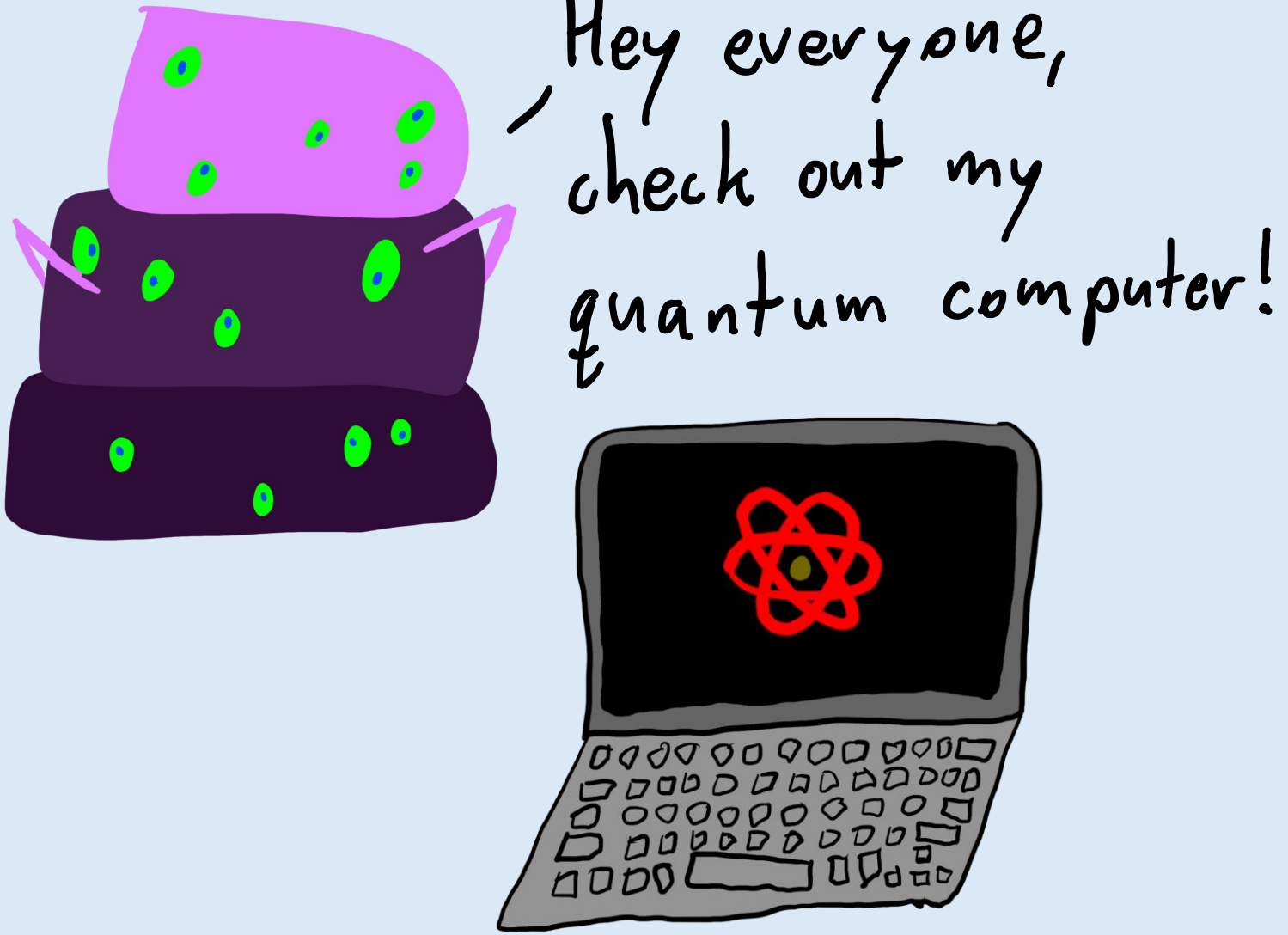
On Cryptography and Distribution Verification

with Applications to Quantum Advantage

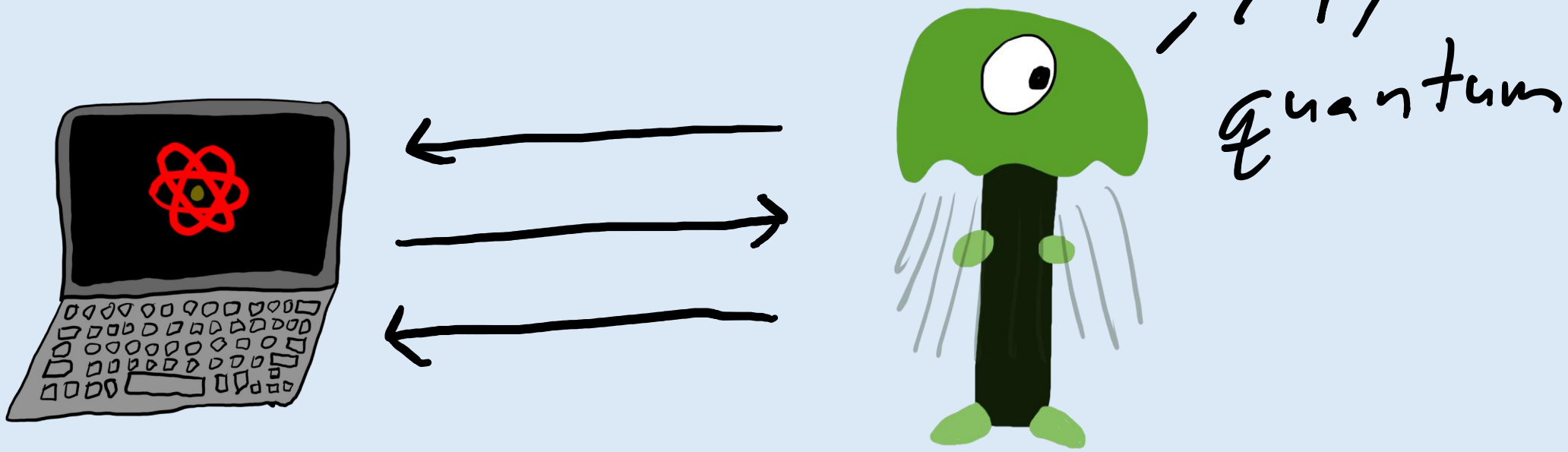
Bruno Cavalar, **Eli Goldin**, Matthew Gray, Taiga Hiroka, Tomoyuki Morimae

