Pseudorandom Unitaries in the Haar Random Oracle Model

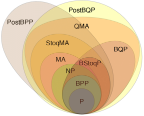
Prabhanjan Ananth (UCSB),
John Bostanci (Columbia),
Aditya Gulati (UCSB),
Yao-Ting Lin (UCSB)

Crypto, 2025

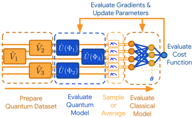
August 18, 2025

Quantum Pseudorandomness

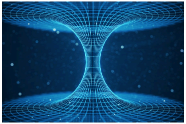
Quantum Complexity



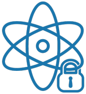
Quantum Learning Theory



Wormholes and AdS/CFT



Quantum Cryptography



Pseudorandom Unitaries

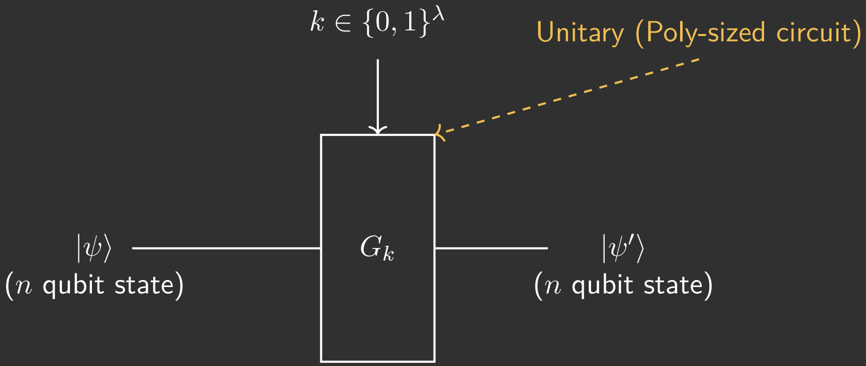
A Central Primitive of Quantum Pseudorandomness

Pseudorandom Unitary (PRU)

Efficiently implementable circuits that “behave like” random unitary.

Pseudorandom Unitary (PRU)

1. Efficient implementation:



Notation: n-PRU

Pseudorandom Unitary (PRU)

2. Pseudorandomness

$$\mathcal{A}^{G_k} \approx \mathcal{A}^{U}$$

U: Haar random unitary

Strong Pseudorandom Unitary (sPRU)

2. Pseudorandomness

$$\mathcal{A}^{G_k, G_k^\dagger} \approx \mathcal{A}^{U, U^\dagger}$$

Previous work

- (JLS18) defined PRU.
- (AGKL22,LQS+23,BM24,MPSY24,CBB+24) gave partial results.
- (MH24) finally gave a construction for adaptive queries.

Defined Path-recording framework

Previous work

- (JLS18) defined PRU.
- (AGKL22,LQS+23,BM24,MPSY24,CBB+24) gave partial results.
- (MH24) finally gave a construction for adaptive queries.

Defined Path-recording framework

Previous work

- (JLS18) defined PRU.
- (AGKL22,LQS+23,BM24,MPSY24,CBB+24) gave partial results.
- (MH24) finally gave a construction for adaptive queries.

Defined Path-recording framework

Previous work

- (JLS18) defined PRU.
- (AGKL22,LQS+23,BM24,MPSY24,CBB+24) gave partial results.
- (MH24) finally gave a construction for adaptive queries.

Defined Path-recording framework

Why Should We Care About PRUs?

- Succinct Commitments to Quantum States (Chen-Movassagh'24)
- Multi-Copy Secure Encryption Scheme (AGKL24)
- Learning Theory and Complexity Theory
- AdS/CFT correspondence (Bouland-Fefferman-Vazirani'20)
- **Kretschmer (Kre21)** showed evidence that:

  *Quantum pseudorandomness may exist **even if one-way functions do not exist**.*

Why Should We Care About PRUs?

- Succinct Commitments to Quantum States (Chen-Movassagh'24)
- Multi-Copy Secure Encryption Scheme (AGKL24)
- Learning Theory and Complexity Theory
- AdS/CFT correspondence (Bouland-Fefferman-Vazirani'20)
- **Kretschmer (Kre21)** showed evidence that:
  Quantum pseudorandomness may exist ***even if one-way functions do not exist****.*

Constructing PRUs Without One-Way Functions

- **Many constructions of quantum pseudorandomness:**
  - JLS18, BS19, BS20, AQY22, AGQY22, BBSS23, LQS+23, ABF+24, AGKL24, MPSY24, BM24

- **Constructions without One-Way Functions?**

Constructing PRUs Without One-Way Functions

- **Many constructions of quantum pseudorandomness:**
  - JLS18, BS19, BS20, AQY22, AGQY22, BBSS23, LQS+23, ABF+24, AGKL24, MPSY24, BM24
- **Constructions without One-Way Functions?**
  - Using Quantum Assumptions [BHHP25]
  - Potentially build in Idealised Models and then try to instantiate the Idealised model

Constructing PRUs Without One-Way Functions

- **Many constructions of quantum pseudorandomness:**
  - JLS18, BS19, BS20, AQY22, AGQY22, BBSS23, LQS+23, ABF+24, AGKL24, MPSY24, BM24
- **Constructions without One-Way Functions?**
  - Using Quantum Assumptions [BHHP25]
  - Potentially build in Idealised Models and then try to instantiate the Idealised model

