Quantum Pseudorandomness

computational

FANG SONG

04/2025 @ BIRS, Banff

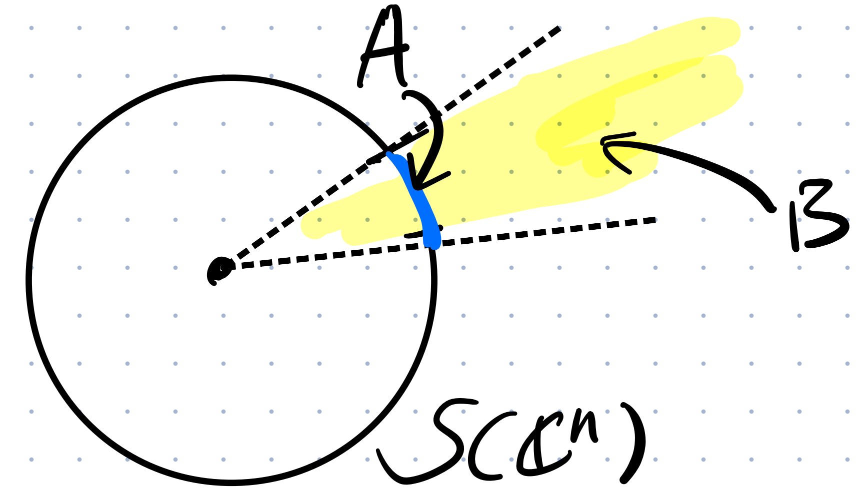
0. Quantum Randomness

Haar measure :

- γ : (Gaussian meas) $\forall S \subseteq \mathbb{C}^N$, $\gamma(S) = \int_S \exp(-\|x\|^2)\, d\nu(x)$

n-qubits

- $\mu(S(\mathbb{C}^n))$: Haar-random States



$\forall A \subseteq S(\mathbb{C}^N)$

$B := \{x \in \mathbb{C}^N : x \neq 0 \ \& \ \frac{x}{\|x\|} \in A\}$

$\mu(A) := \gamma(B)$

n-qubit unitary

- $\eta(\mathcal{U}(\mathbb{C}^n))$: Haar-random unitary

$\forall A \subseteq \mathcal{U}(\mathbb{C}^N)$

Gram-Schmidt

$\eta(A) := \gamma_{n^2}\left(\{\mathrm{vec}(X) : (X)_{N\times N},\ \det(X) \neq 0,\ G.S.(X) \in A\}\right)$

Haar measure : ☆ Operational def

- $\psi \leftarrow \mu(S(\mathbb{C}^N))$

$$\psi = \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_N \end{pmatrix} :$$

① $\forall i,\ \alpha_i \leftarrow \mathcal{N}(0,1)$ indep.

② normalize

- $U \leftarrow \eta(\mathcal{U}(\mathbb{C}^N))$

$$\begin{pmatrix} | & & | \\ \psi_1 & \cdots & \psi_N \\ | & & | \end{pmatrix}$$

- $\psi_i \leftarrow \mu$ indep (cond. on orthogonal.)

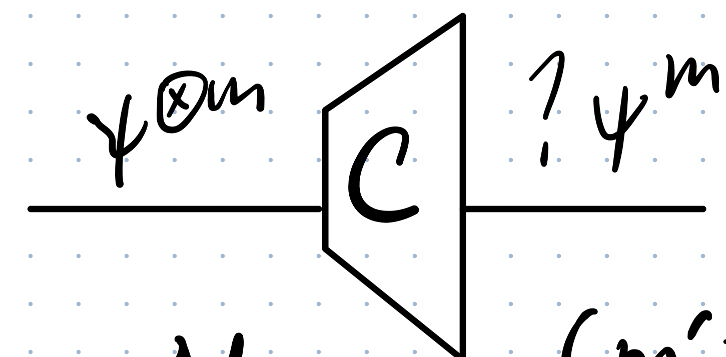
OR

- $\forall i,j\ \alpha_{ij} \leftarrow \mathcal{N}(0,1)$ then Gram-Schmidt.

Haar measure: ☆ Properties of Haar States

- $\mathbb{E}_{\psi \leftarrow \mu} (|\psi\rangle\langle\psi|)^{\otimes m} = \underbrace{\binom{N+m-1}{m}^{-1}}_{N_m} \underbrace{\Pi_m^{\text{Sym}}}_{\text{symmetric subspace } \vee^m \mathbb{C}^N}$ $\left(\mathbb{E}_{\psi\leftarrow\mu} (|\psi\rangle\langle\psi|) = \mathbb{1}/N\right)$

- No-cloning [Werner '98]:

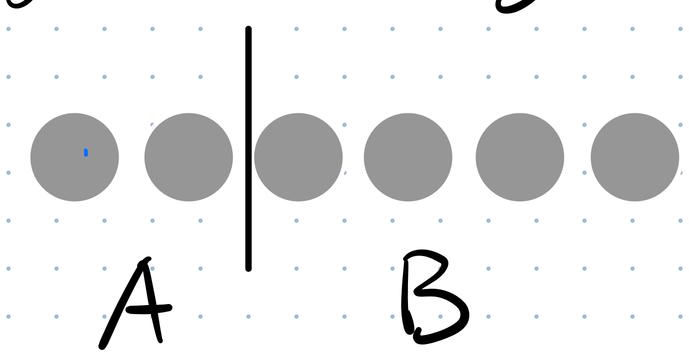


, $m' > m$

$(m' = m+1)$

$$\mathbb{E}_{\psi\leftarrow\mu} \langle C\psi^{\otimes m}, \psi^{m'} \rangle \leq \frac{N_m}{N_{m'}} = m/_{N+m}$$

