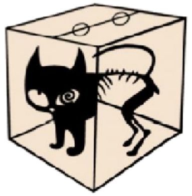
Pseudorandom Quantum States



Fang Song

Portland State U → Texas A&M U

Joint work with

Zhengfeng Ji

U of Technology, Sydney

Yi-Kai Liu

NIST &

U of Maryland

Randomness is useful

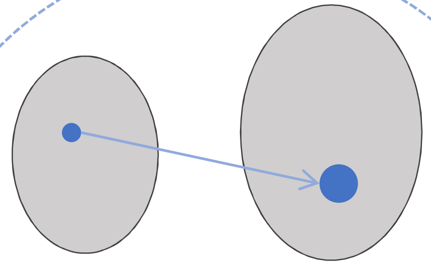
Algorithm Design	Probabilistic constructions	Cryptography

Algorithm Design

Is it Prime?

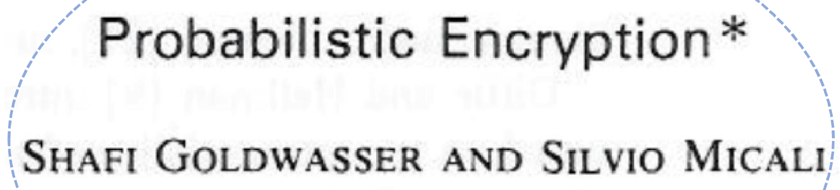
20,988,936,657,440,58
6,486,151,264,256,610
,222,593,863,921

Probabilistic constructions



Good error-correction codes exist: random codes

Cryptography

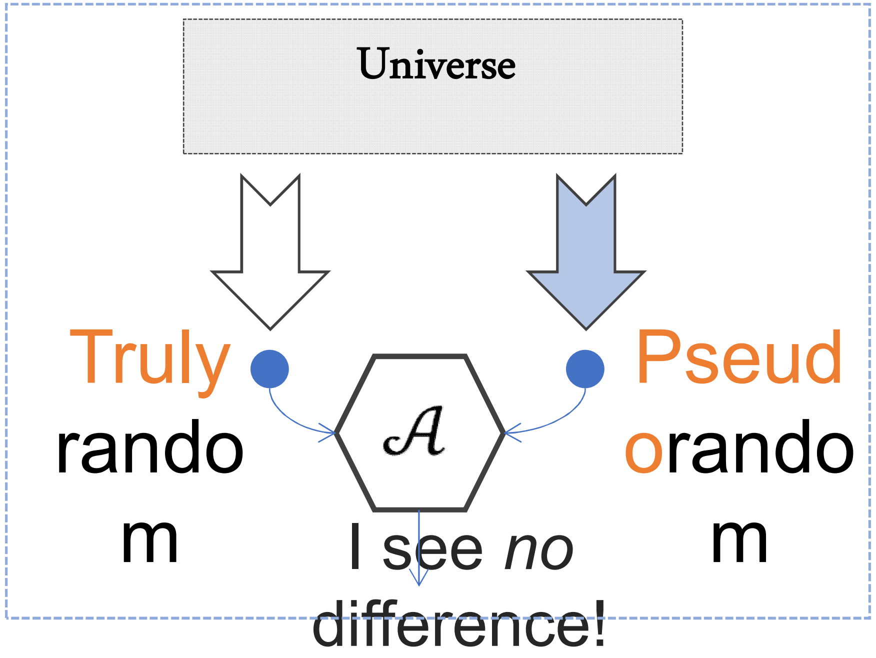

Probabilistic Encryption*

SHAFI GOLDWASSER AND SILVIO MICALI

But randomness can be expensive

EX. Sampling a random Boolean function $f:\{0,1\}^n \to \{0,1\}$ costs 2^n random coins!

