Quantum advantage from one-way functions

Tomoyuki Morimae (Kyoto University)
Takashi Yamakawa (NTT and Kyoto University)

15min
Qcrypt 2023

[M and Yamakawa, arXiv:2302.04749]

Quantum advantage

If [ASSUMPTION] is correct then there is a [PROBLEM] such that
(1) efficient quantum algorithm can solve it
(2) efficient classical algorithm cannot solve it

Two desirable properties:

(1) Assumption should be weaker and standard
(2) Efficiently verifiable

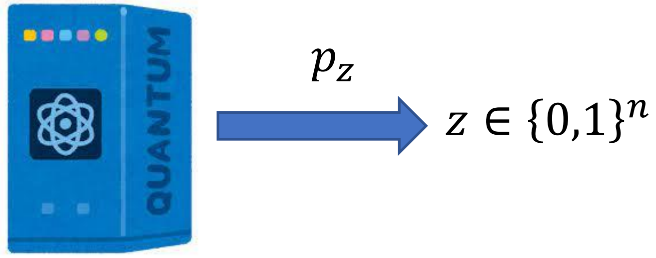
PPT Verifier

Classical communication

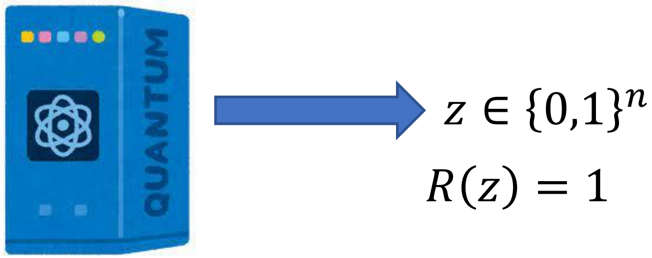
I confirm the quantum advantage!

Previous approaches

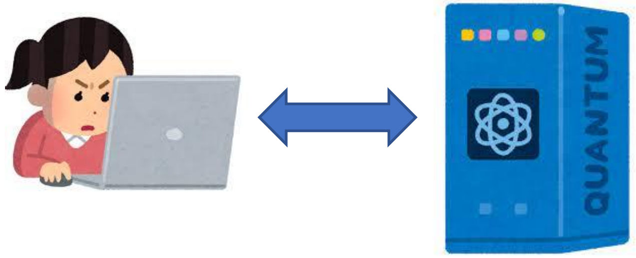
	Assumption	Verifiability
Sampling	Ad hoc	NO
Search problems	Ad hoc	Inefficient
Proofs of quantumness	(noisy)2-1 TDCRHF (LWE) Full-domain TDP QHE (LWE) Random oracle	Efficient



Boson sampling, IQP, random circuit, DQC1⋯



XHOG, Fourier fishing⋯



Proofs of quantumness

Previous approaches

	Assumption	Verifiability
Sampling	Ad hoc	NO
Search problems	Ad hoc	Inefficient
Proofs of quantumness	(noisy)2-1 TDCRHF (LWE) Full-domain TDP QHE (LWE) Random oracle	Efficient

Open problem:

Efficiently verifiable quantum advantage with weaker and standard assumption?

→Extremely challenging open problem

Inefficiently verifiable quantum advantage with weaker and standard assumption?

→Still highly non-trivial

Our result

We show inefficiently-verifiable quantum advantage from weaker and standard assumption

We construct inefficiently-verifiable proofs of quantumness from OWFs

Inefficiently-verifiable
proofs of quantumness

t

PPT V_1

t

Accept/reject

Unbounded V_2

Completeness:
There exists a QPT prover such that $\Pr[V_2\ accepts] \geq 2/3$

Soundness:
For any PPT prover, $\Pr[V_2 accepts] \leq 1/3$

5

Strong, less standard

Newly introduced assumptions

NTCF
2-to-1TDCRHF
Full-domain TDP
QHE, Random oracle
Factoring,
PH will not collapse to 3rd level

PKE
KE
MPC
OT
ZK
Commitments
PRGs
SKE
Digital signature

OWFs

$P \neq NP$

Weak, standard

Construction

PoQ by [KMCVY, Nat. Phys. 2022]

$f_0, f_1 : \{0,1\}^n \to \{0,1\}^n$

verifier

f_0, f_1

pro

Cannot learn both x_0 and x_1

$$|0\rangle \sum_x |x\rangle |f_0(x)\rangle + |1\rangle \sum_x |x\rangle |f_1(x)\rangle$$

y

$$|0\rangle |x_0\rangle + |1\rangle |x_1\rangle$$

$$f_0(x_0) = f_1(x_1) = y$$

Goal: remotely generate this with only OWFs!

