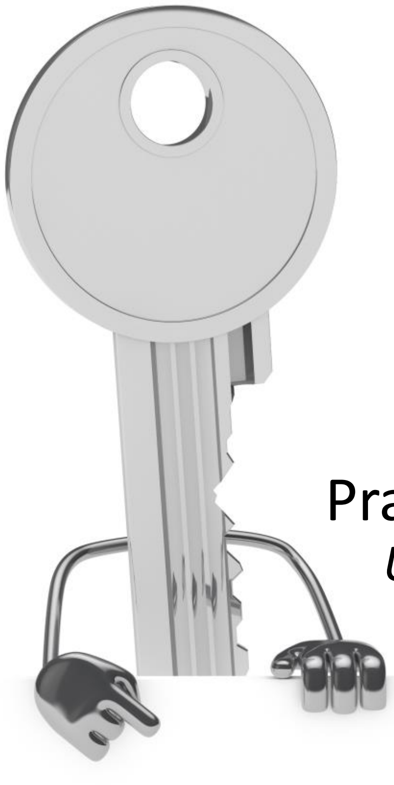
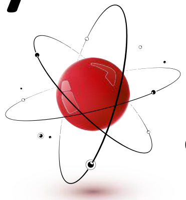
or wormholes!



Cryptography from Pseudorandom  States

Prabhanjan Ananth
UC Santa Barbara

Luowen Qian
Boston University

Henry Yuen
Columbia University

QCRYPT 2022
ia.cr/2021/1663

Is <insert your favorite cryptography> secure?

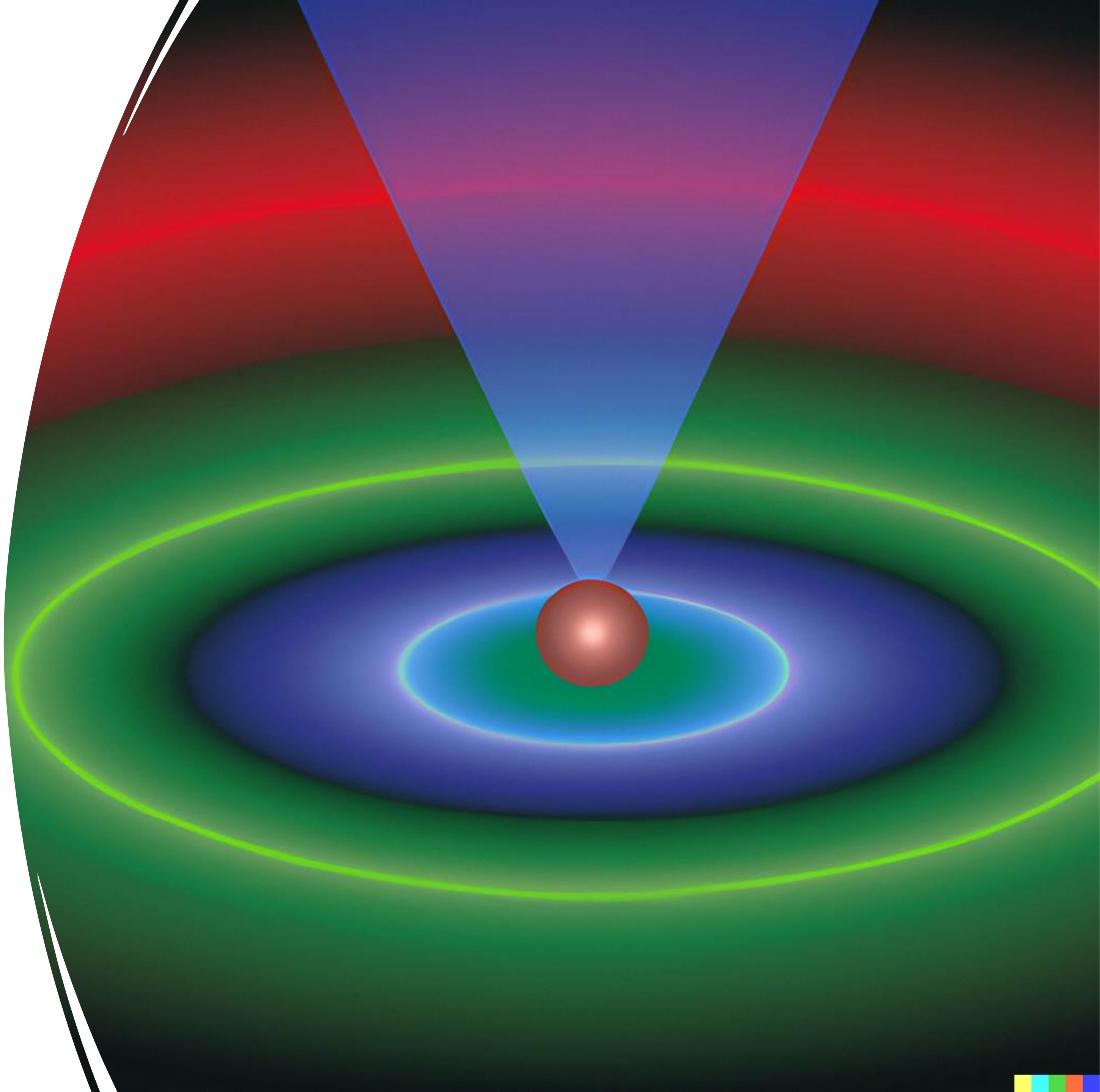
- AES? SHA-3? RSA? Lattices? TLS?
- Any unconditional "computational" security proof
  $\Rightarrow$ OWF (one-way functions) [Impagliazzo and Luby'89; Goldreich'90; …]
  $\Rightarrow$ settle the million-dollar P-vs-NP question
- Quantum cryptography: protocols for quantum parties
- Known quantum crypto: information theoretic or assumes $\geq$OWF
- P vs NP is independent for a broad class of quantum cryptography: no such barriers for security proof!
  [Kretschmer'21; this work and concurrently Morimae—Yamakawa]