Pseudo-randomness is (as or more) useful



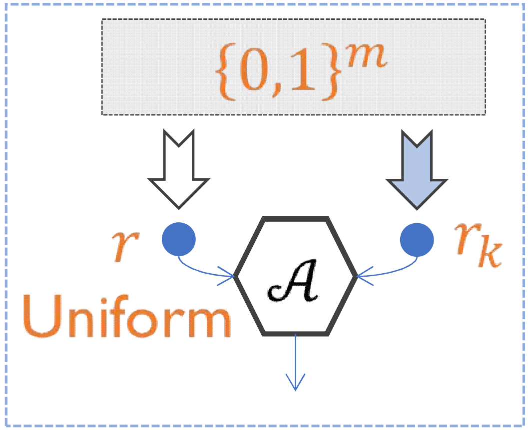
- Efficient sampling algorithm
- Samples "look" random,

… in the eyes of any efficient observer $\mathcal{A}$

(*computationally indistinguishable*)

Important pseudorandom objects

Pseudorandom string generator (PRG) ⟺ One-way functions ⟺ Pseudorandom function family (PRF)



- $\{r_k\} \subseteq \{0,1\}^m$
- $k \leftarrow \{0,1\}^n, m \gg n$: seed
- $\exists G$ efficient: $r_k = G(k)$

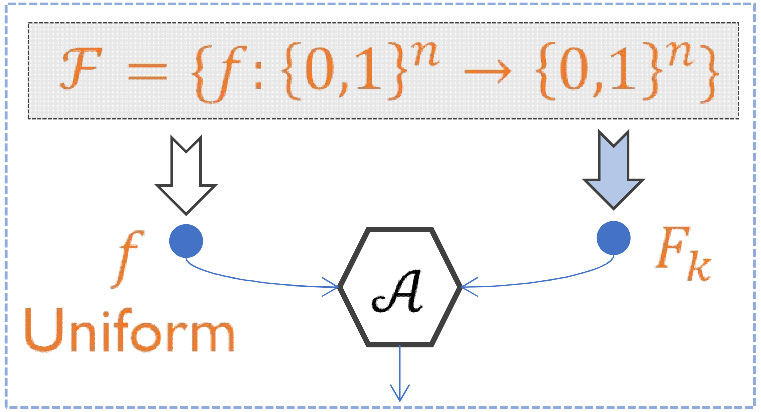
Applications

Stream ciphers,

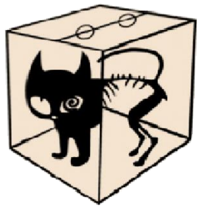
Block ciphers,

Message authentication,

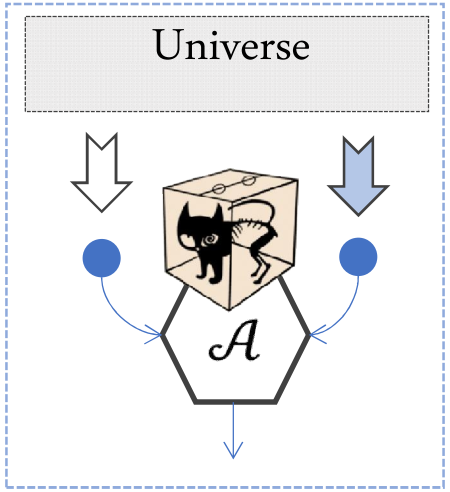
…

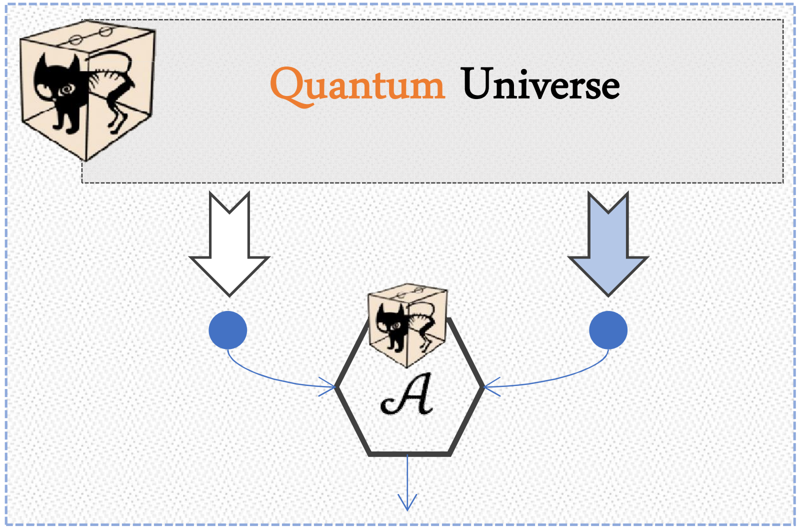


- $\{F_k\} \subseteq \mathcal{F}$
- $k \leftarrow \{0,1\}^n$: key
- Can compute $F_k(x)$ efficiently



What about a quantum world?





