Constructive Post-quantum Reductions

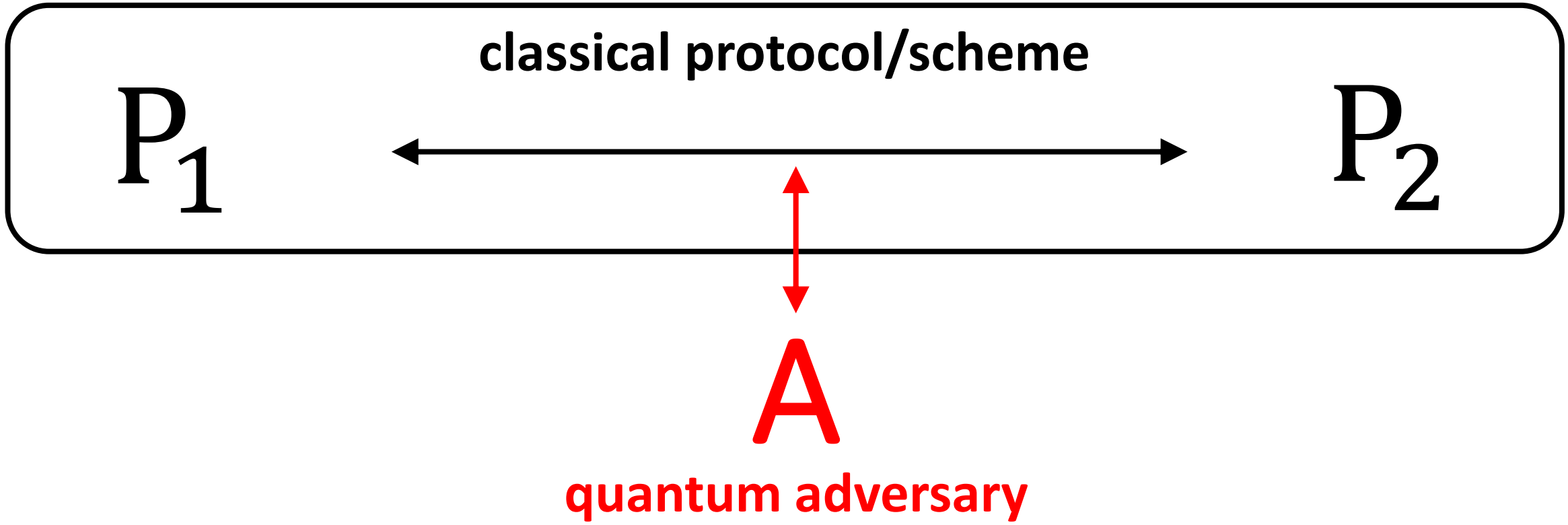
Yael Tauman Kalai

MSR/MIT

Based on joint work with Nir Bitansky and Zvika Brakerski

*Slides taken from talks by Nir and Zvika

Post-quantum Cryptography

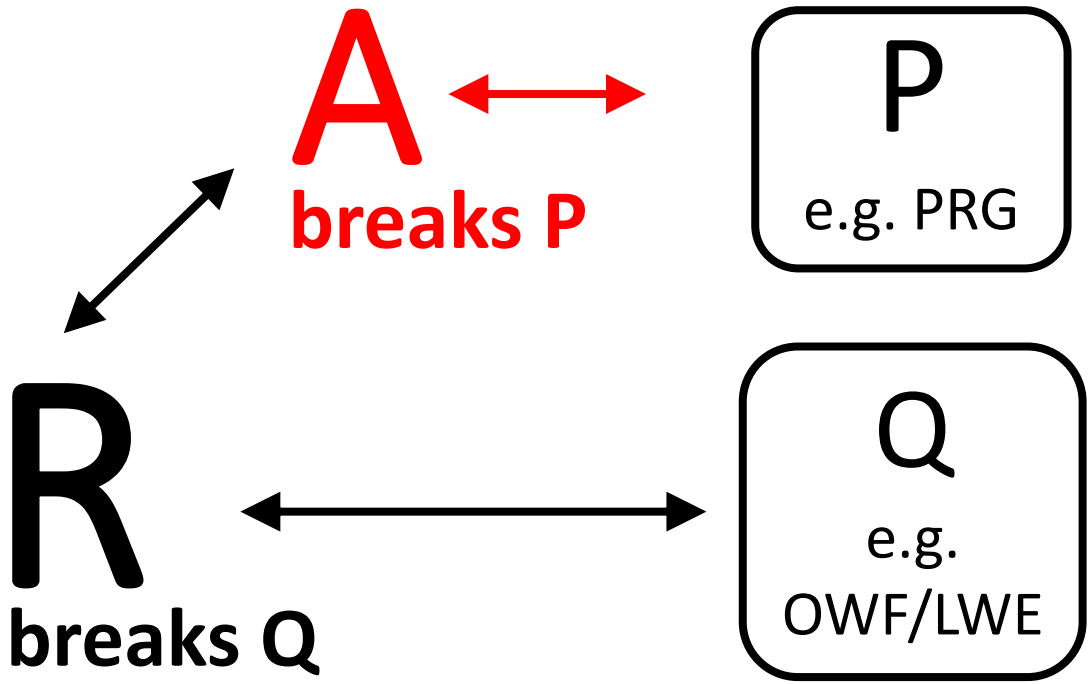


Does security still hold in the presence of a quantum adversary?

