CONJURA · OPEN PROBLEM

Hardness of Double-Sided Zero Search

Random invertible permutation, superposition queries in both directions

Status. Statement: AI-written from Dominique Unruh, *Towards Compressed Permutation Oracles*, IACR Cryptology ePrint Archive (preprint, University of Tartu) 2023, not yet checked by a human. Open unconditionally — no case is settled: the source establishes the statement only under its own Conjecture 2 (soundness of the compressed permutation oracle), and presents that argument as a usage example rather than as a proof.

Category. *Idealized Models & Non-Uniformity.*

Conjecture (informal). *Take a uniformly random permutation on strings of length two n, and give a quantum adversary superposition access both to the permutation and to its inverse. Ask it to find an n-bit string x such that feeding x followed by n zeros into the permutation produces an output that also ends in n zeros. Classically this is a plain search question — not a birthday question — and about two to the n queries are needed. Quantumly, no lower bound can currently be proved at all; the two-to-the-n-over-two figure appearing in the paper is the quantum bound its conditional compressed-permutation-oracle argument yields. The reason is that the available tools do not apply: the standard trick of replacing a random permutation by a random function is only valid when the adversary cannot query the inverse, and the lazy-sampling technique that handles quantum random oracles has never been made to work for permutations. This problem is the paper's chosen example of how thin the ground is: it is about the simplest search question one can ask about an invertible random permutation, and it is open. The paper does give a proof sketch, but only assuming that its candidate lazy-sampling simulator for permutations is sound, which is itself unproven.*

1 The setting

For quantum random oracles there is a rich toolbox of hardness results, and since Zhandry's compressed oracle [Zha19] a general lazy-sampling method as well. For random permutations the situa-

tion splits sharply according to whether the adversary can invert. If it cannot, a random permutation is quantum-indistinguishable from a random function [Zha15], so any question about a non-invertible random permutation reduces to the random-function case and the whole toolbox applies. If it can — the case that actually models block ciphers and permutation-based hash functions — the paper reports that no hardness results whatsoever are known, not even elementary query-complexity statements such as the hardness of finding an input with a prescribed property. The semi-classical one-way-to-hiding theorem [AHU19] does formally cover arbitrarily distributed functions, hence invertible permutations, but the paper notes it is not aware of any work exploiting this.

The problem below is the paper's chosen witness for that gap: find x with both x and its image ending in n zeros, given forward and inverse superposition access. Classically the problem is an easy lazy-sampling exercise and takes $\Theta(2^n)$ queries: there are about 2^n candidate inputs $x\|0^n$, and each forward (or backward) query hits the 2^n-element zero-suffix set with probability about 2^{-n}. The paper itself states no classical bound. What the paper sketches in the compressed-permutation-oracle framework is the quantum bound $\Theta(2^{n/2})$ (p. 13), and only under Conjecture 2: the invariant is that the recorded partial function contains no double-sided zero, a forward query moves the state $O(2^{-n/2})$ away from the invariant subspace, and the crucial new observation is that the inversion operator used to answer backward queries *preserves* the invariant, because h has a double-sided zero exactly when h^{-1} does. That sketch, however, is only as good as the soundness of the simulator, which the paper conjectures but does not prove. Unconditionally, the problem is untouched.

Progress to date. Conditional on the soundness of the compressed permutation oracle, the paper sketches a full proof and in fact a quantitative bound: with the invariant "the recorded partial function contains no x,y with $h(x\|0^n) = y\|0^n$", a forward query moves the state $O(2^{-n/2})$ from the invariant subspace, the inversion operator answering backward queries preserves the invariant exactly, and hence after q queries the state is $O(q\,2^{-n/2})$-close to it, so $\Theta(2^{n/2})$ queries are needed. The paper also explains why the standard reduction is unavailable: replacing the permutation by a random function is sound only for forward-only access.

Why it matters. It would be the first hardness result of any kind for an invertible random permutation under superposition access, in a model where the paper reports that literally none are known. The problem is deliberately minimal — a search problem with a syntactic condition on input and output — so a proof would almost certainly come with a reusable technique rather than a one-off argument, and that technique is what the whole area is missing. It is also a sharp test case in the other direction: the classical answer is a routine $\Theta(2^n)$ search bound, so a surprising quantum algorithm here would say something genuinely new about superposition access to permutation inverses. Finally, it is the smallest concrete consequence of the paper's soundness conjecture, so it is the natural first target for anyone who wants to attack that conjecture from below.

Why it is clean. The statement needs no idealized-model machinery, no simulator, and no definitions beyond concatenation and a standard XOR query unitary: a random permutation on $2n$ bits, two oracles, one output string, one success predicate. It is information-theoretic, so there is no assumption to argue about, and both the conjectured answer and the classical baseline are unambiguous. Anyone who can prove quantum query lower bounds can start on it immediately.

2 Notation and parameters

For $n \in \mathbb{N}$ and strings u, v, $u\|v$ denotes concatenation, and 0^n the all-zero string of length n. For a finite set S, $\mathrm{Perm}(S)$ is the set of bijections $S \to S$.

For a permutation $G \in \mathrm{Perm}(\{0,1\}^m)$, U_G denotes the unitary on $\mathbb{C}^{\{0,1\}^m} \otimes \mathbb{C}^{\{0,1\}^m}$ with $U_G|u\rangle|v\rangle = |u\rangle|v \oplus G(u)\rangle$, where $\oplus$ is bitwise XOR. Superposition ("quantum") access to G means access to U_G as a black box.

An oracle algorithm A with access to two oracles is a quantum algorithm that alternates unitaries on its own registers with invocations of either oracle on designated registers; its *query count* is the total number of such invocations, and $x \leftarrow A^{O_1,O_2}()$ denotes the string obtained by measuring its output register at the end.

A function $\mu : \mathbb{N} \to \mathbb{R}_{\geq 0}$ is *negligible* if for every $c > 0$ there is n_0 with $\mu(n) < n^{-c}$ for all $n \geq n_0$.

Parameters.

- n — half the bit length of the permutation's domain; the permutation acts on $\{0,1\}^{2n}$ and the zero-suffix has length n.
- p — polynomial bounding the adversary's total number of forward and inverse queries as a function of n.
- H — the uniformly random permutation on $\{0,1\}^{2n}$; the adversary gets superposition access to H and to H^{-1}.

3 The conjecture

Conjecture 1 (hardness of double-sided zero search). *For every polynomial p there is a negligible function μ such that for all $n \in \mathbb{N}$ and every oracle algorithm A with query count at most $p(n)$,*

$$\Pr\Big[\ \exists y \in \{0,1\}^n :\ H(x\|0^n) = y\|0^n \ \Big|\ H \xleftarrow{\$} \mathrm{Perm}(\{0,1\}^{2n}),\ x \leftarrow A^{U_H, U_{H^{-1}}}()\ \Big] \ \leq\ \mu(n),$$

where A's output is read as an element $x \in \{0,1\}^n$.

4 Bibliography

[AHU19] A. Ambainis, M. Hamburg, D. Unruh. *Quantum Security Proofs Using Semi-classical Oracles.* Crypto 2019, pages 269–295, Springer, 2019.

[Zha15] M. Zhandry. *A note on the quantum collision and set equality problems.* Quantum Inf. Comput. 15.7&8, pages 557–567, 2015.

[Zha19] M. Zhandry. *How to Record Quantum Queries, and Applications to Quantum Indifferentiability.* Crypto 2019, volume 11693 of LNCS, pages 239–268, Springer, 2019.