Constructing PRUs Without One-Way Functions

- **Many constructions of quantum pseudorandomness:**
  - JLS18, BS19, BS20, AQY22, AGQY22, BBSS23, LQS+23, ABF+24, AGKL24, MPSY24, BM24
- **Constructions without One-Way Functions?**
  - Using Quantum Assumptions [BHHP25]
  - Potentially build in Idealised Models and then try to instantiate the Idealised model

Quantum Haar Random Oracle Model

[Bouland-Fefferman-Vazirani'20, Chen-Movassagh'24]

Quantum Haar Random Oracle Model (QHROM)

All parties P_i as well as the adversary $\mathcal{A}$ get oracle access to a Haar Unitary and its inverse.

$$U \leftarrow \mu_n$$

μ_n: Haar Distribution

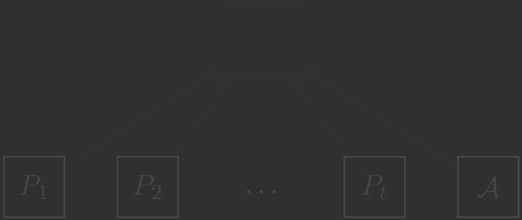
$\boxed{P_1}$ $\boxed{P_2}$ $\cdots$ $\boxed{P_t}$ $\boxed{\mathcal{A}}$

Quantum Haar Random Oracle Model (QHROM)

All parties P_i as well as the adversary $\mathcal{A}$ get oracle access to a Haar Unitary and its inverse.

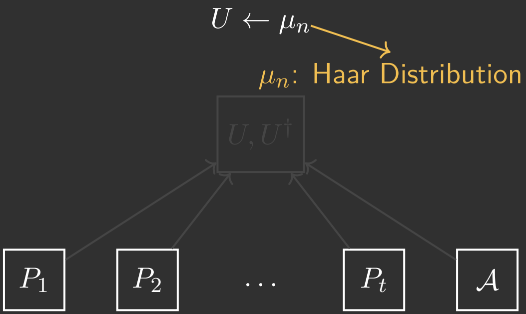
$$U \leftarrow \mu_n$$

μ_n: Haar Distribution



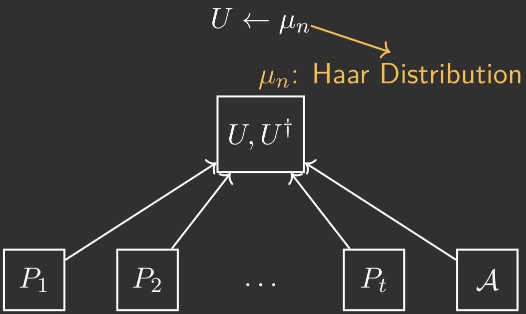
Quantum Haar Random Oracle Model (QHROM)

All parties P_i as well as the adversary $\mathcal{A}$ get oracle access to a Haar Unitary and its inverse.



Quantum Haar Random Oracle Model (QHROM)

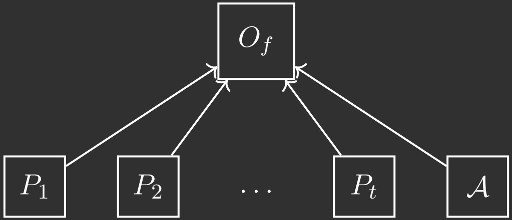
All parties P_i as well as the adversary $\mathcal{A}$ get oracle access to a Haar Unitary and its inverse.



Similarity to QROM

This model is similar to the Quantum Random Oracle Model (QROM) where all parties and the adversary get access to a random function oracle.

$$f \leftarrow \mathcal{F}_n$$



Why use QHROM

- Can Model Behaviour of Random Quantum Circuits.
- Abstraction to study Blackhole Dynamics.
- Gives a pathway to get results from PRU in the plain model.
- Helps show separations.

Why use QHROM

- Can Model Behaviour of Random Quantum Circuits.
- Abstraction to study Blackhole Dynamics.
- Gives a pathway to get results from PRU in the plain model.
- Helps show separations.

Why use QHROM

- Can Model Behaviour of Random Quantum Circuits.
- Abstraction to study Blackhole Dynamics.
- Gives a pathway to get results from PRU in the plain model.
- Helps show separations.

Why use QHROM

- Can Model Behaviour of Random Quantum Circuits.
- Abstraction to study Blackhole Dynamics.
- Gives a pathway to get results from PRU in the plain model.
- Helps show separations.

Strong Pseudorandom Unitary (PRU)

Psuedorandomness

$$\mathcal{A}^{U,U^\dagger,G_k^{U,U^\dagger}} \approx \mathcal{A}^{U,U^\dagger,V}$$

What can we do in QHROM

- [Bouland-Fefferman-Vazirani'21] Give a candidate construction of PRUs in the QHROM without proof.
- [ABGY25,HY25] Made partial progress on showing PRUs exist in QHROM.