Theorem: quantum-secure PRGs & PRFs exist, under reasonable assumptions.

A theory of quantum pseudo-randomness?

Our Contributions

1 Defining Pseudorandom Quantum States (PRS)

- Analogous to pseudorandom string generator

2 Efficient construction of PRS

- Black-box construction from any quantum-secure PRF

3 Properties and applications

- Equivalent formulations
- Cryptographic no-cloning of PRS

➔ Private-key quantum money from any PRS

✧ Initial exploration of pseudorandom unitary operators

- Analogous to pseudorandom functions

Understanding the quantum objects

Quantum states

- Quantum bit (qubit) $|\psi\rangle$: unit vector in complex plane $\mathbb{C}^2$ (continuous!)
- n-qubits $|\psi\rangle$: unit vector in $(\mathbb{C}^2)^{\otimes n} = \mathbb{C}^{2^n}$

Haar-random states $|\psi\rangle \leftarrow \mu$

- Testing physics theories: thermalization …
- Needs $\exp(n)$ bits to describe & sample (a fine discretization)

Contrast with PRG

- Bit $b \in \{0,1\}$
- n-bit string $s \in \{0,1\}^n$
- Uniform distr. on $\{0,1\}^m$

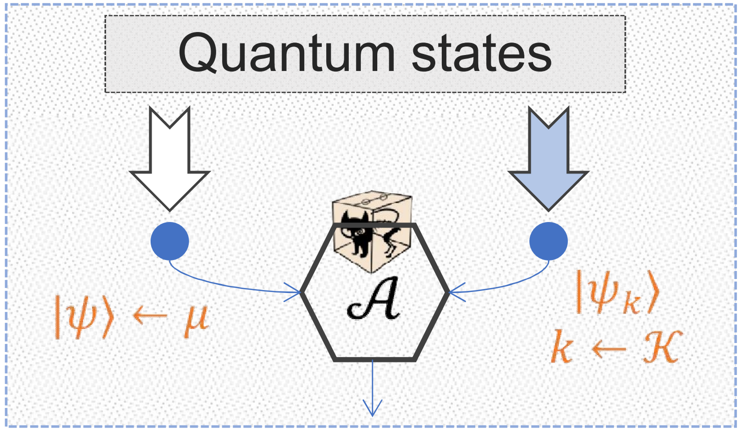
Defining pseudorandom quantum states

- Consider a family of n-qubit states $\{|\psi_k\rangle\}$, $k \in \mathcal{K} \subseteq \{0,1\}^n$

Def. 0. $\{|\psi_k\rangle\}$ is pseudorandom, if

1. Efficient generation of $|\psi_k\rangle$
2. Indistinguishable from Haar-random: $\forall$poly-time $\mathcal{A}$,

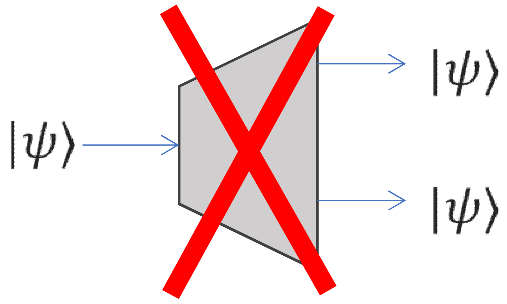
$$\Pr_{k \leftarrow \mathcal{K}}[\mathcal{A}(|\psi_k\rangle) = 1] - \Pr_{\psi \leftarrow \mu}[\mathcal{A}(|\psi\rangle) = 1] \leq negl(n)$$



- An issue with quantum no-cloning

- Classically: one-copy = multi-copy
- Quantum: # of copy matters a lot!

