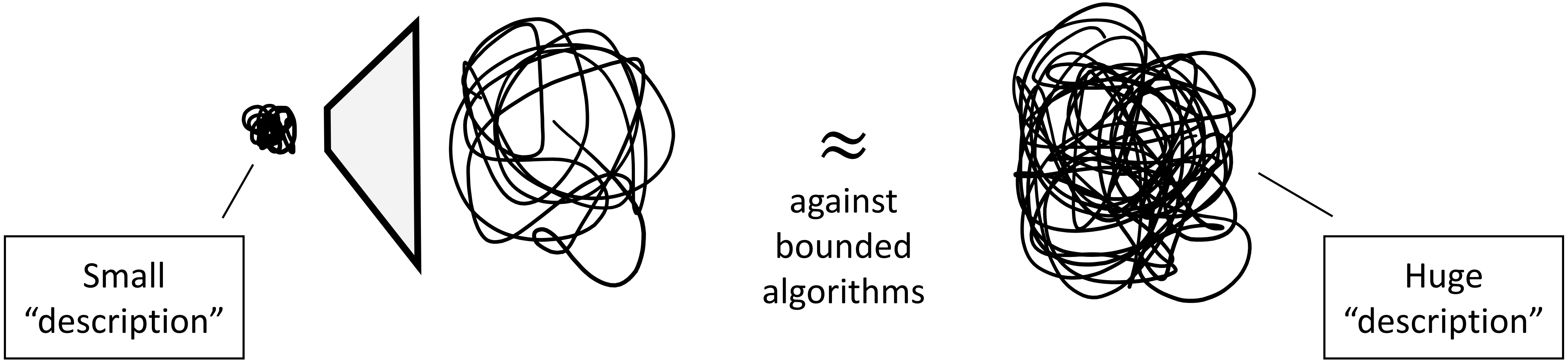
Cryptography from Quantum Pseudorandomness

Luowen Qian (Boston University)

Based on:
2112.10020 (Prabhanjan Ananth, LQ, Henry Yuen);
2211.01444 (PA, Aditya Gulati, LQ, HY)

Pseudorandomness



Central notion in (classical) TCS:

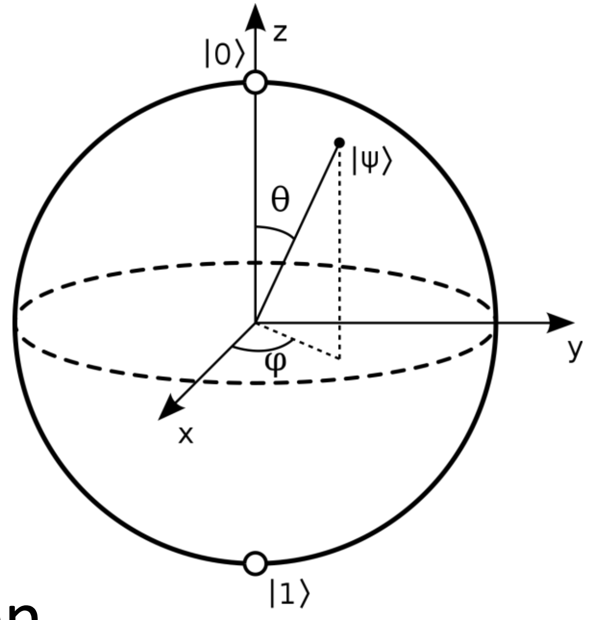
- Expander graphs, list-decodable ECCs, randomness extractors…
- Derandomization
- Cryptography

Haar random states

The uniform distribution Haar that satisfies unitary invariance

$$\forall U : \; U \cdot \mathrm{Haar} \equiv \mathrm{Haar}$$

even if the entire (classical) description is given.



Ubiquitous in quantum information/computing!
(random quantum circuits, benchmarking, etc)

Issue: continuous distribution, infinite length description
(every fresh copy yields more information)

Finitely producing Haar

- State t-designs: close to Haar up to t copies
- Prepare a maximally mixed state over the symmetric subspace

$$\mathrm{Sym}(d,t) = \mathrm{span}\left\{|\psi\rangle^{\otimes t} \middle| |\psi\rangle \in \mathbb{C}^d\right\}$$

Drawbacks:

- State t-designs require $d^{\Omega(t)}$ states! (for moderately large d)
- No guarantees once $t+1$ copies are given!

