2022 IEEE 63rd Annual Symposium on Foundations of Computer Science (FOCS) | 978-1-6654-5519-0/22/$31.00 ©2022 IEEE | DOI: 10.1109/FOCS54457.2022.00014

Verifiable Quantum Advantage without Structure

Takashi Yamakawa
NTT Social Informatics Laboratories
Tokyo, Japan
takashi.yamakawa.ga@hco.ntt.co.jp

Mark Zhandry
NTT Research & Princeton University
Sunnyvale, USA
mzhandry@gmail.com

***Abstract*—We show the following hold, unconditionally unless otherwise stated, relative to a random oracle with probability 1:**

- **There are NP *search* problems solvable by BQP machines but not BPP machines.**
- **There exist functions that are one-way, and even collision resistant, against classical adversaries but are easily inverted quantumly. Similar separations hold for digital signatures and CPA-secure public key encryption (the latter requiring the assumption of a classically CPA-secure encryption scheme). Interestingly, the separation does not necessarily extend to the case of other cryptographic objects such as PRGs.**
- **There are unconditional publicly verifiable proofs of quantumness with the minimal rounds of interaction: for uniform adversaries, the proofs are non-interactive, whereas for non-uniform adversaries the proofs are two message public coin.**
- **Our results do not appear to contradict the Aaronson-Ambanis conjecture. Assuming this conjecture, there exist publicly verifiable certifiable randomness, again with the minimal rounds of interaction.**

By replacing the random oracle with a concrete cryptographic hash function such as SHA2, we obtain plausible Minicrypt instantiations of the above results. Previous analogous results all required substantial structure, either in terms of highly structured oracles and/or algebraic assumptions in Cryptomania and beyond.

I. Introduction

Can NP *search problems have a super-polynomial speed-up on quantum computers?* This is one of the oldest and most important questions in quantum complexity.

The first proposals for such quantum advantage were relative to highly structured oracles. Examples include Simon's oracle [36], or more generally periodic oracles, as well as the Bernstein–Vazirani oracle [10] and welded trees [18].

The first non-relativized quantum advantage for NP problems is due to Shor's famous algorithm for factoring integers and computing discrete logarithms [35]. Since Shor's algorithm, other non-relativized NP problems with quantum advantage include solving Pell's equation [24] and matrix group membership [6]. While the technical details of all these examples are very different, these problems can all be seen as non-relativizing instantiations of *periodic* oracles.

While the above non-relativizing problems are certainly easy on a quantum computer, the classical hardness can only be conjectured since, in particular, the classical hardness would imply P $\neq$ NP, or an analogous statement if one considers probabilistic algorithms. The problem is that, when instantiating an oracle with real-world computational tasks, non-black-box algorithms may be available that render the problem classically easy, despite the oracle problem being hard. For example, index calculus methods [4] yield sub-exponential time attacks for factoring and discrete logarithms, despite black box period-finding being exponentially hard.

To make matters worse, for the known NP search problems with plausible quantum advantage, the classical hardness is widely believed to be a much stronger assumption than P $\neq$ NP, since the problems have significant algebraic structure and are not believed to be NP-complete. In particular, all NP search problems we are aware of yielding a super-polynomial quantum advantage rely on *Cryptomania* tools [26], in the sense that their classical hardness can be used to build public key encryption.[1] This puts the assumptions needed for an NP quantum advantage quite high in the assumption hierarchy.

a) Quantum speed-ups and structure: The above tasks demonstrating speed-ups, both relativized and non-relativized, all have one thing in common: significant "structure." It is natural to wonder whether such structure is necessary. In the oracle-free non-relativized setting, a natural interpretation of this question could be if Minicrypt assumptions—those that give symmetric key but not public key cryptography—can be used to give a quantum advantage. Minicrypt assumptions, such as the one-wayness of SHA2, lack the algebraic structure needed in typical super-polynomial quantum speed-ups. In the oracle setting, this could mean, for example, proving unconditional quantum advantage relative to a uniformly *random* oracle, which is generally seen as beeing structure-less.

Prior work on this topic could be interpreted as negative. As observed above, all non-relativizing NP problems demonstrating quantum advantage imply, or are closely related to problems that imply, public key cryptography. In the random oracle setting, the evidence is even stronger. The most natural problems to reason about—one-wayness and collision resistance of the random oracle, and generalizations—provably only have a polynomial quantum advantage [3], [9], [40], [42]. Additional evidence is given by Aaronson and Ambanis [1], who build on work of Beals et al. [7]. They consider the following conjecture, dating back to at least 1999:

Conjecture 1.1 (Paraphrased from [1]): Let Q be a

The full version is available at [39].