Pseudorandom States (PRS)

[Ji, Liu, Song’19]

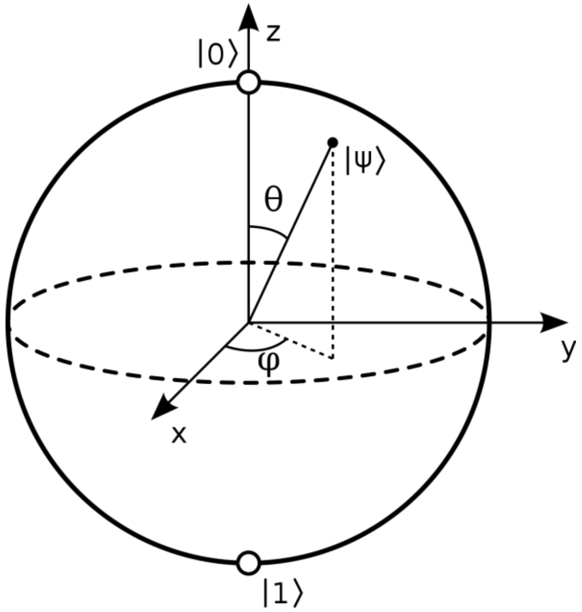
Informally,

- Like a PRG:
  Takes a short seed as input
- Output is quantum state that is pseudo “Haar random”



Quantum states and Haar random states

- Qubit (quantum bit) $|\psi\rangle$: unit vector in $\mathbb{C}^2$
- n qubits $|\psi\rangle$: unit vector in $(\mathbb{C}^2)^{\otimes n} = \mathbb{C}^{2^n}$
- n-qubit Haar random states:
  the uniform distribution μ over unit sphere of $\mathbb{C}^{2^n} \cong \mathbb{R}^{2\cdot 2^n}$
  (Requires $\exp(n)$ bits to describe an approximation)
- Unitary invariance: $\forall U: U \cdot \mathrm{Haar} \equiv \mathrm{Haar}$



Pseudorandom States (PRS) [JLS19]

A quantum algorithm G is an n-qubit PRS generator if:

- Efficient generation
  - Takes as input $k \in \{0,1\}^{\lambda}$
  - Runs in $\mathrm{poly}(\lambda)$ time
  - Outputs a pure state $|\psi_k\rangle\langle\psi_k|$ of $n(\lambda)$ qubits
- Pseudorandomness
  - $|\psi_k\rangle$ "looks" Haar random even with many copies, i.e.
  - $\forall \mathrm{poly}\ t(\cdot)$, $|\psi_k\rangle^{\otimes t(\lambda)} \approx |\phi\rangle^{\otimes t(\lambda)}$ for n-qubit Haar random $|\phi\rangle$

No cloning

Like t-designs
but does not fix t

OWF vs PRS

- JLS19: OWF $\to$ $\omega(\log \lambda)$-qubit PRS
  $\to$ (private-key query-secure) quantum money
- Not clear how $\mathrm{P} = \mathrm{QMA}$ rules out PRS: statement is quantum
- Kretschmer'21: In a relativized world, $\mathrm{P} = \mathrm{QMA}$ but PRS exists (PRS does not imply OWF in a black-box way)
- PRS could be a weaker (quantum) hardness assumption!