Cryptographic pseudorandomness

Instead of restricting the number of copies given,

Let's restrict the computational power of the algorithm instead

Pseudorandom States (PRS) [Ji, Liu, Song'18]

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.
  - $\forall \mathrm{poly}\ t(\cdot)\ \forall \mathrm{QPT}_\lambda\ A$,

$$\left| \Pr_{k \leftarrow \{0,1\}^\lambda}\left[A\left(|\psi_k\rangle^{\otimes t(\lambda)}\right) = 1\right] - \Pr_{|\phi\rangle \leftarrow \mathrm{Haar}_{n(\lambda)}}\left[A\left(|\phi\rangle^{\otimes t(\lambda)}\right) = 1\right] \right| \leq \mathrm{negl}(\lambda)$$

Similar to t-designs but does not fix t

PRS and quantum computing

- State t-designs for efficient observers but much easier to construct!
- Important conceptual notion to understand black hole interior
  [Bouland, Fefferman, Vazirani'20, …]
- Useful techniques for separating complexity of quantum & classical operations [Kretschmer'22; Irani, Natarajan, Nirkhe, Rao, Yuen'22; Kretschmer, Q, Sinha, Tal'23]
- Quantum cryptography (original motivation!)

Roadmap

- Construct PRS from (pseudo)random functions
- Quantum cryptographic applications of PRS
  - Quantum money (from unclonability of Haar random states) [JLS18]
  - EFI, commitments, secure computation, zero knowledge
  - One-time encryptions
  - Quantum cryptography with classical communication using verifiable tomography
- A different flavor of quantum pseudorandomness: PRFS
  - Applications to encryption, authentication, garbling

Binary phase PRS

- Phase oracle for a Boolean function $f: \{0,1\}^n \to \{0,1\}$

$$P_f|x\rangle = (-1)^{f(x)}|x\rangle$$

- Binary phase PRS: $G(f) = P_f H^{\otimes n}|0^n\rangle$ for a random function f
- Proposed in [JLS18]

Theorem: [Brakerski, Shmueli'19; AGQY23]

Statistical distance between $G(f)$ and Haar given t copies is $O\left(\frac{t^2}{2^n}\right)$

Corollary: If $\{f_k\}$ is PRF, then $G(f_k)$ is secure PRS for $n = \omega(\log \lambda)$

Theorem proof sketch

Theorem: [BS19; AGQY23]

Statistical distance between $G(f)$ and Haar given t copies is $O\left(\frac{t^2}{2^n}\right)$

- BS19: Compute trace distance between binary phase PRS and Haar
  - Brute-force calculation of spectral L1-norm, very technical, unintuitive
- AGQY23: A simpler proof, less technical, more intuitive

Theorem proof sketch: hybrid argument

1. Haar random distribution $|\vartheta\rangle^{\otimes t}$
2. Random basis vector of $\mathrm{Sym}(2^n, t)$
   - Given a histogram of t balls into 2^n bins, a basis vector of $\mathrm{Sym}(2^n, t)$ is a uniform superposition over all configurations with that histogram e.g., $|0,0,1\rangle + |0,1,0\rangle + |1,0,0\rangle$ is the basis vector for histogram $(2, 1, 0, \ldots)$
   - Identically distributed as 1

Theorem proof sketch: hybrid argument

1. Haar random distribution $|\vartheta\rangle^{\otimes t}$
2. Random basis vector of $\mathrm{Sym}(2^n, t)$
3. Random basis vector with a collision-less histogram
   (every element appears exactly either 0 or 1 time)
   - If $t \ll 2^n$, collisions are rare
   - We remove very small fraction of histograms from the possible choices
   - Statistical distance to 2 is $O\left(\frac{t^2}{2^n}\right) \approx$ collision probability

Theorem proof sketch: hybrid argument

1. Haar random distribution $|\vartheta\rangle^{\otimes t}$
2. Random basis vector of $\mathrm{Sym}(2^n, t)$
3. Random basis vector with a collision-less histogram
4. Random “binary histogram” vector
    - t balls into 2^n bins, but we treat the histograms as identical if their each respective entries mod 2 are identical
      e.g. (1, 4, 3, 0, 0, 1) is identical to (3, 0, 5, 0, 0, 1) after pointwise mod 2
    - If there is no collision, the vector is identical to collision-less basis vector
    - Statistical distance to 3 is again $O\left(\frac{t^2}{2^n}\right)$

