Pseudorandomness in the (Inverseless) Haar Random Oracle Model

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

Eurocrypt, 2025

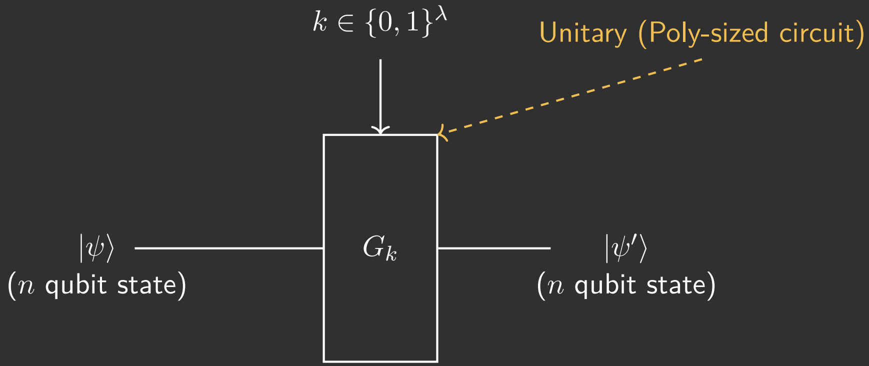
May 5, 2025

Pseudorandom Unitary (PRU)

Efficiently implementable circuits that “behave like” Haar random unitary.

Pseudorandom Unitary (PRU)

1. Efficient implementation:



Notation: n-PRU

Pseudorandom Unitary (PRU)

2. Psuedorandomness

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

Previous work

- (JLS18) defined PRU.
- (AGKL22,LQS+23,BM24) gave constructions on restricted inputs.
- (MPSY24,CBB+24) gave constructions for non-adaptive queries.
- (MH24) finally gave a construction for adaptive queries.

Defined Path-recording framework

Previous work

- (JLS18) defined PRU.
- (AGKL22,LQS+23,BM24) gave constructions on restricted inputs.
- (MPSY24,CBB+24) gave constructions for non-adaptive queries.
- (MH24) finally gave a construction for adaptive queries.

Defined Path-recording framework

Previous work

- (JLS18) defined PRU.
- (AGKL22,LQS+23,BM24) gave constructions on restricted inputs.
- (MPSY24,CBB+24) gave constructions for non-adaptive queries.
- (MH24) finally gave a construction for adaptive queries.

Defined Path-recording framework

Previous work

- (JLS18) defined PRU.
- (AGKL22,LQS+23,BM24) gave constructions on restricted inputs.
- (MPSY24,CBB+24) gave constructions for non-adaptive queries.
- (MH24) finally gave a construction for adaptive queries.

Defined Path-recording framework

Previous work

- (JLS18) defined PRU.
- (AGKL22,LQS+23,BM24) gave constructions on restricted inputs.
- (MPSY24,CBB+24) gave constructions for non-adaptive queries.
- (MH24) finally gave a construction for adaptive queries.

Defined Path-recording framework

Why Should We Care About PRUs?

- (AQY22,MY22,AGQY22,...) builds cryptography from PRU and PRS.
- **Kretschmer (Kre21)** showed evidence that:

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

Why Should We Care About PRUs?

- (AQY22,MY22,AGQY22,...) builds cryptography from PRU and PRS.
- **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?**
  - None ... until now?
  - Potentially build from random circuits

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?**
  - None... until now?
  - Potentially build from random circuits

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?**
  - None... until now?
  - Potentially build from random circuits

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?**
  - None... until now?
  - Potentially build from random circuits

Modelling random circuits as Haar unitaries

- [AQY21] hypothesised random circuits to be PRUs.
- [BHH16] polydepth circuits are t-design.
- [SHH24] low depth circuits are $poly$-design as long as local gates act on $\log$ number of qubits.
  - Sampling this is
  - We can sample once and make it publically accessible

Modelling random circuits as Haar unitaries

- [AQY21] hypothesised random circuits to be PRUs.
- [BHH16] polydepth circuits are t-design.
- [SHH24] low depth circuits are $poly$-design as long as local gates act on $\log$ number of qubits.