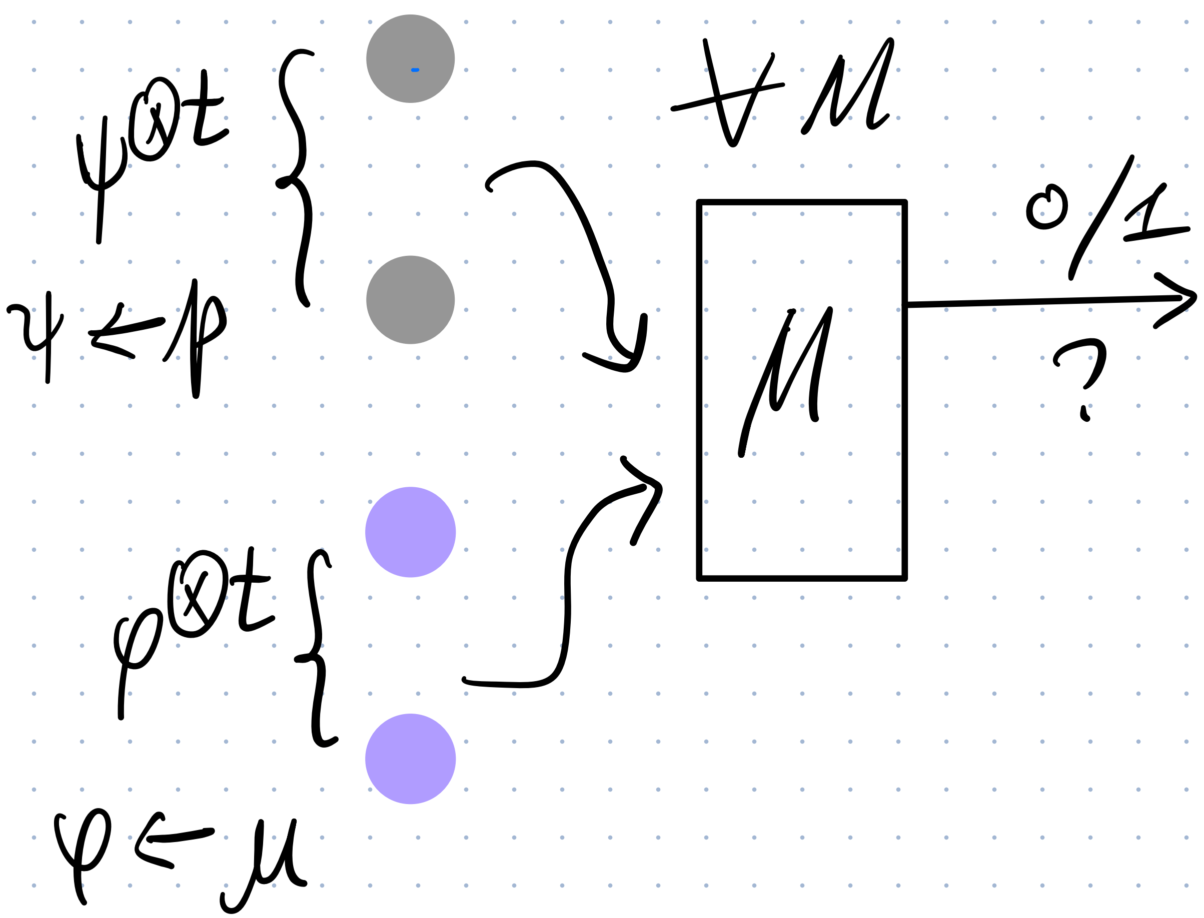
- High entanglement [Page '93]



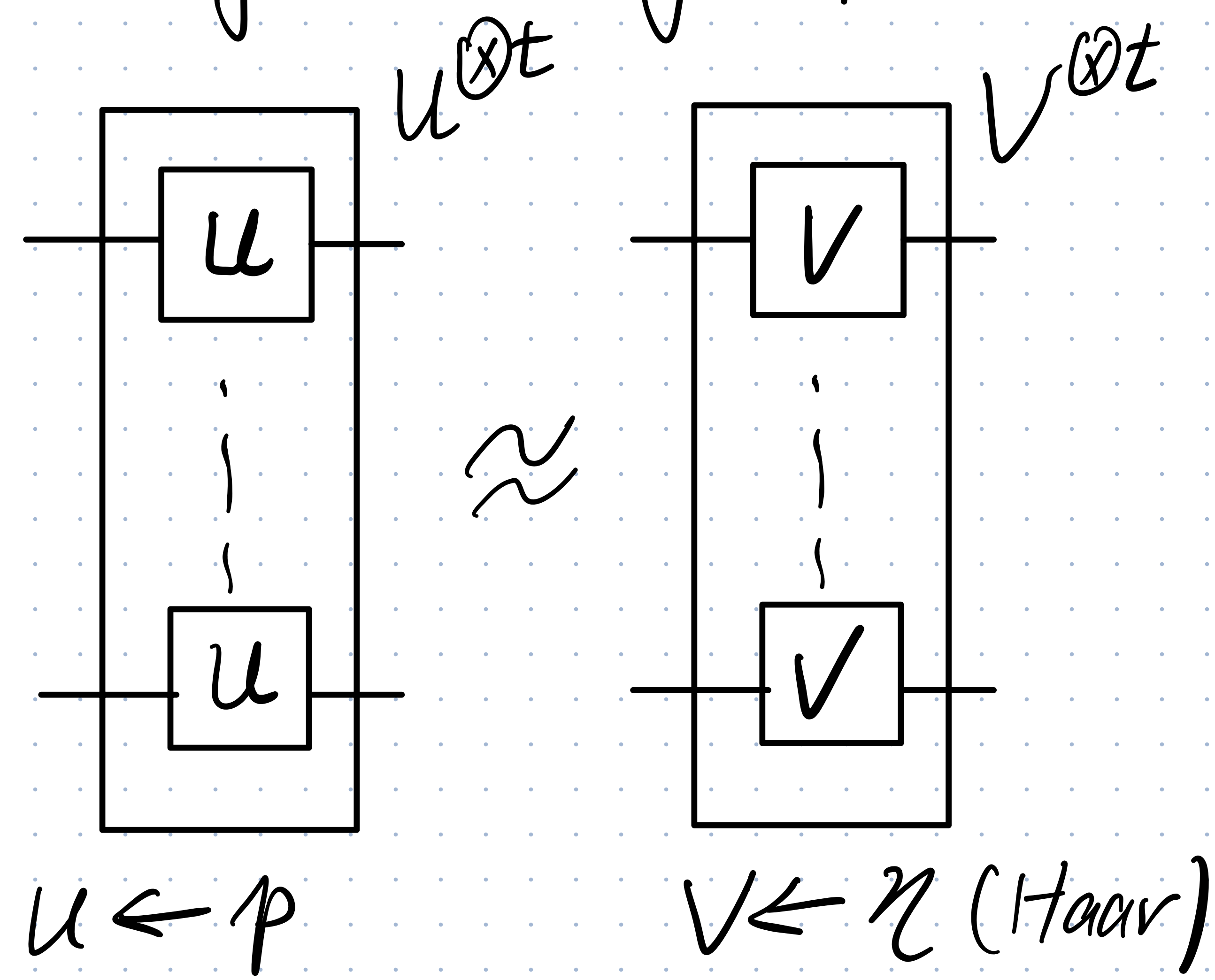
$$\mathbb{E}_{\psi\leftarrow\mu} S(\rho_A) > \log d_A - O(1)$$

Quantum pseudorandomness: t-designs

- p: efficient to sample
- State t-design p



- Unitary t-design p



Δ Apps: enc/auth, decoupling,
Randomized Benchmarking of NISQ

1. Computational Quantum Pseudorandomness

V0.1 [Ji Liu S '18]

How it started:

"non-local games"

2015-2016

"t-designs"

A cryptographic version?

