Quantum Cryptography in Algorithmica

William Kretschmer
University of Texas at Austin
Austin, TX, USA
kretsch@cs.utexas.edu

Luowen Qian
Boston University
Boston, MA, USA
luowenq@bu.edu

Makrand Sinha
Simons Institute and University of California at Berkeley
Berkeley, CA, USA
makrand@berkeley.edu

Avishay Tal
University of California at Berkeley
Berkeley, CA, USA
atal@berkeley.edu

ABSTRACT

We construct a classical oracle relative to which P = NP yet single-copy secure pseudorandom quantum states exist. In the language of Impagliazzo's five worlds, this is a construction of pseudorandom states in "Algorithmica," and hence shows that in a black-box setting, quantum cryptography based on pseudorandom states is possible even if one-way functions do not exist. As a consequence, we demonstrate that there exists a property of a cryptographic hash function that simultaneously (1) suffices to construct pseudorandom states, (2) holds for a random oracle, and (3) is independent of P vs. NP in the black-box setting. We also introduce a conjecture that would generalize our results to multi-copy secure pseudorandom states.

We build on the recent construction by Aaronson, Ingram, and Kretschmer (CCC 2022) of an oracle relative to which P = NP but BQP ≠ QCMA, based on hardness of the OR ∘ Forrelation problem. Our proof also introduces a new discretely-defined variant of the Forrelation distribution, for which we prove pseudorandomness against AC^0 circuits. This variant may be of independent interest.

CCS CONCEPTS

• **Theory of computation** → **Quantum complexity theory**; **Cryptographic primitives**.

KEYWORDS

pseudorandom quantum states, oracles, Forrelation

ACM Reference Format:
William Kretschmer, Luowen Qian, Makrand Sinha, and Avishay Tal. 2023. Quantum Cryptography in Algorithmica. In *Proceedings of the 55th Annual ACM Symposium on Theory of Computing (STOC '23), June 20–23, 2023, Orlando, FL, USA.* ACM, New York, NY, USA, 14 pages. https://doi.org/10.1145/3564246.3585225

1 INTRODUCTION

One-way functions (OWFs) have played a central role in computational cryptography since its birth [19]. On the one hand, the existence of one-way functions would separate P from NP in an average case sense; on the other, their existence has proven to be necessary for almost all classical cryptographic tasks [22, 25]. This reveals a fundamental tension in the classical world: we cannot expect to solve all problems in NP extremely well but also have useful cryptography at the same time. In the language of Impagliazzo's five worlds [24], there is no hope of constructing much useful cryptography in "Algorithmica," a world in which P = NP. Rather, the "Minicrypt" world, where one-way functions exist, is generally considered to capture the bare minimum of cryptography, because one-way functions are implied by almost all other cryptographic primitives. At the same time, even just assuming the existence of one-way functions, a wide range of other cryptographic primitives are possible, including pseudorandom generators, pseudorandom functions, symmetric-key encryption schemes, and digital signatures.

A growing body of work has shown that P ≠ NP may not be necessary to construct various useful *quantum* cryptography. Quantum key distribution (QKD) [12] is arguably the earliest demonstration of this idea: it enables two parties to securely exchange a secret key, assuming only that they share an untrusted quantum channel and an authenticated classical channel. The security proof of QKD is information-theoretic, and relies on no computational assumptions [38]. By contrast, classical key exchange lies in Impagliazzo's "Cryptomania" world, meaning that it relies on computational assumptions that appear to be even stronger than the existence of one-way functions [26].

Unfortunately, much like classically, many interesting cryptographic tasks still remain impossible for information-theoretically secure quantum protocols [31, 32], and thus require some assumptions on the model, e.g. a computational bound on the adversary. More recent works have demonstrated the possibility of building computationally secure quantum cryptography based on computational assumptions that are plausibly weaker than the existence of one-way functions. A prominent example is the construction of cryptography based on *pseudorandom quantum states* (PRSs), introduced by Ji, Liu, and Song [28]. Informally, an ensemble of quantum states is pseudorandom if the states can be efficiently generated, and if no polynomial-time quantum adversary can distinguish a random state drawn from the ensemble from a Haar-random state. PRSs can be defined with either single- [33] or multi-copy security [28], depending on whether the adversary is allowed a single copy, or any polynomial number of copies of the unknown state, respectively. [28] also showed that the existence of quantum-secure

This work is licensed under a Creative Commons Attribution 4.0 International License.

STOC '23, June 20–23, 2023, Orlando, FL, USA
© 2023 Copyright held by the owner/author(s).
ACM ISBN 978-1-4503-9913-5/23/06.
https://doi.org/10.1145/3564246.3585225

one-way functions is sufficient to construct multi-copy pseudorandom states, although the converse is not known. Hence, assuming the existence of PRSs is no stronger than assuming the existence of quantum-secure OWFs.

Despite appearing weaker than one-way functions, pseudorandom states are surprisingly powerful, and suffice to construct a wide variety of cryptography. Even with only single-copy secure pseudorandom states, we can already construct commitment schemes and some form of non-trivial one-time signatures [6, 33], the former of which are equivalent to secure multiparty computation and computational zero knowledge proofs [6, 10, 14, 23, 41, 42]. From the more standard notion of multi-copy security, we can also achieve private-key query-secure quantum money [28] and non-trivial one-time encryption [6].