Modelling random circuits as Haar unitaries

- [AQY21] hypothesised random circuits to be PRUs.
- [BHH16] polydepth circuits are t-design.
- [SHH24] low depth circuits are $poly$-design as long as local gates act on $\log$ number of qubits.
  - Sampling this is inefficient
  - We can sample once and make it publically accesible

Modelling random circuits as Haar unitaries

- [AQY21] hypothesised random circuits to be PRUs.
- [BHH16] polydepth circuits are t-design.
- [SHH24] low depth circuits are $poly$-design as long as local gates act on $\log$ number of qubits.
  - Sampling this is inefficient
  - We can sample once and make it publically accesible

Modelling random circuits as Haar unitaries

- [AQY21] hypothesised random circuits to be PRUs.
- [BHH16] polydepth circuits are t-design.
- [SHH24] low depth circuits are $poly$-design as long as local gates act on $\log$ number of qubits.
  - Sampling this is inefficient
  - We can sample once and make it publically accesible

Quantum Haar Random Oracle Model

[BFV20, CM21, ABGL24]

Quantum Haar Random Oracle Model (QHROM)

Introduced by (BFV20, CM21), but were unable to get provable results.

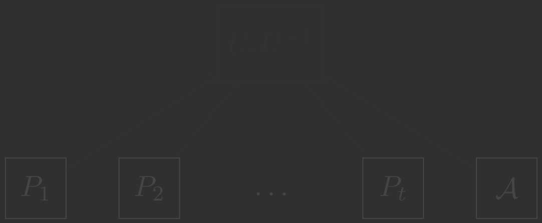
All parties P_i as well as the adversary $\mathcal{A}$ get oracle access to a Haar Unitary and its inverse.

$$U \leftarrow \mu_n$$

Quantum Haar Random Oracle Model (QHROM)

Introduced by (BFV20, CM21), but were unable to get provable results. All parties P_i as well as the adversary $\mathcal{A}$ get oracle access to a Haar Unitary and its inverse.

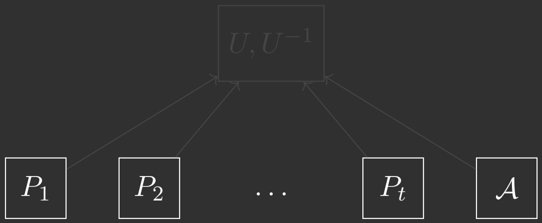
$$U \leftarrow \mu_n$$



Quantum Haar Random Oracle Model (QHROM)

Introduced by (BFV20, CM21), but were unable to get provable results. All parties P_i as well as the adversary $\mathcal{A}$ get oracle access to a Haar Unitary and its inverse.

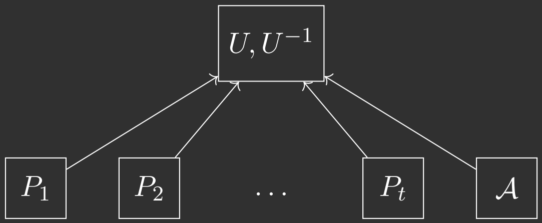
$$U \leftarrow \mu_n$$



Quantum Haar Random Oracle Model (QHROM)

Introduced by (BFV20, CM21), but were unable to get provable results. All parties P_i as well as the adversary $\mathcal{A}$ get oracle access to a Haar Unitary and its inverse.

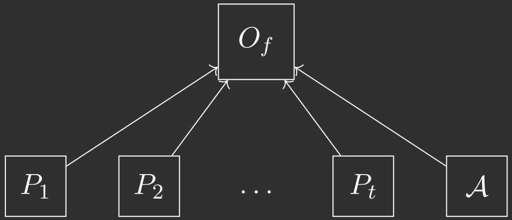
$$U \leftarrow \mu_n$$



Similarity to QROM

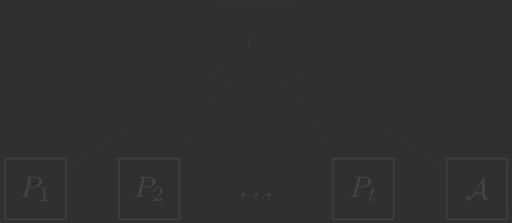
This model is similar to the Quantum Random Oracle Model (QROM) where all parties and the adversary get access to a random function oracle.

