A slightly improved upper bound for quantum statistical zero-knowledge

François Le Gall [1] **Yupan Liu** [2] Qisheng Wang [3]

[1]Nagoya University

[2]École Polytechnique Fédérale de Lausanne

[3]Shanghai Jiao Tong University

Available on arXiv:2512.11597.

Mathematical Foundations of Computer Science (MFCS 2026), Paris

1. Quantum state testing meets quantum statistical zero knowledge (QSZK)
2. First result: Algorithmic Holevo–Helstrom measurement and its implication
3. Second result: Algorithmic Uhlmann transform and its implication
4. Open problems

Definition 1.1 (Statistical zero-knowledge, informal). An interactive proof system admits the *(statistical) zero-knowledge* property if verifier's view ($\mathcal{P}_0$) is *(statistically) indistinguishable* from "verifier's view" ($\mathcal{P}_1$) generated by a polynomial-time simulator.

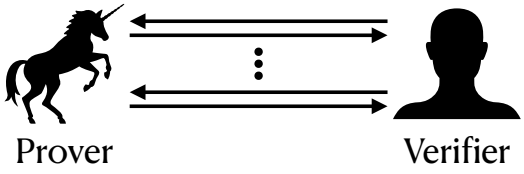


Figure: Verifier's view $\mathcal{P}_0$

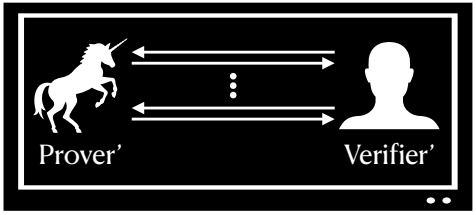


Figure: Simulated "Verifier's view" ($\mathcal{P}_1$)

- The prover in interactive proof system is typically *computationally unbounded* and untrusted.
- A common misuse (*unrelated to science*!): zero-knowledge vs. zero-entropy.
- Intuitively, the views $\mathcal{P}_0$ and $\mathcal{P}_1$ can be treated as distributions p_0 and p_1, respectively. Then *statistical indistinguishablity* is captured by the *total variation distance* between p_0 and p_1.

A complete problem and upper bounds for the class SZK

Definition 1.2 (Statistical Difference Problem, $\mathrm{SD}[\alpha,\beta]$) [Sahai–Vadhan'03].
Given efficiently samplable (namely, using polynomial-size Boolean circuits) distributions p_0 and p_1, decide whether $\mathrm{TV}(p_0,p_1) \geq \alpha$ or $\mathrm{TV}(p_0,p_1) \leq \beta$, where the total variation distance is defined by $\mathrm{TV}(p_0,p_1) := \frac{1}{2}\sum_{x\in S}|p_0(x)-p_1(x)|$.

Specifically, GapSD $:= \mathrm{SD}[\alpha,\beta]$ where $\alpha(n)-\beta(n) \geq 1/\mathrm{poly}(n)$.

Theorem 1.3 [Sahai–Vadhan'03, Goldreich–Sahai–Vadhan'98].
Statistical Difference Problem is SZK-complete. Specifically, $\mathrm{SD}[\alpha,\beta]$ is in SZK if $\alpha^2-\beta>0$ for constant α and β.

Upper bounds for SZK and GapSD

1. $\mathrm{SZK} \subseteq \mathrm{AM}$ [Aiello–Håstad'91, Fortnow'89, Goldreich–Sahai–Vadhan'98].
2. $\mathrm{SZK} = \mathrm{coSZK}$ [Okamoto'00] $\Rightarrow \mathrm{SZK} \subseteq \mathrm{AM}\cap\mathrm{coAM} \subseteq \mathrm{PH} \subseteq \mathrm{P}^{\mathrm{PP}}$.
3. There exists oracle $\mathcal{O}$ such that $\mathrm{SZK}^{\mathcal{O}} \not\subseteq \mathrm{PP}^{\mathcal{O}}$ [Bouland–Chen–Holden–Thaler–Vasudevan'17].
4. GapSD $\in \mathrm{AM}\cap\mathrm{coAM}$ [Bogdanov–Lee'13].

From quantum ℓ_1 norm to QUANTUM STATE DISTINGUISHABILITY PROBLEM

An n-qubit quantum state ρ is a $2^n \times 2^n$ matrix such that $\mathrm{Tr}(\rho) = 1$ and $\rho \succeq 0$.