Classical commitments

$r \leftarrow \{0,1\}^l$

PPT Receiver

$b \in \{0,1\}$

$x \leftarrow \{0,1\}^l$

PPT Sende

$\alpha_1 = f_1(b, x)$ ←

$\beta_1 = g_1(r, \alpha_1)$ →

$\alpha_2 = f_2(b, x, \alpha_1, \beta_1)$ ←

$\beta_2 = g_2(r, \alpha_1, \beta_1, \alpha_2)$ →

$\alpha_3 = f_3(b, x, \alpha_1, \beta_1, \alpha_2, \beta_2)$ ←

$\beta_3 = g_3(r, \alpha_1, \beta_1, \alpha_2, \beta_2, \alpha_3)$ →

Cannot find both x_0 and x_1

Commitment: $t = (\alpha_1, \beta_1, \alpha_2, \beta_2, \ldots)$

Opening: x

Coherent execution of classical commitments

$r \leftarrow \{0,1\}^l$

PPT Receiver

$$\sum_{b\in\{0,1\},x\in\{0,1\}^l} |b\rangle|x\rangle|f_1(b,x)\rangle$$

$$\sum_{b\in\{0,1\}} \sum_{x:f_1(b,x)=\alpha_1} |b\rangle|x\rangle$$

α_1

β_1

$$\sum_{b\in\{0,1\}} \sum_{x:f_1(b,x)=\alpha_1} |b\rangle|x\rangle|f_2(b,x,\alpha_1,\beta_1)\rangle$$

$$\sum_{b\in\{0,1\}} \sum_{x:f_1(b,x)=\alpha_1,f_2(b,x,\alpha_1,\beta_1)=\alpha_2} |b\rangle|x\rangle$$

α_2

β_2

Coherent execution of classical commitments

$r \leftarrow \{0,1\}^l$

PPT Receiver

$t = (\alpha_1, \beta_1, \alpha_2, \beta_2, \dots,)$

$$|0\rangle \sum_{x \in X_{0,t}} |x\rangle + |1\rangle \sum_{x \in X_{1,t}} |x\rangle$$

If $|X_{0,t}| = |X_{1,t}| = 1$, it is $|0\rangle|x_0\rangle + |1\rangle|x_1\rangle$

Then, we can run PoQ of [KMCVY22]

However, in general not…

Hashing technique

$r \leftarrow \{0,1\}^l$

PPT Receiver

Cannot find both x_0 and x_1

$t = (\alpha_1, \beta_1, \alpha_2, \beta_2, \dots,)$

$$|0\rangle \sum_{x \in X_{0,t}} |x\rangle + |1\rangle \sum_{x \in X_{1,t}} |x\rangle$$

Pairwise independent hash h

$$|0\rangle \sum_{x \in X_{0,t}} |x\rangle|h(x)\rangle + |1\rangle \sum_{x \in X_{1,t}} |x\rangle|h(x)\rangle$$

y

$$|0\rangle \sum_{x \in X_{0,t} \cap h^{-1}(y)} |x\rangle + |1\rangle \sum_{x \in X_{1,t} \cap h^{-1}(y)} |x\rangle$$

With a non-negligible probability, $|X_{0,t} \cap h^{-1}(y)| = |X_{1,t} \cap h^{-1}(y)| = 1$

Hence, we a non-negligible probability, the prover gets $|0\rangle|x_0\rangle + |1\rangle|x_1\rangle$

Conclusion

We show (inefficiently-verifiable) quantum advantage based on one-way functions!

	Assumption	Verifiability
Sampling	Ad hoc	NO
Search problems	Ad hoc	Inefficient
Proofs of quantumness	(noisy)2-1 TDCRHF (LWE) Full-domain TDP QHE (LWE) Random oracle	Efficient
Our result	(Classically-secure)One-way functions	Inefficient (BPP^{NP})

Other results: Constructing other variants of inefficiently-verifiable PoQ from worst-case assumptions such as CZK is not in BPP

Thank you!

