Post-Quantum Insecurity from LWE

Alex Lombardi
Simons Institute
&
UC Berkeley

Ethan Mook
Northeastern University

Willy Quach
Northeastern University

Daniel Wichs
Northeastern University
&
NTT Research

TCC 2022

Does proving security under LWE imply post-quantum security?

For Interactive Protocols — No!

Prior Work: Security proofs for interactive protocols can break down for quantum adversaries

- Zero-Knowledge — [vdG97], [Wat06]
- Computational soundness — [Unr12], [ARU14]

Main Issue: Rewinding

For Interactive Protocols — No!

Prior Work: Security proofs for interactive protocols can break down for quantum adversaries

- Zero-Knowledge — [vdG97], [Wat06]
- Computational soundness — [Unr12], [ARU14]

Main Issue: Rewinding

Not just failure of proof techniques:

- [BCMVV18]: explicit counter example

What about *non-interactive* primitives?

- OWF
- PRG
- PRF
- MAC
- Signatures
- CPA SKE
- CCA PKE
- CPA PKE

What about *non-interactive* primitives?

- OWF
- PRG
- PRF
- MAC
- Signatures
- CPA SKE
- CCA PKE
- CPA PKE

Reasonable Hope: Rewinding doesn't come up, so for non-interactive primitives

$$\text{Security from LWE} \overset{?}{\Rightarrow} \text{Post-quantum security}$$

What about *non-interactive* primitives?

- OWF
- PRG
- PRF
- MAC
- Signatures
- CPA SKE
- CCA PKE
- CPA PKE

Reasonable Hope: Rewinding doesn't come up, so for non-interactive primitives

Security from LWE $\not\Rightarrow$ Post-quantum security

<u>Main Result</u>: explicit (contrived) counterexamples for ***non-interactive*** primitives that are

- Classically secure under LWE
- Quantumly broken

Techniques

Core Observation: Many non-interactive primitives have **interactive security games**

↳ Rewinding can be an issue

Techniques

Core Observation: Many non-interactive primitives have **interactive security games**

↳ Rewinding can be an issue

Goal: “Force” the reduction to rewind the adversary

Techniques

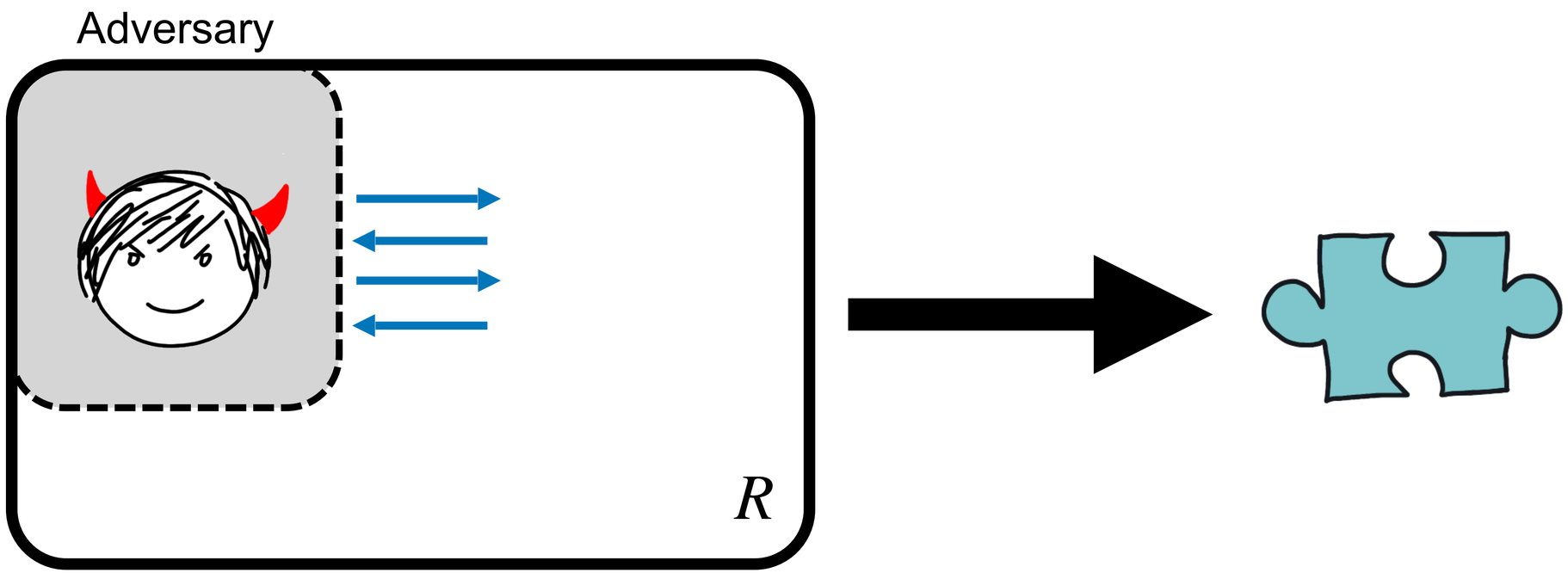
Core Observation: Many non-interactive primitives have **interactive security games**

↳ Rewinding can be an issue

Goal: “Force” the reduction to rewind the adversary

Technique: Embed an “interactive proof of quantumness” into the security game

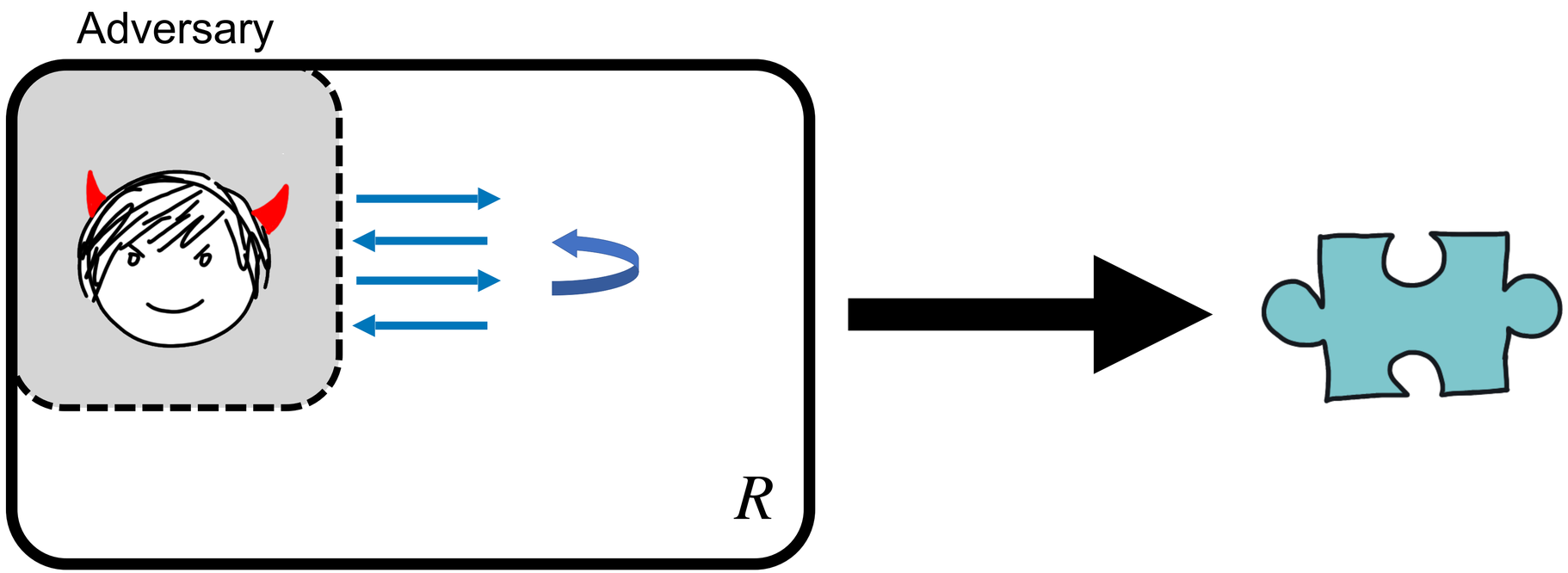
What goes wrong?