Nevertheless, the evidence to suggest that PRSs are actually a weaker assumption than OWFs is extremely limited. Indeed, other than the basic intuition that there is no obvious way to construct OWFs out of PRSs, the only provable separation between these primitives is the result of Kretschmer [29], who constructed an oracle relative to which $\mathsf{BQP} = \mathsf{QMA}$ and yet pseudorandom states exist. This shows that, in the black box setting, quantum-secure OWFs are not implied by PRSs, because quantum algorithms can efficiently invert any classical function if $\mathsf{NP} \subseteq \mathsf{BQP}$.

However, Kretschmer's result comes with the major caveat that the oracle achieving this separation is quantum, meaning that the oracle is some arbitrary unitary transformation that only a quantum algorithm can query. Hence, perhaps it is unsurprising that this quantum oracle lets us achieve quantum cryptography (PRSs) but not classical cryptography (OWFs)—there is no meaningful way to define classical queries to a unitary oracle! In other words, even though $\mathsf{BQP} = \mathsf{QMA}$ implies that quantum-secure OWFs do not exist, the statement "$\mathsf{BQP}^{\mathcal{O}} = \mathsf{QMA}^{\mathcal{O}}$ implies that quantum-secure OWFs do not exist relative to $\mathcal{O}$" is less meaningful when $\mathcal{O}$ is a quantum oracle, because any construction of OWFs cannot depend on $\mathcal{O}$. Furthermore, quantum oracle separations are conceptually weaker than classical oracle separations, because they can produce consequences that fail relative to all classical oracles. Indeed, Aaronson [1] observed that that there exist inclusions of complexity classes that trivially hold relative to all classical oracles (e.g. $\mathsf{BQP} \subseteq \mathsf{ZQEXP}$), but that can be separated relative to certain quantum oracles. Thus, for all we know, the result of [29] could be merely an artifact of the quantumness of the oracle, and there could be a classical relativizing proof that PRSs imply OWFs!

Another conceptual limitation of Kretschmer's separation is that the pseudorandom state construction involves directly generating the state using a Haar-random oracle. However, unlike the classical random oracle model, we very much do not know how to even heuristically instantiate such a Haar random oracle in the real world, other than via ad-hoc approaches such as random quantum circuits. Therefore, [29] offers little insight into plausible constructions of PRSs without OWFs in a non-oracular setting.

1.1 Our Results

In this work, we overcome these limitations of quantum oracles by constructing a separation of PRSs and OWFs relative to a *classical* oracle. Our main result is the following:

Theorem 1 (Proposition 19 and Theorem 22, informal). *There exists a classical oracle relative to which* $\mathsf{P} = \mathsf{NP}$ *and single-copy pseudorandom state ensembles exist.*

Theorem 1 can thus be taken as a relativized construction of PRSs in Impagliazzo's "Algorithmica" [24]. Since OWFs do not exist if $\mathsf{P} = \mathsf{NP}$, our result shows that OWFs are not necessary to construct PRSs in the classical black box setting, answering a question of Ji, Liu, and Song [28]. Note that our result is formally incomparable to the result of [29]: on the one hand, our separation is conceptually stronger, because our oracle is classical, rather than quantum. On the other hand, we achieve single-copy PRSs, whereas [29] achieves multi-copy PRSs.[1]

We briefly describe the oracle and the associated construction of pseudorandom states. Our oracle $\mathcal{O} = (A, B)$ consists of two parts: a random oracle A, and an oracle B that is defined recursively to answer all possible NP predicates of either A or B. Note that similar oracles were used in [4, 11], and that $\mathsf{P}^{\mathcal{O}} = \mathsf{NP}^{\mathcal{O}}$ essentially by definition. Furthermore, B is constructed so that queries to B are roughly equivalent in power to queries to PH^{A}. So, our result can also be interpreted as showing that in the random oracle model, there exist PRSs that are secure against $\mathsf{BQP}^{\mathsf{PH}}$ adversaries.

Our pseudorandom state ensemble is defined using what we call *t-Forrelation states*, which are n-qubit states $|\Phi_F\rangle$ of the form:

$$|\Phi_F\rangle = U_{f^t} \cdot H \cdot U_{f^{t-1}} \cdot H \cdots H \cdot U_{f^1} |+^n\rangle ,$$

where $F = (f^1, f^2, \ldots, f^t)$ is a t-tuple of n-bit Boolean functions $f^i : \{\pm 1\}^n \to \{\pm 1\}$, U_{f^i} is the phase oracle corresponding to f^i, and H is the n-qubit Hadamard transform. t-Forrelation states are a generalization of so-called "phase states", which correspond to the case $t = 1$ [7, 15, 27, 28]. t-Forrelation states are so called because of their connection to the t-fold Forrelation problem [3, 9]. We take the states in our PRS ensemble to be a set of randomly-chosen 2-Forrelation states with F specified by the random oracle. That is, we view A as defining a pair of random functions (f_k, g_k) for each key $k \in \{0, 1\}^{\kappa}$ (where κ is the security parameter), and we take the pseudorandom state keyed by k to be:

$$|\varphi_k\rangle := |\Phi_{(f_k, g_k)}\rangle = U_{g_k} \cdot H \cdot U_{f_k} |+^n\rangle .$$

Here, we can pick n to be any polynomial in κ, although since we only achieve single-copy security, it is only non-trivial if $n > \kappa$, as also observed in prior works [28, 33].