$\boxed{\text{What classical crypto task can we achieve just with PRS?}}$

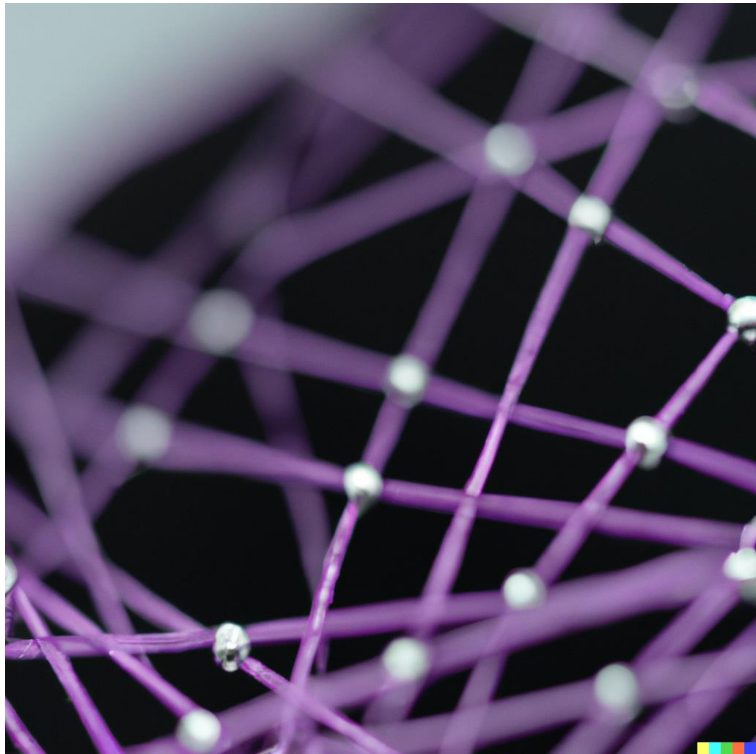
Difficulties of using PRS (vs PRG)

- Output is highly entangled and "brittle" [JLS19]
- We do not know: [Brakerski, Shmueli'20]

  n-qubit PRS $\rightarrow$ n'-qubit PRS for any nontrivial $n \neq n'$

  (for example, $n = 4\lambda$ and $n' = 2\lambda$)
  - Even shrinking naïvely causes the state to be mixed (PRG outputs however can always be shrinked)
- Output might not be expanding: $n \leq \lambda$

Our solution: state analogue of **PRF**



Our results

PRS $\rightarrow$ PRFS $\rightarrow$ Useful crypto

Using PRFS as an important intermediate step, we show

1. One-time encryption of messages of any length exists assuming $\omega(\log \lambda)$-qubit PRS
2. Statistically binding commitments exists assuming $2 \log \lambda + \omega(\log \log \lambda)$-qubit PRS (Corollary: coin flipping, OT and MPC via [BCKM21])

$\exists O(\log \lambda)$-qubit
statistical PRS
[Brakerski, Shmueli'20]

[Morimae, Yamakawa'22]: commitments and one-time signatures assuming $\Omega(\lambda)$-qubit (single-copy-secure length-increasing) PRS

Pseudorandom Function-like States (PRFS)

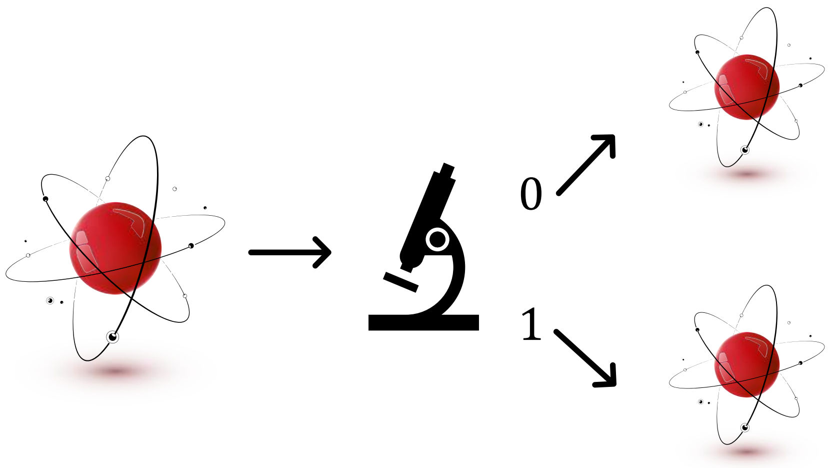
As useful as PRF
(SKE, MAC, …)

A quantum algorithm G is a PRFS generator if:

- Efficient generation
  - Takes as input $k \in \{0,1\}^\lambda$, $x \in \{0,1\}^d$
  - Runs in $\mathrm{poly}(\lambda)$ time
  - Outputs a state $|\psi_{k,x}\rangle$ of n qubits
- Pseudorandomness
  - $\forall \mathrm{poly}\ t$, $\forall$poly # of (distinct) indices $x_{1\ldots s}$ (known to distinguisher),
    $\left(|\psi_{k,x_1}\rangle \cdots |\psi_{k,x_s}\rangle\right)^{\otimes t}$ for random k is computationally indistinguishable from
    $\left(|\phi_1\rangle \cdots |\phi_s\rangle\right)^{\otimes t}$ for n-qubit Haar random states $\{|\phi_i\rangle\}$