Black-box Reduction

Computationally Hard Problem

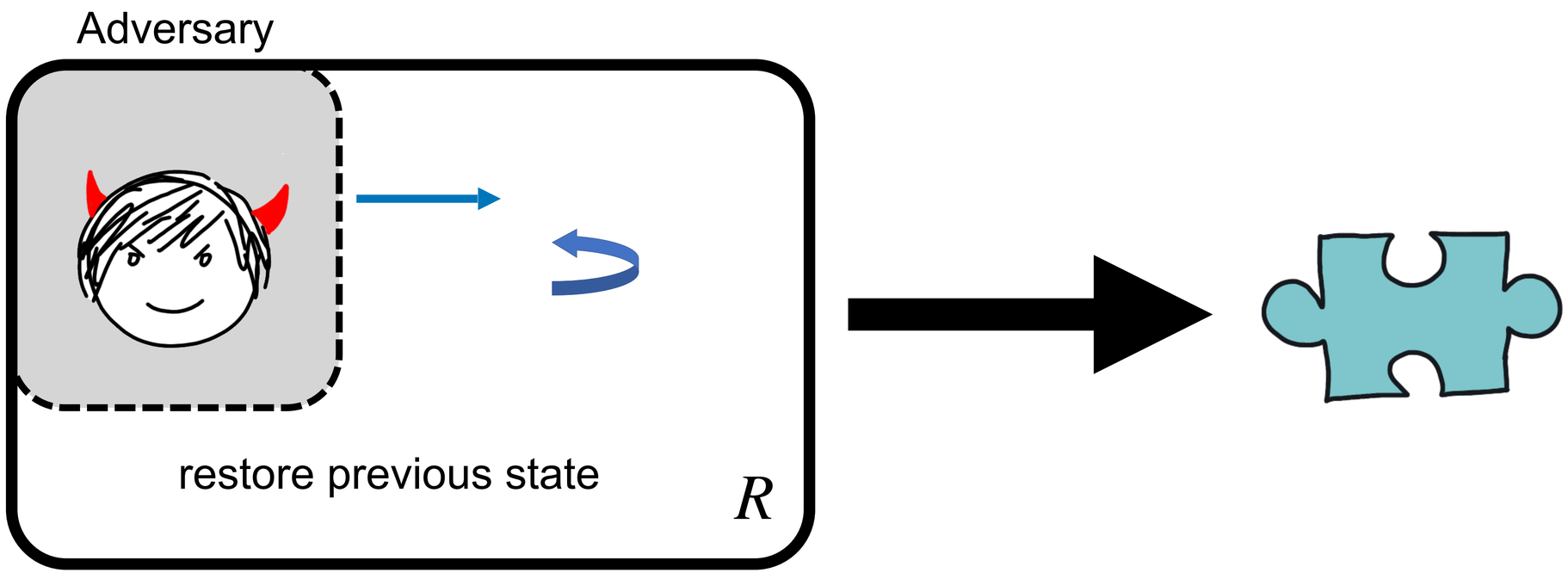
Rewinding



Black-box Reduction

Computationally Hard Problem

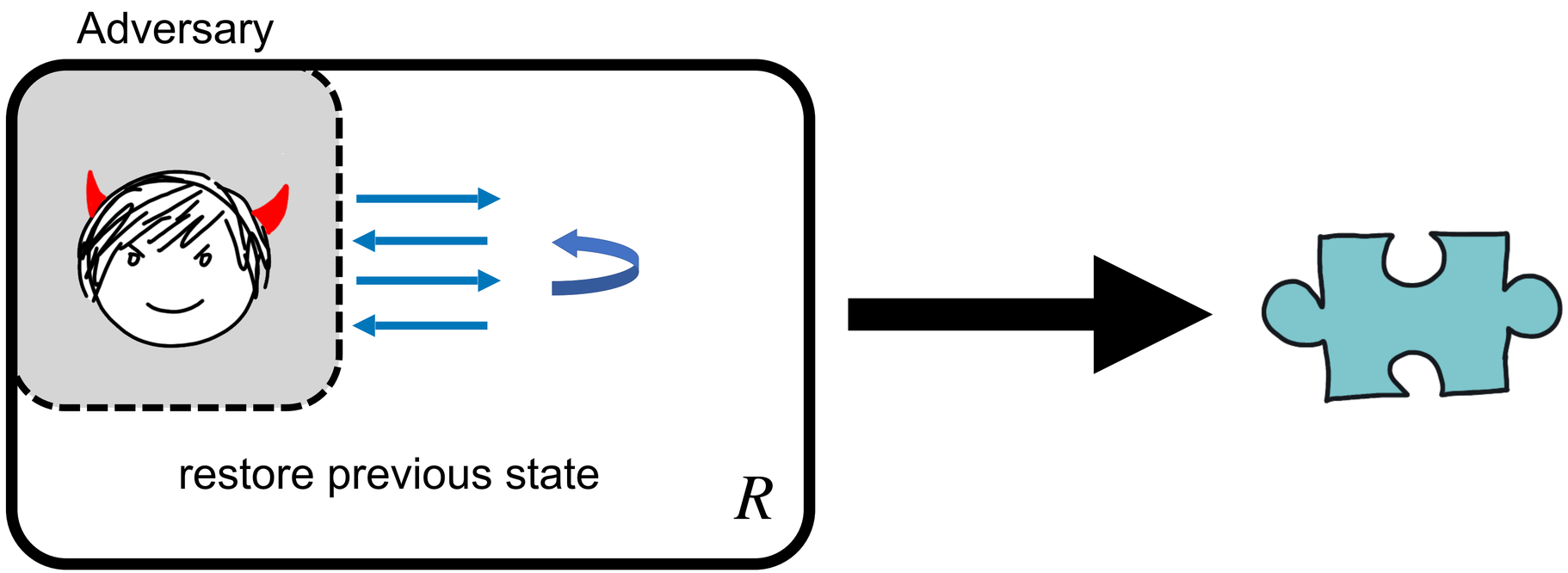
Rewinding



Black-box Reduction

Computationally Hard Problem

