The Round Complexity of Quantum Zero-Knowledge

Orestis Chardouvelis [1] Giulio Malavolta [2]

[1]National Technical University of Athens

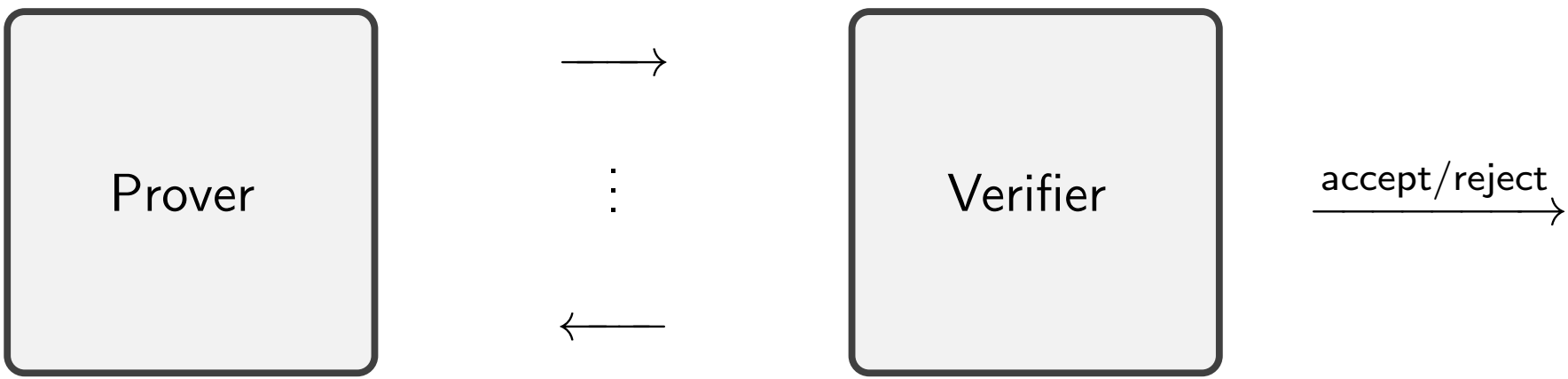
[2]Max Planck Institute for Security and Privacy

TCC 2021

Table of Contents

ZK Protocol [GMR89]

Interactive Protocol which allows a Prover to prove the veracity of a statement while revealing nothing beyond that.



Round Complexity of ZK

- Number of messages exchanged in the protocol.

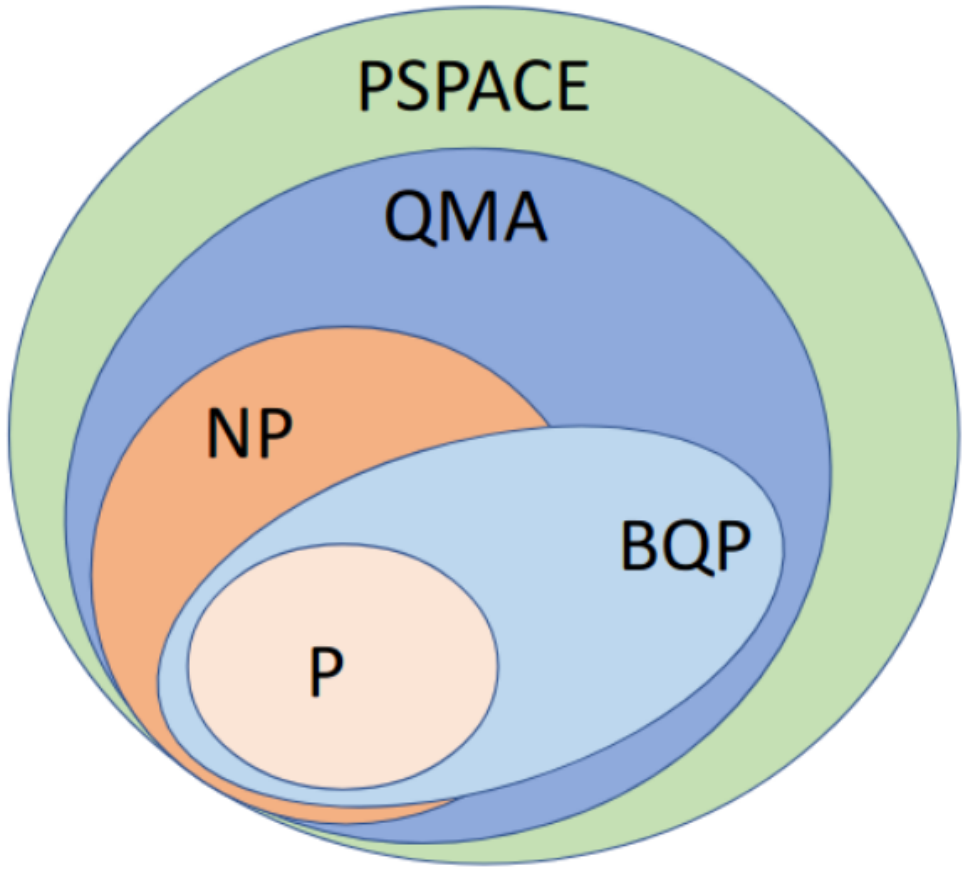
Round Complexity of ZK

- Number of messages exchanged in the protocol.
- Any NP statement can be proven in as few as four rounds of interaction [GMW86, GK96].

Round Complexity of ZK

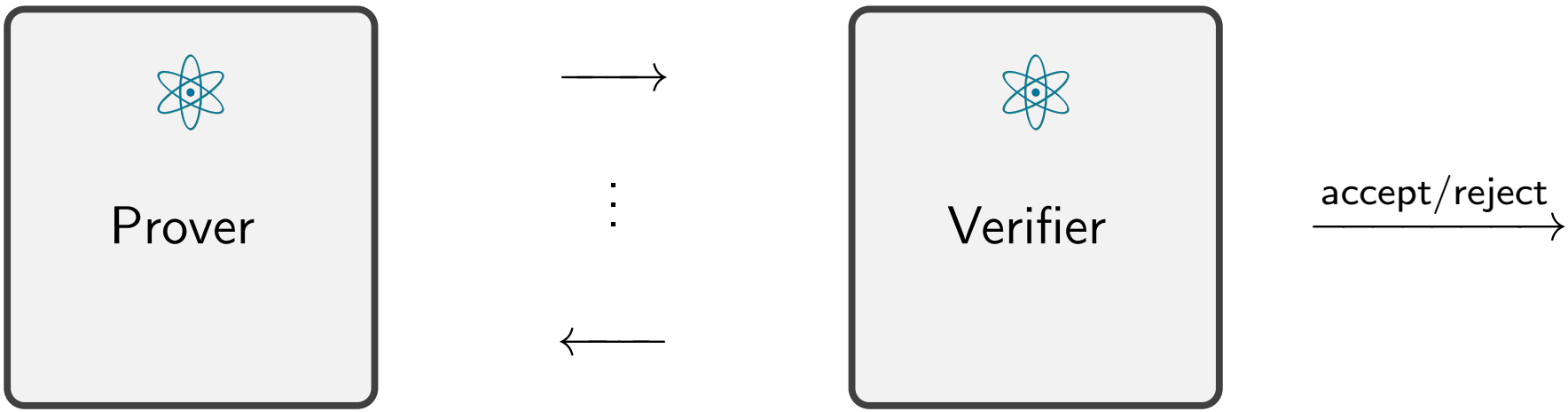
- Number of messages exchanged in the protocol.
- Any NP statement can be proven in as few as four rounds of interaction [GMW86, GK96].
- 3-round statistical ZK argument for NP (not post-quantum secure) [BP19].

Quantum Complexity



Quantum ZK Protocol [BJSW16]

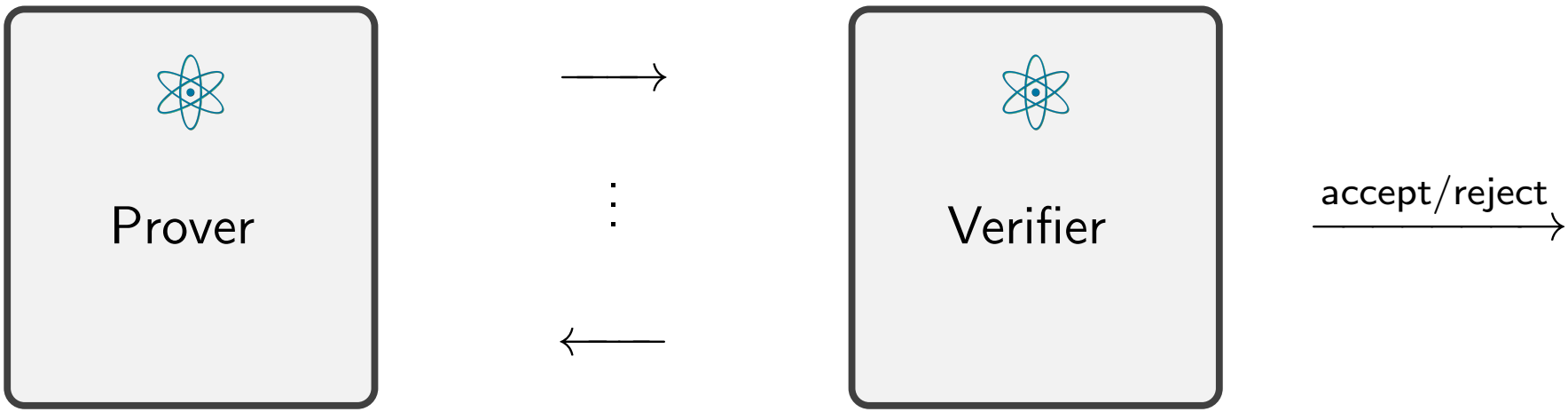
Allows a Prover to prove the veracity of a statement in QMA while revealing nothing beyond that.



wants to prove that $x \in \mathcal{L}$

Quantum ZK Protocol [BJSW16]

Allows a Prover to prove the veracity of a statement in QMA while revealing nothing beyond that.



wants to prove that $x \in \mathcal{L}$

Best known result in terms of round complexity is in constant rounds [BS20].

Results

2-round statistical WI argument for QMA

Assuming the quantum quasi-polynomial hardness of LWE, there exists a 2-round statistical WI argument for QMA.

Results

2-round statistical WI argument for QMA

Assuming the quantum quasi-polynomial hardness of LWE, there exists a 2-round statistical WI argument for QMA.

4-round statistical ZK argument for QMA (and NP)

Assuming the quantum quasi-polynomial hardness of LWE and a quasi-polynomially secure QFHE scheme, there exists a 4-round statistical ZK argument for QMA (and NP) with no trusted setup.

Results

2-round statistical WI argument for QMA

Assuming the quantum quasi-polynomial hardness of LWE, there exists a 2-round statistical WI argument for QMA.

