$$\begin{tikzcd}
 & PRS \arrow[dr] & \\
OWF \arrow[ur, "(13)"] \arrow[dr, "(12)"'] & & EFI \arrow[dl] \\
 & \text{comm} \arrow[r] & OT \arrow[u]
\end{tikzcd}$$

Def

EFI pair: non-trivial computational indistinguishability

1. <u>E</u>fficient generation: QPT procedure Gen:

$$\mathrm{Gen}(1^\lambda, 0) \to \rho_{0,\lambda} \qquad \mathrm{Gen}(1^\lambda, 1) \to \rho_{1,\lambda}$$

2. Statistical <u>F</u>arness: $\underset{\frac{1}{2}\|\rho-\sigma\|_1}{\overset{}{\mathrm{TD}}}(\rho_{0,\lambda}, \rho_{1,\lambda}) \geq 1 - 2^{-\lambda}$.

$\frac{1}{2}\|\rho - \sigma\|_1$ $=$ (Holevo-Helstrom)

3. Computational <u>I</u>ndistinguishability: $\rho_0 \approx_c \rho_1$

$$\left(\begin{array}{l} \forall \text{QPT } A \ \forall \{\alpha_\lambda\}_\lambda \ \exists \text{ negligible } \nu \ \forall \lambda: \\ \quad \left| \Pr[A(\alpha_\lambda, \rho_{0,\lambda}) = 1] - \Pr[A(\alpha_\lambda, \rho_{1,\lambda}) = 1] \right| \leq \nu(\lambda). \end{array} \right)$$

<u>Ex</u>

1. PKE $\Rightarrow$ EFI

   $\{pk, \mathrm{Enc}(pk, 0)\}$ vs $\{pk, \mathrm{Enc}(pk, 1)\}$

2. stat binding commitment $\Rightarrow$ EFI

   $$\mathrm{Comm}(0)_R \qquad \text{vs} \qquad \mathrm{Comm}(1)_R$$

   $F(\mathcal{E}_0, \mathcal{E}_1) \leq 1 - \mathrm{TD}(\mathcal{E}_0, \mathcal{E}_1)^2$ is negl. (Fuchs-van de Graaf)

3. PRS

Theorem Let $G: \{0,1\}^\lambda \to S(2^n)$ be PRS secure against t copies. Then $\exists$ EFI if

$$\binom{2^n+t-1}{t} \gg 2^\lambda.$$

Proof $\mathcal{E}_0 = \mathbb{E}_k[G(k)^{\otimes t}]$. rank $\mathcal{E}_0 \leq 2^\lambda$.

$\cap$

$\mathcal{E}_1 = \dfrac{\Pi_{sym}^{2^n,t}}{\mathrm{Tr}(\Pi_{sym}^{2^n,t})}$. rank $\mathcal{E}_1 = \mathrm{Tr}(\Pi_{sym}^{2^n,t})$.

$$\Rightarrow TD \geq 1 - \frac{\text{rank } \mathcal{E}_0}{\text{rank } \mathcal{E}_1}$$

Select t $n \geq \lambda + 1$: $t = 1$

$n \geq \log_2 \lambda$: $t = \lambda + 1$

Theorem EFI $\Rightarrow$ commitment. [Chailloux, Kerenidis, Rosgen'11]

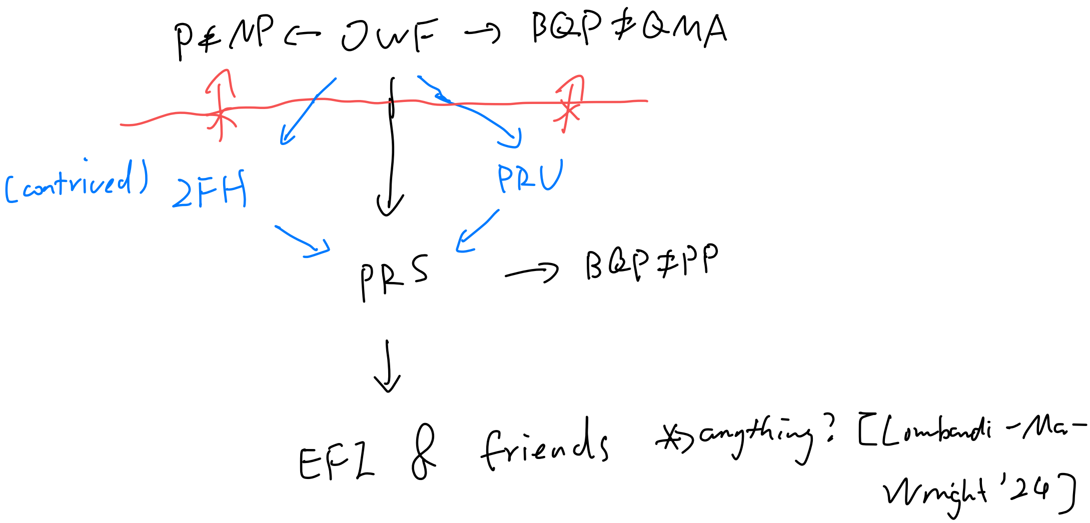
Proof Purify $\mathcal{E}_b \to |\mathcal{E}_b\rangle_{OP}$