Defining Pseudorandom States (PRS)

- PRS family

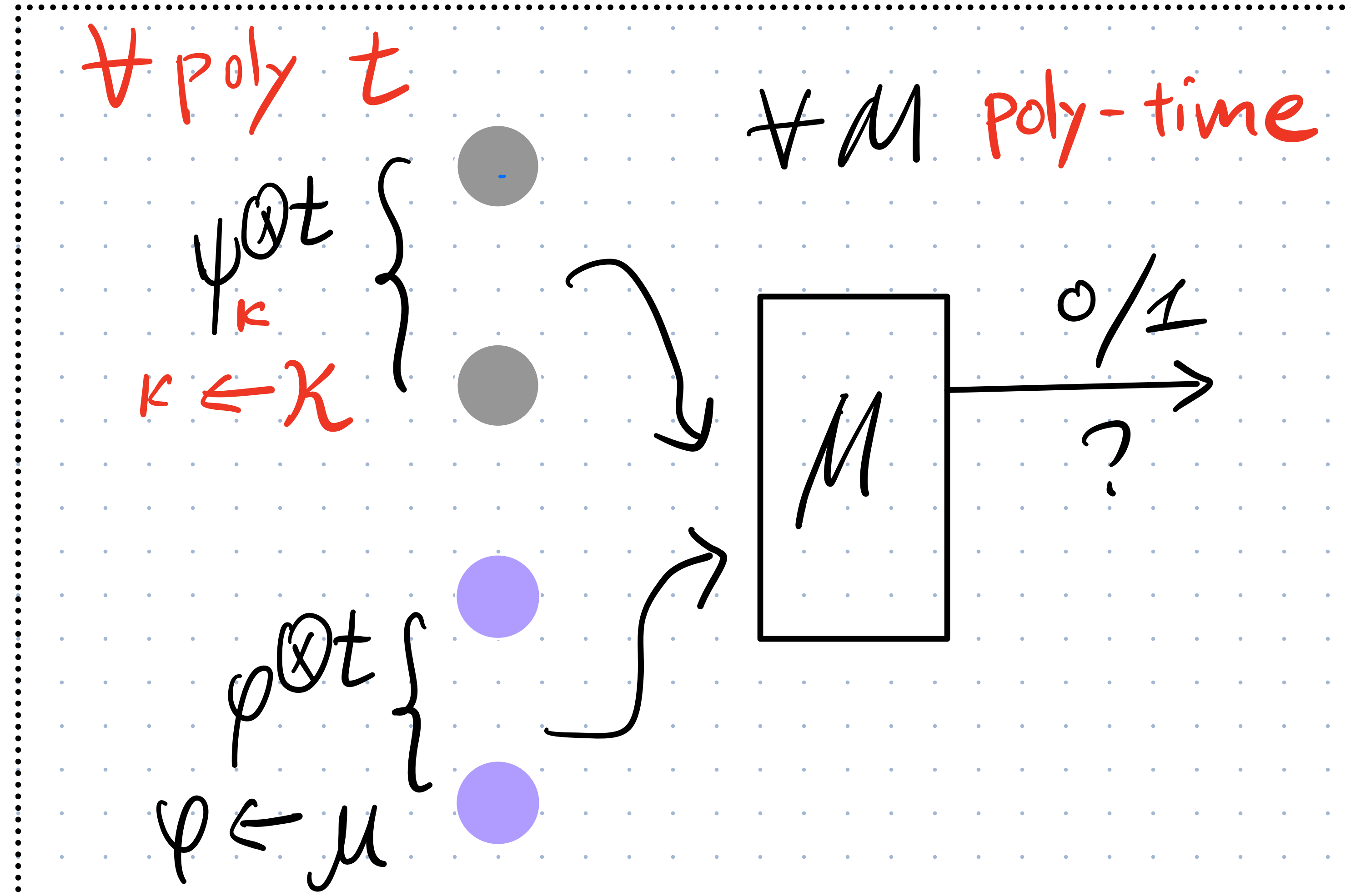
  a. $\{\psi_k\} \approx_c \psi \leftarrow \mu$

  "

  Unitary family $\{U_k\}$

  $\{U_k|0\rangle\} \approx_c \{V|0\rangle\}$

  b. ψ_k eff. to prepare



- OBS. single-copy trivial: random basis $|k\rangle$

  (if long key is permitted)

  ∀ poly-copy to $\mathcal{M}$ both reasonable & useful

Constructing PRS

☆ Randomizing technique 1 : Random phase

$$|\psi_k\rangle \propto \sum \omega_q^{F_k(x)} |x\rangle$$

- $\omega_q = e^{2\pi i/q}$
- $\{F_k\}$: PRF
- $q = N = 2^n$

- let $F_k : |x\rangle \longmapsto \omega_q^{F_k(x)} |x\rangle$ ← efficient
- $\{|\psi_k\rangle\} = \{U_k|0\rangle\}$: $U_k = F_k H$
- special case : $|\psi_k\rangle = \sum (-1)^{F_k(x)} |x\rangle$

Proving Security

★ Analyzing tech. 1 : 1st principle (i.e. brute-force)

- Hybrid : $\{|\psi_k\rangle\} \approx_c \{|\psi_f\rangle := \sum \omega_N^{f(x)} |x\rangle\}$
- Explicit calculation of distance.

$$\forall\, t = \mathrm{poly}(n),\ \mathbb{E}_f \left(|\psi_f\rangle\langle\psi_f|\right)^{\otimes t} \approx \mathbb{E}_{\phi \leftarrow \mu} \left(|\phi\rangle\langle\phi|\right)^{\otimes t}$$

$\boxed{\text{OWF} \Longrightarrow \text{PRS}}$

(Binary Phase [BS'19])

Another PRS Candidate

★ Randomizing technique 2: Random subset (permutation)

$$|\psi_k\rangle \propto \sum |P_k(x\|0^n)\rangle$$

· $\{P_k\}$: PRP on $\{0,1\}^{2n}$

$$= \sum_{x \in S} |x\rangle$$

$S \overset{\$}{\subseteq} \{0,1\}^n$

· Efficient: ✓

▽ Security?

Apps. of PRS

1. Computational no-cloning

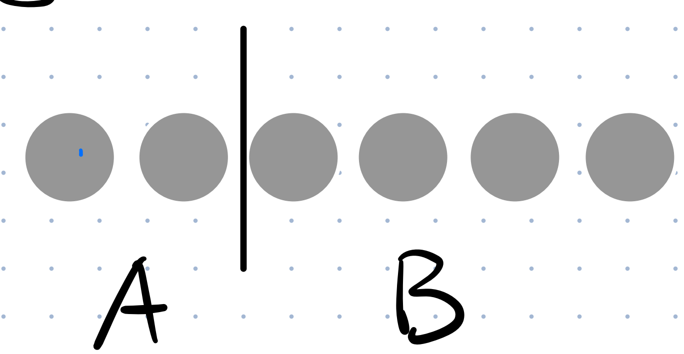
$\Rightarrow$ private-key QM : k : \$ seriel #

$|\psi_k\rangle$: money (coin) state

Security: no-cloning given <u>Verf. oracle</u>

▷ Side tech: simulating $\boxed{R_\psi = \mathbb{1} - 2|\psi\rangle\langle\psi|}$ w. $|\psi\rangle^{\otimes \ell}$

2. "High" Entanglement



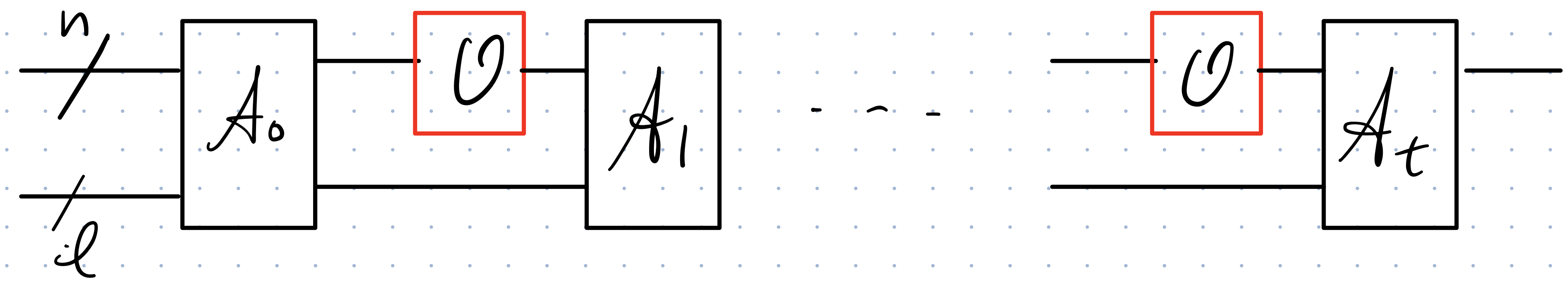
$\mathbb{E}_{k}\, S(\rho_k^A) \geq \omega(\log n)$

What about PRUs?

