Efficient Simulation of Random States and Random Unitaries

Gorjan Alagic, **Christian Majenz** and Alexander Russell

QCrypt 2020, in Cyberspace

Joint Center for Quantum Information and Computer Science

QuSoft Research Center for Quantum Software

UCONN

Results — overview

- We study the **simulation of random quantum objects**, i.e. random quantum states and random unitary operations
- We develop a **theory of** their **stateful simulation**, a quantum analogue of “lazy sampling”
- For random states, we develop an efficient protocol for stateful simulation
- For random unitaries, we show that simulation can be done in polynomial space
- As an **application**, we design a **quantum money** scheme that is unconditionally unforgeable and untraceable.

Introduction

Randomness…

…is extremely useful. Applications:

- All of cryptography
- Monte Carlo simulation
- Randomized algorithms
- …

Easy example: random string

Random element $x \in_R \{0,1\}^n$

Easy example: random string

Random element $x \in_R \{0,1\}^n$

	Randomness cost	Runtime limit distinguisher
Exact	n	No

Easy example: random string

Random element $x \in_R \{0,1\}^n$

	Randomness cost	Runtime limit distinguisher
Exact	n	No
Pseudorandom generator	$\text{poly}(\lambda)$	$\text{poly}(\lambda)$

Another example: random function

Function $f : \{0,1\}^m \rightarrow \{0,1\}^n$ such that $f(x) \in_R \{0,1\}^n$ independently

Another example: random function

Function $f : \{0,1\}^m \rightarrow \{0,1\}^n$ such that $f(x) \in_R \{0,1\}^n$ independently

Oracle simulation for f	Randomness cost	Stateful simulation	Limit distinguisher
Exact	$n \cdot 2^m$	No	None

Another example: random function

Function $f : \{0,1\}^m \rightarrow \{0,1\}^n$ such that $f(x) \in_R \{0,1\}^n$ independently

$\leq$ runtime, memory

Oracle simulation for f	Randomness cost	Stateful simulation	Limit distinguisher
Exact	$n \cdot 2^m$	No	None

Another example: random function

Function $f : \{0,1\}^m \to \{0,1\}^n$ such that $f(x) \in_R \{0,1\}^n$ independently

Oracle simulation for f	Randomness cost	Stateful simulation	Limit distinguisher
Exact	$n \cdot 2^m$ ☠	No	None
t-wise independent function	$O(t \cdot n)$	No	$q \leq t$

# of queries

Another example: random function

Function $f : \{0,1\}^m \to \{0,1\}^n$ such that $f(x) \in_R \{0,1\}^n$ independently

Oracle simulation for f	Randomness cost	Stateful simulation	Limit distinguisher
Exact	$n \cdot 2^m$	No	None
t-wise independent function	$O(t \cdot n)$	No	$q \leq t$
Pseudorandom function	$\text{poly}(\lambda)$	No	$time \leq \text{poly}(\lambda)$

Another example: random function

Function $f : \{0,1\}^m \to \{0,1\}^n$ such that $f(x) \in_R \{0,1\}^n$ independently

Oracle simulation for f	Randomness cost	Stateful simulation	Limit distinguisher
Exact	$n \cdot 2^m$	No	None
t-wise independent function	$O(t \cdot n)$	No	$q \leq t$
Pseudorandom function	$\mathrm{poly}(\lambda)$	No	$time \leq \mathrm{poly}(\lambda)$
"Lazy sampling"	$q \cdot n$	Yes	None

Another example: random function

Function $f : \{0,1\}^m \to \{0,1\}^n$ such that $f(x) \in_R \{0,1\}^n$ independently

Oracle simulation for f	Randomness cost	Stateful simulation	Limit distinguisher
Exact	$n \cdot 2^m$	No	None
t-wise independent function	Information-theoretically secure message authentication		
Pseudorandom function	$\text{poly}(\lambda)$	No	$time \leq \text{poly}(\lambda)$
"Lazy sampling"	$q \cdot n$	Yes	None

Another example: random function

Function $f : \{0,1\}^m \to \{0,1\}^n$ such that $f(x) \in_R \{0,1\}^n$ independently

Oracle simulation for f	Randomness cost	Stateful simulation	Limit distinguisher
Exact	$n \cdot 2^m$	No	None
t-wise independent function	Information-theoretically secure message authentication		
Pseudorandom function	Computationally secure symmetric-key crypto		
"Lazy sampling"	$q \cdot n$	Yes	None

Another example: random function

Function $f : \{0,1\}^m \rightarrow \{0,1\}^n$ such that $f(x) \in_R \{0,1\}^n$ independently

Oracle simulation for f	Randomness cost	Stateful simulation	Limit distinguisher
Exact	$n \cdot 2^m$	No	None
t-wise independent function	Information-theoretically secure message authentication		
Pseudorandom function	Computationally secure symmetric-key crypto		
"Lazy sampling"	Random oracle model security (e.g. indifferentiability)		

Quantum states and operations

Quantum states and operations

Quantum state: unit vector

$|\phi\rangle \in \mathbb{S} \subset \mathbb{C}^{2^n}$

Sphere

Quantum states and operations

Quantum state: unit vector

$|\phi\rangle \in \mathbb{S} \subset \mathbb{C}^{2^n}$

~~Sphere~~

Strictly speaking:

$|\phi\rangle \in \mathrm{P}_{2^n-1}(\mathbb{C})$,

projective space

Quantum states and operations

Quantum state: unit vector
$|\phi\rangle \in \mathrm{S} \subset \mathbb{C}^{2^n}$

~~Sphere~~

Strictly speaking:
$|\phi\rangle \in \mathrm{P}_{2^n-1}(\mathbb{C})$,
projective space

Quantum operation: unitary
matrix $U \in \mathrm{U}(2^n) \subset \mathbb{C}^{2^n \times 2^n}$

(Compact Lie-)group
of unitary
$2^n \times 2^n$-matrices

Quantum states and operations

Quantum state: unit vector
$|\phi\rangle \in \mathrm{S} \subset \mathbb{C}^{2^n}$

~~Sphere~~

Strictly speaking:
$|\phi\rangle \in \mathrm{P}_{2^n-1}(\mathbb{C})$,
projective space

Quantum operation: unitary
matrix $U \in \mathrm{U}(2^n) \subset \mathbb{C}^{2^n \times 2^n}$

(Compact Lie-)group
of unitary
$2^n \times 2^n$-matrices

Really nice mathematical objects with a
natural notion of a uniform distribution!

Quantum states and operations

Quantum state: unit vector $|\phi\rangle \in \mathrm{S} \subset \mathbb{C}^{2^n}$

~~Sphere~~

Strictly speaking: $|\phi\rangle \in \mathrm{P}_{2^n-1}(\mathbb{C})$, projective space

Quantum operation: unitary matrix $U \in \mathrm{U}(2^n) \subset \mathbb{C}^{2^n \times 2^n}$

(Compact Lie-)group of unitary $2^n \times 2^n$-matrices

Really nice mathematical objects with a natural notion of a uniform distribution!

Haar measure

Example application: Haar money

No-cloning principle: quantum information cannot be copied.

Example application: Haar money

No-cloning principle: quantum information cannot be copied.

Oldest idea in quantum crypto: Let's make money out of it!

Example application: Haar money

No-cloning principle: quantum information cannot be copied.