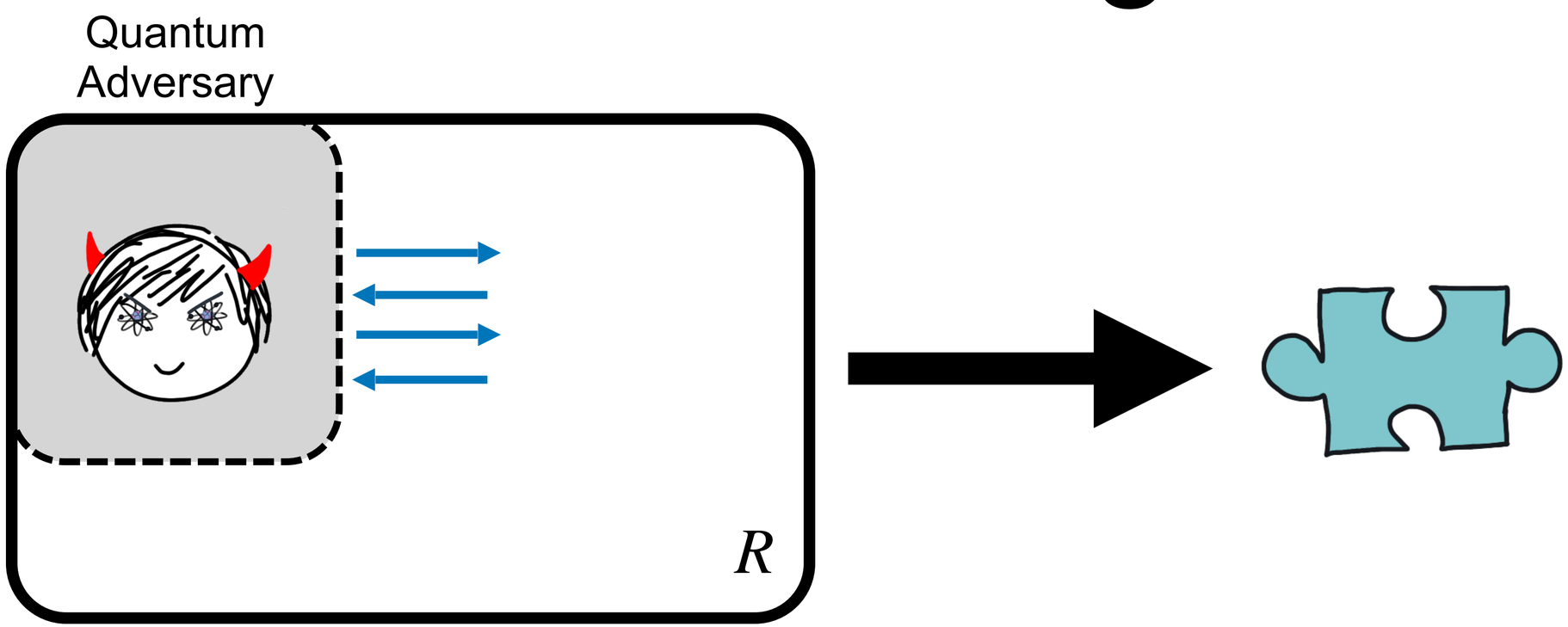
Rewinding



Black-box Reduction

Computationally Hard Problem

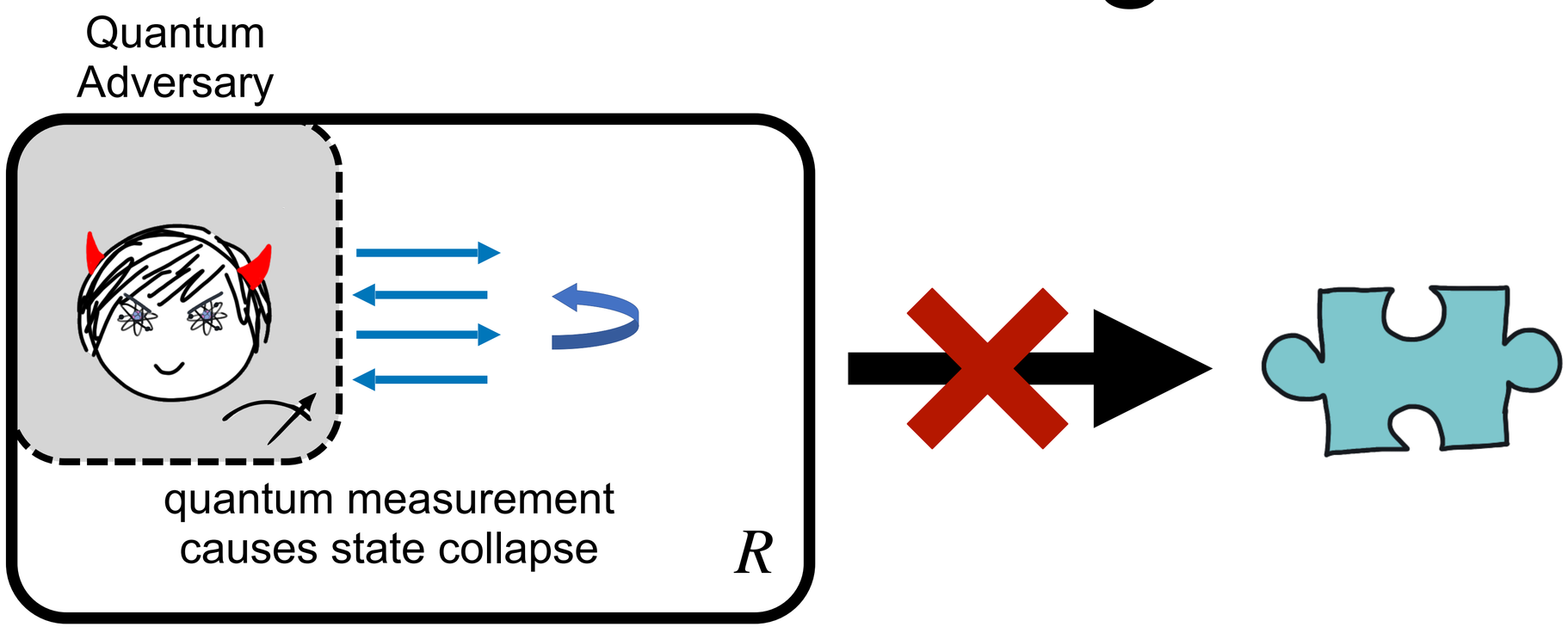
Rewinding



Black-box Reduction

Computationally Hard
Problem

Rewinding

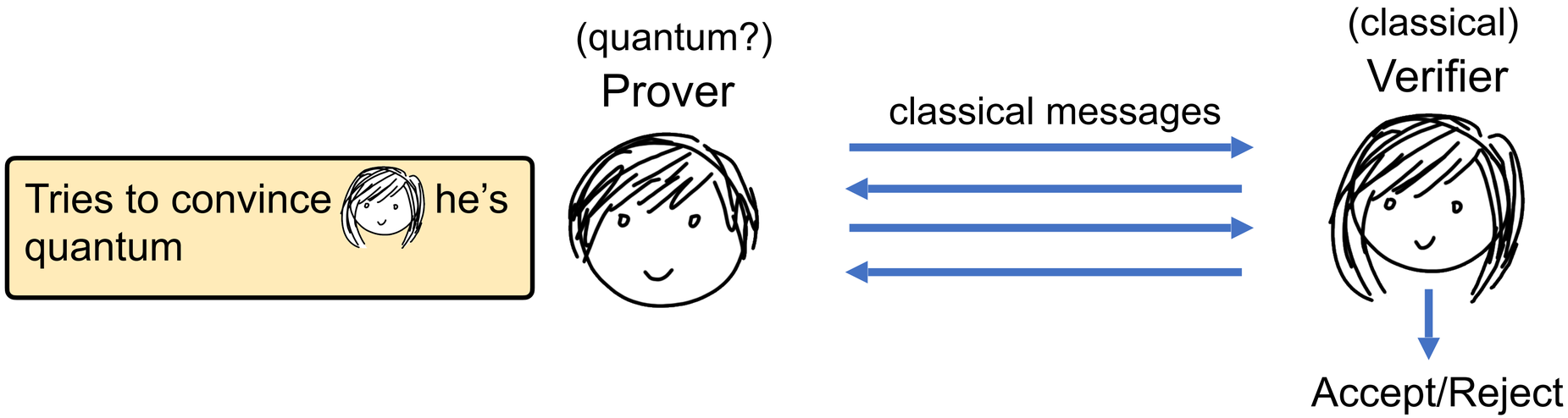


