatOst04]
- **5 rounds** are necessary when the sender is computationally unbounded [Katz08]

Optimal 2-PC (with black-box simulation) in 4 rounds

- Security against a **computationally unbounded receiver** and **computationally bounded sender**
- Termed as “One-sided Statistical Security” [KhuranaMughees20]
  - Focus of this talk

Chapter I

One Sided
Statistically Secure
2-PC

Related Work

What do we know about one-sided statistically secure 2-PC?

Related Work

What do we know about one-sided statistically secure 2-PC?

Matching Upper Bound [KM20]

- **4 rounds** sufficient when **only** receiver learns the output
- **5 rounds** sufficient when **both** receiver and sender learn the output

Related Work

What do we know about one-sided statistically secure 2-PC?

Matching Upper Bound [KM20]

- **4 rounds** sufficient when **only** receiver learns the output
- **5 rounds** sufficient when **both** receiver and sender learn the output

- **Ingredients:**
  - 2 round Statistically sender-private (SSP) OT

Related Work

What do we know about one-sided statistically secure 2-PC?

Matching Upper Bound [KM20]

- **4 rounds** sufficient when **only** receiver learns the output
- **5 rounds** sufficient when **both** receiver and sender learn the output

- **Ingredients:**
  - 2 round Statistically sender-private (SSP) OT

- Instantiations from **decisional hardness assumptions**:
  - DDH [NP01,HK12], QR/DCR [HK12], LWE [BD18], decisional CSIDH [ADMP20], LPN (extremely low-noise) + de-randomization [BF22]

Related Work

What do we know about one-sided statistically secure 2-PC?

Matching Upper Bound [KM20]

- **4 rounds** sufficient when **only** receiver learns the output
- **5 rounds** sufficient when **both** receiver and sender learn the output

- **Ingredients:**
  - 2 round Statistically sender-private (SSP) OT

Instantiations from computational assumptions, like CDH?

- Instantiations from **decisional hardness assumptions**:
  - DDH [NP01,HK12], QR/DCR [HK12], LWE [BD18], decisional CSIDH [ADMP20], LPN (extremely low-noise) + de-randomization [BF22]

Our Results

Our Contributions

- A new generic compiler for one-sided statistically-secure 2-PC

Our Results

Our Contributions

- A new generic compiler for one-sided statistically-secure 2-PC
- Relies on **weaker ingredients** (implied by 2 round SSP-OT)
    - Three round elementary OT (eOT) with statistical receiver privacy
    - Non-interactive commitments

Our Results

Our Contributions

- A new generic compiler for one-sided statistically-secure 2-PC
- Relies on **weaker ingredients** (implied by 2 round SSP-OT)
  - Three round elementary OT (eOT) with statistical receiver privacy
  - Non-interactive commitments
- Enables new instantiations from **computational hardness assumptions:**

Our Results

Our Contributions

- A new generic compiler for one-sided statistically-secure 2-PC

- Relies on **weaker ingredients** (implied by 2 round SSP-OT)
  - Three round elementary OT (eOT) with statistical receiver privacy
  - Non-interactive commitments

- Enables new instantiations from **computational hardness assumptions:**
  - *First* instantiation from CDH *and* reciprocal CSIDH (quantum equivalent to computational CSIDH)

Our Results

Our Contributions

- A new generic compiler for one-sided statistically-secure 2-PC

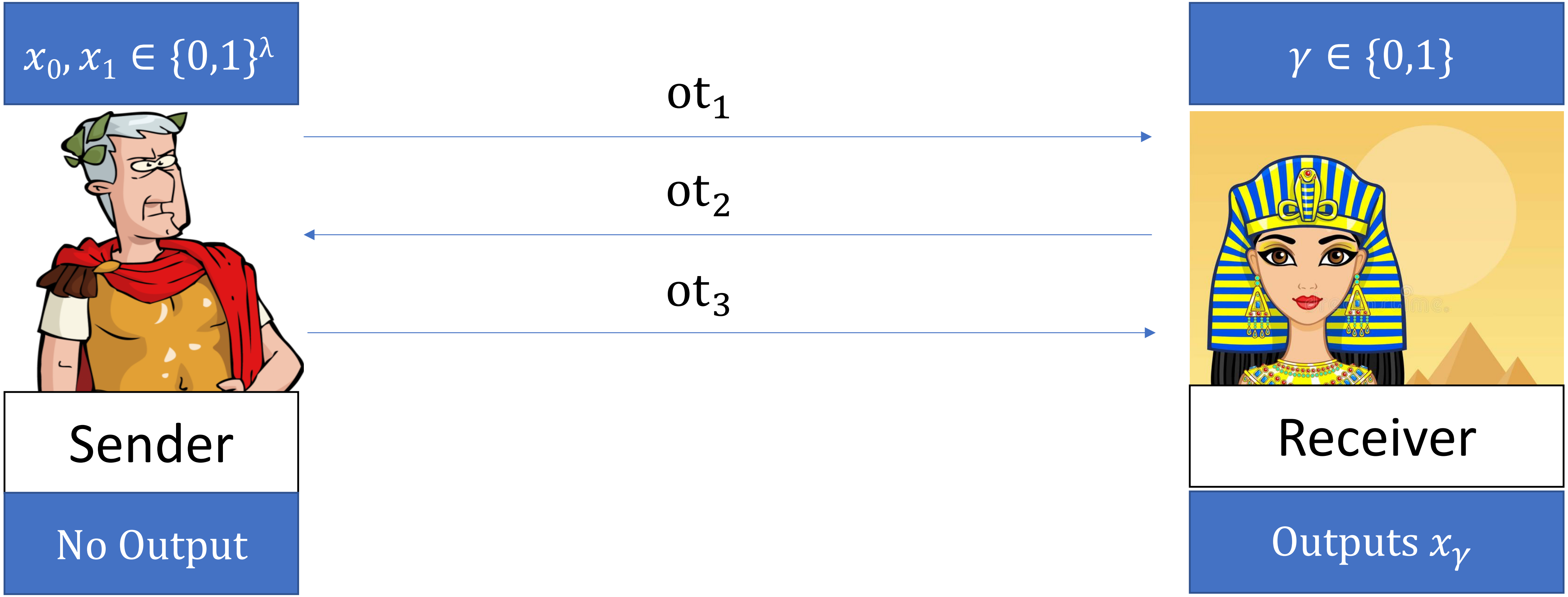
- Relies on **weaker ingredients** (implied by 2 round SSP-OT)
    - Three round elementary OT (eOT) with statistical receiver privacy
    - Non-interactive commitments

