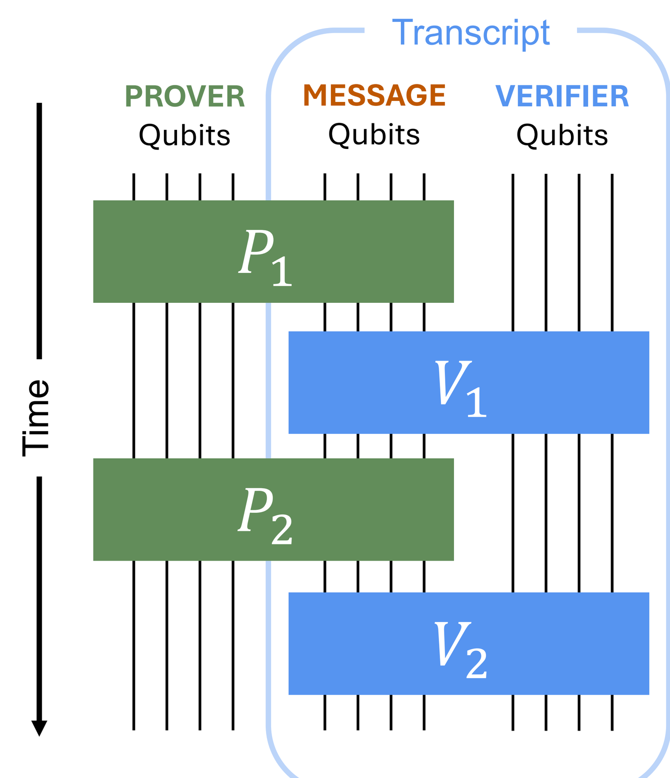
Quantum Statistical Witness Indistinguishability

Shafik Nassar (shafik@cs.utexas.edu), Ronak Ramachandran (ronakr@utexas.edu)
Department of Computer Science, The University of Texas at Austin

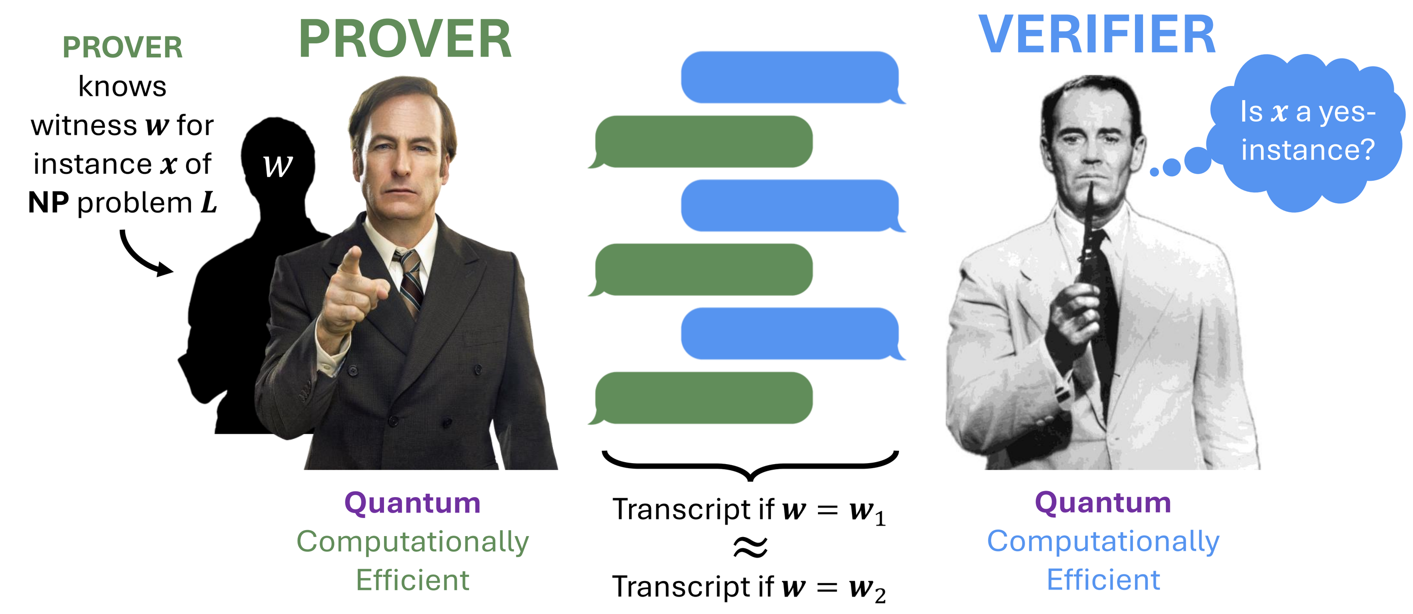
The University of Texas at Austin Computer Science College of Natural Sciences