4-round statistical ZK argument for QMA (and NP)

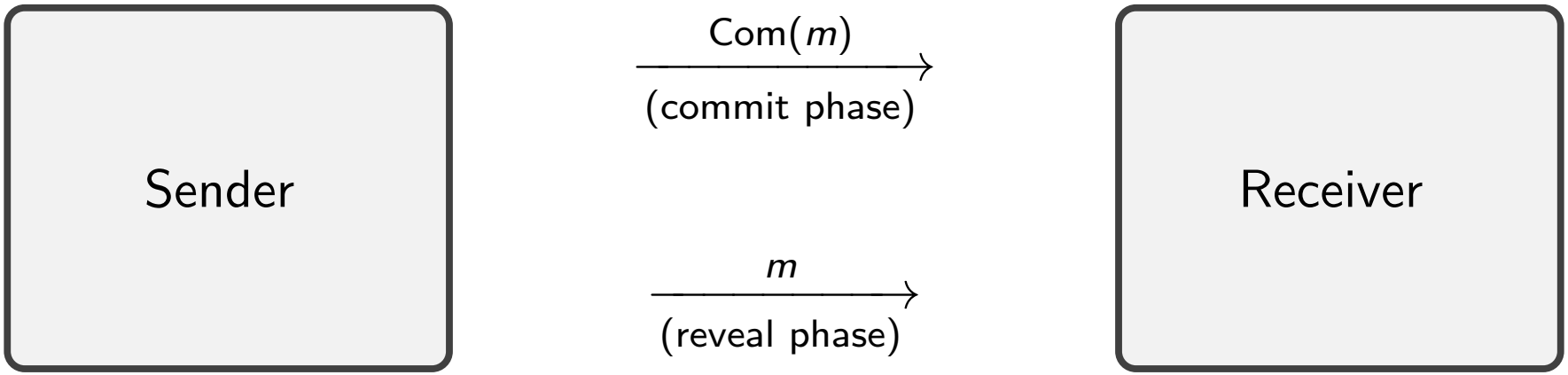
Assuming the quantum quasi-polynomial hardness of LWE and a quasi-polynomially secure QFHE scheme, there exists a 4-round statistical ZK argument for QMA (and NP) with no trusted setup.

2-round ZK argument for QMA in the Timing Model

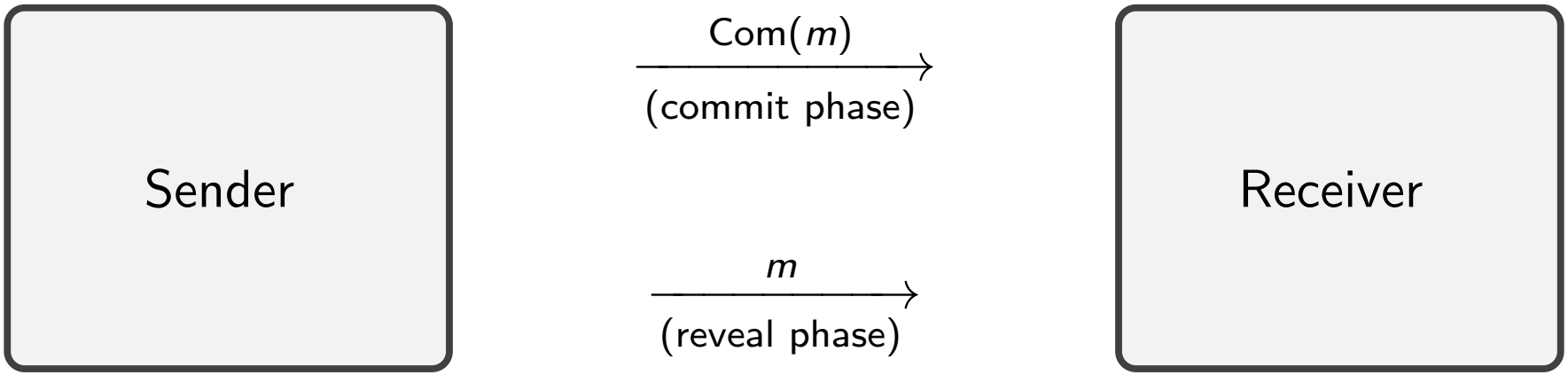
Assuming the quantum quasi-polynomial hardness of LWE, and a non-parallelizing function (resp. a post-quantum time-lock puzzle), there exists a 2-round computational (resp. statistical) ZK argument for QMA in the timing model.

Table of Contents

Commitment Scheme



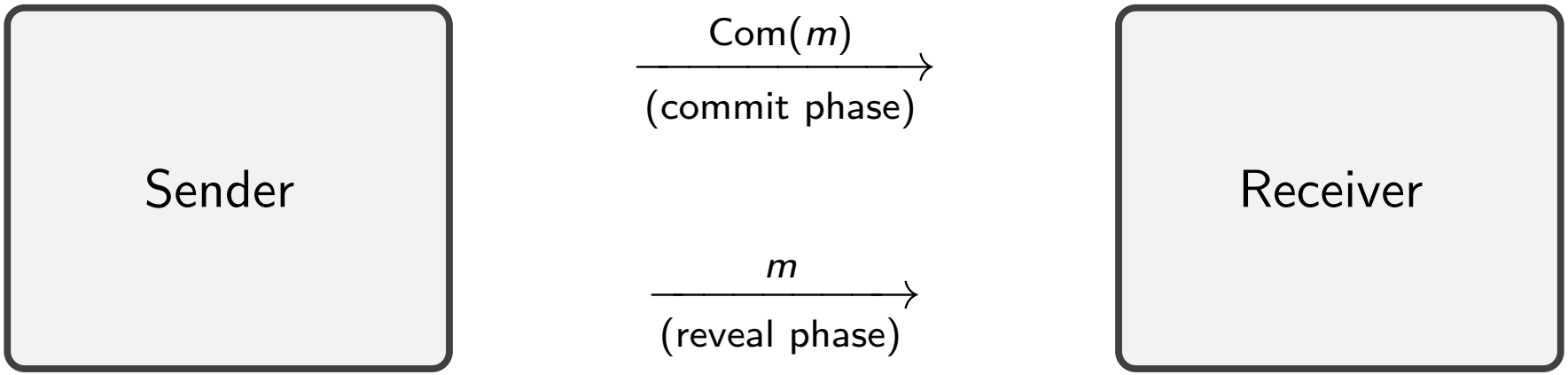
Commitment Scheme



- Hiding: The message m remains hidden from the receiver (before the reveal phase).

$$\mathrm{Com}(m_0) \approx \mathrm{Com}(m_1)$$

Commitment Scheme



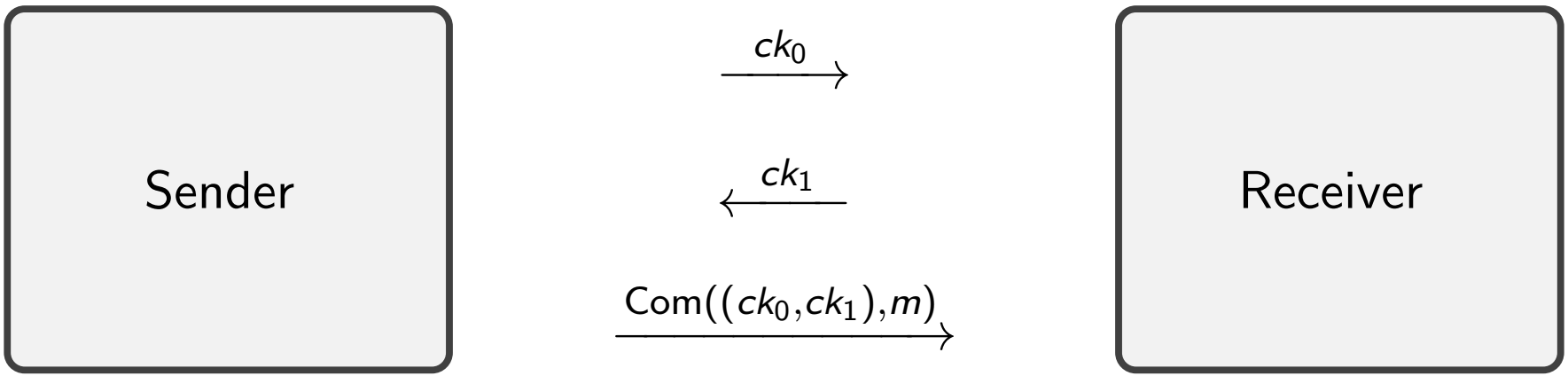
- Hiding: The message m remains hidden from the receiver (before the reveal phase).

$$\mathrm{Com}(m_0) \approx \mathrm{Com}(m_1)$$

- Binding: The commitment $\mathrm{Com}(m)$ can only be opened to the message m.

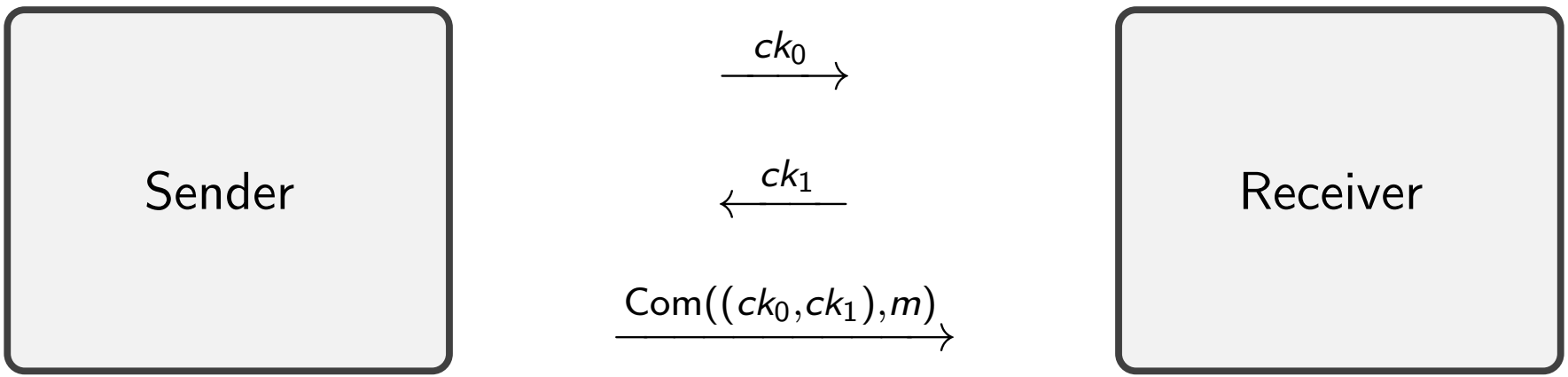
Sometimes Binding Statistically Hiding Commitment

An SBSH commitment is a a special type of commitment [LVW20].



Sometimes Binding Statistically Hiding Commitment

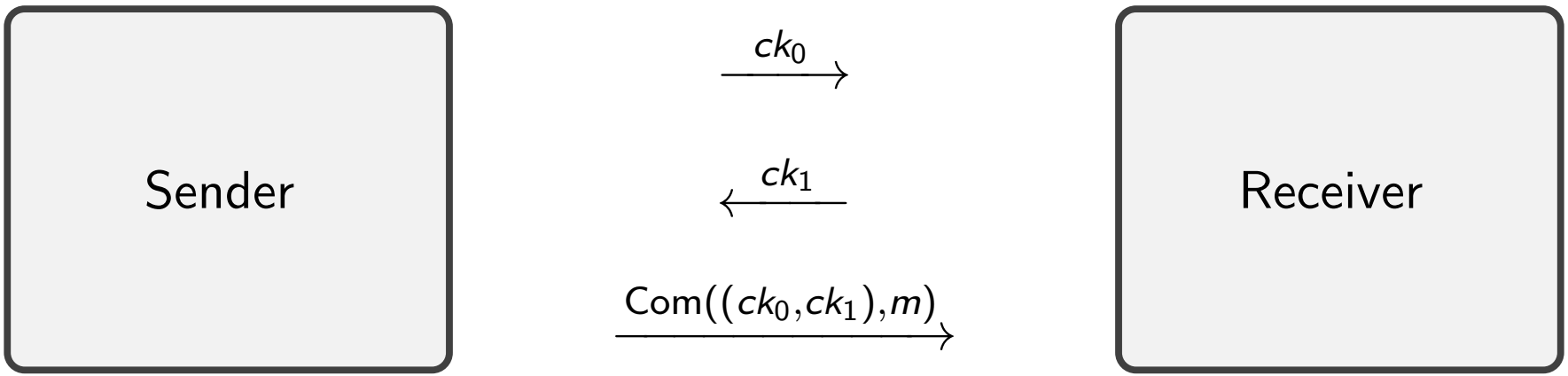
An SBSH commitment is a a special type of commitment [LVW20].