[1] Matrix group membership includes discrete logarithms as a special case. For a public key system based on Pell's equations, see [32].

978-1-6654-5519-0/22/$31.00 ©2022 IEEE
DOI 10.1109/FOCS54457.2022.00014

quantum algorithm with *Boolean* output that makes T queries to a random oracle $\mathcal{O}$, and let $\epsilon, \delta > 0$. Then there exists a deterministic classical algorithm C that makes $\mathsf{poly}(T, 1/\epsilon, 1/\delta)$ queries, such that

$$\Pr_{\mathcal{O}}\left[\ \left|\ C^{\mathcal{O}}() - \Pr[Q^{\mathcal{O}}() = 1]\ \right| \leq \epsilon\ \right] \geq 1 - \delta\ ,$$

Where the expectation is over the randomness of Q.

Aaronson and Ambanis give some evidence for Conjecture 1.1, by reducing it to a plausible *mathematical* conjecture closely related to known existing results. If Conjecture 1.1 is true, any quantum *decision* algorithm Q making queries to a random oracle can be simulated classically with only polynomially-more queries.

Note that the conjectured classical simulator may be *computationally* inefficient, and indeed we would expect it to be if, say, Q ignored its oracle and just factored integers. But for any particular algorithm Q, proving computational inefficiency amounts to an unconditional hardness result, which is beyond the reach of current complexity theory. Thus, Conjecture 1.1, if true, essentially shows that random oracles are equivalent to the non-relativizing world with respect to NP decision problems, and cannot be used to provide provable quantum advantage for such problems.

A. *Our Results*

In this work, we make progress toward justifying super-polynomial quantum advantage for NP problems, under less structured oracles or milder computational assumptions. We show, perhaps surprisingly, that for certain *search* problems in NP, random oracles do in fact give provable unconditional super-polynomial quantum speed-ups.

a) Random oracles: Our starting point is to prove the following theorem:

Theorem 1.2 (Informal): Relative to a random oracle with probability 1, there exists a non-interactive proof of quantumness, with unconditional security against any computationally-unbounded uniform adversary making a polynomial number of classical queries.

Here, a proof of quantumness [13] is a protocol between a quantum prover and classical verifier (meaning in particular that messages are classical) where no cheating classical prover can convince the verifier. By being non-interactive, our protocol is also publicly verifiable. Prior LWE-based proofs of quantumness [13], [14] lacked verifiability. The only previous publicly verifiable proof of quantumness [5] required highly non-trivial structured oracles.

Remark 1: We note the restriction to uniform adversaries is necessary in the non-interactive setting, as a non-uniform adversary (that may take oracle-dependent advice) can simply have a proof hardcoded. Our protocol also readily gives a two-message public coin (and hence also publicly verifiable) protocol against non-uniform adversaries, which is the best one can hope for in the non-uniform setting.

Theorem 1.2 has a number of interesting immediate consequences:

Corollary 1.3: Relative to a random oracle, there exists an NP search problem that is solvable by BQP machines but not by BPP machines.

Our construction also readily adapts to give one-way functions that are classically secure but quantum insecure. We can alternatively use minimal-round proofs of quantumness generically to give a one-way function separation, and even a collision resistance separation:

Theorem 1.4: Relative to a random oracle, there exists a compressing function that is collision resistant against any computationally unbounded uniform adversary making a polynomial number of classical queries, but is not even one-way against quantum adversaries.

Using results from [38], we also obtain an unconditional analogous separation for digital signatures and CPA-secure public key encryption (the latter requiring assuming classically CPA-secure public key encryption). Previous such results required LWE (in the case of signatures) or highly structured additional oracles (in the case of CPA-secure encryption).

Our results do not appear to contradict Conjecture 1.1, since they are for *search* problems as opposed to *decision* problems. In particular, our quantum algorithm for generating proofs of quantumness/breaking the one-wayness does not compute a function, but rather samples from a set of possible values. Assuming Conjecture 1.1 shows that this is inherent. We leverage this feature to yield the following:

Theorem 1.5: Assuming Conjecture 1.1, relative to a random oracle there exists a one- (resp. two-) message certifiable randomness protocol against a single uniform (resp. non-uniform) quantum device. By adding a final message from the verifier to the prover, our protocols become public coin and publicly verifiable.

Here, certifiable randomness [13] means the classical verifier, if it accepts, is able to expand a small random seed s into a truly random bit-string $x, |x| \gg |s|$, with the aid of a single quantum device. Conditioned on the verifier accepting, x remains truly random even if the device is adversarial.