[M and Yamakawa, arXiv:2302.04749]

Problems

$$|0\rangle \sum_{x \in X_{0,t}} |x\rangle|h(x)\rangle + |1\rangle \sum_{x \in X_{1,t}} |x\rangle|h(x)\rangle \Longrightarrow |0\rangle \sum_{x \in X_{0,t} \cap h^{-1}(y)} |x\rangle + |1\rangle \sum_{x \in X_{1,t} \cap h^{-1}(y)} |x\rangle$$

With a non-negligible probability, $\left|X_{0,t} \cap h^{-1}(y)\right| = \left|X_{1,t} \cap h^{-1}(y)\right| = 1$

To achieve this,

(1) $\left|X_{0,t}\right| \simeq \left|X_{1,t}\right|$ should be satisfied

→Statistical hiding of the commitment!

(2) $\left|X_{0,t}\right|, \left|X_{1,t}\right|$ should be known in advance

→Random guess works!

Summary

PPT verifier

Classical communication

Honest QPT prover

$|0\rangle|x_0\rangle + |1\rangle|x_1\rangle$

Run [KMCVY22]!

Completeness is hence shown.

How about soundness?

Classical commitments

$r \leftarrow \{0,1\}^l$

PPT Receiver

$b \in \{0,1\}$

$x \leftarrow \{0,1\}^l$

PPT Sender

$\alpha_1 = f_1(b,x)$ ←

$\beta_1 = g_1(r,\alpha_1)$ →

$\alpha_2 = f_2(b,x,\alpha_1,\beta_1)$ ←

$\beta_2 = g_2(r,\alpha_1,\beta_1,\alpha_2)$ →

$\alpha_3 = f_3(b,x,\alpha_1,\beta_1,\alpha_2,\beta_2)$ ←

$\beta_3 = g_3(r,\alpha_1,\beta_1,\alpha_2,\beta_2,\alpha_3)$ →

Cannot find $x_0 \in X_{0,t}$ and $x_1 \in X_{1,t}$

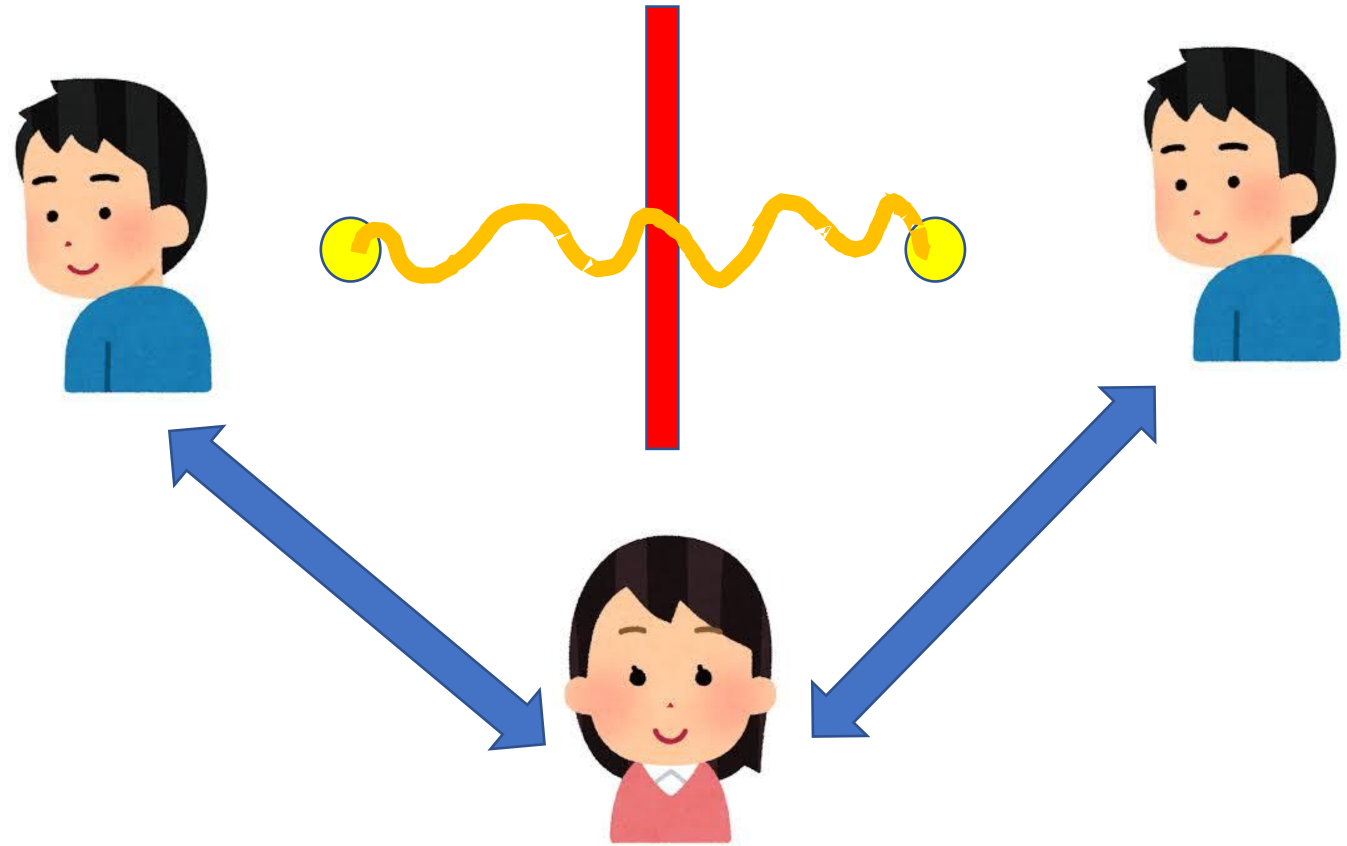
Commitment: $t = (\alpha_1,\beta_1,\alpha_2,\beta_2,\ldots)$