Oldest idea in quantum crypto: Let's make money out of it!

Haar money (JLS '19):

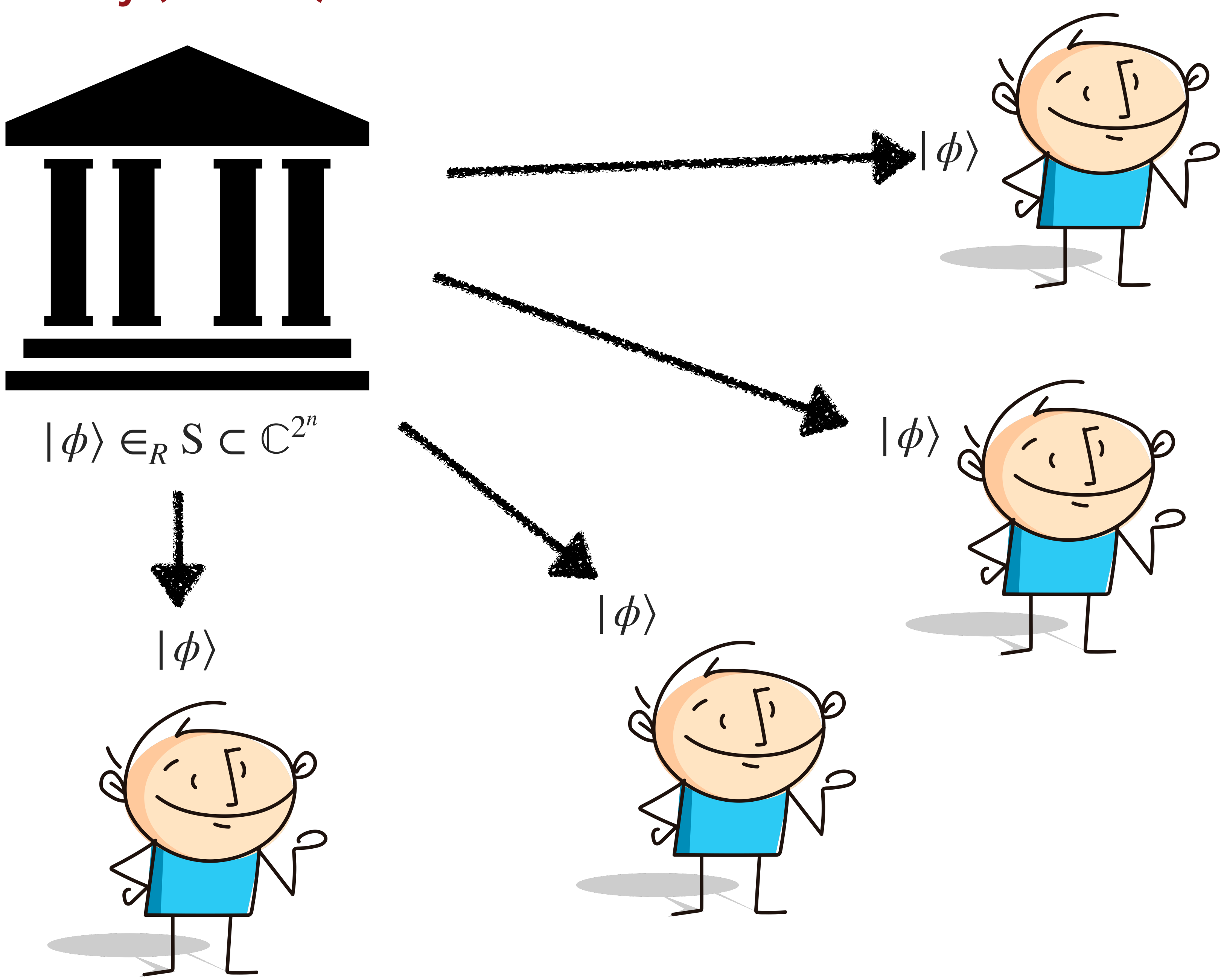
$|\phi\rangle \in_R S \subset \mathbb{C}^{2^n}$

Example application: Haar money

No-cloning principle: quantum information cannot be copied.

Oldest idea in quantum crypto: Let's make money out of it!

Haar money (JLS '19):

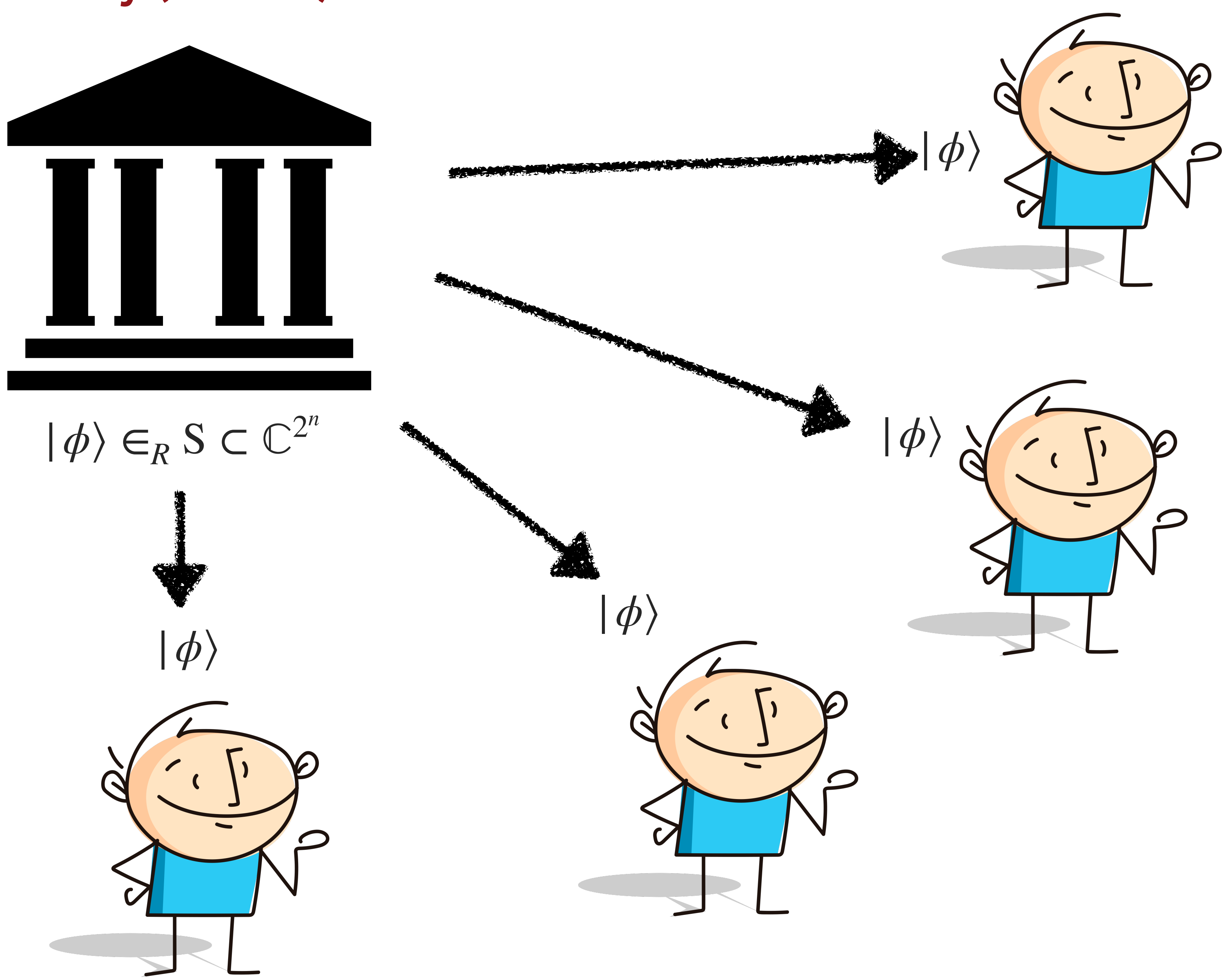


Example application: Haar money

No-cloning principle: quantum information cannot be copied.