We note that our results are the best possible: if the final message is from prover to verifier, the protocols cannot be publicly verifiable. Indeed, the prover could force, say, the first output bit to be 0 by generating a candidate final message, computing the what the outputted string would be, and then re-sampling the final message until the first output bit is 1. Our one- and two-message protocols therefore require verifier random coins that are kept from the prover. In our protocols, however, these secret random coins can be sampled and even published after the prover's message. The result is that, by adding a final message from the verifier, our protocols are public coin and publicly verifiable.

b) Instantiating the random oracle: We next instantiate the random oracle in the above construction with a standard-model cryptographic hash, such as SHA2. We cannot hope to prove security unconditionally. Nevertheless, the resulting construction is quite plausibly secure. Indeed, it is common practice in cryptography to prove security of a hash-based protocol relative to random oracles [8], and then assume that security also applies when the random oracle is replaced with a concrete well-designed cryptographic hash. While there are known counter-examples to the random oracle assumption [16], they are quite contrived and are not known to apply to our construction.

We thus obtain a plausible assumption on, say SHA2, under which non-interactive proofs of quantumness exist. This gives a completely new approach to non-relativized quantum advantage. What's more, it is widely believed that SHA2 is only capable of yielding symmetric key cryptosystems. Impagliazzo and Rudich [27] show that there is no classical black box construction of public key encryption from cryptographic hash functions, and no quantum or non-black box techniques are known to overcome this barrier. In fact, what [27] show is that, in the world of computationally unbounded but query bounded (classical) attackers, random oracles cannot be used to construct public key encryption. But this is exactly the setting of the random oracle model we consider.

Therefore, by instantiating the random oracle with a well-designed hash such as SHA2, we obtain a Minicrypt construction of a proof of quantumness. We likewise obtain candidate Minicrypt examples of NP search problems in $\mathsf{BQP} \setminus \mathsf{BPP}$, functions that are classically one-way but quantumly easy, and even certifiable randomness.

B. Discussion

a) Other sources of quantum advantage: Other candidates for super-polynomial quantum speed-ups are known. Aaronson and Arkhipov [2] and Bremner, Jozsa, and Shepherd [15] give a sampling task with such a speed-up, based on plausible complexity-theoretic constructions. Similar sampling tasks are at the heart of current real-world demonstrations of quantum advantage. More recently, Brakerski et al. [13] provided a proof of quantumness from the Learning With Errors (LWE) assumption.

We note, however, that none of the these alternate sources of quantum advantage correspond to NP search problems.

b) Why NP *search problems?:* Most real-life problems of interest can be phrased as NP search problems, so it is a natural class of problems to study. Our work gives the first evidence besides period finding of a quantum advantage for this class.

Moreover, NP means that solutions can be efficiently verified. For existing sampling-based demonstrations of quantum advantage [2], [15], verification is roughly as hard as classically sampling. Proofs of quantumness from LWE [13] do admit verification, but the verifier must use certain secrets computed during the protocol in order to verify. This means that only the verifier involved in the protocol is convinced of the quantumness of the prover.

In contrast, using an NP problem means anyone can look at the solution and verify that it is correct. Moreover, our particular instantiation allows for sampling the problems obliviously, meaning we obtain a *public coin* proof of quantumness where the verifier's message is simply uniform random coins. Against uniform adversaries, we can even just set the verifier's message to $000\cdots$, eliminating the verifier's message altogether.

c) The QROM: In classical cryptography, the Random Oracle Model (ROM) [8] models a hash function as a truly random function, and proves security in such a world. This model is very important for providing security justifications of many practical cryptosystems.

Boneh et al. [12] explain that, when moving to the quantum setting, one needs to model the random oracle as a *quantum random oracle model* (QROM). Many works (e.g. [17], [20], [28], [29], [31], [34], [37], [41]) have been devoted to lifting classical ROM results to the QROM. To date, most of the main classcal ROM results have successfully been lifted. This leads to a natural question: do all ROM results lift to the QROM?

Recently, Yamakawa and Zhandry [38], leveraging recent proofs of quantumness [14] in the random oracle, give a counter-example assuming the hardness of learning with errors (LWE). Their counter-examples were limited to highly interactive security models such as digital signatures and CCA-secure public key encryption.

By relying on LWE, [38] left open the possibility that *unconditional* ROM results may all lift to the QROM. Our proof of quantumness refutes this, showing that the ROM and QROM are separated even in the unconditional setting. Our results also give separations for many more objects, especially for objects like one-way functions and collision resistance which have essentially non-interactive security experiments.