O is commitment/output, P is reveal/purification

$$\begin{array}{ccc} |\mathcal{E}_b\rangle_{OP} & \xrightarrow{\text{comm}} & O \leftarrow \mathcal{E}_b \\ \downarrow & & \downarrow \\ P & \xrightarrow{\text{open}} & |\mathcal{E}_b\rangle \end{array}$$

$\Rightarrow$ comm. hiding

binding $\Leftarrow$ s.f. + Uhlmann



$\boxed{\text{Def}}$ PRU is a pseudorandom unitary if [JLS18]

(1.) $\forall k$ $\exists$ unitary U_k on n qubits s.t. $PRU(k, |\psi\rangle) = U_k|\psi\rangle$

(2.) PRU is efficient.

(3.) $\forall$ QPT A, $\left| \Pr_{k \sim \{0,1\}^\lambda} \left[A^{U_k}(1^\lambda) = 1 \right] - \Pr_{U \sim \mu_{2^n}} \left[A^{U}(1^\lambda) = 1 \right] \right| = negl.$

Non-adaptive if (3.) only holds $\forall$ QPT A w/ query depth 1.

$\boxed{\text{Claim}}$ OWF $\Rightarrow$ naPRU. [Metger-Poremba-Sinha-Yuen '24]

$\boxed{\text{Open}}$ OWF $\Rightarrow$ PRU?

$\boxed{\text{Claim}}$ n-qubit PRU $\Rightarrow$ n-qubit PRS.

Proof $PRS(k) = PRU(k, |0^n\rangle) \Rightarrow t$ copies can be prepared w/ t queries.

$\boxed{\text{Open}}$ $PRS \Rightarrow$ naPRU? (Classically $PRG \Rightarrow PRP$)

Theorem [Kretschmer '21] $\exists$ quantum oracle $\mathcal{U}$, $BQP^{\mathcal{U}} = QMA^{\mathcal{U}}$, and $\exists PRU$ relative to $\mathcal{U}$.

Construction $\mathcal{U}$ is Haar random: $\mathcal{U} = (\mathcal{U}_x : x \in \{0,1\}^*)$

$$\mathcal{U}_x \xleftarrow{\$} \mu_{2^{n(|x|)}}$$

P is a PSPACE-complete language.

(so that $BQP^P = QMA^P$)

$\exists PRU^{\mathcal{U}, P}$: $PRU^{\mathcal{U}}(k, |\psi\rangle) = \mathcal{U}_k |\psi\rangle$.

Hyb 0: $A^{\mathcal{U}, P, U_k}(1^\lambda)$.

BBBV theorem

Hyb 1: $A^{\mathcal{U}', P, U_k}(1^\lambda)$.

$$\mathcal{U}'_{k'} = \begin{cases} \mathcal{U}_{k'}, & k' \neq k \\ U', & k' = k \end{cases}$$

Hyb 2: $A^{\mathcal{U}, P, U'}(1^\lambda)$ identical

$BQP^{\mathcal{U},P} = QMA^{\mathcal{U},P}$: $QMA^{\mathcal{U},P} \to QMA^{\mathcal{U}',P}$

Fact Let f be an L-Lipschitz real function in the Frobenius norm. Then $\forall \Delta > 0$,

double exp!

$$\Pr_{U \sim \mu_d} \left[f(U) \geq \mathbb{E}[f] + \Delta \right] \leq \exp\left(- \frac{(d-2)\Delta^2}{24 L^2} \right).$$

Fact A^U makes T queries to $U \Rightarrow \Pr[A^U = 1]$ is $2T$-Lip.

(Cor: BQP algs cannot extract classical info from $\mu_\lambda^{U(1)}$)

Fact $\max_{|\varphi\rangle} \Pr[A^U(|\phi\rangle) = 1]$ is $2T$-Lipschitz.

Proof Fix U, V. Let $|\psi\rangle, |\varphi\rangle$ be resp. maximizers. Then,

$$\left| \max \Pr[A^U = 1] - \max \Pr[A^V = 1] \right|$$

$$= \left| \Pr[A^U(|\psi\rangle) = 1] - \Pr[A^V(|\varphi\rangle) = 1] \right|$$

$$= \max \{ \Pr[A^U(|\psi\rangle) = 1] - \Pr[A^V(|\varphi\rangle) = 1], \\ \Pr[A^V(|\varphi\rangle) = 1] - \Pr[A^U(|\psi\rangle) = 1] \}$$

$$\leq \max \{ \Pr[A^U(|\psi\rangle) = 1] - \Pr[A^V(|\psi\rangle) = 1], \\ \Pr[A^V(|\varphi\rangle) = 1] - \Pr[A^U(|\varphi\rangle) = 1] \} \leq 2T \|U - V\|_F.$$

(Cor: QMA algs cannot extract classical info from $\mu_x^{\omega(1)}$)

<u>Pf sketch</u> 0. $QMA^{\mathcal{U}, P}$ makes $\leq T$ queries.