- Enables new instantiations from **computational hardness assumptions:**
    - *First* instantiation from CDH *and* reciprocal CSIDH (quantum equivalent to computational CSIDH)
    - Instantiations from *previous* decisional hardness assumptions

Chapter II

Elementary OT
(eOT)

Elementary OT (3-round statistically receiver private random-OT)



$x_0, x_1 \in \{0,1\}^\lambda$

Sender

No Output

ot_1

ot_2

ot_3

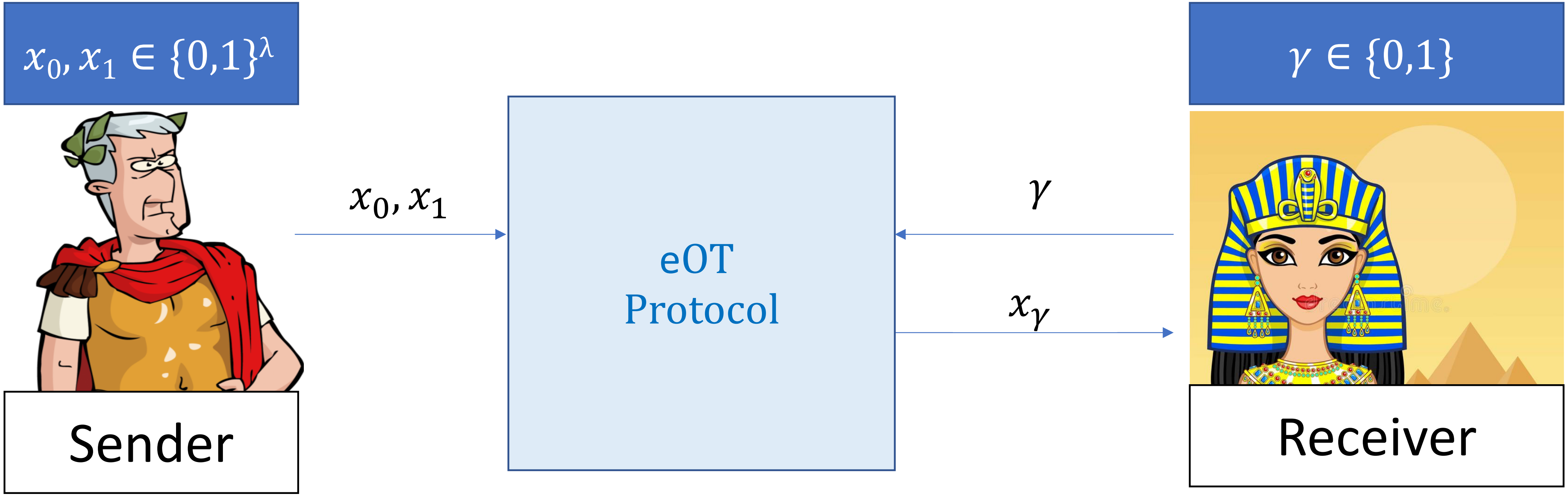
$\gamma \in \{0,1\}$

Receiver

Outputs x_γ

- 3-round OT protocol with sender sending the first message
- Sender is computationally unbounded, while receiver is computationally bounded

Elementary OT (3-round statistically receiver private random-OT)



$x_0, x_1 \in \{0,1\}^\lambda$

$\gamma \in \{0,1\}$

x_0, x_1

eOT Protocol

γ

x_γ

Sender

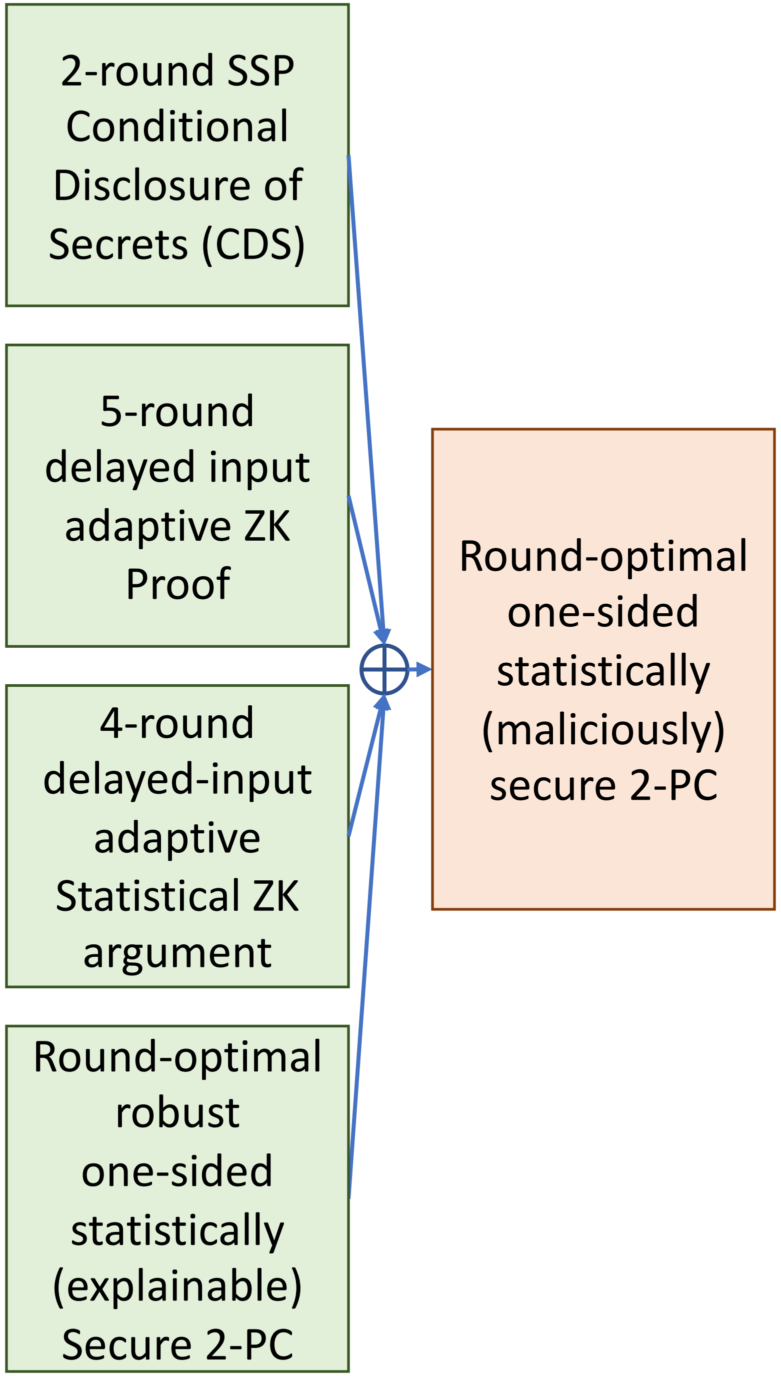
Receiver

- Correctness: Receiver outputs x_γ
- **Statistical Receiver Privacy (SRP):** γ is statistically hidden from the (computationally unbounded) sender
- **Elementary Sender Privacy:** the (computationally bounded) receiver cannot compute both x_0 and x_1