- Statistically Hiding: $\mathsf{Com}(m_0) \approx_S \mathsf{Com}(m_1)$

Sometimes Binding Statistically Hiding Commitment

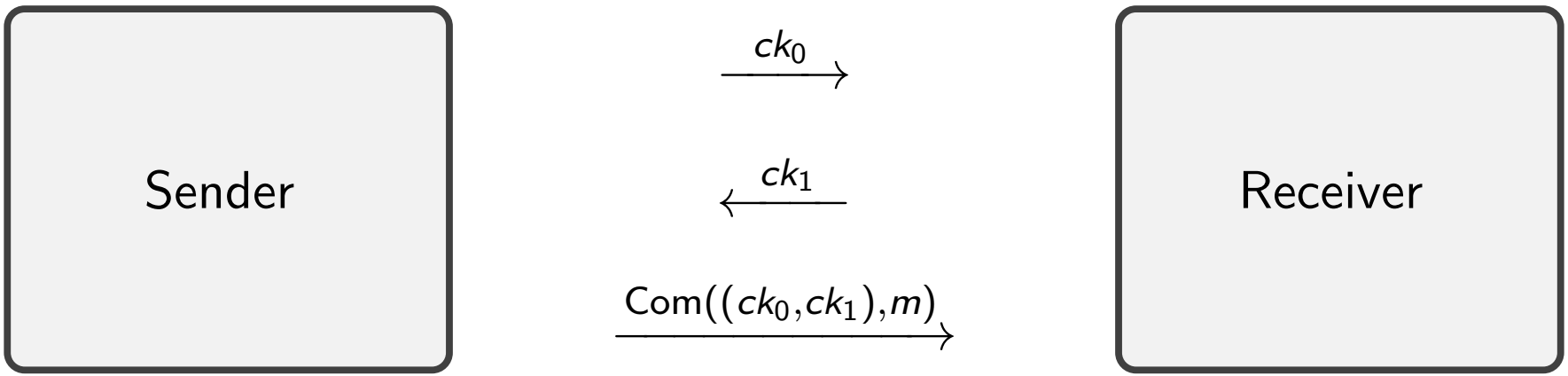
An SBSH commitment is a a special type of commitment [LVW20].



- Statistically Hiding: $\mathsf{Com}(m_0) \approx_S \mathsf{Com}(m_1)$
- Sometimes Binding: There's a negligibly small probability for the commitment to be perfectly binding.

Sometimes Binding Statistically Hiding Commitment

An SBSH commitment is a a special type of commitment [LVW20].



- Statistically Hiding: $\mathsf{Com}(m_0) \approx_S \mathsf{Com}(m_1)$
- Sometimes Binding: There's a negligibly small probability for the commitment to be perfectly binding.
- Straight line Extraction of m when binding.

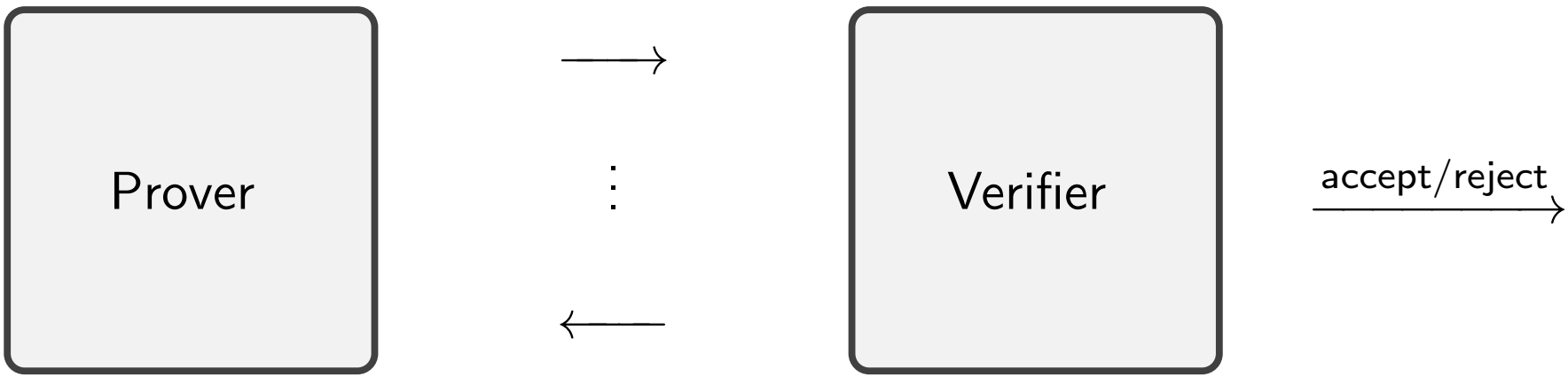
Table of Contents

Witness Indistinguishability [FS90]

- Weaker notion of ZK.

Witness Indistinguishability [FS90]

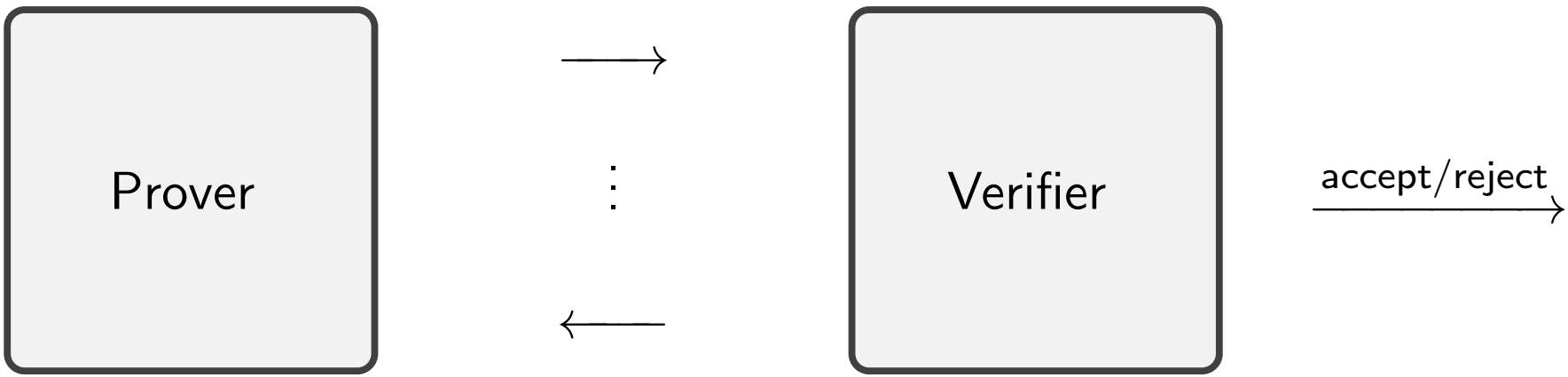
- Weaker notion of ZK.



wants to prove
that $x \in \mathcal{L}$

Witness Indistinguishability [FS90]

- Weaker notion of ZK.



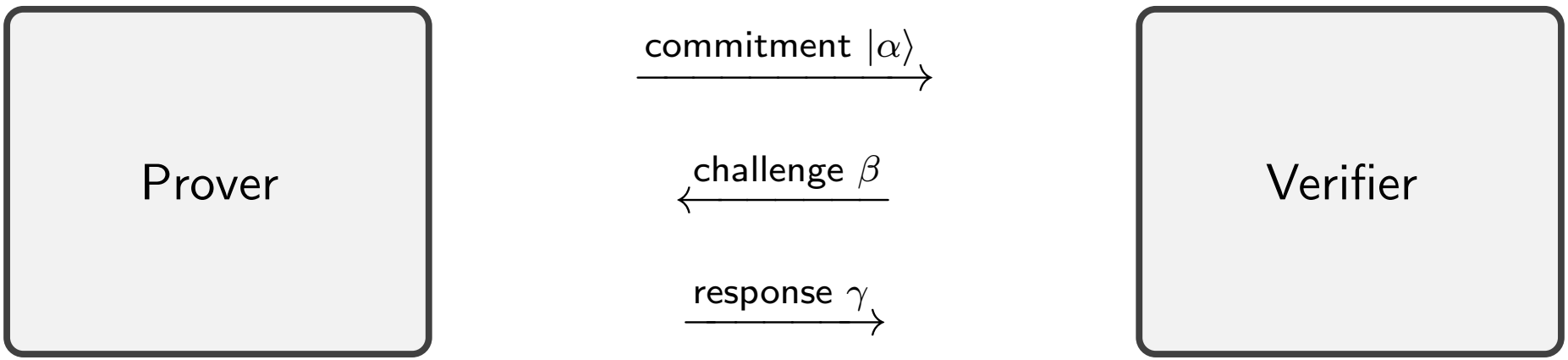
- The verifier cannot tell the difference between valid witnesses used by the prover.

Sigma Protocol for QMA

- Relaxation of ZK, assuming an Honest Verifier.

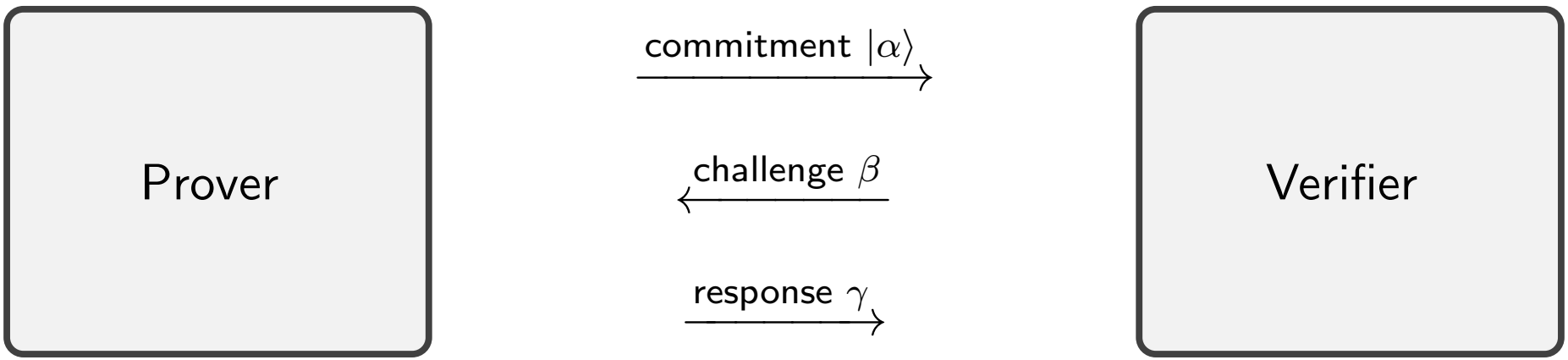
Sigma Protocol for QMA

- Relaxation of ZK, assuming an Honest Verifier.



Sigma Protocol for QMA

- Relaxation of ZK, assuming an Honest Verifier.



- Quantum Σ-Protocol where the computation of β and γ is completely classical [BG20].

Sigma Protocol for QMA

Statistical HVZK

- The Sigma-Protocol [BG20] works for computational ZK and statistical soundness.