Theorem proof sketch: hybrid argument

1. Haar random distribution $|\vartheta\rangle^{\otimes t}$
2. Random basis vector of $\mathrm{Sym}(2^n, t)$
3. Random basis vector with a collision-less histogram
4. Random “binary histogram” vector
5. Binary phase PRS $\left((-1)^{f(x)}|x\rangle\right)^{\otimes t}$
   - Identically distributed as 4 via a direct expansion of density matrices

Comments on binary phase states

- Beyond PRS, binary phase states also appeared in quantum information theory, quantum algorithm, quantum advantage, quantum complexity…
- K22: if $\mathrm{P} = \mathrm{NP}$, binary phase PRS can be distinguished
- t-Forrelation state: $G(f_1, \dots, f_t) = P_{f_t} H^{\otimes n} \cdots P_{f_2} H^{\otimes n} P_{f_1} H^{\otimes n} |0^n\rangle$
  - KQST23: 2-Forrelation states are single-copy secure PRS against $\mathrm{BQP}^{\mathrm{PH}}$ adversaries if $\{f_{k,b}\}$ is instantiated by a random oracle
  - Even if $\mathrm{P} = \mathrm{PH}$, this construction is still plausibly secure when instantiated by some efficient $\{f_{k,b}\}$ (like SHA-3)

Interlude: consequence to quantum cryptography

- K22+KQST23: Quantum pseudorandomness could exist even if $\mathrm{P} = \mathrm{NP}$
- All classical (computational) cryptography relies on $\mathrm{P} \neq \mathrm{NP}$
- Formal evidence that quantum cryptography could potentially be constructed from weaker computational assumptions! (Indeed, not even $\mathrm{P} \neq \mathrm{NP}$ is required)
  - Later we construct these quantum cryptographic object from quantum pseudorandomness in a “black-box” way, which would extend separations
- Open question: barrier to proving security of quantum cryptography?