Black-box Reduction

Computationally Hard
Problem

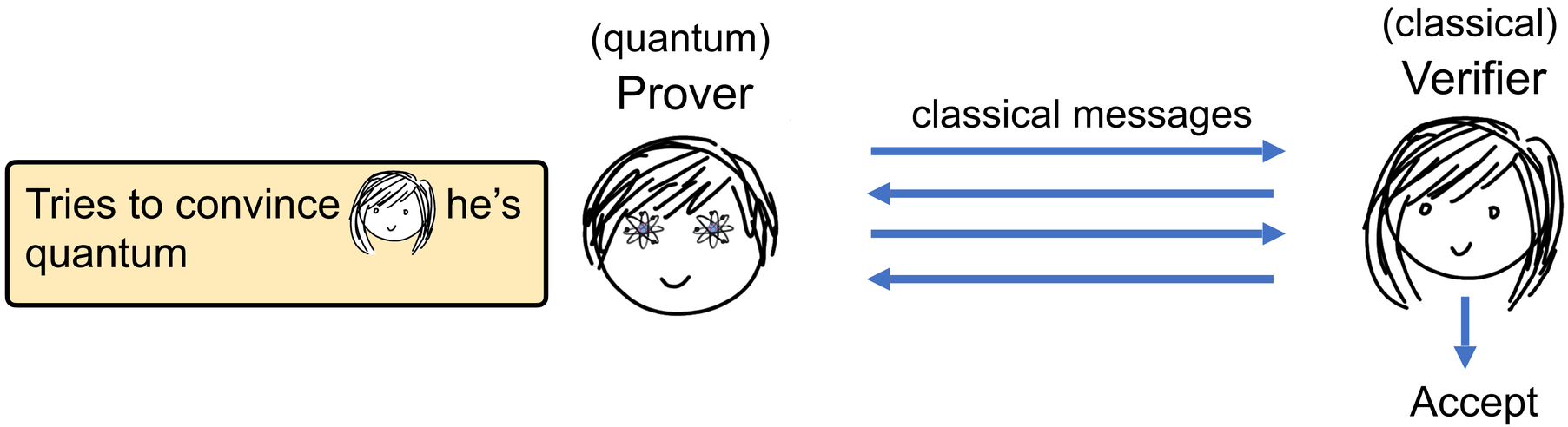
Interactive Proofs of Quantumness (IPQs)

[BCMVV18]



Interactive Proofs of Quantumness (IPQs)

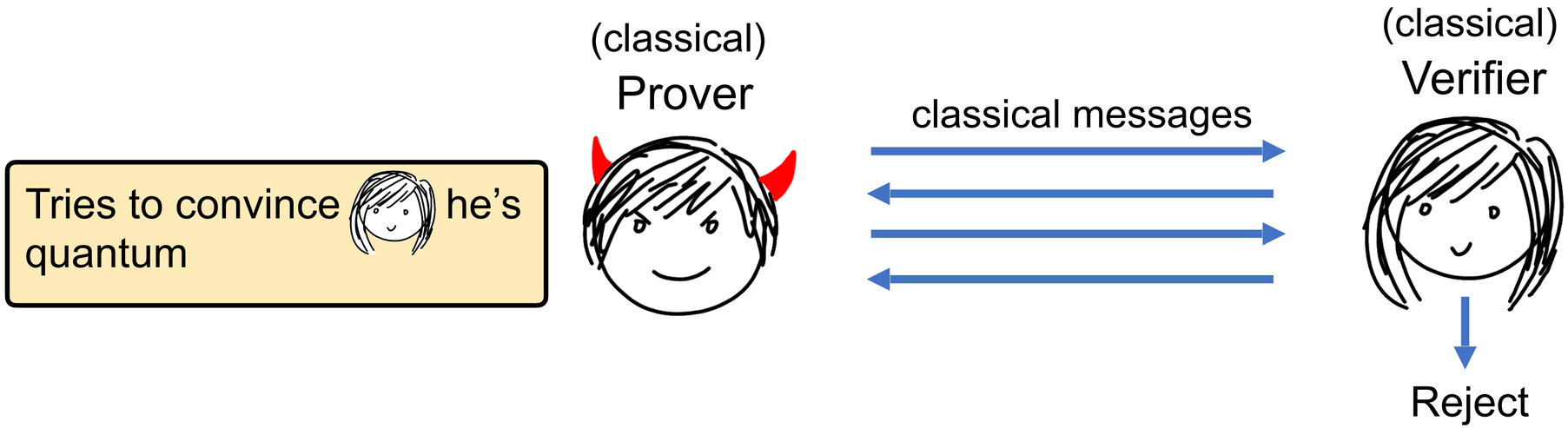
[BCMVV18]