Sigma Protocol for QMA

Statistical HVZK

- The Sigma-Protocol [BG20] works for computational ZK and statistical soundness.
- Extend to statistical ZK and computational soundness:

Sigma Protocol for QMA

Statistical HVZK

- The Sigma-Protocol [BG20] works for computational ZK and statistical soundness.
- Extend to statistical ZK and computational soundness:
  - use SBSH commitment (parameters of other primitives are set accordingly).

Sigma Protocol for QMA

Statistical HVZK

- The Sigma-Protocol [BG20] works for computational ZK and statistical soundness.
- Extend to statistical ZK and computational soundness:
  - use SBSH commitment (parameters of other primitives are set accordingly).
  - parallel repetition of [BS20] to get negligible soundness.

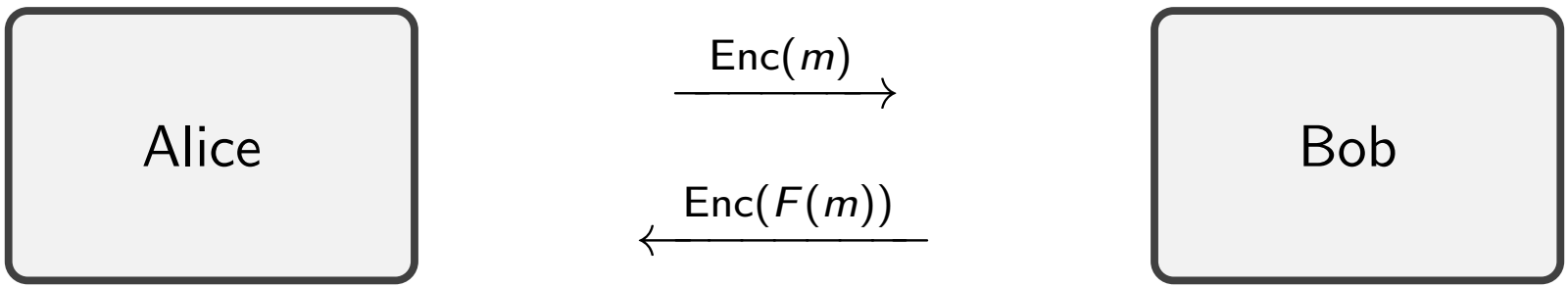
Necessary tools

- Pseudorandom Function: Given a key, produces a seemingly random string.

Necessary tools

- Pseudorandom Function: Given a key, produces a seemingly random string.

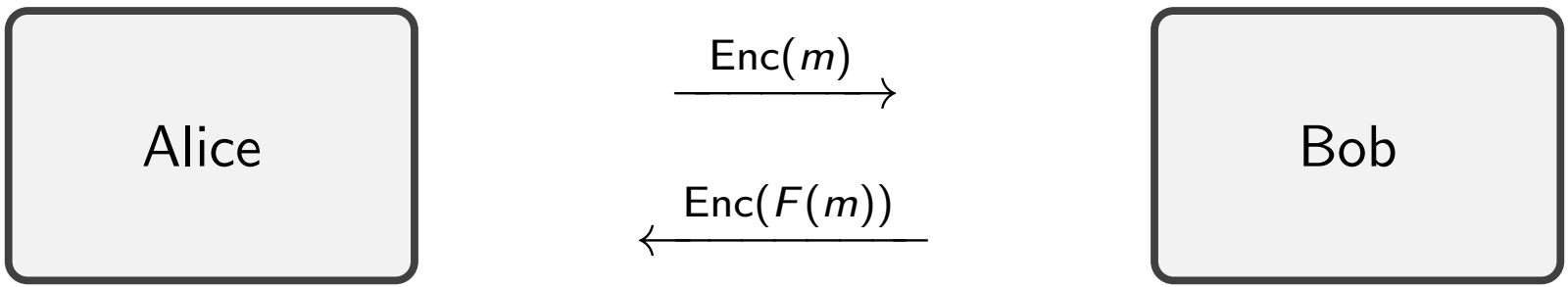
- Fully Homomorphic Encryption Scheme: Compute evaluations over encrypted data.



Necessary tools

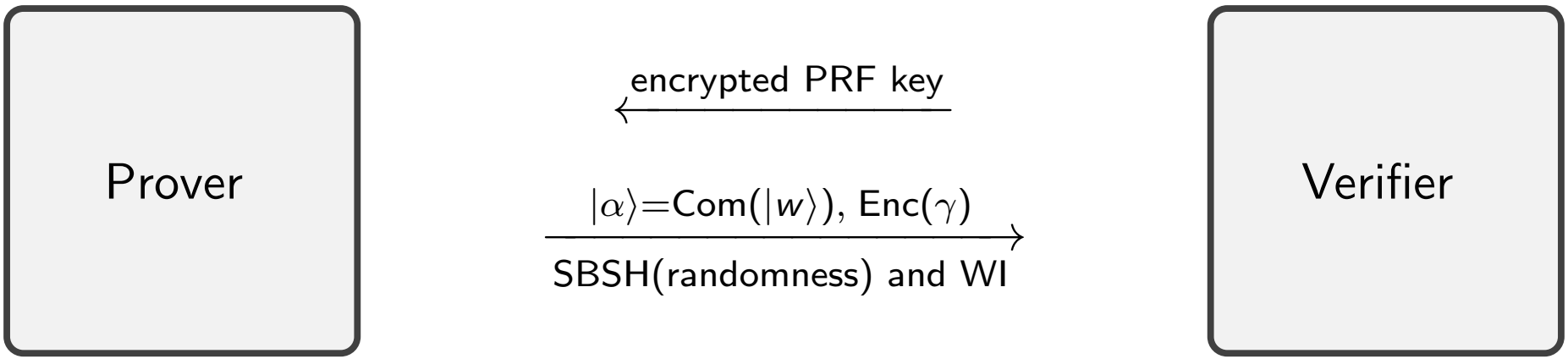
- Pseudorandom Function: Given a key, produces a seemingly random string.

- Fully Homomorphic Encryption Scheme: Compute evaluations over encrypted data.



- Non-Interactive WI argument for NP [BFJ+20, GJJM20].

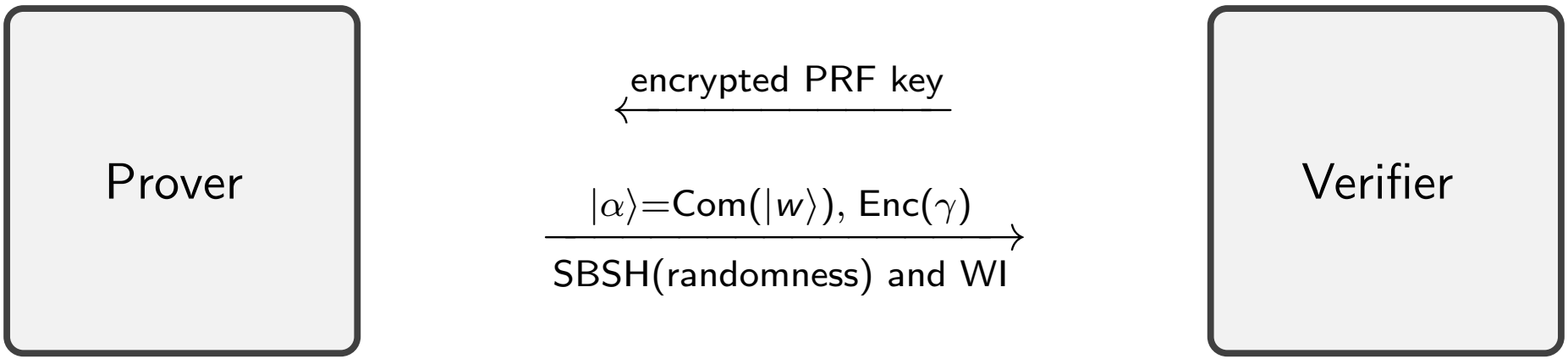
2-Round WI Argument for QMA



recomputes β and decrypts Enc(γ).

- The process is repeated twice.

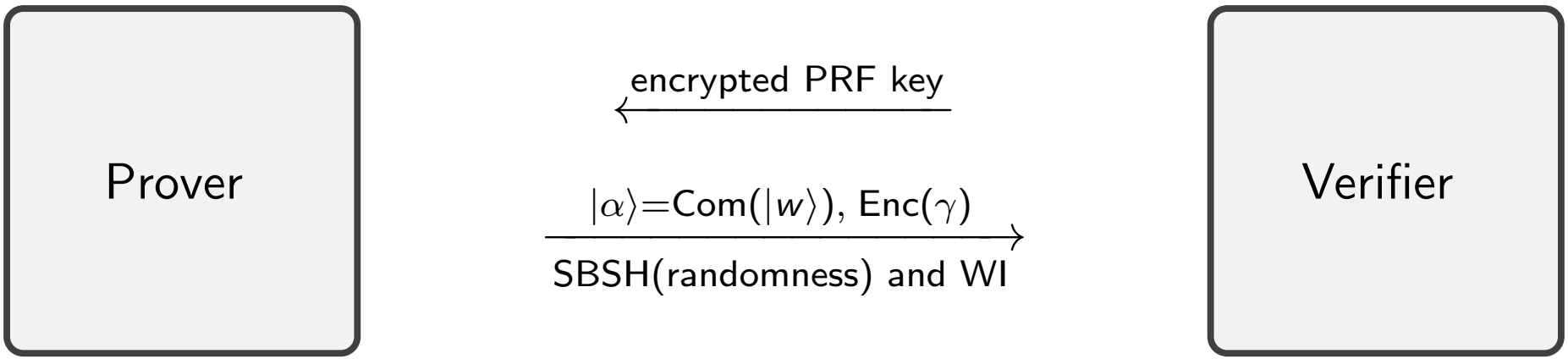
2-Round WI Argument for QMA



recomputes β and decrypts Enc(γ).

- The process is repeated twice.
- Computational Soundness and Statistical WI.

2-Round WI Argument for QMA

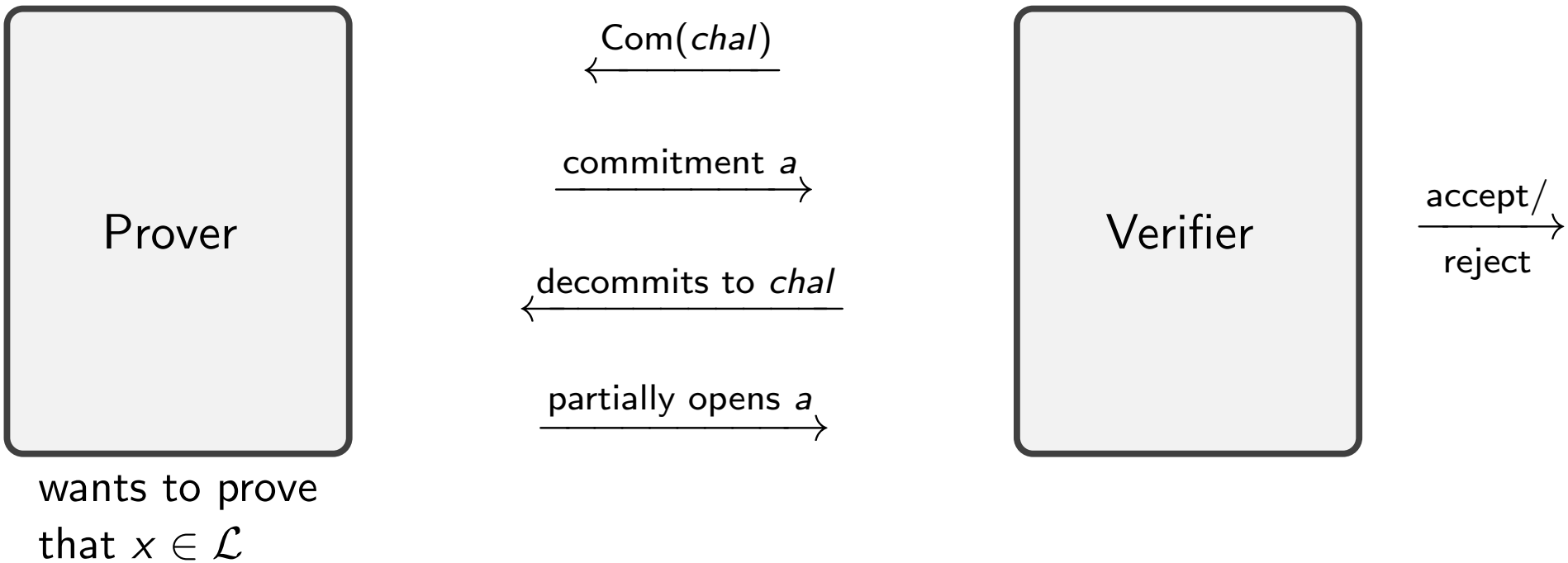


recomputes β and decrypts Enc(γ).