EX. Random basis states $\{|k\rangle\}$
1 copy: indistinguishable from Haar-random
≥ 2 copies: trivially distinguishable

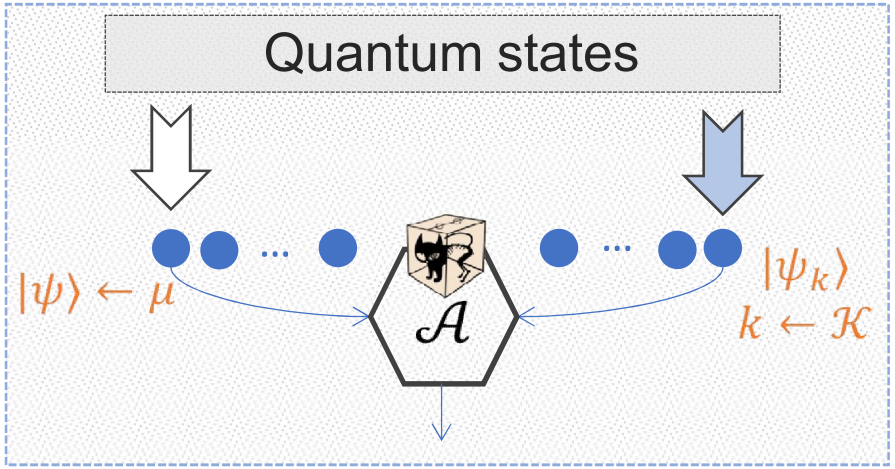


A right def. of pseudorandom quantum states

Def. 1. $\{|\psi_k\rangle\}$ is pseudorandom, if

1. Efficient generation of $|\psi_k\rangle$
2. Indist. from Haar-random with multi-copy:

$$\forall \text{poly-time } \mathcal{A}, \forall \text{poly } q(\cdot)$$
$$\Pr_{k \leftarrow \mathcal{K}}\left[\mathcal{A}(|\psi_k\rangle^{\otimes q(n)}) = 1\right] - \Pr_{\psi \leftarrow \mu}\left[\mathcal{A}(|\psi\rangle^{\otimes q(n)}) = 1\right] \le negl(n)$$



Our Contributions

1 Defining Pseudorandom Quantum States (PRS)

2 Efficient construction of PRS

3 Properties and applications

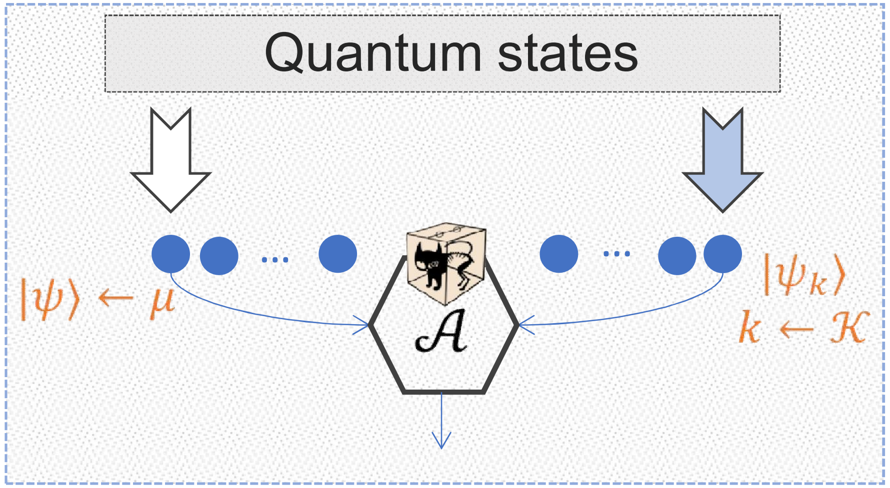
- Equivalent formulations
- Cryptographic no-cloning of PRS

➔ Private-key quantum money from any PRS

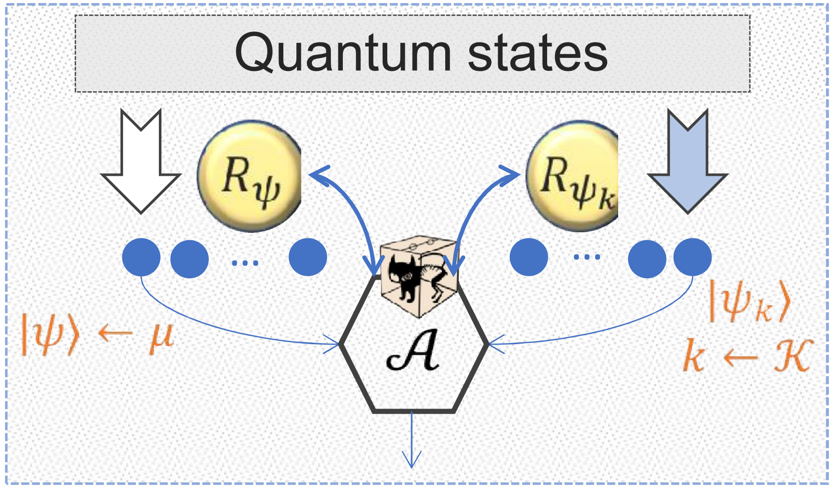
✦ Initial exploration of pseudorandom unitary operators