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



All parties P_i as well as the adversary $\mathcal{A}$ get oracle access to a Haar Unitary and but not its inverse.

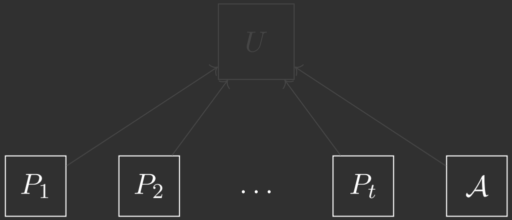
$$U \leftarrow \mu_n$$



iQHROM (inverseless)

All parties P_i as well as the adversary $\mathcal{A}$ get oracle access to a Haar Unitary and but not its inverse.

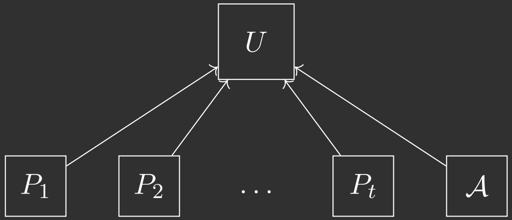
$$U \leftarrow \mu_n$$



iQHROM (inverseless)

All parties P_i as well as the adversary $\mathcal{A}$ get oracle access to a Haar Unitary and but not its inverse.

$$U \leftarrow \mu_n$$



Consequences of iQHROM

- Make progress towards results in QHROM and from random circuits.
- Results give a pathway to get PRU results in the plain model.
- Potentially help show separations.

Consequences of iQHROM

- Make progress towards results in QHROM and from random circuits.
- Results give a pathway to get PRU results in the plain model.
- Potentially help show separations.

Consequences of iQHROM

- Make progress towards results in QHROM and from random circuits.
- Results give a pathway to get PRU results in the plain model.
- Potentially help show separations.

Results

Our Contributions

- **Unbounded-query secure PRUs in iQHROM:**
  Achieved with **two queries** to the Haar random oracle.
- **Impossibility of single-query PRUs in iQHROM:**
  No construction with **one query** to the Haar random oracle.
- **Constructing PRSGs and PRFSs in iQHROM:**
  Achieved with **one query** to the Haar random oracle.

Our Contributions

- **Unbounded-query secure PRUs in iQHROM:**
  Achieved with **two queries** to the Haar random oracle.
- **Impossibility of single-query PRUs in iQHROM:**
  No construction with **one query** to the Haar random oracle.
- **Constructing PRSGs and PRFSs in iQHROM:**
  Achieved with **one query** to the Haar random oracle.

Our Contributions

- **Unbounded-query secure PRUs in iQHROM:**
  Achieved with **two queries** to the Haar random oracle.
- **Impossibility of single-query PRUs in iQHROM:**
  No construction with **one query** to the Haar random oracle.
- **Constructing PRSGs and PRFSs in iQHROM:**
  Achieved with **one query** to the Haar random oracle.

Plain Model Implications

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

Plain Model Implications

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

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

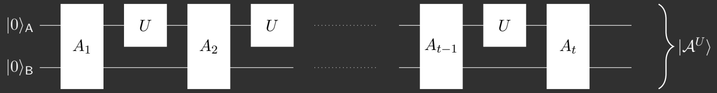
Plain Model Implications

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

Techniques

Primitive in iQHROM

$$U \leftarrow \mu_n$$

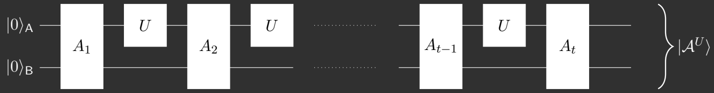


$$\rho^{\mathcal{A}}_{\mathsf{AB}} = \mathop{\mathbb{E}}_{U \leftarrow \mu_n} \left[|\mathcal{A}^U\rangle\langle\mathcal{A}^U|_{\mathsf{AB}} \right]$$

Very hard to understand this state.