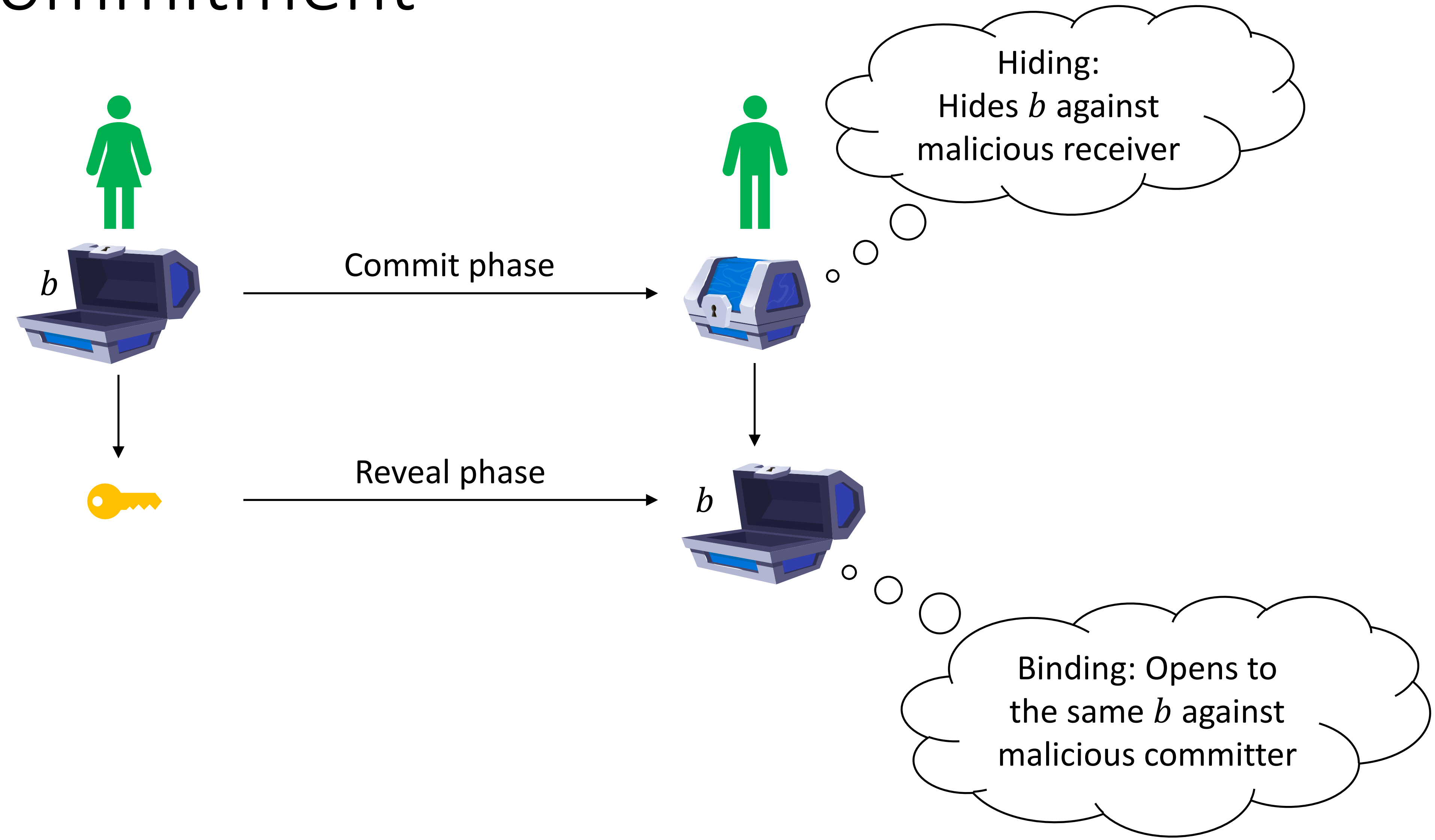
Statistical PRS

- A statistical attack using von Neumann entropy: [AGQY23]
  - Entropy of t copies of a Haar random state goes to infinity as $t \to \infty$
  - Entropy of t copies of a PRS is at most λ bits (entropy of seed)
  - Take t large enough so that entropy of Haar is $\geq \lambda + 1$ bits
  - $O(\lambda)$ copies suffice if $n \geq \log \lambda$,
    but $\lambda^{\omega(1)}$ copies required if $n = \big(1 - o(1)\big) \log \lambda$
  - Thus, computational constraints are required for security of long PRS
- BS20: construct statistical PRS for $n \leq .01 \log \lambda$
  - Idea: (simplified) sample a discretized Haar random state/ϵ-net
- Open: what is the sharp threshold for statistical PRS?

Construct cryptography from PRS

- Focus on computational cryptography
  (the task is impossible without computational constraints)
  Examples:
  - Commitments (Mayer–Lo–Chau)
  - Securely encrypting $n + 1$ bits of message with n bits of key
  - …
- Statistical PRS cannot be used; we must consider computational ones