- **Completeness:** quantum can convince

Interactive Proofs of Quantumness (IPQs)

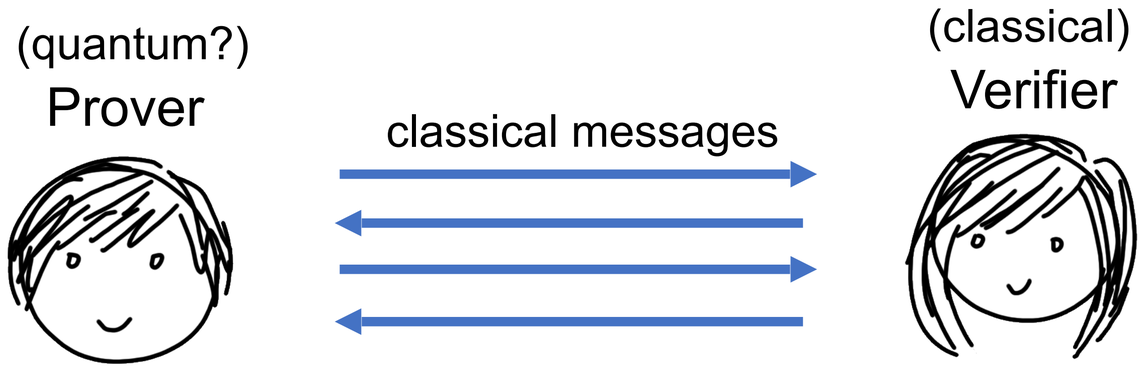
[BCMVV18]



- **Completeness:** quantum can convince
- **Soundness:** classical cannot convince but with negligible probability

Interactive Proofs of Quantumness (IPQs)

[BCMVV18]

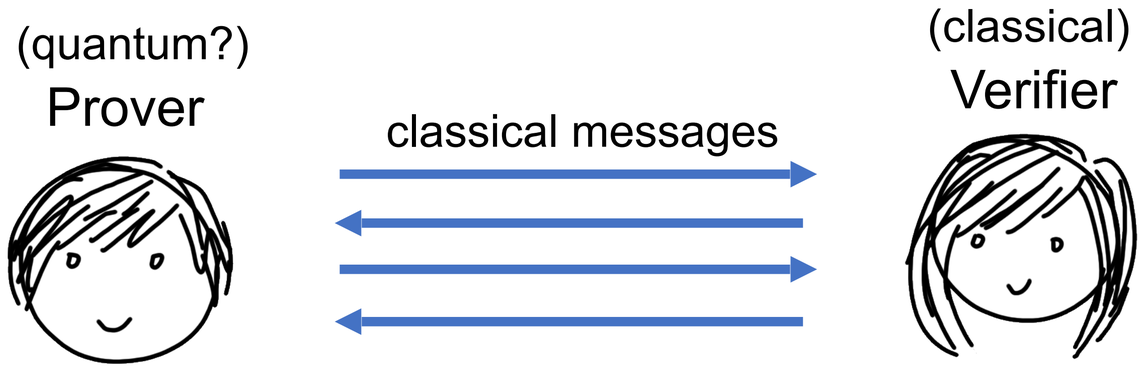


IPQs = Primitives where rewinding issues are inherent

Any reduction will fail for quantum adversaries

Interactive Proofs of Quantumness (IPQs)

[BCMVV18]

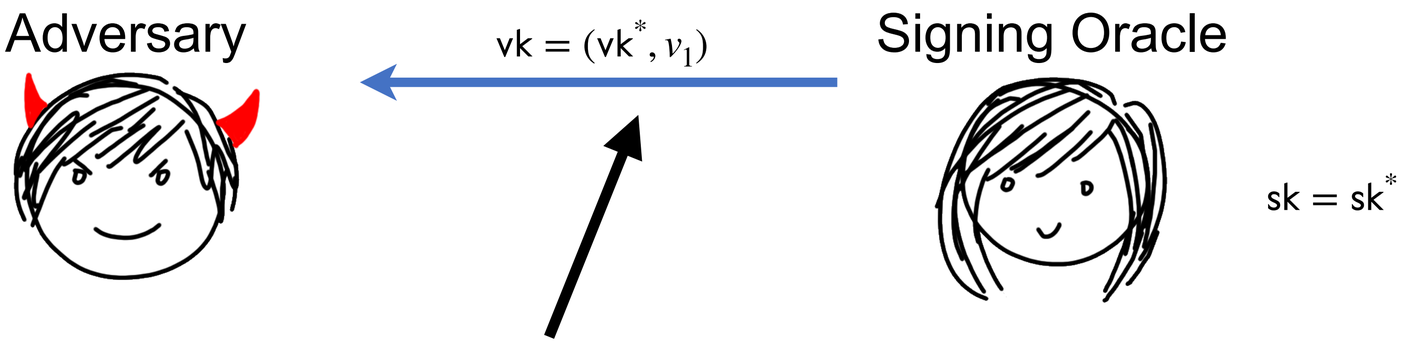


IPQs = Primitives where rewinding issues are inherent

Any reduction will fail for quantum adversaries

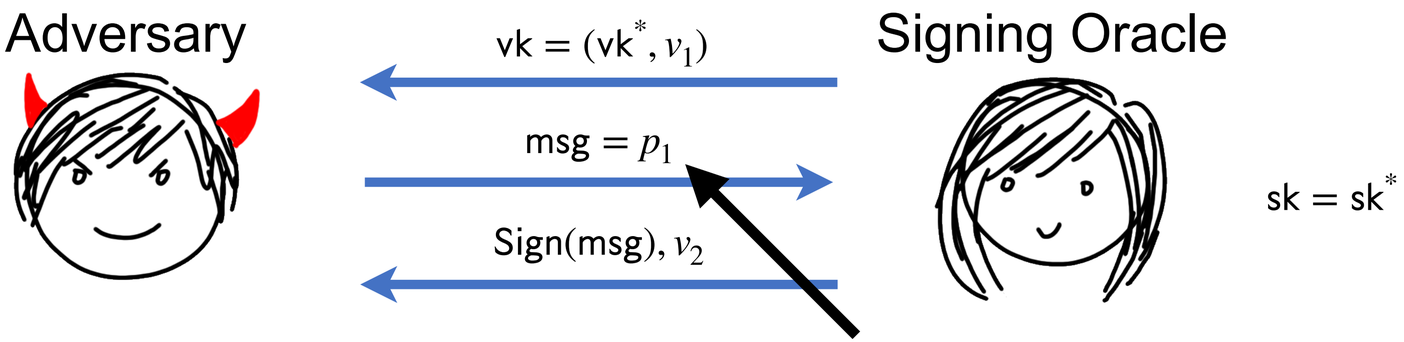
<u>Theorem</u> [BCMVV18]**:** 4-round IPQ from LWE