Primitive in iQHROM

$$U \leftarrow \mu_n$$



$$\rho^{\mathcal{A}}_{\mathsf{AB}} = \mathop{\mathbb{E}}_{U \leftarrow \mu_n} \left[|\mathcal{A}^U\rangle\langle\mathcal{A}^U|_{\mathsf{AB}} \right]$$

Very hard to understand this state.

Primitive in iQHROM

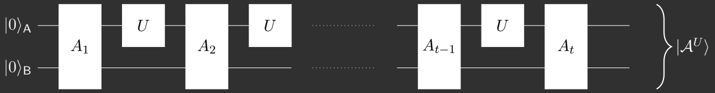
$$U \leftarrow \mu_n$$

$$\rho^{\mathcal{A}}_{\mathsf{AB}} = \underline{\mathop{\mathbb{E}}_{U \leftarrow \mu_n} \left[|\mathcal{A}^U\rangle\langle\mathcal{A}^U|_{\mathsf{AB}} \right]}$$

Very hard to understand this state.

Purification

$$U \leftarrow \mu_n$$



$$\rho^{\mathcal{A}}_{\mathsf{AB}} = \mathop{\mathbb{E}}_{U \leftarrow \mu_n} \left[|\mathcal{A}^U\rangle\langle\mathcal{A}^U|_{\mathsf{AB}} \right]$$

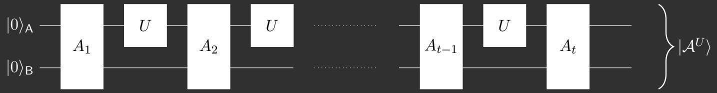
Not unique and still hard to find

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

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

Purification

$$U \leftarrow \mu_n$$



$$\rho^{\mathcal{A}}_{AB} = \mathop{\mathbb{E}}_{U \leftarrow \mu_n} \left[|\mathcal{A}^U\rangle\langle\mathcal{A}^U|_{AB} \right]$$

Not unique and still hard to find

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

$$\rho^{\mathcal{A}}_{AB} = Tr_E \left(|\psi_{\mathcal{A}}\rangle\langle\psi_{\mathcal{A}}|_{ABE} \right)$$

Path Recording framework

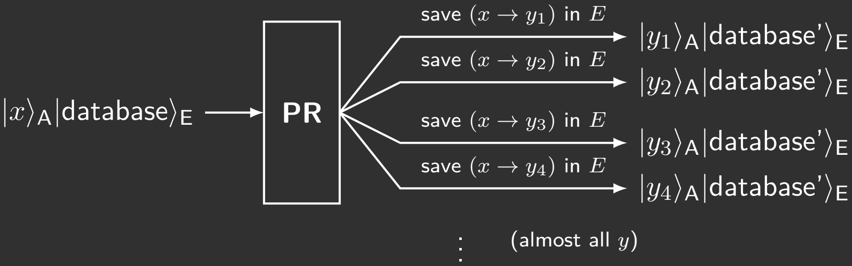
[MH24]

Compressed Purification

AIM: Find a state close to the purification:

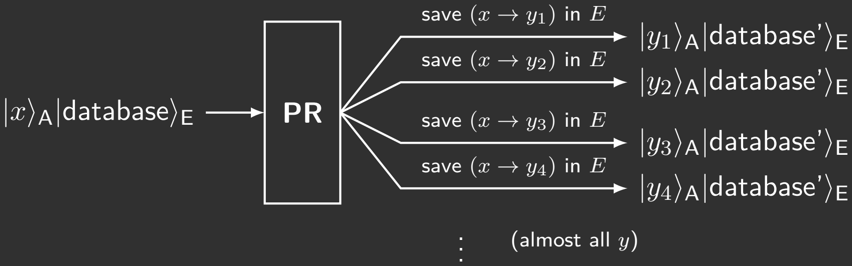
$$\underset{U\leftarrow\mu_n}{\mathbb{E}}\left[|\mathcal{A}^U\rangle\langle\mathcal{A}^U|_{\mathsf{AB}}\right] \approx Tr_{\mathsf{E}}\left(|\mathcal{A}^{PR}\rangle\langle\mathcal{A}^{PR}|_{\mathsf{ABE}}\right)$$