Oldest idea in quantum crypto: Let's make money out of it!

Haar money (JLS '19):



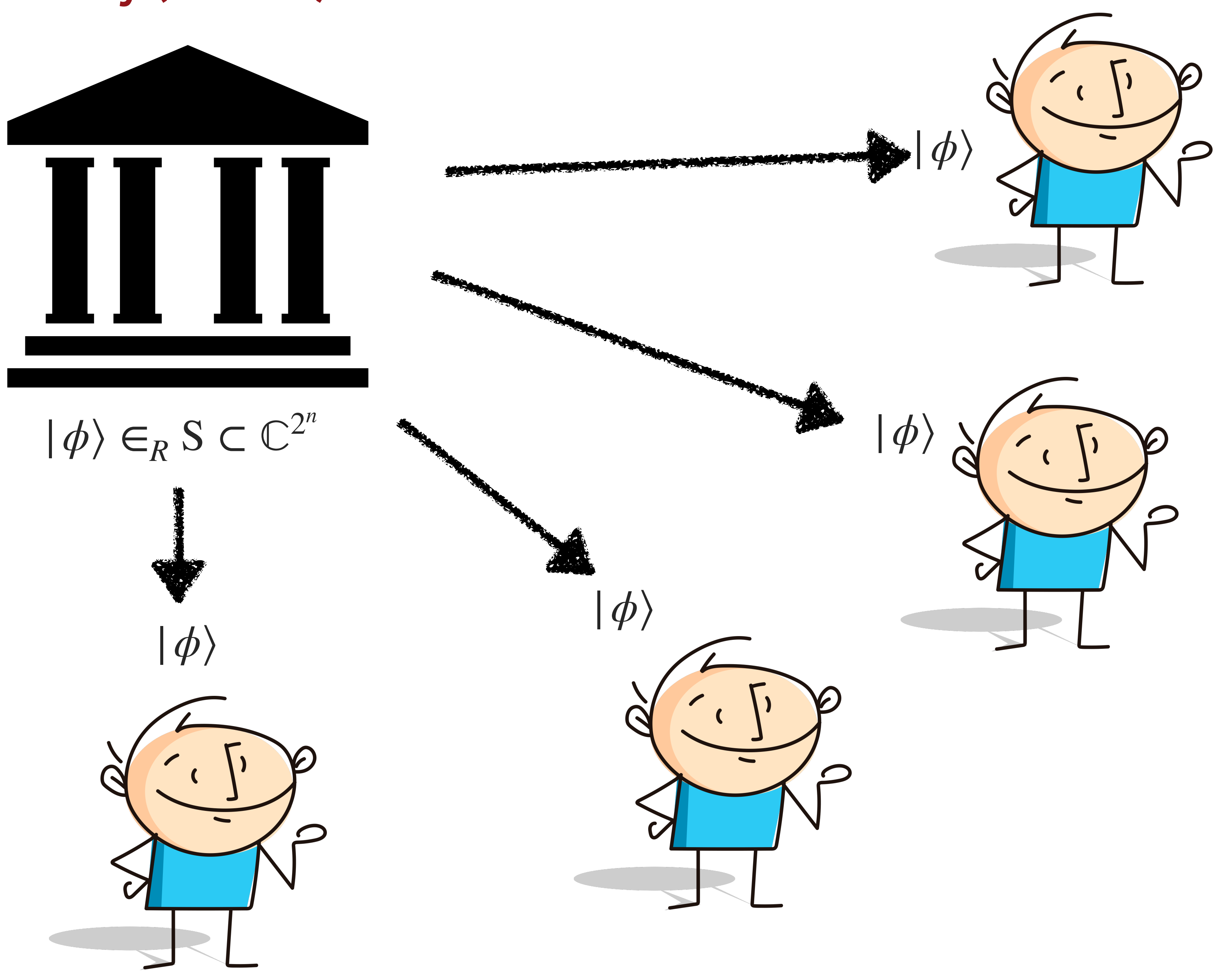
Unforgeable ✓

Example application: Haar money

No-cloning principle: quantum information cannot be copied.

Oldest idea in quantum crypto: Let's make money out of it!

Haar money (JLS '19):