Embedding an IPQ in Signatures



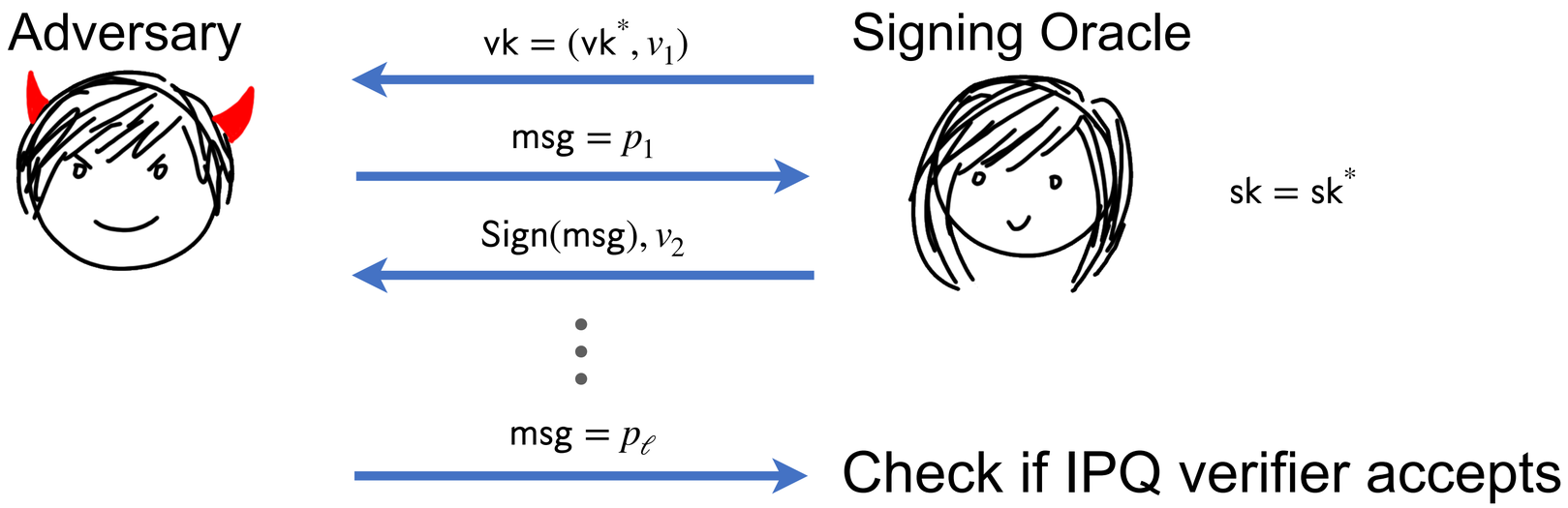
Verification key contains
first IPQ verifier message