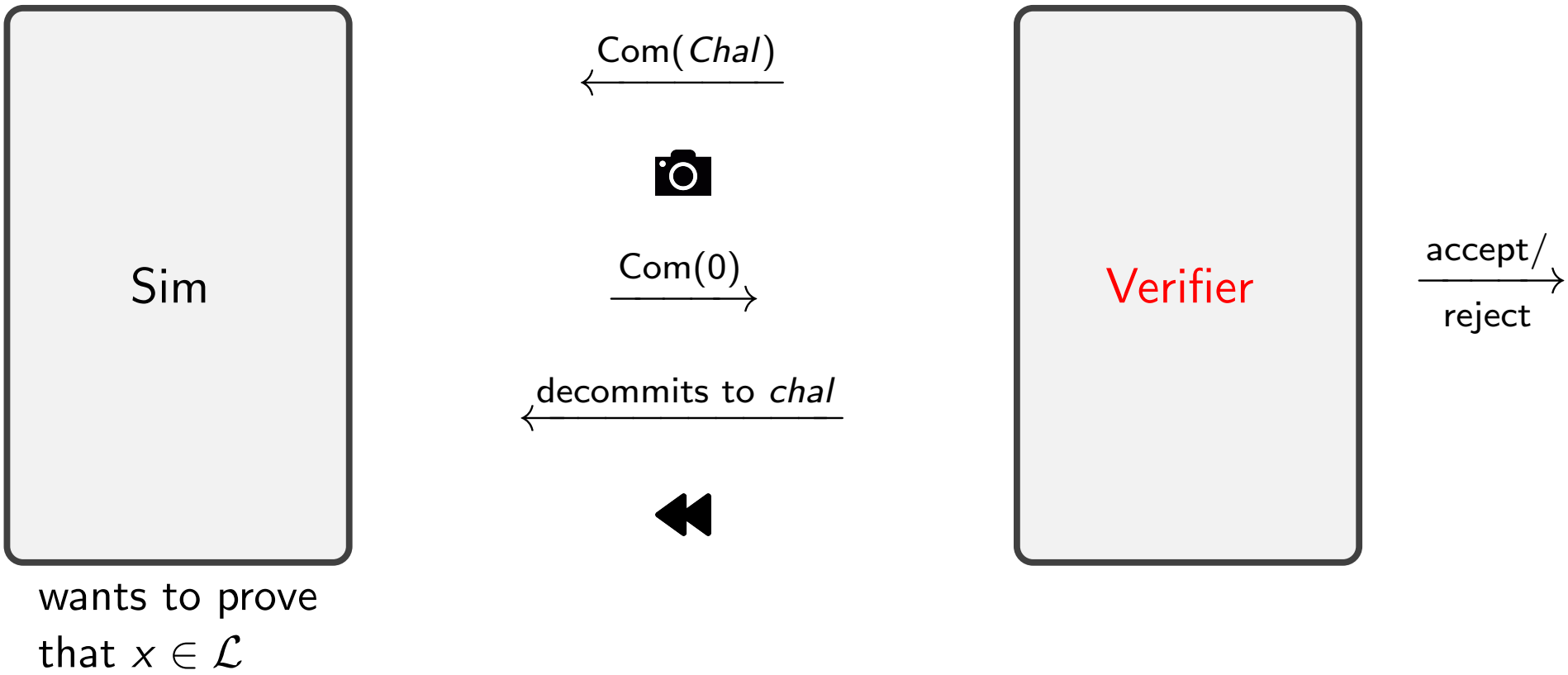
- The process is repeated twice.
- Computational Soundness and Statistical WI.
- Assume quasi-polynomial hardness of LWE.

