Workshop on pseudorandom unitaries

Fermi Ma

This workshop is about **pseudorandom unitaries (PRUs)**.

This workshop is about **pseudorandom unitaries (PRUs)**.

Definition [JLS18]: a **PRU** is a family of efficient n-qubit unitaries $\{U_k\}_{k\in[K]}$ such that no $\mathbf{poly}(n)$-time algorithm A can distinguish:

This workshop is about **pseudorandom unitaries (PRUs)**.

Definition [JLS18]: a **PRU** is a family of efficient n-qubit unitaries $\{U_k\}_{k\in[K]}$ such that no $\mathbf{poly}(n)$-time algorithm A can distinguish:

- $U = U_k$ for random $k \leftarrow [K]$, or

This workshop is about **pseudorandom unitaries (PRUs)**.

Definition [JLS18]: a **PRU** is a family of efficient n-qubit unitaries $\{U_k\}_{k \in [K]}$ such that no $\mathbf{poly}(n)$-time algorithm A can distinguish:

- $U = U_k$ for random $k \leftarrow [K]$, or
- $U =$ Haar-random unitary

This workshop is about **pseudorandom unitaries (PRUs)**.

Definition [JLS18]: a **PRU** is a family of efficient n-qubit unitaries $\{U_k\}_{k\in[K]}$ such that no $\mathrm{poly}(n)$-time algorithm A can distinguish:

- $U = U_k$ for random $k \leftarrow [K]$, or
- $U =$ Haar-random unitary

given **oracle access** to U.

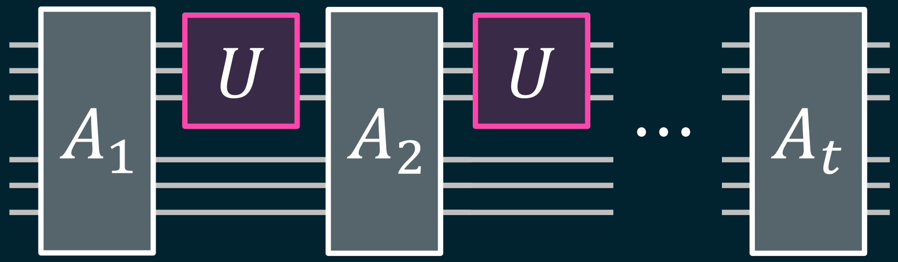
This workshop is about **pseudorandom unitaries (PRUs)**.

Definition [JLS18]: a **PRU** is a family of efficient n-qubit unitaries $\{U_k\}_{k \in [K]}$ such that no $\mathrm{poly}(n)$-time algorithm A can distinguish:

- $U = U_k$ for random $k \leftarrow [K]$, or
- $U =$ Haar-random unitary

given **oracle access** to U.

In [JLS18], this means:



Why study PRUs?

Why study PRUs?

- **Cryptography:** PRUs → commitments, uncloneable crypto, …
  [CM22,GJMZ23,LQSYZ23,…]

Why study PRUs?

- **Cryptography:** PRUs → commitments, uncloneable crypto, …
  [CM22,GJMZ23,LQSYZ23,…]

- **Quantum gravity:** model black-hole dynamics as a PRU
  [KP23,EFLVY24,YE24]

Why study PRUs?

- **Cryptography:** PRUs → commitments, uncloneable crypto, …
  [CM22,GJMZ23,LQSYZ23,…]
- **Quantum gravity:** model black-hole dynamics as a PRU
  [KP23,EFLVY24,YE24]
- **Learning**: low-depth PRUs → hardness of quantum learning

Why study PRUs?

- **Cryptography:** PRUs → commitments, uncloneable crypto, …
  [CM22,GJMZ23,LQSYZ23,…]

- **Quantum gravity:** model black-hole dynamics as a PRU
  [KP23,EFLVY24,YE24]

- **Learning**: low-depth PRUs → hardness of quantum learning

- **Algorithms:** low-depth PRUs → faster quantum algorithms

Open question: do PRUs exist? (under cryptographic assumptions)

Open question: do PRUs exist? (under cryptographic assumptions)

Prior work: PRUs secure against **restricted** adversaries

Open question: do PRUs exist? (under cryptographic assumptions)

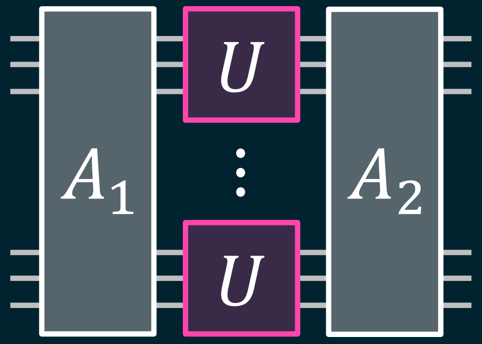
Prior work: PRUs secure against **restricted** adversaries

- [LQSYZ23,AGKL23,BM24]: non-adaptive + restricted input states

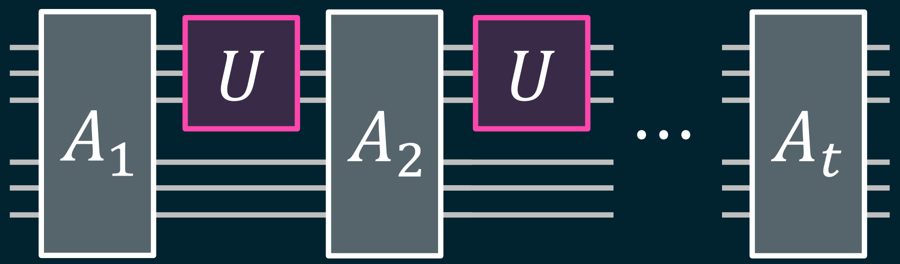
Open question: do PRUs exist? (under cryptographic assumptions)