Results

In QHROM

- **Unbounded-poly-query secure strong PRUs in QHROM:** Achieved with **two queries** to the Haar random oracle.
-

In QHROM

- **Unbounded-poly-query secure strong PRUs in QHROM:**
  Achieved with **two queries** to the Haar random oracle.
- **Strong Gluing Theorem for Haar Unitaries:**
  How to construct “Large” Haar Unitaries from smaller ones.
  [SHH24] shows how to do this in the inverseless case.

Consequences

Shrinking strong PRU Keys for Free, in Plain Model:

Unbounded query secure strong PRUs exist with keys of size $O(\lambda^{1/c})$ for any constant c, if strong PRU exists

Previously, GJMZ22 showed 1 query PRU with short keys exists if PRU exists.

Construction of other primitives in QHROM:

sPRU $\rightarrow$ PRU $\rightarrow$ PRFS $\rightarrow$ PRS $\rightarrow$ OWSG $\rightarrow$ EFI.

Consequences

Shrinking strong PRU Keys for Free, in Plain Model:
Unbounded query secure strong PRUs exist with keys of size $O(\lambda^{1/c})$ for any constant c, if strong PRU exists
Previously, GJMZ22 showed 1 query PRU with short keys exists if PRU exists.

Construction of other primitives in QHROM:
sPRU $\rightarrow$ PRU $\rightarrow$ PRFS $\rightarrow$ PRS $\rightarrow$ OWSG $\rightarrow$ EFI.

Consequences

Shrinking strong PRU Keys for Free, in Plain Model:
Unbounded query secure strong PRUs exist with keys of size $O(\lambda^{1/c})$ for any constant c, if strong PRU exists
Previously, GJMZ22 showed 1 query PRU with short keys exists if PRU exists.

Construction of other primitives in QHROM:
sPRU $\rightarrow$ PRU $\rightarrow$ PRFS $\rightarrow$ PRS $\rightarrow$ OWSG $\rightarrow$ EFI.

Consequences

Shrinking strong PRU Keys for Free, in Plain Model:
Unbounded query secure strong PRUs exist with keys of size $O(\lambda^{1/c})$ for any constant c, if strong PRU exists
Previously, GJMZ22 showed 1 query PRU with short keys exists if PRU exists.

Construction of other primitives in QHROM:
sPRU $\rightarrow$ PRU $\rightarrow$ PRFS $\rightarrow$ PRS $\rightarrow$ OWSG $\rightarrow$ EFI.

Techniques

Strong PRU in QHROM

Potential constructions

Single Query

$$A_k \, U \, B_k$$

Potential constructions

Single Query

$$A_k \, U \, B_k$$

$$(A_k U B_k \otimes I)|EPR\rangle = (A_k U \otimes B_k^T)|EPR\rangle$$

Potential constructions

Single Query

$$A_k \, U \, B_k$$

$$(A_k U B_k \otimes I)|EPR\rangle = (A_k U \otimes B_k^T)|EPR\rangle$$

Apply on EPR and "OR lemma" attack

Potential constructions

Single Query

$$A_k U B_k$$

$$(A_k U B_k \otimes I)|EPR\rangle = (A_k U \otimes B_k^T)|EPR\rangle$$

Apply on EPR and "OR lemma" attack

Potential constructions

Single Query

$$A_k U B_k$$

$$(A_k U B_k \otimes I)|EPR\rangle = (A_k U \otimes B_k^T)|EPR\rangle$$

Apply on EPR and "OR lemma" attack

Parallel Query

$$A_k \, U^{\otimes s} \, B_k$$

Potential constructions

Single Query

$$A_k\, U\, B_k$$

$$(A_k U B_k \otimes I)|EPR\rangle = (A_k U \otimes B_k^T)|EPR\rangle$$

Apply on EPR and "OR lemma" attack

Parallel Query

$$A_k\, U^{\otimes s}\, B_k$$

$$(A_k U^{\otimes s} B_k \otimes I)|EPR\rangle = (A_k U^{\otimes s} \otimes B_k^T)|EPR\rangle$$

Potential constructions

Single Query

$$A_k\, U\, B_k$$

$$(A_k U B_k \otimes I)|EPR\rangle = (A_k U \otimes B_k^T)|EPR\rangle$$

Apply on EPR and "OR lemma" attack

Parallel Query

$$A_k\, U^{\otimes s}\, B_k$$

$$(A_k U^{\otimes s} B_k \otimes I)|EPR\rangle = (A_k U^{\otimes s} \otimes B_k^T)|EPR\rangle$$

Apply on EPR and "OR lemma" attack

Potential constructions

Single Query

$$A_k U B_k$$

$$(A_k U B_k \otimes I)|EPR\rangle = (A_k U \otimes B_k^T)|EPR\rangle$$

Apply on EPR and "OR lemma" attack

Parallel Query

$$A_k U^{\otimes s} B_k$$

$$(A_k U^{\otimes s} B_k \otimes I)|EPR\rangle = (A_k U^{\otimes s} \otimes B_k^T)|EPR\rangle$$

Apply on EPR and "OR lemma" attack

Potential constructions

Single Query

$$A_k U B_k$$

$$(A_k U B_k \otimes I)|EPR\rangle = (A_k U \otimes B_k^T)|EPR\rangle$$

Apply on EPR and "OR lemma" attack

Parallel Query

$$A_k U^{\otimes s} B_k$$

$$(A_k U^{\otimes s} B_k \otimes I)|EPR\rangle = (A_k U^{\otimes s} \otimes B_k^T)|EPR\rangle$$