Unforgeable ✓

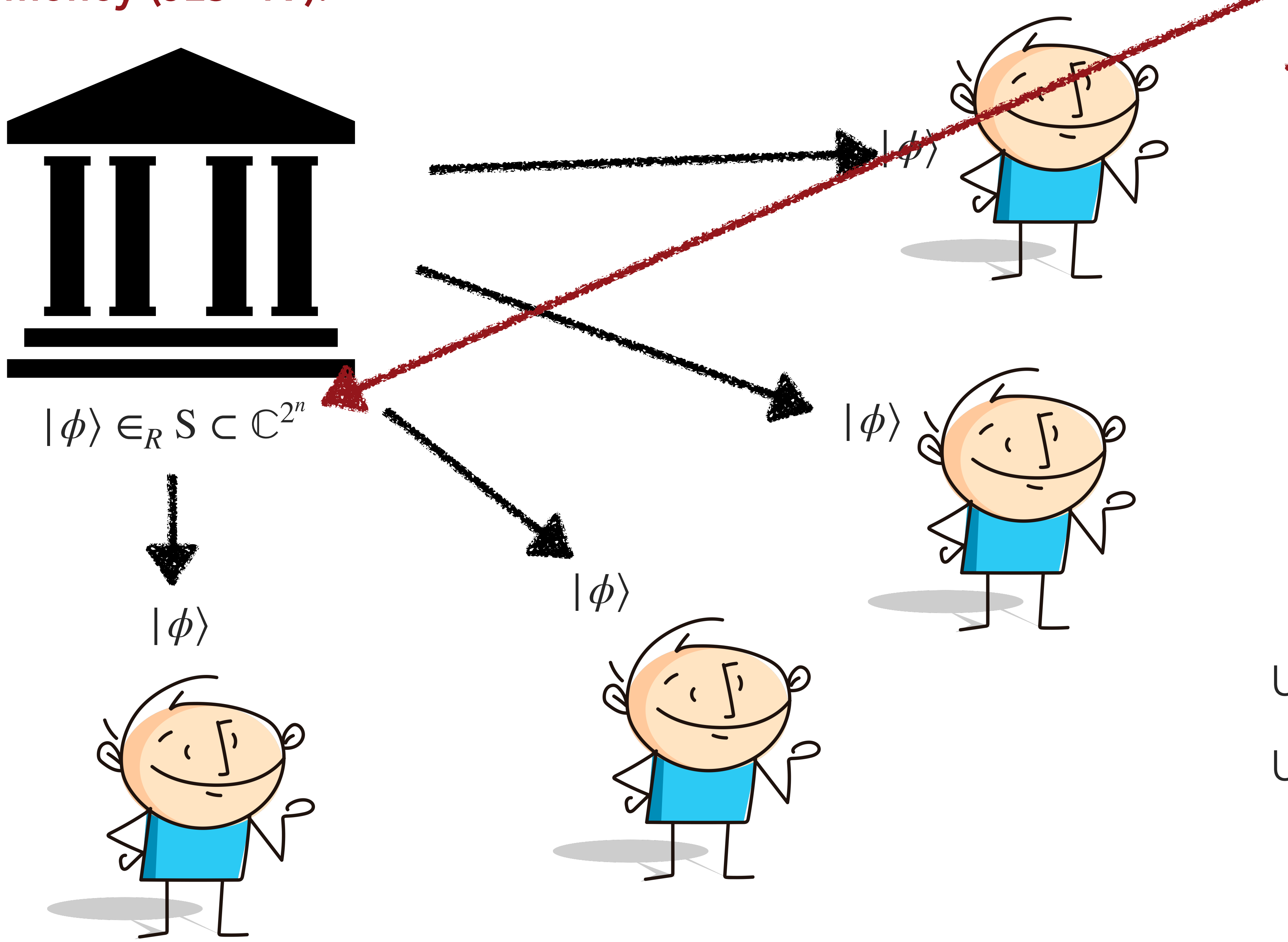
Untraceable ✓

Example application: Haar money

No-cloning principle: quantum information cannot be copied.

Oldest idea in quantum crypto: Let's make money out of it!

Haar money (JLS '19):



Can the Bank sample such a random state?

Unforgeable ✓

Untraceable ✓

Simulation of random quantum objects

Can we sample a random quantum state?

Haar-random state $|\phi\rangle \in S \subset \mathbb{C}^{2^n}$.

Can we sample a random quantum state?

Haar-random state $|\phi\rangle \in S \subset \mathbb{C}^{2^n}$.

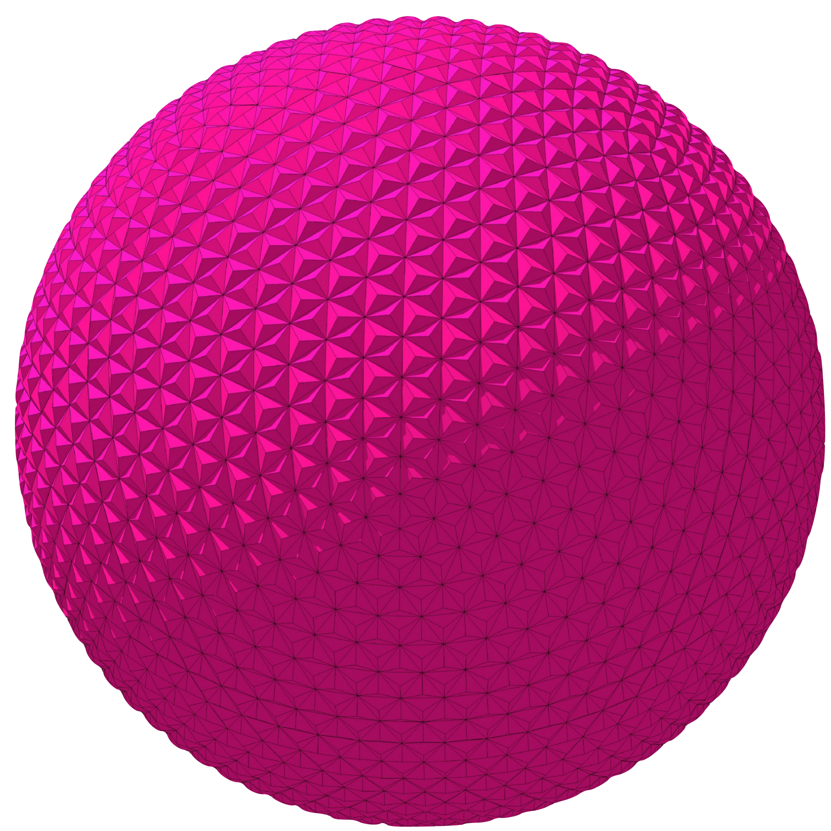
Oracle simulation for $1 \mapsto	\phi\rangle$	Randomness/ Memory cost	Simulation	Limit distinguisher
Exact	∞	inefficient, stateless	None

Can we sample a random quantum state?

Haar-random state $|\phi\rangle \in S \subset \mathbb{C}^{2^n}$.

Oracle simulation for $1 \mapsto	\phi\rangle$	Randomness/ Memory cost	Simulation	Limit distinguisher
Exact	∞	inefficient, stateless	None
ε -Net	$O(\log(1/\varepsilon) \cdot 2^n)$	inefficient, stateless	$q \leq O(1/\varepsilon)$

# of queries



Can we sample a random quantum state?

Haar-random state $|\phi\rangle \in S \subset \mathbb{C}^{2^n}$.

Oracle simulation for $1 \mapsto	\phi\rangle$	Randomness/ Memory cost	Simulation	Limit distinguisher
Exact	∞	inefficient, stateless	None
ε -Net	$O(\log(1/\varepsilon) \cdot 2^n)$	inefficient, stateless	$q \leq O(1/\varepsilon)$
State t-design	$\mathrm{poly}(n, t)$	efficient, stateless	$q \leq t$

Can we sample a random quantum state?

Haar-random state $|\phi\rangle \in S \subset \mathbb{C}^{2^n}$.

Oracle simulation for $1 \mapsto	\phi\rangle$	Randomness/ Memory cost	Simulation	Limit distinguisher
Exact	∞	inefficient, stateless	None
ε -Net	$O(\log(1/\varepsilon) \cdot 2^n)$	inefficient, stateless	$q \leq O(1/\varepsilon)$
State t-design	$\mathrm{poly}(n, t)$	efficient, stateless	$q \leq t$
Pseudorandom quantum state (JLS '19, BS '20)	$\mathrm{poly}(\lambda)$	efficient, stateless	$time \leq \mathrm{poly}(\lambda)$

Can we sample a random quantum state?

Haar-random state $|\phi\rangle \in S \subset \mathbb{C}^{2^n}$.

Oracle simulation for $1 \mapsto	\phi\rangle$	Randomness/ Memory cost	Simulation	Limit distinguisher
Exact	∞	inefficient, stateless	None
ε -Net	$O(\log(1/\varepsilon) \cdot 2^n)$	inefficient, stateless	$q \leq O(1/\varepsilon)$
State t-design	$\mathrm{poly}(n, t)$	efficient, stateless	$q \leq t$
Pseudorandom quantum state (JLS '19, BS '20)	$\mathrm{poly}(\lambda)$	efficient, stateless	$time \leq \mathrm{poly}(\lambda)$
This work: quantum state "lazy sampling"	$\mathrm{poly}(q, n)$	efficient, stateful	None

Can we simulate a random unitary?

Haar-random unitary $U \in \mathrm{U}(2^n)$

Can we simulate a random unitary?

Haar-random unitary $U \in \mathrm{U}(2^n)$

Oracle simulation for U	Randomness/ Memory cost	Simulation	Limit distinguisher
Exact	∞	inefficient, stateless	None
ε-Net	$O(\log(1/\varepsilon) \cdot 2^{2n})$	inefficient, stateless	$q \leq O(1/\varepsilon)$

Can we simulate a random unitary?