We remark that similar "Hadamard/phase cocktails"[2] have appeared elsewhere in quantum information [5, 34, 35], including also in Ji, Liu, and Song's candidate construction of *pseudorandom unitaries* [28, Section 6.2], which are a strengthening of pseudorandom states.

1.2 Proof Overview

Our proof builds on the recent construction by Aaronson, Ingram, and Kretschmer [4] of an oracle relative to which $\mathsf{P} = \mathsf{NP}$ and $\mathsf{BQP} \neq \mathsf{QCMA}$. Their proof of this separation involves showing that an oracle distinguishing problem called $\mathsf{OR} \circ$ Forrelation is not in $\mathsf{BQP}^{\mathsf{PH}}$. Informally, in the $\mathsf{OR} \circ$ Forrelation problem, we

[1] Another technical difference is that we construct a world where $\mathsf{P} = \mathsf{NP}$, whereas [29] constructs a world where $\mathsf{BQP} = \mathsf{QMA}$, and these are also incomparable [4, Theorems 4 and 9].

[2] We credit Scott Aaronson (personal communication) for suggesting this term.

are given an exponentially-long list $\{(f_k, g_k)\}_{k\in\{0,1\}^\kappa}$ of pairs of n-bit Boolean functions, and we must distinguish between:

(YES) There exists a single $k \in \{0,1\}^\kappa$ such that the functions f_k and g_k are *Forrelated*, meaning that $\left|\langle +^n|\Phi_{(f_k,g_k)}\rangle\right| \ge \varepsilon$ for some $\varepsilon \ge 1/\mathrm{poly}(\kappa)$,[3] or

(NO) For every $k \in \{0,1\}^\kappa$, f_k and g_k are uniformly random, in which case $\left|\langle +^n|\Phi_{(f_k,g_k)}\rangle\right|$ is negligible for every k, with high probability.

Our main insight is that viewing the Forrelation problem as a state overlap problem allows us to relate OR ∘ Forrelation to the 2-Forrelation state PRS distinguishing task. In fact, we will formally relate these problems via a reduction: we show that any $\mathsf{BQP}^{\mathsf{PH}}$ adversary that distinguishes the PRS ensemble from random would give rise to a $\mathsf{BQP}^{\mathsf{PH}}$ algorithm for solving OR ∘ Forrelation. Given an instance $\{(f'_k, g'_k)\}_{k\in\{0,1\}^\kappa}$ of OR ∘ Forrelation, we choose a uniformly random function $h : \{\pm 1\}^n \to \{\pm 1\}$. Then, the PRS adversary is given the input state $|\Phi_h\rangle = U_h|+^n\rangle$, and it is allowed queries to the oracle $\{(f_k, g_k)\}_{k\in\{0,1\}^\kappa}$ defined by $(f_k, g_k) := (f'_k, g'_k \cdot h)$.

Observe that if $\{(f'_k, g'_k)\}_{k\in\{0,1\}^\kappa}$ is a YES instance of OR ∘ Forrelation, then there exists some k such that

$$\begin{aligned}|\langle\Phi_h|\varphi_k\rangle| = \left|\langle\Phi_h|\Phi_{(f_k,g_k)}\rangle\right| &= \left|\langle +^n|U_hU_h|\Phi_{(f'_k,g'_k)}\rangle\right| \\ &= \left|\langle +^n|\Phi_{(f'_k,g'_k)}\rangle\right| \ge \varepsilon.\end{aligned}$$

In other words, the state $|\Phi_h\rangle$ given to the adversary has some non-negligible overlap with a state $|\varphi_k\rangle$ drawn from the PRS ensemble. On the other hand, if $\{(f'_k, g'_k)\}_{k\in\{0,1\}^\kappa}$ is a NO instance of OR ∘ Forrelation, then $|\Phi_h\rangle$ is far from *all* states in the PRS ensemble, with high probability.

Though this reduction does not perfectly map OR∘Forrelation onto the security challenge of the PRS, we nevertheless show that our reduction is quantitatively "close enough," at least in the single-copy case. Specifically, we prove that the distinguishing advantage of the adversary between the YES and NO instances of OR ∘ Forrelation is polynomially related to its distinguishing advantage between the pseudorandom and Haar-random security challenges of the PRS. This polynomial dependence scales with the parameter ε.

Proving this dependence requires a delicate analysis based on a carefully constructed distributional version of the OR∘Forrelation problem. Along the way, we introduce a new variant of the *Forrelation distribution* [2, 37]—i.e., a distribution over pairs of Boolean functions (f, g) that are Forrelated with high probability. This distribution is defined as follows: first, we choose f to be uniformly random. Then, independently for each $x \in \{\pm 1\}^n$, we sample $g(x) \in \{\pm 1\}$ with bias proportional to the Fourier coefficient $\hat{f}(x)$, modulo a rounding step in case $\left|\hat{f}(x)\right|$ is too large. Our Forrelation distribution has the advantage that it is discretely defined, in contrast to the distributions given by Aaronson [2] or Raz and Tal [37], which involve multivariate Gaussians. Thus, in some applications, it may be easier to analyze. We prove that our Forrelation distribution is pseudorandom against AC^0 using techniques similar to [16] based on polarizing random walks.