An equivalent definition

Def. 1. (Multi-copy) PRS



Def. 1'. PRS w. reflection oracle



$R_\phi = I - 2|\phi\rangle\langle\phi|$

- $|\phi\rangle \to -|\phi\rangle$
- Identity on $|\phi\rangle^\perp$

Theorem A. Def. 1. $\equiv$ Def. 1'.

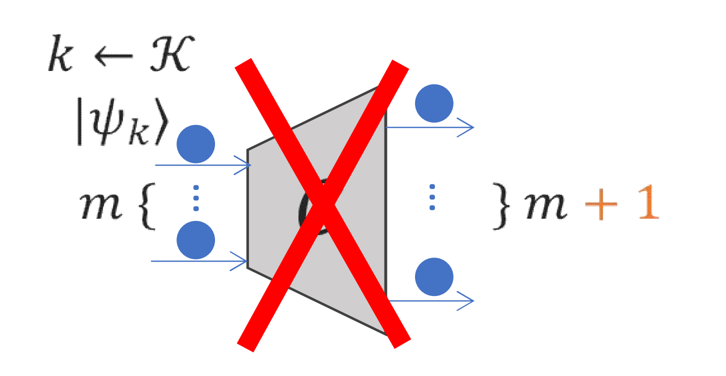
Proof Idea. Use multiple copies of $|\phi\rangle$ to simulate R_ϕ.

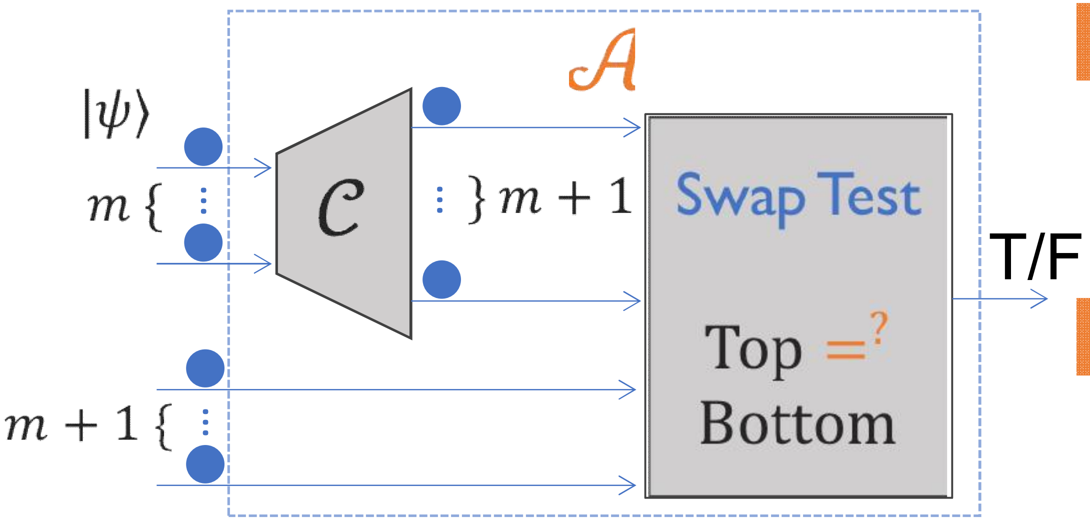
PRS is hard to clone, efficiently

Theorem B. For any efficient $\mathcal{C}$,

$$\mathbb{E}_k \langle (|\psi_k\rangle)^{\otimes m}, \mathcal{C}(|\psi_k\rangle^{\otimes m}) \rangle \leq negl(n)$$