arXiv link

Quantum Interactive Proofs



Quantum Statistical Witness Indistinguishability



Definition (QSWI). An **NP** problem is in **QSWI** if there exists a quantum interactive proof with an efficient quantum prover that takes a witness w as input, such that for all instances x, for any two valid witnesses w_1 and w_2, the verifier's view after each round of interaction when $w = w_1$ is statistically close to its view when $w = w_2$.

Relevant Variants

QSWI by default requires transcripts for different valid witnesses to be indistinguishable no matter what the verifier does. It will be easier to reason about honest verifiers:

Honest-Verifier (hvQSWI): The transcripts for different valid witnesses are only guaranteed to be indistinguishable for some specific verifier following a fixed protocol.

The opposite is **Malicious-Verifier**.

Public-Coin (pubQSWI): All verifier messages are uniformly random classical strings.

The opposite is **Private-Coin**.

By definition, all are in **NP**, and **pubQSWI ⊆ QSWI ⊆ hvQSWI**, and **pubSWI ⊆ SWI ⊆ hvSWI ⊆ hvQSWI.**

Simple 3-Message Public-Coin Protocols Suffice

Theorem 1.1. *Any problem in* **hvQSWI** *has a 3-message, public-coin quantum interactive proof that satisfies quantum statistical witness indistinguishability against malicious verifiers. In particular:* **pubQSWI = QSWI = hvQSWI.** *Moreover, the witness indistinguishability error in the resulting protocol is polynomially related to that in the original protocol.*

No analogous results are known for SWI.

Corollary 1.2. SWI ⊆ QSWI

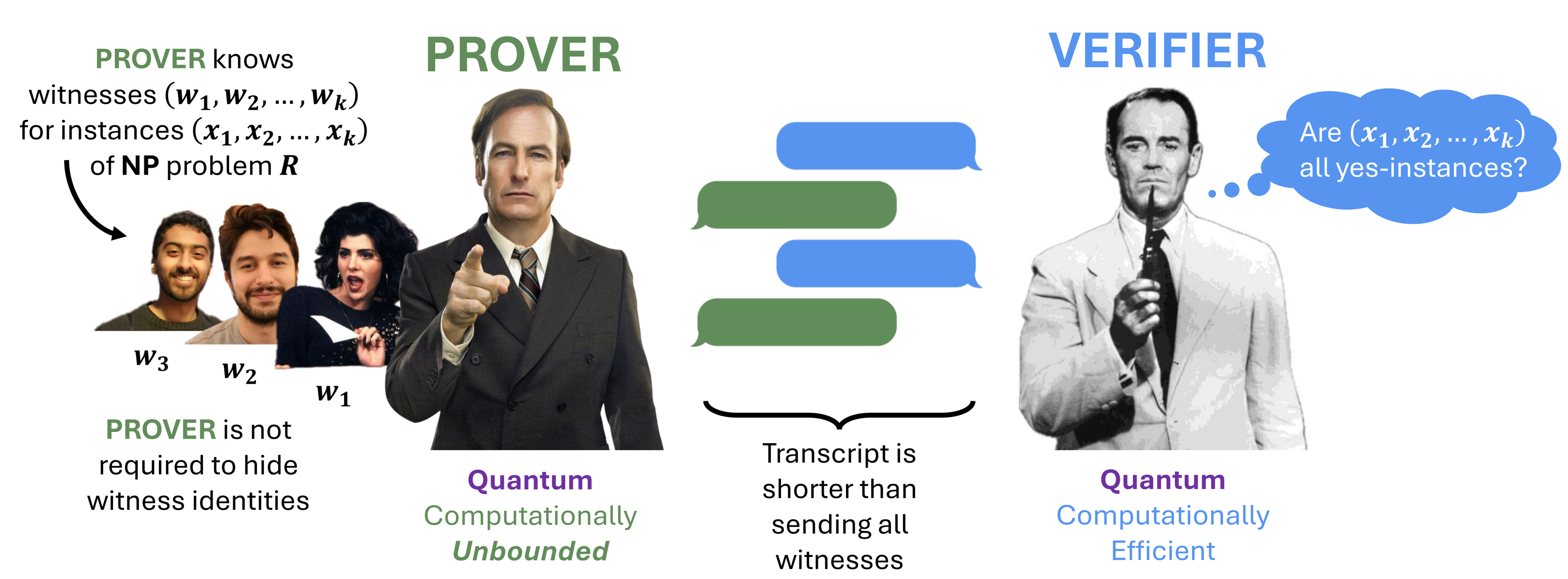
Note: Corollary 1.2 does not follow from definitions. *A priori*, malicious quantum verifiers might have had new quantum strategies for distinguishing witnesses.