Opening: x

Soundness is also OK!

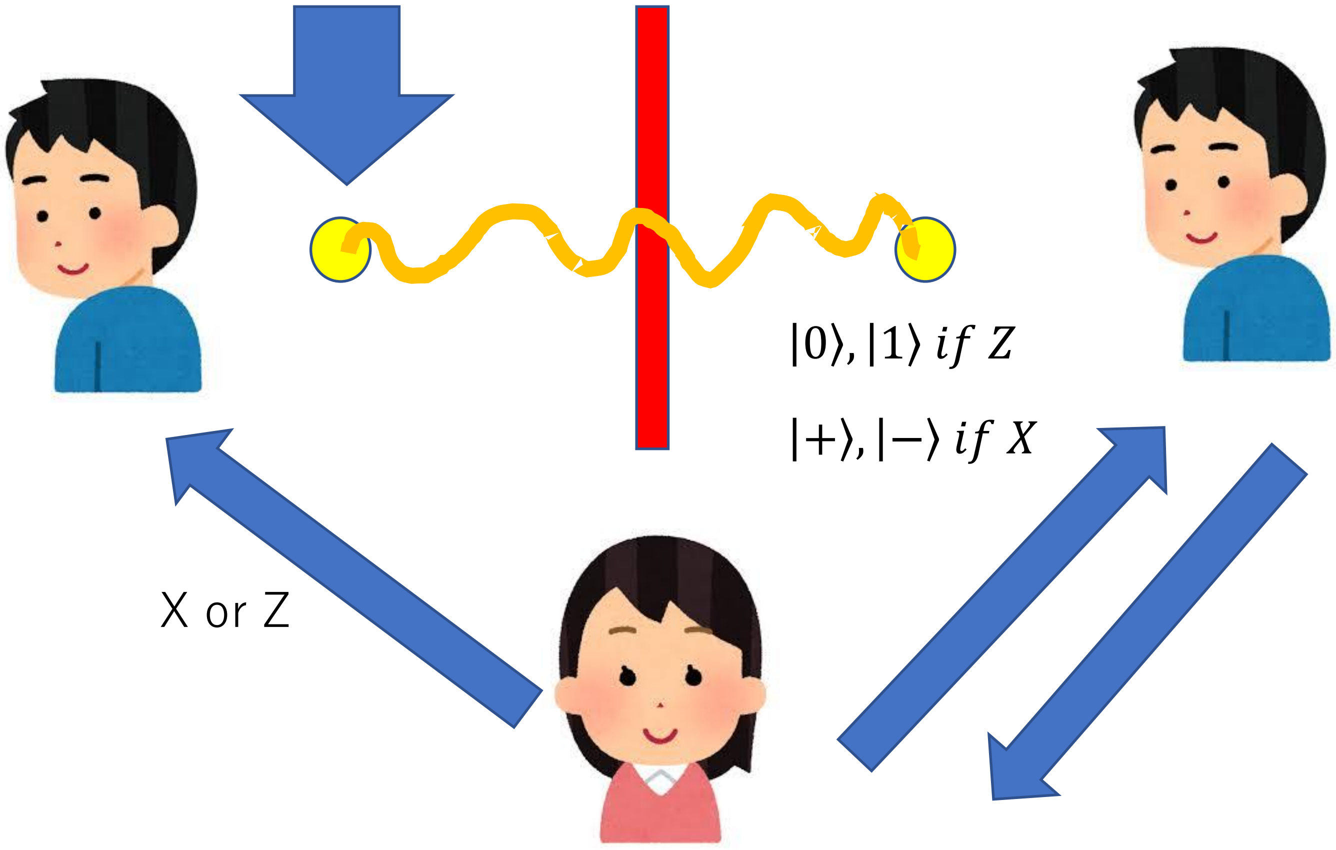
Backgrounds: proofs of quantumness

Bell's inequality

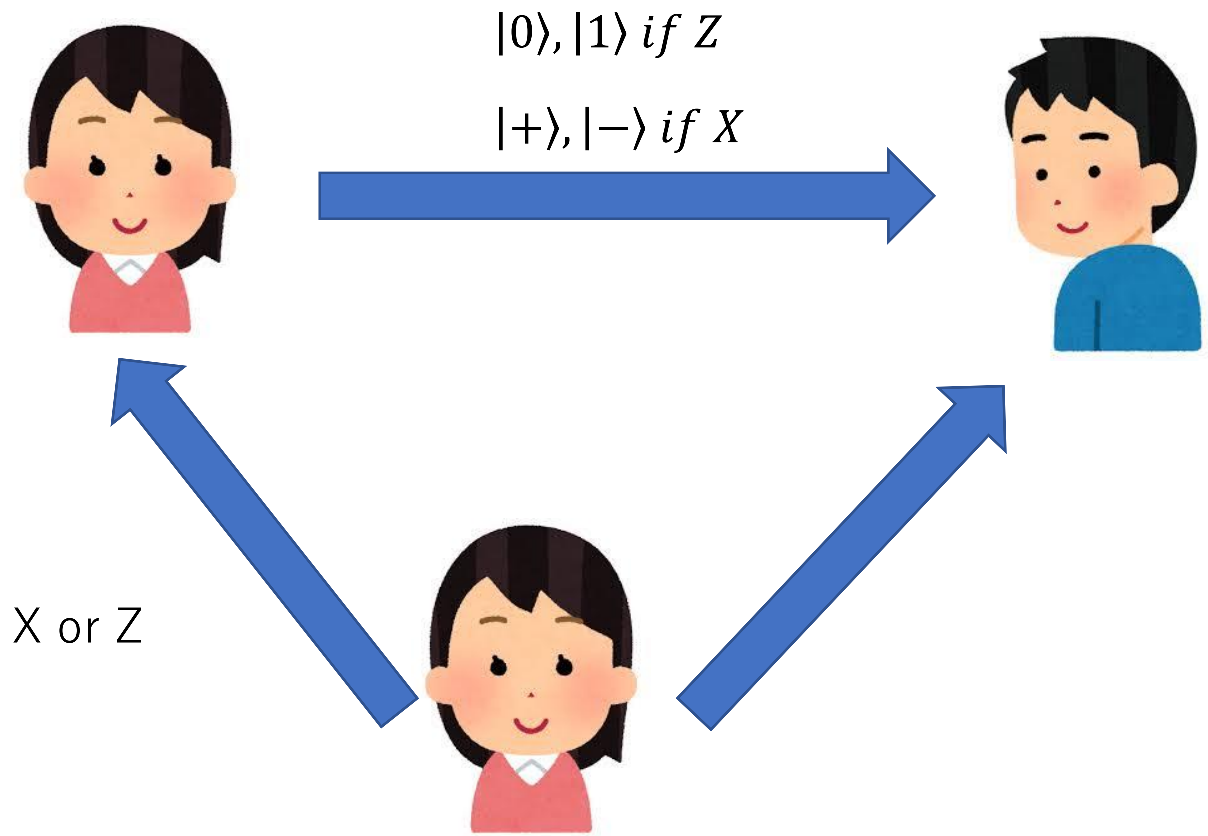


（1） If Bob and Charlie share entanglement, Alice accepts
（2） If they do not share entanglement, Alice rejects

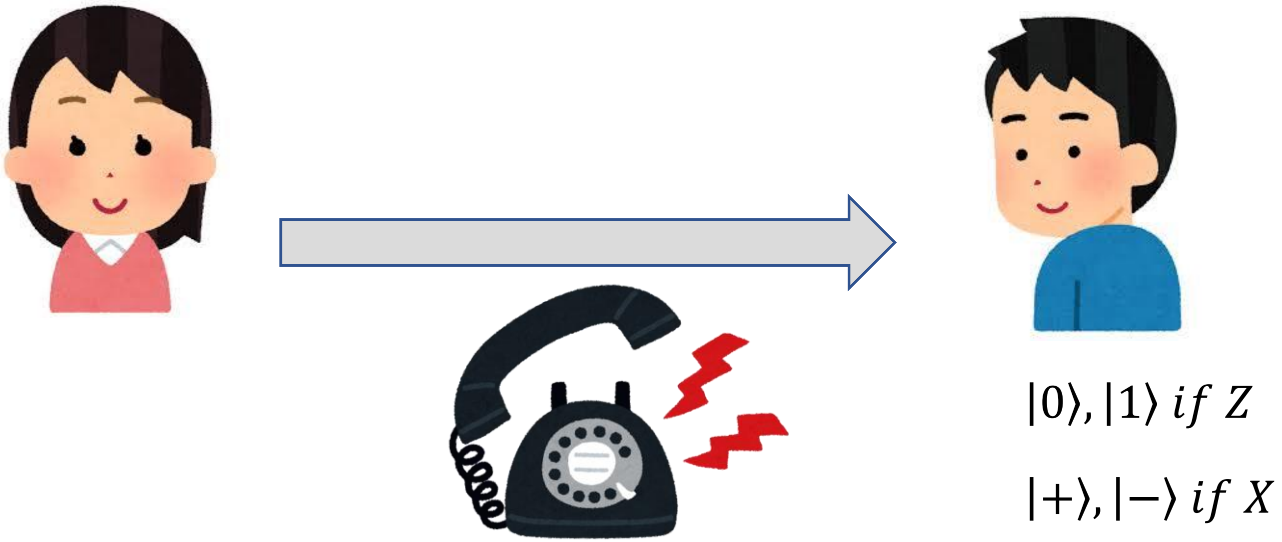
Unconditional proof of quantumness! However, the no-communication has to be assumed