1.3 Cryptographic Implications

From a practical standpoint, a non-oracular version of our PRS construction can be instantiated by choosing $\{(f_k, g_k)\}_{k\in\{0,1\}^\kappa}$ according to a cryptographic hash function, or from a pseudorandom function (PRF) ensemble keyed by k. This generalizes the construction of PRSs using phase states with PRF-chosen phases [15, 28]. Theorem 1 then suggests that our construction based on Forrelation states is secure against a much broader class of attacks than phase state constructions: whereas PRF-based phase states can be distinguished from Haar-random by a $\mathsf{BQP}^{\mathsf{NP}}$ adversary [29], our construction remains secure even against the stronger class of $\mathsf{BQP}^{\mathsf{PH}}$ adversaries.[4]

Alternatively, the proof of Theorem 1 can be understood as showing that there exists a cryptographically useful property of hash functions that is plausibly independent of the P vs. NP problem.Informally, this property is the following hardness assumption of a hash function F:

Property 2 (Property 33, informal)**.** *Let $F = \{(f_k, g_k)\}_{k\in\{0,1\}^\kappa}$ be a list of pairs of efficiently computable functions. Given quantum query access to an auxiliary function h, it is hard for an adversary to distinguish whether:*

(i) There exists a k such that f_k is Forrelated with $g_k \cdot h$, or
(ii) h is uniformly random.

In other words, Property 2 posits the hardness of detecting Forrelations between two parts (f_k, g_k) of F relative to a "shift" specified by h. Note that although this is a QCMA-style problem in the sense that the shifted Forrelation is efficiently verifiable given the classical secret k, it is actually unclear whether it could be broken if BQP = QCMA. This is because in this problem, an oracle of h is given instead of (some succinct representation of) its code.

The key step in our proof involves reducing the security of the pseudorandom state ensemble to this problem, while also showing that a version of Property 2 holds for the oracle $\mathcal{O}$ that we construct. As a result, we conclude that this property is simultaneously:

(a) Powerful enough to construct various useful quantum cryptographic schemes, including commitments, zero knowledge, one-time signatures, etc., because it suffices to construct pseudorandom states,
(b) Plausibly true for existing hash functions like SHA-3, because it holds for a random oracle, and
(c) Independent of the existence of one-way functions in the black-box setting (and, indeed, even independent of P vs. NP).

Prior to this work, we could only find properties that achieve any two of these three: the existence of one-way functions satisfies (a) [6, 28, 33] and (b) [26]; the quantum oracle constructed in

[3] The Forrelation between f and g is usually defined directly in terms of the correlation between $\hat{f}$ and g [2, 3], but our definition is equivalent. Indeed, $\left|\langle +^n|\Phi_{(f_k,g_k)}\rangle\right|^2$ is exactly the acceptance probability of the 2-query quantum algorithm for estimating the Forrelation between f and g [2, Section 3.2].

[4] Strictly speaking, the $\mathsf{BQP}^{\mathsf{NP}}$ attack on phase states requires a polynomial number of copies of the state, while our proof of security against $\mathsf{BQP}^{\mathsf{PH}}$ adversaries only applies in the singe-copy case. However, we conjecture that the t-Forrelation construction remains secure even in the multi-copy case, at least for some sufficiently large t. We outline a plausible path towards proving this in Section 1.4.

[29] achieves (a) and (c); and the trivial property satisfies (b) and (c) [8]. Most notably, unlike the result of [29], we do not require a practical realization of Haar-random oracles in order to build OWF-independent pseudorandom states. For further discussion, see Section 6.

1.4 Open Problems

Perhaps the most natural question left for future work is whether our result can be strengthened to an oracle relative to which P = NP and *multi-copy* PRSs exist. It seems reasonable to conjecture that t-Forrelation states should remain secure against $\mathsf{BQP}^{\mathsf{PH}}$ adversaries even in the multi-copy setting. However, our strategy based on reduction from the OR ∘ Forrelation problem might not suffice to prove this, at least in the $t = 2$ case. For example, if we try to naively extend our reduction to the the multi-copy case, then the adversary receives $|\Phi_h\rangle^{\otimes T}$ for some arbitrary polynomially-bounded T, rather than a single copy of $|\Phi_h\rangle$. And though $|\langle\Phi_h|\varphi_k\rangle| \geq \varepsilon$ may be non-negligible, $\left|\langle\Phi_h|^{\otimes T} |\varphi_k\rangle^{\otimes T}\right| = |\langle\Phi_h|\varphi_k\rangle|^T \geq \varepsilon^T$ could in general be negligible if T is large enough. As a result, the distinguishing advantage of the adversary between the YES and NO instances of OR ∘ Forrelation may no longer be polynomially related to its distinguishing advantage between the pseudorandom and Haar-random security challenges of the PRS.