Path Recording



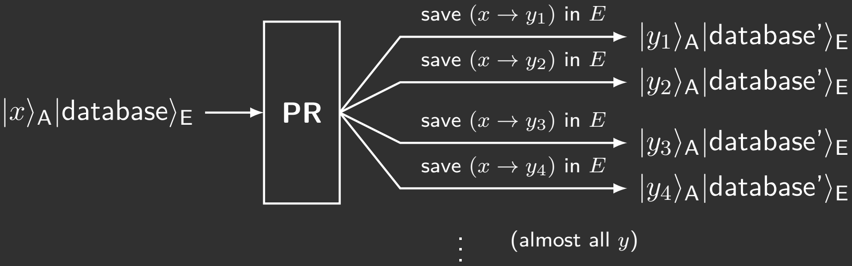
$$\mathrm{PR}_{\mathsf{AE}} : |x\rangle_{\mathsf{A}}|R\rangle_{\mathsf{E}} \mapsto \frac{1}{\sqrt{N-|R|}} \sum_{\substack{y\in[N],\\ y\notin \mathrm{Im}(R)}} |y\rangle_{\mathsf{A}} \underbrace{|R\cup\{(x,y)\}\rangle_{\mathsf{E}}}_{\text{Path}} .$$

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

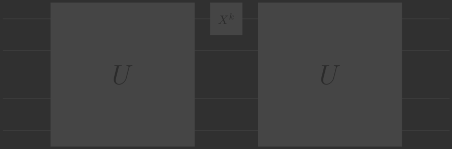


$$\mathrm{PR}_{AE} : |x\rangle_A|R\rangle_E \mapsto \frac{1}{\sqrt{N-|R|}} \sum_{\substack{y\in[N],\\ y\notin \mathrm{Im}(R)}} |y\rangle_A \underbrace{|R \cup \{(x,y)\}\rangle_E}_{\text{Path}} .$$

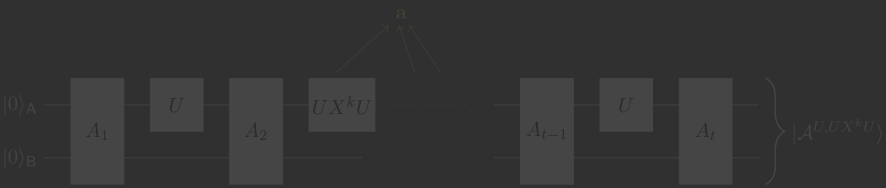
PRU in iQHROM

Analysis in iQHROM

PRU in iQHROM : $G^U(k) = UX^kU$

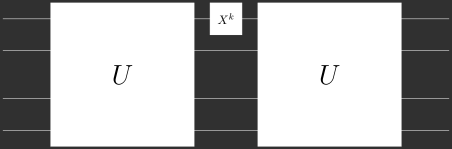


Adversaries state :

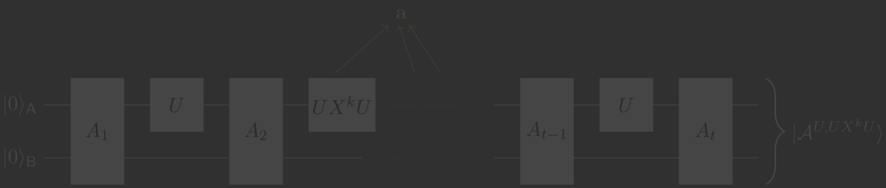


Analysis in iQHROM

PRU in iQHROM : $G^U(k) = UX^kU$

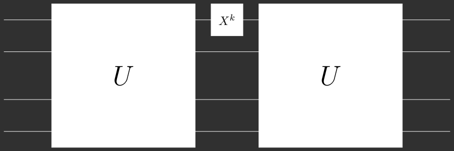


Adversaries state :

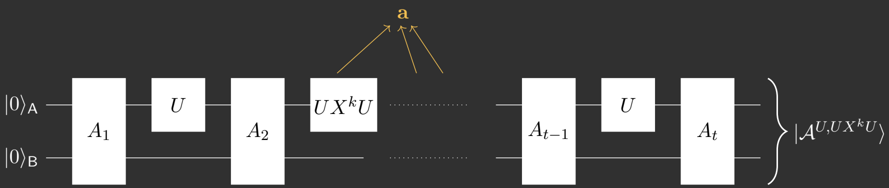


Analysis in iQHROM

PRU in iQHROM : $G^U(k) = UX^kU$



Adversaries state :



What does the purification look like?