Table of Contents

Classical ZK

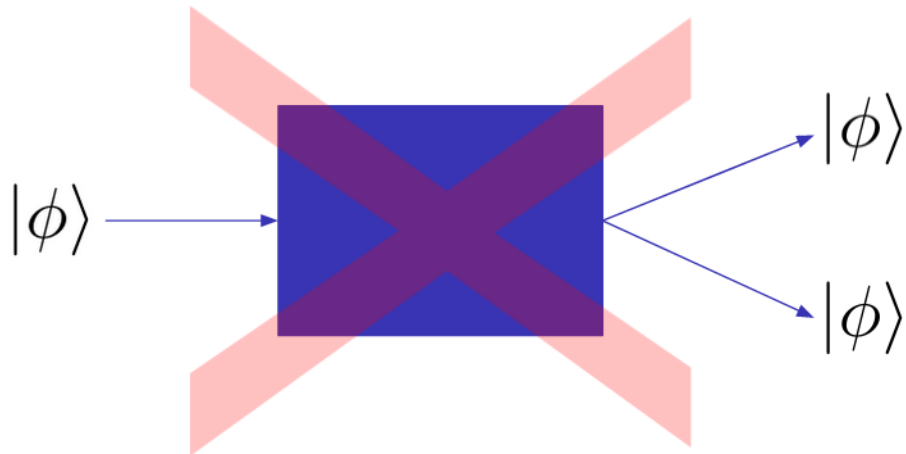


Classical ZK

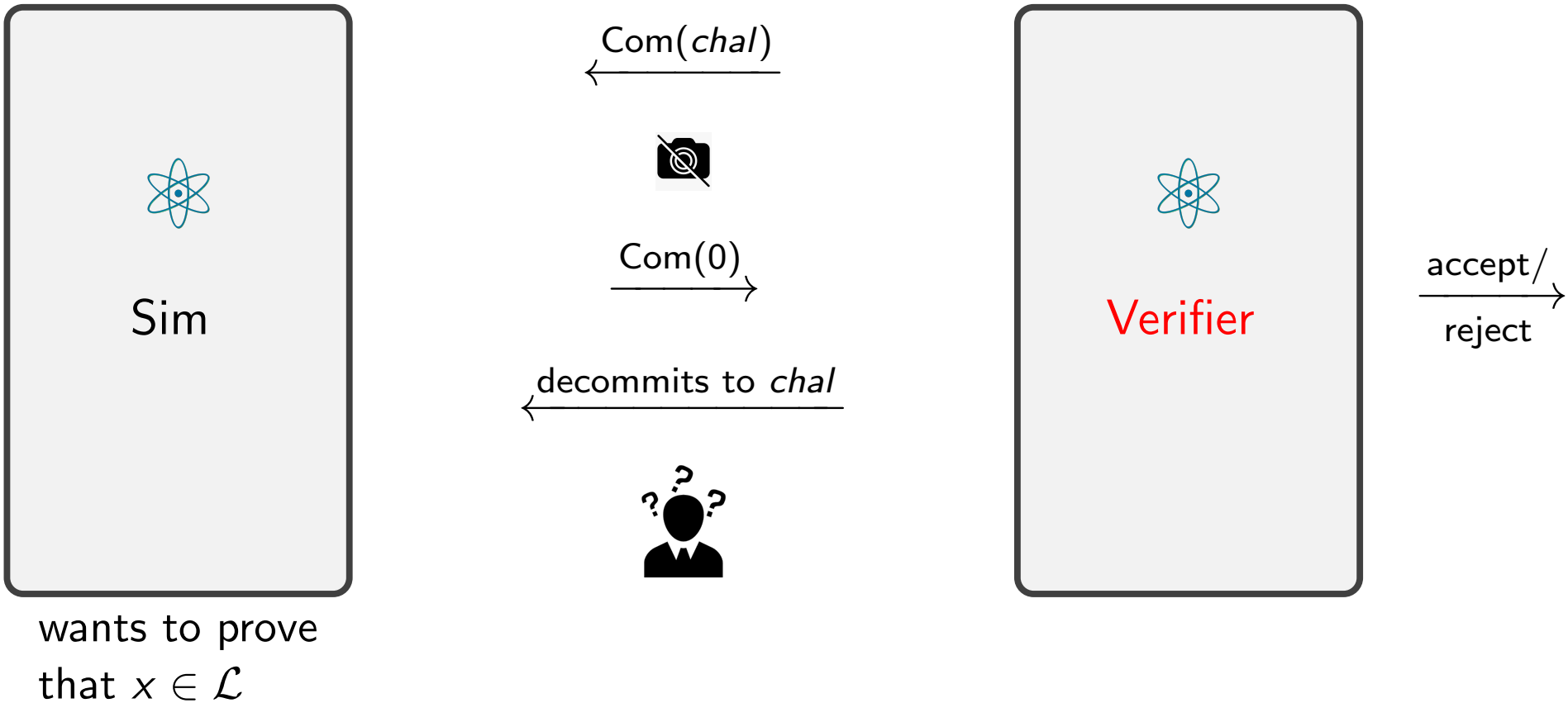


No-Cloning Theorem

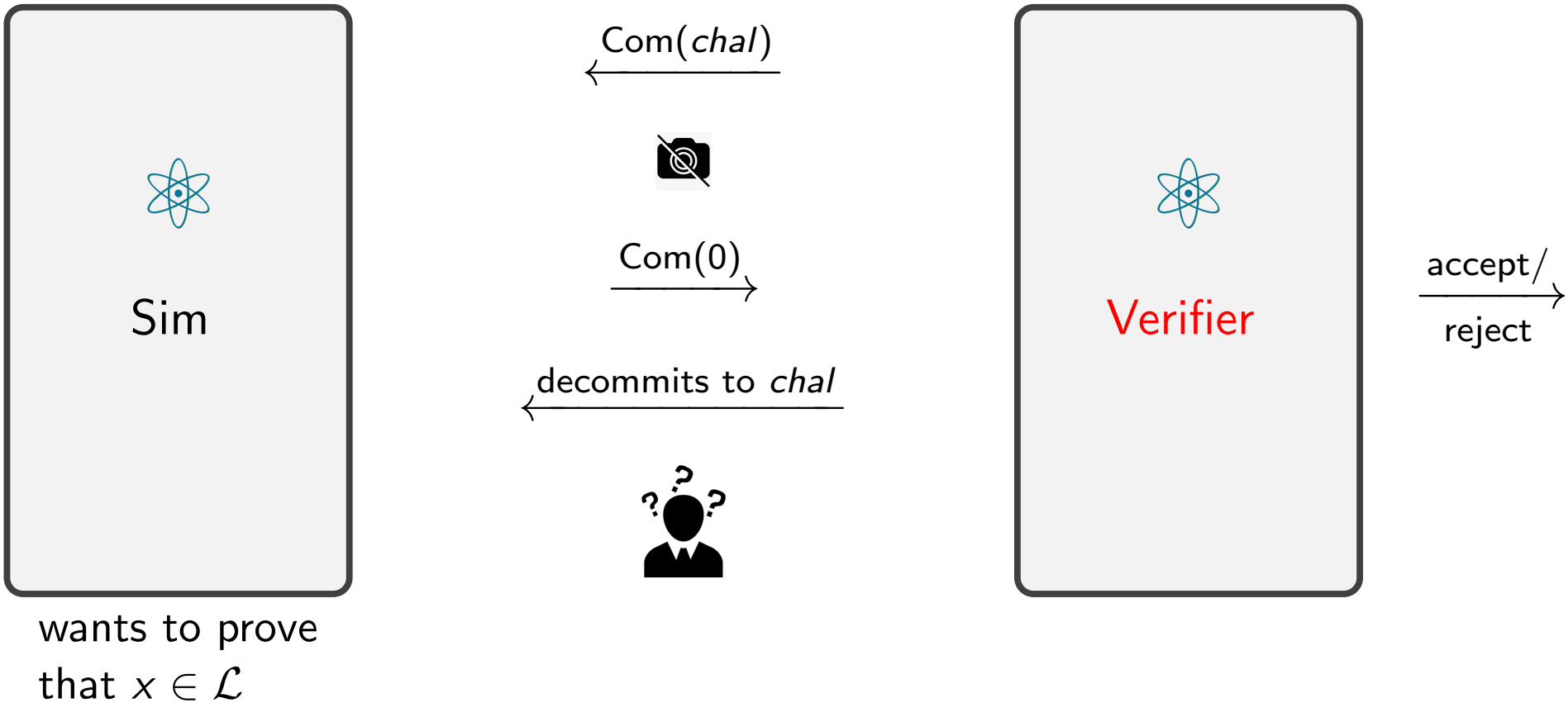
No quantum procedure transforms $|\phi\rangle \rightarrow |\phi\rangle\,|\phi\rangle$, for all $|\phi\rangle$.



Quantum ZK

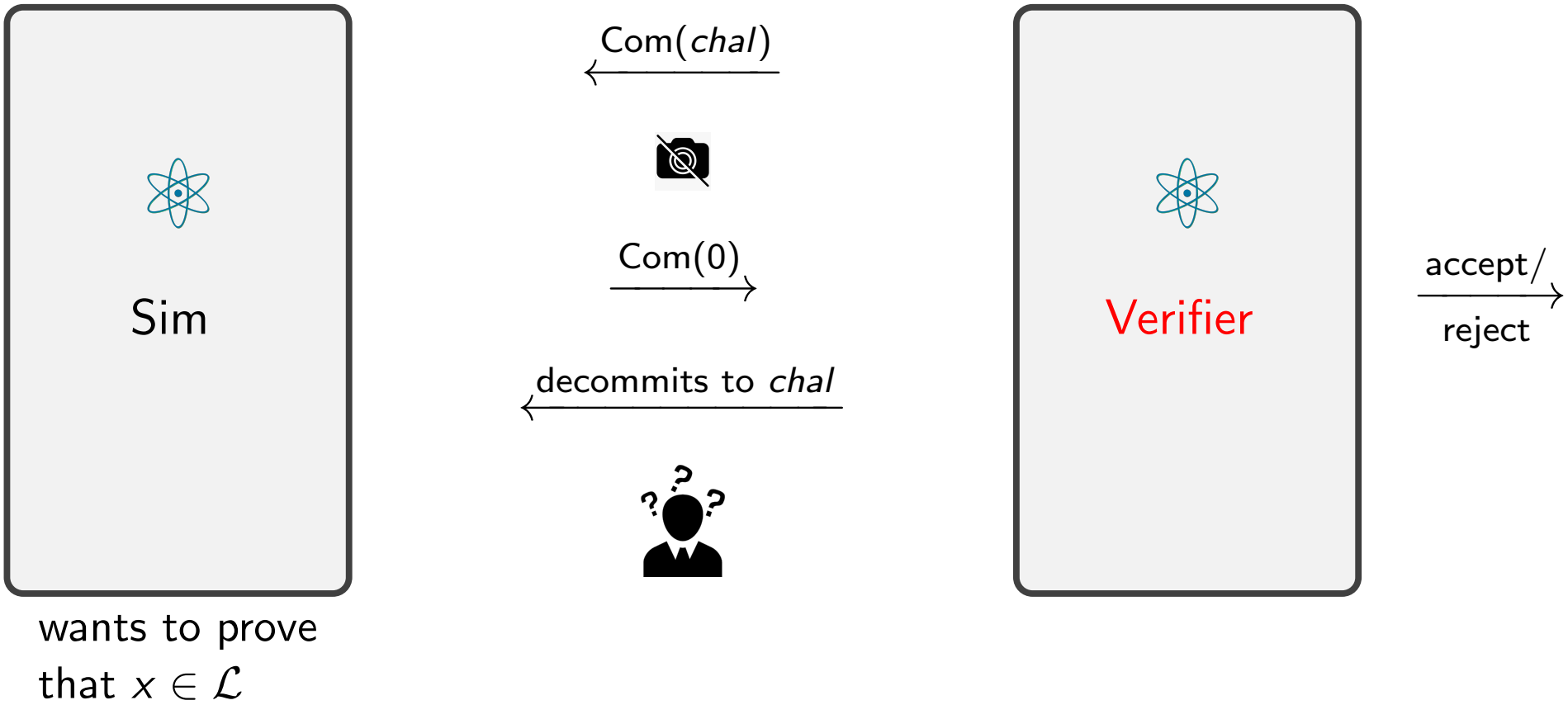

Sim
wants to prove
that $x \in \mathcal{L}$
Com(*chal*)
Com(0)
decommits to *chal*
Verifier
accept/
reject

Quantum ZK



- Simulation techniques that don't use rewinding still rely on cloning.

Quantum ZK

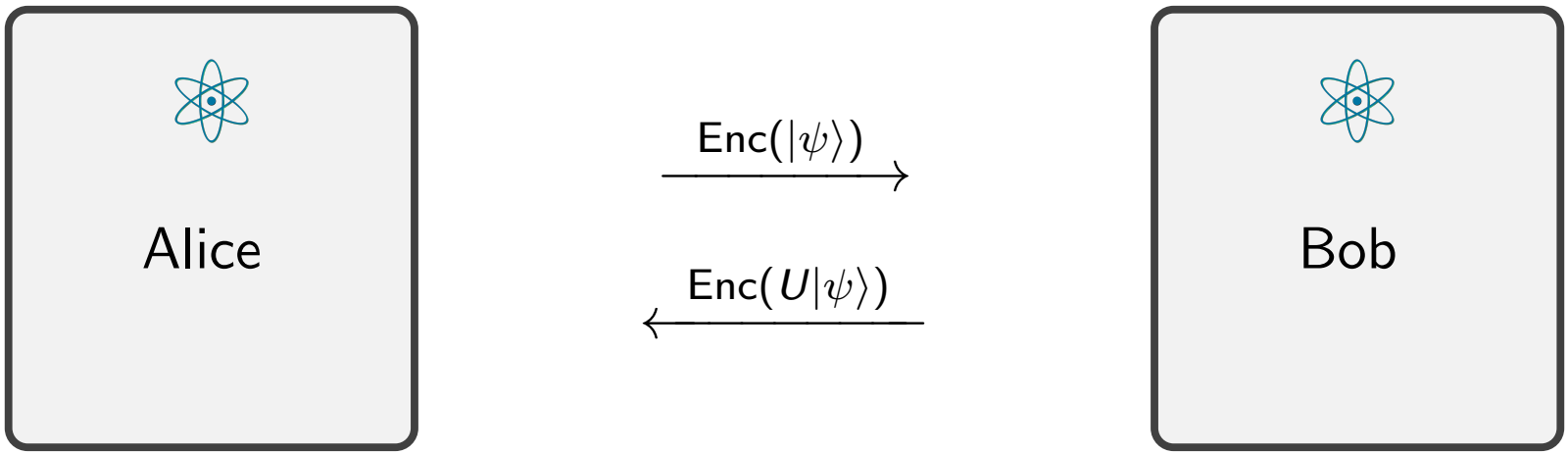


- Simulation techniques that don't use rewinding still rely on cloning.
- Linear Extraction Technique in [AL20, BS20].

Necessary Tools

Quantum FHE Scheme [Mah18, Bra18]

A Quantum FHE scheme [Mah18, Bra18] allows Alice to encrypt some message $|\psi\rangle$ such that later Bob (holding any unitary U) can compute



Necessary Tools

Compute-and-Compare Obfuscation [WZ17, GKW17, GKVW19]

- Compute-and-Compare Program:

$$\mathbf{CC}[f, s, z](x) = \begin{cases} z, & f(x) = s \\ \perp, & \text{else} \end{cases}$$

Necessary Tools

Compute-and-Compare Obfuscation [WZ17, GKW17, GKVW19]

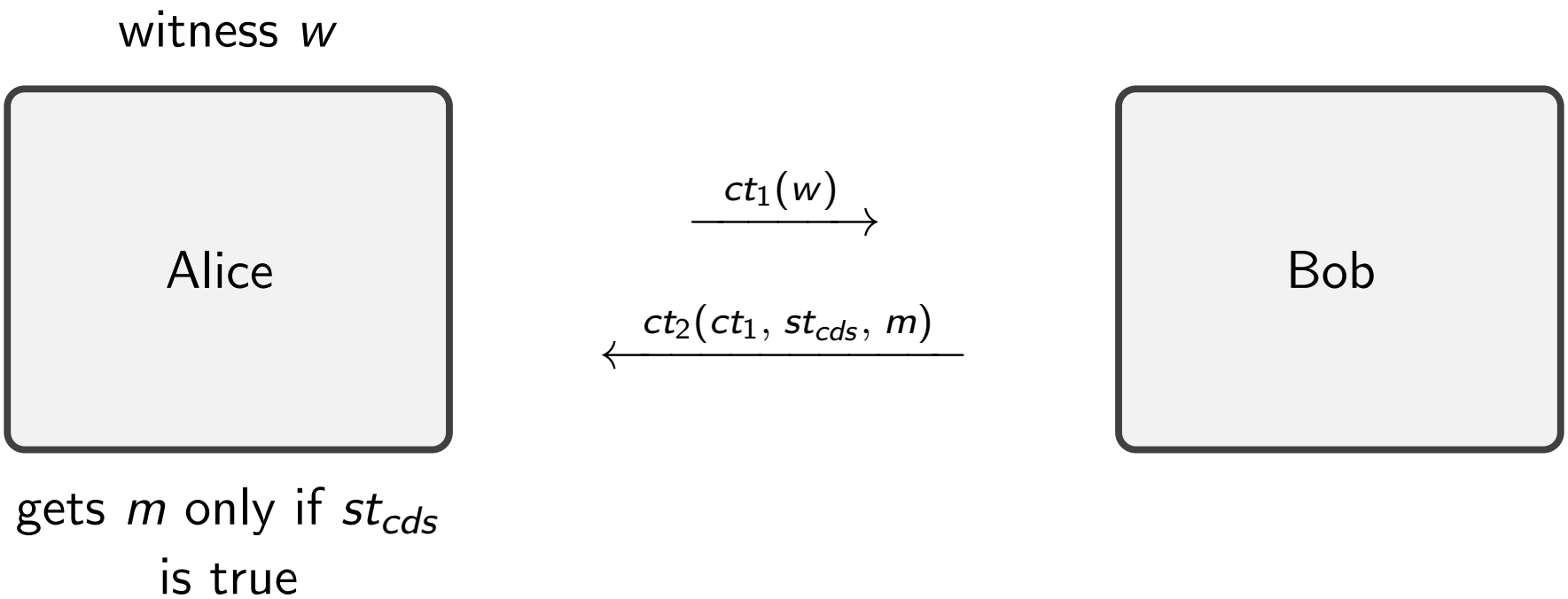
- Compute-and-Compare Program:

$$\mathbf{CC}[f, s, z](x) = \begin{cases} z, & f(x) = s \\ \perp, & \text{else} \end{cases}$$