Chapter III

Compilers
for
One-Sided
Statistical 2PC

[KM20] Compiler



2-round SSP Conditional Disclosure of Secrets (CDS)

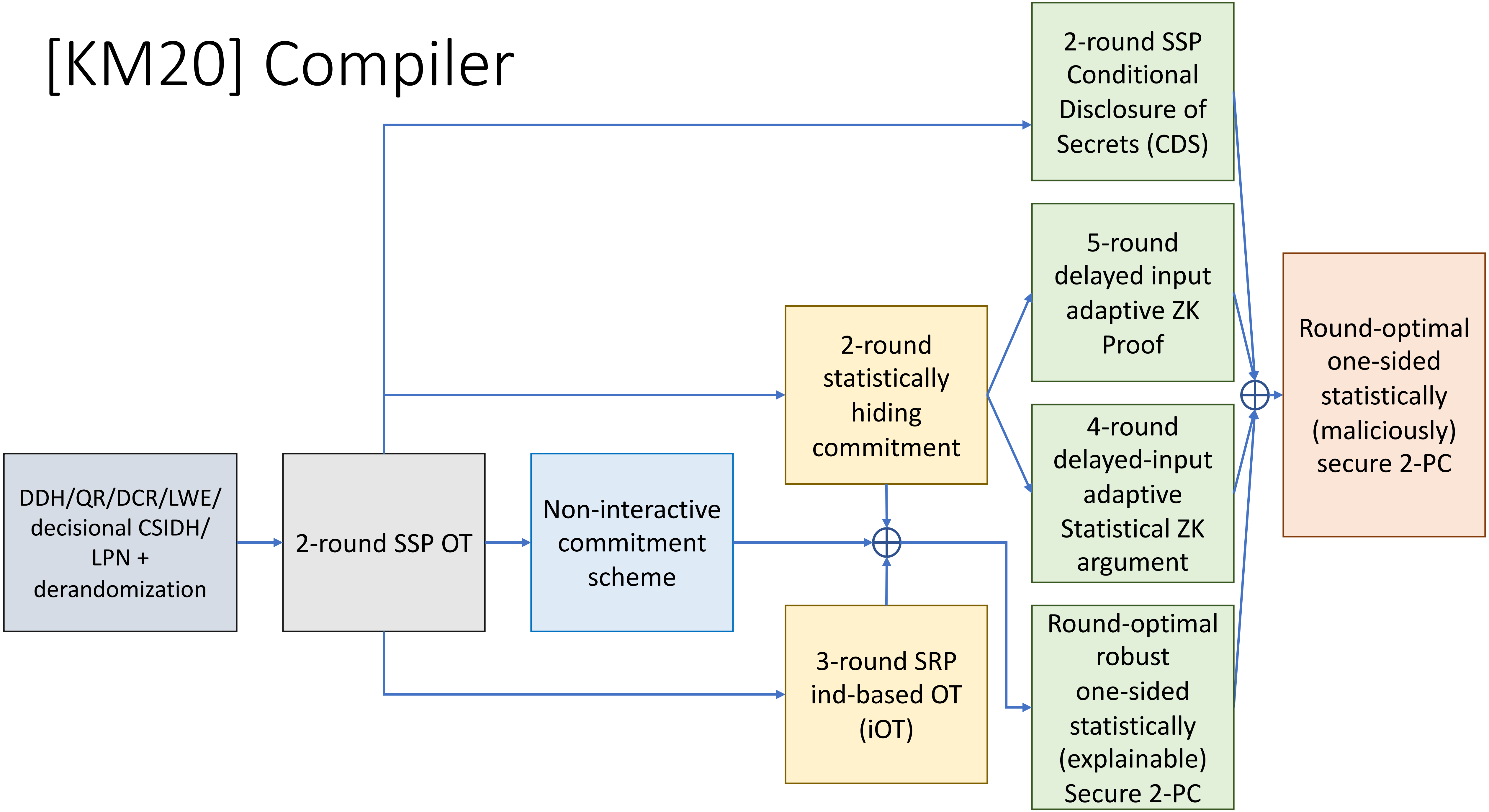
5-round delayed input adaptive ZK Proof

4-round delayed-input adaptive Statistical ZK argument

Round-optimal robust one-sided statistically (explainable) Secure 2-PC

Round-optimal one-sided statistically (maliciously) secure 2-PC

[KM20] Compiler



DDH/QR/DCR/LWE/ decisional CSIDH/ LPN + derandomization

2-round SSP OT

Non-interactive commitment scheme

2-round statistically hiding commitment

3-round SRP ind-based OT (iOT)

2-round SSP Conditional Disclosure of Secrets (CDS)