Ideal

- U_1, U_2
- Separate "paths"
- (x^1, y^1) added to the first path
- (x^2, y^2) added to the second path
- $|\{(x^1, y^1)\}\rangle|\{(x^2, y^2)\}\rangle$

Real

- U, UX^kU
- Single combined path
- (x^1, y^1) added to the combined path
- $(x^2, z^2), (z^2 \oplus k, y^2)$ added to the combined path
- $|\{(x^1, y^1)\} \cup \{(x^2, z^2), (z^2 \oplus k, y^2)\}\rangle$

For most keys

What does the purification look like?

Ideal

- U_1, U_2
- Separate "paths"
- (x^1, y^1) added to the first path
- (x^2, y^2) added to the second path
- $|\{(x^1, y^1)\}\rangle|\{(x^2, y^2)\}\rangle$

Real

- U, UX^kU
- Single combined path
- (x^1, y^1) added to the combined path
- $(x^2, z^2), (z^2 \oplus k, y^2)$ added to the combined path
- $|\{(x^1, y^1)\} \cup \{(x^2, z^2), (z^2 \oplus k, y^2)\}\rangle$

For most keys

What does the purification look like?

Ideal

- U_1, U_2
- Separate "paths"
- (x^1, y^1) added to the first path
- (x^2, y^2) added to the second path
- $|\{(x^1, y^1)\}\rangle|\{(x^2, y^2)\}\rangle$

Real

- U, UX^kU
- Single combined path
- (x^1, y^1) added to the combined path
- $(x^2, z^2), (z^2 \oplus k, y^2)$ added to the combined path
- $|\{(x^1, y^1)\} \cup \{(x^2, z^2), (z^2 \oplus k, y^2)\}\rangle$

For most keys

What does the purification look like?

Ideal

- U_1, U_2
- Separate "paths"
- (x^1, y^1) added to the first path
- (x^2, y^2) added to the second path
- $|\{(x^1, y^1)\}\rangle|\{(x^2, y^2)\}\rangle$

Real

- U, UX^kU
- Single combined path
- (x^1, y^1) added to the combined path
- $(x^2, z^2), (z^2 \oplus k, y^2)$ added to the combined path
- $|\{(x^1, y^1)\} \cup \{(x^2, z^2), (z^2 \oplus k, y^2)\}\rangle$

For most keys

What does the purification look like?

Ideal

- U_1, U_2
- Separate "paths"
- (x^1, y^1) added to the first path
- (x^2, y^2) added to the second path
- $|\{(x^1, y^1)\}\rangle|\{(x^2, y^2)\}\rangle$

Real

- U, UX^kU
- Single combined path
- (x^1, y^1) added to the combined path
- $(x^2, z^2), (z^2 \oplus k, y^2)$ added to the combined path
- $|\{(x^1, y^1)\} \cup \{(x^2, z^2), (z^2 \oplus k, y^2)\}\rangle$

For most keys

What does the purification look like?

Ideal

- U_1, U_2
- Separate “paths”
- (x^1, y^1) added to the first path
- (x^2, y^2) added to the second path
- $|\{(x^1, y^1)\}\rangle|\{(x^2, y^2)\}\rangle$

Real

- U, UX^kU
- Single combined path
- (x^1, y^1) added to the combined path
- $(x^2, z^2), (z^2 \oplus k, y^2)$ added to the combined path
- $|\{(x^1, y^1)\} \cup \{(x^2, z^2), (z^2 \oplus k, y^2)\}\rangle$

For most keys

What does the purification look like?