Haar-random unitary $U \in \mathrm{U}(2^n)$

Oracle simulation for U	Randomness/ Memory cost	Simulation	Limit distinguisher
Exact	∞	inefficient, stateless	None
ε-Net	$O(\log(1/\varepsilon) \cdot 2^{2n})$	inefficient, stateless	$q \leq O(1/\varepsilon)$
Unitary t-design	$\mathrm{poly}(n, t)$	efficient, stateless	$q \leq t$

Can we simulate a random unitary?

Haar-random unitary $U \in \mathrm{U}(2^n)$

Oracle simulation for U	Randomness/ Memory cost	Simulation	Limit distinguisher
Exact	∞	inefficient, stateless	None
ε-Net	$O(\log(1/\varepsilon) \cdot 2^{2n})$	inefficient, stateless	$q \leq O(1/\varepsilon)$
Unitary t-design	$\mathrm{poly}(n, t)$	efficient, stateless	$q \leq t$
Pseudorandom unitary??? (JLS '19)	$\mathrm{poly}(\lambda)$	efficient, stateless	$time \leq \mathrm{poly}(\lambda)$

Can we simulate a random unitary?

Haar-random unitary $U \in \mathrm{U}(2^n)$

Oracle simulation for U	Randomness/ Memory cost	Simulation	Limit distinguisher
Exact	∞	inefficient, stateless	None
ε-Net	$O(\log(1/\varepsilon) \cdot 2^{2n})$	inefficient, stateless	$q \leq O(1/\varepsilon)$
Unitary t-design	$\mathrm{poly}(n, t)$	efficient, stateless	$q \leq t$
Pseudorandom unitary??? (JLS '19)	$\mathrm{poly}(\lambda)$	efficient, stateless	$time \leq \mathrm{poly}(\lambda)$
This work	$\mathrm{poly}(q, n)$	**space**-efficient, stateful	None

Example application: Haar money

No-cloning principle: quantum information cannot be copied.

Oldest idea in quantum crypto: Let's make money out of it!

Haar money (JLS '19):

$|\phi\rangle \in_R S \subset \mathbb{C}^{2^n}$

Unforgeable ✓

Untraceable ✓

Can the Bank sample such a random state?

Example application: Haar money

No-cloning principle: quantum information cannot be copied.

Oldest idea in quantum crypto: Let's make money out of it!

Haar money (JLS '19):

$|\phi\rangle \in_R S \subset \mathbb{C}^{2^n}$

Unforgeable ✓

Untraceable ✓

Can the Bank sample such a random state?

No, but they can *simulate* it!

Example application: Haar money

No-cloning principle: quantum information cannot be copied.

Oldest idea in quantum crypto: Let's make money out of it!

Can the Bank sample such a random state?

Haar money (JLS '19):

Unforgeable ✓

Untraceable ✓

$|\phi\rangle \in_R S \subset \mathbb{C}^{2^n}$

No, but they can *simulate* it!

Two options:

- Use pseudorandom quantum state, computationally secure untraceable quantum money (JLS '19)

Example application: Haar money

No-cloning principle: quantum information cannot be copied.

Oldest idea in quantum crypto: Let's make money out of it!

Can the Bank sample such a random state?

Haar money (JLS '19):

Unforgeable ✓

Untraceable ✓

$|\phi\rangle \in_R S \subset \mathbb{C}^{2^n}$

No, but they can *simulate* it!

Two options:

- Use pseudorandom quantum state, computationally secure untraceable quantum money (JLS '19)
- **Use stateful simulation, unconditionally secure untraceable quantum money (AMR)**

Limitations of stateless simulation

Stateless simulation scheme $\Leftrightarrow \{|\phi_k\rangle\}_{k\in K}$, pick $k \in_R K$, output copies of $|\phi_k\rangle$

Limitations of stateless simulation

Stateless simulation scheme $\Leftrightarrow \{ |\phi_k\rangle \}_{k \in K}$, pick $k \in_R K$, output copies of $|\phi_k\rangle$

Problem:

$|\phi\rangle \neq |\psi\rangle$ quantum states $\Rightarrow |\phi\rangle^{\otimes n}, |\psi\rangle^{\otimes n}$ can be distinguished with probability $p(n) \to 1 \; (n \to \infty)$

Limitations of stateless simulation

Stateless simulation scheme $\Leftrightarrow \{|\phi_k\rangle\}_{k\in K}$, pick $k \in_R K$, output copies of $|\phi_k\rangle$

Problem:

$|\phi\rangle \neq |\psi\rangle$ quantum states $\Rightarrow |\phi\rangle^{\otimes n}, |\psi\rangle^{\otimes n}$ can be distinguished with probability $p(n) \to 1 \ (n \to \infty)$

Also works for random states sampled according to different measures.

Limitations of stateless simulation

Stateless simulation scheme $\Leftrightarrow \{|\phi_k\rangle\}_{k\in K}$, pick $k \in_R K$, output copies of $|\phi_k\rangle$

Problem:

$|\phi\rangle \neq |\psi\rangle$ quantum states $\Rightarrow |\phi\rangle^{\otimes n}, |\psi\rangle^{\otimes n}$ can be distinguished with probability $p(n) \to 1 \ (n \to \infty)$

Also works for random states sampled according to different measures.

Statelessness implies query limit!

Limitations of stateless simulation

Stateless simulation scheme $\Leftrightarrow \{|\phi_k\rangle\}_{k\in K}$, pick $k \in_R K$, output copies of $|\phi_k\rangle$

Problem:

$|\phi\rangle \neq |\psi\rangle$ quantum states $\Rightarrow |\phi\rangle^{\otimes n}, |\psi\rangle^{\otimes n}$ can be distinguished with probability $p(n) \to 1 \ (n \to \infty)$

Also works for random states sampled according to different measures.

Statelessness implies query limit!

Similar argument for unitaries.

Techniques

Going to both churches…

A random state and *part of an entangled state* look the same.

Going to both churches…

A random state and *part of an entangled state* look the same.

Going to both churches…

A random state and *part of an entangled state* look the same.

Going to both churches…

A random state and *part of an entangled state* look the same.

⇒ stateful oracle simulation without any randomness, just by maintaining entanglement with the distinguisher!

Going to both churches…

A random state and *part of an entangled state* look the same.

⇒ stateful oracle simulation without any randomness, just by maintaining entanglement with the distinguisher!

What do ℓ copies of a Haar random state look like to the distingusher?

Going to both churches…

A random state and *part of an entangled state* look the same.

⇒ stateful oracle simulation without any randomness, just by maintaining entanglement with the distinguisher!

What do ℓ copies of a Haar random state look like to the distingusher?