- DEF. Efficient unitary family $\{U_k\}$

  $\forall$ poly t, $\forall$ poly-time $\mathcal{A} = (\mathcal{A}_0, \cdots, \mathcal{A}_t)$

  $\mathcal{O} \in \{U_k, V \leftarrow \eta\}$



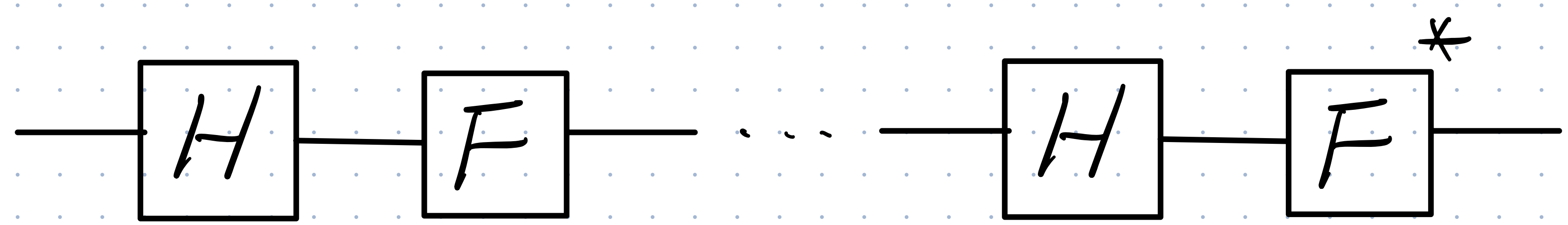
$$\mathbb{E}_{k \leftarrow \mathcal{K}} \mathcal{A}^{U_k} \approx \mathbb{E}_{V \leftarrow \eta} \mathcal{A}^{V}$$

- Strong PRU: $\mathcal{O}$ can be inverse $U_k^\dagger / V^\dagger$ too.

what about PRUs ?

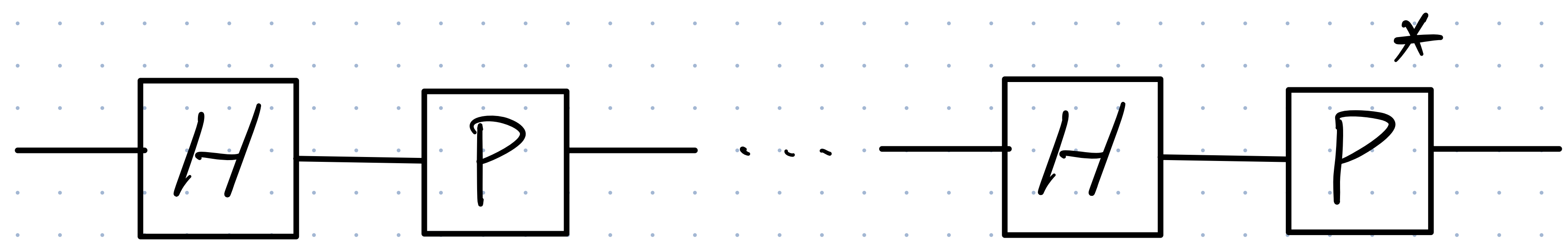
- Candidates in [JLS'18]

a.



<u>Yi-Kai's conj</u>: one-&-half i.e. FHF'

b.



*: indep. keys

Recap: at the dusk of v.0.1

? Provable PRU

A

? Is Random Subset State PRS

? entanglement bound

B

OWF

$\downarrow \quad \uparrow ?$

PRS

$? \downarrow$ more crypto

C

2. QPR : V0.1 → V1.0

? Provable PRU

A

? Is Random Subset State PRS

? entanglement bound

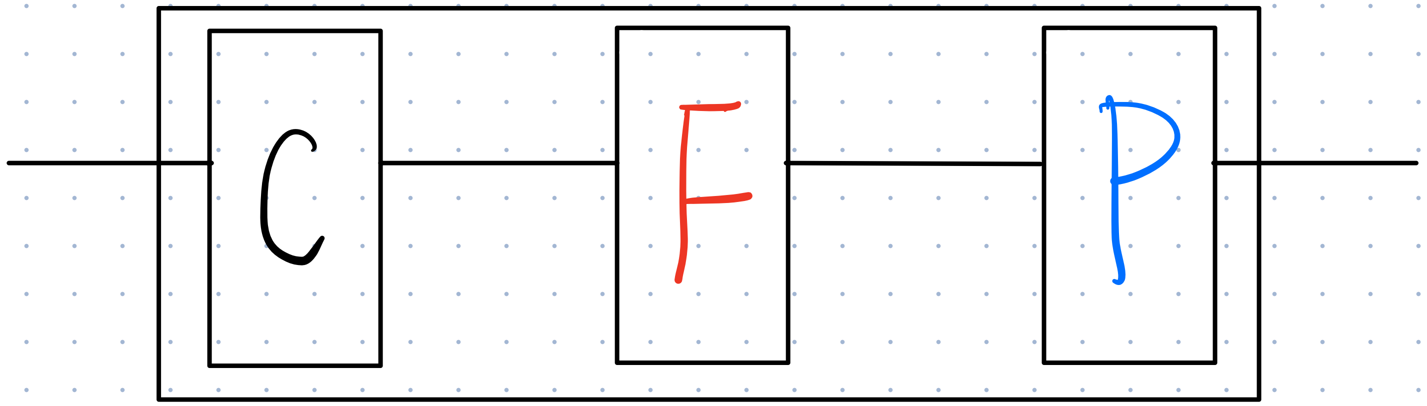
B

$$\begin{tikzcd} \text{OWF} \arrow[d, shift right] \\ \text{PRS} \arrow[u, shift right, "?"'] \arrow[d, "?"'] \\ \text{more crypto} \end{tikzcd}$$

C

& beyond

V1.0 PART A : Provable PRU



C : R. Clifford (2-design)

F : R. phase

(F_k : $|x\rangle \longmapsto \omega_q^{F_k(x)} |x\rangle$)

P : R. perm.