Post-quantum Cryptography

1. **Post-quantum assumptions:** Lattice instead of Factoring…

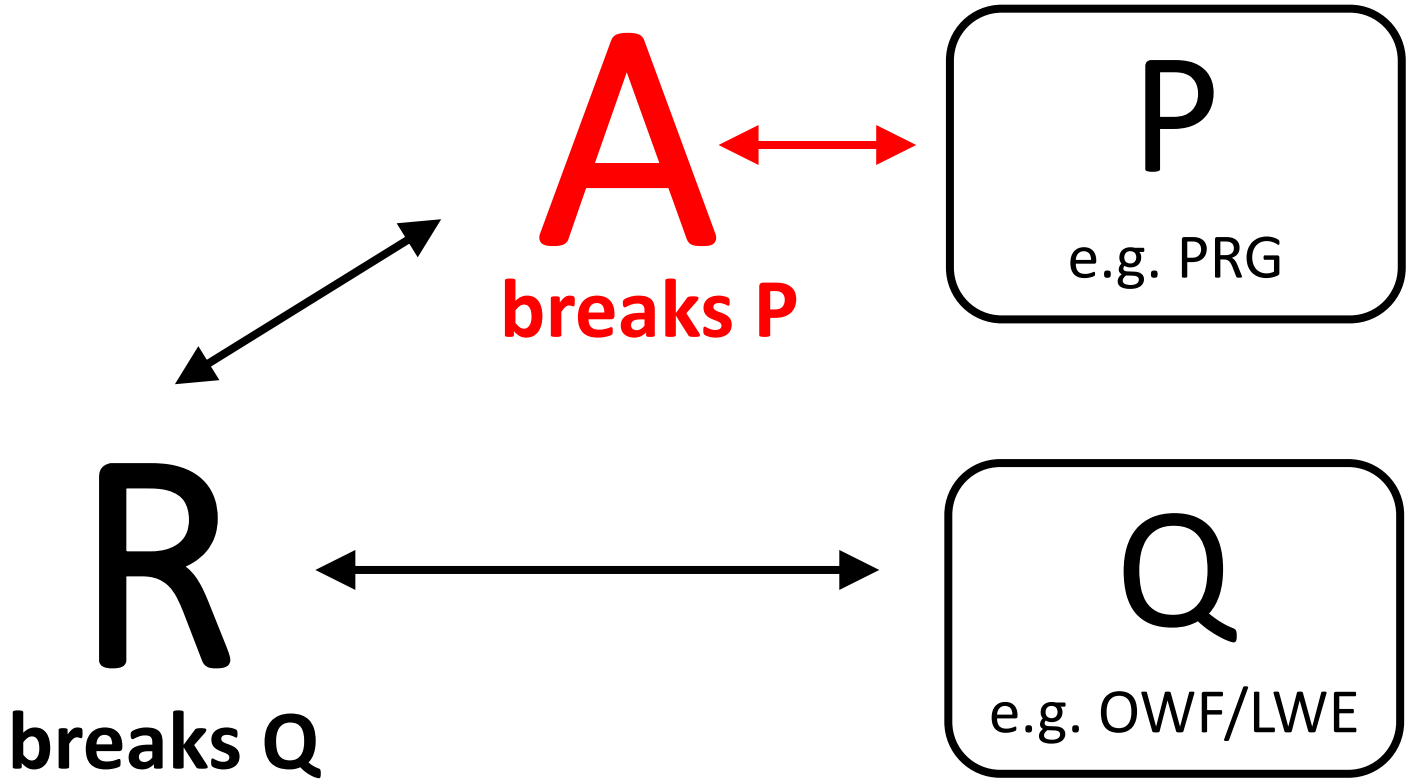
2. **Post-quantum reductions:**



Do our classical reductions carry over to the post-quantum setting?

For example, do OWFs imply PRGs?

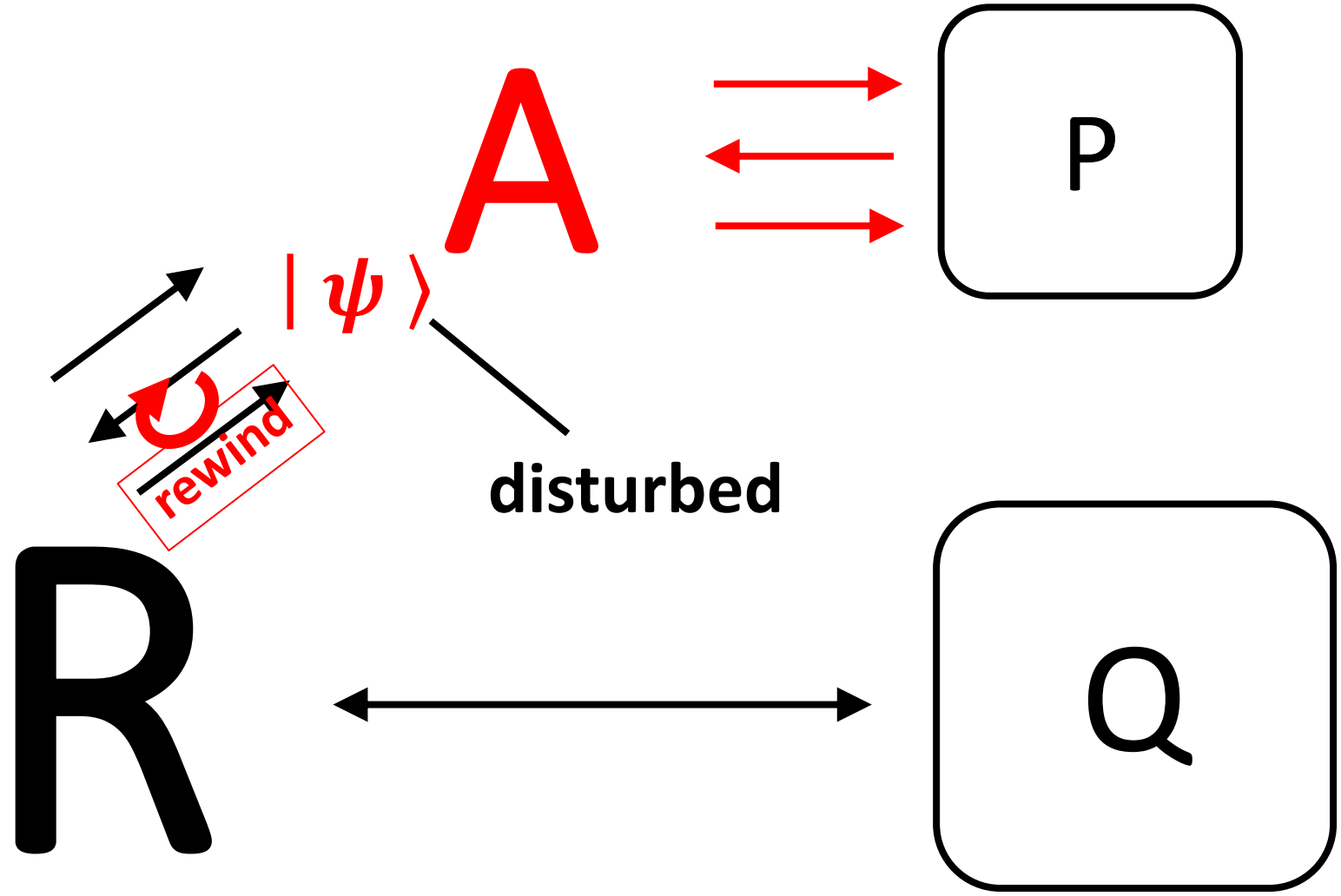
(Security) Reductions



Can classical reductions be lifted to post-quantum setting?