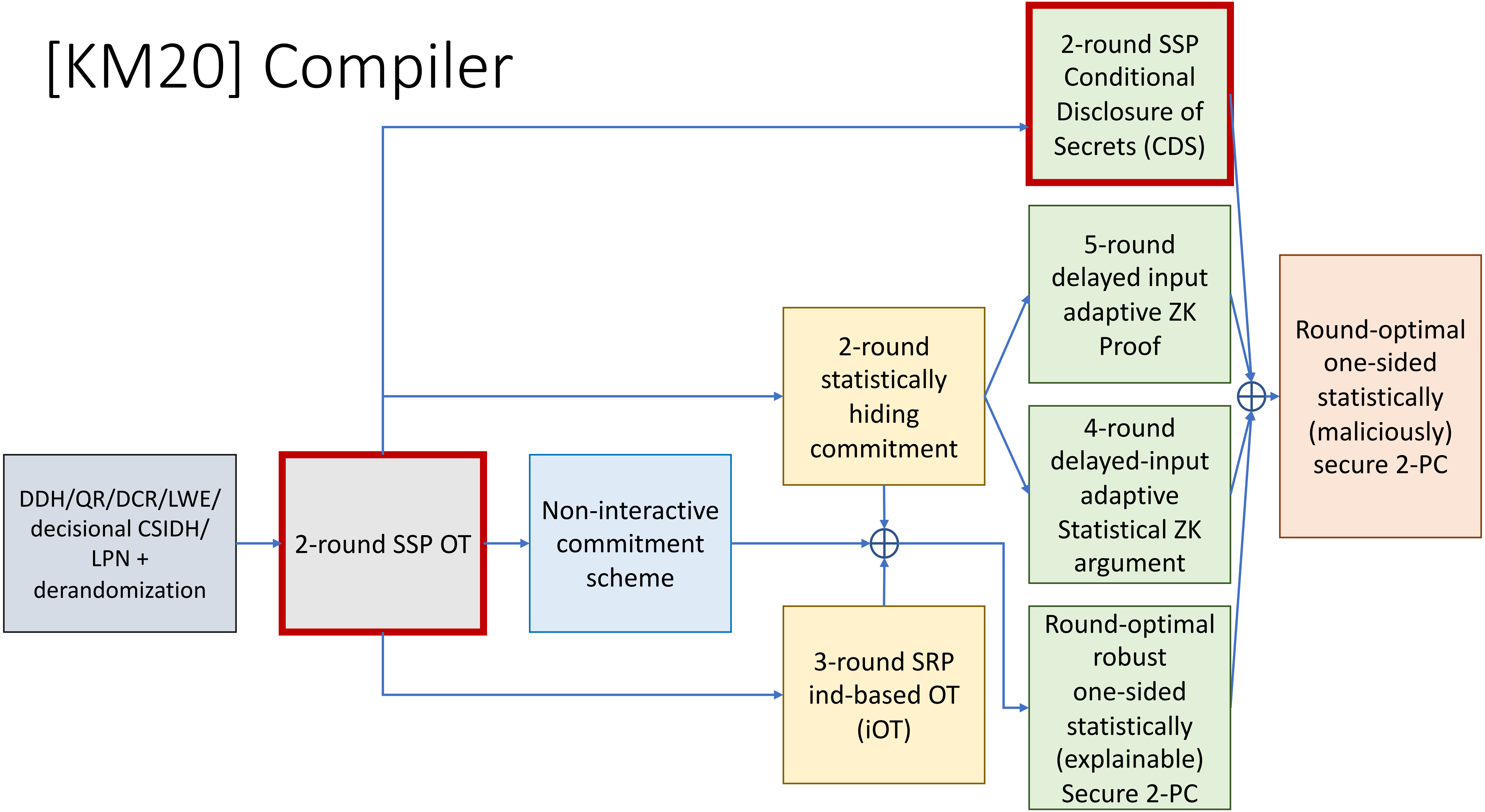
5-round delayed input adaptive ZK Proof

4-round delayed-input adaptive Statistical ZK argument

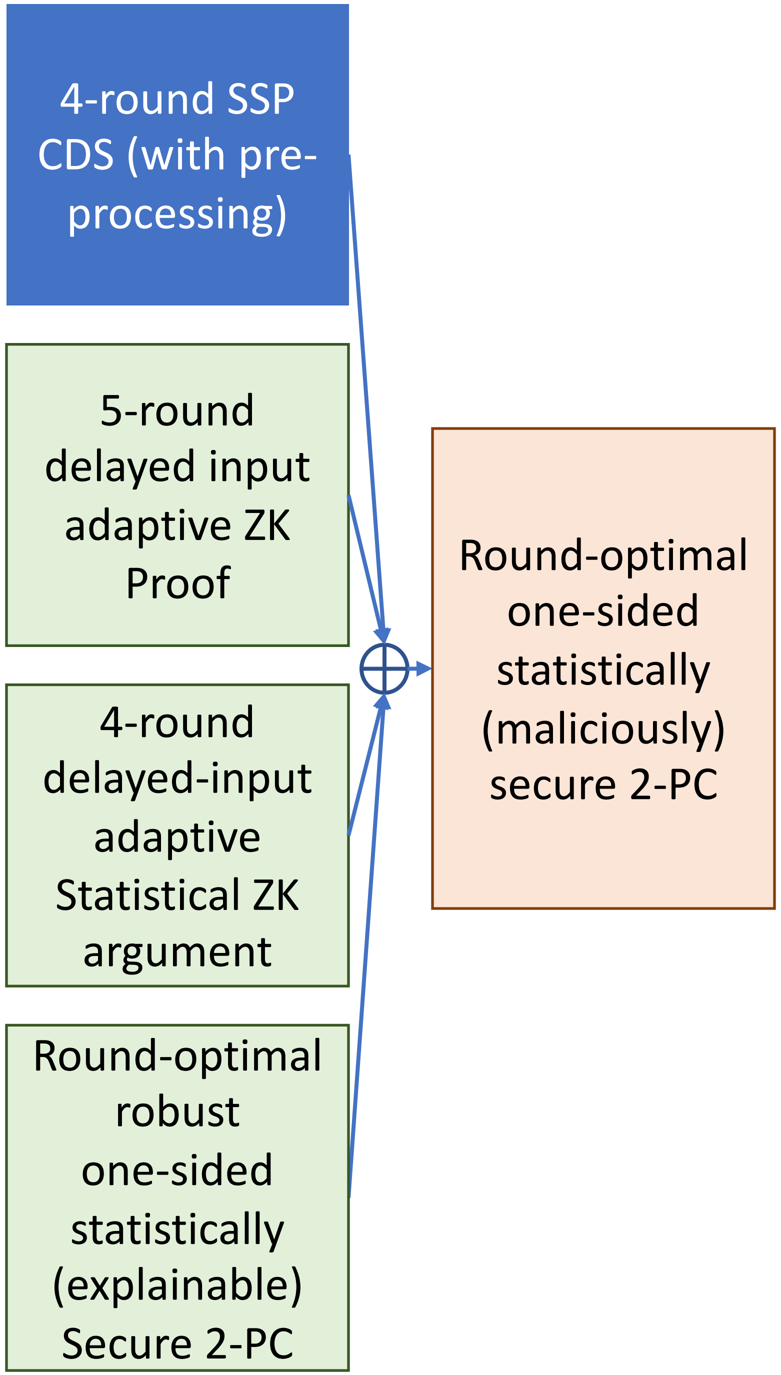
Round-optimal robust one-sided statistically (explainable) Secure 2-PC

Round-optimal one-sided statistically (maliciously) secure 2-PC

[KM20] Compiler



Our Compiler



4-round SSP CDS (with pre-processing)