Definition 1.4 (QUANTUM STATE DISTINGUISHABILITY PROBLEM, $\mathrm{QSD}[\alpha, \beta]$) [Watrous'02]. Given efficiently preparable (i.e., using polynomial-size quantum circuits) quantum states ρ_0 and ρ_1, decide whether $\mathrm{T}(\rho_0, \rho_1) \geq \alpha$ or $\mathrm{T}(\rho_0, \rho_1) \leq \beta$, where the trace distance $\mathrm{T}(\rho_0, \rho_1) := \frac{1}{2}\mathrm{Tr}|\rho_0 - \rho_1|$.

Write $\mathrm{GAPQSD} := \mathrm{QSD}[\alpha, \beta]$ when $\alpha(n) - \beta(n) \geq 1/\mathrm{poly}(n)$.

Theorem 1.5 [Watrous'02, Watrous'09]. QUANTUM STATE DISTINGUISHABILITY PROBLEM is QSZK-complete. Specifically, $\mathrm{QSD}[\alpha, \beta]$ is in QSZK if $\alpha^2 - \beta > 0$ for constant α and β.

Upper bounds for QSZK and GAPQSD

1. $\mathrm{QSZK} = \mathrm{QSZK_{HV}} \subseteq \mathrm{QIP(2)} \cap \text{co-QIP(2)} \cap \mathrm{PSPACE}$ [Watrous'02, Watrous'09].
2. $\mathrm{GAPQSD} \in \mathrm{PSPACE}$ [Watrous'02, Le Gall–**L.**–Wang'23].
3. $\mathrm{QSZK} \subseteq \mathrm{QIP(2)} \cap \text{co-QIP(2)} \subseteq \mathrm{PSPACE}$ [Jain–Upadhyay–Watrous'09].

★ **This work**: $\mathrm{QSZK} \subseteq \mathrm{QIP(2)} \cap \text{co-QIP(2)}$ with a *quantum linear-space* honest prover.

1. Quantum state testing meets quantum statistical zero knowledge (QSZK)
2. First result: Algorithmic Holevo–Helstrom measurement and its implication
3. Second result: Algorithmic Uhlmann transform and its implication
4. Open problems

Problem 2.1 (Computational Quantum Hypothesis Testing). Let Q_0 and Q_1 be two polynomial-size quantum circuits acting on n qubits and having r designated output qubits. Let ρ_b denote the quantum state obtained by performing Q_b on the initial state $|0\rangle^{\otimes n}$ and tracing out the non-output qubits for $b \in \{0,1\}$. Now, consider the following computational task:

- **Input:** A quantum state ρ, either ρ_0 or ρ_1, is chosen uniformly at random.
- **Output:** A bit b indicates that $\rho = \rho_b$.

Holevo–Helstrom bound

Theorem 2.2 [Holevo'73, Helstrom'69]. Given a quantum state ρ, either ρ_0 or ρ_1, that is chosen uniformly at random, the maximum success probability to discriminate between quantum states ρ_0 and ρ_1 is given by $\frac{1}{2} + \frac{1}{2}\mathrm{T}(\rho_0, \rho_1)$.

An optimal two-outcome measurement $\{\Pi_0, \Pi_1\}$ achieving the maximum discrimination probability:

$$\Pi_0 = \frac{I}{2} + \frac{1}{2}\mathrm{sgn}^{(\mathrm{SV})}\left(\frac{\rho_0 - \rho_1}{2}\right) \text{ and } \Pi_1 = \frac{I}{2} - \frac{1}{2}\mathrm{sgn}^{(\mathrm{SV})}\left(\frac{\rho_0 - \rho_1}{2}\right).$$

It is straightforward to see that $\mathrm{T}(\rho_0, \rho_1) = \frac{1}{2}\mathrm{Tr}|\rho_0 - \rho_1| = \mathrm{Tr}(\Pi_0\rho_0) - \mathrm{Tr}(\Pi_0\rho_1)$.

An approximately explicit implementation of the Holevo–Helstrom measurement

Theorem 2.3 (Algorithmic Holevo–Helstrom measurement). Let ρ_0 and ρ_1 be states prepared by n-qubit quantum circuits Q_0 and Q_1, respectively, as defined in Problem 2.1. An approximate version of the Holevo–Helstrom measurement Π_0, denoted by $\tilde{\Pi}_0$, can be implemented such that

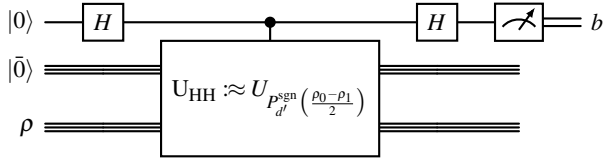
$$|\mathrm{T}(\rho_0,\rho_1) - \big(\mathrm{Tr}(\tilde{\Pi}_0\rho_0) - \mathrm{Tr}(\tilde{\Pi}_0\rho_1)\big)| \le 2^{-n}.$$

The quantum circuit implementation of $\tilde{\Pi}_0$, acting on $O(n)$ qubits, requires $2^{O(n)}$ uses to the circuits Q_0, Q_1, one-, and two-qubit gates. Moreover, the circuit description can be computed in deterministic time $2^{O(n)}$ and space $O(n)$.