C. Overview

Let Σ be an exponentially-sized alphabet, and $C \subseteq \Sigma^n$ be an error correcting code over Σ. Let $O : \Sigma \to \{0,1\}$ be a function. Consider the following function $f_C^O : C \to \{0,1\}^n$ derived from C, O:

$$f_C^O(c_1, \ldots, c_n) = (O(c_1), \ldots, O(c_n))$$

In other words, f_C^O simply applies O independently to each symbol in the input codeword. We will model O as a uniformly random function. Note that if f were applied to arbitrary words in Σ^n, then it would just be the parallel application of a function with one-bit outputs, which can be trivially inverted. By restricting the domain to only codewords, we show, under a suitable choice of code elaborated on below, that:

- f_C^O is unconditionally one-way against classical probabilistic algorithms making polynomially-many queries to O. It is even infeasible to find $c \in C$ such that $f_C^O(c) = 0^n$.
- There exists a quantum algorithm which, given any $y \in \{0,1\}^n$, samples statistically close to uniformly from the set of pre-images $c \in C$ such that $f_C^O(c) = y$.

From these properties, we immediately obtain a weak version of Theorem 1.4 which only considers classical one-wayness. We explain in the full version how to obtain the full Theorem 1.4. To prove quantumness, one simply produces $c \in C$ such that $f_C^O(c) = 0^n$, giving Theorem 1.2. Since one-way functions are in NP, this also immediately gives Corollary 1.3. We now explain how we justify these facts about f_C^O.

a) Classical hardness: Assume C satisfies the following properties: (1) the set of symbols obtained at each position are distinct, and (2) C is information-theoretically **list-recoverable**.[2] Here, we take list-recoverability to mean that, given polynomial-sized sets $S_i, i \in [n]$ of possible symbols for each position, there exist a sub-exponential sized (in n) list of codewords c such that $c_i \in S_i$ for all $i \in [n]$. The list size remains sub-exponential even if we include codewords such that $c_i \notin S_i$ for a few positions.

Property (1) can be obtained generically by replacing $\Sigma \mapsto [n] \times \Sigma$, where $(c_1, \dots, c_n) \mapsto ((1, c_1), \dots, (n, c_n))$. Property (2) is satisfied by folded Reed-Solomon codes, as shown by Guruswami and Rudra [21].

Assuming (1) and (2), we can show classical hardness. Fix an image y. We can assume without loss of generality that the adversary always evaluates $f_C^O(c)$ for any pre-image c it outputs. Suppose for our discussion here that all queries to O were made in parallel. Then any polynomial-sized set of queries corresponds to a collection of S_i. List recoverability means that there are at most $2^{n^c}, c < 1$ codewords consistent with the S_i. For each consistent codeword, the probability of being a pre-image of y is at most 2^{-n} over the choice of random oracle. Union-bounding over the list of consistent codewords shows that the probability that *any* consistent codeword is a pre-image is exponentially small. With some effort, we can show the above holds even for adaptively chosen queries.

Remark 2: Haitner et al. [23] construct a very similar hash function from list-recoverable codes. Their hash functions assumes a multi-bit O, but then XORs the results together, rather than concatenating them. They prove that their hash function is collision-resistant. Our proof of one-wayness is based on a similar idea to their proof of collision-resistance. Our novelty, and what does not appear to be possible for their construction, is the quantum pre-image finder, which we discuss next.

We note that we could, similar to [23], prove the collision resistance of f_C^O by choosing C to have an appropriate rate. However, our quantum pre-image finder constrains C to having a rate where we only know how to prove one-wayness. Proving Theorem 1.4 therefore requires a different construction, which we elaborate on in the full version.

b) Quantum easiness: Our algorithm can be seen as loosely inspired by Regev's quantum reduction between SIS and LWE [33]. Given an image y, our goal will be to create a uniform superposition over pre-images of y:

$$|\psi_y\rangle \propto \sum_{c \in C : f_C^O(c) = y} |c\rangle$$

We can view $|\psi_y\rangle$ as the point-wise product of two vectors:

$$|\phi\rangle \propto \sum_{c \in C} |c\rangle \ , \qquad \text{and} \qquad |\tau_y\rangle \propto \sum_{c \in \mathbf{\Sigma^n} : f_C^O(c) = y} |c\rangle$$

Obseve that $|\tau_y\rangle$ looks like $|\psi_y\rangle$, except that the domain is no longer constrained to codewords. Once we have the state $|\psi_y\rangle$, we can simply measure it to obtain a random pre-image of y. We will show how to construct $|\psi_y\rangle$ in reverse: we will show a sequence of reversible transformations that transform $|\psi_y\rangle$ into states we can readily construct. By applying these transformations in reverse we obtain $|\psi_y\rangle$. To do so, we will now impose that Σ is a vector space over $\mathbb{F}_q$ for some prime q, and that C is **linear** over $\mathbb{F}_q$. This means there is a dual code $C^\perp$, such that $c \cdot d = 0$ for all $c \in C, d \in C^\perp$.