Prior work: PRUs secure against **restricted** adversaries

- [LQSYZ23,AGKL23,BM24]: non-adaptive + restricted input states



non-adaptive

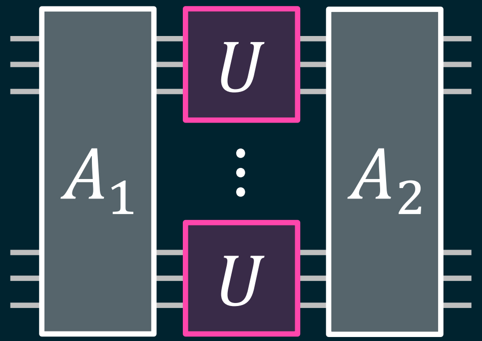


adaptive

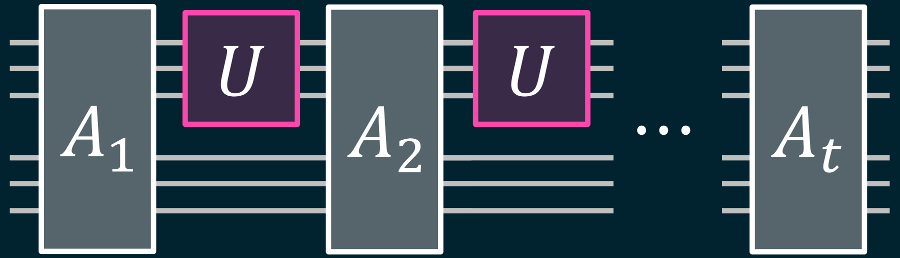
Open question: do PRUs exist? (under cryptographic assumptions)

Prior work: PRUs secure against **restricted** adversaries

- [LQSYZ23,AGKL23,BM24]: non-adaptive + restricted input states
- [MPSY24]: adaptive + restricted input states



non-adaptive

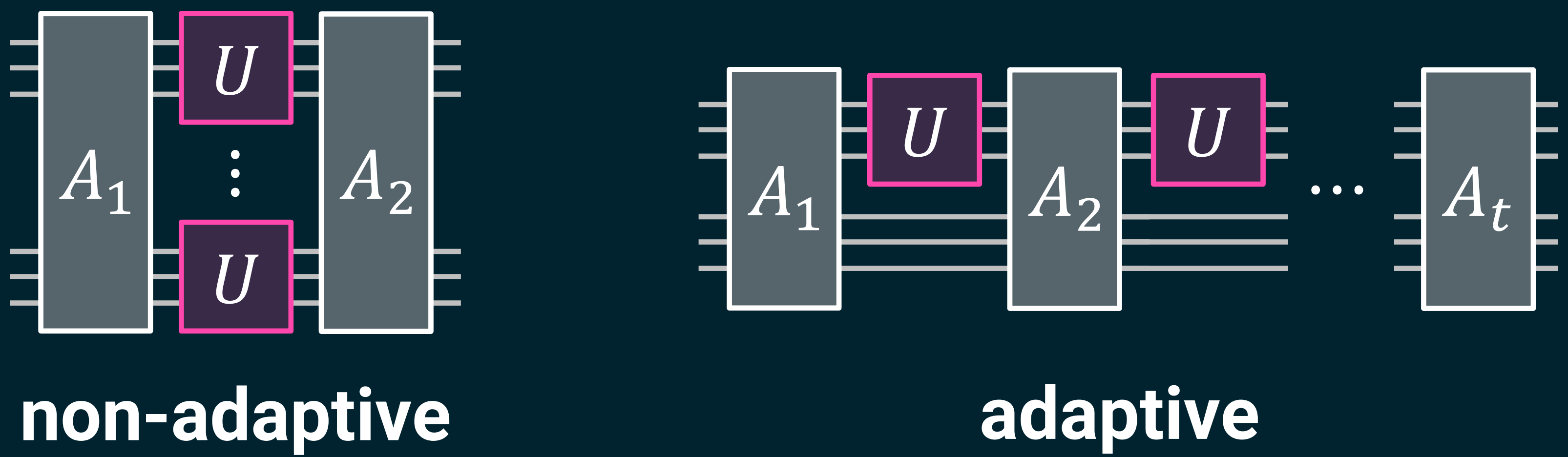


adaptive

Open question: do PRUs exist? (under cryptographic assumptions)

Prior work: PRUs secure against **restricted** adversaries

- [LQSYZ23,AGKL23,BM24]: non-adaptive + restricted input states
- [MPSY24]: adaptive + restricted input states
- [MPSY24,CBBDHX24]: non-adaptive