PRFS via splitting Haar: post-selection

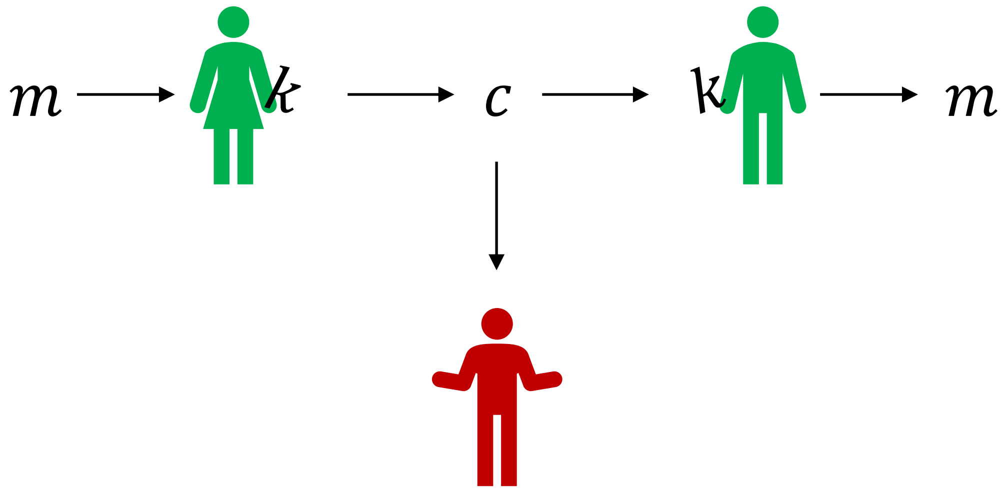
Theorem: $(d+n)$-qubit PRS $\Rightarrow$ n-qubit PRFS with d-bit inputs for $d = O(\log \lambda)$



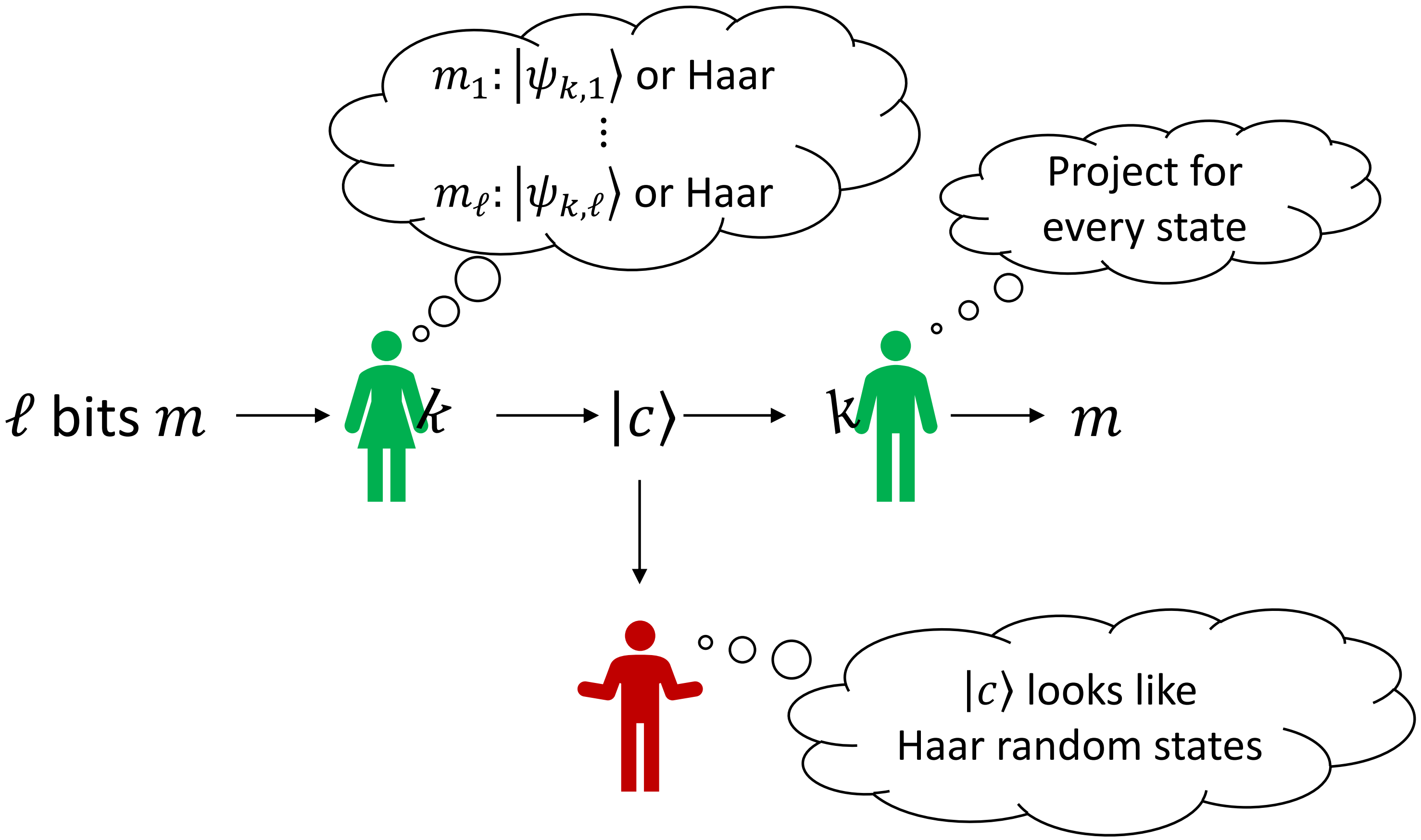
- Given $|\psi_k\rangle$, measure the first d qubits and conditioned on getting x, output the post-measurement state on the remaining $n-d$ qubits
- Post-selection success probability for Haar is exponentially concentrated around $\frac{1}{2^d}$ $\rightarrow$ post-selection is efficient if $d = O(\log \lambda)$