Embedding an IPQ in Signatures

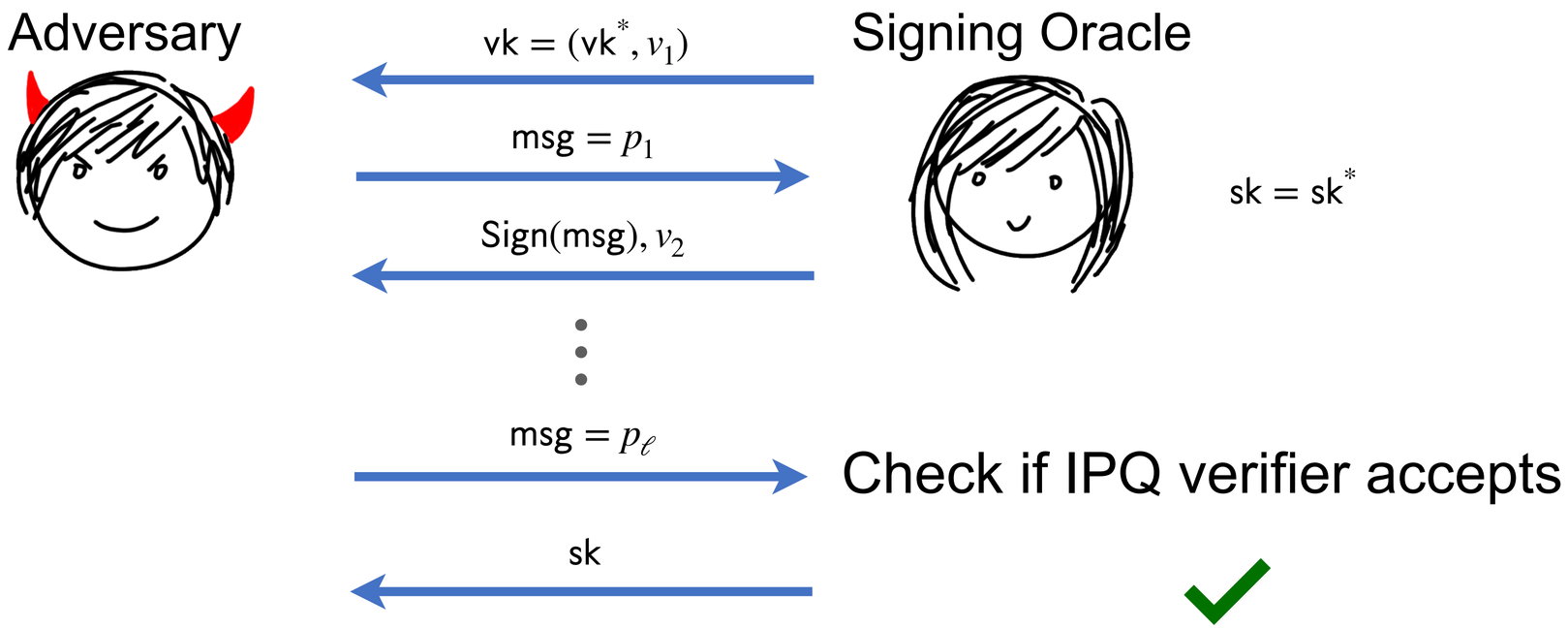


Parse each signing query as an IPQ prover message

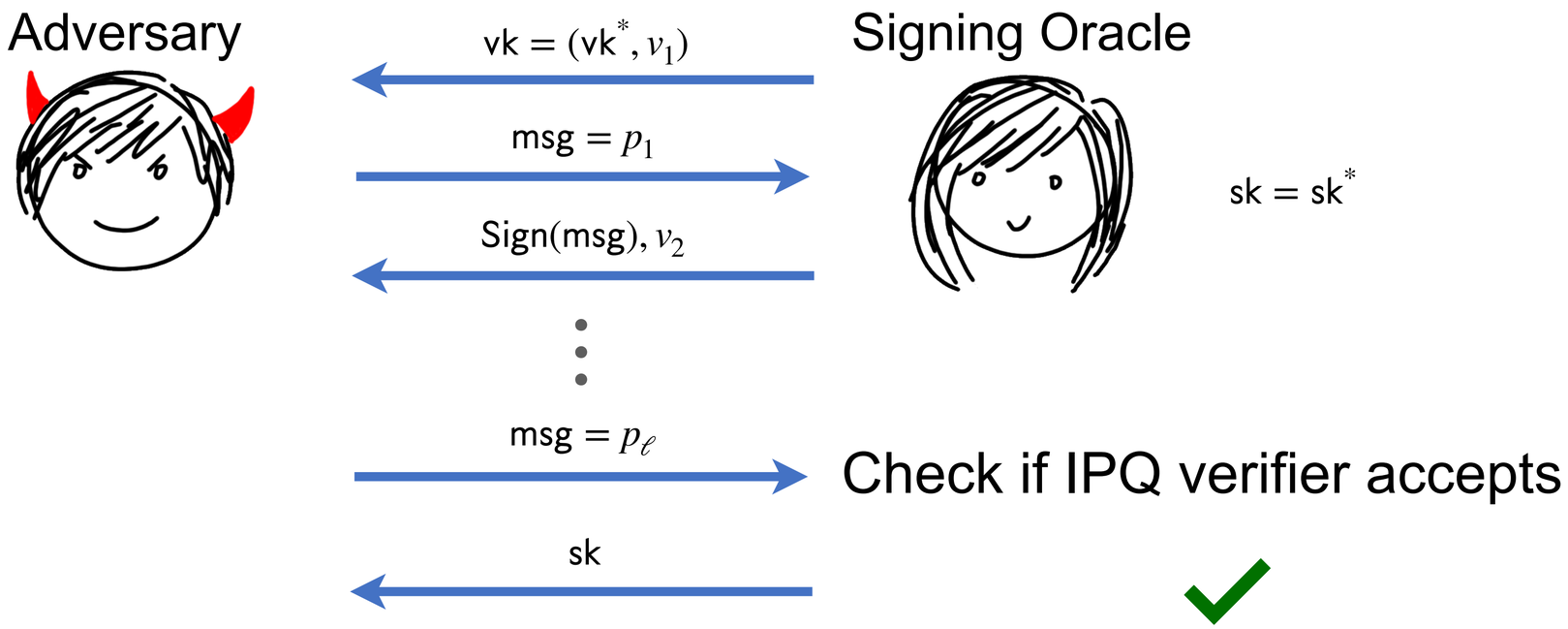
Embedding an IPQ in Signatures



Embedding an IPQ in Signatures



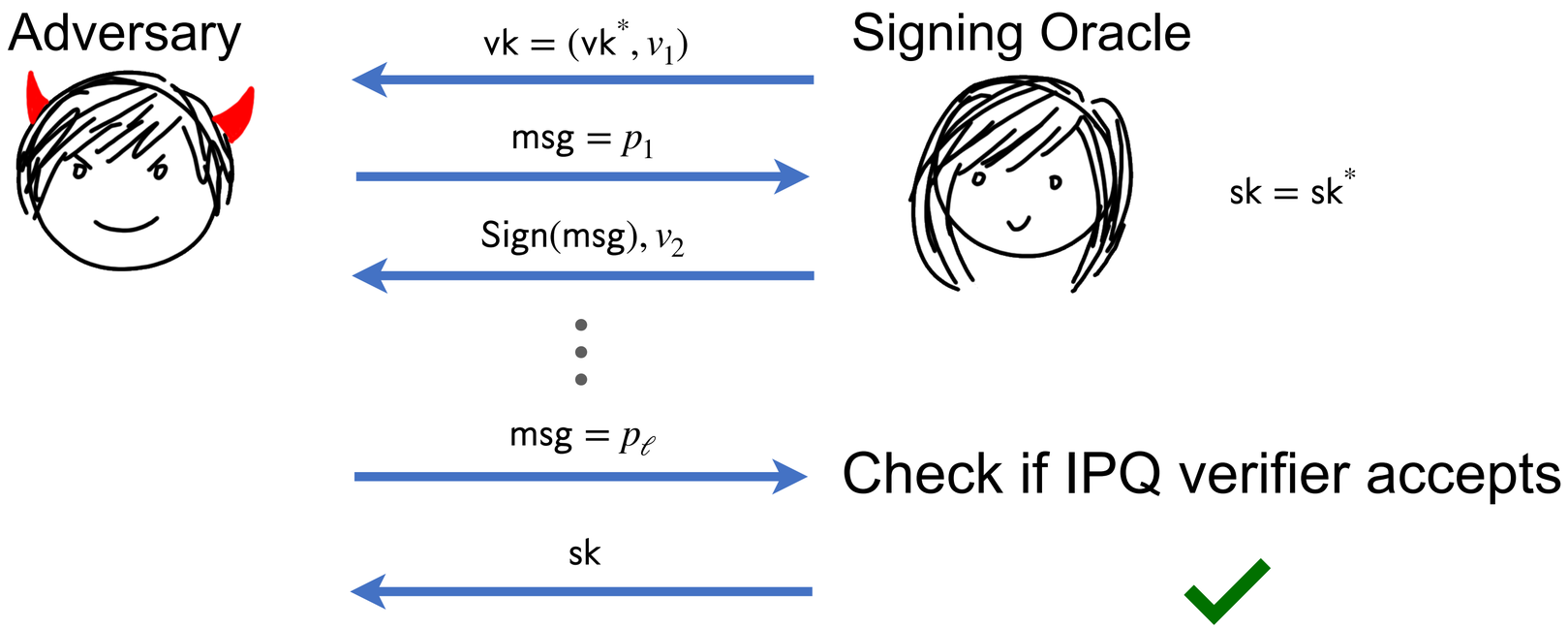
Embedding an IPQ in Signatures



IPQ Soundness ⇒ Classical security

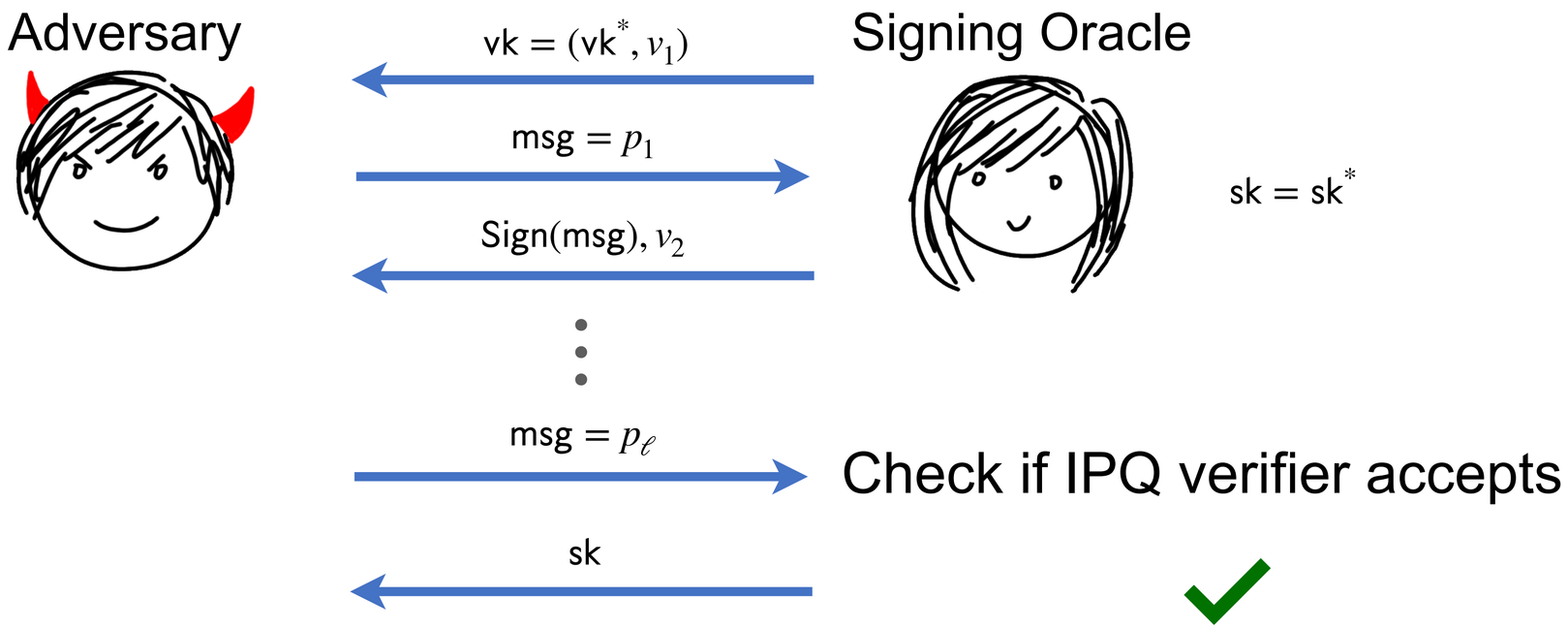
IPQ Completeness ⇒ Quantum break

Embedding an IPQ in Signatures



Problem: Signing oracle now stateful

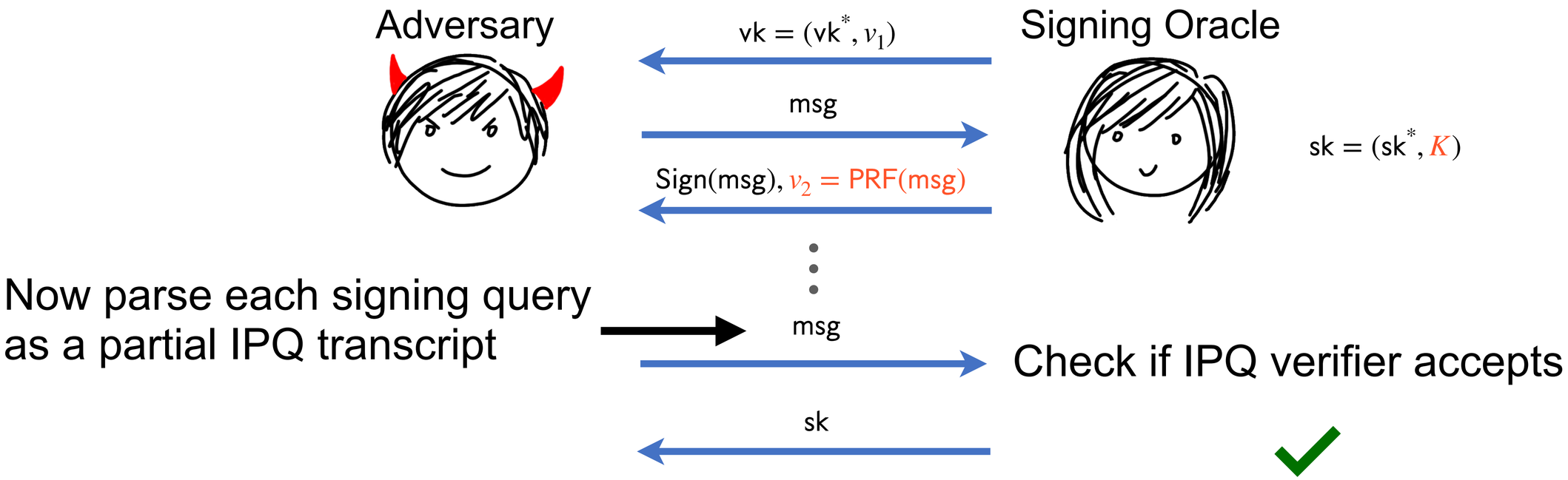
Embedding an IPQ in Signatures



Observation: IPQ from [BCMVV18] is public coin after first verifier message

$\Rightarrow$ it satisfies a notion of *resettable soundness*

Embedding an IPQ in Signatures



Observation: IPQ from [BCMVV18] is public coin after first verifier message

$\Rightarrow$ it satisfies a notion of *resettable soundness*

Other Results

<u>Theorem</u>: construct a **3-round** protocol where classical sender sends a message m such that

- m is hidden from classical receivers
- quantum receiver learns m

<u>Theorem</u>: counterexamples for non-interactive primitives that are

- ***"One-time"*** classically secure under LWE
- Quantumly broken in fewer queries

→

- One-time signatures
- One-time MAC
- One-time PRF
- One-time SKE
- One-time CCA PKE

Open Problems

Can we get counterexamples for CPA public-key encryption?

↳ Our techniques fall short b/c adversary win is publicly verifiable

Open Problems

Can we get counterexamples for CPA public-key encryption?

↳ Our techniques fall short b/c adversary win is publicly verifiable

What about truly non-interactive primitives (OWFs, PRGs,…)?

↳ No interaction in security game ⇒ no rewinding
↳ Seemingly would require non black-box techniques
↳ [YZ22]: Counterexample for OWFs in ROM

Summary

<u>Main Theorem</u>: explicit (contrived) counterexamples for ***non-interactive*** primitives that are

- Classically secure under LWE
- Quantumly broken

- PRF
- Signatures
- MAC
- CPA SKE
- CCA PKE

<u>Theorem</u>: counterexamples for “one-time” versions of the same primitives

Reductions for post-quantum security must be quantum compatible regardless of “post-quantumness” of assumption