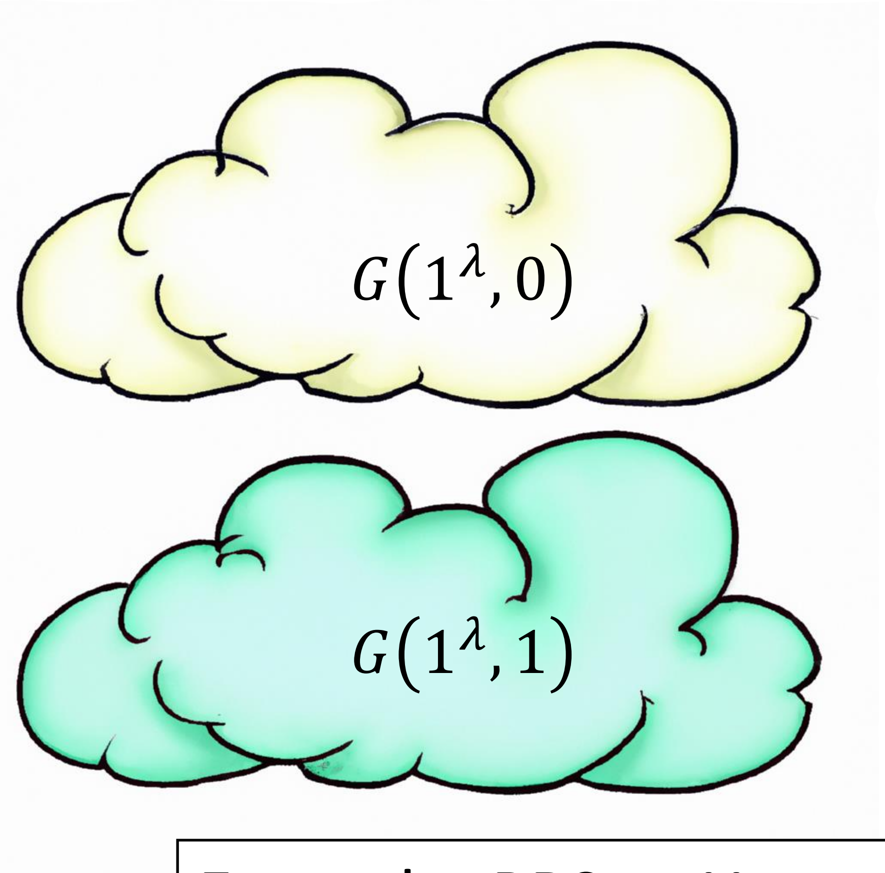
Bit commitment



Commitments from computational PRS

- AQY: (also concurrently by Morimae, Yamakawa'22)
  quantum analogue of Naor commitment from classical PRG
  - Conceptually simple assuming you know Naor commitment
  - Analysis is messy
- The "EFI" approach: [Brakerski, Canetti, Q'23]
  construct commitment from statistical-computational gap
- Once we have commitments, we can do OT MPC ZK…

EFI pairs (of quantum states)



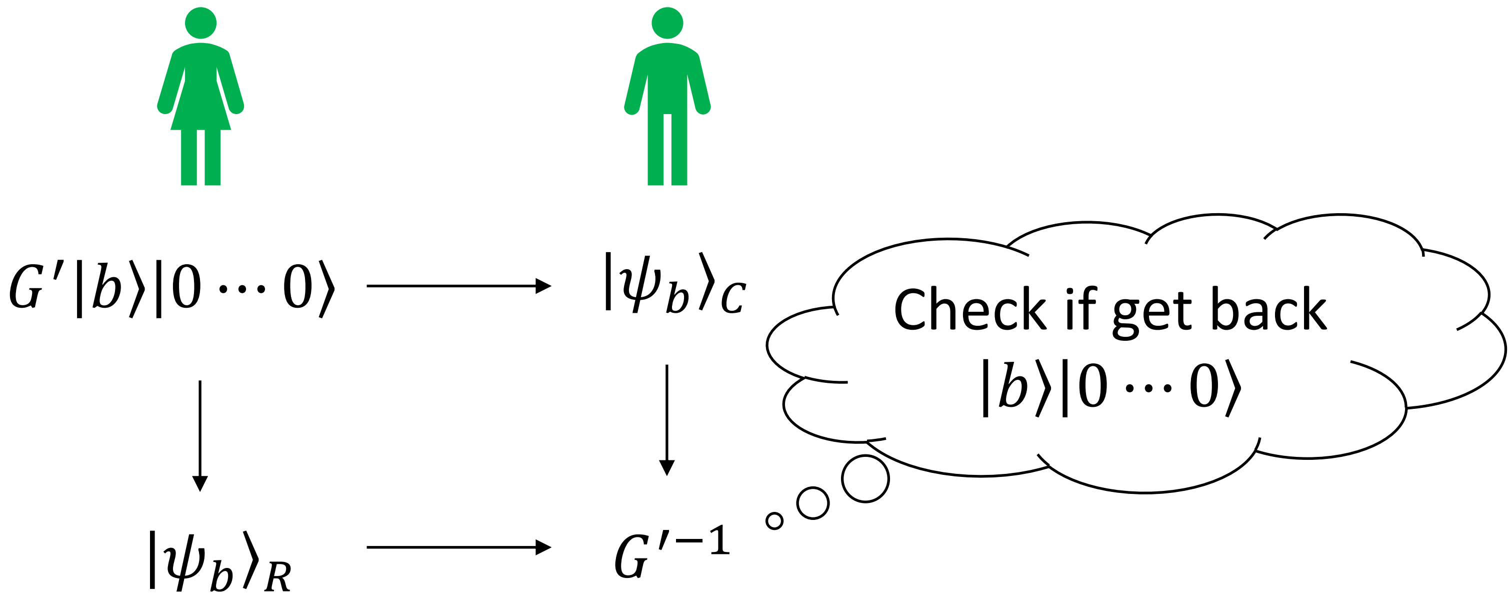
- **E**fficient generation: $G(1^\lambda, b)$ is an efficient quantum algorithm outputting an arbitrary mixed state (distribution over pure states)
- Statistical **F**arness:
  $G(1^\lambda, 0)$ vs $G(1^\lambda, 1)$ are statistically far (in trace distance)
- Computational **I**ndistinguishability:
  $G(1^\lambda, 0) \approx_c G(1^\lambda, 1)$