Apply on EPR and "OR lemma" attack

Unprotected Query

$$U\ A_k\ U$$

Potential constructions

Single Query

$$A_k U B_k$$

$$(A_k U B_k \otimes I)|EPR\rangle \; = \; (A_k U \otimes B_k^T)|EPR\rangle$$

Apply on EPR and "OR lemma" attack

Parallel Query

$$A_k U^{\otimes s} B_k$$

$$(A_k U^{\otimes s} B_k \otimes I)|EPR\rangle \; = \; (A_k U^{\otimes s} \otimes B_k^T)|EPR\rangle$$

Apply on EPR and "OR lemma" attack

Unprotected Query

$$U \, A_k \, U$$

$$U^\dagger (U \, A_k \, U) U^\dagger \; = \; A_k$$

Potential constructions

Single Query

$$A_k U B_k$$

$$(A_k U B_k \otimes I)|EPR\rangle = (A_k U \otimes B_k^T)|EPR\rangle$$

Apply on EPR and "OR lemma" attack

Parallel Query

$$A_k U^{\otimes s} B_k$$

$$(A_k U^{\otimes s} B_k \otimes I)|EPR\rangle = (A_k U^{\otimes s} \otimes B_k^T)|EPR\rangle$$

Apply on EPR and "OR lemma" attack

Unprotected Query

$$U\, A_k\, U$$

$$U^\dagger (U\, A_k\, U) U^\dagger = A_k$$

Apply on $U^\dagger$ and Learn A_k

Potential constructions

Single Query

$$A_k U B_k$$

$$(A_k U B_k \otimes I)|EPR\rangle = (A_k U \otimes B_k^T)|EPR\rangle$$

Apply on EPR and "OR lemma" attack

Parallel Query

$$A_k U^{\otimes s} B_k$$

$$(A_k U^{\otimes s} B_k \otimes I)|EPR\rangle = (A_k U^{\otimes s} \otimes B_k^T)|EPR\rangle$$

Apply on EPR and "OR lemma" attack

Unprotected Query

$$U A_k U$$

$$U^\dagger (U A_k U) U^\dagger = A_k$$

Apply on $U^\dagger$ and Learn A_k

Potential constructions

Single Query

$$A_k U B_k$$

$(A_k U B_k \otimes I)|EPR\rangle = (A_k U \otimes B_k^T)|EPR\rangle$

Apply on EPR and "OR lemma" attack

Parallel Query

$$A_k U^{\otimes s} B_k$$

$(A_k U^{\otimes s} B_k \otimes I)|EPR\rangle = (A_k U^{\otimes s} \otimes B_k^T)|EPR\rangle$

Apply on EPR and "OR lemma" attack

Unprotected Query

$$U A_k U$$

$U^\dagger (U A_k U) U^\dagger = A_k$

Apply on $U^\dagger$ and Learn A_k

Two Query

$$A_k U B_k U C_k$$

Potential constructions

Single Query

$$A_k U B_k$$

$$(A_k U B_k \otimes I)|EPR\rangle = (A_k U \otimes B_k^T)|EPR\rangle$$

Apply on EPR and "OR lemma" attack

Parallel Query

$$A_k U^{\otimes s} B_k$$

$$(A_k U^{\otimes s} B_k \otimes I)|EPR\rangle = (A_k U^{\otimes s} \otimes B_k^T)|EPR\rangle$$

Apply on EPR and "OR lemma" attack

Unprotected Query

$$U A_k U$$

$$U^\dagger (U A_k U) U^\dagger = A_k$$

Apply on $U^\dagger$ and Learn A_k

Two Query

$$A_k U B_k U C_k$$

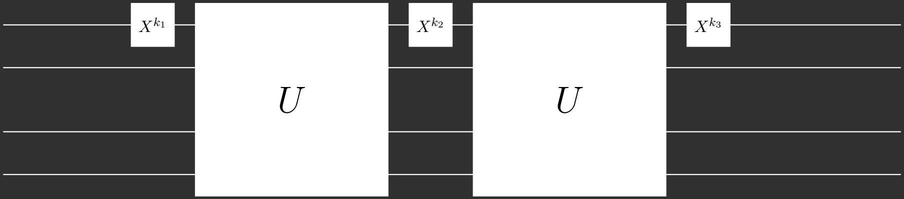
No easy way to attack

PRU in QHROM

PRU in QHROM : $G^U(k_1||k_2||k_3) = X^{k_3}UX^{k_2}UX^{k_1}$

PRU in QHROM

PRU in QHROM : $G^U(k_1||k_2||k_3) = X^{k_3} U X^{k_2} U X^{k_1}$



PRU in QHROM

$$U \leftarrow \mu_n$$

$$\rho_{\mathsf{AB}}^{\mathcal{A}} = \mathop{\mathbb{E}}_{\substack{U \leftarrow \mu_n \\ k \leftarrow \{0,1\}^\lambda}} \left[|\mathcal{A}^{U,U^\dagger,G_k^U}\rangle\langle\mathcal{A}^{U,U^\dagger,G_k^U}|_{\mathsf{AB}} \right]$$

Very hard to understand this state.