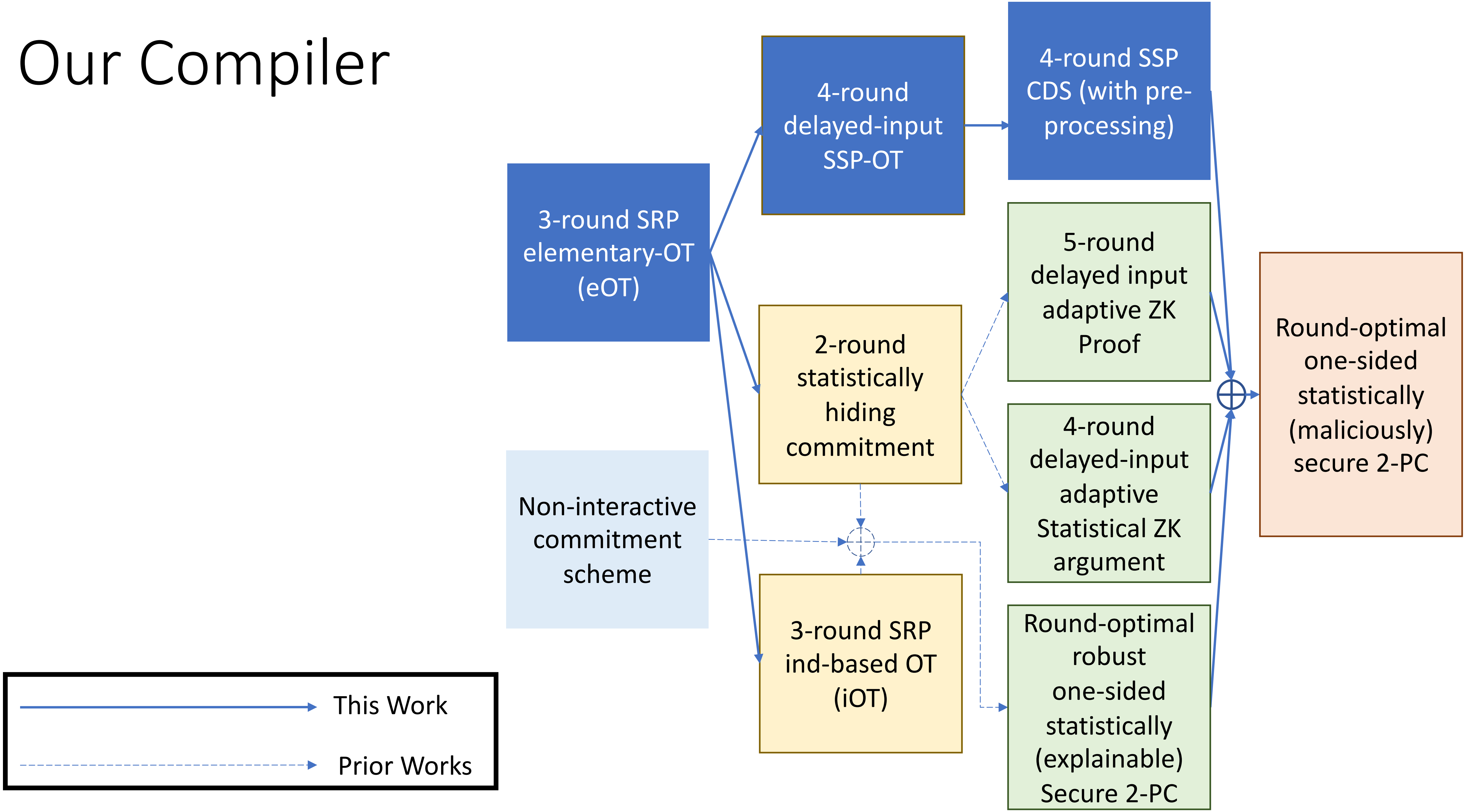
5-round delayed input adaptive ZK Proof

4-round delayed-input adaptive Statistical ZK argument

Round-optimal robust one-sided statistically (explainable) Secure 2-PC

Round-optimal one-sided statistically (maliciously) secure 2-PC

Our Compiler



3-round SRP elementary-OT (eOT)

4-round delayed-input SSP-OT

4-round SSP CDS (with pre-processing)

2-round statistically hiding commitment

Non-interactive commitment scheme

3-round SRP ind-based OT (iOT)

5-round delayed input adaptive ZK Proof

4-round delayed-input adaptive Statistical ZK argument

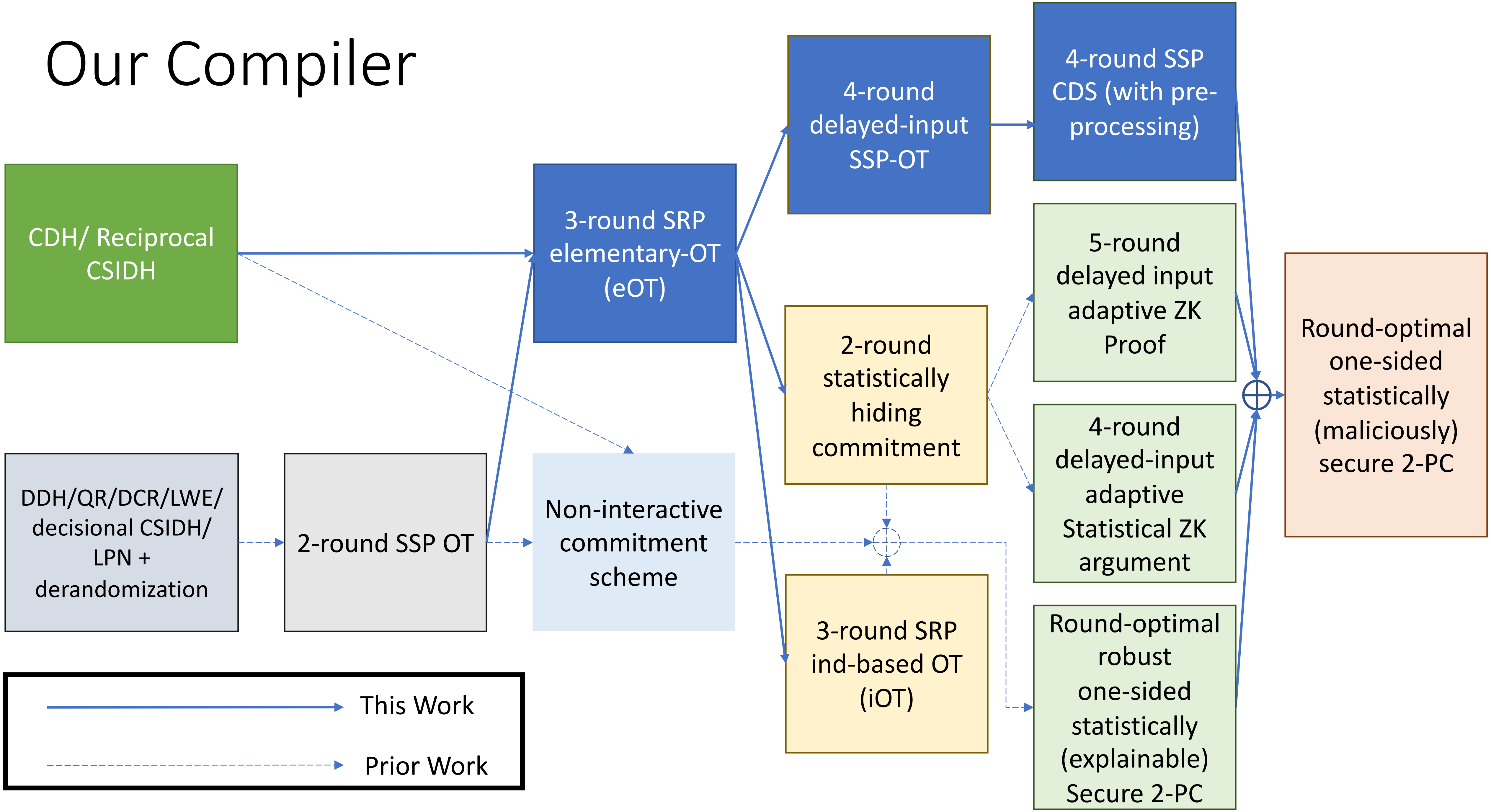
Round-optimal robust one-sided statistically (explainable) Secure 2-PC