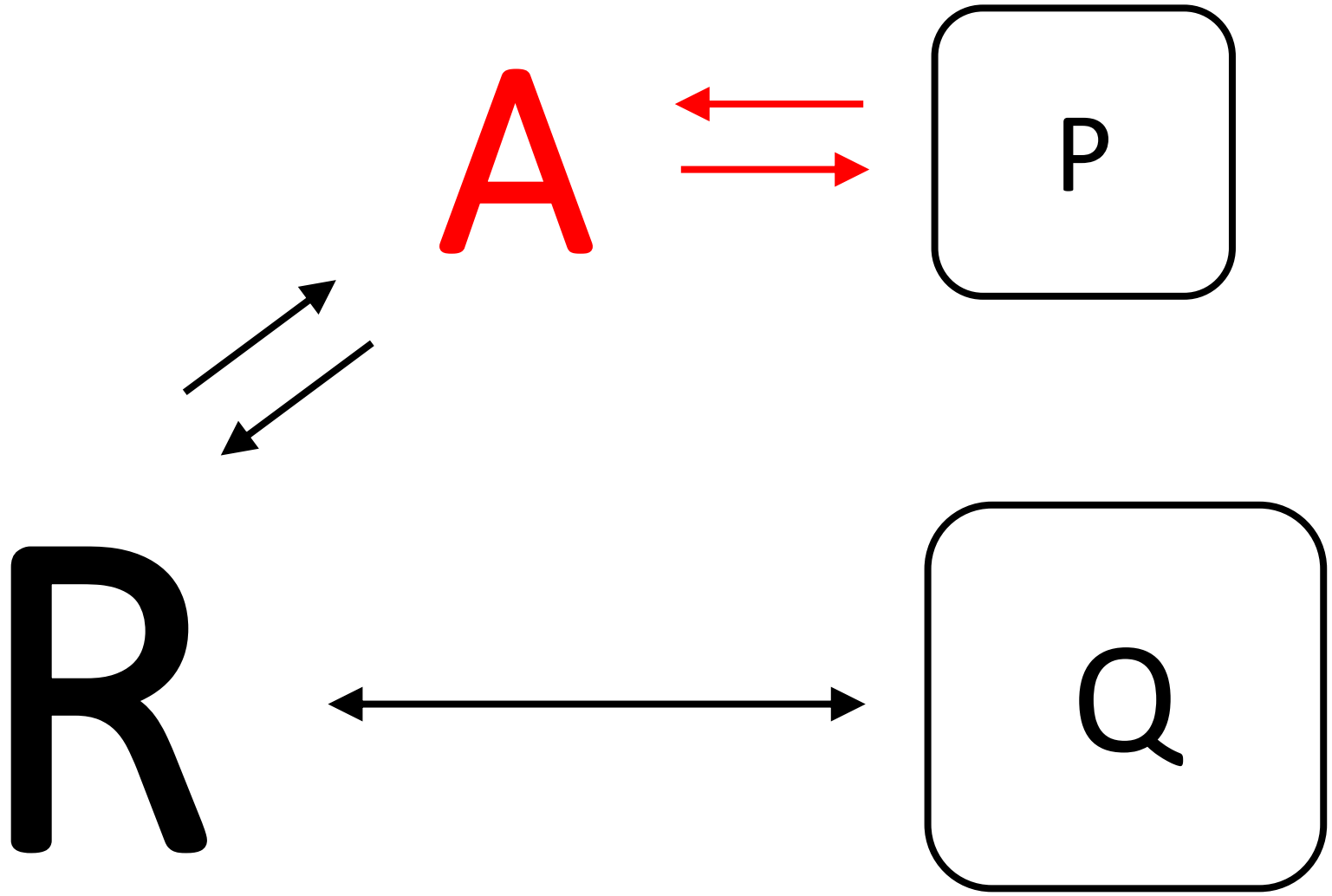
Most classical reductions treat A as a **black box**....

Problematic in Interactive Setting

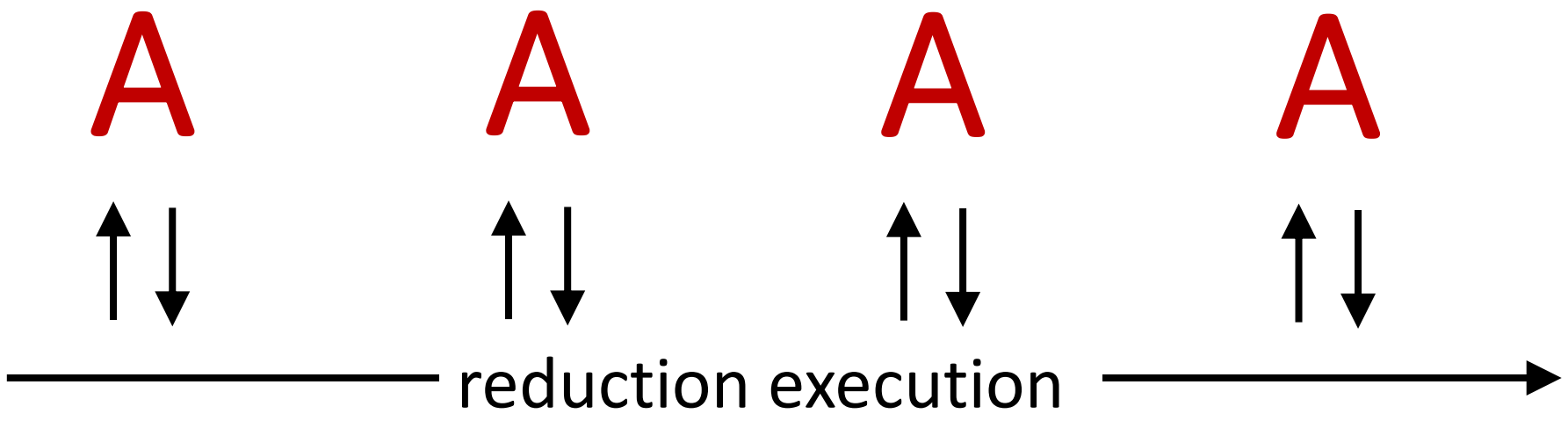


∃ interactive P BB-reducible to LWE, but quantumly broken [BCMVV18]