Proof Sketch of Theorem 1.1.

(Proofs closely mirror similar results for QZK [Kobayashi 2008], but with efficient provers and WI error)

	Initial Protocol							Final Protocol						
	Rand.	Verifier	# msgs	C	S	WI Error		Rand.	Verifier	# msgs	C	S	WI Error	Technique
Lemma 4.1.	Private	Honest	m	$1-\varepsilon_c$	ε_s	ε_{WI}	→	Private	Honest	3	$1-\frac{\varepsilon_c}{2}$	$1-\frac{(1-\varepsilon_s)^2}{32(M+1)^2}$	$m\varepsilon_{WI}$	QIP = QIP(3) [Kitaev Watrous 2000]
Lemma 4.2.	Private	Honest	3	$1-\varepsilon_c$	ε_s	ε_{WI}	→	Private	Honest	3	$\left(1-\frac{\varepsilon_c}{2}\right)^p$	${\varepsilon_s}^p$	$p\varepsilon_{WI}$	p parallel repetitions
Lemma 4.3.	Private	Honest	m	$2/3$	$1/3$	ε_{WI}	→	Private	Honest	3	$1-2^{-p}$	2^{-p}	$\mathrm{negl(n)}$	Sequential repetition + Lemmas 4.1 and 4.2
Lemma 4.4.	Private	Honest	3	$1-\varepsilon_c$	ε_s	ε_{WI}	→	Public	Honest	3	$1-\frac{\varepsilon_c}{2}$	$\frac{1}{2}-\frac{\sqrt{\varepsilon_c}}{2}$	ε_{WI}	Verifier message can be single random bit [Marriott Watrous 2005]
Lemma 4.5.	Public	Honest	3	$1-\varepsilon_c$	ε_s	ε_{WI}	→	Public	Malicious	3	$1-\varepsilon_c$	ε_s	ε_{WI}	Careful simulation
Theorem 4.6.	Private	Honest	m	$2/3$	$1/3$	ε_{WI}	→	Public	Malicious	3	$1-2^{-p}$	2^{-p}	$\mathrm{negl(n)}$	Lemmas 4.1 - 4.5

Quantum Batch Proofs Imply QSWI



Definition (Quantum Batch Proof). For any **NP** relation R, a quantum batch proof for R is a quantum interactive proof for the relation

$$R^{\otimes k} \coloneqq \{((x_1, x_2, \dots, x_k), (w_1, w_2, \dots, w_k)) : \forall i \in [k], (x_i, w_i) \in R\}.$$

If the total communication in the interaction is a ρ fraction of the communication required for the prover to send all witnesses to the verifier, then we say the batch proof is ρ-compressing.

Theorem 1.3. *Let R be any* **NP** *relation. If R has a ρ-compressing quantum batch proof, then R has a quantum interactive proof with a non-uniform honest prover that satisfies quantum statistical witness indistinguishability against honest verifiers, with witness indistinguishability error $\sqrt{\rho}$.*

Proof Sketch of Theorem 1.3. Proof closely mirrors proof that batch proofs imply **SWI** [BKP+24] but uses *quantum* distributional stability [Drucker 2012]. The idea is that compression loses information about many witnesses, so the prover for **QSWI** can hide their witness among many "dummy" witnesses, still proving the desired instance to the verifier without revealing their witness. Note that, for this to work, the QSWI prover requires non-uniform advice.