From representation theory: $\mathbb{E}_{|\psi\rangle \sim \mathrm{Haar}}\left[|\psi\rangle\langle\psi|^{\otimes \ell} \right] = \tau_{\mathrm{Sym}^{\ell}\mathbb{C}^d}$

Stateful simulation algorithm

Fact: ℓ copies of a Haar random state look like a single Haar random state on the symmetric subspace $\mathrm{Sym}_{d,\ell}$ of $\mathbb{C}^d \otimes \mathbb{C}^d \otimes \ldots \otimes \mathbb{C}^d$ looks like half a maximally entangled state on $\mathrm{Sym}_{d,\ell} \otimes \mathrm{Sym}_{d,\ell}$

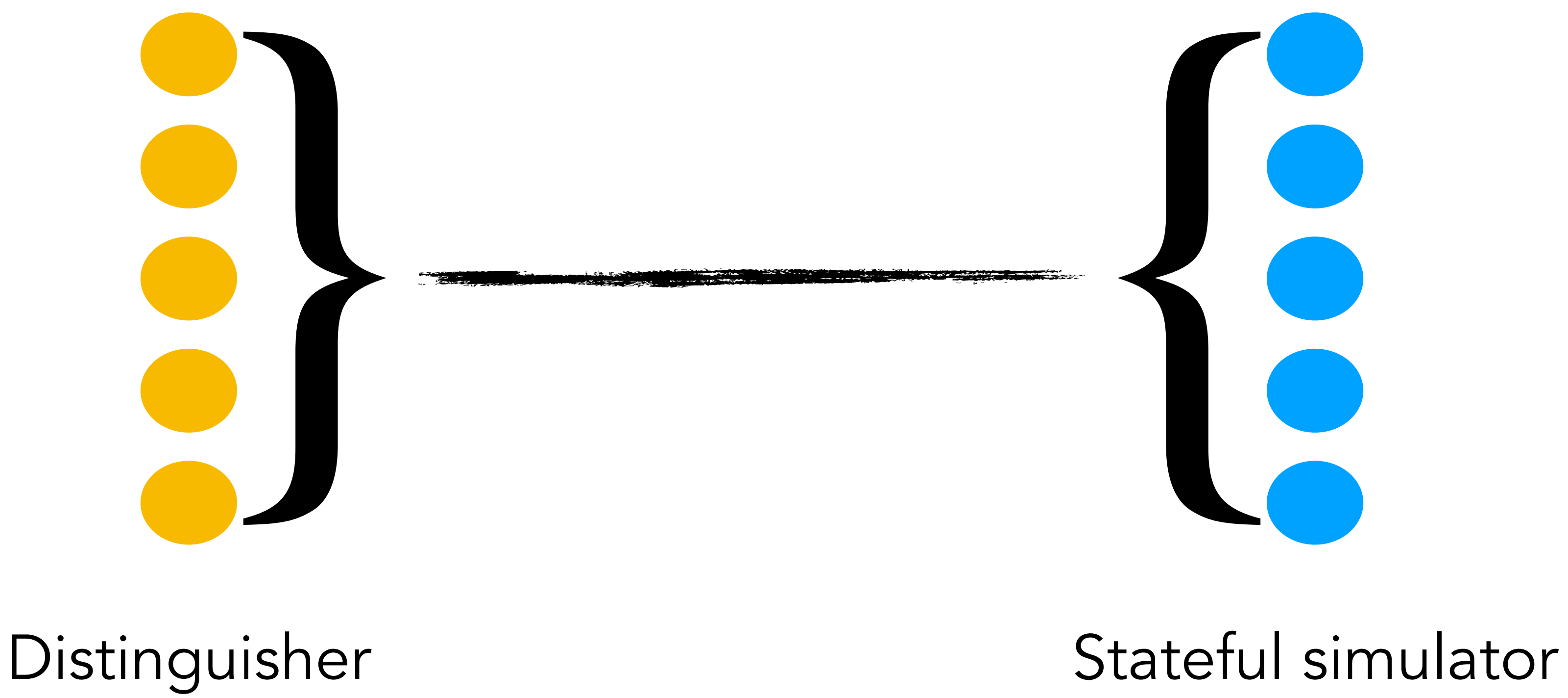
Stateful simulation algorithm

Fact: ℓ copies of a Haar random state look like a single Haar random state on the symmetric subspace $\mathrm{Sym}_{d,\ell}$ of $\mathbb{C}^d \otimes \mathbb{C}^d \otimes \ldots \otimes \mathbb{C}^d$ looks like half a maximally entangled state on $\mathrm{Sym}_{d,\ell} \otimes \mathrm{Sym}_{d,\ell}$

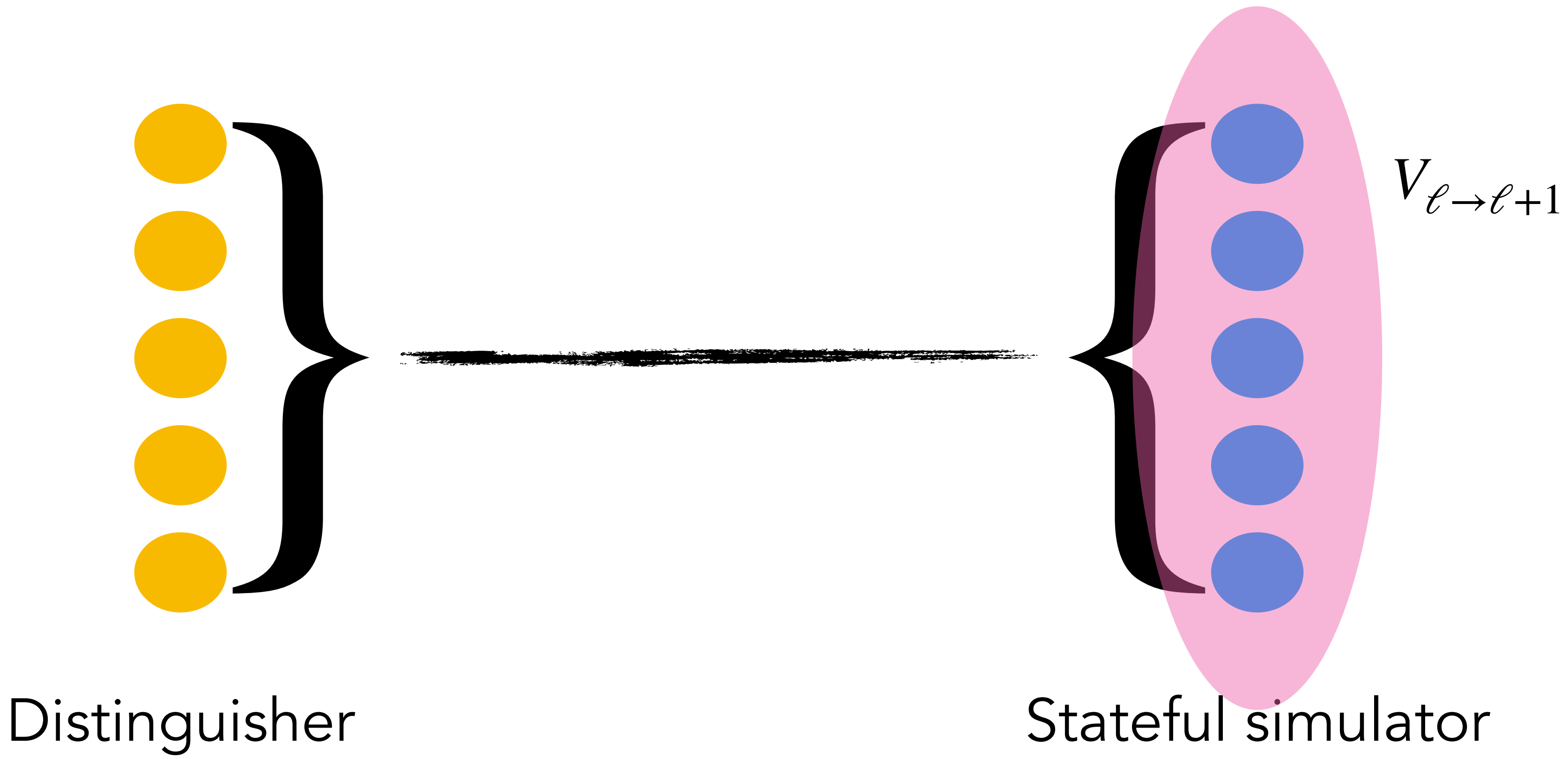
Strategy:

1. Maintain maximally entangled state of two copies of $\mathrm{Sym}_{d,\ell}$.
2. On query: extend it from ℓ to $\ell + 1$ by acting on one of the copies only.