Proof Sketch. Instead of implementing $\{\Pi_0,\Pi_1\}$, it suffices to *approximately* implement $\{\hat{\Pi}_0,\hat{\Pi}_1\}$ by the space-efficient QSVT associated with the sign function [Le Gall–**L.**–Wang'23]:

$$\hat{\Pi}_0 = \frac{I}{2} + \frac{1}{2}P^{\mathrm{sgn}}_{d'}\Big(\frac{\rho_0-\rho_1}{2}\Big) \text{ and } \hat{\Pi}_1 = \frac{I}{2} - \frac{1}{2}P^{\mathrm{sgn}}_{d'}\Big(\frac{\rho_0-\rho_1}{2}\Big).$$

Once we have a block-encoding of $P^{\mathrm{sgn}}_{d'}\big(\frac{\rho_0-\rho_1}{2}\big)$, we can implement Π_0:



GapQSD is in QIP(2) with a quantum linear space honest prover

Theorem 2.4 (GapQSD is in QIP(2) with a quantum linear-space honest prover). There is a two-message quantum interactive proof system for $\mathrm{QSD}[\alpha(n),\beta(n)]$ with completeness $c(n) = \left(1+\alpha(n)-2^{-n}\right)/2$ and soundness $s(n) = (1+\beta(n))/2$. Moreover, a *near-optimal* prover strategy for this protocol can be implemented in quantum $2^{O(n)}$ time and $O(n)$ space.

Protocol: Two-message proof system for GapQSD (quantum linear-space prover).

1. The verifier $\mathcal{V}$ first chooses $b \in \{0,1\}$ uniformly at random. Subsequently, $\mathcal{V}$ applies Q_b to $|0\rangle^{\otimes n}$, traces out all non-output qubits, and sends the resulting state ρ_b.
2. The verifier $\mathcal{V}$ receives a single-qubit state $\hat{\sigma}$, measures the state in the computational basis, and denotes the outcome by $\hat{b} \in \{0,1\}$.

   The *honest* prover $\mathcal{P}$ measures the received state ρ using the algorithmic Holevo–Helstrom measurement $\{\tilde{\Pi}_0, \tilde{\Pi}_1\}$ (Theorem 2.3), and sends the outcome $\hat{b}$. In particular, the outcome equals $\hat{b}$ if the measurement indicates ρ is $\rho_{\hat{b}}$.

3. The verifier $\mathcal{V}$ accepts if $b = \hat{b}$; otherwise $\mathcal{V}$ rejects.

1. Quantum state testing meets quantum statistical zero knowledge (QSZK)
2. First result: Algorithmic Holevo–Helstrom measurement and its implication
3. Second result: Algorithmic Uhlmann transform and its implication
4. Open problems

Problem 3.1 (Computational Uhlmann Fidelity Test). Let Q_0 and Q_1 be polynomial-size quantum circuits acting on n qubits in registers (A,R), each with r output qubits in register A. Let $|\psi_b\rangle$ be the pure state obtained by performing Q_b on $|0^n\rangle$, and let ρ_b be the state obtained by further tracing out the non-output qubits in R for $b \in \{0,1\}$. Now, consider the following computational task:

- **Input:** The qubits of the purification $|\psi_1\rangle$ in the reference register R, while all qubits in the output register A are fixed and cannot be modified.
- **Output:** A bit z obtained from the measurement $\{\Pi, I-\Pi\}$, where $\Pi := |\psi_0\rangle\langle\psi_0|$.

$\star$ The probability that the Uhlmann fidelity test (Problem 3.1) succeeds (i.e., obtaining the first outcome) is characterized by *the (squared) Uhlmann fidelity* $\mathrm{F}^2(\rho_0,\rho_1) := \mathrm{Tr}\left(|\sqrt{\rho_0}\sqrt{\rho_1}|\right)^2$.