Nevertheless, we show that there is some hope in extending our approach to the multi-copy setting. Assuming a strong conjecture about t-Forrelation states for some $t = \mathrm{poly}(n)$, we conditionally prove, via techniques similar to the single-copy case, the $\mathsf{BQP}^{\mathsf{PH}}$-security of t-Forrelation states. We give a formal statement of the conjecture in Section 7. Roughly speaking, the conjecture posits that for any given t-Forrelation state $|\Phi_G\rangle$, it is hard for AC^0 circuits of $2^{\mathrm{poly}(n)}$ size to distinguish a t-tuple of functions $F = (f^1, f^2, \ldots, f^t)$ chosen uniformly at random, from an F chosen subject to the constraint that $|\langle\Phi_F|\Phi_G\rangle|$ is negligibly close to 1. We expect that choosing t to be a large polynomial would be necessary for this conjecture to hold, as otherwise there might be very few Fs for which $|\langle\Phi_F|\Phi_G\rangle|$ is close to 1.

Independent of the issue of single-copy versus multi-copy security, can our oracle be strengthened in other ways? For example, can one build an oracle relative to which P = NP and *pseudorandom unitaries* (PRUs) [28] exist?[5] Alternatively, could one give an oracle relative to which P = QMA and PRSs exist? One challenge is that if multi-copy PRSs exist, then P ≠ PP, as observed by Kretschmer [29]. Thus, any oracle relative to which P = QMA and multi-copy PRSs exist must also be an oracle relative to which P = QMA ≠ PP, which is still an open problem [4]. However, it is not clear whether a similar barrier exists in the single-copy case. Indeed, another important direction for future work is to better understand what computational assumptions are required to construct single-copy PRSs, and also seemingly weaker quantum cryptographic primitives such as EFI pairs [14]. In particular, does the existence of single-copy PRSs imply P ≠ PSPACE?

Finally, we seek to better understand whether there is any sense in which Forrelation, or an oracle problem like it, is necessary for our construction. Could the binary phase construction of pseudorandom states [15, 28] in fact also be secure against $\mathsf{BQP}^{\mathsf{PH}}$ adversaries in the single-copy setting? (Recall that in the multi-copy setting, it is insecure against $\mathsf{BQP}^{\mathsf{PH}}$, and indeed $\mathsf{BQP}^{\mathsf{NP}}$, as shown by Kretschmer [29].)

2 PRELIMINARIES

2.1 Basic Notation

We denote by $[n]$ the set $\{1, 2, \ldots, n\}$. If $\mathcal{D}$ is a probability distribution, then $x \sim \mathcal{D}$ means that x is a random variable sampled from $\mathcal{D}$. If S is a finite set, then $x \sim S$ means that x is a uniformly random element of S. We let $\mathbb{1}\{P\}$ be the indicator function that evaluates to 1 if the predicate P is true, and 0 otherwise.

We use $\log(x)$ to denote the base-2 logarithm of x, while $\ln(x)$ is the base-e logarithm. For two n-dimensional vectors v, w, $v \odot w$ denotes their Hadamard (entrywise) product, that is $(v \odot w)_i := v_i w_i$. For $a > 0$, we let $\mathrm{trnc}_a : \mathbb{R} \to [-a, a]$ be the function that truncates to the interval $[-a, a]$, i.e. $\mathrm{trnc}_a(z) := \min\{a, \max\{-a, z\}\}$. We may also omit the subscript a if $a = 1$. Observe that $\mathrm{trnc}_a(z) = a \cdot \mathrm{trnc}(z/a)$.

We use $\mathrm{TVD}(X, Y)$ to denote the total variation distance between probability distributions, and $\mathrm{TD}(\rho, \sigma)$ to denote the trace distance between quantum states. We denote by $\mathrm{diag}(X)$ the diagonal of a matrix X.

As in standard cryptographic notation, we use $\mathrm{poly}(n)$ to denote an arbitrary polynomially-bounded function of n, i.e. a function f for which there is a constant $c > 0$ such that $f(n) \leq n^c$ for all sufficiently large n. Likewise, we use $\mathrm{polylog}(n)$ for an arbitrary f satisfying $f(n) \leq \log(n)^c$ for all sufficiently large n, and $\mathrm{quasipoly}(n)$ for an arbitrary f satisfying $f(n) \leq 2^{\log(n)^c}$ for all sufficiently large n. $\mathrm{negl}(n)$ denotes an arbitrary negligibly-bounded function of n, i.e. a function f with the property that for every $c > 0$, for all sufficiently large n, $f(n) \leq n^{-c}$.

2.2 Boolean Functions

For convenience, we use the ±1 basis for Boolean functions. Every function $f : \{\pm 1\}^n \to \mathbb{R}$ can be represented uniquely as a real multilinear polynomial:

$$f(x) = \sum_{S \subseteq [n]} \hat{f}(S) \cdot \prod_{i \in S} x_i,$$

where $\hat{f}(S)$ are the Fourier coefficients of f. This allows us to extend the domain of f to arbitrary inputs in $\mathbb{R}^n$. The Fourier coefficients can be computed via:

$$\hat{f}(S) = \frac{1}{2^n} \sum_{x \in \{\pm 1\}^n} f(x) \cdot \prod_{i \in S} x_i.$$

for each $S \subseteq [n]$. In a slight abuse of notation, whenever $x \in \{\pm 1\}^n$, we let $\hat{f}(x) = \hat{f}(S)$ where $S := \{i \in [n] : x_i = -1\}$. For $\ell \in [n]$, we denote by

$$L_{1,\ell}(f) := \sum_{S \subseteq [n] : |S| = \ell} \left|\hat{f}(S)\right|.$$

If $f : \{\pm 1\}^n \to \{\pm 1\}$ is a Boolean function, we let $\mathrm{tt}(f) \in \{\pm 1\}^{2^n}$ denote the truth table of f, i.e. the concatenation of f evaluated on all possible Boolean inputs, in lexicographic order. We denote by

[5] Actually, to our knowledge, it is open even to construct PRUs relative to *any* classical oracle.