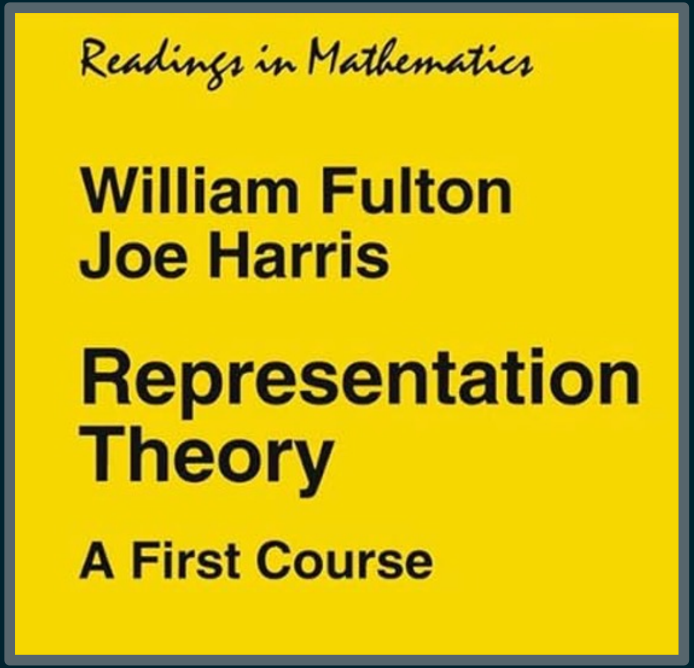
Why has it been so hard to build a PRU?

Why has it been so hard to build a PRU?

One reason: the math behind Haar-random unitaries is quite subtle!

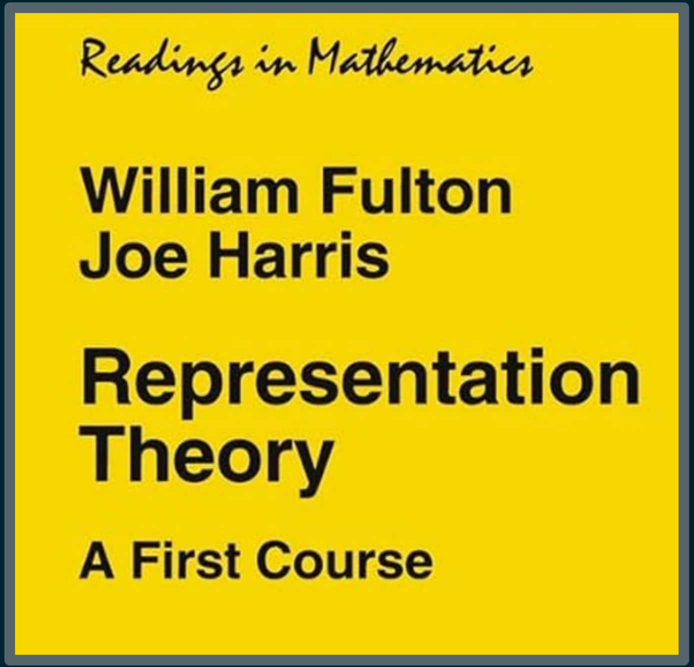
Why has it been so hard to build a PRU?

One reason: the math behind Haar-random unitaries is quite subtle!



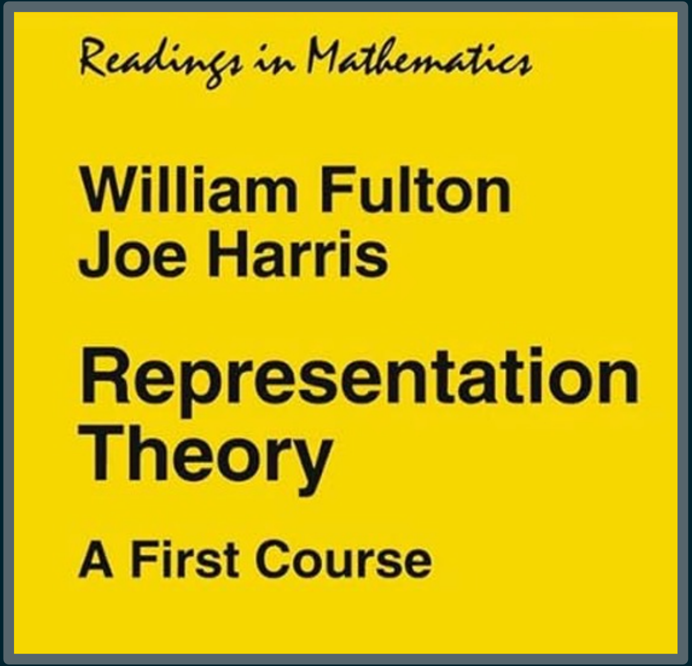
Why has it been so hard to build a PRU?

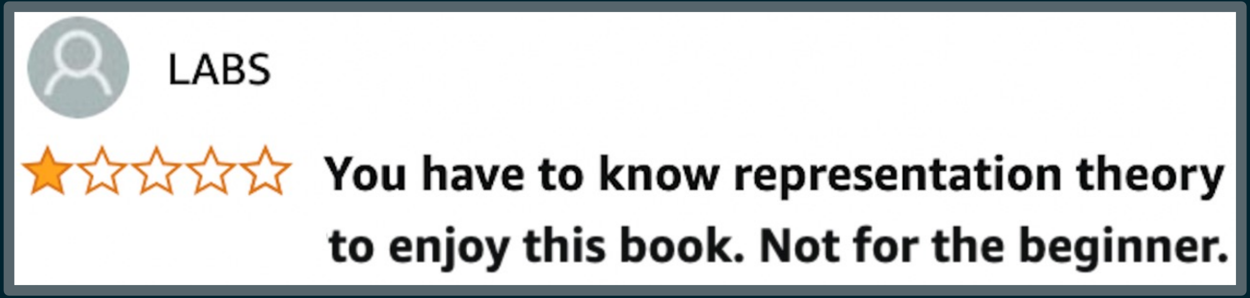
One reason: the math behind Haar-random unitaries is quite subtle!