We now consider the quantum Fourier transform QFT of $|\psi_y\rangle$. Write:

$$|\widehat{\phi}\rangle := \mathsf{QFT}|\phi\rangle \propto \sum_{c \in \Sigma^n} \alpha_c |c\rangle = \sum_{c \in C^\perp} |c\rangle$$
$$|\widehat{\tau}_y\rangle := \mathsf{QFT}|\tau_y\rangle \propto \sum_{c \in \Sigma^n} \beta_{y,c} |c\rangle$$

Above, we used the fact that the QFT of a uniform superposition over a linear space is just the uniform superposition over the dual space. Then, by the Convolution Theorem, the QFT of $|\psi_y\rangle$ is the convolution of $|\widehat{\phi}\rangle$ and $|\widehat{\tau}_y\rangle$:

$$|\widehat{\psi}_y\rangle := \mathsf{QFT}|\psi_y\rangle \propto \sum_{c,e \in \Sigma^n} \alpha_c \beta_{y,e} |c{+}e\rangle = \sum_{c \in C^\perp, e \in \Sigma^n} \beta_{y,e} |c{+}e\rangle$$

The next step is to decode c and e from $c + e$; assuming we had such a decoding, we can apply it to obtain the state proportional to

$$\sum_{c \in C^\perp, e \in \Sigma^n} \beta_{y,e} |c, e\rangle = |\widehat{\phi}\rangle |\widehat{\tau}_y\rangle$$

We can then construct $|\widehat{\phi}\rangle$ as the QFT of $|\phi\rangle$, which we can generate using the generator matrix for C. We will likewise construct $|\widehat{\tau}_y\rangle$ as the QFT of $|\tau_y\rangle$. To construct $|\tau_y\rangle$, we note that $|\tau_y\rangle$ is a product of n states that look like:

$$|\tau_{i,y_i}\rangle \propto \sum_{\sigma \in \Sigma : O(\sigma) = y_i} |\sigma\rangle$$

Since each y_i is just a single bit, we can construct such states by applying O to a uniform superposition of inputs, measuring the result, and starting over if we obtain the incorrect y_i.

It remains to show how to decode c, e from $c{+}e$. We observe that $|\widehat{\tau}_{i,y_i}\rangle$ has roughly half of its weight on 0, whereas the remaining half the weight is essentially uniform (though with complex phases) since O is a random function. This means we can think of e as a vector where each symbol is 0 with probability $1/2$, and random otherwise. In other words, $c + e$ is a noisy version of c following an analog of the binary symmetric channel generalized to larger alphabets. If the dual code $C^\perp$ were efficiently decodable under such noise, then can decode c (and hence e) from $c + e$.

Toward that end, we show that c is uniquely information-theoretically decodable (whp) provided the rate of $C^\perp$ is not too high. In our case where C is a folded Reed-Solomon code,

[2] List-recoverable codes have been used in cryptography in the contexts of domain extension of hash functions [11], [23], [30] and the Fiat-Shamir transform [25].

$C^{\perp}$ is essentially another Reed-Solomon code, and we can decode efficiently using **list-decoding** algorithms [22]. We can show that the list-decoding results in a unique codeword (whp) for the above described error distribution assuming C to have an appropriate rate.

There are a couple important caveats with the above. First is that, to use list-recoverability to prove one-wayness, we actually needed to augment C, which broke linearity. This is easily overcome by only applying the QFT to the linear part of C.

More importantly, and much more challenging, we can only decode $c + e$ as long as e has somewhat small Hamming weight. While such e occur with overwhelming probability, there will always be a negligible fraction of decoding errors. The problem is that the constant of proportionality in the Convolution Theorem is exponentially large, and therefore the negligible decoding errors from our procedure could end up being blown up and drowning out $|\widehat{\psi_y}\rangle$. This is not just an issue with our particular choice of decoding algorithm, as for large enough Hamming wieght decoding errors are guaranteed. What this means is that the map $|\widehat{\phi}\rangle|\widehat{\tau}_y\rangle \mapsto |\widehat{\psi_y}\rangle$ is not even unitary, and $|\widehat{\psi_y}\rangle$ is not even unit norm.

By exploiting the particular structure of our coding problem and the uniform randomness of the oracle O, we are able to resolve the above difficulties and show that our algorithm does, in fact, produce pre-images of y as desired.

c) Certifiable randomness.: We next explain that *any* efficient quantum algorithm for inverting f_C^O likely produces random inputs. After all, suppose there was an alternative quantum algorithm which inverted f_C^O, such that its output on any given y is deterministic. If we look at any single bit of the output, then Conjecture 1.1 would imply that this bit can be simulated by a polynomial-query classical algorithm. By applying Conjecture 1.1 to every bit of output, we thus obtain a classical query algorithm for inverting f_C^O, which we know is impossible.