Ideal

- U_1, U_2
- Separate "paths"
- (x^1, y^1) added to the first path
- (x^2, y^2) added to the second path
- $|\{(x^1, y^1)\}\rangle|\{(x^2, y^2)\}\rangle$

Real

- U, UX^kU
- Single combined path
- (x^1, y^1) added to the combined path
- $(x^2, z^2), (z^2 \oplus k, y^2)$ added to the combined path
- $|\{(x^1, y^1)\}\cup\{(x^2, z^2), (z^2 \oplus k, y^2)\}\rangle$

For most keys

Real experiment close to Ideal experiment

Ideal:

$$\sum_{\vec{x},\vec{y}} |\phi_{\vec{x},\vec{y}}\rangle_{\mathsf{AB}} \otimes$$

$$|\{(x_i^1, y_i^1)\}_{i\in\mathbf{a}}\rangle_{\mathsf{E}_1} |\{(x_i^2, y_i^2)\}_{i\in\mathbf{b}}\rangle_{\mathsf{E}_2}$$

Isometry I for most keys

Real:

$$\sum_{\vec{x},\vec{y}} |\phi_{\vec{x},\vec{y}}\rangle_{\mathsf{AB}} \otimes$$

$$\sum_{k,\vec{z}} |\{(x_i^1, y_i^1)\}_{i\in\mathbf{b}} \cup \{(x_i^2, z_i^2), (z_i^2 \oplus k, y_i^2)\}_{i\in\mathbf{a}}\rangle_{\mathsf{E}_1} |k\rangle_{\mathsf{K}}$$

Real experiment close to Ideal experiment

Ideal:

$$\sum_{\vec{x},\vec{y}} |\phi_{\vec{x},\vec{y}}\rangle_{\mathsf{AB}} \otimes \, |\{(x_i^1, y_i^1)\}_{i\in\mathbf{a}}\rangle_{\mathsf{E}_1} |\{(x_i^2, y_i^2)\}_{i\in\mathbf{b}}\rangle_{\mathsf{E}_2}$$

Isometry I for most keys ↑

Real:

$$\sum_{\vec{x},\vec{y}} |\phi_{\vec{x},\vec{y}}\rangle_{\mathsf{AB}} \otimes \, \sum_{k,\vec{z}} |\{(x_i^1, y_i^1)\}_{i\in\mathbf{b}} \cup \{(x_i^2, z_i^2), (z_i^2 \oplus k, y_i^2)\}_{i\in\mathbf{a}}\rangle_{\mathsf{E}_1} |k\rangle_{\mathsf{K}}$$

Real experiment close to Ideal experiment

Ideal:

$$\sum_{\vec{x},\vec{y}} |\phi_{\vec{x},\vec{y}}\rangle_{\mathsf{AB}} \otimes$$

$$|\{(x_i^1, y_i^1)\}_{i\in\mathbf{a}}\rangle_{\mathsf{E}_1} |\{(x_i^2, y_i^2)\}_{i\in\mathbf{b}}\rangle_{\mathsf{E}_2}$$

Isometry I for most keys

Real:

$$\sum_{\vec{x},\vec{y}} |\phi_{\vec{x},\vec{y}}\rangle_{\mathsf{AB}} \otimes$$

Any isometry on purification doesn't change state

Ideal$\approx$ Real

$$\sum_{k,\vec{z}} |\{(x_i^1, y_i^1)\}_{i\in\mathbf{b}} \cup \{(x_i^2, z_i^2), (z_i^2 \oplus k, y_i^2)\}_{i\in\mathbf{a}}\rangle_{\mathsf{E}_1} |k\rangle_{\mathsf{K}}$$

Real experiment close to Ideal experiment

Ideal:

$$\sum_{\vec{x},\vec{y}} |\phi_{\vec{x},\vec{y}}\rangle_{\mathsf{AB}} \otimes$$

$$|\{(x_i^1, y_i^1)\}_{i\in\mathbf{a}}\rangle_{\mathsf{E}_1} |\{(x_i^2, y_i^2)\}_{i\in\mathbf{b}}\rangle_{\mathsf{E}_2}$$

Isometry I for most keys $\uparrow$

Real:

$$\sum_{\vec{x},\vec{y}} |\phi_{\vec{x},\vec{y}}\rangle_{\mathsf{AB}} \otimes$$

Any isometry on purification doesn't change state

Ideal$\approx$ Real

$$\sum_{k,\vec{z}} |\{(x_i^1, y_i^1)\}_{i\in\mathbf{b}} \cup \{(x_i^2, z_i^2), (z_i^2 \oplus k, y_i^2)\}_{i\in\mathbf{a}}\rangle_{\mathsf{E}_1} |k\rangle_{\mathsf{K}}$$