Our Focus: Non-interactive Primitives/Assumptions

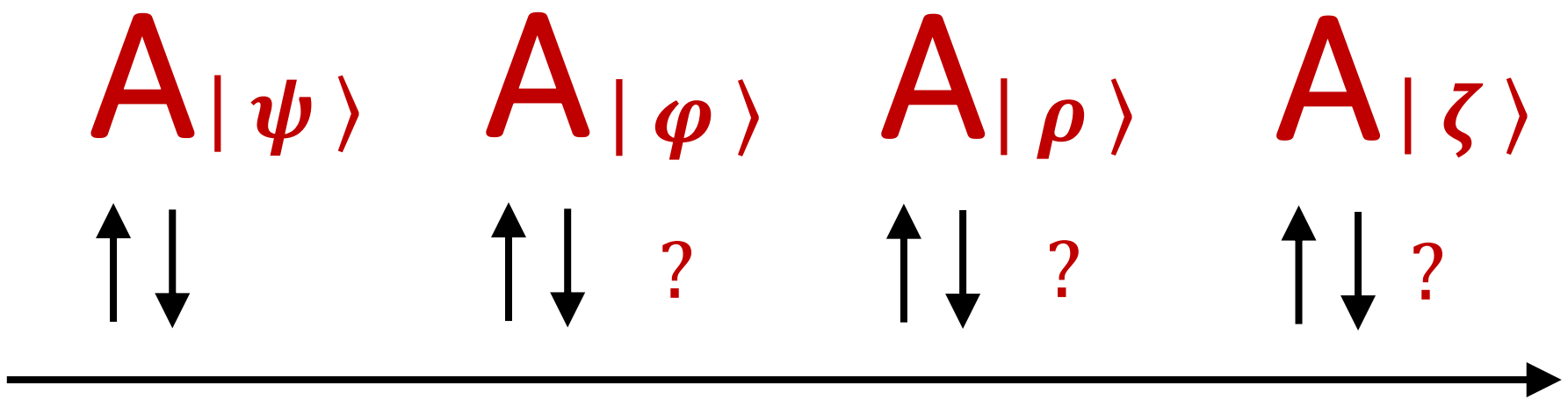


Our Focus: Non-interactive Primitives/Assumptions



R

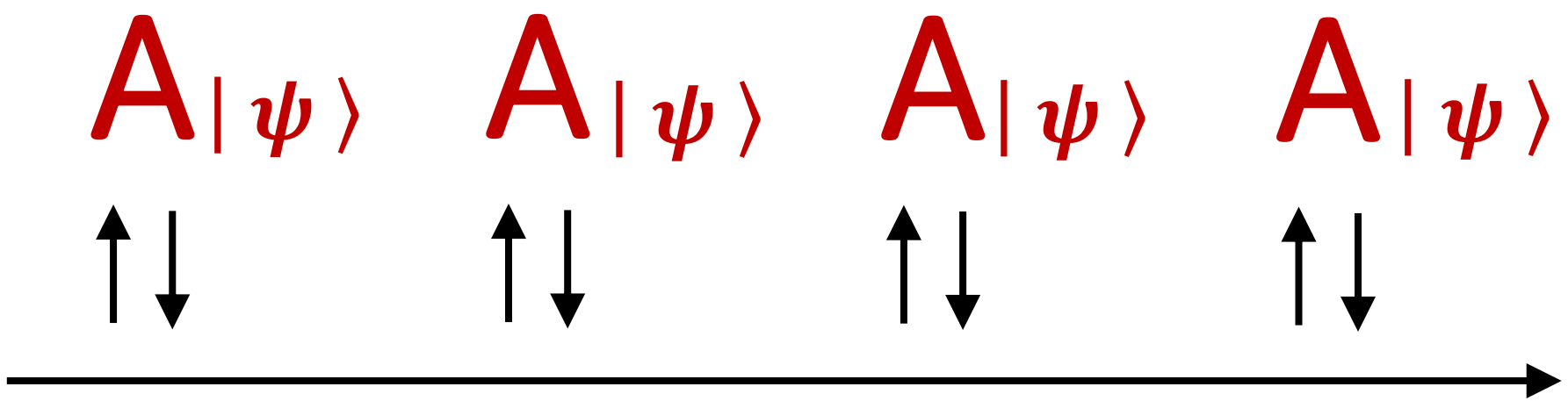
Quantum Auxiliary Input



R

Auxiliary input state disturbed

Just Copy the State?



R

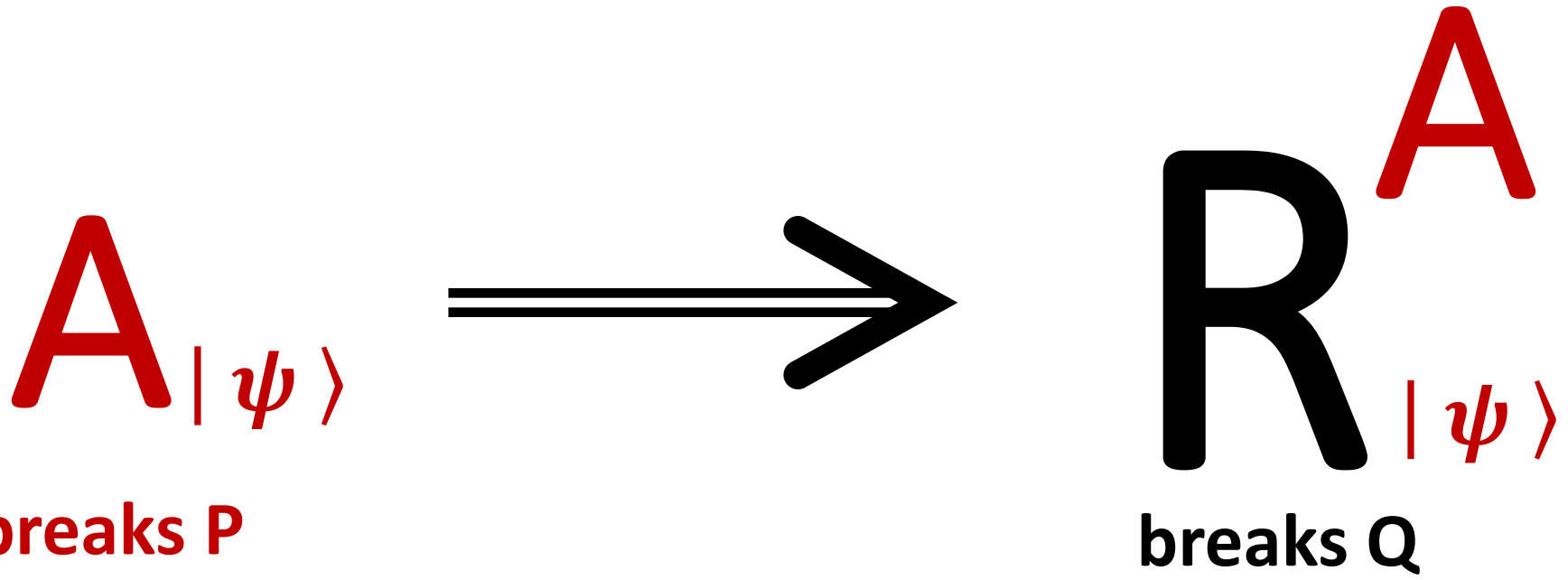
Where does $|\psi\rangle$ come from?

- Intermediate state in a protocol
- Expensive preprocessing

Quantum cloning impossible!

Non-constructive reduction

Goal: Constructive Reductions



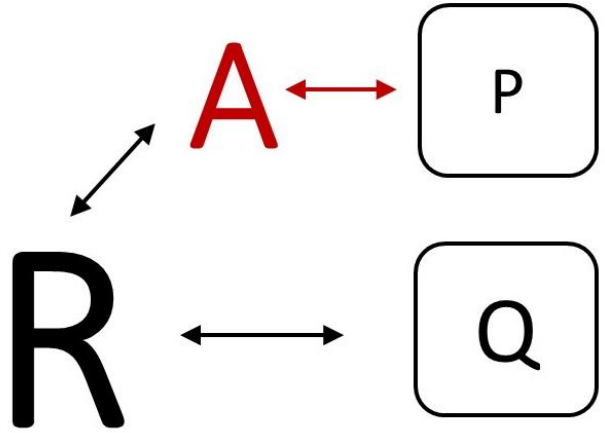
Win-Win: broken scheme ⇒ explicit algorithmic advance

Targeted also classically (**uniform** reductions) [Bellare, Rogaway]

Goal II: Durability, new algorithm should work forever.