Why has it been so hard to build a PRU?

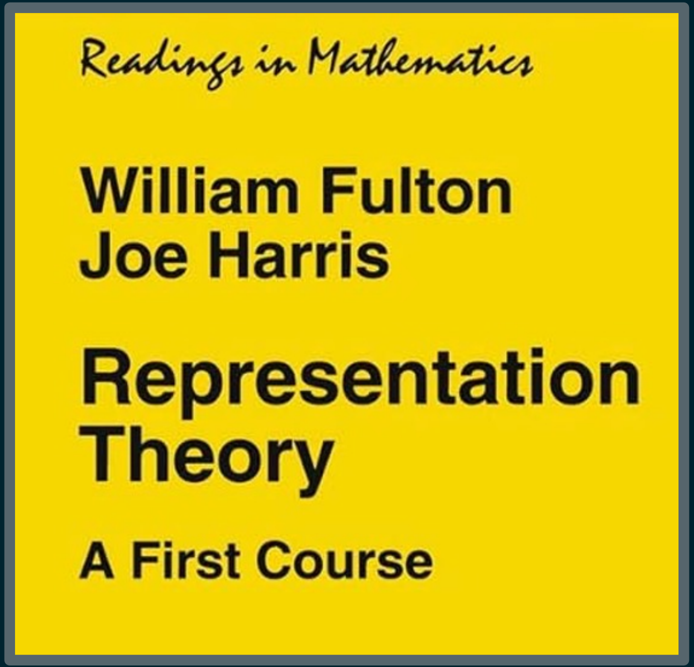
One reason: the math behind Haar-random unitaries is quite subtle!

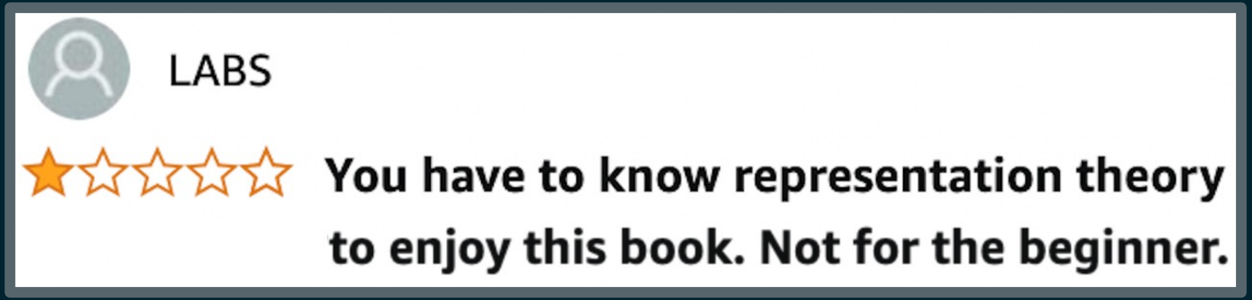




Why has it been so hard to build a PRU?

One reason: the math behind Haar-random unitaries is quite subtle!

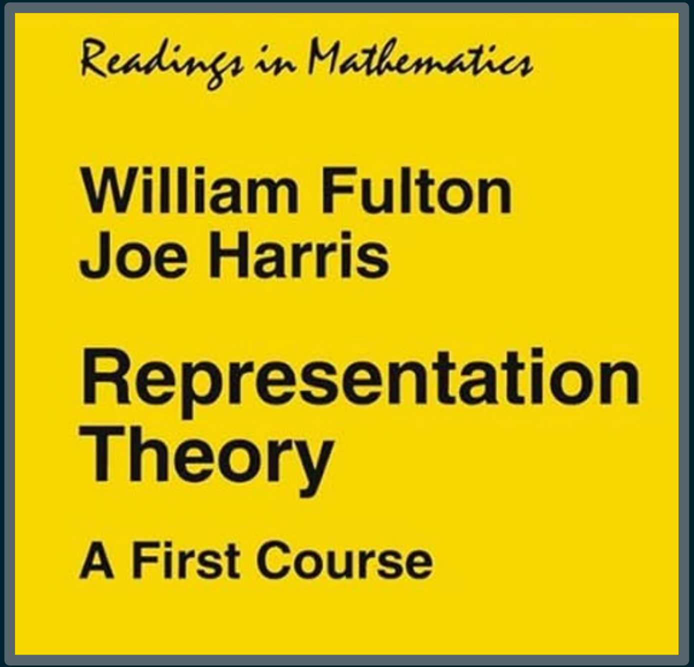


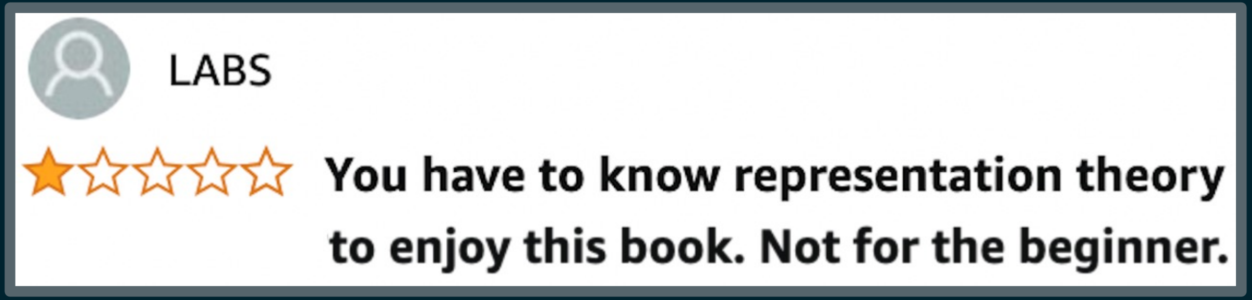


(just kidding, most of the reviews are very positive)

Why has it been so hard to build a PRU?