Round-optimal one-sided statistically (maliciously) secure 2-PC

This Work

Prior Works

Our Compiler



CDH/ Reciprocal CSIDH

DDH/QR/DCR/LWE/ decisional CSIDH/ LPN + derandomization

2-round SSP OT

3-round SRP elementary-OT (eOT)

Non-interactive commitment scheme

4-round delayed-input SSP-OT

2-round statistically hiding commitment

3-round SRP ind-based OT (iOT)

4-round SSP CDS (with pre-processing)

5-round delayed input adaptive ZK Proof

4-round delayed-input adaptive Statistical ZK argument

Round-optimal robust one-sided statistically (explainable) Secure 2-PC

Round-optimal one-sided statistically (maliciously) secure 2-PC

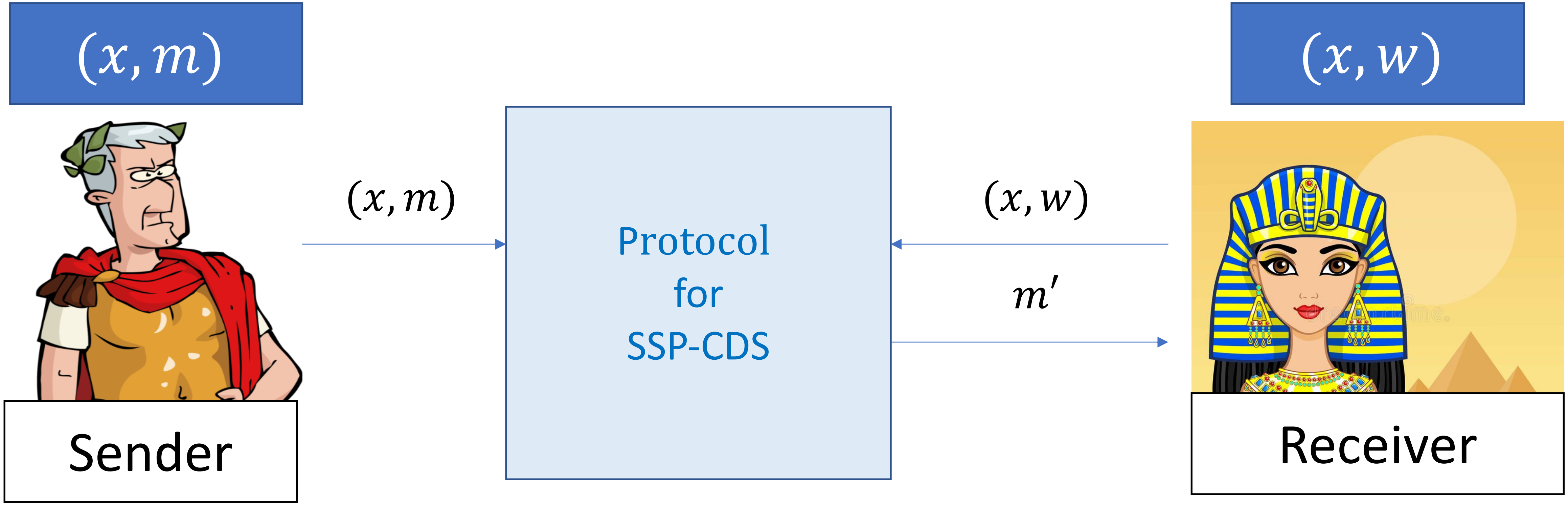
This Work

Prior Work

Chapter IV

Conditional Disclosure of Secrets

SSP Conditional Disclosure of Secrets for a language L



(x, m)

(x, w)

(x, m)

Protocol
for
SSP-CDS

(x, w)

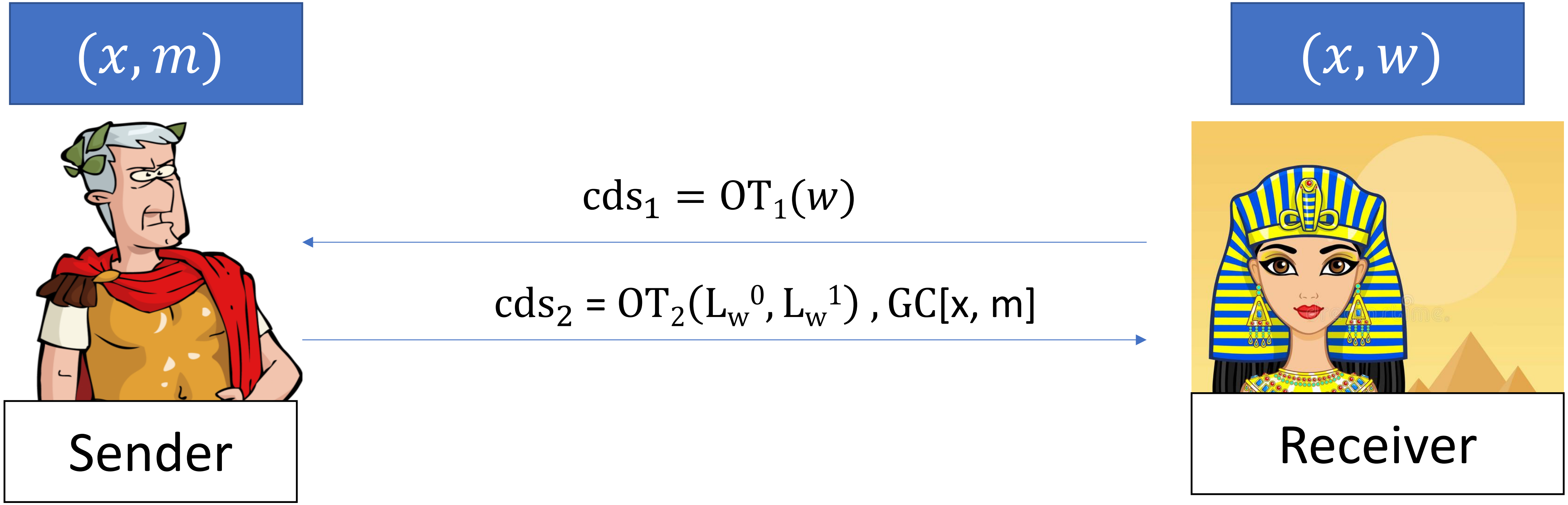
m'