Non-trivial encryption

$|k| < |m|$



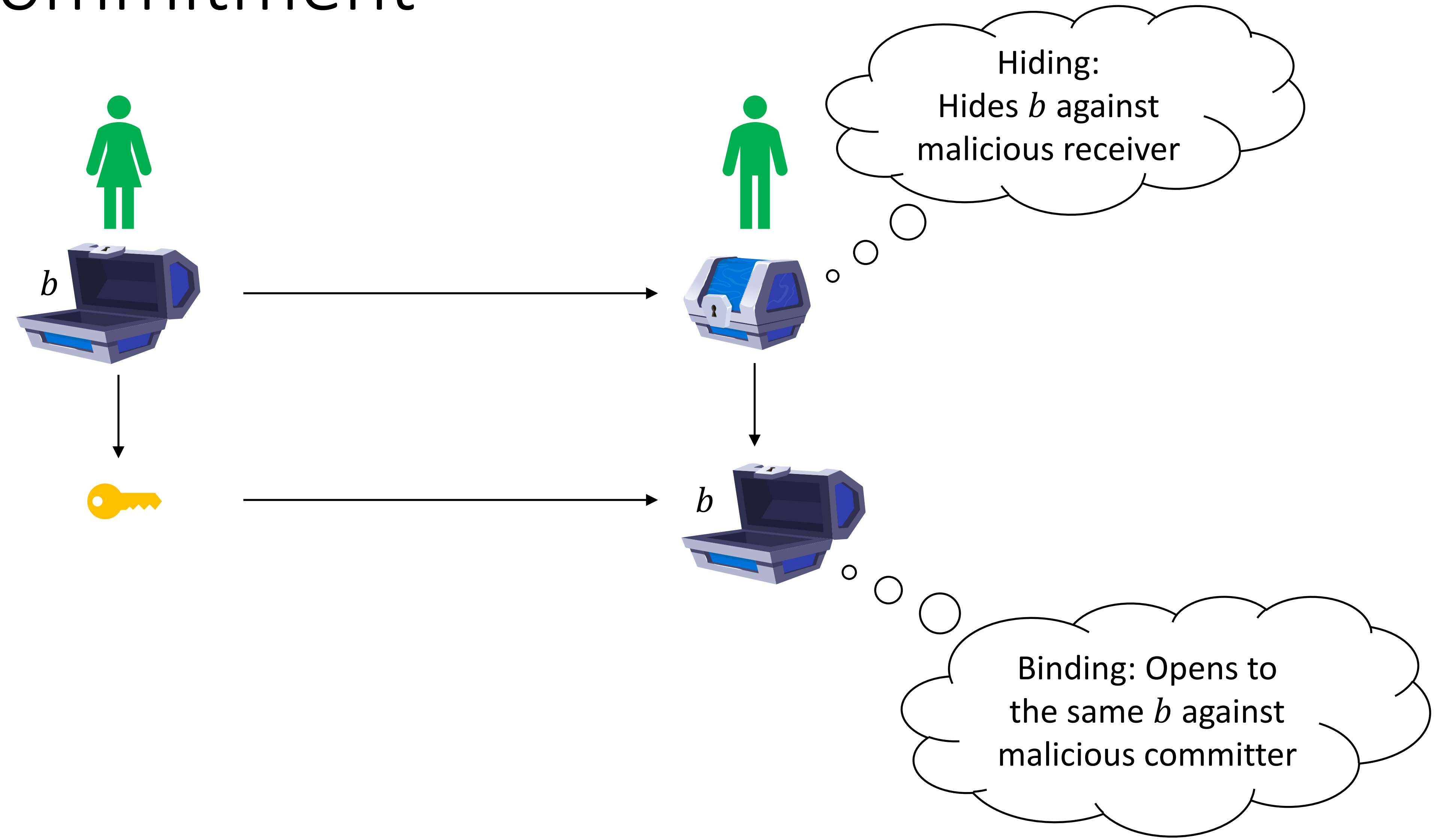
One-time encryption of arbitrarily many bits



Correct with probability $1 - \frac{1}{2^n}$ (needs $n = \omega(\log \lambda)$)