Quantum Advantage



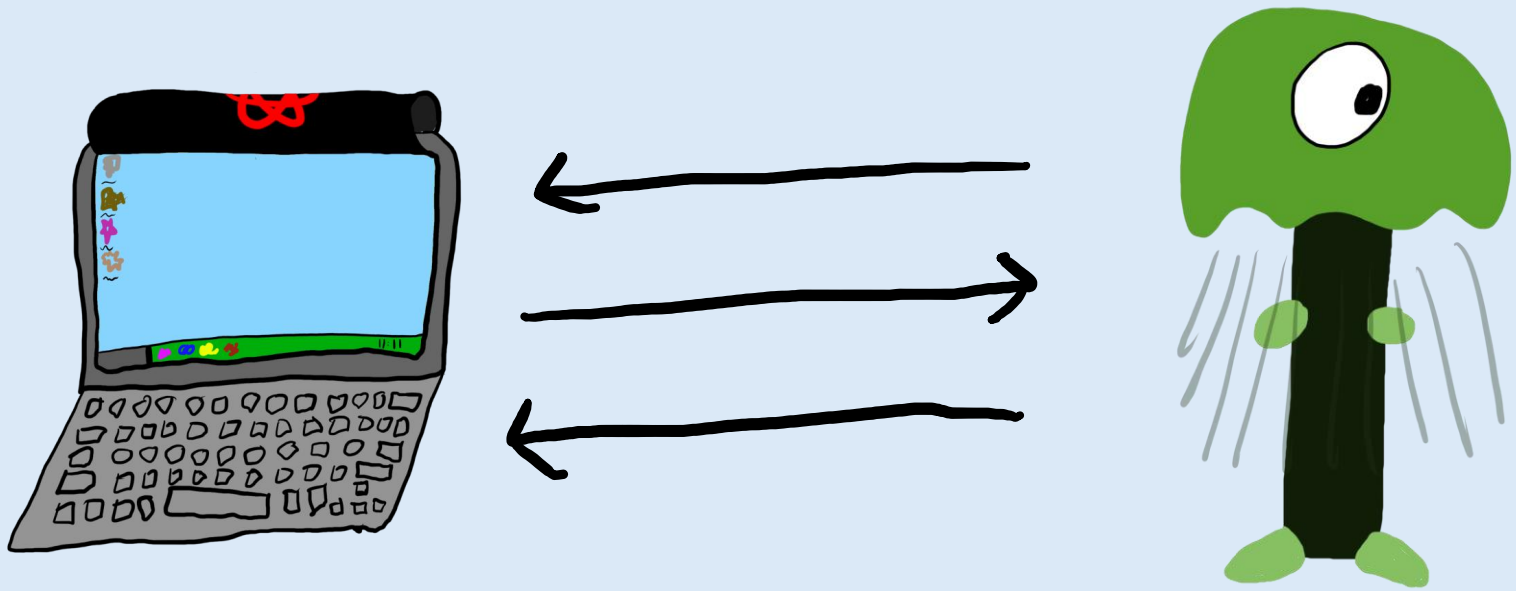
Quantum Advantage

Proof of Quantumness



Proof of Quantumness

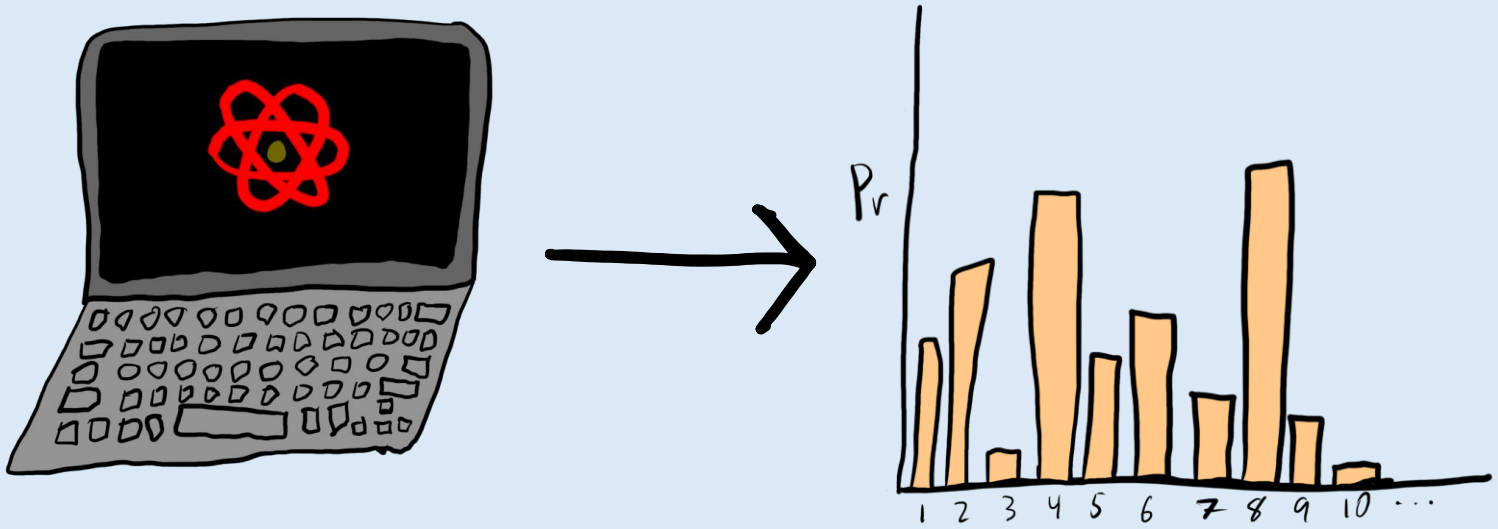
Proof of Quantumness



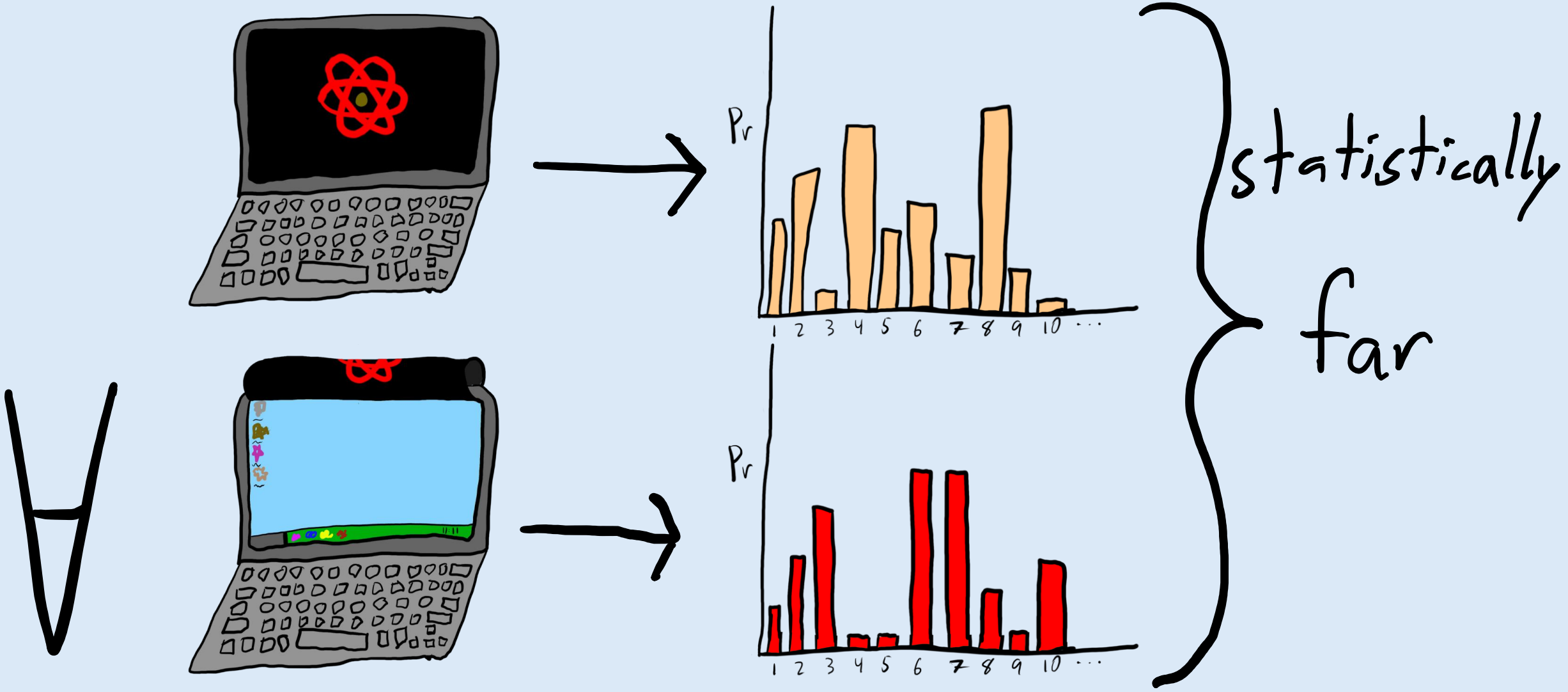
EXPENSIVE

[BCM+18, BKVV20, KMCVY21, MY22, YZ22, KLVY23, NZ23, BK

Quantum Advantage Samplers



Quantum Advantage Samplers

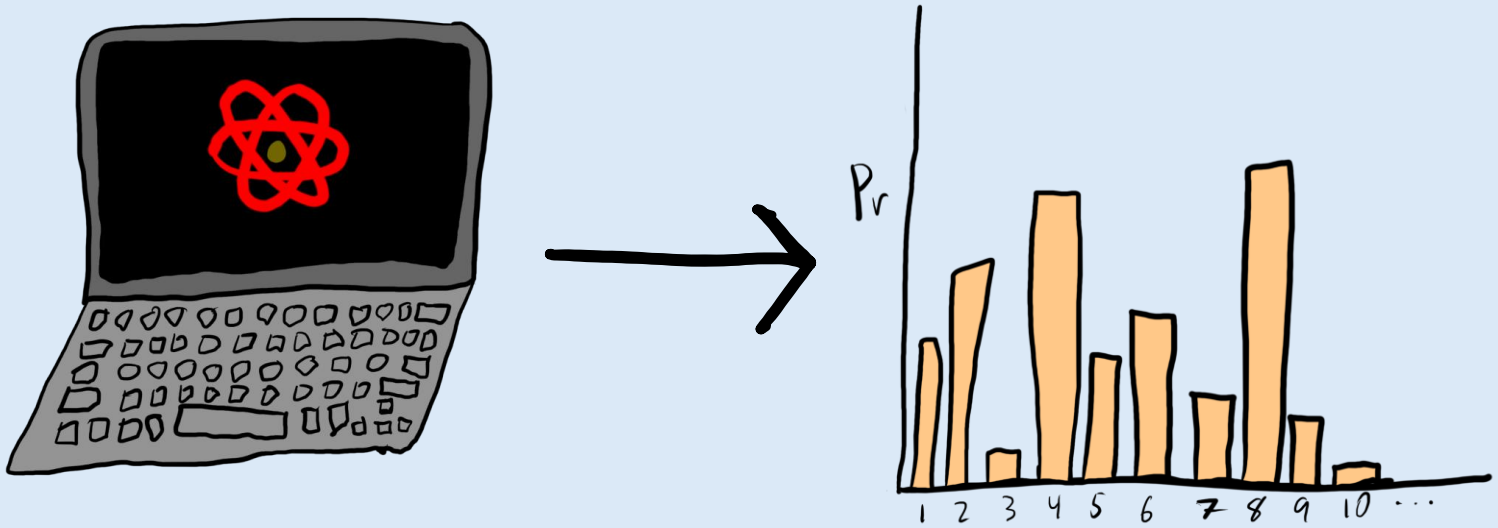


Quantum Advantage Samplers

Examples:

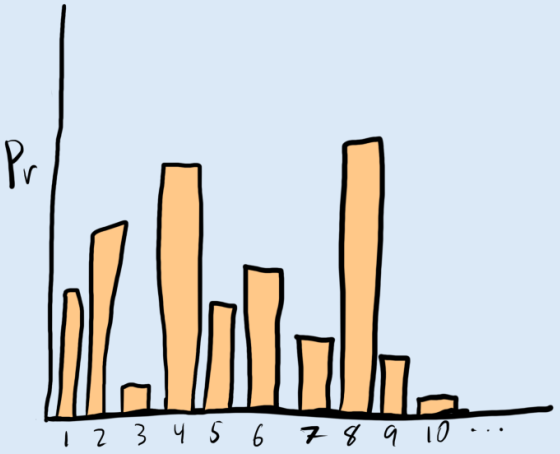
- Random circuit sampling [BFNV19]
- IQP circuits [BJS11]
- Boson sampling [AA11]