Sender

Receiver

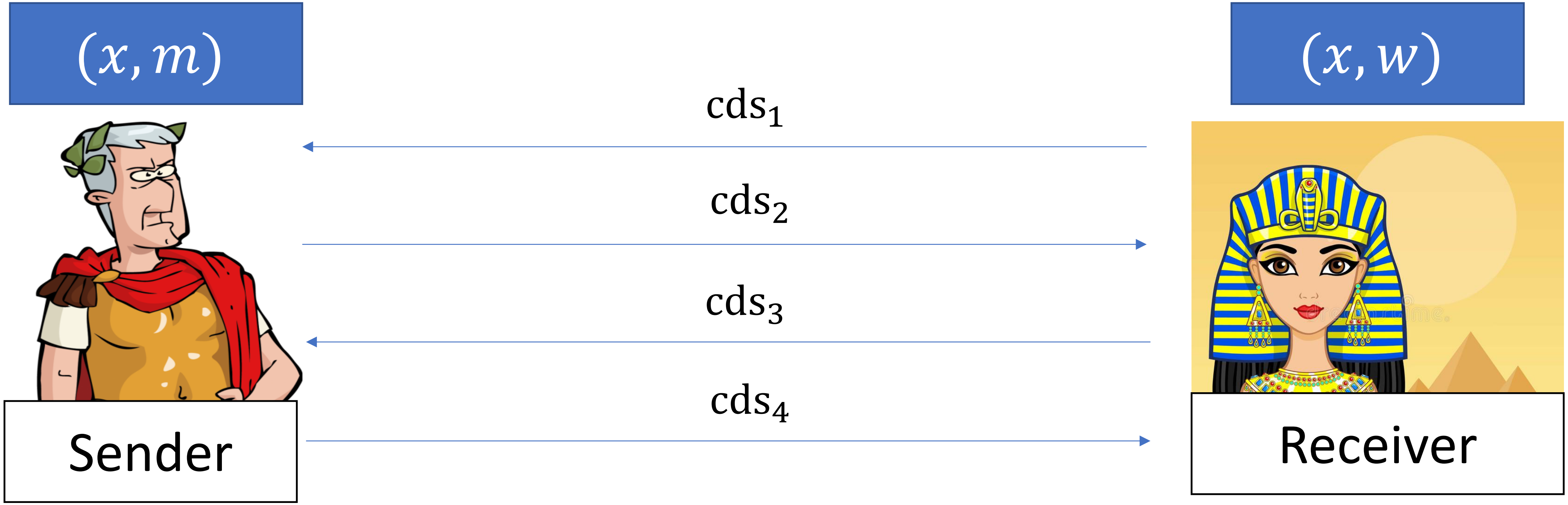
- Correctness: Receiver outputs $m' = m$ if $(x, w) \in L$
- Computational Receiver Privacy: w is hidden from the (computationally bounded) sender
- Statistical Sender Privacy: for (computationally unbounded) receiver: $m \approx m^*$ whenever $(x, w) \notin L$

SSP Conditional Disclosure of Secrets for a language L [KM20]



- Construct an NC1 circuit which checks the validity of receiver's witness by relying on the result of [KM20]
- Combine two-round SSP OT protocol with information theoretic garbling scheme [Kol05] for NC1 circuit, where the GC outputs m if w is a valid witness
- Receiver obtains wire labels for w and evaluates the garbled circuit

SSP Conditional Disclosure of Secrets ***with preprocessing*** for a language L



(x, m)

(x, w)