(P_k : $|x\rangle \longmapsto |P_k(x)\rangle$)

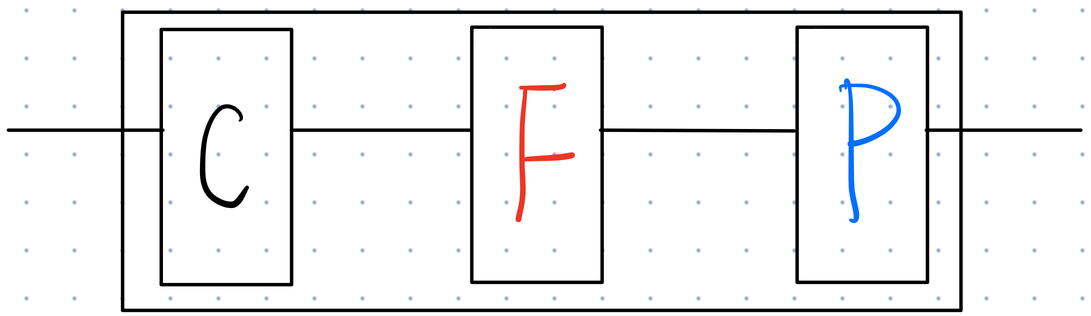
[MPSY'24] non-adaptive PRU

→ Analysis : 1st principle (rep. theory ...)

[MH'24] adaptive & strong PRU

(CFPC') ← $q \geq 3$

V1.0 PART A : Provable PRU



[MH'24] adaptive & strong PRU

☆ → Analyzing tech. 2 : efficient simulation of random unitary (PATH-Recording)

(Fermi's talk next)

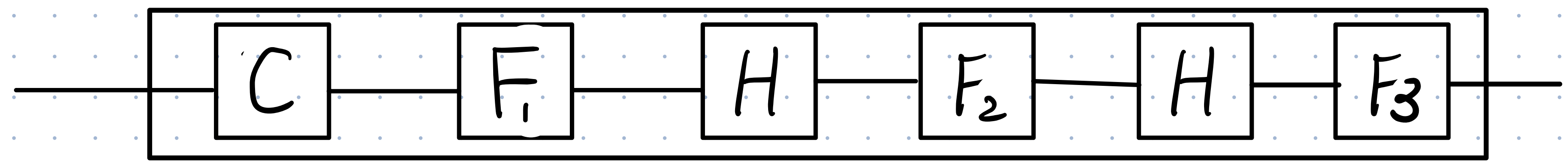
- [AMR'20]: stateful (inefficient) simulation

V1.0 PART A

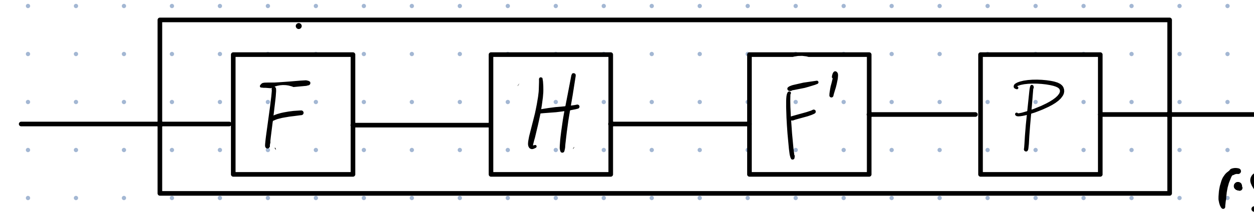
Other developments

C+2.5 rand 1

- [BHHP'24] : PRU

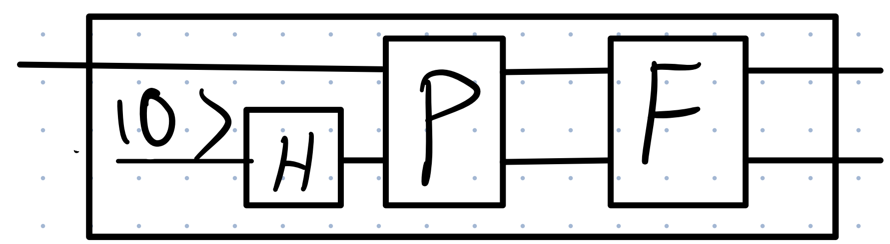


- [BM'24] : non-adaptive somewhat PRU



1.5 rand + P

- [AGKL'24] : randomize certain input states



ALL follow R. phase + R. permutation paradigm.

- [LQSYZ'23 '25] : Parallel Kac Walk

☆ new randomizing strategy & proof tech.

V1.0 PART A   Parallel Kac Walk

- Kac Walk $\boxed{\text{Randomizing technique 3}}$

$$v = \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ \vdots \\ v_N \end{pmatrix}$$

① Sample random coordinate pair (i, j)

$\longrightarrow \tilde{v}$

② Sample 2-D Haar-V

$$\begin{pmatrix} v_i \\ v_j \end{pmatrix} \xmapsto{V} \begin{pmatrix} \tilde{v}_i \\ \tilde{v}_j \end{pmatrix}$$

- Thm [PS'17] Kac Walk $\rightsquigarrow \mu(S(\mathbb{C}^N))$ in $O(N \log N)$ steps.

$\boxed{\text{Analyzing technique 3}}$: Rapid mixing

Parallel Kac Walk

- Mixing in $N\log N \to \log N$: N steps in one-shot?

- :) Parallel Kac Walk [LQSYZ'23]

① R. pairing $\begin{matrix} i_1 & \cdots & i_{N/2} \\ j_1 & & j_{N/2} \end{matrix}$ ② R. each pair, indep.

$$\begin{pmatrix} v_{i_k} \\ v_{j_k} \end{pmatrix} \xmapsto{U_k} \begin{pmatrix} \tilde{v}_{i_k} \\ \tilde{v}_{j_k} \end{pmatrix}$$