Proof Idea. A good copier gives a good distinguisher





1

$|\psi\rangle \leftarrow \mu$, Haar-random

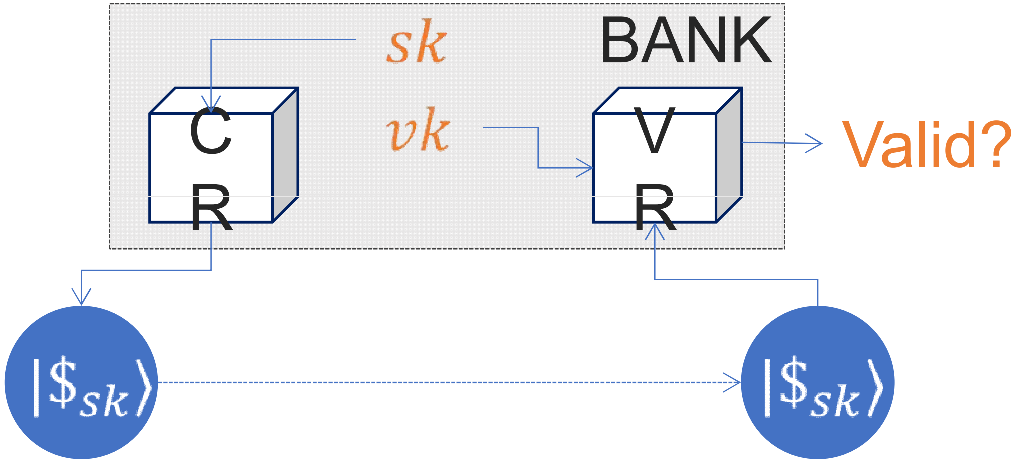
- Unconditionally no-cloneable [Werner'98]
- Swap Test outputs **Fail**

2

$|\psi\rangle = |\psi_k\rangle, k \leftarrow \mathcal{K}$, PRS

- If $\mathcal{C}$ a good copier
- Then Swap Test outputs **True**

Quantum money from any PRS



- Private-key vs. Public-key

  $sk = vk$, only bank can verify

  $sk \neq vk$, anyone w. vk can verify

- Security: no-counterfeiter (VR available for free)
  - Classically impossible

Theorem: any PRS yields a private-key money scheme

Proof. Given PRS $\{|\psi_k\rangle\}$, let $|\$_{sk}\rangle := |\psi_k\rangle$

Theorem A + Theorem B $\Rightarrow$ $|\psi_k\rangle$ hard to clone given VR oracle

- Wisner'69 – present
- 1^{st} provable-secure scheme: AC'STOC12 (from a specific algebraic assumption)
- Our scheme: generic, based on PRF (better confidence & efficiency)

Our Contributions

1. Defining Pseudorandom Quantum States (PRS)

2. Efficient construction of PRS
   - Black-box construction from any quantum-secure PRF

3. Properties and applications

✦ Initial exploration of pseudorandom unitary operators

Random phase states are pseudorandom

$$|\psi_k\rangle := \sum_{x\in[N]} \omega_N^{F_k(x)} |x\rangle$$

$F_k: \{0,1\}^n \to \{0,1\}^n$
quantum-secure PRF

- $N = 2^n, \omega_N = e^{2\pi i/N}$

Theorem. $\{|\psi_k\rangle\}$ is a PRS.

- Pseudorandom

1. Switch F_k to truly random f: $|\tilde{\psi}_k\rangle := \sum_{x\in[N]} \omega_N^{f(x)} |x\rangle$
2. Small expected distance between $|\tilde{\psi}_k\rangle$ and $|\psi\rangle \leftarrow \mu$