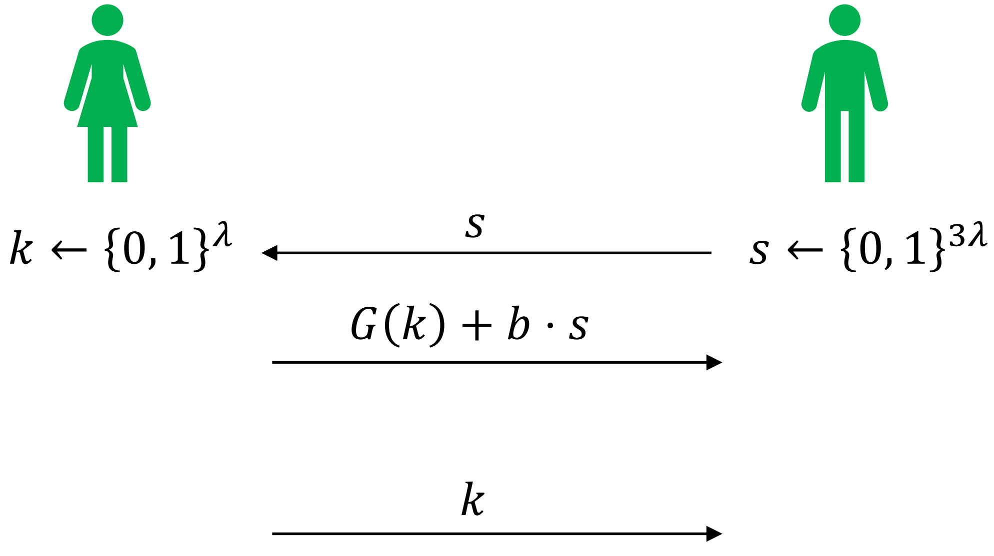
Only need to construct PRFS with input domain $2^d \geq \ell$

Bit commitment



Naor commitment from PRG [Naor'91]

G is a PRG mapping λ bits to 3λ bits



- Hiding: $G(k) + b \cdot s$ looks random as $G(k)$ looks random
- Binding: b is uniquely determined with high probability over s

Naor commitment from PRFS

G is a PRFS with $2^d \cdot n \geq 7\lambda$

$k \leftarrow \{0,1\}^\lambda \quad \xleftarrow{\quad P \quad} \quad P \leftarrow \{0,1\}^{7\lambda}$ (interpret as a Pauli)

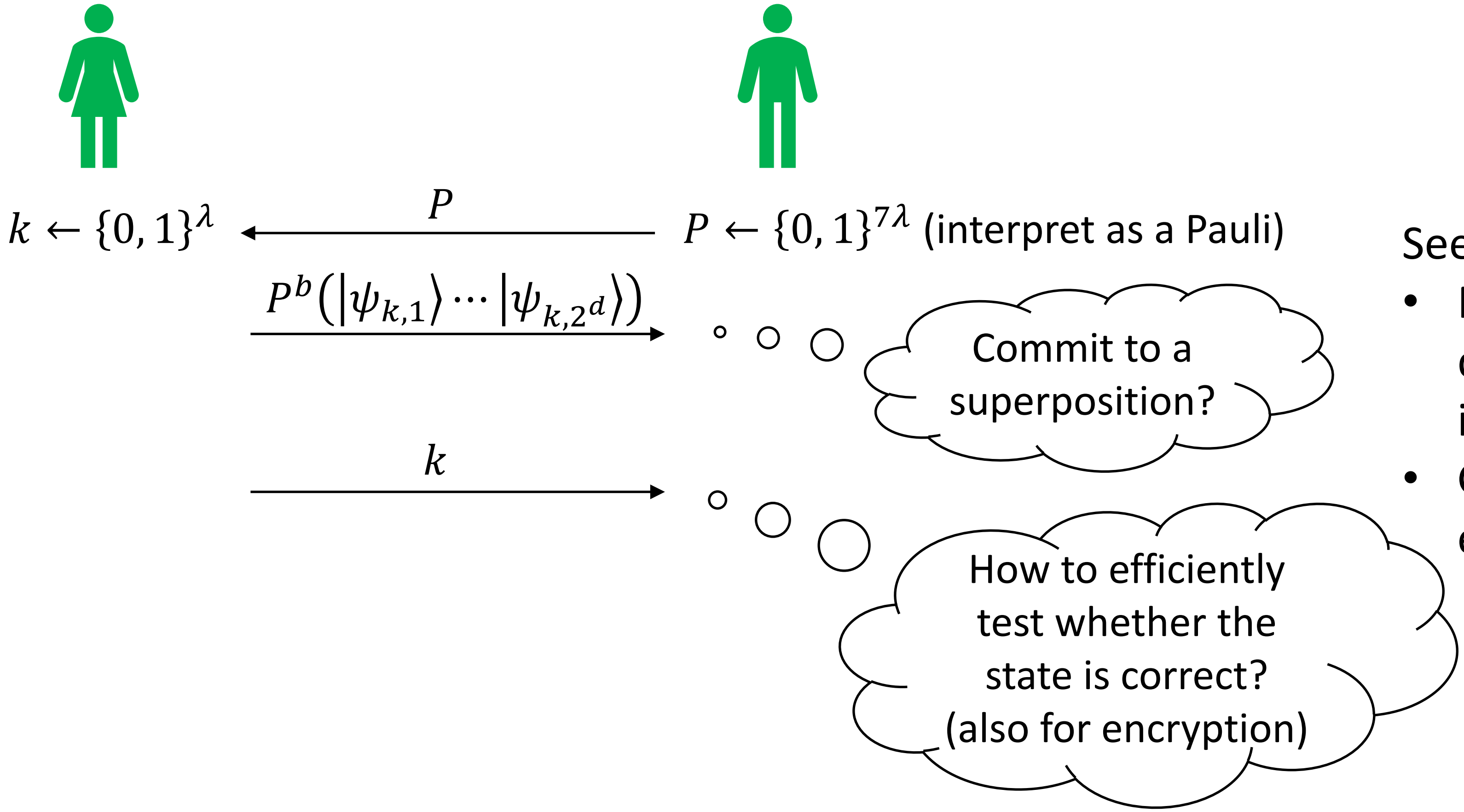
$\xrightarrow{P^b\left(|\psi_{k,1}\rangle \cdots |\psi_{k,2^d}\rangle\right)}$