- Thm: PKAC $\rightsquigarrow \mu(S(\mathbb{C}^N))$ in $O(\log N)$

  Pf: A new coupling argument

Parallel Kac Walk

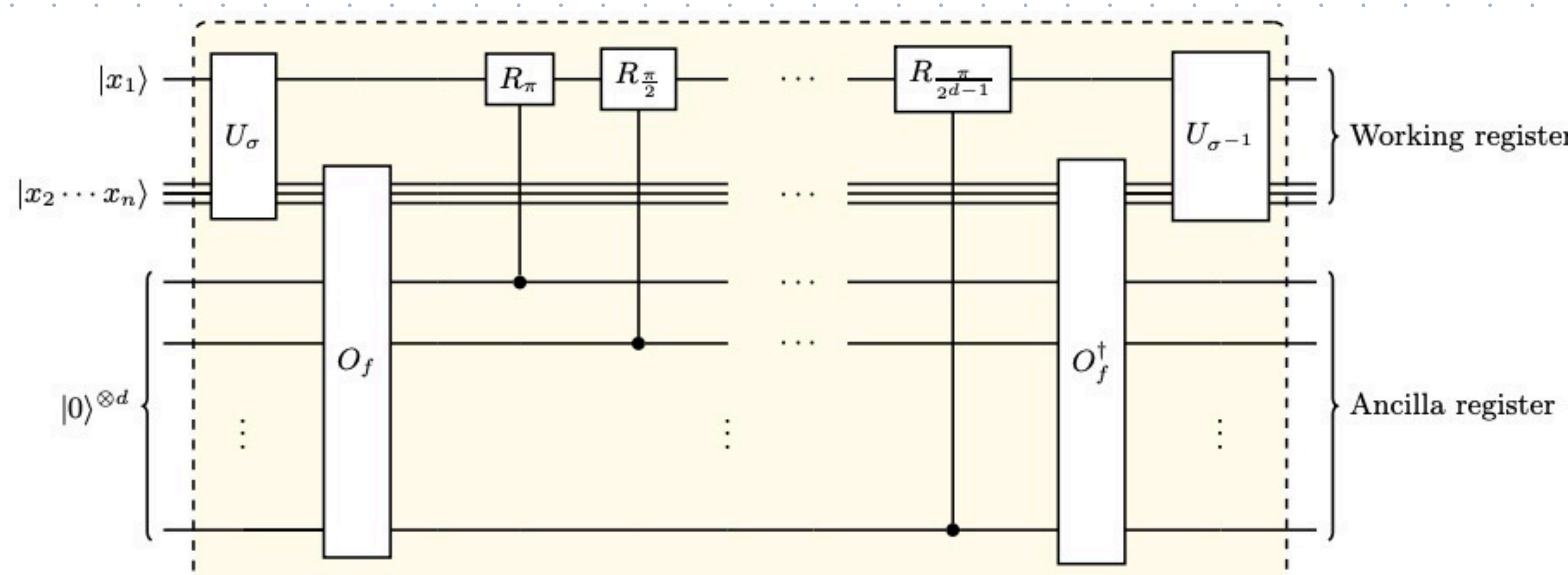
$\longrightarrow$ (Pseudo) Random State Scrambler (P)RSS $\{R_k\}$

$\forall \psi$, poly m, $\mathbb{E}_{k} \left(R_k|\psi\rangle\right)^{\otimes m} \approx \mathbb{E}_{V \leftarrow \eta} \left(V|\psi\rangle\right)^{\otimes m}$

(vs. PRS. fixed input state, may fail elsewhere)

☆ "Dispersing": $\{PKAC_k|\psi\rangle\}$ is an ε-net in $S(\mathbb{C}^N)$

- Q2KT Implementation



- Generalization:

t-level PRSS

$\{R_k^{\otimes t}|\psi\rangle\} \approx \{V^{\otimes t}|\psi\rangle\}$

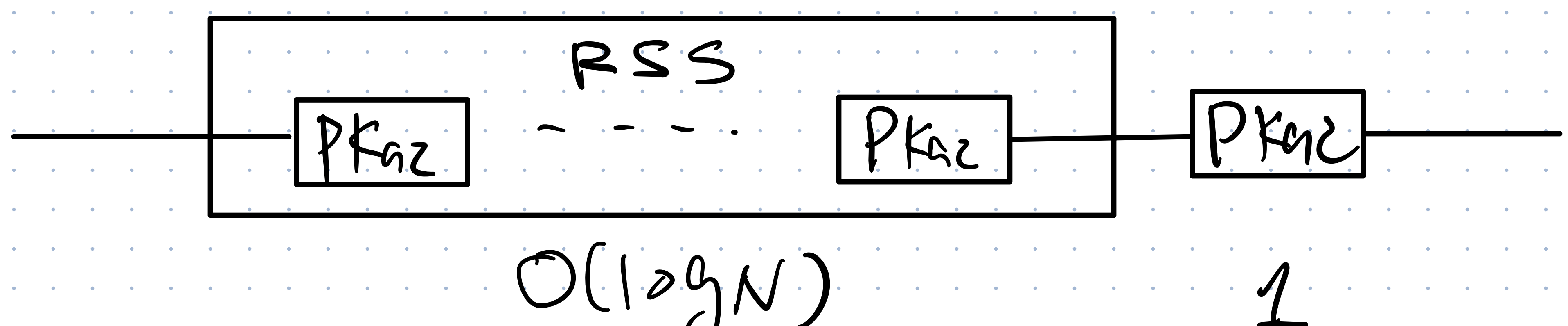
Parallel Kac Walk $\Rightarrow$ PRU?

- Thm [Oliveira'09] : KAC Walk $\rightsquigarrow$ Haar-U in $O(N^2 \log N)$

  ↪ Parallel Kac Walk - - - - $O(N \log N)$

  ? mixing in <u>polylog N</u> (✓ $\Rightarrow$ PRU)

- YES, it's (Strong) PRU by PATH-REC [MH'25]
  (arxiv:2504.14957)



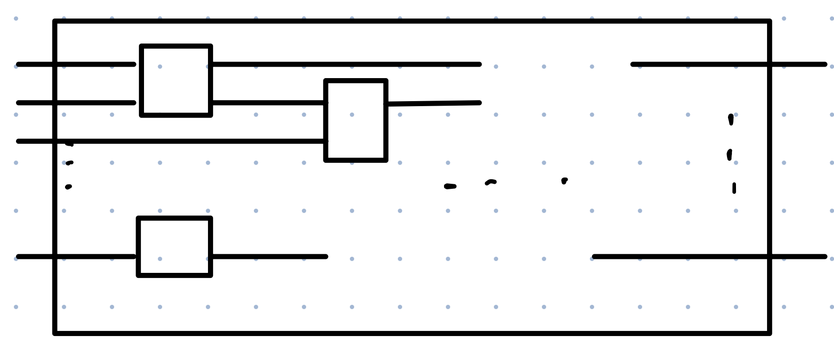
V1.0 PART A : Provable PRU

Beyond :

- Generic construztions (à la Luby-Rackoff)?
  C'PFC
- Killer apps of PRU?
  (that PRS, t-designs cannot)

physics?

- Random quantum circuits



PFC

RQC

PKAC

Structured

V1.0 PART B

? Is Random Subset State PRS

? entanglement bound

B

$$|\psi_k\rangle \propto \sum |P_k(x\|0^n)\rangle \equiv \sum_{x\in S} |x\rangle, \quad S \overset{\$}{\subseteq} \{0,1\}^n$$

Thm [ABFGVZZ'24, JMSW'24]

$$\text{err} \quad \frac{m}{\sqrt{s}} + \frac{s\cdot m}{d}$$

$\{\psi_k\}$ is PRS. $\forall t = \omega(\text{poly}(n))$, $t < s < N/t$,

$\Rightarrow$ Ent. entropy can be tuned : $(\omega(\log n), O(n))$

- Pseudoentanglement : . $\{\psi_k\} \approx \{\phi_k\}$

  $\{(\psi_k, \phi_k)\}$. entropy gap.

$\rightarrow$ potentially useful in AdS/DFT.