- Efficient generation: Quantum Fourier Transform

Our Contributions

1 Defining Pseudorandom Quantum States (PRS)

2 Efficient construction of PRS

3 Properties and applications

✧ Initial exploration of pseudorandom unitary operators

- Analogous to pseudorandom functions

Pseudorandom Unitary Operators

Unitary operator U

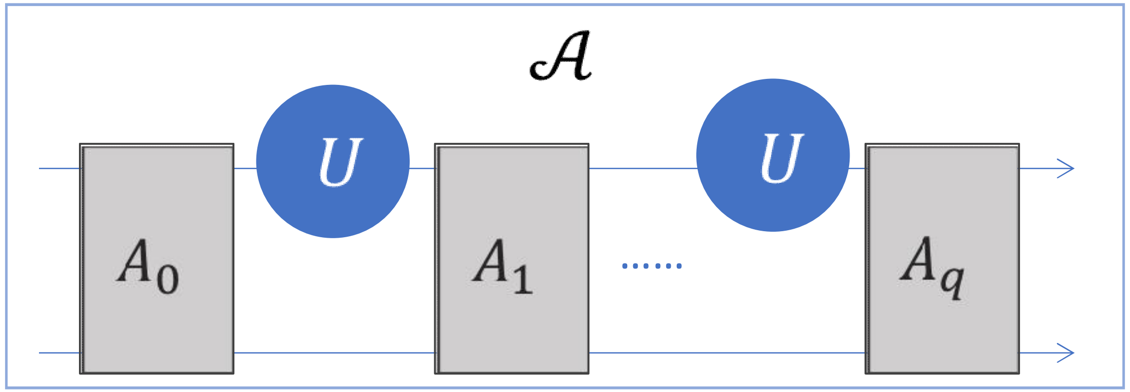
- $UU^* = I$: reversible, length-preserving
- Ex. rotation, phase change, …

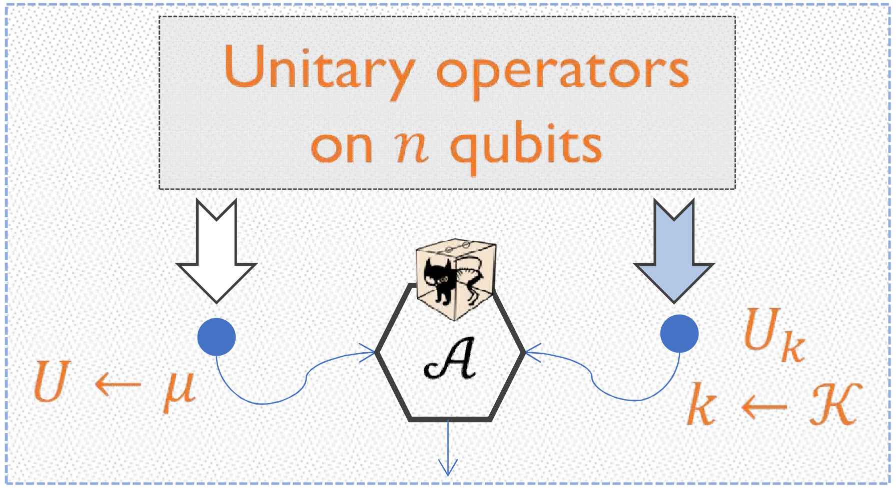
Haar-random unitary $U \leftarrow \mu$

- Apps in algorithms, crypto …
- Needs $\exp(n)$ bits to describe & sample (a fine discretization)