$\mathrm{AC}^0[s,d]$ the set of Boolean circuits of size at most s and depth at most d consisting of unbounded fan-in AND, OR, and NOT gates.

2.3 Concentration Inequalities

The concentration inequalities stated below are standard (see e.g. [40, Chapter 2]).

Fact 3 (Hoeffding's inequality)**.** *Suppose $X_1, \ldots, X_n$ are independent random variables such that $X_i \in [a_i, b_i]$ for all i. Let $X = \sum_{i=1}^n X_i$ and let $\mu = \mathbf{E}[X]$. Then for all $s \geq 0$ it holds that:*

$$\Pr[|X - \mu| \geq s] \leq 2\exp\left(-\frac{2s^2}{\sum_{i=1}^n (b_i - a_i)^2}\right).$$

A real-valued random variable X is σ-subgaussian if $\Pr[|X - \mathbb{E}[X]| \geq s\sigma] \leq 2e^{-s^2/2}$ holds for all $s \geq 0$. It follows from Hoeffding's inequality that for any vector $a \in \mathbb{R}^m$, the random variable $X = \langle a, Y\rangle$ where Y is uniform in $\{\pm 1\}^m$ is σ-subgaussian with $\sigma = \|a\|_2$.

Fact 4 (Bernstein's inequality)**.** *Let $X_1, \ldots, X_L$ be independent σ-subgaussian random variables. Let $X = \frac{1}{L}\sum_{i=1}^L X_i^2$ and let $\mu = \mathbb{E}[X]$. Then there exists an absolute constant $c > 0$ such that for every $s \geq 0$:*

$$\Pr\left[|X - \mu| \geq s\right] \leq 2\exp\left(-cL\min\left\{\frac{s^2}{\sigma^4}, \frac{s}{\sigma^2}\right\}\right).$$

We use the previous inequality to prove the following lemma.

Lemma 5. *Let $f_1, \cdots, f_L : \{\pm 1\}^n \to \{\pm 1\}$ be independent samples of uniformly random Boolean functions. Then, there exists an absolute constant $C > 0$, such that for any $z \in \{\pm 1\}^n$, we have*

$$\mathbf{E}\left|\frac{1}{L}\sum_{k=1}^L \hat{f}_k(z)^2 - \frac{1}{2^n}\right| \leq \frac{C}{2^n\sqrt{L}}.$$

Proof. For a uniformly random Boolean function $f : \{\pm 1\}^n \to \{\pm 1\}$, the Fourier coefficient is given by $\hat{f}(z) = \langle a, Y\rangle$ where Y is uniform in $\{\pm 1\}^{2^n}$ and $\|a\|_2 = 2^{-n/2}$. Thus, $\hat{f}(z)$ is σ-subgaussian and $\mathbf{E}[|\hat{f}(z)|^2] = \sigma^2$ for $\sigma = 2^{-n/2}$. Fact 4 then implies the following tail bound

$$\Pr\left[\left|\frac{1}{L}\sum_{k=1}^L \hat{f}_k(z)^2 - \frac{1}{2^n}\right| \geq s\right] \leq 2\exp\left(-cL\min\left\{\frac{s^2}{\sigma^4}, \frac{s}{\sigma^2}\right\}\right).$$

Since $\mathbf{E}[X] = \int_0^\infty \Pr[X \geq s]ds$ for any non-negative random variable X, we have

$$\begin{aligned}\mathbf{E}\left|\frac{1}{L}\sum_{k=1}^L \hat{f}_k(z)^2 - \frac{1}{2^n}\right| &\leq 2\int_0^{\sigma^2} e^{-cLs^2/\sigma^4}ds + 2\int_{\sigma^2}^\infty e^{-cLs/\sigma^2}ds \\ &= \frac{2\sigma^2}{\sqrt{cL}}\int_0^{\sqrt{cL}} e^{-s^2}ds + \frac{2\sigma^2}{cL}\int_{cL}^\infty e^{-s}ds \\ &\leq \frac{C\sigma^2}{\sqrt{L}},\end{aligned}$$

for an absolute constant $C > 0$. Plugging in the value of σ gives us the required bound. □

2.4 Quantum States

We also use the ±1 basis for quantum states. So, the space of n-qubit pure states is spanned by the orthonormal basis $\{|x\rangle : x \in \{\pm 1\}^n\}$, which we call the *computational basis*. We denote by μ_{Haar}^n the Haar measure over n-qubit pure states. We let $|+\rangle = \frac{|1\rangle + |-1\rangle}{\sqrt{2}}$, and use $|+^n\rangle$ as shorthand for $|+\rangle^{\otimes n}$. When the context is clear, H will generally denote the n-qubit Hadamard transform defined by

$$H := \begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{bmatrix}^{\otimes n}.$$

If f is a Boolean function, we let U_f be the phase oracle corresponding to f, i.e. the unitary transformation that acts as $U_f|x\rangle = f(x)|x\rangle$ on computational basis states $|x\rangle$. Note that for any Boolean function f and $x \in \{\pm 1\}^n$, $\langle x| HU_f |+^n\rangle = \hat{f}(x)$.