This immediately gives us a proof of entropy: the prover generates a pre-image c of an arbitrary y (even $y = 0^n$), and the verifier checks that $f_C^O(c) = y$. If the check passes, the verifier can be convinced that c was not deterministically generated, and therefore has some randomness. By using the fact that f_C^O is one-way even against sub-exponential-query algorithms, we can show that the min-entropy must be polynomial.

Once we have a string with min-entropy, we can easily get uniform random bits by having the verifier extract using a private random seed.

d) Extension to non-uniform adversaries: Note that the above results all considered fixing an adversary first, and then sampling a random oracle. A standard complexity theoretic argument shows that, in the case of uniform adversaries, we can switch the order of quantifiers, and choose the random oracle first and then the adversary.

For non-uniform adversaries, we have to work harder, and direct analogs of the results above may in fact be impossible: for example, a non-uniform adversary (chosen after the random oracle) could have a valid proof of quantumness hardcoded.

For proofs of quantumness, we can leverage the "salting defeats preprocessing" result of [19] to readily get a two-message public coin proof of quantumness against non-uniform attackers. For certifiable entropy/randomness, this also works, except the known bounds would end up requiring the verifiers message to be longer than the extracted string. This is a consequence of leveraging the sub-exponential one-wayness of f_C^O to obtain polynomially-many random bits. Since the verifier's message must be uniform, this would somewhat limit the point of a proof of randomness. We show via careful arguments how to overcome this limitation, obtaining two message proofs of randomness where the verifier's message remains small.

e) Extension to worst-case completeness: Our analysis of the quantum algorithm seems to inherently rely on the oracle being uniformly random. We show how to tweak our scheme so that correctness holds for *any* oracle. The idea is to set $O = O' \oplus P$, where O' is the oracle, and where P is a k-wise independent function for some sufficiently large k. The point is that P is supplied as part of the problem solution, and so is chosen by the quantum algorithm. This makes O k-wise independent regardless of O', which is sufficient for the analysis.

Of course, introducing P makes the classical problem easier, since now the classical adversary has some flexibility in constructing O. We handle this by asking the adversary to find many solutions relative to different O', but the same P. This amplifies hardness, after which we can union-bound over all possible P and still maintain classical hardness. The quantum algorithm, on the other hand, can solve each of the individual instances with high probability, so it can easily solve all instances.

This gives the following conceptual implication: we obtain an NP relation where the oracle is the (exponentially-sized) instance, and the corresponding NP search problem is to find a polynomial-sized witness satisfying the relation. Computing the relation only requires polynomially-many queries. Our relation that is hard for BPP machines but easy for BQP machines. Note that this is a slightly different setting than our NP relation above, where there instances and witnesses were both polynomial-length strings, and the oracle is used to determine which witnesses are valid for a given instance.

D. Acknowledgements

We thank Scott Aaronson for helpful suggestions, including the conceptual implication of worst-case completeness. We thank anonymous reviewers of FOCS 2022 for their helpful comments. Mark Zhandry is supported in part by an NSF CAREER award.

References

[1] Scott Aaronson and Andris Ambainis. The need for structure in quantum speedups. *Theory Comput.*, 10:133–166, 2014.

[2] Scott Aaronson and Alex Arkhipov. The computational complexity of linear optics. In Lance Fortnow and Salil P. Vadhan, editors, *43rd ACM STOC*, pages 333–342. ACM Press, June 2011.

[3] Scott Aaronson and Yaoyun Shi. Quantum lower bounds for the collision and the element distinctness problems. *J. ACM*, 51(4):595–605, 2004.

[4] Leonard Adleman. A subexponential algorithm for the discrete logarithm problem with applications to cryptography. In *20th Annual Symposium on Foundations of Computer Science (sfcs 1979)*, pages 55–60, 1979.

[5] Ryan Amos, Marios Georgiou, Aggelos Kiayias, and Mark Zhandry. One-shot signatures and applications to hybrid quantum/classical authentication. In Konstantin Makarychev, Yury Makarychev, Madhur Tulsiani, Gautam Kamath, and Julia Chuzhoy, editors, *52nd ACM STOC*, pages 255–268. ACM Press, June 2020.

[6] László Babai, Robert Beals, and Ákos Seress. Polynomial-time theory of matrix groups. In Michael Mitzenmacher, editor, *41st ACM STOC*, pages 55–64. ACM Press, May / June 2009.