One reason: the math behind Haar-random unitaries is quite subtle!





(just kidding, most of the reviews are very positive)

This workshop: build secure PRUs using the **purification technique** [M24,MH24]; proofs only require basic quantum info.

This workshop: build secure PRUs using the **purification technique** [M24,MH24]; proofs only require basic quantum info.

1) adaptive PRUs [MH24]

This workshop: build secure PRUs using the **purification technique** [M24,MH24]; proofs only require basic quantum info.

1) adaptive PRUs [MH24]

$$U = P \cdot F \cdot C$$ [MPSY24]

This workshop: build secure PRUs using the **purification technique** [M24,MH24]; proofs only require basic quantum info.

1) adaptive PRUs [MH24]

$$U = P \cdot F \cdot C$$ [MPSY24]

permutation function Clifford

This workshop: build secure PRUs using the **purification technique** [M24,MH24]; proofs only require basic quantum info.

1) adaptive PRUs [MH24]

$$U = P \cdot F \cdot C$$ [MPSY24]

permutation function Clifford

2) low-depth PRUs [SSH24]
+ simple analysis of [MH24]

This workshop: build secure PRUs using the **purification technique** [M24,MH24]; proofs only require basic quantum info.

1) adaptive PRUs [MH24]

$$\underset{\text{permutation}}{U = P} \cdot \underset{\text{function}}{F} \cdot \underset{\text{Clifford}}{C}$$ [MPSY24]

2) low-depth PRUs [SSH24]
\+ simple analysis of [MH24]

$$U = \begin{array}{c} \boxed{V}\,\boxed{V}\,\boxed{V} \\ \boxed{V}\,\boxed{V} \end{array} \Big\} \ \omega(\log n)$$ depth PRU

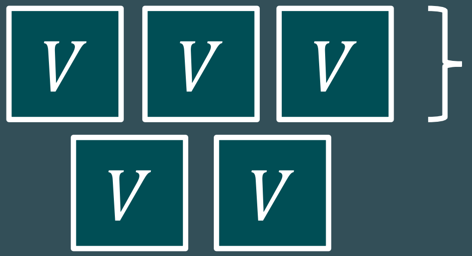
This workshop: build secure PRUs using the **purification technique** [M24,MH24]; proofs only require basic quantum info.

1) adaptive PRUs [MH24]

$$U = P \cdot F \cdot C$$ [MPSY24]

permutation function Clifford

2) low-depth PRUs [SSH24]
+ simple analysis of [MH24]

$U =$ 

$\omega(\log n)$
depth PRU

3) adaptive PRUs + inverse security [MH24]

This workshop: build secure PRUs using the **purification technique** [M24,MH24]; proofs only require basic quantum info.

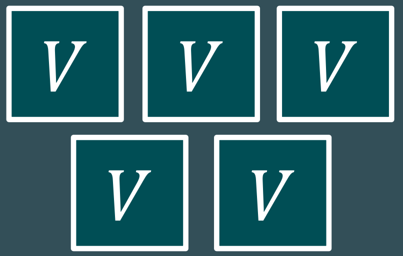
1) adaptive PRUs [MH24]

$$U = P \cdot F \cdot C$$ [MPSY24]

permutation function Clifford

2) low-depth PRUs [SSH24]
+ simple analysis of [MH24]

$U =$



$\}$ $\omega(\log n)$
depth PRU

3) adaptive PRUs + inverse security [MH24]

$$U = C^{\dagger} \cdot P \cdot F \cdot C$$

Rest of this talk: purification for pseudorandom states [M24]

Rest of this talk: purification for pseudorandom states [M24]

We'll prove pseudorandomness of a random binary phase state

$$|\psi_f\rangle = \sum_{x \in [N]} (-1)^{f(x)} |x\rangle$$

Rest of this talk: purification for pseudorandom states [M24]

We'll prove pseudorandomness of a random binary phase state

$$|\psi_f\rangle = \sum_{x\in[N]} (-1)^{f(x)}|x\rangle$$

The high-level idea:

Rest of this talk: purification for pseudorandom states [M24]

We'll prove pseudorandomness of a random binary phase state

$$|\psi_f\rangle = \sum_{x\in[N]} (-1)^{f(x)}|x\rangle$$

The high-level idea:

1) write down a purification of $\mathbb{E}_f\, |\psi_f\rangle\langle\psi_f|$.

Rest of this talk: purification for pseudorandom states [M24]

We'll prove pseudorandomness of a random binary phase state

$$|\psi_f\rangle = \sum_{x\in[N]} (-1)^{f(x)} |x\rangle$$

The high-level idea:

1) write down a purification of $\mathbb{E}_f\, |\psi_f\rangle\langle\psi_f|$.
2) find a nice basis for the purifying register.

Rest of this talk: purification for pseudorandom states [M24]

We'll prove pseudorandomness of a random binary phase state

$$|\psi_f\rangle = \sum_{x\in[N]} (-1)^{f(x)}|x\rangle$$

The high-level idea:

1) write down a purification of $\mathbb{E}_f\, |\psi_f\rangle\langle\psi_f|$.
2) find a nice basis for the purifying register.
3) use 2) to prove closeness to $\mathbb{E}_{\psi\leftarrow\mathrm{Haar}}\, |\psi\rangle\langle\psi|$.