Classical Bob 2 cannot answer the correct measurement result because he does not know the state



This is Bad because now Alice is quantum



How can Alice remotely prepare BB84 states over only classical channel in such a way that Bob cannot learn the state?

We can use cryptography!

PoQ by [KMCVY, Nat. Phys. 2022]

$f_0, f_1 : \{0,1\}^n \rightarrow \{0,1\}^n$

Claw-free:
Finding x_0, x_1 $s.t.$ $f_0(x_0) = f_1(x_1)$ is hard

Trapdoor:
With td, it is easy to find, given y,
x_0, x_1 $s.t.$ $f_0(x_0) = f_1(x_1) = y$

verifier

td

prover

Cannot learn both x_0 and x_1

$\xrightarrow{f_0, f_1}$

$|0\rangle \sum_x |x\rangle|f_0(x)\rangle + |1\rangle \sum_x |x\rangle|f_1(x)\rangle$

$\xleftarrow{y}$

$|0\rangle|x_0\rangle + |1\rangle|x_1\rangle$

$f_0(x_0) = f_1(x_1) = y$

$\xrightarrow{r}$

$|r \cdot x_0\rangle|x_0\rangle + |r \cdot x_1 \oplus 1\rangle|x_1\rangle$

$|r \cdot x_0\rangle + (-1)^{d \cdot (x_0 \oplus x_1)}|r \cdot x_1 \oplus 1\rangle$