[7] Robert Beals, Harry Buhrman, Richard Cleve, Michele Mosca, and Ronald de Wolf. Quantum lower bounds by polynomials. In *39th FOCS*, pages 352–361. IEEE Computer Society Press, November 1998.

[8] Mihir Bellare and Phillip Rogaway. Random oracles are practical: A paradigm for designing efficient protocols. In Dorothy E. Denning, Raymond Pyle, Ravi Ganesan, Ravi S. Sandhu, and Victoria Ashby, editors, *ACM CCS 93*, pages 62–73. ACM Press, November 1993.

[9] Charles H. Bennett, Ethan Bernstein, Gilles Brassard, and Umesh V. Vazirani. Strengths and weaknesses of quantum computing. *SIAM J. Comput.*, 26(5):1510–1523, 1997.

[10] Ethan Bernstein and Umesh V. Vazirani. Quantum complexity theory. In *25th ACM STOC*, pages 11–20. ACM Press, May 1993.

[11] Nir Bitansky, Yael Tauman Kalai, and Omer Paneth. Multi-collision resistance: a paradigm for keyless hash functions. In Ilias Diakonikolas, David Kempe, and Monika Henzinger, editors, *50th ACM STOC*, pages 671–684. ACM Press, June 2018.

[12] Dan Boneh, Özgür Dagdelen, Marc Fischlin, Anja Lehmann, Christian Schaffner, and Mark Zhandry. Random oracles in a quantum world. In Dong Hoon Lee and Xiaoyun Wang, editors, *ASIACRYPT 2011*, volume 7073 of *LNCS*, pages 41–69. Springer, Heidelberg, December 2011.

[13] Zvika Brakerski, Paul Christiano, Urmila Mahadev, Umesh V. Vazirani, and Thomas Vidick. A cryptographic test of quantumness and certifiable randomness from a single quantum device. In Mikkel Thorup, editor, *59th FOCS*, pages 320–331. IEEE Computer Society Press, October 2018.

[14] Zvika Brakerski, Venkata Koppula, Umesh V. Vazirani, and Thomas Vidick. Simpler proofs of quantumness. In *TQC 2020*, volume 158 of *LIPIcs*, pages 8:1–8:14, 2020.

[15] Michael J. Bremner, Richard Jozsa, and Dan J. Shepherd. Classical simulation of commuting quantum computations implies collapse of the polynomial hierarchy. *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences*, 467:459 – 472, 2010.

[16] Ran Canetti, Oded Goldreich, and Shai Halevi. The random oracle methodology, revisited (preliminary version). In *30th ACM STOC*, pages 209–218. ACM Press, May 1998.

[17] Alessandro Chiesa, Peter Manohar, and Nicholas Spooner. Succinct arguments in the quantum random oracle model. In Dennis Hofheinz and Alon Rosen, editors, *TCC 2019, Part II*, volume 11892 of *LNCS*, pages 1–29. Springer, Heidelberg, December 2019.

[18] Andrew M. Childs, Richard Cleve, Enrico Deotto, Edward Farhi, Sam Gutmann, and Daniel A. Spielman. Exponential algorithmic speedup by a quantum walk. In *35th ACM STOC*, pages 59–68. ACM Press, June 2003.

[19] Kai-Min Chung, Siyao Guo, Qipeng Liu, and Luowen Qian. Tight quantum time-space tradeoffs for function inversion. In *61st FOCS*, pages 673–684. IEEE Computer Society Press, November 2020.

[20] Jelle Don, Serge Fehr, Christian Majenz, and Christian Schaffner. Security of the Fiat-Shamir transformation in the quantum random-oracle model. In Alexandra Boldyreva and Daniele Micciancio, editors, *CRYPTO 2019, Part II*, volume 11693 of *LNCS*, pages 356–383. Springer, Heidelberg, August 2019.

[21] Venkatesan Guruswami and Atri Rudra. Explicit codes achieving list decoding capacity: Error-correction with optimal redundancy. *IEEE Trans. Inf. Theory*, 54(1):135–150, 2008.

[22] Venkatesan Guruswami and Madhu Sudan. Improved decoding of reed-solomon and algebraic-geometry codes. *IEEE Trans. Inf. Theory*, 45(6):1757–1767, 1999.

[23] Iftach Haitner, Yuval Ishai, Eran Omri, and Ronen Shaltiel. Parallel hashing via list recoverability. In Rosario Gennaro and Matthew J. B. Robshaw, editors, *CRYPTO 2015, Part II*, volume 9216 of *LNCS*, pages 173–190. Springer, Heidelberg, August 2015.

[24] Sean Hallgren. Polynomial-time quantum algorithms for Pell's equation and the principal ideal problem. In *34th ACM STOC*, pages 653–658. ACM Press, May 2002.