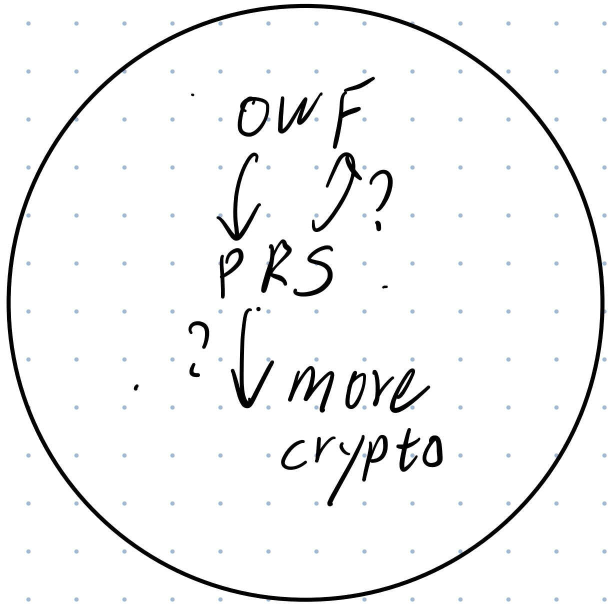
V1.0 PART B

→ Beyond: Computational lens to physics

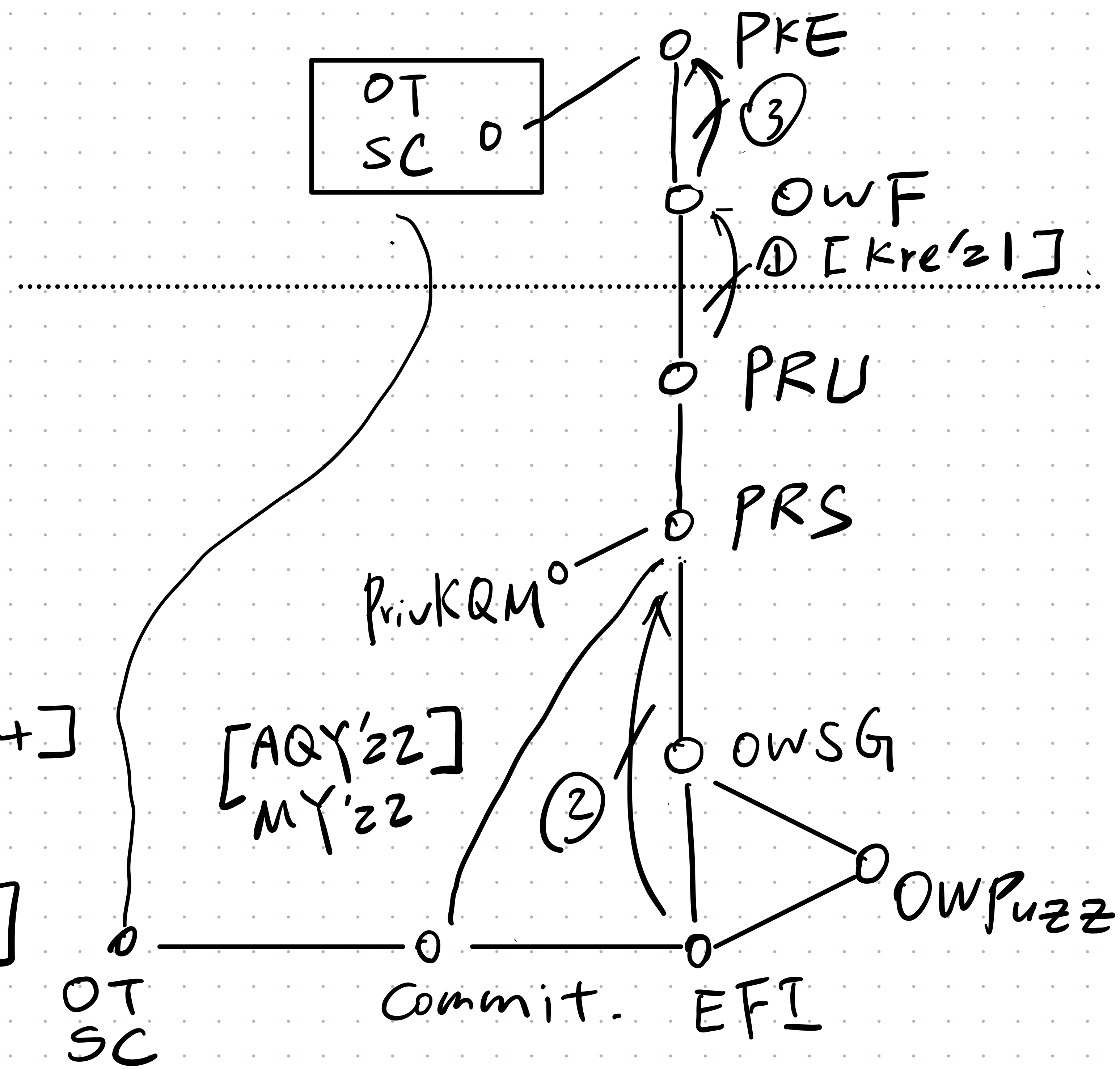
- Computational Entanglement theory [ABV'23, LREJ'25]
- pseudo-magic [GLGEYQ'24]
- pseudo-resource [GY'25]
- pseudo-thermalization
- Quantum gravity [BFV'19]

V1.0 PART C

A new Q CRYPTO Landscape



C



Oracle Separation

① $P=NP$, $\exists$ QC-OWF [KQT'25]

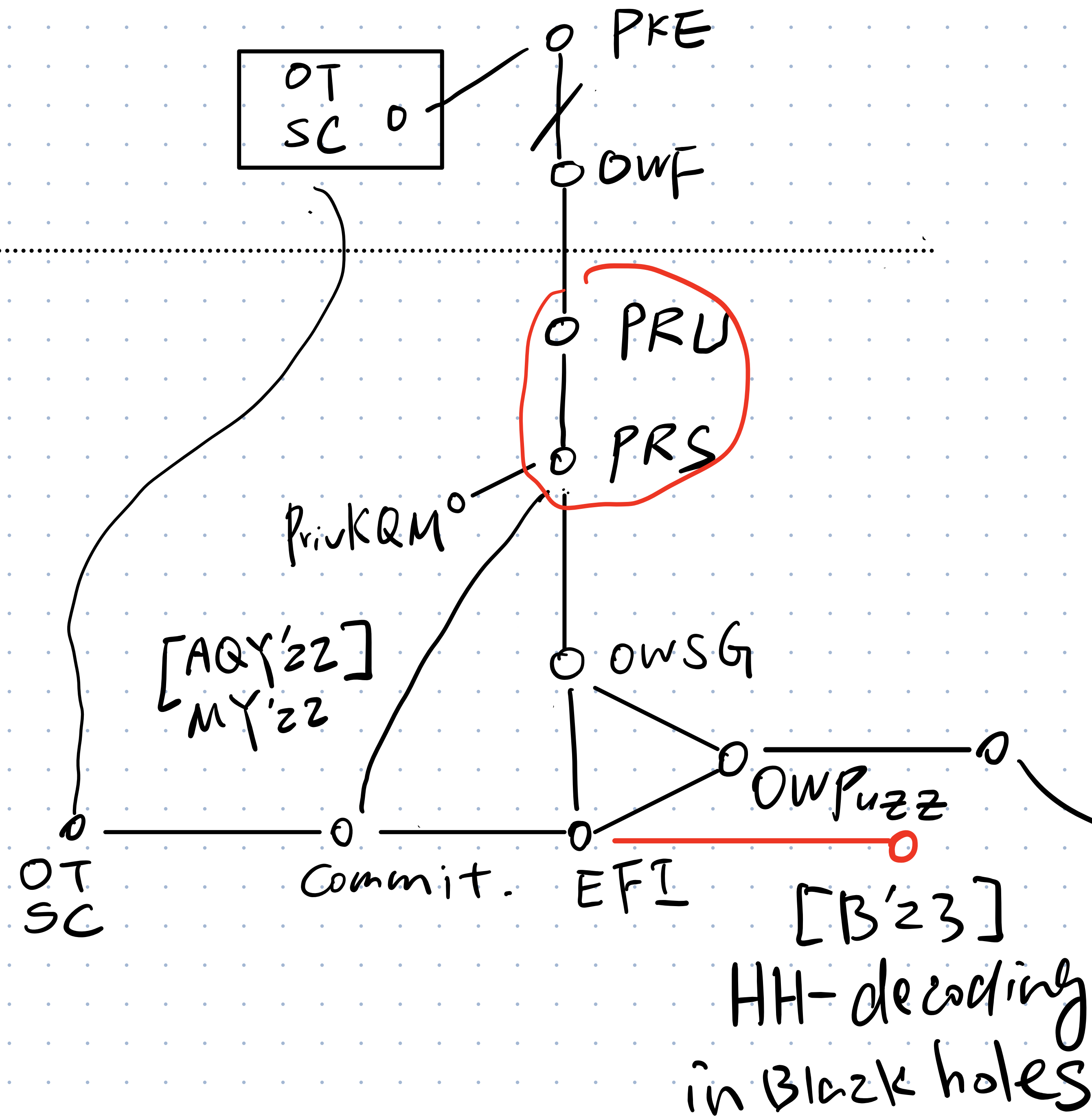
② $\exists$ Comm, !$\exists$ PRS [CCS'25 ++]