PRU in QHROM

$$U \leftarrow \mu_n$$

$$\rho_{\mathsf{AB}}^{\mathcal{A}} = \mathop{\mathbb{E}}_{\substack{U \leftarrow \mu_n \\ k \leftarrow \{0,1\}^\lambda}} \left[|\mathcal{A}^{U,U^\dagger,G_k^U}\rangle\langle\mathcal{A}^{U,U^\dagger,G_k^U}|_{\mathsf{AB}} \right]$$

Very hard to understand this state.

PRU in QHROM

$$U \leftarrow \mu_n$$

$$\rho_{\mathsf{AB}}^{\mathcal{A}} = \mathop{\mathbb{E}}_{\substack{U \leftarrow \mu_n \\ k \leftarrow \{0,1\}^\lambda}} \left[|\mathcal{A}^{U,U^\dagger,G_k^U}\rangle\langle\mathcal{A}^{U,U^\dagger,G_k^U}|_{\mathsf{AB}} \right]$$

Very hard to understand this state.

Techniques

Path Recording framework

[MH24]

Purification

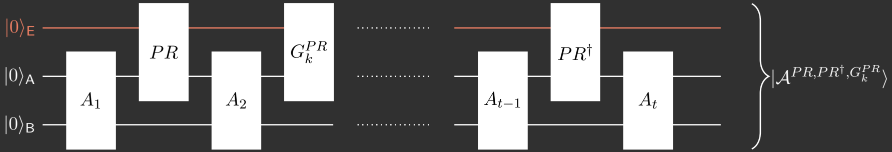
$$U \leftarrow \mu_n$$

$$\rho_{\mathsf{AB}}^{\mathcal{A}} = \mathop{\mathbb{E}}_{\substack{U \leftarrow \mu_n \\ k \leftarrow \{0,1\}^\lambda}} \left[|\mathcal{A}^{U,U^\dagger,G_k^U}\rangle\langle\mathcal{A}^{U,U^\dagger,G_k^U}|_{\mathsf{AB}} \right]$$

By Schmidt decomposition, for some $|\psi_{\mathcal{A}}\rangle$

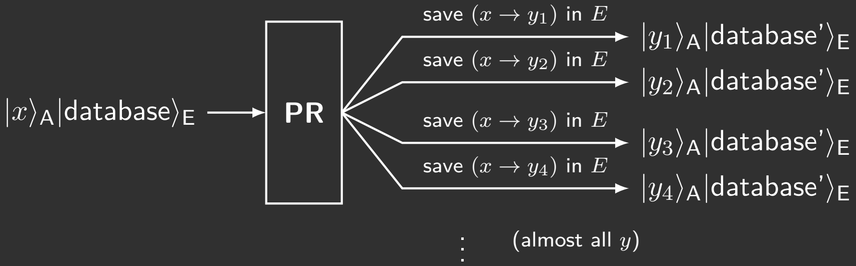
$$\rho_{\mathsf{AB}}^{\mathcal{A}} = Tr_{\mathsf{E}} \left(|\psi_{\mathcal{A}}\rangle\langle\psi_{\mathcal{A}}|_{\mathsf{ABE}} \right)$$

Compressed Purification



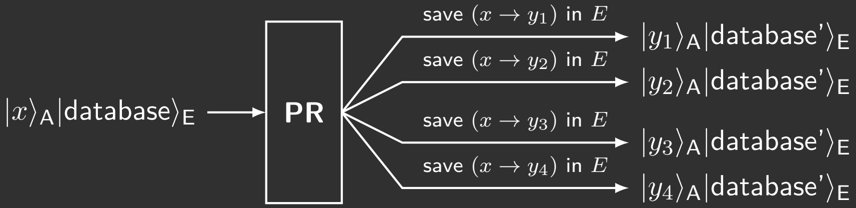
$$\mathop{\mathbb{E}}_{U \leftarrow \mu_n}\left[|\mathcal{A}^{U,U^\dagger,G_k^U}\rangle\langle\mathcal{A}^{U,U^\dagger,G_k^U}|_{\mathsf{AB}}\right] \approx Tr_{\mathsf{E}}\left(|\mathcal{A}^{PR,PR^\dagger,G_k^{PR}}\rangle\langle\mathcal{A}^{PR,PR^\dagger,G_k^{PR}}|_{\mathsf{ABE}}\right)$$

Path Recording



$$\mathsf{PR}_{\mathsf{AE}} : |x\rangle_{\mathsf{A}}|R\rangle_{\mathsf{E}} \mapsto \frac{1}{\sqrt{N-|R|}} \sum_{\substack{y\in[N],\\ y\notin \mathrm{Im}(R)}} |y\rangle_{\mathsf{A}}\underbrace{|R \cup \{(x,y)\}\rangle_{\mathsf{E}}}_{\text{Path}}.$$