Example: PRS vs Haar random distribution with sufficiently many copies

Commitment from EFI via purification

"Canonical form" commitment [Chailloux, Kerenidis, Rosgen'11; Yan, Weng, Lin, Quan'15; Yan'22]

- Run purified generation $G'|b\rangle|000\cdots0\rangle \rightarrow |\psi_b\rangle_{CR}$
  (C is output register, R is its purification)



- Computational hiding $\Leftarrow$ computational indistinguishability
- Statistical binding $\Leftarrow$ statistical farness + Uhlmann's theorem

Difficulties of using PRS for encryption

Naïve idea: replace PRG-based encryptions with PRS

- Haar random states are highly entangled [JLS19]
  - PRG-based encryptions crucially uses the fact that the output of PRG is classical/a product state
- We do not know: [BS20]

  n-qubit PRS $\rightarrow n'$-qubit PRS for any nontrivial $n \neq n'$
  - Even shrinking naïvely causes the state to be mixed
- Non-trivial PRS need not be expanding $n \leq \lambda$

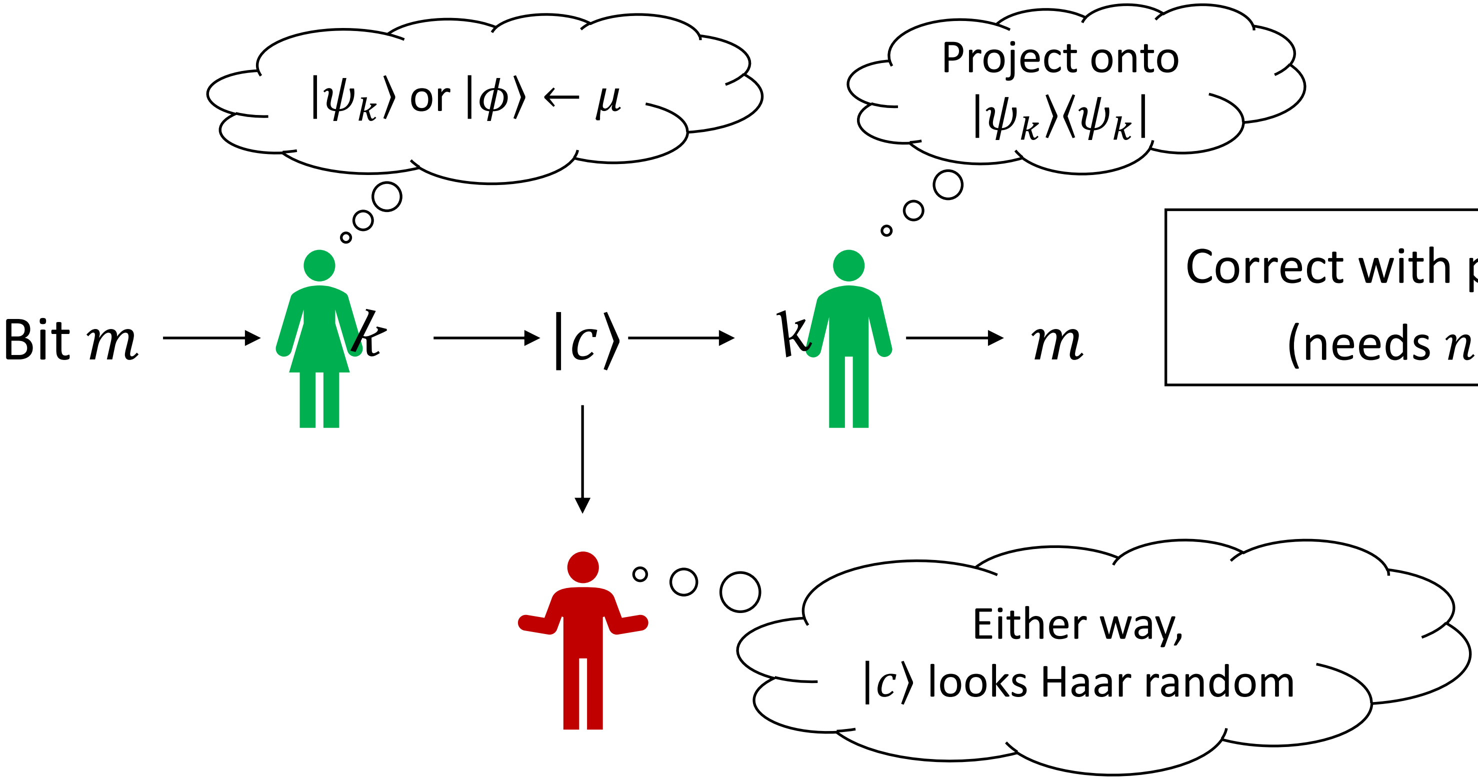
Solution: chop a Haar random state into a longer product state