✓ $|\psi\rangle \rightarrow R_{|\psi\rangle}$ useful!

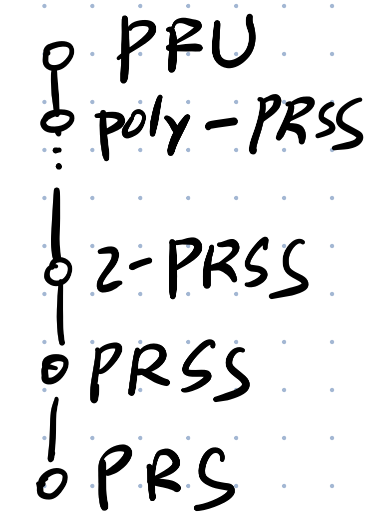
③ $\exists$OWF, !$\exists$QPKE [LLLL'25]
w/classical key

V1.0 PART C

→ Beyond:



1. More Separations
   - → unified oracles ?
   - → Pseudo-random Hierarchy



   - → A unifying primitive:
     [SW'14] iO + OWF ⇒ PKE. → Quantum?

2. Complexity foundations
   - → Minimal assumptions?
     [KT'25, HM'24, CGGH'25]
     Q sampling, Meta-Complexity.
   - → New Q Complexity theory
     [BEMPQY'24, CCHS'24]

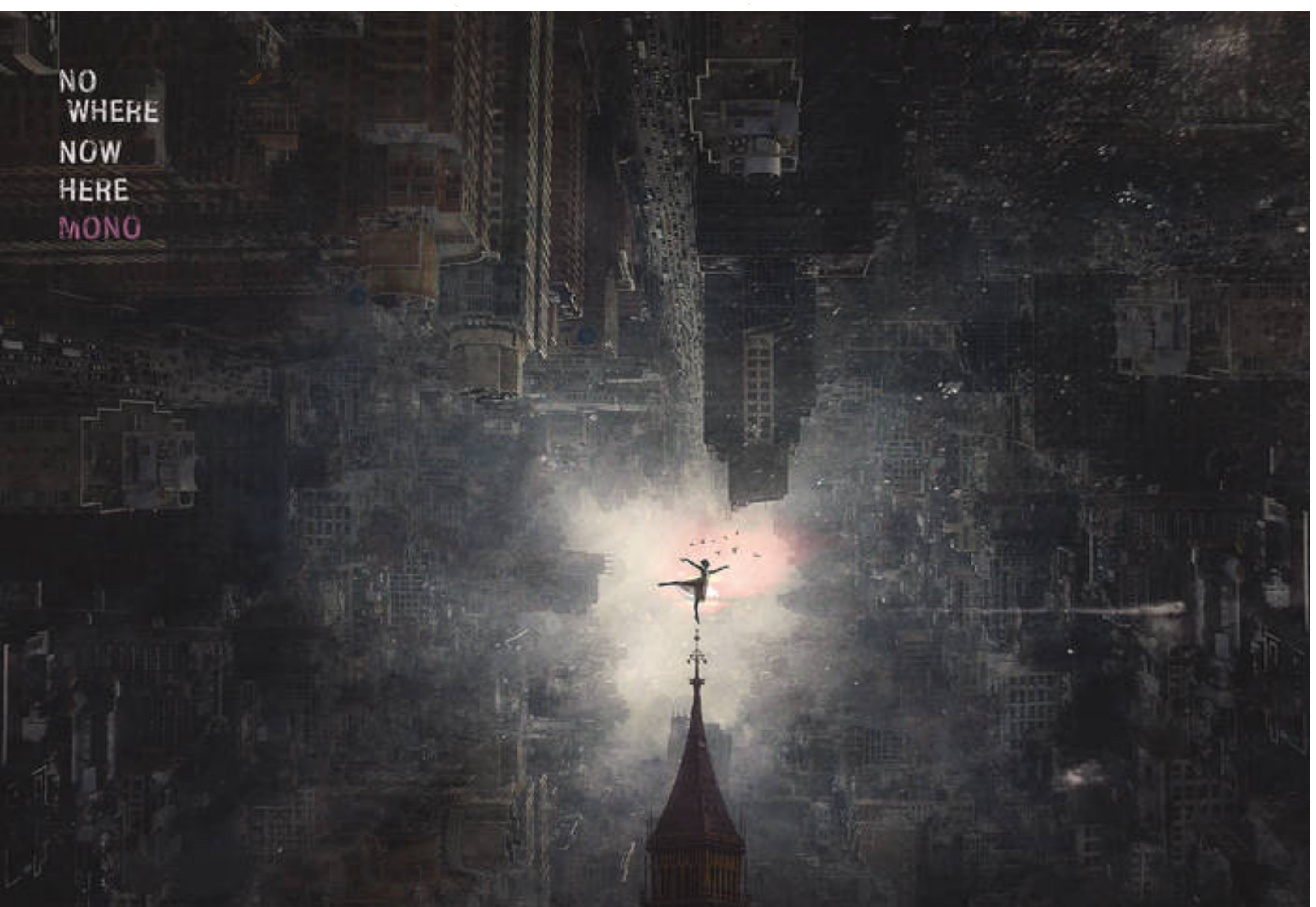
Quantum Pseudorandomness

V0.1 → V1.0

☆ Randomizing methods : R. phase, R. subset (π), Kaz-like

Analyzing methods : 1st principle, PATH-Recording, Rapid Mixing

V2.0?



A. Post - PRU

B. Comp. lense to physics

C. Brave-new QCRYPTO