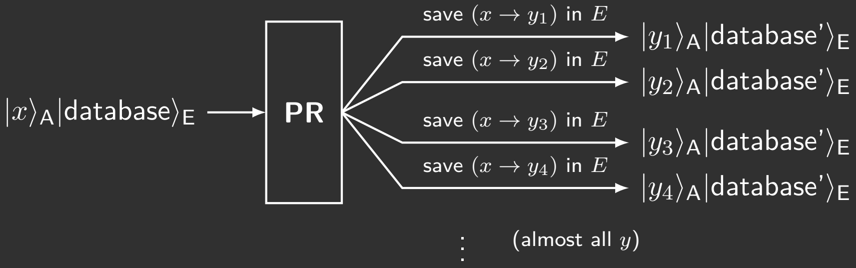
Path Recording



$\vdots$ (almost all y)

$$\mathsf{PR}_{\mathsf{AE}} : |x\rangle_{\mathsf{A}}|R\rangle_{\mathsf{E}} \mapsto \frac{1}{\sqrt{N - |R|}} \sum_{\substack{y\in[N],\\ y\notin \mathrm{Im}(R)}} |y\rangle_{\mathsf{A}}\underbrace{|R \cup \{(x,y)\}\rangle_{\mathsf{E}}}_{\text{Path}}.$$

Path Recording



$$\mathrm{PR}_{\mathsf{AE}} : |x\rangle_{\mathsf{A}}|R\rangle_{\mathsf{E}} \mapsto \frac{1}{\sqrt{N-|R|}} \sum_{\substack{y\in[N],\\ y\notin \mathrm{Im}(R)}} |y\rangle_{\mathsf{A}} \underbrace{|R \cup \{(x,y)\}\rangle_{\mathsf{E}}}_{\text{Path}} .$$

Techniques

Analysing our construction

Ideal vs Real

Ideal

- First oracle: U_1
- Second oracle: U_2
- Purification is Two "Paths"
- $|\text{Path}_1\rangle \otimes |\text{Path}_2\rangle$

Real

- First oracle: U
- Second oracle: $X^{k_3} U X^{k_2} U X^{k_1}$
- Purification is one "Path" and Keys
- $|\text{Path}\rangle \otimes |\text{Keys}\rangle$

Key Simulator $\mathcal{I}^{\mathsf{Sim}}$

Ideal vs Real

Ideal

- First oracle: U_1
- Second oracle: U_2
- Purification is Two "Paths"
- $|\text{Path}_1\rangle \otimes |\text{Path}_2\rangle$

Real

- First oracle: U
- Second oracle: $X^{k_3} U X^{k_2} U X^{k_1}$
- Purification is one "Path" and Keys
- $|\text{Path}\rangle \otimes |\text{Keys}\rangle$

Key Simulator $\mathcal{I}^{\text{Sim}}$

Ideal vs Real

Ideal

- First oracle: U_1
- Second oracle: U_2
- Purification is Two "Paths"
- $|\text{Path}_1\rangle \otimes |\text{Path}_2\rangle$

Real

- First oracle: U
- Second oracle: $X^{k_3} U X^{k_2} U X^{k_1}$
- Purification is one "Path" and Keys
- $|\text{Path}\rangle \otimes |\text{Keys}\rangle$

Key Simulator $\mathcal{I}^{\text{Sim}}$

Ideal vs Real

Ideal

- First oracle: U_1
- Second oracle: U_2
- Purification is Two "Paths"
- $|\text{Path}_1\rangle \otimes |\text{Path}_2\rangle$

Real

- First oracle: U
- Second oracle: $X^{k_3} U X^{k_2} U X^{k_1}$
- Purification is one "Path" and Keys
- $|\text{Path}\rangle \otimes |\text{Keys}\rangle$

Key Simulator $\mathcal{I}^{\text{Sim}}$

Ideal vs Real

Ideal

- First oracle: U_1
- Second oracle: U_2
- Purification is Two "Paths"
- $|\text{Path}_1\rangle \otimes |\text{Path}_2\rangle$

Real

- First oracle: U
- Second oracle: $X^{k_3} U X^{k_2} U X^{k_1}$
- Purification is one "Path" and Keys
- $|\text{Path}\rangle \otimes |\text{Keys}\rangle$

Key Simulator $\mathcal{I}^{\mathsf{Sim}}$

Ideal vs Real

Ideal

- First oracle: U_1
- Second oracle: U_2
- Purification is Two "Paths"
- $|\text{Path}_1\rangle \otimes |\text{Path}_2\rangle$

Real

- First oracle: U
- Second oracle: $X^{k_3} U X^{k_2} U X^{k_1}$
- Purification is one "Path" and Keys
- $|\text{Path}\rangle \otimes |\text{Keys}\rangle$

Key Simulator $\mathcal{I}^{\mathsf{Sim}}$

Ideal vs Real

Ideal

- First oracle: U_1
- Second oracle: U_2
- Purification is Two "Paths"
- $|\text{Path}_1\rangle \otimes |\text{Path}_2\rangle$

Real

- First oracle: U
- Second oracle: $X^{k_3} U X^{k_2} U X^{k_1}$
- Purification is one "Path" and Keys
- $|\text{Path}\rangle \otimes |\text{Keys}\rangle$

Key Simulator $\mathcal{I}^{\text{Sim}}$

Ideal vs Real

Ideal

- First oracle: U_1
- Second oracle: U_2
- Purification is Two "Paths"
- $|\text{Path}_1\rangle \otimes |\text{Path}_2\rangle$

Real

- First oracle: U
- Second oracle: $X^{k_3} U X^{k_2} U X^{k_1}$
- Purification is one "Path" and Keys
- $|\text{Path}\rangle \otimes |\text{Keys}\rangle$