$\xleftrightarrow{\text{Bell test}}$

$|0\rangle, |1\rangle, |+\rangle, |-\rangle$

Approach 1: Sampling

Not standard

If average-case #P-hardness conjecture is true and PH does not collapse to the third level, there is no PPT algorithm that outputs z with probability q_z such that

$$\sum_z |p_z - q_z| \leq \epsilon$$

Advantage:
(1) simpler models are enough (boson sampling, IQP, random circuits, DQC1, etc.)

Disadvantage:
(1) ad hoc assumption is required
(2) Non-verifiable

Approach 2: Search problems

If [ASSUMPTION] is true then QPT algorithm can find z such that $R(z) = 1$, but no PPT algorithm can

Ex: XHOG[Aaronson-Gunn]
Find $z_1, \ldots, z_k$ s.t. $E_i[|\langle z_i|C|0^n\rangle|^2] \geq b/2^n$

XQUATH
There is no PPT algorithm that outputs p such that
$E[(p_0 - p)^2] = E[(p_0 - 2^n)^2] - \Omega(2^{-3n})$

Advantage:
(1) simpler models are enough (random circuits)
(2) Inefficiently verifiable

Disadvantage:
(1) ad hoc assumption is required

Approach 3: Proofs of quantumness (PoQ)

PPT

Classical communication

Efficiently verifiable!

Completeness:
There exists a QPT prover s.t. $\Pr[\mathit{Verifier\ accepts}] \geq 2/3$

Soundness:
For any PPT prover, $\Pr[\mathit{Verifier\ accepts}] \leq 1/3$

Assumptions:
NTCF [Brakerski, Christiano, Mahadev, Vazirani, Vidick, FOCS 2018]
2-to-1 TDCRHF [Kahanamoku-Meyer, Choi, Vazirani, Yao, Nat. Phys. 2022]
Full-domain TDP [Morimae, Yamakawa, ITCS 2023]
QHE [Kalai, Lombardi, Vaikuntanathan, Yang, STOC 2023]
Random Oracle [Yamakawa, Zhandry, FOCS 2022]

Previous approaches

	Assumption	Verifiability
Sampling	Ad hoc	NO
Search problems	Ad hoc	Inefficient
Proofs of quantumness	(noisy)2-1 TDCRHF (LWE) Full-domain TDP QHE (LWE) Random oracle	Efficient

Open problem:
Quantum advantage with weaker and standard assumption + efficient verifiability?

→We do not know how to solve it⋯

Open problem:
Quantum advantage with weaker and standard assumption + inefficient verifiability?

→Even this one is highly non-trivial!

OWF is the most fundamental in cryptography

[Russell Impagliazzo and Michael Luby, 1989, One-way functions are essential for complexity based cryptography]

Cryptomania

PKE

Key exchange

Multiparty computation

[IR89]

Minicrypt

OWFs

PRGs

SKE

Zero knowledge

Commitments

Digital signatures

OWFs

28

Our result

We show (inefficiently-verifiable) quantum advantage based on one-way functions!

	Assumption	Verifiability
Sampling	Ad hoc	NO
Search problems	Ad hoc	Inefficient
Proofs of quantumness	(noisy)2-1 TDCRHF (LWE) Full-domain TDP QHE (LWE) Random oracle	Efficient
Our result	(Classically-secure)One-way functions	Inefficient (BPP^{NP})

$x \to f(x)$: $easy$

$f(x) \to x$: $hard$

Proof Idea

$x \to f(x)$: *easy*

$f(x) \to x$: *hard*

Classical OWFs

[HNO+09]

Classical commitments
(statistically-hiding and
Computationally-binding)

``Quantize"

Inefficiently-verifiable
proofs of quantumness

PoQ by KMCVY22

Inefficiently-verifiable
proofs of quantumness

PPT V_1

t

t

Accept/reject

Unbounded time V_2

Completeness:
There exists a QPT prover such that $\Pr[V_2\ accepts] \geq 2/3$

Soundness:
For any PPT prover, $\Pr[V_2 accepts] \leq 1/3$