Pseudorandom Function-like States (PRFS)

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 $\text{poly}(\lambda)$ time
  - Outputs a state $|\psi_{k,x}\rangle$ of n qubits
- Pseudorandomness
  - $\forall$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
    $(|\phi_1\rangle \cdots |\phi_s\rangle)^{\otimes t}$ for n-qubit Haar random states $\{|\phi_i\rangle\}$

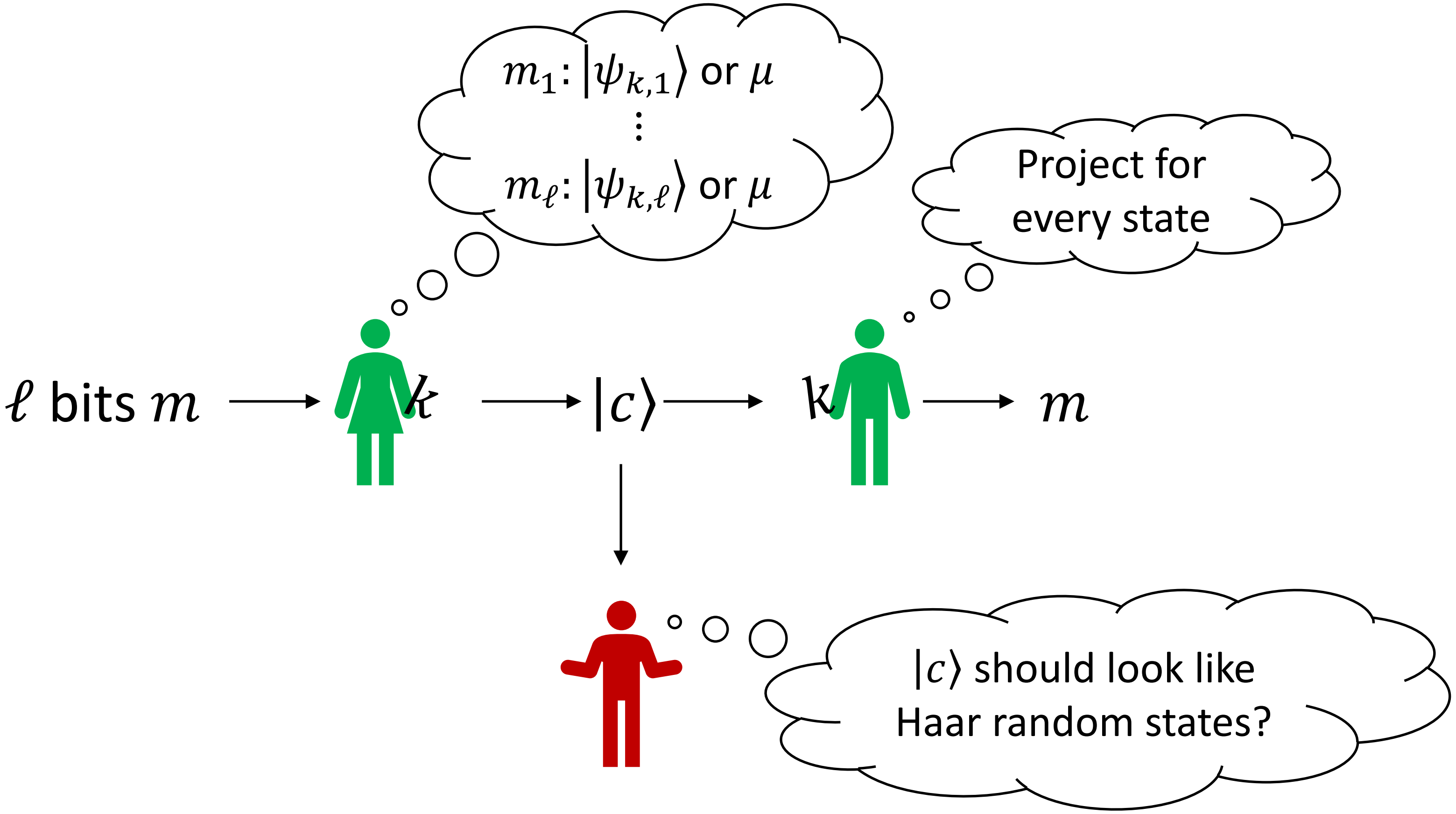
One-time encryption of a single bit w/ PRS



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

How to encrypt many bits?