Real experiment close to Ideal experiment

Ideal:

$$\sum_{\vec{x},\vec{y}} |\phi_{\vec{x},\vec{y}}\rangle_{\mathsf{AB}} \otimes$$

$$|\{(x_i^1, y_i^1)\}_{i\in\mathbf{a}}\rangle_{\mathsf{E}_1} |\{(x_i^2, y_i^2)\}_{i\in\mathbf{b}}\rangle_{\mathsf{E}_2}$$

Isometry I for most keys

Real:

$$\sum_{\vec{x},\vec{y}} |\phi_{\vec{x},\vec{y}}\rangle_{\mathsf{AB}} \otimes$$

Any isometry on purification doesn't change state

Ideal $\approx$ Real

$$\sum_{k,\vec{z}} |\{(x_i^1, y_i^1)\}_{i\in\mathbf{b}} \cup \{(x_i^2, z_i^2), (z_i^2 \oplus k, y_i^2)\}_{i\in\mathbf{a}}\rangle_{\mathsf{E}_1} |k\rangle_{\mathsf{K}}$$

Results and open-problems

Our Contributions

- **Unbounded-query secure PRUs in iQHROM**
- **Impossibility of single-query PRUs in iQHROM**
- **Constructing PRSGs and PRFSs in iQHROM**
- **Shrinking PRU Keys for Free**

Our Contributions

- **Unbounded-query secure PRUs in iQHROM**
- **Impossibility of single-query PRUs in iQHROM**
- **Constructing PRSGs and PRFSs in iQHROM**
- **Shrinking PRU Keys for Free**

Our Contributions

- **Unbounded-query secure PRUs in iQHROM**
- **Impossibility of single-query PRUs in iQHROM**
- **Constructing PRSGs and PRFSs in iQHROM**
- **Shrinking PRU Keys for Free**

Our Contributions

- **Unbounded-query secure PRUs in iQHROM**
- **Impossibility of single-query PRUs in iQHROM**
- **Constructing PRSGs and PRFSs in iQHROM**
- **Shrinking PRU Keys for Free**

Open Questions and follow-up

- **Unbounded-query secure PRUs in QHROM**
  Follow-up [ABGL25] shows strong PRU exists in QHROM

- **LOCC for QHROM**: Useful for Black-Box Separations
  Follow-up [ACL25] shows LOCC* for nQHROM

- **Instantiating QHROM**

- **Intantiating (Kre21) oracle in QHROM**

Open Questions and follow-up

- **Unbounded-query secure PRUs in QHROM**
  Follow-up [ABGL25] shows strong PRU exists in QHROM
- **LOCC for QHROM**: Useful for Black-Box Separations
  Follow-up [AGL25] shows LOCC for iQHROM
- **Instantiating QHROM**
- **Intantiating (Kre21) oracle in QHROM**

Open Questions and follow-up

- **Unbounded-query secure PRUs in QHROM**
  Follow-up [ABGL25] shows strong PRU exists in QHROM
- **LOCC for QHROM**: Useful for Black-Box Separations
  Follow-up [AGL25] shows LOCC for iQHROM
- **Instantiating QHROM**
- **Intantiating (Kre21) oracle in QHROM**

Open Questions and follow-up

- **Unbounded-query secure PRUs in QHROM**
  Follow-up [ABGL25] shows strong PRU exists in QHROM
- **LOCC for QHROM**: Useful for Black-Box Separations
  Follow-up [AGL25] shows LOCC for iQHROM
- **Instantiating QHROM**
- **Intantiating (Kre21) oracle in QHROM**

Open Questions and follow-up

- **Unbounded-query secure PRUs in QHROM**
  Follow-up [ABGL25] shows strong PRU exists in QHROM
- **LOCC for QHROM**: Useful for Black-Box Separations
  Follow-up [AGL25] shows LOCC for iQHROM
- **Instantiating QHROM**
- **Intantiating (Kre21) oracle in QHROM**

Thank You