Key Simulator $\mathcal{I}^{\mathsf{Sim}}$

Ideal vs Real

Ideal

- First oracle: U_1
- Second oracle: U_2
- Purification is Two "Paths"
- $|\mathsf{Path}_1\rangle \otimes |\mathsf{Path}_2\rangle$

Real

- First oracle: U
- Second oracle: $X^{k_3} U X^{k_2} U X^{k_1}$
- Purification is one "Path" and Keys
- $|\mathsf{Path}\rangle \otimes |\mathsf{Keys}\rangle$

Key Simulator $\mathcal{I}^{\mathsf{Sim}}$

Ideal vs Real

Ideal

- First oracle: U_1
- Second oracle: U_2
- Purification is Two "Paths"
- $|\text{Path}_1\rangle \otimes |\text{Path}_2\rangle$

Real

- First oracle: U
- Second oracle: $X^{k_3} U X^{k_2} U X^{k_1}$
- Purification is one "Path" and Keys
- $|\text{Path}\rangle \otimes |\text{Keys}\rangle$

Key Simulator $\mathcal{I}^{\mathsf{Sim}}$

Ideal Experiment

First Oracle

$$|\text{Path}_1\rangle \otimes |\text{Path}_2\rangle$$

$$\downarrow$$

first oracle

U_1

$$\downarrow$$

$$|\text{Path}_1 + \text{Entry}\rangle \otimes |\text{Path}_2\rangle$$

Second Oracle

$$|\text{Path}_1\rangle \otimes |\text{Path}_2\rangle$$

$$\downarrow$$

second oracle

U_2

$$\downarrow$$

$$|\text{Path}_1\rangle \otimes |\text{Path}_2 + \text{Entry}\rangle$$

Ideal Experiment

First Oracle

$$|\text{Path}_1\rangle \otimes |\text{Path}_2\rangle$$

$$\downarrow$$

$$\boxed{\begin{array}{c}\text{first oracle}\\ U_1\end{array}}$$

$$\downarrow$$

$$|\text{Path}_1 + \text{Entry}\rangle \otimes |\text{Path}_2\rangle$$

Second Oracle

$$|\text{Path}_1\rangle \otimes |\text{Path}_2\rangle$$

$$\downarrow$$

$$\boxed{\begin{array}{c}\text{second oracle}\\ U_2\end{array}}$$

$$\downarrow$$

$$|\text{Path}_1\rangle \otimes |\text{Path}_2 + \text{Entry}\rangle$$

Real Experiment

First Oracle

$|\text{Path}\rangle \otimes |\text{Keys}\rangle$

$\downarrow$

first oracle

U

$\downarrow$

$|\text{Path} + \text{entry}\rangle \otimes |\text{Keys}\rangle$

Second Oracle

$|\text{Path}\rangle \otimes |\text{Keys}\rangle$

$\downarrow$

second oracle

$X^{k_3} U X^{k_2} U X^{k_1}$

$\downarrow$

$|\text{Path} + \underbrace{\{\text{entry}_1, \text{entry}_2\}}_{}\rangle \otimes |\text{Keys}\rangle$

Entries Correlated by Keys

Real Experiment

First Oracle

$|\text{Path}\rangle \otimes |\text{Keys}\rangle$

$\downarrow$

first oracle
U

$\downarrow$

$|\text{Path} + \text{entry}\rangle \otimes |\text{Keys}\rangle$

Second Oracle

$|\text{Path}\rangle \otimes |\text{Keys}\rangle$

$\downarrow$

second oracle
$X^{k_3} U X^{k_2} U X^{k_1}$

$\downarrow$

$|\text{Path} + \{\text{entry}_1, \text{entry}_2\}\rangle \otimes |\text{Keys}\rangle$

Entries Correlated by Keys

Real Experiment

First Oracle

$|\text{Path}\rangle \otimes |\text{Keys}\rangle$

$\downarrow$

first oracle
U

$\downarrow$

$|\text{Path} + \text{entry}\rangle \otimes |\text{Keys}\rangle$

Second Oracle

$|\text{Path}\rangle \otimes |\text{Keys}\rangle$

$\downarrow$

second oracle
$X^{k_3} U X^{k_2} U X^{k_1}$

$\downarrow$

$|\text{Path} + \underline{\{\text{entry}_1, \text{entry}_2\}}\rangle \otimes |\text{Keys}\rangle$

Entries Correlated by Keys

Measuring Closeness

To prove closeness, we do Query-by-Query Analysis:

- Take any intermediate state
- The following two processes are close:
- Ideal Oracle query followed by Key Simulation
- Key Simulation followed by Real Oracle query

Measuring Closeness

To prove closeness, we do Query-by-Query Analysis:

- Take any intermediate state
- The following two processes are close:
- Ideal Oracle query followed by Key Simulation
- Key Simulation followed by Real Oracle query

Measuring Closeness

To prove closeness, we do Query-by-Query Analysis:

- Take any intermediate state
- The following two processes are close:
- Ideal Oracle query followed by Key Simulation
- Key Simulation followed by Real Oracle query

Measuring Closeness

To prove closeness, we do Query-by-Query Analysis:

- Take any intermediate state
- The following two processes are close:
- Ideal Oracle query followed by Key Simulation
- Key Simulation followed by Real Oracle query