Def. $\{U_k\}$ is pseudorandom, if

1. Efficient circuit computing U_k
2. $U_k \approx U \leftarrow \mu$



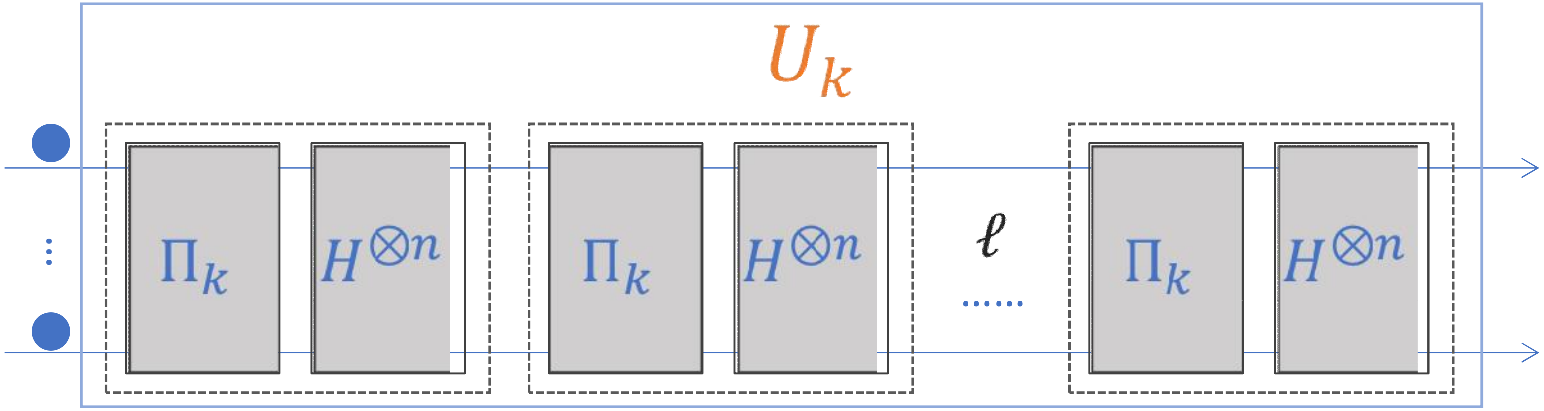


PRU Candidate

Q-Secure PRF ➔

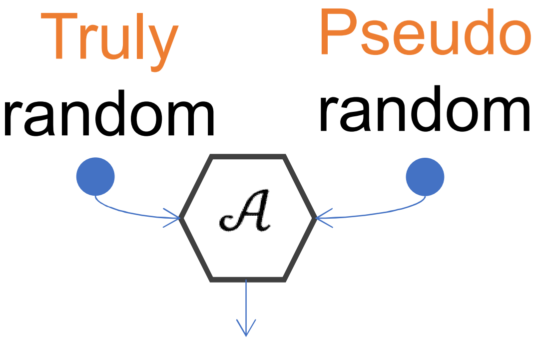
$\Pi_k: \{0,1\}^n \to \{0,1\}^n$
quantum-secure
pseudorandom permutation

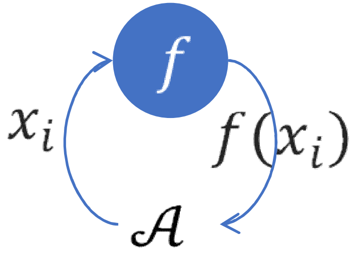
H: change of basis

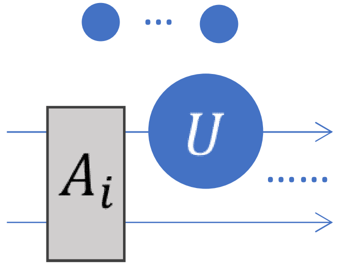


Conjecture. $\{U_k\}$ is PRU when $\ell \geq 3$.

Related work: statistical pseudorandom







True Randomness	Statistical Pseudorandomness (t-wise independence)	Computational Pseudorandomness
Unbounded $\mathcal{A}$	Unbounded $\mathcal{A}$ $\leq t$ obs	Poly-time $\mathcal{A}$ $\leq$ poly observations
Uniform Random Func.	t-wise indep. Hash (t pre-determined)	PRF ($\forall$poly-many queries)
Haar-R State	State t-design	PRS
Haar-R Unitary	Unitary t-design	PRU
	A lot work & apps (quantum auth./enc.)	Plug-n-play?

1 Defining Pseudorandom Quantum States (PRS)

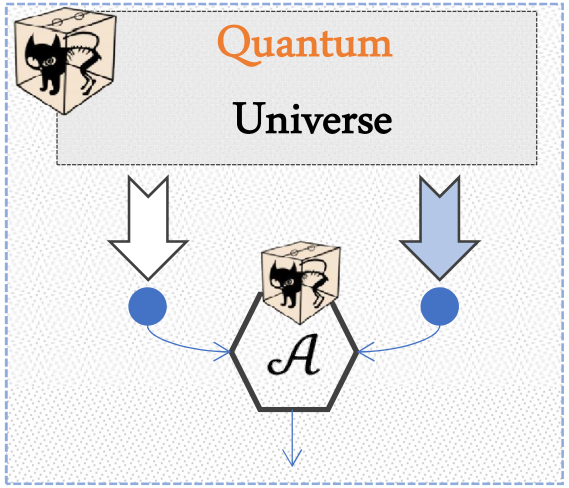
- Multi-copy$\neq$single copy

2 Efficient PRS from any PRF

- $|\psi_k\rangle := \sum \omega_N^{F_k(x)} |x\rangle$

Q1. How about: $|\phi_k\rangle := \sum_{x \in [N]} (-1)^{F_k(x)} |x\rangle$?

Q2. Is PRF necessary? PRS→OWF?



3 Properties and applications

- Private-key quantum money
- High entanglement; thermalization,

Q3. Public-key quantum money from PRS?

Thank you!

✧ Pseudorandom unitary operators

Q4. Proving candidate constructions?

A unified theory of quantum pseudo-randomness?