cds_1

cds_2

cds_3

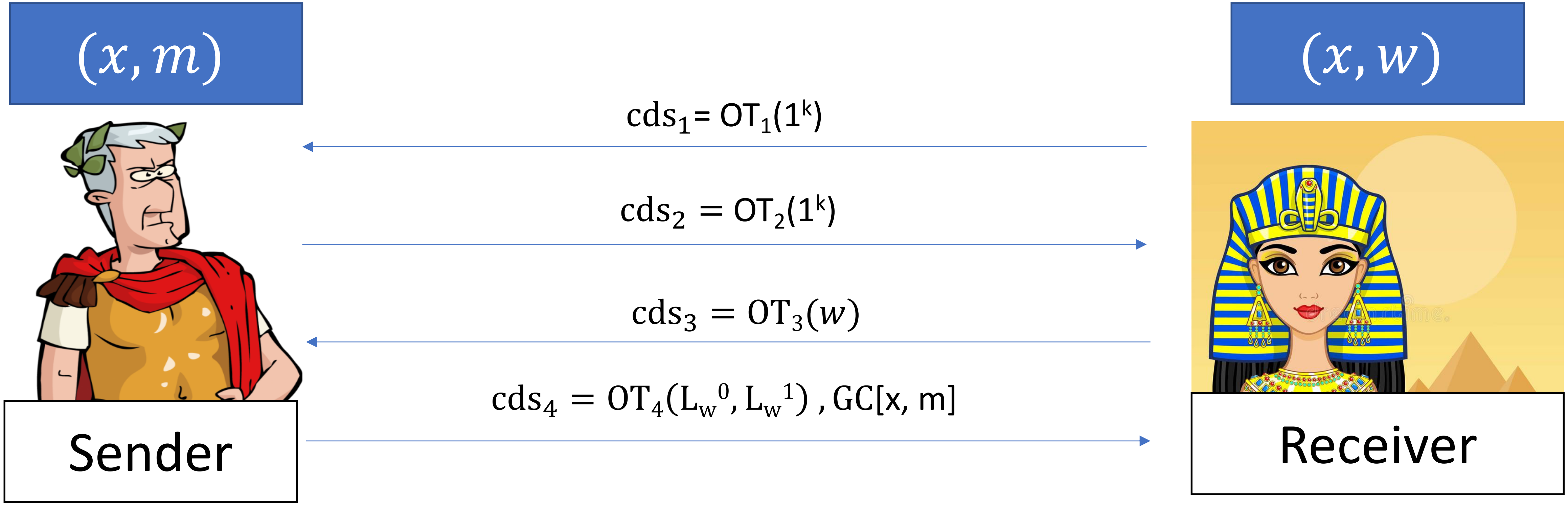
cds_4

Sender

Receiver

- A 4-round protocol with receiver sending the first message
- $(\mathrm{cds}_1 , \mathrm{cds}_2)$ are *independent* of the inputs
- Receiver is statistical, while sender is computationally bounded

SSP Conditional Disclosure of Secrets *with preprocessing* for a language L



(x, m)

Sender

$$\xleftarrow{\mathrm{cds}_1 = \mathrm{OT}_1(1^k)}$$

$$\xrightarrow{\mathrm{cds}_2 = \mathrm{OT}_2(1^k)}$$

$$\xleftarrow{\mathrm{cds}_3 = \mathrm{OT}_3(w)}$$

$$\xrightarrow{\mathrm{cds}_4 = \mathrm{OT}_4(\mathrm{L_w}^0, \mathrm{L_w}^1)\ , \mathrm{GC}[x, m]}$$

(x, w)

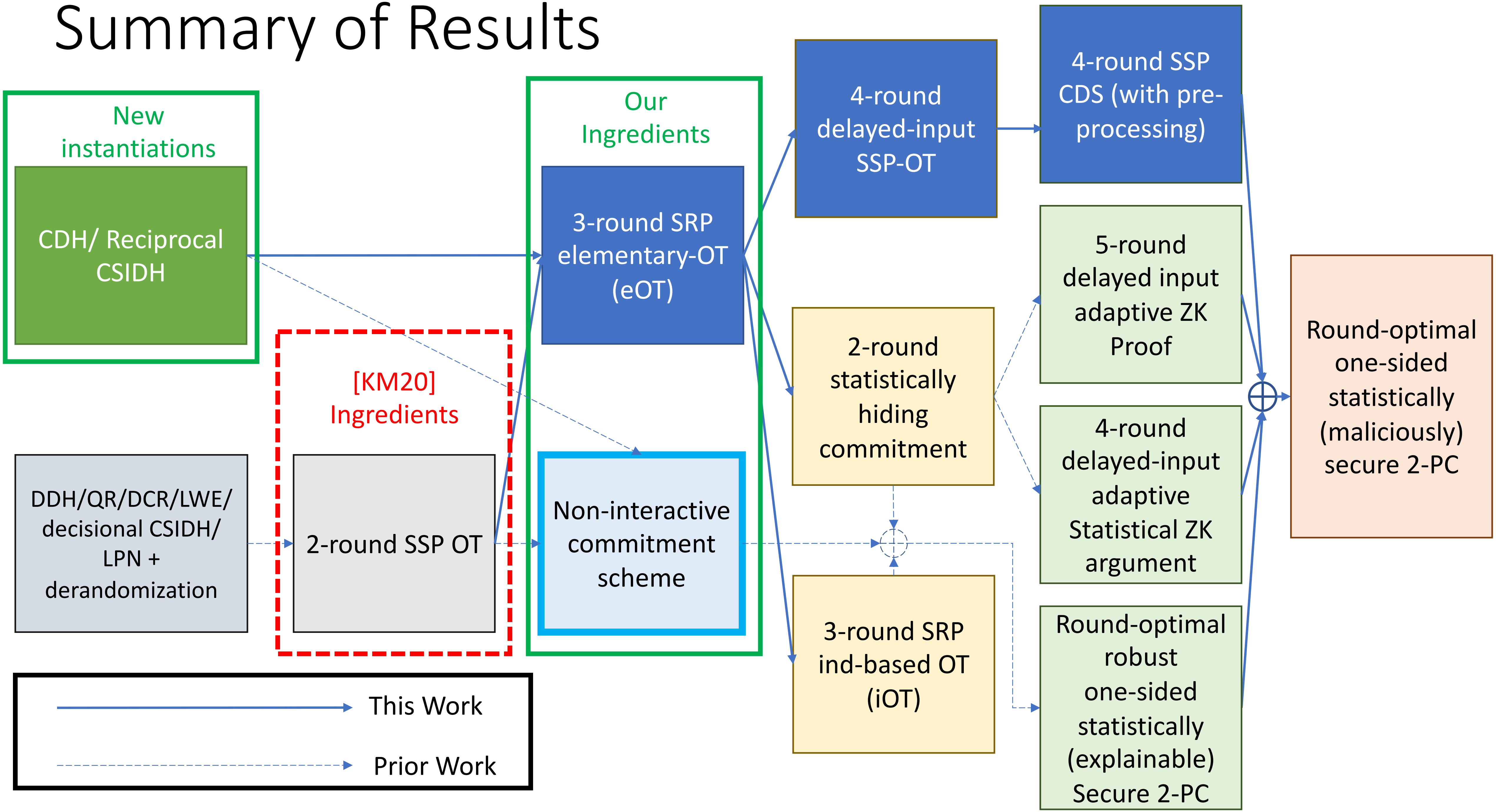
Receiver

- Construct an NC1 circuit which checks the validity of receiver’s witness by relying on the result of [KM20]
- Combine four-round (delayed-input) SSP OT protocol with information theoretic garbling scheme [Kol05] for NC1 circuit to construct SSP CDS
- Receiver obtains wire labels for w and the GC outputs m if w is a valid witness

Chapter V

Summary

Summary of Results



Conclusion

- Constructed round optimal one-sided 2PC from wide variety of assumptions
- Proposed delayed input SSP-Conditional Disclosure of Secrets with preprocessing

Conclusion

- Constructed round optimal one-sided 2PC from wide variety of assumptions
- Proposed delayed input SSP-Conditional Disclosure of Secrets with preprocessing

Open Questions

- Round optimality of one-sided statistical 2-PC with black-box use of cryptographic primitives
- Statistical security in the multi-party setting : At least one party is computationally unbounded

Thank you