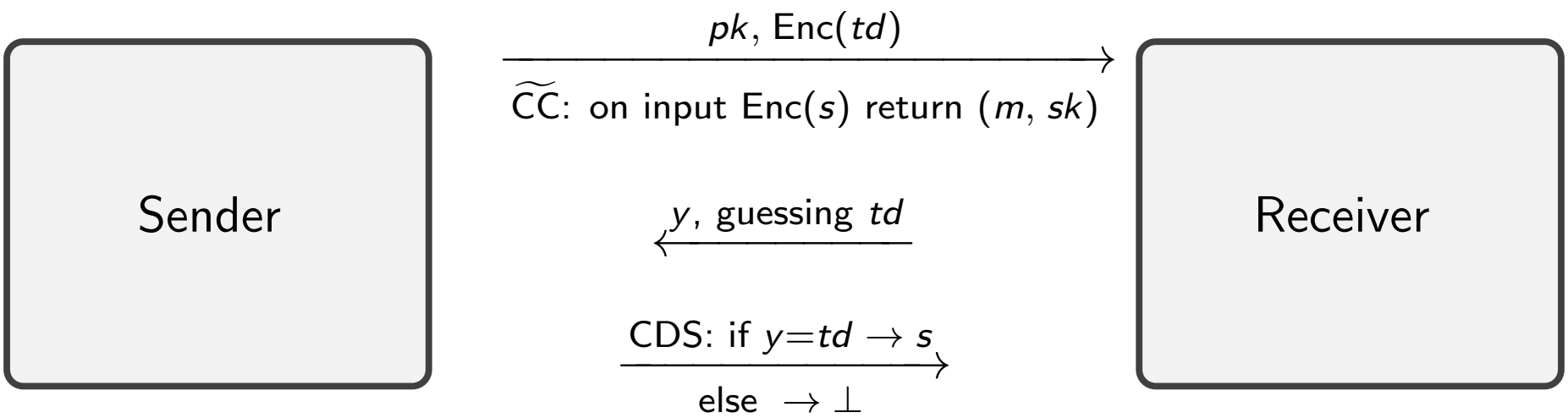
- Compute-and-Compare Obfuscator: Compiles a **CC** program to the obfuscated program $\widetilde{\mathbf{CC}}$, where the implementation is hidden.

Necessary Tools

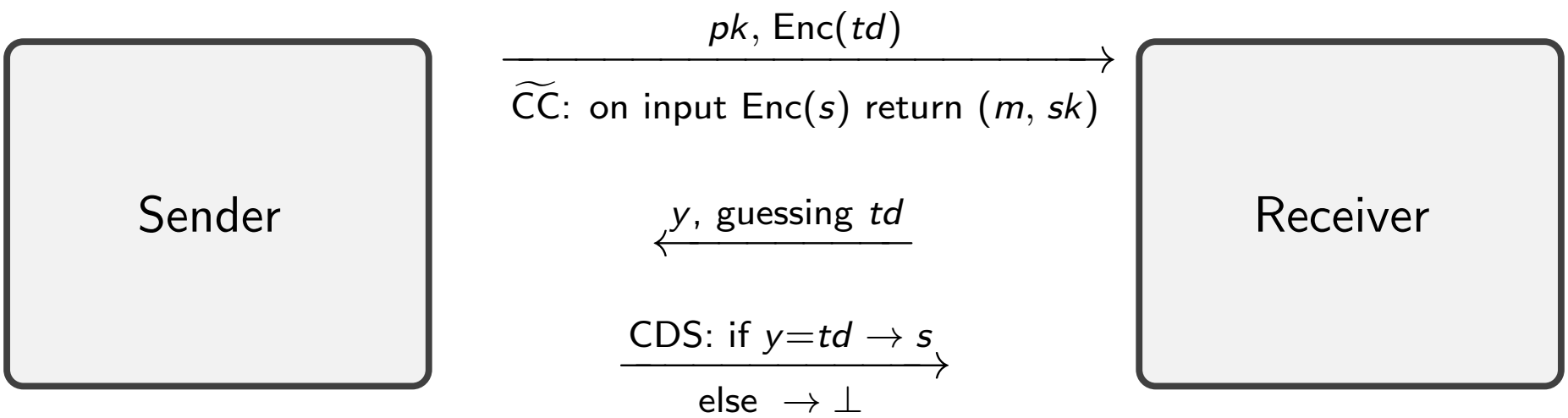
Conditional Disclosure of Secrets [AIR01]



Homomorphic Trapdoor Technique [AL20, BS20]

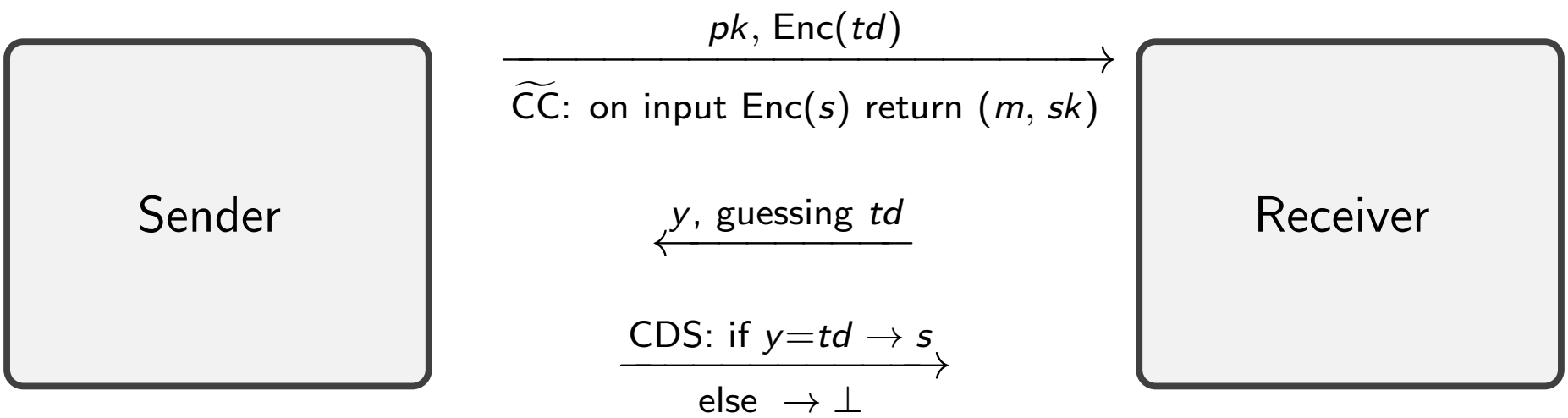


Homomorphic Trapdoor Technique [AL20, BS20]



Hiding: Receiver cannot guess td due to the security of FHE.

Homomorphic Trapdoor Technique [AL20, BS20]

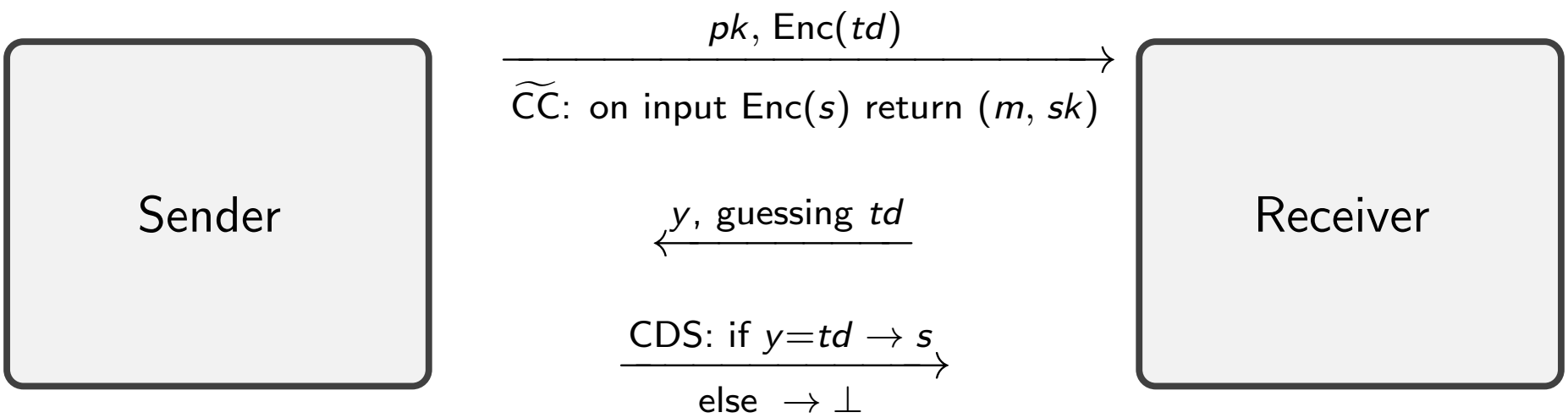


Hiding: Receiver cannot guess td due to the security of FHE.

Extraction:

- Extractor has access to inner state of the sender.

Homomorphic Trapdoor Technique [AL20, BS20]



Hiding: Receiver cannot guess td due to the security of FHE.

Extraction:

- Extractor has access to inner state of the sender.
- $\text{Enc}(td) \xrightarrow{\text{homomorphically}} \text{Enc}(s)$.

ZK Protocols for QMA

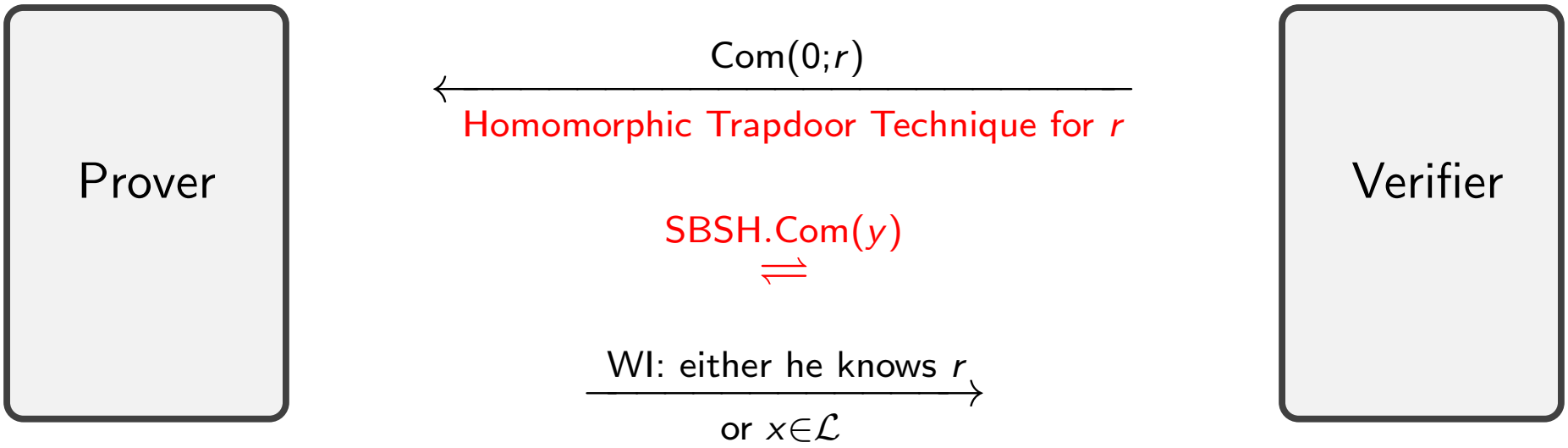
- No Cloning Extraction $\rightarrow$ Constant-Round Computational ZK Argument for QMA [BS20]