[25] Justin Holmgren, Alex Lombardi, and Ron D. Rothblum. Fiat-shamir via list-recoverable codes (or: parallel repetition of GMW is not zero-knowledge). In Samir Khuller and Virginia Vassilevska Williams, editors, *STOC '21: 53rd Annual ACM SIGACT Symposium on Theory of Computing, Virtual Event, Italy, June 21-25, 2021*, pages 750–760. ACM, 2021.

[26] R. Impagliazzo. A personal view of average-case complexity. In *Proceedings of Structure in Complexity Theory. Tenth Annual IEEE Conference*, pages 134–147, 1995.

[27] Russell Impagliazzo and Steven Rudich. Limits on the provable consequences of one-way permutations. In *21st ACM STOC*, pages 44–61. ACM Press, May 1989.

[28] Shuichi Katsumata, Shota Yamada, and Takashi Yamakawa. Tighter security proofs for GPV-IBE in the quantum random oracle model. In Thomas Peyrin and Steven Galbraith, editors, *ASIACRYPT 2018, Part II*, volume 11273 of *LNCS*, pages 253–282. Springer, Heidelberg, December 2018.

[29] Eike Kiltz, Vadim Lyubashevsky, and Christian Schaffner. A concrete treatment of Fiat-Shamir signatures in the quantum random-oracle model. In Jesper Buus Nielsen and Vincent Rijmen, editors, *EUROCRYPT 2018, Part III*, volume 10822 of *LNCS*, pages 552–586. Springer, Heidelberg, April / May 2018.

[30] Ilan Komargodski, Moni Naor, and Eylon Yogev. Collision resistant hashing for paranoids: Dealing with multiple collisions. In Jesper Buus Nielsen and Vincent Rijmen, editors, *EUROCRYPT 2018, Part II*, volume 10821 of *LNCS*, pages 162–194. Springer, Heidelberg, April / May 2018.

[31] Qipeng Liu and Mark Zhandry. Revisiting post-quantum Fiat-Shamir. In Alexandra Boldyreva and Daniele Micciancio, editors, *CRYPTO 2019, Part II*, volume 11693 of *LNCS*, pages 326–355. Springer, Heidelberg, August 2019.

[32] Sahadeo Padhye. A Public Key Cryptosystem Based On Pell Equation. Cryptology ePrint Archive, Report 2006/191, 2006. https://eprint.iacr.org/2006/191.

[33] Oded Regev. On lattices, learning with errors, random linear codes, and cryptography. In Harold N. Gabow and Ronald Fagin, editors, *37th ACM STOC*, pages 84–93. ACM Press, May 2005.

[34] Tsunekazu Saito, Keita Xagawa, and Takashi Yamakawa. Tightly-secure key-encapsulation mechanism in the quantum random oracle model. In Jesper Buus Nielsen and Vincent Rijmen, editors, *EUROCRYPT 2018, Part III*, volume 10822 of *LNCS*, pages 520–551. Springer, Heidelberg, April / May 2018.

[35] Peter W. Shor. Algorithms for quantum computation: Discrete logarithms and factoring. In *35th FOCS*, pages 124–134. IEEE Computer Society Press, November 1994.

[36] Daniel R. Simon. On the power of quantum computation. *SIAM J. Comput.*, 26(5):1474–1483, oct 1997.

[37] Ehsan Ebrahimi Targhi and Dominique Unruh. Post-quantum security of the Fujisaki-Okamoto and OAEP transforms. In Martin Hirt and Adam D. Smith, editors, *TCC 2016-B, Part II*, volume 9986 of *LNCS*, pages 192–216. Springer, Heidelberg, October / November 2016.

[38] Takashi Yamakawa and Mark Zhandry. Classical vs quantum random oracles. In Anne Canteaut and François-Xavier Standaert, editors, *EUROCRYPT 2021, Part II*, volume 12697 of *LNCS*, pages 568–597. Springer, Heidelberg, October 2021.

[39] Takashi Yamakawa and Mark Zhandry. Verifiable quantum advantage without structure. *arXiv*, 2204.02063, 2022.

[40] Henry Yuen. A quantum lower bound for distinguishing random functions from random permutations. *Quantum Info. Comput.*, 14(13–14):1089–1097, oct 2014.

[41] Mark Zhandry. Secure identity-based encryption in the quantum random oracle model. In Reihaneh Safavi-Naini and Ran Canetti, editors, *CRYPTO 2012*, volume 7417 of *LNCS*, pages 758–775. Springer, Heidelberg, August 2012.

[42] Mark Zhandry. A note on the quantum collision and set equality problems. *Quantum Info. Comput.*, 15(7–8):557–567, may 2015.