Quantum Advantage Samplers

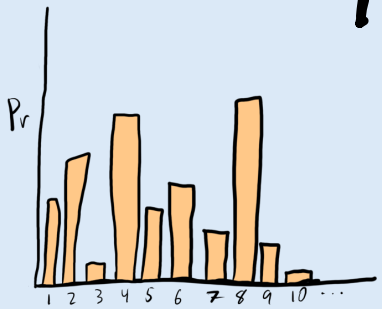


No verifier :(

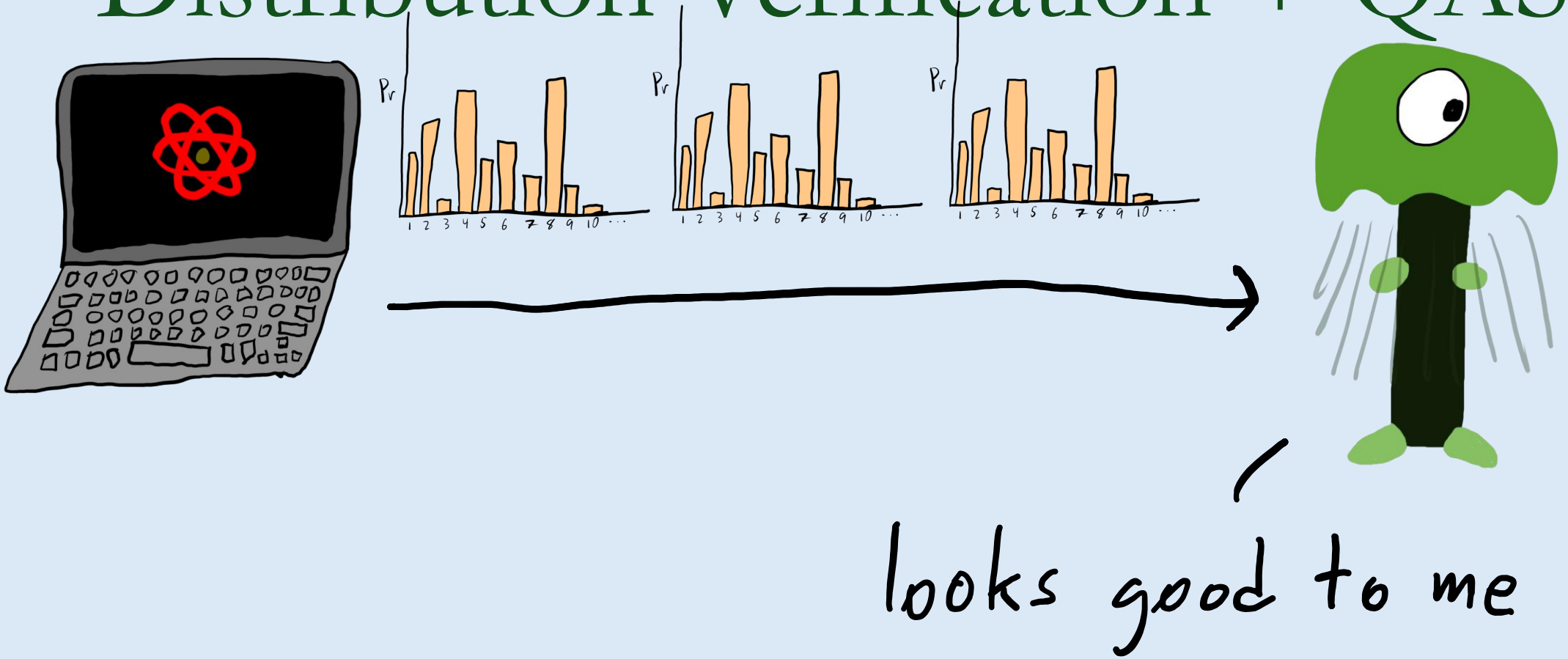
Distribution Verification

Input: 

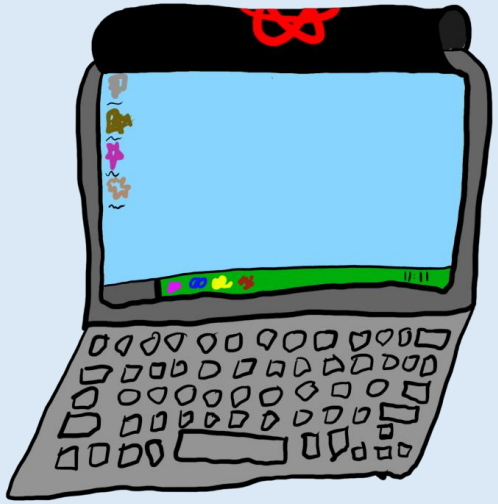
, $x_1, \ldots, x_t$

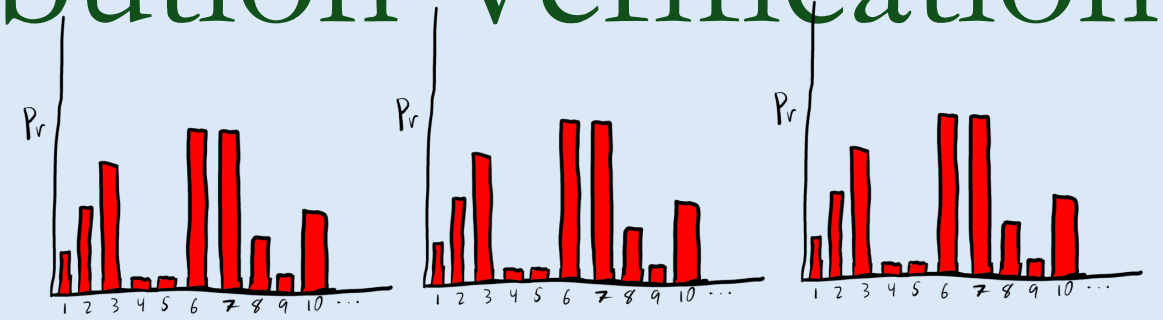
Goal: Test if $x_1, \ldots, x_t$ came from 

Distribution Verification + QAS



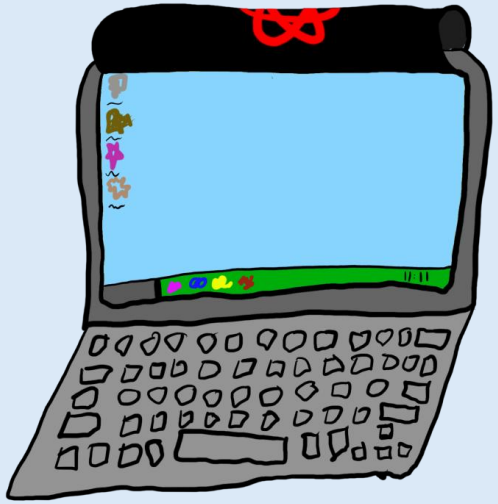
Distribution Verification + QAS

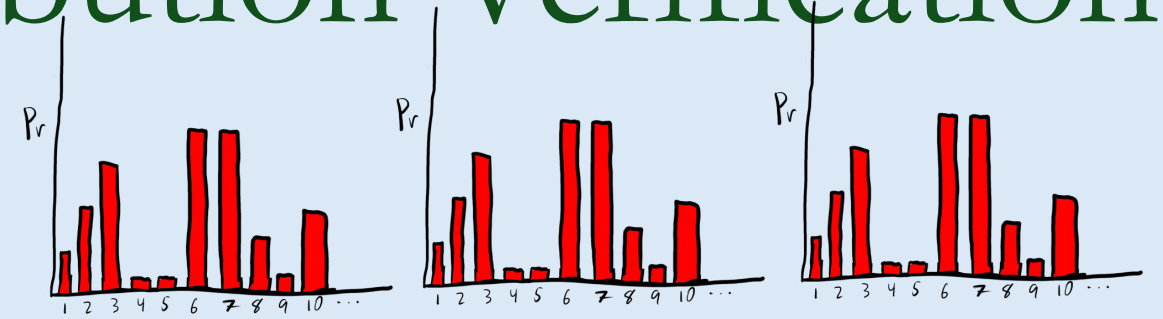




IMPOSTER

Distribution Verification + QAS





IMPOSTER

*uniform adversaries

Distribution Verification

Well studied in setting of property testing (identity test)

[BFR+00, BFR+01, DKN15, Pan08, VV17, ...]

Identity Testing

Identity test for D: Ver s.t.

- (Correctness): $\Pr_{D^+ \to x_1, \ldots, x_t} [\text{Ver}(x_1, \ldots, x_t) \to 1] \geq \text{high}$

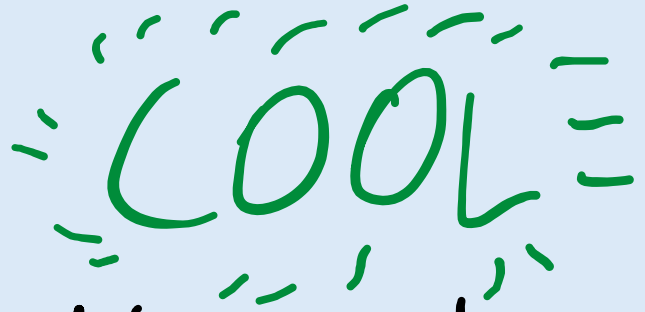
Identity Testing

Identity test for D: Ver s.t.

- (Correctness): $\Pr_{D^+ \to x_1, \ldots, x_t} [\text{Ver}(x_1, \ldots, x_t) \to 1] \geq \text{high}$
- (Security): $\forall$ inefficient G, $\Delta(G, D) \geq \varepsilon$

$$\Pr_{G^+ \to x'_1, \ldots, x'_t} [\text{Ver}(x'_1, \ldots, x'_t) \to 1] \leq \text{low}$$

Identity Testing



Identity test for D: Ver s.t.