$\xrightarrow{\quad k \quad}$

- Hiding: commitment looks like 2^d many Haar random states
- Binding: b is "uniquely determined" with high probability over P

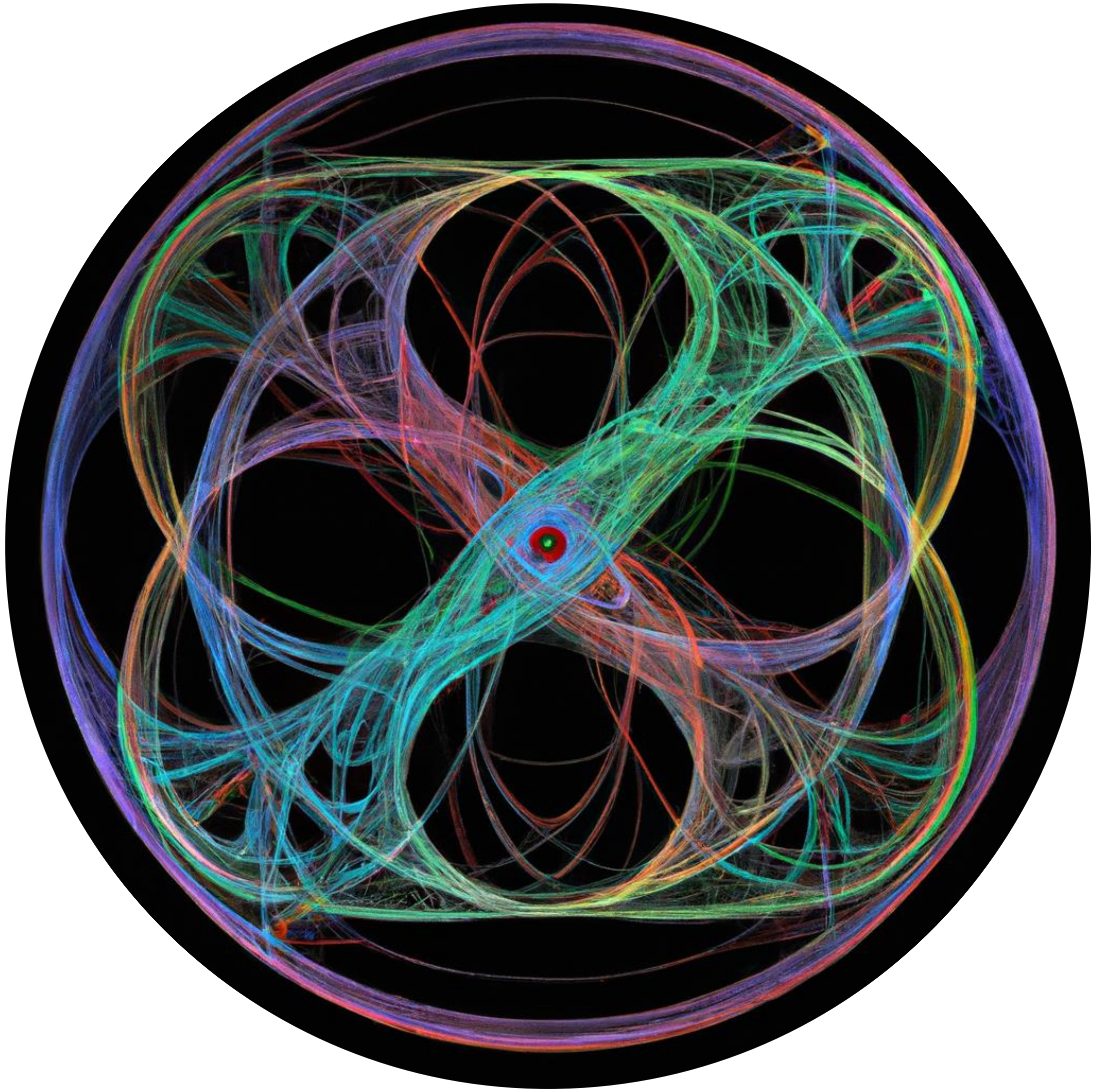
Subtleties

G is a PRFS with $2^d \cdot n \geq 7\lambda$



See paper for resolution:

- New statistical binding definition via collapsing the ideal world
- Generic PRS tester that works even for mixed state outputs