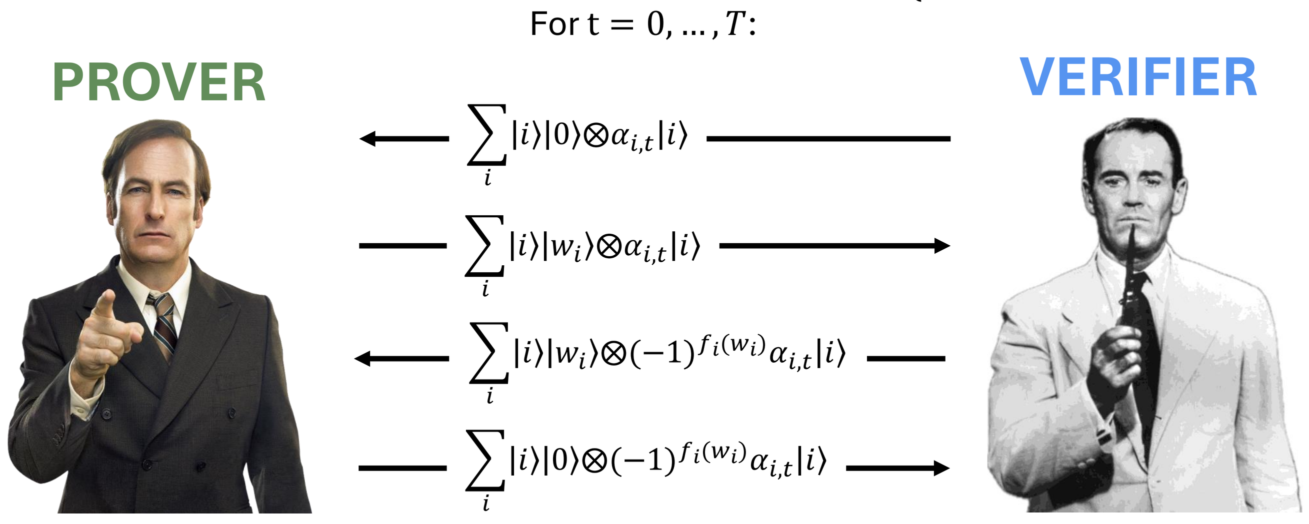
OPEN: NP = QSWI?

Theorem 1.3. suggests a path to proving **NP ⊆ QSWI**: prove every **NP** instance has quantum batch proofs.

A distributed Grover Search for invalid witnesses almost works:

VERIFIER samples $b \in \{0,1\}$ and j $\in [k]$. Define $f_i(w_i) = \begin{cases} (x_i, w_i) \notin R & \text{if } b = 0 \\ i = j & \text{if } b = 1. \end{cases}$

For t $= 0, \dots, T$:



VERIFIER applies Grover Diffusion and repeats

VERIFIER then measures last register to get i^*.
If $b = 0$, accept if $(x_{i^*}, w_{i^*}) \in R$. If $b = 1$, accept if $i^* = j$. Otherwise, reject.

Unfortunately, this fails if the prover entangles private registers with the message registers. Please let us know if you have ideas!

OPEN: Perfect Completeness?

[Kobayashi 2008] was able to prove completeness errors can be generically eliminated in any **QZK** protocol, but the techniques used do not preserve prover efficiency.

Can every **QSWI** proof be made to have perfect completeness?

Solving the following toy problem would imply yes:

Problem 6.1. *Construct an efficient quantum circuit that uses polynomially many copies of $\sqrt{p}|0\rangle + \sqrt{1-p}|1\rangle$ to exactly produce the state $\sqrt{1-\frac{c}{p}}|0\rangle + \sqrt{\frac{c}{p}}|1\rangle$ for some known efficiently computable constant c and unknown p.*

References

[BKP+24] Nir Bitansky, Chethan Kamath, Omer Paneth, Ron D Rothblum, and Prashant Nalini Vasudevan. Batch proofs are statistically hiding. In Proceedings of the 56th Annual ACM Symposium on Theory of Computing, pages 435–443, 2024.

[Drucker 2012] Andrew Drucker. New limits to classical and quantum instance compression. In 2012 IEEE 53rd Annual Symposium on Foundations of Computer Science, pages 609–618. IEEE, 2012.

[Kobayashi 2008] Hirotada Kobayashi. General properties of quantum zero-knowledge proofs. In Theory of Cryptography: Fifth Theory of Cryptography Conference, TCC 2008, New York, USA, March 19-21, 2008. Proceedings 5, pages 107–124. Springer, 2008.

[Kitaev Watrous 2000] Alexei Kitaev and John Watrous. Parallelization, amplification, and exponential time simulation of quantum interactive proof systems. In Proceedings of the thirty-second annual ACM symposium on Theory of computing, pages 608–617, 2000.

[Marriott Watrous 2005] Chris Marriott and John Watrous. Quantum arthur–merlin games. computational complexity,14(2):122–152, 2005.