One-time encryption of many bits w/ PRFS

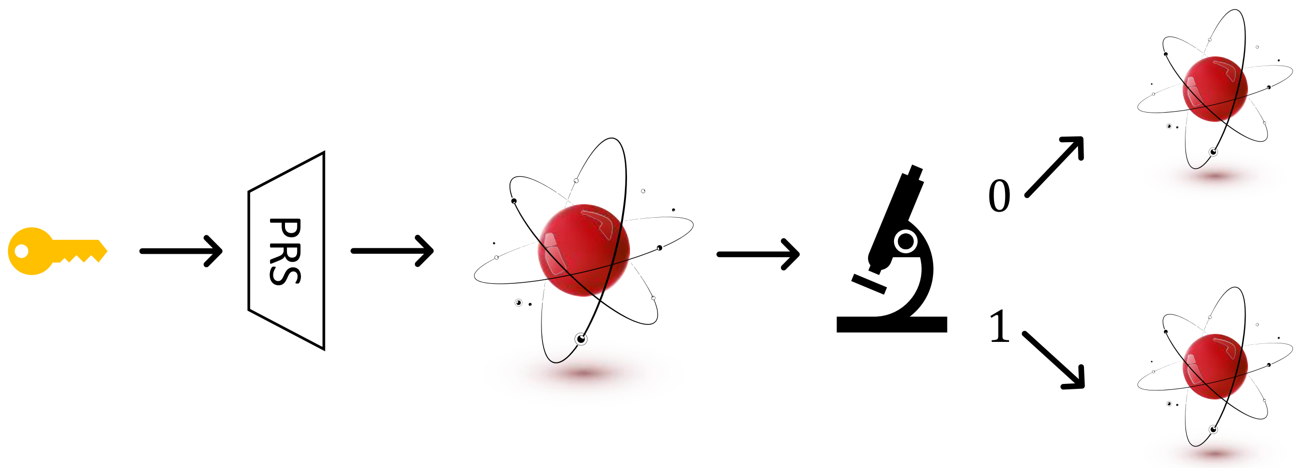


Only need to construct PRFS with input domain $2^d \geq \ell$

Construct PRFS from PRS?

PRFS: $d = O(\log \lambda)$
PRS: $n = \omega(\log \lambda)$

PRFS via chopping Haar: post-selection



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

Cryptography from PRFS

- PRS with $n = \omega(\log \lambda)$-qubit output

  $\rightarrow$ PRFS with $\log \ell = O(\log \lambda)$-bit input domain
  and $n - \log \ell = \omega(\log \lambda)$-qubit output

  $\rightarrow$ ℓ-bit encryption

Generalize Zhandry's small range distribution technique for unitaries

- Ideal PRFS: polynomial input/output length
  - Can be constructed from PRF by adapting binary phase PRS [AGQY23]
  - Or constructed from pseudorandom unitary (PRU) [AGQY23]
    (Also separated from post-quantum OWF [K22])
  - Could be immediately used as a PRF replacement in crypto applications
    (secret-key encryptions, message authentication, garbling, …)

Crypto with classical communication

- So far, all the protocols we construct use quantum communication
- Need to send pseudorandom states in the communication
- Idea: dequantize the communication using tomography!
  - Can only efficiently tomograph if $n = O(\log \lambda)$
  - Need a way to verify the correctness of tomography
- AGQY23: Verifiable tomography from PRS & application to commitments and encryptions

More open questions

- Construction of PRU using any classical oracle?
- Does single-copy secure PRS imply $\mathrm{P} \neq \mathrm{PSPACE}$ or other unproven complexity conjecture?
- Can we construct (single-copy/multi-copy) PRS from less structured hardness? (EFI/commitments, single-copy PRS, etc)

Thank you! Questions?