Our Results

Lifting large class of classical reductions



Lift any **R** such that:

- **R** is **black box**
- **R** is **non-adaptive**
- **P** is a **decision assumption** (e.g. PRG) or has few solutions (e.g Injective OWF)

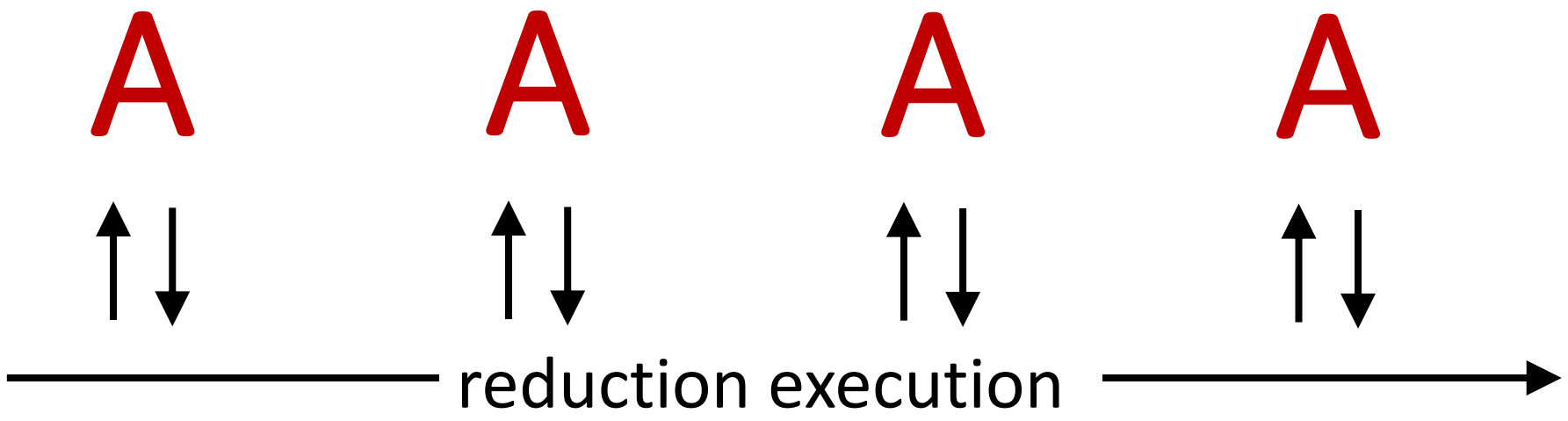
Resulting **post-quantum reduction** is **constructive** and **durable**.

Negative result

Restriction on **P** being a **decision assumption** is somewhat inherent.

A taste of the techniques

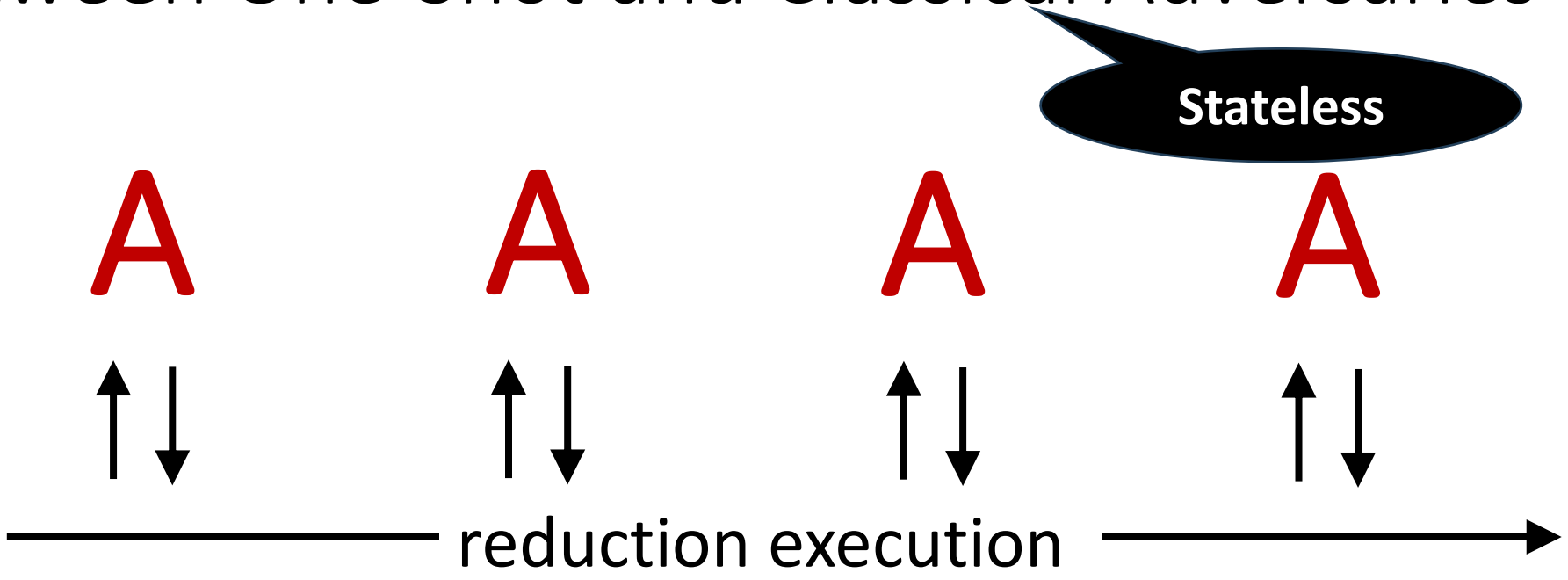
Observation:



R

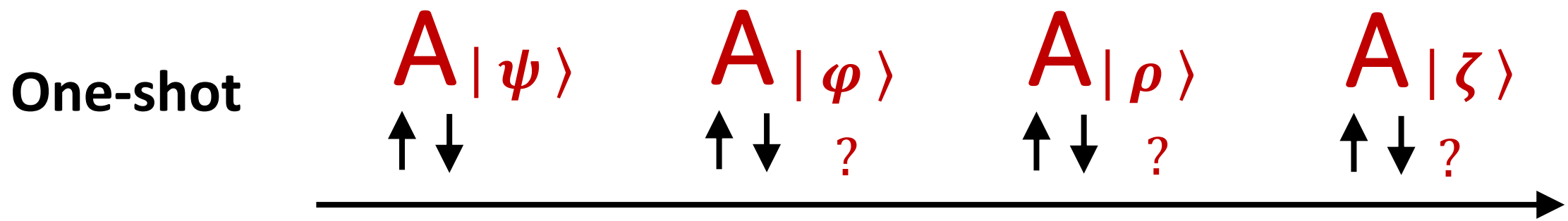
Post-quantum reduction

Bridge Between One-Shot and Classical Adversaries

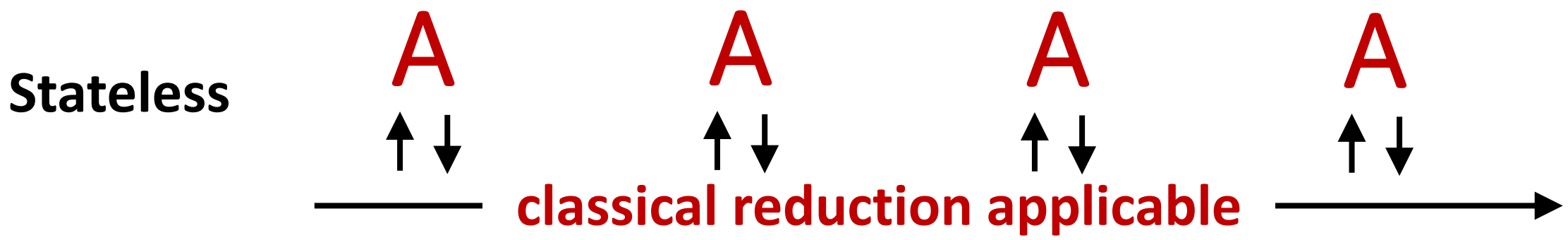


R

Bridge Between One-Shot and Stateless Adversaries

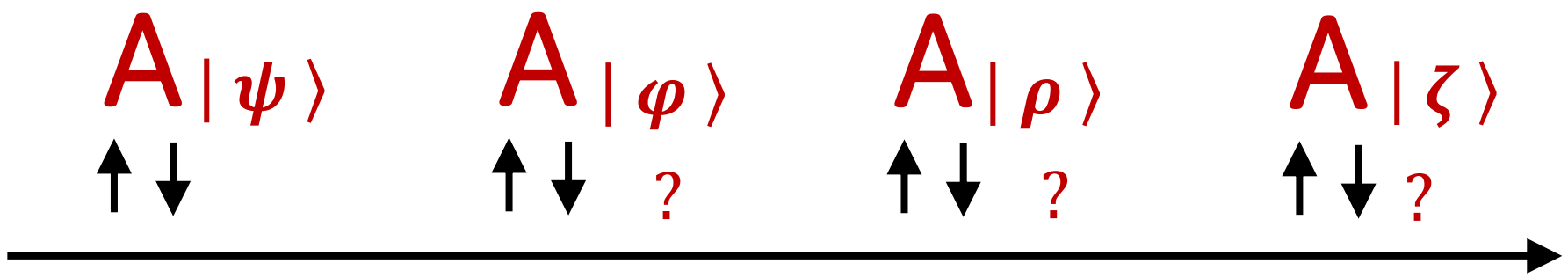


Gap



Bridge 1: One-Shot to Persistent

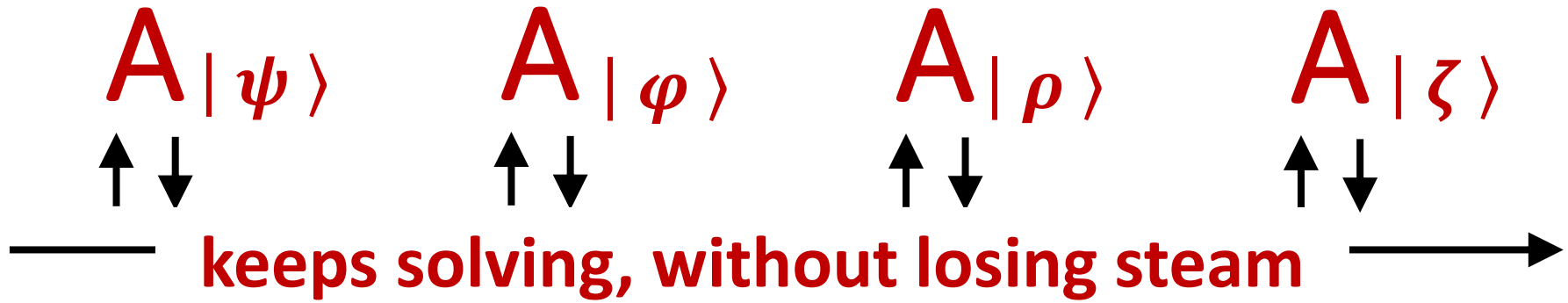
One-shot



[CMSZ21]: For any non-interactive ~~publicly-verifiable~~ decisional assumption, convert one-time solver to a persistent one

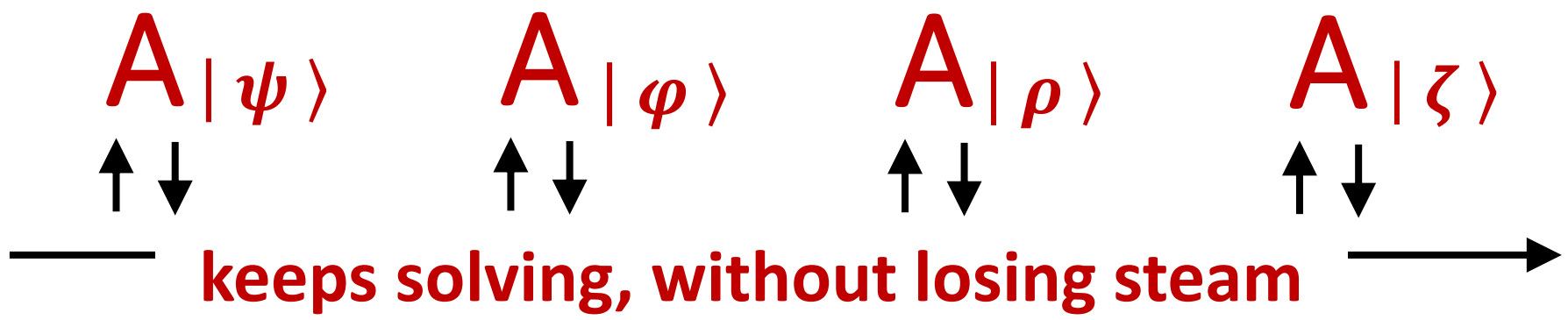
[BBK22] **inherent**

Persistent

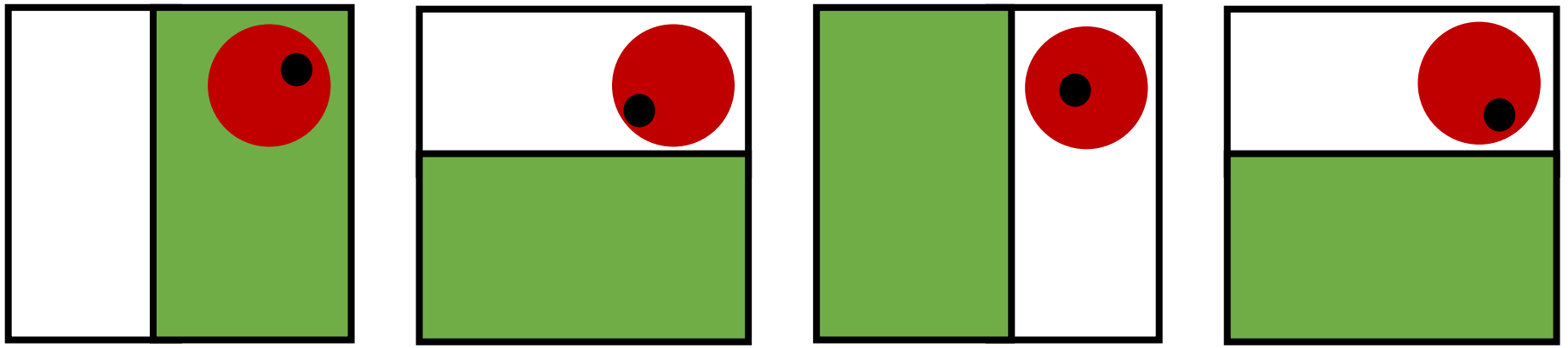


Isn’t Persistent Enough?