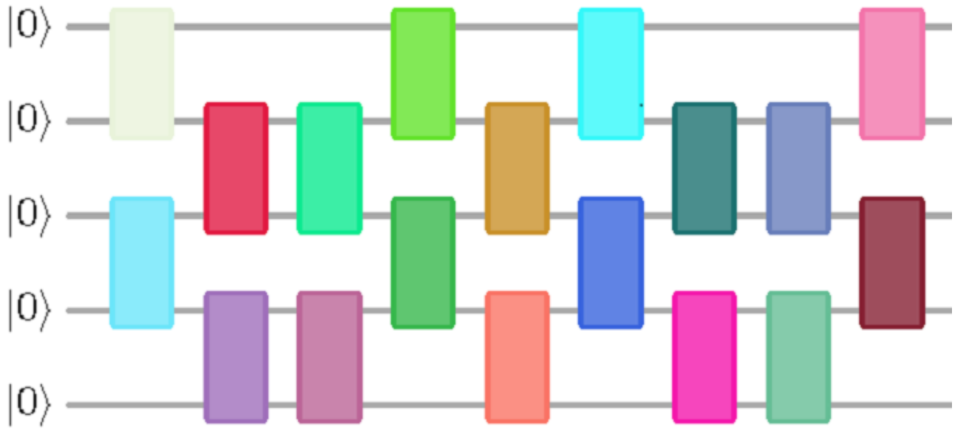


What about candidate constructions?

…and why should they be independent of one-way functions, if at all?

Candidate PRS from random quantum circuits

- Key describes a "sufficiently" large 2-local random unitary U_k
- Output: $U_k|0^n\rangle$
- Already studied in various contexts: quantum supremacy, black holes…
- Realizable on near-term quantum devices?



Candidate PRS from wormholes

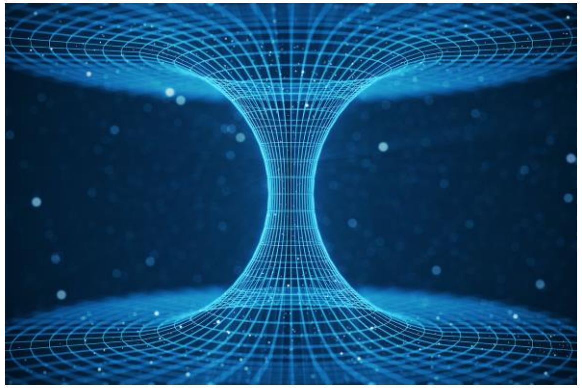
Wormhole: 2 black holes connecting 2 distinct regions of space-time

- Initial (Thermofield Double) state $|TFD\rangle$
- Highly "scrambling" evolution of black holes $U = e^{-iH_{CFT}t}$
- "Shock" O_i: (key) random Pauli operator applied on the first qubit

Conjecture: $UO_\ell UO_{\ell-1} \cdots O_1 U|TFD\rangle$ is PRS [Bouland, Fefferman, Vazirani 2020]

BFV20: conjecture is true if U is a random black-box unitary

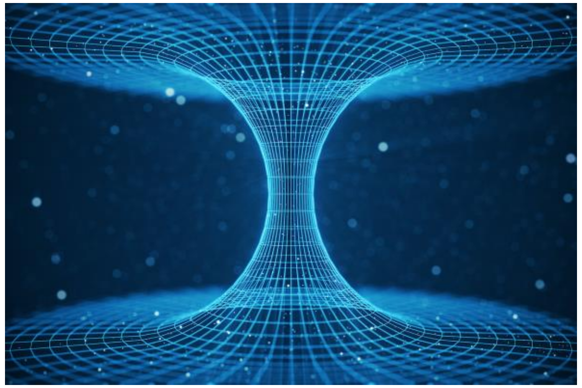
Evidence from black-hole physics?

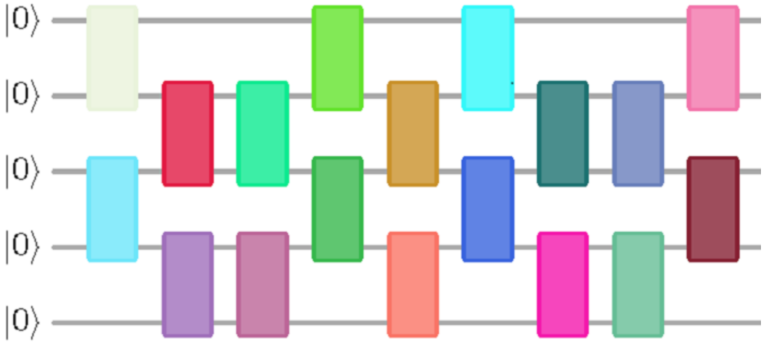


Summary of PRS candidates

Wormhole dynamics & random quantum circuits

- More candidates?
- Formal evidence that they are secure/insecure?
- Formal evidence that they are independent of one-way functions?
- Possibility to achieve better performance from such hardness?





Conclusion & open questions

Quantum cryptography from quantum computational hardness!

- Construct crypto from PRS with even smaller output length?
  (Construct statistical PRS with larger output length?)
- What other interesting quantum hardness lies beyond PRS?

(Some progress in upcoming work: a minimal primitive)

Thank you!

Image references: freepik.com; Image of Bloch sphere from Wikipedia; DALL-E