Rest of this talk: purification for pseudorandom states [M24]

We'll prove pseudorandomness of a random binary phase state

$$|\psi_f\rangle = \sum_{x\in[N]} (-1)^{f(x)}|x\rangle$$

The high-level idea:

1) write down a purification of $\mathbb{E}_f\, |\psi_f\rangle\langle\psi_f|$.
2) find a nice basis for the purifying register.
3) use 2) to prove closeness to $\mathbb{E}_{\psi\leftarrow\text{Haar}}\, |\psi\rangle\langle\psi|$.

Recap of whiteboard proof

$$\sum_{f \in \{0,1\}^N} |\psi_f\rangle^{\otimes t} |f\rangle$$

Recap of whiteboard proof

$$\sum_{f\in\{0,1\}^N} |\psi_f\rangle^{\otimes t}\,|f\rangle = \sum_{f\in\{0,1\}^N} \left(\sum_{x\in[N]} (-1)^{f\cdot e_x}|x\rangle\right)^{\otimes t} |f\rangle$$

Recap of whiteboard proof

$$\sum_{f\in\{0,1\}^N} |\psi_f\rangle^{\otimes t}\, |f\rangle = \sum_{f\in\{0,1\}^N} \left(\sum_{x\in[N]} (-1)^{f\cdot e_x} |x\rangle\right)^{\otimes t} |f\rangle$$

$$\equiv \sum_{x_1,\ldots,x_t\in[N]} |x_1,\ldots,x_t\rangle\, |e_{x_1} \oplus \cdots \oplus e_{x_t}\rangle$$

(see whiteboard)

Recap of whiteboard proof

$$\sum_{f \in \{0,1\}^N} |\psi_f\rangle^{\otimes t} |f\rangle = \sum_{f \in \{0,1\}^N} \left(\sum_{x \in [N]} (-1)^{f \cdot e_x} |x\rangle \right)^{\otimes t} |f\rangle$$

$$\equiv \sum_{x_1, \ldots, x_t \in [N]} |x_1, \ldots, x_t\rangle |e_{x_1} \oplus \cdots \oplus e_{x_t}\rangle$$

(see whiteboard)

(after isometry)

$$\approx \sum_{x_1, \ldots, x_t \in [N]} |x_1, \ldots, x_t\rangle \frac{1}{\sqrt{t!}} \sum_{\pi \in S_t} R_\pi |x_1, \ldots, x_t\rangle$$

(see whiteboard)

Recap of whiteboard proof

$$\sum_{f\in\{0,1\}^N} |\psi_f\rangle^{\otimes t}\,|f\rangle = \sum_{f\in\{0,1\}^N}\left(\sum_{x\in[N]}(-1)^{f\cdot e_x}|x\rangle\right)^{\otimes t}|f\rangle$$

$$\equiv \sum_{x_1,\ldots,x_t\in[N]} |x_1,\ldots,x_t\rangle\,|e_{x_1}\oplus\cdots\oplus e_{x_t}\rangle$$

(see whiteboard)

(after isometry)

$$\approx \sum_{x_1,\ldots,x_t\in[N]} |x_1,\ldots,x_t\rangle \frac{1}{\sqrt{t!}}\sum_{\pi\in S_t} R_\pi|x_1,\ldots,x_t\rangle$$

(see whiteboard)

For any unitary U:

Recap of whiteboard proof

$$\sum_{f\in\{0,1\}^N} |\psi_f\rangle^{\otimes t}\,|f\rangle = \sum_{f\in\{0,1\}^N}\left(\sum_{x\in[N]}(-1)^{f\cdot e_x}|x\rangle\right)^{\otimes t}|f\rangle$$

$$\equiv \sum_{x_1,\dots,x_t\in[N]} |x_1,\dots,x_t\rangle\,|e_{x_1}\oplus\cdots\oplus e_{x_t}\rangle$$ (see whiteboard)

(after isometry) $$\approx \sum_{x_1,\dots,x_t\in[N]} |x_1,\dots,x_t\rangle \frac{1}{\sqrt{t!}}\sum_{\pi\in S_t} R_\pi|x_1,\dots,x_t\rangle$$ (see whiteboard)

For any unitary U:

$$\sum_{x_1,\dots,x_t\in[N]} U^{\otimes t}|x_1,\dots,x_t\rangle \sum_{\pi\in S_t} R_\pi|x_1,\dots,x_t\rangle$$

Recap of whiteboard proof

$$\sum_{f\in\{0,1\}^N} |\psi_f\rangle^{\otimes t}\,|f\rangle = \sum_{f\in\{0,1\}^N} \left(\sum_{x\in[N]} (-1)^{f\cdot e_x}|x\rangle\right)^{\otimes t} |f\rangle$$

$$\equiv \sum_{x_1,\ldots,x_t\in[N]} |x_1,\ldots,x_t\rangle\,|e_{x_1}\oplus\cdots\oplus e_{x_t}\rangle$$

(see whiteboard)

(after isometry)

$$\approx \sum_{x_1,\ldots,x_t\in[N]} |x_1,\ldots,x_t\rangle \frac{1}{\sqrt{t!}} \sum_{\pi\in S_t} R_\pi|x_1,\ldots,x_t\rangle$$

(see whiteboard)