Persistent

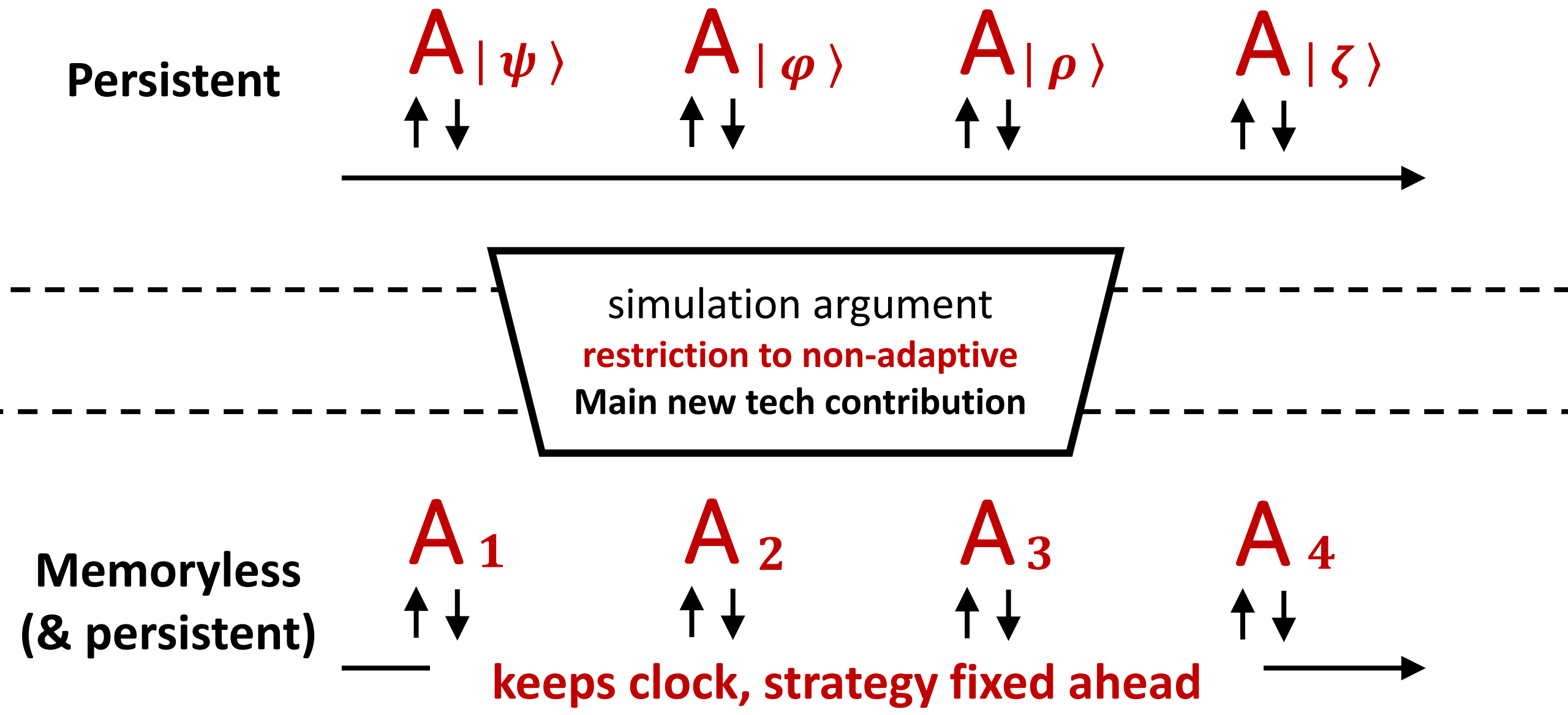


Solvable set drifts



reduction queries may be correlated (e.g., Goldreich-Levin)

Bridge 2: Persistent to Memoryless



Simulating Memoryless Behavior

Idea: **dazzle the adv with an abundance of dummy queries, sampled i.i.d. from the marginal distribution of the "real" queries**

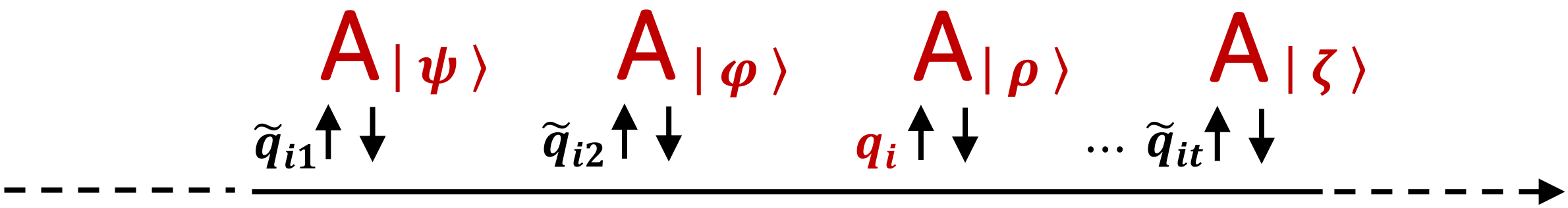
Observation: adv state **poly-bounded**, limited memory of past queries

We assume the reduction is non-adaptive so the marginal distribution is well defined

Simulating Memoryless Behavior

To make i-th query q_i:

$\tilde{q}_{i1}, \ldots, \tilde{q}_{it} \leftarrow Q_i$ marginal of i-th query
plant "real" q_i in random location