- (Correctness): $\Pr_{D^+ \to x_1, \ldots, x_t} [\text{Ver}(x_1, \ldots, x_t) \to 1] \geq \text{high}$
- (Security): $\forall$ inefficient G, $\Delta(G, D) \geq \varepsilon$

$$\Pr_{G^+ \to x'_1, \ldots, x'_t} [\text{Ver}(x'_1, \ldots, x'_t) \to 1] \leq \text{low}$$

Identity Testing

[BFF+01, Pan08, VV17]:

D over $\{0,1\}^n$

optimal sample complexity: $\Omega(2^{n/2})$

Identity Testing

[BFF+01, Pan08, VV17]:

D over $\{0,1\}^n$

optimal sample complexity: $\Omega(2^{n/2})$

Our Approach

Identity test for D: Ver s.t.

- (Correctness): $\Pr_{D^+ \to x_1, \ldots, x_t} [\text{Ver}(x_1, \ldots, x_t) \to 1] \geq \text{high}$
- (Security): $\forall$ inefficient G, $\Delta(G, D) \geq \varepsilon$

$$\Pr_{G^+ \to x'_1, \ldots, x'_t} [\text{Ver}(x'_1, \ldots, x'_t) \to 1] \leq \text{low}$$

Our Approach

Identity test for D: Ver s.t.

- (Correctness): $\Pr_{D^+ \to x_1, \ldots, x_t} [\text{Ver}(x_1, \ldots, x_t) \to 1] \geq \text{high}$
- (Security): $\forall$ inefficient G, $\Delta(G, D) \geq \varepsilon$

$$\Pr_{G^+ \to x'_1, \ldots, x'_t} [\text{Ver}(x'_1, \ldots, x'_t) \to 1] \leq \text{low}$$

Our Approach

Identity test for D: Ver s.t.

- (Correctness): $\Pr_{D^+ \to x_1, \ldots, x_t} [\text{Ver}(x_1, \ldots, x_t) \to 1] \geq \text{high}$
- (Security): ~~$\forall$~~ efficient G, $\Delta(G, D) \geq \varepsilon$

$$\Pr_{G^+ \to x'_1, \ldots, x'_t} [\text{Ver}(x'_1, \ldots, x'_t) \to 1] \leq \text{low}$$

Our Approach

Identity test for D: Ver s.t.

- (Correctness): $\Pr_{D^+ \to x_1, \ldots, x_t} [\text{Ver}(x_1, \ldots, x_t) \to 1] \geq \text{high}$
- (Security): $\forall$ ~~inefficient~~ efficient G, $\Delta(G, D) \geq \varepsilon$

$$\Pr_{G^+ \to x'_1, \ldots, x'_t} [\text{Ver}(x'_1, \ldots, x'_t) \to 1] \leq \text{low}$$

Our Approach

Identity test for D: Ver s.t.

- (Correctness): $\Pr_{D^+ \to x_1, \ldots, x_t} [\text{Ver}(x_1, \ldots, x_t) \to 1] \geq \text{high}$
- (Security): $\forall$ efficient G, $\Delta(G, D) \geq \varepsilon$

$$\Pr_{G^+ \to x'_1, \ldots, x'_t} [\text{Ver}(x'_1, \ldots, x'_t) \to 1] \leq \text{low}$$

Our Approach

Identity test for D: Ver s.t.

- (Correctness): $\Pr_{D^+ \to x_1, \ldots, x_t} [\text{Ver}(x_1, \ldots, x_t) \to 1] \geq \text{high}$
- (Security): $\forall$ efficient G, $\Delta(G, D) \geq \varepsilon$

$$\Pr_{G^+ \to x'_1, \ldots, x'_t} [\text{Ver}(x'_1, \ldots, x'_t) \to 1] \leq \text{low}$$

Our Approach

Identity test for D: Ver s.t.

- (Correctness): $\Pr_{D^+ \to x_1, \ldots, x_t} [\text{Ver}(x_1, \ldots, x_t) \to 1] \geq \text{high}$
- (Security): $\forall$ efficient G, $\Delta(G, D) \geq \varepsilon$

$$\Pr_{G^+ \to x'_1, \ldots, x'_t} [\text{Ver}(x'_1, \ldots, x'_t) \to 1] \leq \text{low}$$

Our Approach

Identity test for D: Ver s.t.

- (Correctness): $\Pr_{D^+ \to x_1, \ldots, x_t} [\text{Ver}(x_1, \ldots, x_t) \to 1] \geq \text{high}$
- (Security): $\forall$ efficient G, $\Delta(G, D) \geq \varepsilon$

$$\Pr_{G^+ \to x'_1, \ldots, x'_t} [\text{Ver}(x'_1, \ldots, x'_t) \to 1] \leq \text{low}$$

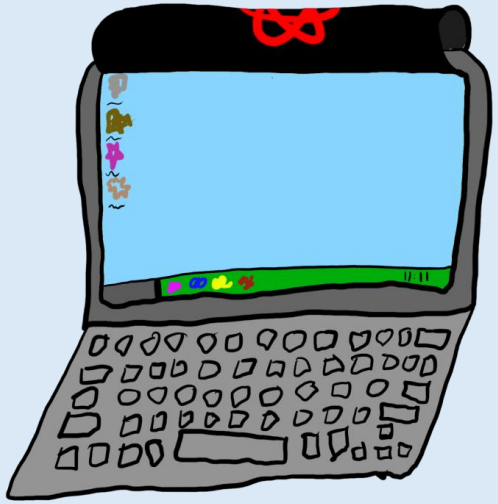
Our Approach

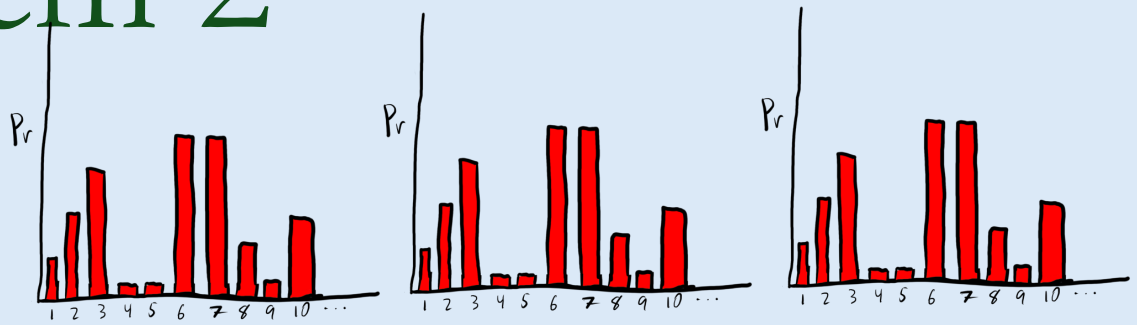
Identity test for D: Ver s.t.

- (Correctness): $\Pr_{D^+ \to x_1, \ldots, x_t} [\text{Ver}(x_1, \ldots, x_t) \to 1] \geq \text{high}$
- (Security): $\forall$ efficient G, $\Delta(G, D) \geq \varepsilon$

$$\Pr_{G^+ \to x'_1, \ldots, x'_t} [\text{Ver}(x'_1, \ldots, x'_t) \to 1] \leq \text{low}$$