1. Tomography $\mathcal{U}_x$ for $|x| \leq 100 \cdot \log T$ & replace $\mathcal{U}_x$ to $\tilde{\mathcal{U}}_x$
2. Replace $\mathcal{U}_x$ for $|x| > 100 \cdot \log T$ w/ $\mu_{2^{|x|}}$. (now $\widetilde{QMA}^{P}$).
3. BQP^{P} compute step 2.

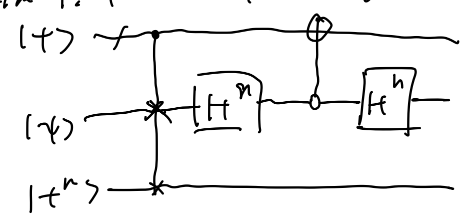
Q: Which PRS constructions remain secure if OWFs do not exist?

Hope: existing recipe might work even if function is not OW/PR?

<u>Prop [K21]</u> Binary phase PRS are insecure against BQP^{NP}.

$f(k, x) \in \{\pm 1\}$ is efficient, $|\varphi_k\rangle \propto \sum_x f(k,x)|x\rangle$.

Claim 1: $|\langle +_n|\varphi_k\rangle|$ is negl. Claim 2: distinguishable.



$$|+\rangle|\varphi_k\rangle|+^n\rangle \to |0\rangle|\varphi_k\rangle|+^n\rangle + |1\rangle|+^n\rangle|\varphi_k\rangle$$

$\approx_{\text{negl}} |0\rangle \left(|\varphi_k\rangle |+^n\rangle + |+^n\rangle |\varphi_k\rangle \right)$

$\Rightarrow$ measure gives collision of f_k.

$\Rightarrow$ find k from collisions + NP.

Interlude: What can BQP solve but not BPP if $P = NP$?

$\boxed{\text{Def}}$ (2-)Forrelation problem: $(f, g) : \{0,1\}^n \to \{\pm 1\}$,

[Aar 09]

is $\left| \langle +^n | \; g \circ H^{\otimes n} \circ f \; |+^n\rangle \right| \geq 0.01$?

Theorem [Raz-Tal '18] Forrelation is hard for PH.

Our goal is to find crypto against $BQP^{PH} \Rightarrow$ BBBV

Theorem [Aaronson-Ingram-Kretschmer '22] OR $\circ$ Forrelation hard BQP^{PH}.

$$\exists k : \left| \langle +^n | \; g_k \circ H^{\otimes n} \circ \underbrace{\boxed{f_k \; |+^n\rangle}}_{\text{binary phase}} \right| \geq 0.01?$$

$\boxed{\text{Def}}$ 2-Forrelation state for (f_k, g_k) is

$$g_k \circ H^{\otimes n} \circ f_k \, |+^n\rangle .$$

Theorem 2-Forrelation state for random oracles are

[Kretschmer-Q-Sinha-Tal '23] 1-copy pseudorandom against BQP^{PH}

Today: w/ advantage $\geq .99$.

Interpretation 2-Forrelation-hardness (2FH) is plausibly strictly weaker than OWFs & $P \neq NP$.

(see KQST23 for a formal treatment of 2FH.)

Proof sketch H_0: f, g u.a.r.

$$A^{f,g}(g_k \circ H^{\otimes n} \circ f_k |+^n\rangle)$$

H_1: f'_k, g'_k are Forrelated

$f'_{k'}, g'_{k'}, h$ are u.a.r. for $k' \neq k$.

$f = f'$, $g_{k'} = g'_{k'} \oplus h$ $\forall k'$.

$$A^{f,g}(g_k \circ H^{\otimes n} \circ f_k |+^n\rangle)$$

$$= A^{f,g}(h \circ g'_k \circ H^{\otimes n} \circ f'_k |+^n\rangle)$$

H_2: f, g, h as above

$$A^{f,g}(h \circ |+^n\rangle)$$

Forrelation $\Rightarrow$ $g'_k \circ H^{\otimes n} \circ f'_k |+^n\rangle \approx |+^n\rangle$

H_3: f'_k, g'_k are now u.a.r.

(indist for BQP^{PH} by AIK22)

$$A^{f,g}(\underbrace{h\,0|+^n\rangle}) $$

binary phase but A has 0 info on h. $\square$

$\boxed{\text{Open}}$: 1. Does MPSY24 PRU survive $P = NP$ / BQP^{PH}-secure?

2. How about random phase states w/ bigger r.o.u.?

Bonus: $BQP \not\subseteq PP$

Theorem [Huang-Kueng-Preskill '20] (Classical Shadow)

Let $O_1, \cdots, O_M$ be obs. Then $\exists$ classical PP algorithm that on input T samples of random Clifford measurements of ρ, estimate $\mathrm{Tr}(O_i \rho)$ $\forall i$ w.p. $\geq 1-\delta$ w/ add. error ε, if $T = O\left(\frac{\max \mathrm{Tr}(O_i^2)}{\varepsilon^2} \cdot \log \frac{M}{\delta}\right)$.

Thm [K21] Multi-copy PRS $\Rightarrow$ $BQP \not\subseteq PP$.

Open: Single-copy PRS $\Rightarrow$ multi-copy?