Uhlmann's theorem

Theorem 3.2 [Uhlmann'76, Jozsa'94]. Let ρ_0 and ρ_1 be states on register A. For any fixed purification $|\psi_0\rangle$ of ρ_0 on registers (A,R), the maximum overlap between $|\psi_0\rangle$ and any purification $|\psi_1\rangle$ of ρ_1 on the same registers is given by the fidelity, with $|\psi_1\rangle = U^{\mathrm{R}}|\psi_1'\rangle$:

$$\mathrm{F}^2(\rho_0,\rho_1) = \max_{|\psi_1\rangle} |\langle\psi_0|\psi_1\rangle|^2 = \max_{U} \left|\langle\psi_0|\left(I^{\mathrm{A}}\otimes U^{\mathrm{R}}\right)|\psi_1'\rangle\right|^2.$$

An explicit form of the Uhlmann transform

Lemma 3.3 (Explicit form of the Uhlmann transform, [Jozsa'94, Metger–Yuen'23]).
Let $|\psi_0\rangle$ and $|\psi_1\rangle$ be purifications of quantum states ρ_0 and ρ_1 on register A, defined on registers (A,R), where R is the reference register. Let X_{Uhl} be a linear operator on register R. A unitary $U_\star$ on register R that attains the maximum in Uhlmann's theorem (Theorem 3.2) is given by

$$U_\star = \mathrm{sgn}^{(\mathrm{SV})}(X_{\mathrm{Uhl}}), \quad \text{where } X_{\mathrm{Uhl}} \coloneqq \mathrm{Tr}_{\mathsf{A}}\left(|\psi_0\rangle\langle\psi_1|^{\mathsf{AR}}\right).$$

Lemma 3.4 (Exact block-encoding of $\mathrm{Tr}_{\mathsf{A}}\left(|\psi_0\rangle\langle\psi_1|^{\mathsf{AR}}\right)$, [Utsumi–Nakata–Wang–Takagi'25]).
An *exact* block encoding of X_{Uhl} using n ancillary qubits, implemented by the unitary W on registers $(\mathsf{A}',\mathsf{R},\mathsf{E})$, where A' is identical to A and E contains the same number of qubits as R, is given by

$$\langle\bar{0}|^{\mathsf{A}'}\langle\bar{0}|^{\mathsf{E}} W |\bar{0}\rangle^{\mathsf{A}'}|\bar{0}\rangle^{\mathsf{E}} = X_{\mathrm{Uhl}}, \text{ where } W \coloneqq \left(Q_1^{\mathsf{A}'\mathsf{R}}\right)^\dagger \left(I^{\mathsf{A}'} \otimes \mathrm{SWAP}^{\mathsf{R},\mathsf{E}}\right) Q_0^{\mathsf{A}'\mathsf{R}}.$$

This block-encoding can be implemented using one query to each state-preparation circuit Q_0 and Q_1, together with $O(n)$ one- and two-qubit quantum gates.

★ When one state is pure, $\mathrm{sgn}^{(\mathrm{SV})}$ is no longer needed in the explicit form of $U_\star$, and thus the exact block-encoding (Lemma 3.4) leads to an optimal estimator for the fidelity [**L.**–Wang'26].

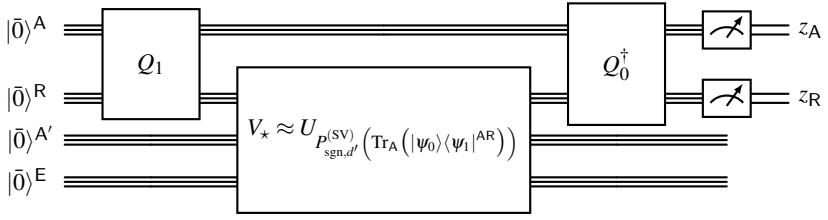
An approximately explicit implementation of the Uhlmann transform

Theorem 3.5 (Algorithmic Uhlmann transform). Let ρ_0 and ρ_1 be quantum states prepared by n-qubit quantum circuits Q_0 and Q_1, and let $|\psi_0\rangle$ and $|\psi_1\rangle$ denote their purifications before tracing out the non-output qubits, as in Problem 3.1. An approximate version of the Uhlmann transform $U_\star$ specified in Lemma 3.3, denoted by $\tilde{U}_\star$, can be implemented so that

$$\mathrm{F}^2(\rho_0,\rho_1) - 2^{-n} \leq \left|\langle\psi_0|^{\mathsf{AR}}\left(I^{\mathsf{A}}\otimes\tilde{U}_\star^{\mathsf{R}}\right)|\psi_1\rangle^{\mathsf{AR}}\right|^2 \leq \mathrm{F}^2(\rho_0,\rho_1).$$

The quantum circuit implementation of $\tilde{U}_\star$, acting on $O(n)$ qubits, requires $2^{O(n)}$ uses to the quantum circuits Q_0 and Q_1, as well as $2^{O(n)}$ one- and two-qubit quantum gates. Moreover, the circuit description can be computed in deterministic time $2^{O(n)}$ and space $O(n)$.