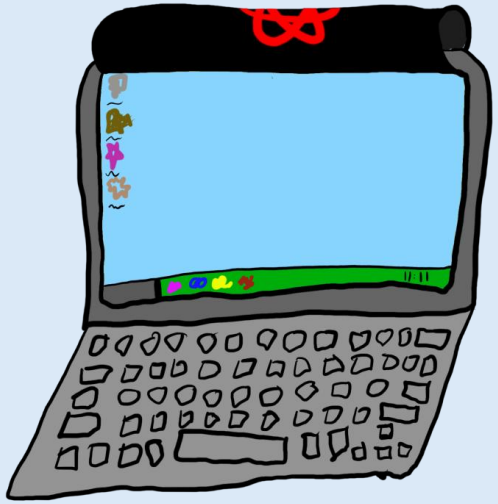
Problem 2

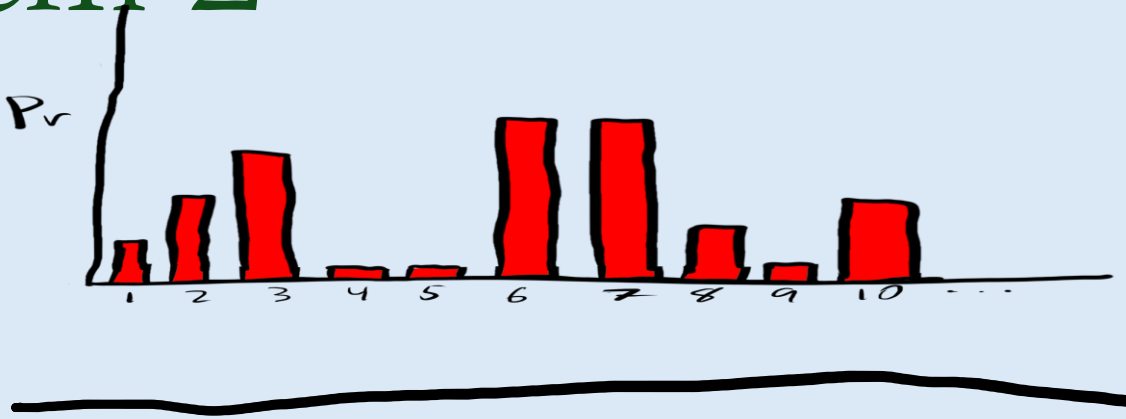




IMPOSTER

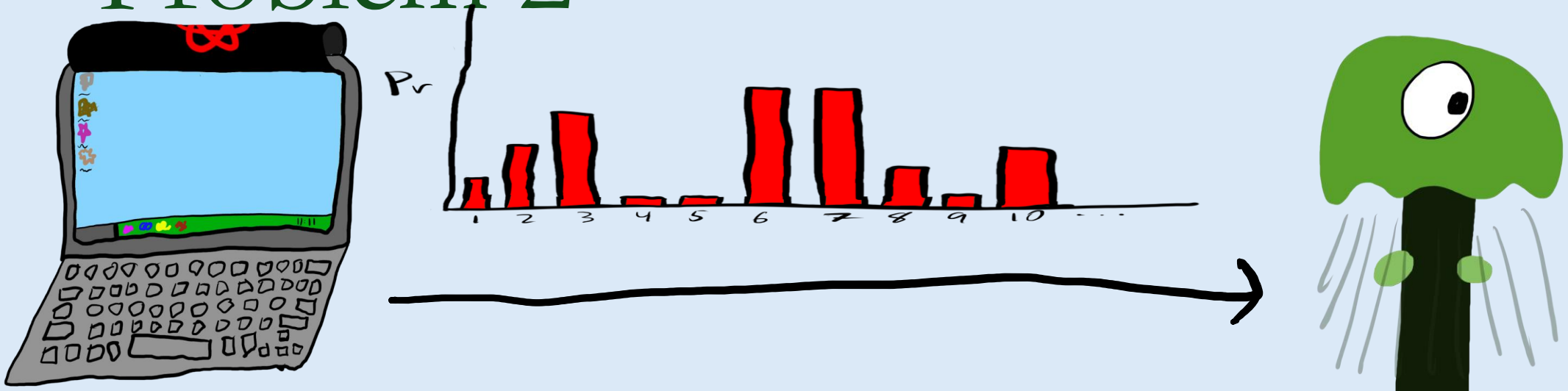
Problem 2





hmm, looks quantum to me...

Problem 2



FOOLED YOU, AGAIN!

hmm, looks quantum to me...

Distribution Verification

D efficiently verifiable if $\exists$ eff. Ver st.

- (Correctness): $\Pr_{D^+ \to x_1, \ldots, x_t} [\mathrm{Ver}(x_1, \ldots, x_t) \to 1] \geq 1 - \frac{1}{n^c}$

Distribution Verification

D efficiently verifiable if $\exists$ eff. Ver st.

- (Correctness): $\Pr_{D^+ \to x_1, \ldots, x_t}[\mathrm{Ver}(x_1, \ldots, x_t) \to 1] \geq 1 - \frac{1}{n^c}$

- (Adaptive Security): $\forall$ efficient $G \to (x_1', \ldots, x_t')$

Distribution Verification

D efficiently verifiable if $\exists$ eff. Ver s.t.

- (Correctness): $\Pr_{D^+ \to x_1, \ldots, x_t}[\mathrm{Ver}(x_1, \ldots, x_t) \to 1] \geq 1 - \frac{1}{n^c}$

- (Adaptive Security): $\forall$ efficient $G \to (x_1', \ldots, x_t')$ s.t. $\Delta(x_u', D) \geq \varepsilon$

Distribution Verification

D efficiently verifiable if $\exists$ eff. Ver s.t.

- (Correctness): $\Pr_{D^+ \to x_1, \ldots, x_t} [\mathrm{Ver}(x_1, \ldots, x_t) \to 1] \geq 1 - \frac{1}{n^c}$

- (Adaptive Security): $\forall$ efficient $G \to (x_1', \ldots, x_t')$
  s.t. $\Delta(x_u', D) \geq \varepsilon$
  $\Pr [\mathrm{Ver}(x_1', \ldots, x_t') \to 1] \leq (1 - \varepsilon) + \frac{1}{n^c}$

gets ε + runtime of G

Distribution Verification

D efficiently verifiable if $\exists$ eff. Ver s.t.

- (Correctness): $\Pr_{D^+ \to x_1, \ldots, x_t}\left[Ver(x_1, \ldots, x_t) \to 1\right] \geq 1 - \frac{1}{n^c}$

- (Adaptive Security): $\forall$ efficient $G \to (x_1', \ldots, x_t')$
  s.t. $\Delta(x_u', D) \geq \varepsilon$
  $\Pr\left[Ver(x_1', \ldots, x_t') \to 1\right] \leq (1-\varepsilon) + \frac{1}{n^c}$

Main Question

When is a (classical/quantum) distribution efficiently verifiable?

Our Results

Classical Setting

- if OWFs exist, then every sufficiently random samplable dist. is NOT efficiently verifiable.

Classical Setting

$H_\infty \geq \omega(\log n)$

- if OWFs exist, then every sufficiently random samplable dist. is NOT efficiently verifiable.

Classical Setting

$H_\infty \geq \omega(\log n)$

- if OWFs exist, then every sufficiently random samplable dist. is NOT efficiently verifiable.

- if OWFs do not exist, then every samplable dist. IS efficiently verifiable. !!

Quantum Setting

- If one-way puzzles do not exist, then every quantum advantage sampler is efficiently verifiable with security against PPT machines

Quantum Setting

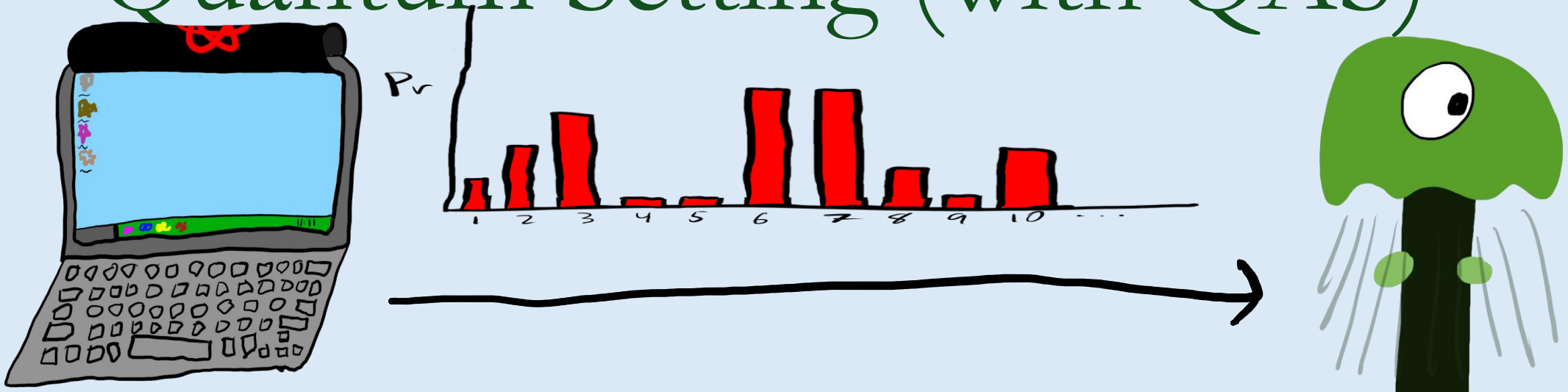
- If one-way puzzles do not exist, then every quantum advantage sampler is efficiently verifiable with security against PPT machines

Note: Ver is quantum

Quantum Setting (with QAS)

GOOD ENOUGH

Quantum Setting (with QAS)



GOOD ENOUGH

Ha! Nice try.

Techniques

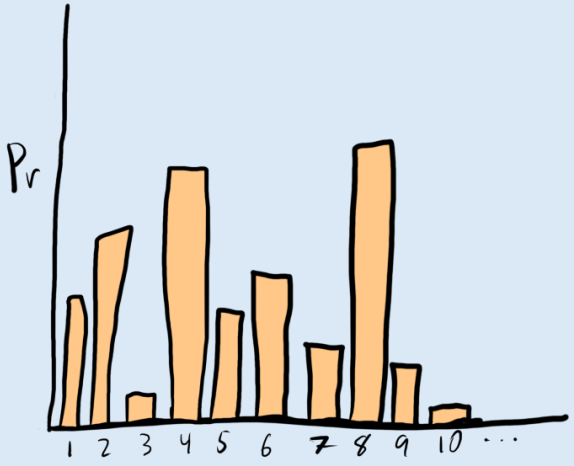
Classical Setting

$H_\infty \geq \omega(\log n)$

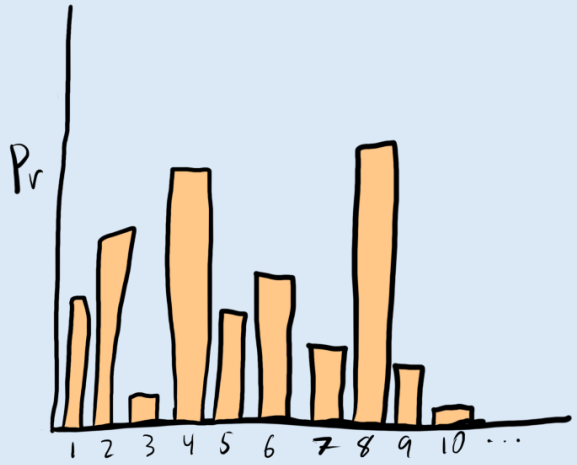
- if OWFs exist, then every sufficiently random samplable dist. is NOT efficiently verifiable.