We define multi-copy pseudorandom quantum states as follows.

Definition 6 (Multi-copy pseudorandom quantum states [28])**.** *Let $\kappa \in \mathbb{N}$ be the security parameter, and let $n(\kappa)$ be the number of qubits in the quantum system. A keyed family of n-qubit quantum states $\{|\varphi_k\rangle\}_{k\in\{0,1\}^\kappa}$ is* multi-copy pseudorandom *if the following two conditions hold:*

- *(i) (Efficient generation) There is a polynomial-time quantum algorithm G that generates $|\varphi_k\rangle$ on input k, meaning $G(k) = |\varphi_k\rangle$.*
- *(ii) (Computationally indistinguishable) For any polynomial-time quantum adversary $\mathcal{A}$ and every $T = \mathrm{poly}(\kappa)$:*

$$\left|\Pr_{k\sim\{0,1\}^\kappa}\left[\mathcal{A}\left(1^\kappa, |\varphi_k\rangle^{\otimes T}\right) = 1\right] - \Pr_{|\psi\rangle\sim\mu_{\mathrm{Haar}}^n}\left[\mathcal{A}\left(1^\kappa, |\psi\rangle^{\otimes T}\right) = 1\right]\right| \leq \mathrm{negl}(\kappa).$$

We emphasize that the above security definition must hold for *all* polynomial values of T (i.e. T is not bounded in advance).

We also define single-copy pseudorandom states. Unlike in the multi-copy case, we require $n > \kappa$ in order for the definition to be nontrivial, analogous to how a classical pseudorandom generator stretches a seed of length κ into a pseudorandom string of length $n > \kappa$ (see [33, Section 2.2] for further discussion).

Definition 7 (Single-copy pseudorandom states [33])**.** *Let $\kappa \in \mathbb{N}$ be the security parameter, and let $n(\kappa) > \kappa$ be the number of qubits in the quantum system. A keyed family of n-qubit quantum states $\{|\varphi_k\rangle\}_{k\in\{0,1\}^\kappa}$ is* single-copy pseudorandom *if the following two conditions hold:*

- *(i) (Efficient generation) There is a polynomial-time quantum algorithm G that generates $|\varphi_k\rangle$ on input k, meaning $G(k) = |\varphi_k\rangle$.*
- *(ii) (Computationally indistinguishable) For any polynomial-time quantum adversary $\mathcal{A}$:*

$$\left|\Pr_{k\sim\{0,1\}^\kappa}[\mathcal{A}(1^\kappa, |\varphi_k\rangle) = 1] - \Pr_{|\psi\rangle\sim\mu_{\mathrm{Haar}}^n}[\mathcal{A}(1^\kappa, |\psi\rangle) = 1]\right| \leq \mathrm{negl}(\kappa).$$

In this work, we only consider uniform quantum adversaries. That is, the adversary $\mathcal{A}$ is specified by a polynomial-time Turing machine M, where $M(1^\kappa)$ outputs a quantum circuit that implements $\mathcal{A}$ on security challenges of size κ. However, our construction is plausibly secure against non-uniform adversaries as-is, or possibly via the addition of a salting step [18].

3 PSEUDORANDOMNESS OF THE FORRELATION DISTRIBUTION

We define our discrete version of the Forrelation distribution as follows:

Definition 8. *The* Forrelation distribution $\mathcal{F}_n$ *is a distribution over a pair of functions* $f, g : \{\pm 1\}^n \to \{\pm 1\}$ *sampled as follows. First,* f *is sampled uniformly at random. Then, for each* $x \in \{\pm 1\}^n$, $g(x)$ *is sampled independently via:*

$$g(x) = \begin{cases} 1 & \text{with probability } \frac{1+\mathrm{trnc}\left(\sqrt{\varepsilon 2^n}\hat{f}(x)\right)}{2} \\ -1 & \text{with probability } \frac{1-\mathrm{trnc}\left(\sqrt{\varepsilon 2^n}\hat{f}(x)\right)}{2}, \end{cases}$$

where $\varepsilon = \frac{1}{100n}$.

The main technical result of this section is that the above Forrelation distribution $\mathcal{F}_n$ is pseudorandom against all constant-depth $2^{\mathrm{poly}(n)}$-size AC^0 circuits.