ZK Protocols for QMA

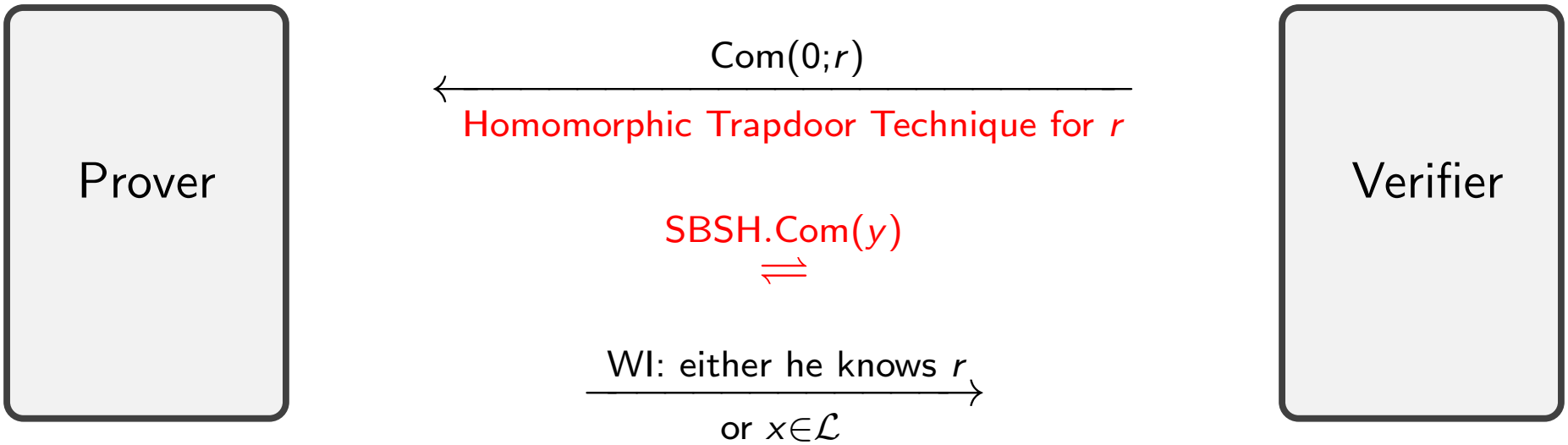
- No Cloning Extraction $\rightarrow$ Constant-Round Computational ZK Argument for QMA [BS20]
- Statistical WI for QMA $\xrightarrow[\text{Extraction}]{\text{No Cloning}}$ 4-Round Statistical ZK Argument for QMA

Table of Contents

4-round ZK Argument for QMA Construction

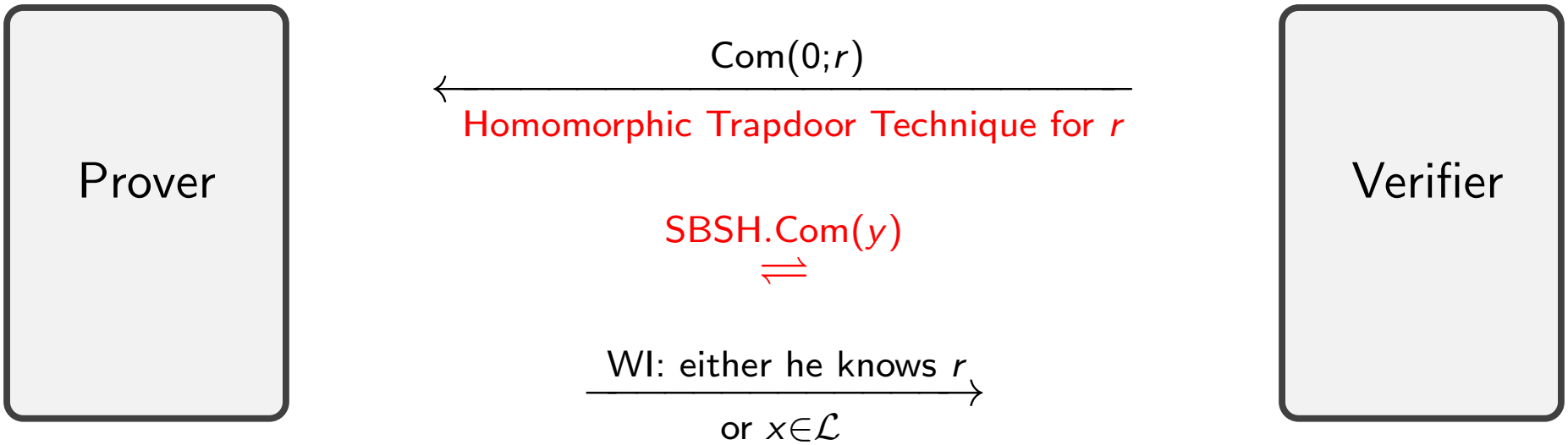


4-round ZK Argument for QMA Construction



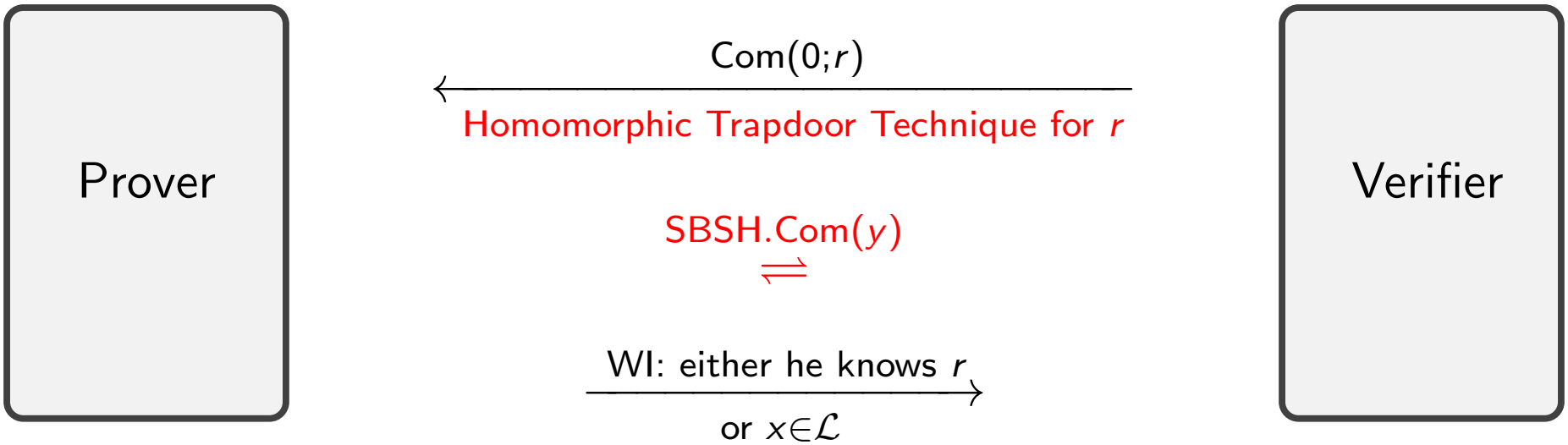
- Simulator extracts r and proves the other WI clause.

4-round ZK Argument for QMA Construction



- Simulator extracts r and proves the other WI clause.
- Works for non-Malicious Verifiers:

4-round ZK Argument for QMA Construction



- Simulator extracts r and proves the other WI clause.
- Works for non-Malicious Verifiers:
  - Non-Aborting.
  - Explainable (messages can always be explained).

Extend to Malicious Verifiers

Aborting

- Our simulator fails in the aborting case, gets stuck with Verifier's encrypted inner state.

Extend to Malicious Verifiers

Aborting

- Our simulator fails in the aborting case, gets stuck with Verifier's encrypted inner state.
- Following the template of [BS20], we construct two Simulators:
  - one aborting
  - one non-aborting

Extend to Malicious Verifiers

Aborting

- Our simulator fails in the aborting case, gets stuck with Verifier's encrypted inner state.
- Following the template of [BS20], we construct two Simulators:
  - one aborting
  - one non-aborting
- A combined simulator guesses which one should be used, using Watrous' Quantum Rewinding Lemma [Wat09].

Extend to Malicious Verifiers

Non-Explainable

- Add proof from the verifier to the prover that the messages were computed honestly.

Extend to Malicious Verifiers

Non-Explainable

- Add proof from the verifier to the prover that the messages were computed honestly.
- Verifier's messages are classical, so ZK for NP suffices.

Extend to Malicious Verifiers

Non-Explainable

- Add proof from the verifier to the prover that the messages were computed honestly.
- Verifier's messages are classical, so ZK for NP suffices.
- To maintain statistical ZK and round complexity we need a 3-round post-quatum ZK proof for NP.

Obstacles

- We need a 3-round post-quantum ZK proof.

Obstacles

- We need a 3-round post-quantum ZK proof.
- Existing 2-round (post-quantum) CDS protocols only provide computational security for the receiver.

Obstacles

- We need a 3-round post-quantum ZK proof.
- Existing 2-round (post-quantum) CDS protocols only provide computational security for the receiver.
- **Solved by constructing a 3-round sometimes-extractable statistically receiver private oblivious transfer (SRP-OT).**

Sometimes-Simulatable ZK

- Weaker ZK notion.

Sometimes-Simulatable ZK

- Weaker ZK notion.
- Simulation is possible with some (negligibly) small probability.

Sometimes-Simulatable ZK

- Weaker ZK notion.
- Simulation is possible with some (negligibly) small probability.
- Simulator (straight line) runs in polynomial time with an exponentially small success probability.

Sometimes-Simulatable ZK

- Weaker ZK notion.
- Simulation is possible with some (negligibly) small probability.
- Simulator (straight line) runs in polynomial time with an exponentially small success probability.
- Security parameters of other primitives are set to account for this exponential loss.

Table of Contents

Conclusion

- Assuming quasi-polynomial hardness of LWE we construct:

Conclusion

- Assuming quasi-polynomial hardness of LWE we construct:
  - A 2-round Statistical Witness Indistinuishability Argument for QMA without trusted setup.

Conclusion

- Assuming quasi-polynomial hardness of LWE we construct:
  - A 2-round Statistical Witness Indistinuishability Argument for QMA without trusted setup.
  - A 4-round Statistical Zero Knowledge-Argument for QMA without trusted setup.

Conclusion

- Assuming quasi-polynomial hardness of LWE we construct:
  - A 2-round Statistical Witness Indistinuishability Argument for QMA without trusted setup.
  - A 4-round Statistical Zero Knowledge-Argument for QMA without trusted setup.
  - A 2-round Zero-Knowledge Argument in the Timing Model without trusted setup.

Conclusion

- Assuming quasi-polynomial hardness of LWE we construct:
  - A 2-round Statistical Witness Indistinuishability Argument for QMA without trusted setup.
  - A 4-round Statistical Zero Knowledge-Argument for QMA without trusted setup.
  - A 2-round Zero-Knowledge Argument in the Timing Model without trusted setup.

- https://eprint.iacr.org/2021/918
  Orestis Chardouvelis and Giulio Malavolta.