OWF Counterexample

$D(r) \rightarrow$



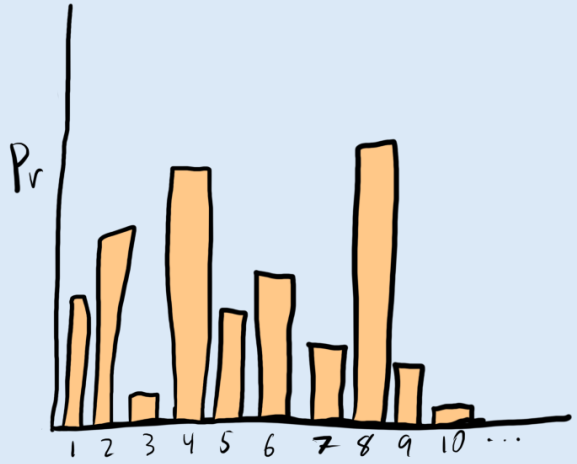
OWF Counterexample

$D(r) \rightarrow$ 

, G a PRG

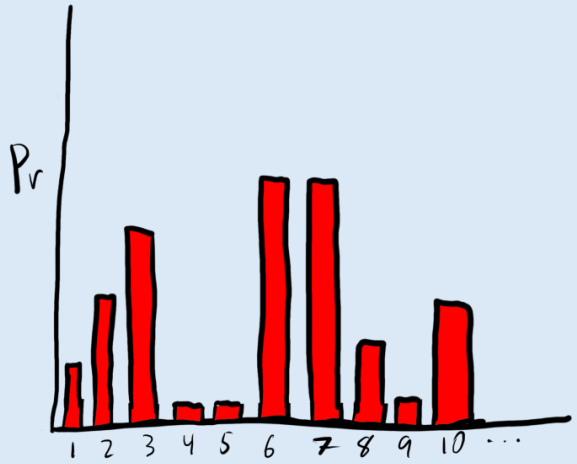
OWF Counterexample

$D(r) \rightarrow$



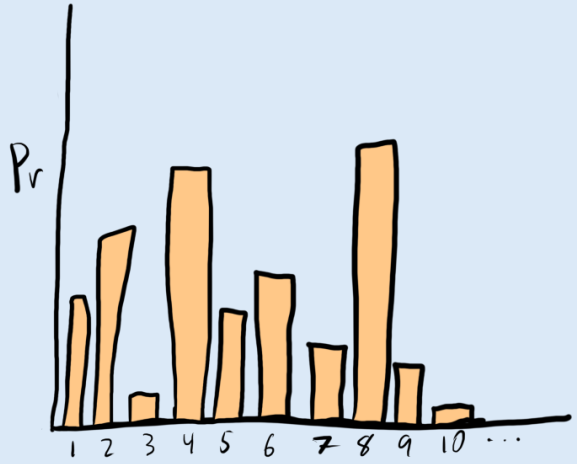
, G a PRG

$D(G(r)) \rightarrow$



OWF Counterexample

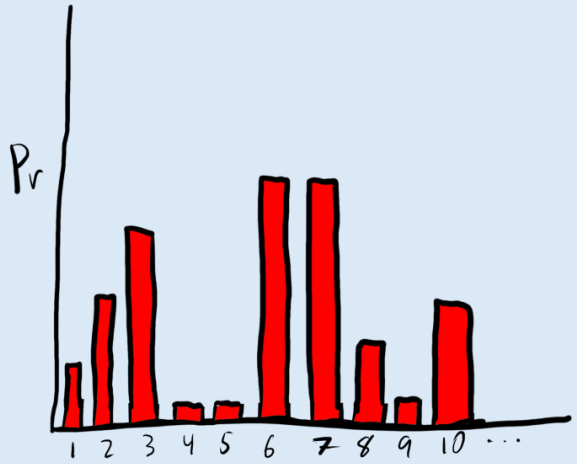
$D(r) \rightarrow$



, G a PRG

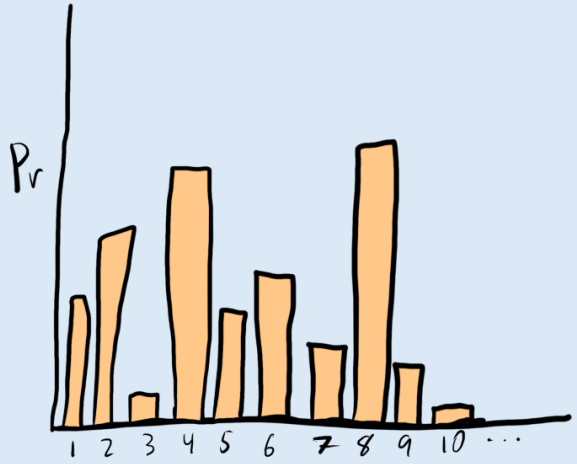
Statistically far!

$D(G(r)) \rightarrow$



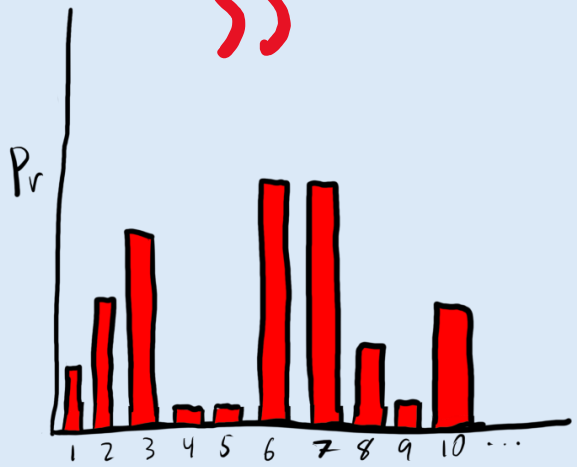
OWF Counterexample

$D(r) \rightarrow$



$\approx_S$

$D(G(r)) \rightarrow$



, G a PRG

Statistically far!

Indistinguishable!

Classical Setting

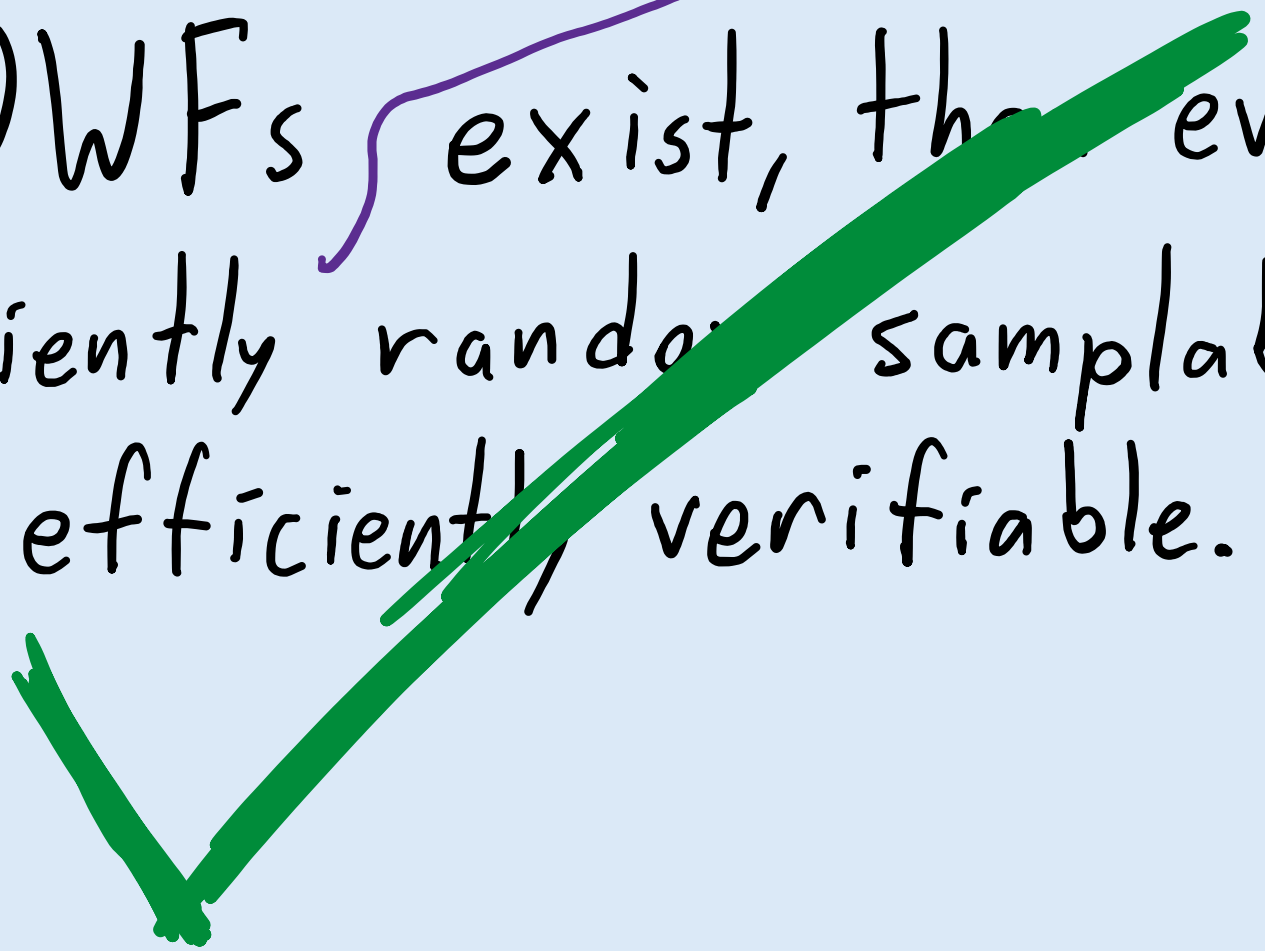
$H_\infty \geq \omega(\log n)$

- if OWFs exist, then every sufficiently random samplable dist. is NOT efficiently verifiable.

Classical Setting

$H_\infty \geq \omega(\log n)$

- if OWFs exist, then every sufficiently random samplable dist. is NOT efficiently verifiable.



Classical Setting

- if OWFs do not exist, then every samplable dist. IS efficiently verifiable.

Classical Setting

Key Tool: Kolmogorov Complexity

- if OWFs do not exist, then every samplable dist. IS efficiently verifiable.

Kolmogorov Complexity

$K(x)$ = length of the shortest Turing machine outputting x.

Kolmogorov Complexity

$K(x)$ = length of the shortest Turing machine outputting x.

$K(\overbrace{1010\ldots10}^{\times 1000})$

Kolmogorov Complexity

$K(x)$ = length of the shortest Turing machine outputting x.