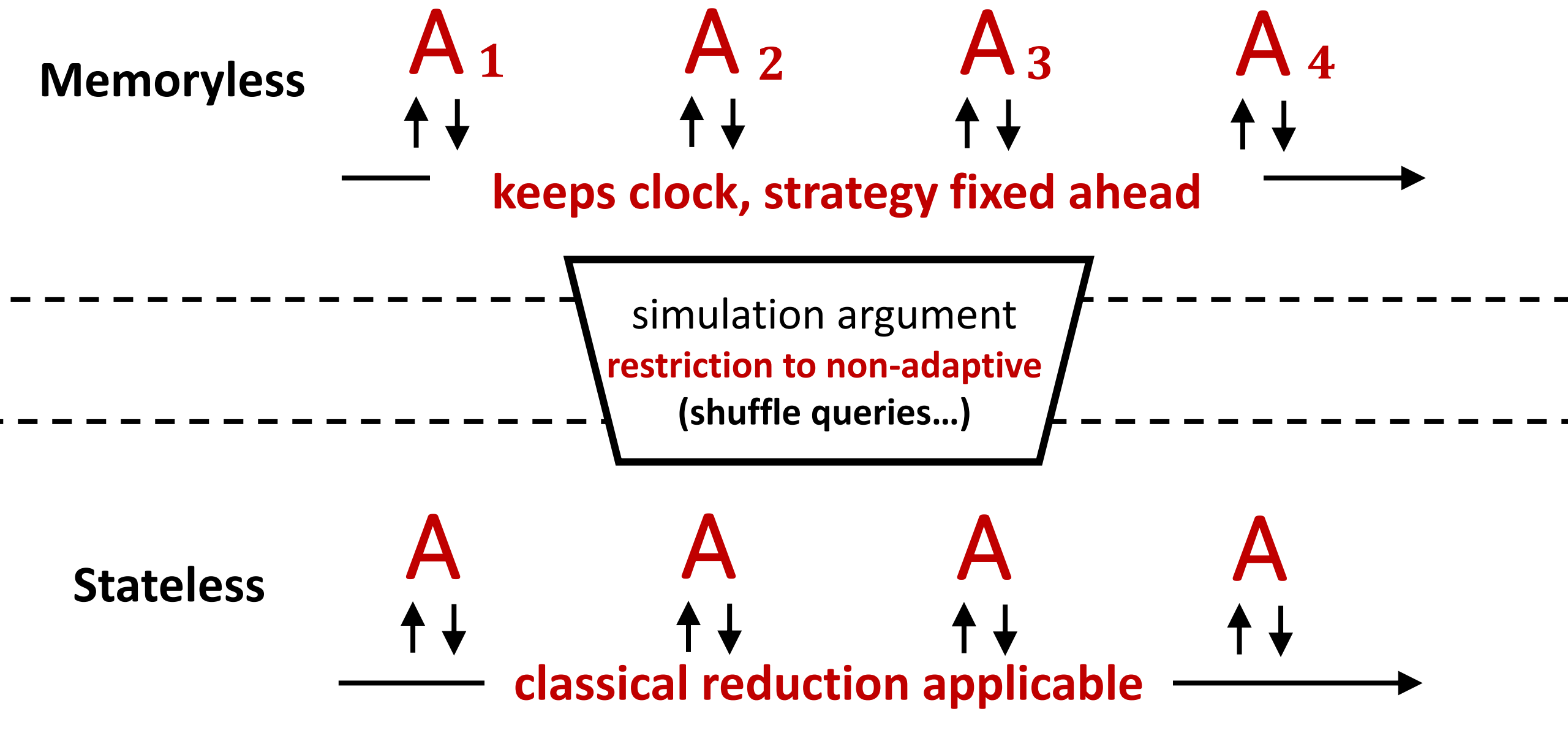


#state-qubits

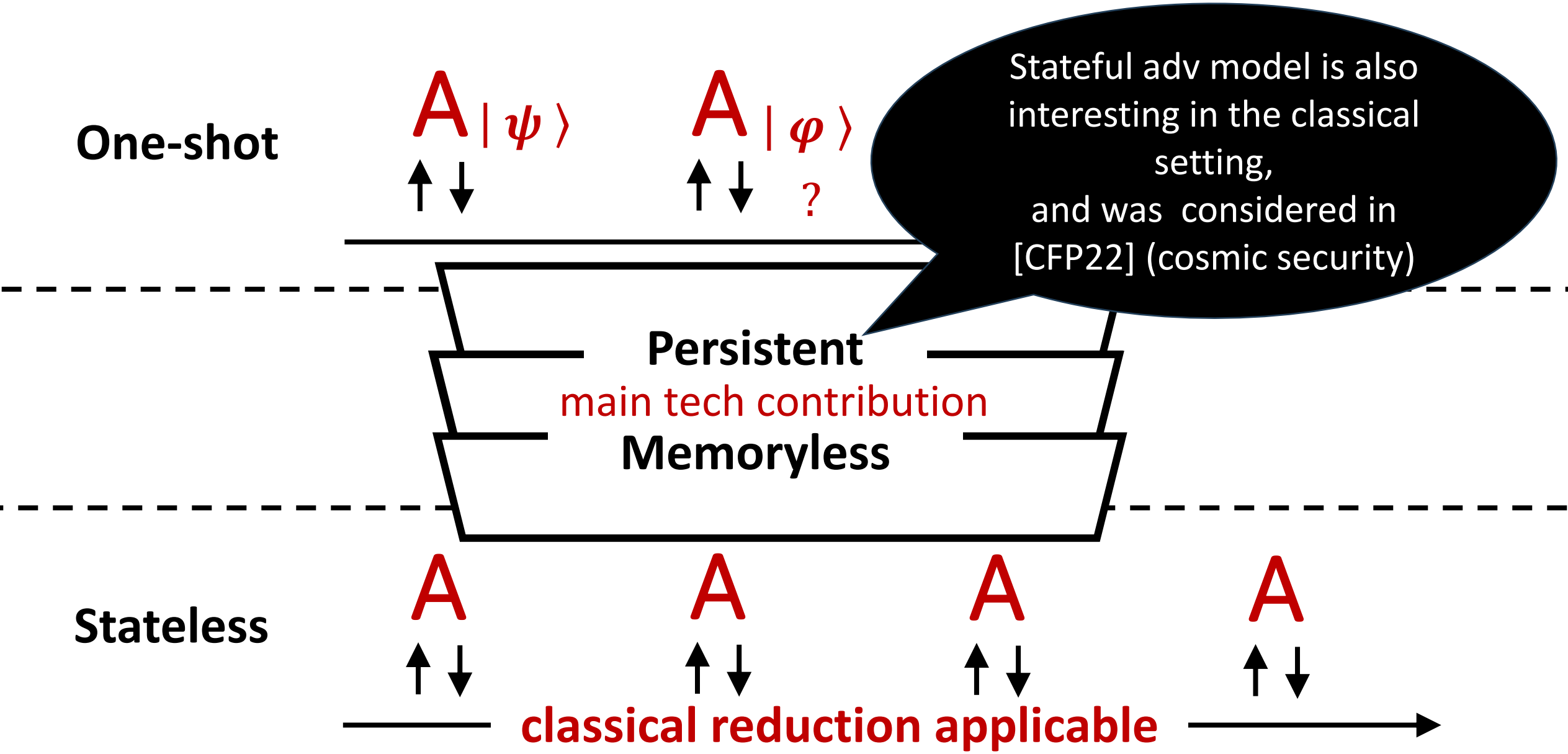
δ-close to execution with queries $\tilde{q}_{i1}, \ldots, \tilde{q}_{it} \leftarrow Q_i$ for $t \approx \frac{\ell}{\delta^2}$

(quantum mutual information argument)

Bridge 3: Memoryless to Stateless



Bridge Between Stateful and Stateless Adversaries



A Counterexample for Search Assumptions

Non-interactive problems P,Q with classical reduction, but no constructive post-quantum reduction

P: Given vk for digital signature scheme, and a random message m, output sig which is a valid signature for m.

Q: Given vk for digital signature scheme, and random messages (m_1, m_2), output (sig_1, sig_2) which are valid signature for (m_1, m_2).

Classically: P-Solver ⇒ Q-Solver

Quantumly: *tokenized signature schemes* [BS18,CLLZ21] allow to generate a quantum state that can be used to generate exactly one valid signature.

Food for Thought

What about adaptive reductions?
(PRGs from OWFs [HILL])

Thanks!