Proof Sketch. The quantum circuit construction uses the space-efficient QSVT associated with the sign function [Le Gall–**L.**–Wang'23] and the exact block-encoding of $\mathrm{Tr}_{\mathsf{A}}(|\psi_0\rangle\langle\psi_1|^{\mathsf{AR}})$:



GapF^{2}Est is in QIP(2) with a quantum linear space honest prover

Definition 3.6 (Quantum Squared Fidelity Estimation Problem, F^{2}Est$[\alpha,\beta]$). Given efficiently preparable quantum states ρ_0 and ρ_1, decide whether $\mathrm{F}^2(\rho_0,\rho_1) \geq \alpha$ or $\mathrm{F}^2(\rho_0,\rho_1) \leq \beta$.

Write GapF^{2}Est $\coloneqq$ F^{2}Est$[\alpha,\beta]$ when $\alpha(n) - \beta(n) \geq 1/\mathrm{poly}(n)$.

Theorem 3.7 (GapF^{2}Est is in QIP(2) with a quantum linear-space honest prover). There exists a two-message quantum interactive proof system for F^{2}Est$[\alpha(n),\beta(n)]$ with completeness $c(n) = \alpha(n) - 2^{-n}$ and soundness $s(n) = \beta(n)$. Moreover, a *near-optimal* prover strategy for this proof system can be implemented in quantum $2^{O(n)}$ time and $O(n)$ space.

A consequence for Quantum State Closeness Problem (QSC), the *complement* of QSD:

Corollary 3.8. For any efficiently computable functions $\alpha(n)$ and $\beta(n)$ satisfying $0 \leq \beta(n) < \alpha(n) \leq 1$ and $\alpha^2(n) - \beta(n) \geq 1/O(\log n)$, QSC$[\beta,\alpha]$ is in QIP(2) with a quantum linear-space honest prover.

GapF^{2}Est is in QIP(2) with a quantum linear space honest prover (Cont.)

The two-message quantum interactive proof system underlying Theorem 3.7:

Protocol: Two-message proof system for GapF^{2}Est (quantum linear-space prover).

---

1. The verifier $\mathcal{V}$ applies Q_0 to $|0\rangle^{\otimes n}$, and sends the *non-output* qubits in register R, while keeping output qubits in register A.
2. The verifier $\mathcal{V}$ receives the (possibly modified) qubits in register R.

   The *honest* prover $\mathcal{P}$ applies the algorithmic Uhlmann transform $\tilde{U}_\star$ (Theorem 3.5) to the received qubits, and sends the resulting qubits back.

3. The verifier $\mathcal{V}$ applies $Q_1^\dagger$ to the registers (A,R), where register A contains the output qubits of Q_0 and register R contains the received qubits. $\mathcal{V}$ then measures all qubits in (A,R) in the computational basis and accepts if the measurement outcome is the n-bit all-zero string; otherwise, $\mathcal{V}$ rejects.

---

1. Quantum state testing meets quantum statistical zero knowledge (QSZK)
2. First result: Algorithmic Holevo–Helstrom measurement and its implication
3. Second result: Algorithmic Uhlmann transform and its implication
4. Open problems

Conclusions and open problems

Take-home messages

1. The Holevo–Helstrom measurement can be *approximately* implemented by the space-efficient QSVT in quantum $2^{O(n)}$ time and $O(n)$ space. Consequently, GAPQSD is in QIP(2) with a *quantum linear-space* honest prover.
2. The Uhlmann transform can be *approximately* implemented by the space-efficient QSVT in quantum $2^{O(n)}$ time and $O(n)$ space. Consequently, GAPF^{2}EST (and thus QSC) is in QIP(2) with a *quantum linear-space* honest prover.

Open problems

1. Could the quantum upper bound for QSZK be improved to a subclass of QIP(2) defined via "public-coin" quantum interactive proof systems [Marriott–Watrous'05, Kobayashi–Le Gall–Nishimura'19]?
2. Could the classical upper bounds for QSZK be improved to any subclass of PSPACE?
3. Could the honest prover's strategy in any two-message quantum interactive proof system be *approximately* implemented in quantum *linear* space? Namely, the space complexity of the algorithmic implementation scales *linearly* with # of qubits used by the verifier's first action.

Merci!