$K(\overbrace{1010\ldots10}^{\times 1000}) = |\text{"output 10 1000 times"}|$

Kolmogorov Complexity

$K(x)$ = length of the shortest Turing machine outputting x.

$K(\overbrace{1010\ldots10}^{\times 1000}) = |\text{"output 10 1000 times"}| = 20$

Kolmogorov Complexity

$K(x)$ = length of the shortest Turing machine outputting x.

$K(\overbrace{1010\ldots10}^{\times 1000}) = |\text{"output 10 1000 times"}| = 20$

$K(\underbrace{10110001010011\ldots}_{1000 \text{ random characters}})$

Kolmogorov Complexity

$K(x)$ = length of the shortest Turing machine outputting x.

$K(\overbrace{1010\ldots10}^{\times 1000}) = |\text{"output 10 1000 times"}| = 20$

$K(\underbrace{10110001010011\ldots}_{1000 \text{ random characters}}) \approx 1000$

Kolmogorov Complexity

Fact: D samplable dist.,

w.h.p. $D \to x$, $K(x) \approx \log \frac{1}{\Pr[D \to x]}$

Kolmogorov Complexity

Fact: D samplable dist.,

w.h.p. $D \to x$, $K(x) \approx \log \frac{1}{\Pr[D \to x]}$

[LOZ1] Coding Theorem

$\forall x$,

$K(x) \leq |D| + \log\left(\frac{1}{\Pr[D \to x]}\right) + c$

Kolmogorov Complexity

Fact: D samplable dist.,

w.h.p. $D \to x$, $K(x) \approx \log \frac{1}{\Pr[D \to x]}$

[LV93] Incompressability

w.h.p. over $D \to x$,

$$K(x) \geq \log\left(\frac{1}{\Pr[D \to x]}\right) - c$$

[Oz1] Coding Theorem

$\forall x$,

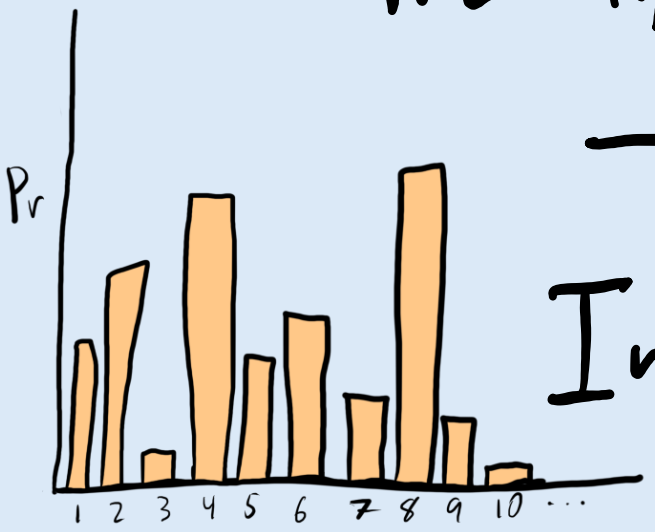
$$K(x) \leq |D| + \log\left(\frac{1}{\Pr[D \to x]}\right) + c$$

Inefficient Verifier [Aaronson14]

$$Ver(x_1, \ldots, x_t): \text{output } 1 \iff$$

$$\log \frac{1}{Pr[D \to x_1] \cdots Pr[D \to x_t]} \leq K(x_1, \ldots, x_t) + c$$

$$\longrightarrow x_1, \ldots, x_t$$



Incompressability: w.h.p. ✓

Inefficient Verifier [Aaronson14]

$$Ver(x_1, \ldots, x_t) : \text{output } 1 \iff$$

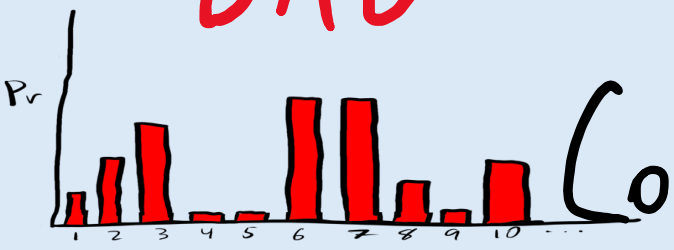
$$\log \frac{1}{Pr[D \to x_1] \cdots Pr[D \to x_t]} \leq K(x_1, \ldots, x_t) + c$$

Inefficient Verifier [Aaronson14]

$Ver(x_1, \ldots, x_t)$: output 1 $\Leftrightarrow$

$$\log \frac{1}{Pr[D \to x_1] \cdots Pr[D \to x_t]} \leq K(x_1, \ldots, x_t) + c$$

BAD $\to x'_1, \ldots, x'_t$



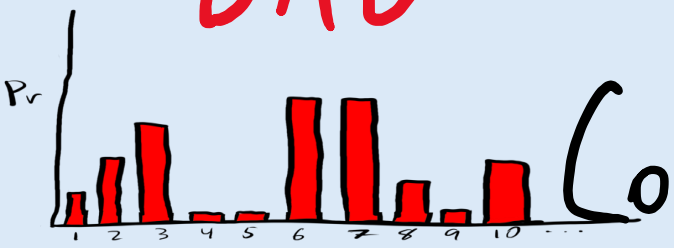
Coding thm: $K(x_1, \ldots, x_t) \leq \log \frac{1}{Pr[D' \to (x_1, \ldots, x_t)]} + c$

Inefficient Verifier [Aaronson14]

$Ver(x_1, \ldots, x_t)$: output 1 $\Leftrightarrow$

$$\log \frac{1}{Pr[D \to x_1] \cdots Pr[D \to x_t]} \leq K(x_1, \ldots, x_t) + c$$

BAD $\to x'_1, \ldots, x'_t$



Coding thm: $K(x_1, \ldots, x_t) \leq \log \frac{1}{Pr[D' \to (x_1, \ldots, x_t)]} + c$

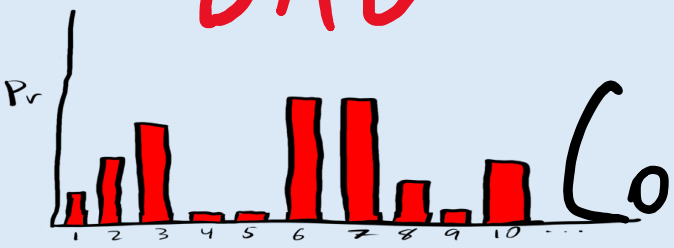
w.h.p. $\leq$ LHS

Inefficient Verifier [Aaronson14]

$Ver(x_1, \ldots, x_t)$: output 1 $\Leftrightarrow$

$$\log \frac{1}{Pr[D \to x_1] \cdots Pr[D \to x_t]} \leq K(x_1, \ldots, x_t) + c$$

BAD $\to x'_1, \ldots, x'_t$



Coding thm: $K(x_1, \ldots, x_t) \leq \log \frac{1}{Pr[D' \to (x_1, \ldots, x_t)]} + c$

w.h.p. $\leq$ LHS ✓

Efficient Verifier

Idea: if OWFs don't exist, can estimate $\log \frac{1}{\Pr[D \to x_1] \cdots \Pr[D \to x_2]}$ (prob. estimation) [IL89]

Probability Estimation

[IL89]: For all dist. D, there exists Est s.t. w.h.p. $D \to x$,

$$Est(x) \approx -\log \Pr[D \to x]$$

Probability Estimation

[IL89]: For all dist. D, there exists Est s.t. w.h.p. $D \to x$,

$$Est(x) \approx -\log \Pr[D \to x]$$

(1-sided error): $\forall x$, $Est(x) \geq -\log \Pr[D \to x]$

Efficient Verifier

Idea: if OWFs don't exist, can estimate $\log \frac{1}{\Pr[D \to x_1] \cdots \Pr[D \to x_t]}$ (prob. estimation) [IL89]

Problem: $K(x_1, \ldots, x_t)$ uncomputable

Efficient Verifier

Idea: if OWFs don't exist, can estimate $\log \frac{1}{\Pr[D \to x_1] \cdots \Pr[D \to x_2]}$ (prob. estimation) [IL89]

Problem: $K(x_1, \ldots, x_t)$ uncomputable

Solution: Use different type of K-complexity

$uK^t(x)$

$uK^t(x) = -\log \Pr[\text{random TM outputs } x]$

$uK^t(x)$

$$uK^t(x) = -\log \Pr[\text{random TM outputs } x]$$

$$= -\log_{\pi \leftarrow \{0,1\}^t} \Pr\left[\left(UTM^t(\pi)\right) \to x\right]$$

$uK^t(x)$

$uK^t(x) = -\log \Pr[\text{random TM outputs } x]$

Coding theorem + incompressability still hold!

$uK^t(x)$

$uK^t(x) = -\log \Pr[\text{random TM outputs } x]$

Coding theorem + incompressability still hold!

$$Ver(x_1, \ldots, x_t) \to 1 \Leftrightarrow \log \frac{1}{\Pr[D \to x_1] \cdots \Pr[D \to x_t]} \leq uK^t(x) + c$$

works!