For any unitary U:

$$\sum_{x_1,\ldots,x_t\in[N]} U^{\otimes t}|x_1,\ldots,x_t\rangle \sum_{\pi\in S_t} R_\pi|x_1,\ldots,x_t\rangle = \sum_{x_1,\ldots,x_t\in[N]} |x_1\rangle\cdots|x_t\rangle \sum_{\pi\in R_\pi} R_\pi\cdot U^{\top,\otimes t}|x_1,\ldots,x_t\rangle$$

Recap of whiteboard proof

$$\sum_{f\in\{0,1\}^N} |\psi_f\rangle^{\otimes t}\,|f\rangle = \sum_{f\in\{0,1\}^N} \left(\sum_{x\in[N]} (-1)^{f\cdot e_x}|x\rangle\right)^{\otimes t} |f\rangle$$

$$\equiv \sum_{x_1,\dots,x_t\in[N]} |x_1,\dots,x_t\rangle\,|e_{x_1}\oplus\cdots\oplus e_{x_t}\rangle$$

(see whiteboard)

(after isometry)

$$\approx \sum_{x_1,\dots,x_t\in[N]} |x_1,\dots,x_t\rangle \frac{1}{\sqrt{t!}} \sum_{\pi\in S_t} R_\pi|x_1,\dots,x_t\rangle$$

(see whiteboard)

For any unitary U:

$$\sum_{x_1,\dots,x_t\in[N]} U^{\otimes t}|x_1,\dots,x_t\rangle \sum_{\pi\in S_t} R_\pi|x_1,\dots,x_t\rangle = \sum_{x_1,\dots,x_t\in[N]} |x_1\rangle\cdots|x_t\rangle \sum_{\pi\in R_\pi} R_\pi\cdot U^{\top,\otimes t}|x_1,\dots,x_t\rangle$$

using $\sum_{x\in[N]} U|x\rangle|x\rangle = \sum_{x\in[N]}|x\rangle\, U^\top|x\rangle$

Recap of whiteboard proof

$$\sum_{f\in\{0,1\}^N} |\psi_f\rangle^{\otimes t}\,|f\rangle = \sum_{f\in\{0,1\}^N} \left(\sum_{x\in[N]} (-1)^{f\cdot e_x}|x\rangle\right)^{\otimes t} |f\rangle$$

$$\equiv \sum_{x_1,\ldots,x_t\in[N]} |x_1,\ldots,x_t\rangle\,|e_{x_1}\oplus\cdots\oplus e_{x_t}\rangle$$ (see whiteboard)

(after isometry) $$\approx \sum_{x_1,\ldots,x_t\in[N]} |x_1,\ldots,x_t\rangle \frac{1}{\sqrt{t!}} \sum_{\pi\in S_t} R_\pi|x_1,\ldots,x_t\rangle$$ (see whiteboard)

For any unitary U: (by applying $\overline{U}^{\otimes t}$)

$$\sum_{x_1,\ldots,x_t\in[N]} U^{\otimes t}|x_1,\ldots,x_t\rangle \sum_{\pi\in S_t} R_\pi|x_1,\ldots,x_t\rangle = \sum_{x_1,\ldots,x_t\in[N]} |x_1\rangle\cdots|x_t\rangle \sum_{\pi\in R_\pi} R_\pi \cdot \cancel{U^{\top,\otimes t}}|x_1,\ldots,x_t\rangle$$

using $\sum_{x\in[N]} U|x\rangle|x\rangle = \sum_{x\in[N]}|x\rangle\, U^\top|x\rangle$

Recap of whiteboard proof

$$\sum_{f\in\{0,1\}^N} |\psi_f\rangle^{\otimes t} |f\rangle = \sum_{f\in\{0,1\}^N} \left(\sum_{x\in[N]} (-1)^{f\cdot e_x} |x\rangle\right)^{\otimes t} |f\rangle$$

$$\equiv \sum_{x_1,\ldots,x_t\in[N]} |x_1,\ldots,x_t\rangle\, |e_{x_1}\oplus\cdots\oplus e_{x_t}\rangle$$

(see whiteboard)

(after isometry)

$$\approx \sum_{x_1,\ldots,x_t\in[N]} |x_1,\ldots,x_t\rangle \frac{1}{\sqrt{t!}} \sum_{\pi\in S_t} R_\pi |x_1,\ldots,x_t\rangle$$

(see whiteboard)

For any unitary U:

(by applying $\overline{U}^{\otimes t}$)

$$\sum_{x_1,\ldots,x_t\in[N]} U^{\otimes t} |x_1,\ldots,x_t\rangle \sum_{\pi\in S_t} R_\pi |x_1,\ldots,x_t\rangle = \sum_{x_1,\ldots,x_t\in[N]} |x_1\rangle\cdots|x_t\rangle \sum_{\pi\in R_\pi} R_\pi \cdot \cancel{U^{\top,\otimes t}} |x_1,\ldots,x_t\rangle$$

using $\sum_{x\in[N]} U|x\rangle|x\rangle = \sum_{x\in[N]} |x\rangle\, U^\top |x\rangle$

This implies:

$$\mathbb{E}_f\, |\psi_f\rangle\langle\psi_f|^{\otimes t}$$

Recap of whiteboard proof

$$\sum_{f\in\{0,1\}^N} |\psi_f\rangle^{\otimes t}\,|f\rangle = \sum_{f\in\{0,1\}^N}\left(\sum_{x\in[N]}(-1)^{f\cdot e_x}|x\rangle\right)^{\otimes t}|f\rangle$$

$$\equiv \sum_{x_1,\ldots,x_t\in[N]} |x_1,\ldots,x_t\rangle\,|e_{x_1}\oplus\cdots\oplus e_{x_t}\rangle$$