Measuring Closeness

To prove closeness, we do Query-by-Query Analysis:

- Take any intermediate state
- The following two processes are close:
- Ideal Oracle query followed by Key Simulation
- Key Simulation followed by Real Oracle query

Progress Measure

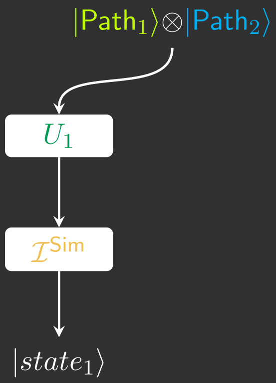
First Oracle

$|\text{Path}_1\rangle \otimes |\text{Path}_2\rangle$

Second Oracle

Progress Measure

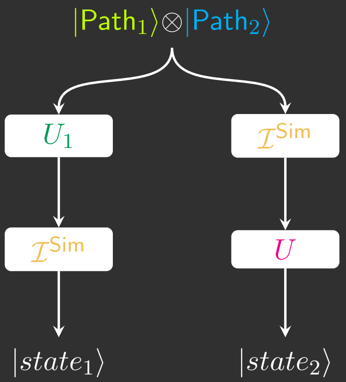
First Oracle



Second Oracle

Progress Measure

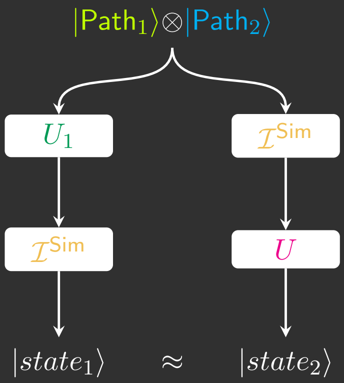
First Oracle



Second Oracle

Progress Measure

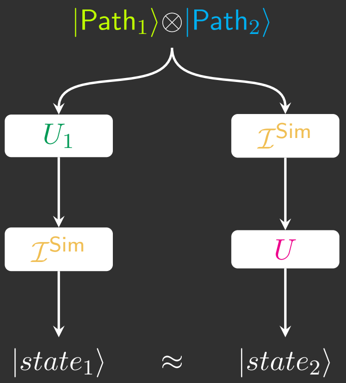
First Oracle



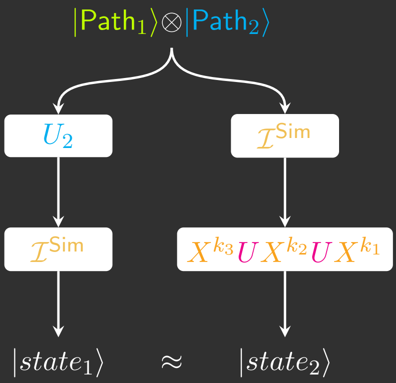
Second Oracle

Progress Measure

First Oracle



Second Oracle



Conclusions and open-problems

Results

- **Unbounded-poly-query secure strong PRUs in QHROM**
- **Strong Gluing Theorem for Haar Unitaries**
- **Shrinking strong PRU Keys for Free, in Plain Model**

Results

- **Unbounded-poly-query secure strong PRUs in QHROM**
- **Strong Gluing Theorem for Haar Unitaries**
- **Shrinking strong PRU Keys for Free, in Plain Model**

Results

- **Unbounded-poly-query secure strong PRUs in QHROM**
- **Strong Gluing Theorem for Haar Unitaries**
- **Shrinking strong PRU Keys for Free, in Plain Model**

Open Questions

- **Super-strong PRU in strong QHROM**
  Conjugate and Transpose to Haar oracle and PRU
- **LOCC in QHROM and blackbox separations**
  Partial results in a concurrent work
- **Instantiating QHROM**
- **Constructing Unclonable primitives in QHROM.**

Open Questions

- **Super-strong PRU in strong QHROM**
  Conjugate and Transpose to Haar oracle and PRU
- **LOCC in QHROM and blackbox separations**
  Partial results in a concurrent work
- **Instantiating QHROM**
- **Constructing Unclonable primitives in QHROM.**

Open Questions

- **Super-strong PRU in strong QHROM**
  Conjugate and Transpose to Haar oracle and PRU
- **LOCC in QHROM and blackbox separations**
  Partial results in a concurrent work
- **Instantiating QHROM**
- **Constructing Unclonable primitives in QHROM.**

Open Questions

- **Super-strong PRU in strong QHROM**
  Conjugate and Transpose to Haar oracle and PRU
- **LOCC in QHROM and blackbox separations**
  Partial results in a concurrent work
- **Instantiating QHROM**
- **Constructing Unclonable primitives in QHROM.**

Open Questions

- **Super-strong PRU in strong QHROM**
  Conjugate and Transpose to Haar oracle and PRU
- **LOCC in QHROM and blackbox separations**
  Partial results in a concurrent work
- **Instantiating QHROM**
- **Constructing Unclonable primitives in QHROM.**

Open Questions

- **Super-strong PRU in strong QHROM**
  Conjugate and Transpose to Haar oracle and PRU
- **LOCC in QHROM and blackbox separations**
  Partial results in a concurrent work
- **Instantiating QHROM**
- **Constructing Unclonable primitives in QHROM.**

Thank You