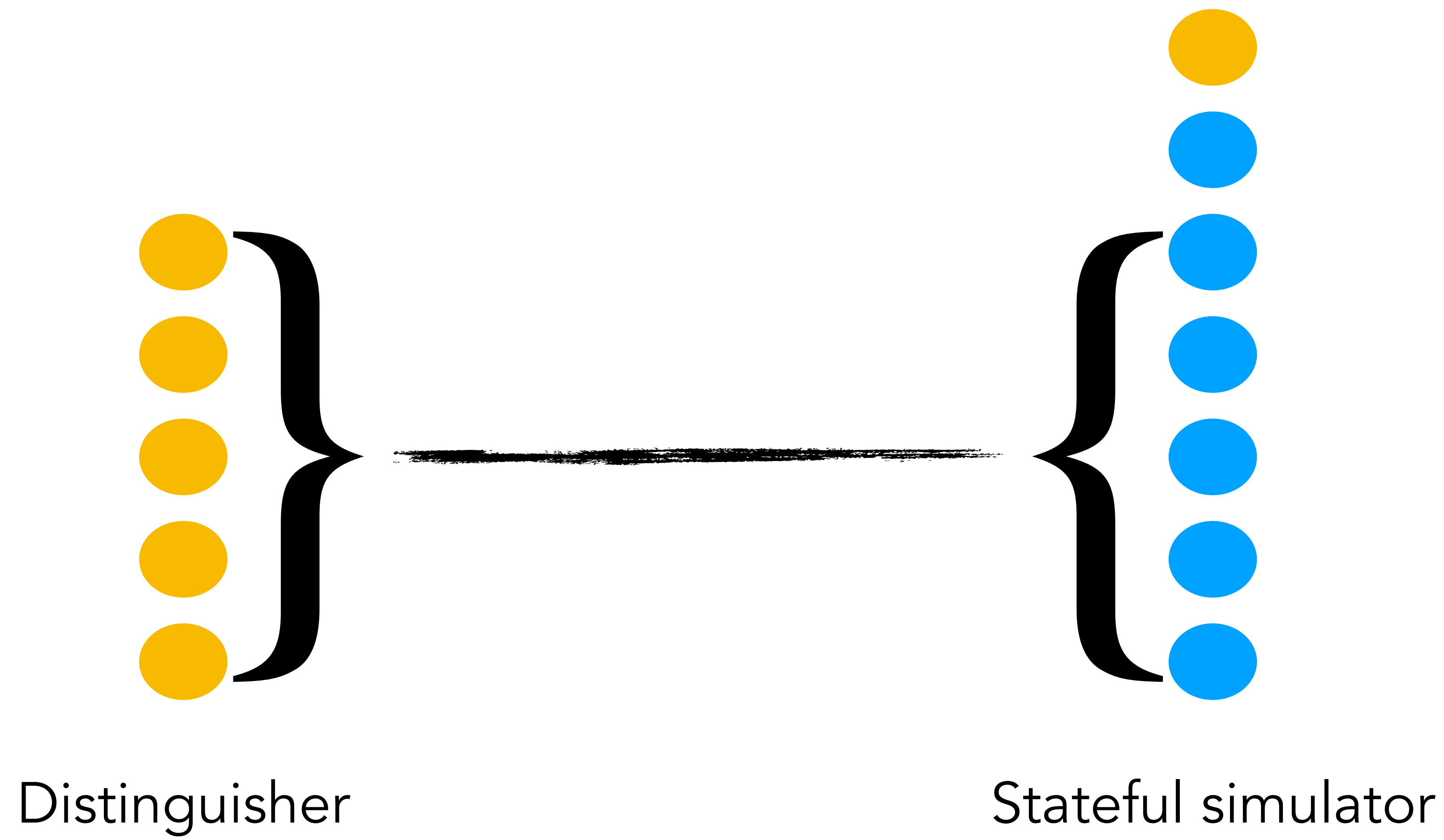
Stateful simulation algorithm



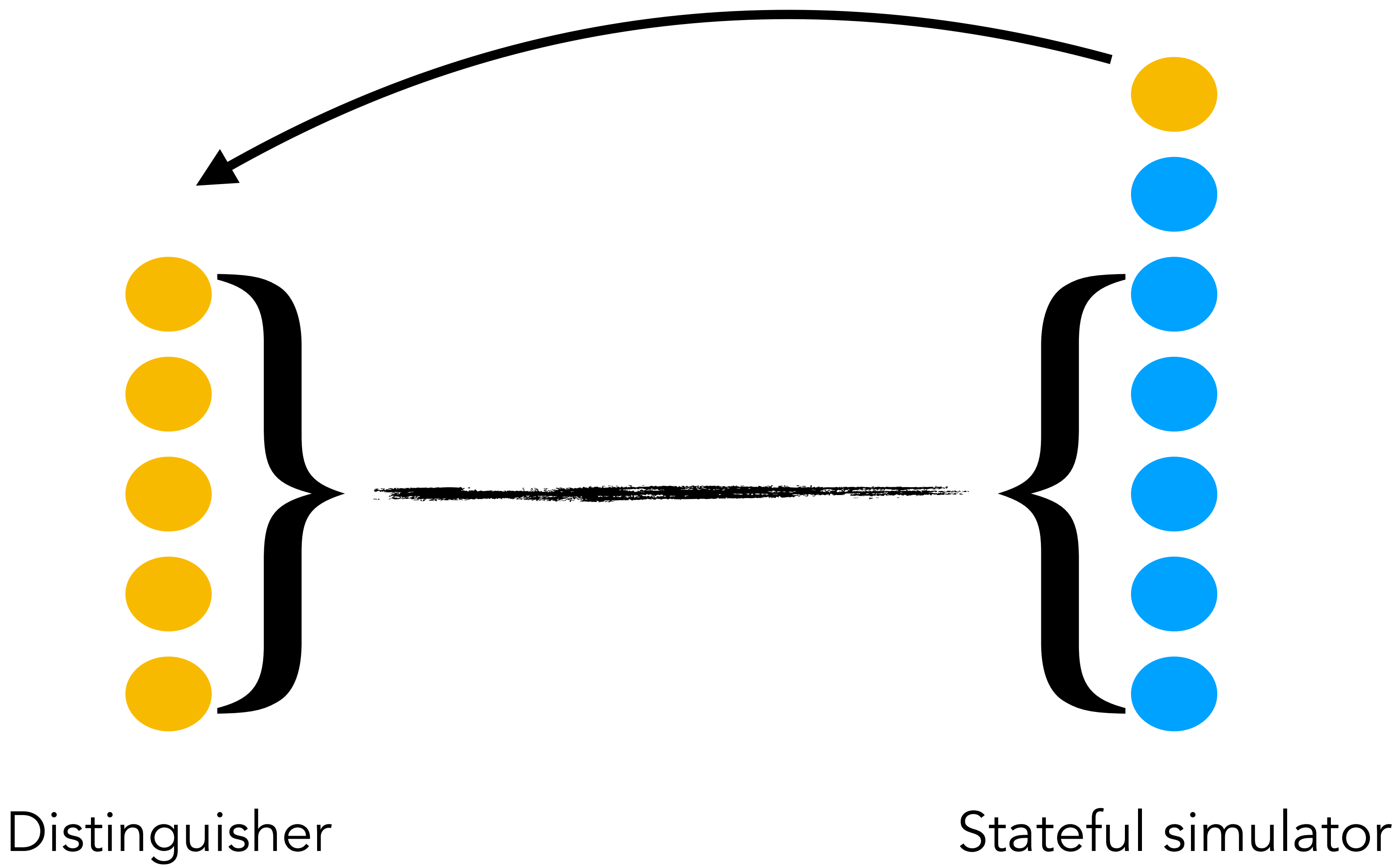
Stateful simulation algorithm



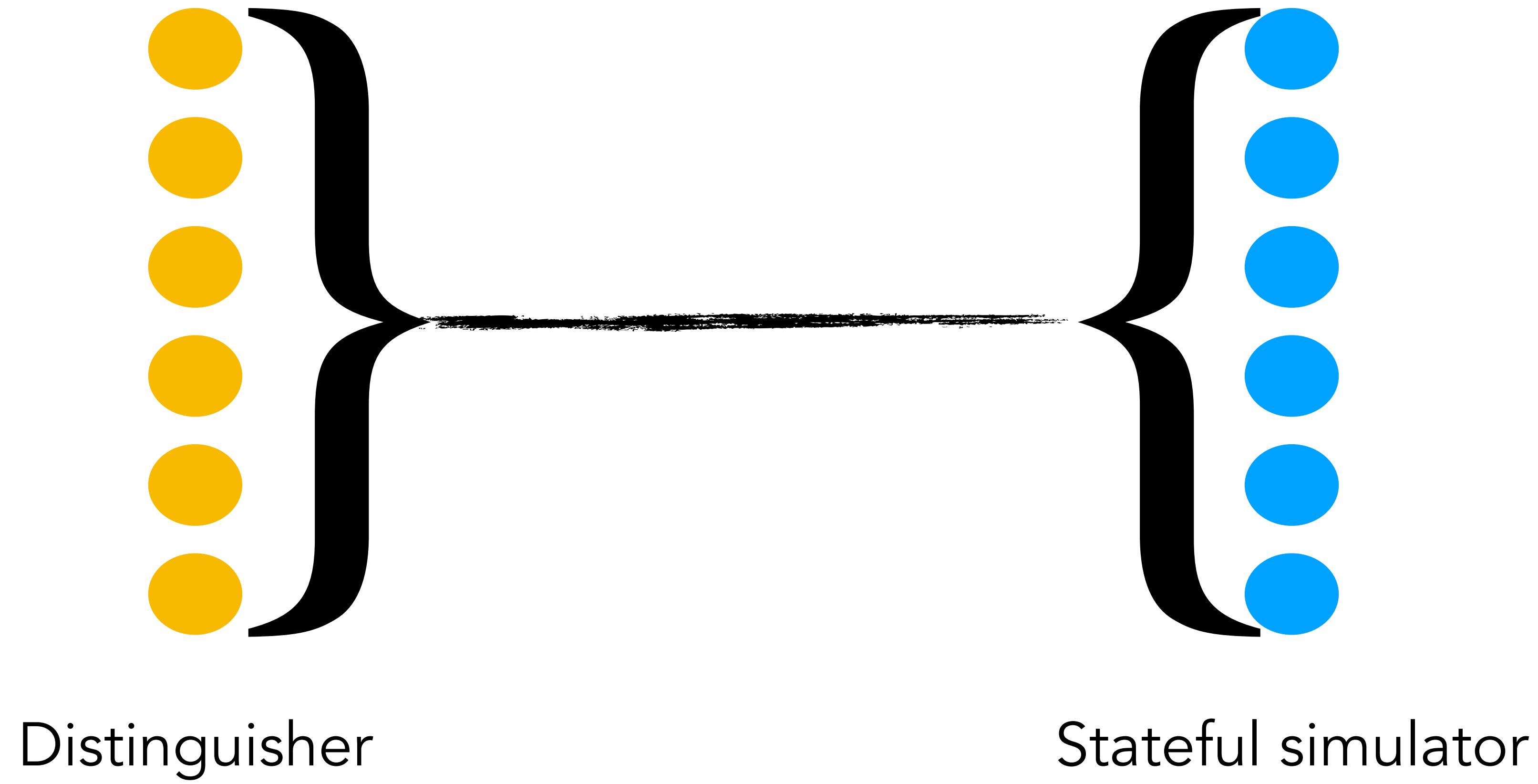
Stateful simulation algorithm



Stateful simulation algorithm



Stateful simulation algorithm



Technical contributions

Technical contributions

- Several new algorithmic tools for garbageless quantum state preparation

Technical contributions

- Several new algorithmic tools for garbageless quantum state preparation
- Concrete algorithms: approximate algorithms for the extension of maximally entangled states on symmetric subspaces by an additional copy

Technical contributions

- Several new algorithmic tools for garbageless quantum state preparation
- Concrete algorithms: approximate algorithms for the extension of maximally entangled states on symmetric subspaces by an additional copy
- Stateful simulation of random unitaries: combining several nice ingredients.

Technical contributions

- Several new algorithmic tools for garbageless quantum state preparation
- Concrete algorithms: approximate algorithms for the extension of maximally entangled states on symmetric subspaces by an additional copy
- Stateful simulation of random unitaries: combining several nice ingredients.
    - first (we think) quantum application of exact unitary designs (Kane '15)

Technical contributions

- Several new algorithmic tools for garbageless quantum state preparation
- Concrete algorithms: approximate algorithms for the extension of maximally entangled states on symmetric subspaces by an additional copy
- Stateful simulation of random unitaries: combining several nice ingredients.
  - first (we think) quantum application of exact unitary designs (Kane '15)
  - Exact adaptive-to-nonadaptive reduction using "postselection"

Technical contributions

- Several new algorithmic tools for garbageless quantum state preparation
- Concrete algorithms: approximate algorithms for the extension of maximally entangled states on symmetric subspaces by an additional copy
- Stateful simulation of random unitaries: combining several nice ingredients.
  - first (we think) quantum application of exact unitary designs (Kane '15)
  - Exact adaptive-to-nonadaptive reduction using "postselection"
  - Uniqueness property of the Stinespring dilation

Summary, open questions

Summary:

- We develop a theory of stateful simulation of random quantum primitives.
- Random quantum states can be approximately simulated efficiently using a stateful algorithm
- Random unitaries can be simulated exactly in a space-efficient way using a stateful algorithm.
- The random state simulator can be used to construct unconditionally secure untraceable quantum money.

Open questions:

- Can we simulate random unitaries efficiently?
- (From JLS '19) Construct pseudorandom unitaries!