(see whiteboard)

(after isometry)

$$\approx \sum_{x_1,\ldots,x_t\in[N]} |x_1,\ldots,x_t\rangle\frac{1}{\sqrt{t!}}\sum_{\pi\in S_t} R_\pi|x_1,\ldots,x_t\rangle$$

(see whiteboard)

For any unitary U:

(by applying $\overline{U}^{\otimes t}$)

$$\sum_{x_1,\ldots,x_t\in[N]} U^{\otimes t}|x_1,\ldots,x_t\rangle\sum_{\pi\in S_t} R_\pi|x_1,\ldots,x_t\rangle = \sum_{x_1,\ldots,x_t\in[N]} |x_1\rangle\cdots|x_t\rangle\sum_{\pi\in R_\pi} R_\pi\cdot\cancel{U^{\top,\otimes t}}|x_1,\ldots,x_t\rangle$$

using $\sum_{x\in[N]} U|x\rangle|x\rangle = \sum_{x\in[N]}|x\rangle\,U^\top|x\rangle$

This implies:

$$\mathbb{E}_f\,|\psi_f\rangle\langle\psi_f|^{\otimes t} \approx \mathbb{E}_{U\leftarrow\mathrm{Haar}}\,\mathbb{E}_f\,(U|\psi_f\rangle\langle\psi_f|U^\dagger)^{\otimes t}$$

(true for any U)

Recap of whiteboard proof

$$\sum_{f\in\{0,1\}^N} |\psi_f\rangle^{\otimes t}\,|f\rangle = \sum_{f\in\{0,1\}^N}\left(\sum_{x\in[N]}(-1)^{f\cdot e_x}|x\rangle\right)^{\otimes t}|f\rangle$$

$$\equiv \sum_{x_1,\ldots,x_t\in[N]} |x_1,\ldots,x_t\rangle\,|e_{x_1}\oplus\cdots\oplus e_{x_t}\rangle \qquad \text{(see whiteboard)}$$

(after isometry)

$$\approx \sum_{x_1,\ldots,x_t\in[N]} |x_1,\ldots,x_t\rangle\frac{1}{\sqrt{t!}}\sum_{\pi\in S_t} R_\pi|x_1,\ldots,x_t\rangle \qquad \text{(see whiteboard)}$$

For any unitary U: (by applying $\overline{U}^{\otimes t}$)

$$\sum_{x_1,\ldots,x_t\in[N]} U^{\otimes t}|x_1,\ldots,x_t\rangle\sum_{\pi\in S_t}R_\pi|x_1,\ldots,x_t\rangle = \sum_{x_1,\ldots,x_t\in[N]}|x_1\rangle\cdots|x_t\rangle\sum_{\pi\in R_\pi}R_\pi\cdot\cancel{U^{\top,\otimes t}}|x_1,\ldots,x_t\rangle$$

using $\sum_{x\in[N]} U|x\rangle|x\rangle = \sum_{x\in[N]}|x\rangle\, U^{\top}|x\rangle$

This implies:

$$\mathbb{E}_f\,|\psi_f\rangle\langle\psi_f|^{\otimes t} \approx \mathbb{E}_{U\leftarrow\mathrm{Haar}}\,\mathbb{E}_f\,(U|\psi_f\rangle\langle\psi_f|U^\dagger)^{\otimes t} = \mathbb{E}_{|\psi\rangle\leftarrow\mathrm{Haar}}\,|\psi\rangle\langle\psi|^{\otimes t}$$

(true for any U)

Recap of whiteboard proof

$$\sum_{f\in\{0,1\}^N} |\psi_f\rangle^{\otimes t}\,|f\rangle = \sum_{f\in\{0,1\}^N}\left(\sum_{x\in[N]}(-1)^{f\cdot e_x}|x\rangle\right)^{\otimes t}|f\rangle$$

$$\equiv \sum_{x_1,\dots,x_t\in[N]} |x_1,\dots,x_t\rangle\,|e_{x_1}\oplus\cdots\oplus e_{x_t}\rangle$$ (see whiteboard)

(after isometry) $$\approx \sum_{x_1,\dots,x_t\in[N]} |x_1,\dots,x_t\rangle\frac{1}{\sqrt{t!}}\sum_{\pi\in S_t} R_\pi|x_1,\dots,x_t\rangle$$ (see whiteboard)

For any unitary U: (by applying $\overline{U}^{\otimes t}$)

$$\sum_{x_1,\dots,x_t\in[N]} U^{\otimes t}|x_1,\dots,x_t\rangle\sum_{\pi\in S_t}R_\pi|x_1,\dots,x_t\rangle = \sum_{x_1,\dots,x_t\in[N]}|x_1\rangle\cdots|x_t\rangle\sum_{\pi\in R_\pi}R_\pi\cdot\cancel{U^{\top,\otimes t}}|x_1,\dots,x_t\rangle$$

using $\sum_{x\in[N]} U|x\rangle|x\rangle = \sum_{x\in[N]}|x\rangle\,U^\top|x\rangle$

This implies:

$$\mathbb{E}_f\,|\psi_f\rangle\langle\psi_f|^{\otimes t} \approx \mathbb{E}_{U\leftarrow\text{Haar}}\,\mathbb{E}_f\,(U|\psi_f\rangle\langle\psi_f|U^\dagger)^{\otimes t} = \mathbb{E}_{|\psi\rangle\leftarrow\text{Haar}}\,|\psi\rangle\langle\psi|^{\otimes t}$$

(true for any U) (invariance of Haar measure)