Estimating uK^t

Thm [HN23]: If OWFs do not exist, then there exists Est such that for ALL samplable D,

w.h.p. $x \leftarrow D$, $Est(x) \approx uK^t(x)$

Final Verifier

$$Ver(x_1, \ldots, x_t) \to 1 \Leftrightarrow \log \frac{1}{\Pr[D \to x_1] \cdots \Pr[D \to x_t]} \leq u K^t(x) + c$$

replace w/ approximations you get via no OWFs

Final Verifier

$$Ver(x_1, \ldots, x_t) \to 1 \Leftrightarrow \log \frac{1}{\Pr[D \to x_1] \cdots \Pr[D \to x_t]} \leq u K^t(x) + c$$

replace w/ approximations you get via no OWFs

D good $\Rightarrow$ approximations right $\Rightarrow$ passes Ver

Final Verifier

$$Ver(x_1, \ldots, x_t) \to 1 \Leftrightarrow \log \frac{1}{\Pr[D \to x_1] \cdots \Pr[D \to x_t]} \leq uK^t(x) + c$$

replace w/ approximations you get via no OWFs

So far

Final Verifier

$$Ver(x_1, \ldots, x_t) \to 1 \Leftrightarrow \log \frac{1}{\Pr[D \to x_1] \cdots \Pr[D \to x_t]} \leq uK^t(x) + c$$

replace w/ approximations you get via no OWFs

So far ⇒ right

Final Verifier

$$Ver(x_1, \ldots, x_t) \to 1 \iff \log \frac{1}{\Pr[D \to x_1] \cdots \Pr[D \to x_t]} \leq uK^t(x) + c$$

replace w/ approximations you get via no OWFs

So far $\Rightarrow$ right, lower bounded

Final Verifier

$$Ver(x_1, \ldots, x_t) \to 1 \Leftrightarrow \log \frac{1}{\Pr[D \to x_1] \cdots \Pr[D \to x_t]} \leq uK^t(x) + c$$

replace w/ approximations you get via no OWFs

G far $\Rightarrow$ right, lower bounded $\Rightarrow$ test fails

Final Verifier

$$Ver(x_1, \ldots, x_t) \to 1 \Leftrightarrow \log \frac{1}{\Pr[D \to x_1] \cdots \Pr[D \to x_t]} \leq uK^t(x) + c$$

replace w/ approximations you get via no OWFs

Gfar ⇒ right, lower bounded ⇒ test fails

1-sided error critical!

Classical Setting

- if OWFs do not exist, then every samplable dist. IS efficiently verifiable.

Quantum Setting

- If one-way puzzles do not exist, then every quantum advantage sampler is efficiently verifiable with security against PPT machines

Quantum Setting

OWPuzz: quantum analogue of OWF

Quantum Setting

OWPuzz: quantum analogue of OWF

quantum

$\text{Samp} \to (\overbrace{k}^{\text{classical}}, s)$

Quantum Setting

OWPuzz: quantum analogue of OWF

quantum

$\text{Samp} \to (\overbrace{k}^{\text{classical}}, s)$

Security: Given s, hard to sample from conditional dist. on k.

Quantum Setting

OWPuzz: quantum analogue of OWF

quantum

$\text{Samp} \to (\overbrace{k}^{\text{classical}}, s)$

Security: Given s, hard to sample from conditional dist. on k.

OWF $\Rightarrow$ OWPuzz $\Rightarrow$ quantum commitments

Quantum Setting

OWPuzz: quantum analogue of OWF

Quantum Setting

OWPuzz: quantum analogue of OWF

$qK^t(x) = -\log \Pr[\text{random QTM} \to x]$

Quantum Setting

OWPuzz: quantum analogue of OWF

$qK^t(x) = -\log \Pr[\text{random } QTM \to x]$

[CGGH25, HM25, KTZ25]

No OWPuzz $\Rightarrow$ prob. est. for quantum samplable dists

Quantum Setting

OWPuzz: quantum analogue of OWF

$qK^t(x) = -\log \Pr[\text{random } QTM \to x]$

[CGGH25, HM25, KTZ25]

No OWPuzz $\Rightarrow$ prob. est. for quantum samplable dists

$\Rightarrow$ estimator for qK^t

Quantum Setting

OWPuzz: quantum analogue of OWF

$qK^t(x) = -\log \Pr[\text{random } QTM \to x]$

[CGGHZ5, HM25, KTZ5]

No OWPuzz $\Rightarrow$ prob. est. for quantum samplable dists

$\Rightarrow$ estimator for qK^t

Problem: no 1-sided error!

Quantum Setting

Key idea: If D is samplable quantumly but NOT classically,

Quantum Setting

Key idea: If D is samplable quantumly but NOT classically,

w.h.p. $D \to x$

$$qu K^t(x) \ll u K^t(x)$$

Quantum Setting

Key idea: If D is samplable quantumly but NOT classically, To verify, estimate both!

w.h.p. $D \to x$

$$qK^t(x) \ll uK^t(x)$$

Quantum Setting

D a QAS:

$\mathrm{Ver}(x_1, \ldots, x_t)$: estimate $q_u K^t(x_1, \ldots, x_t)$ and $u K^t(x_1, \ldots, x_t)$. Output 1

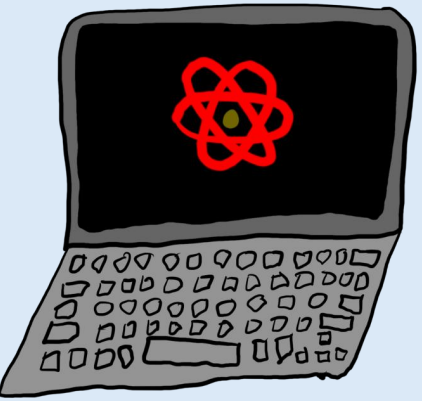
$\Leftrightarrow q_u K^t \ll u K^t$

Quantum Setting

D a QAS:

$\mathrm{Ver}(x_1,\dots,x_t)$: estimate $qu\mathrm{K}^t(x_1,\dots,x_t)$ and $u\mathrm{K}^t(x_1,\dots,x_t)$. Output 1

$\Leftrightarrow qu\mathrm{K}^t \ll u\mathrm{K}^t$



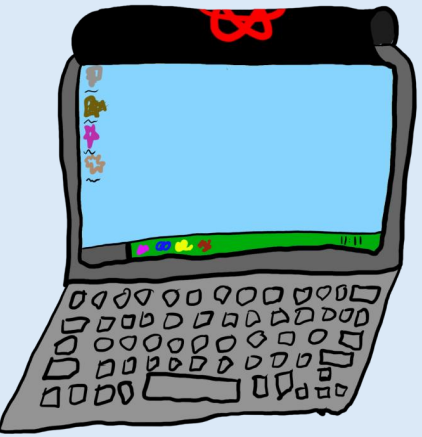
$\rightarrow qu\mathrm{K}^t \ll u\mathrm{K}^t$ ✓

Quantum Setting

D a QAS:

$\mathrm{Ver}(x_1,\dots,x_t)$: estimate $qu K^t(x_1,\dots,x_t)$ and $u K^t(x_1,\dots,x_t)$. Output 1

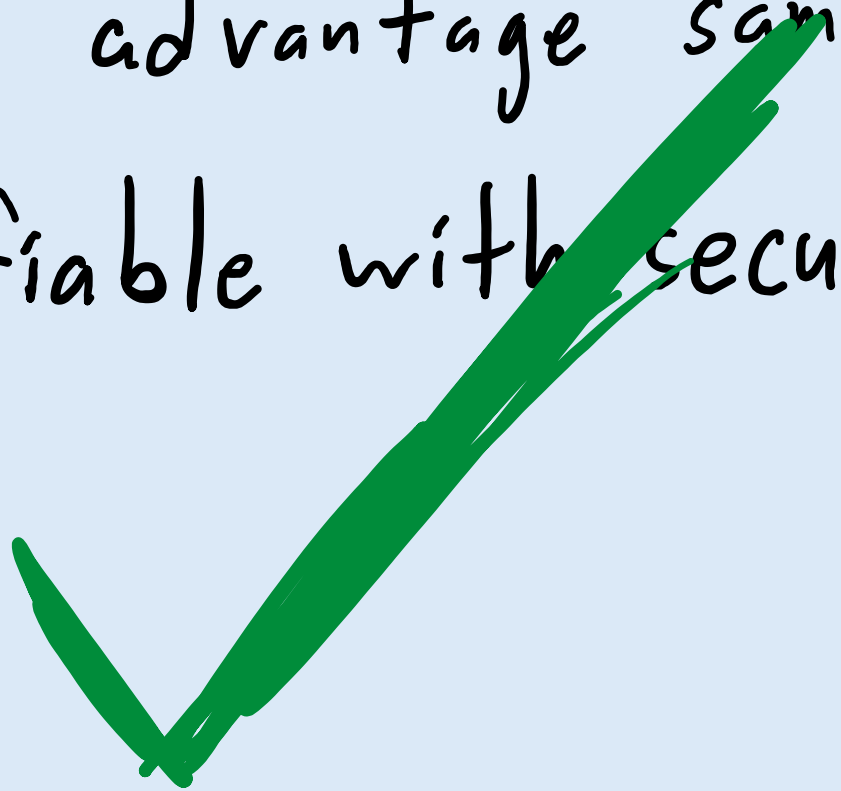
$\Leftrightarrow qu K^t \ll u K^t$



$\rightarrow qu K^t \approx u K^t$ ✗

Quantum Setting

- If one-way puzzles do not exist, then every quantum advantage sampler is efficiently verifiable with security against PPT machines



Open Questions

- Eff. ver. for quantum from no OWPuzz

Open Questions

- Eff. ver. for quantum from no OWPuzz
- 1-sided error for prob. est. from no OWPuzz

Open Questions

- Eff. ver. for quantum from no OWPuzz
- 1-sided error for prob. est. from no OWPuzz
- OWPuzz $\Rightarrow$ no dist. verifiable?

Open Questions

- Eff. ver. for quantum from no OWPuzz
- 1-sided error for prob. est. from no OWPuzz
- OWPuzz $\Rightarrow$ no dist. verifiable?
- Can we achieve weaker verifiability if OWF exist?

Open Questions

- Eff. ver. for quantum from no OWPuzz
- 1-sided error for prob. est. from no OWPuzz
- OWPuzz $\Rightarrow$ no dist. verifiable?
- Can we achieve weaker verifiability if OWF exist?
- Lower complexity classes?

Thank You!