Theorem 9. *For every* $C \in \mathrm{AC}^0[2^{\mathrm{poly}(n)}, O(1)]$, *the Forrelation distribution* $\mathcal{F}_n$ *satisfies*

$$\left| \mathop{\mathbf{E}}_{(f,g)\sim\mathcal{F}_n} [C(\mathrm{tt}(f), \mathrm{tt}(g))] - \mathop{\mathbf{E}}_{z\sim\{\pm 1\}^{2\cdot 2^n}} [C(z)] \right| \leq \frac{\mathrm{poly}(n)}{\sqrt{2^n}}.$$

Theorem 9 will be a special case of the following theorem. The special case holds since for any $C \in \mathrm{AC}^0[2^{\mathrm{poly}(n)}, O(1)]$ it holds that $L_{1,2}(C) \leq \mathrm{poly}(n)$, as proved in [39].

Theorem 10. *Let* $N = 2^n$. *Let* $\mathcal{C}$ *be a family of* $2N$*-variate Boolean functions, which is closed under restrictions. Assume that for any* $C \in \mathcal{C}$ *it holds that* $L_{1,2}(C) \leq t$. *Then, for any* $C \in \mathcal{C}$ *it holds that*

$$\left| \mathop{\mathbf{E}}_{f,g\sim\mathcal{F}_n} [C(\mathrm{tt}(f), \mathrm{tt}(g))] - \mathbf{E}[C] \right| \leq O\left(\frac{t\cdot \log N}{\sqrt{N}}\right).$$

Proof. We show how to obtain the distribution $\mathcal{F}_n$ approximately as a result of a random walk, taking $\mathrm{polylog}(N)$ steps, where each step is a multi-variate Gaussian.

(1) Let $m = 200 \ln(N)/\varepsilon$.
(2) Let $X^{(\leq 0)} = \vec{0}$, $Y^{(\leq 0)} = \vec{0}$.
(3) For $i = 1, \ldots, m$:

```
    Let $X^{(i)} \sim N(0, \varepsilon)^N$
    Let $D = (1 - |X^{(\leq i-1)}|)$
        $X^{(\leq i)} = X^{(\leq i-1)} + D \odot \mathrm{trnc}(X^{(i)})$
        $Y^{(\leq i)} = \mathrm{trnc}(Y^{(\leq i-1)} + \mathrm{trnc}_{1/2}(\sqrt{\varepsilon} HD \odot X^{(i)}))$
```

(4) Output $(X^{(\leq m)}, Y^{(\leq m)})$.

We observe that by definition, the coordinates of $X^{(\leq i)}$ and $Y^{(\leq i)}$ are bounded in $[-1, 1]$, and the coordinates of $X^{(\leq i)}$ are independent. We further make the following three claims/observations.

The first claim should be interpreted as "with high probability, truncations are irrelevant".

Claim 11. *With probability at least* $1 - m/N^{10}$, *for all* $i \in [m]$

$$Y^{(\leq i)} = \sqrt{\varepsilon} HX^{(\leq i)} \text{ and } Y^{(\leq i)} \in [-1/2, 1/2]^N.$$

The second claim should be interpreted as "$X^{(\leq i)}$ polarizes", i.e., coordinates get closer to ±1.

Claim 12. *With probability at least* $1 - 1/N^2$, *we have*

$$|X^{(\leq m)}| \in [1 - 1/N^3, 1]^N.$$

The third claim should be interpreted as "with high probability, the change under the i-th step is small (with respect to C)".

Claim 13. *For any* $i \in [m]$, *with probability at least* $1 - 2/N^2$ *over* $(X^{(\leq i-1)}, Y^{(\leq i-1)})$ *(i.e., the history before step i), the i-th step size satisfies*

$$\mathop{\mathbf{E}}_{X^{(i)}} \left[C\left(X^{(\leq i)}, Y^{(\leq i)}\right) - C\left(X^{(\leq i-1)}, Y^{(\leq i-1)}\right) \right] \leq O\left(t\varepsilon/\sqrt{N}\right).$$

We defer the proof of the claims to the end of the section, after Theorem 15. We show how to complete the proof given the three claims. Let $\mathcal{E}$ be the event that:

$$Y^{(\leq m)} = \sqrt{\varepsilon} HX^{(\leq m)} \tag{1}$$

$$Y^{(\leq m)} \in [-1/2, 1/2]^N \tag{2}$$

$$\left|X^{(\leq m)}\right| \in [1 - 1/N^3, 1]^N \tag{3}$$

$$\forall i \in [m] : \left(X^{(\leq i-1)}, Y^{(\leq i-1)}\right) \text{ satisfies}$$
$$\mathop{\mathbf{E}}_{X^{(i)}} \left[C\left(X^{(\leq i)}, Y^{(\leq i)}\right) - C\left(X^{(\leq i-1)}, Y^{(\leq i-1)}\right) \right] \leq O\left(t\varepsilon/\sqrt{N}\right). \tag{4}$$

Let $\delta := \Pr[\neg\mathcal{E}]$ which by the three claims is at most $1/N$ for sufficiently large N. For each $i \in [m]$, we have

$$\left| \mathbf{E}[C(X^{(\leq i)}, Y^{(\leq i)}) \mid \mathcal{E}] - \mathbf{E}[C(X^{(\leq i-1)}, Y^{(\leq i-1)}) \mid \mathcal{E}] \right| \leq O\left(\delta + t\varepsilon/\sqrt{N}\right) \leq O\left(t\varepsilon/\sqrt{N}\right),$$

since conditioned on $\mathcal{E}$, the $(i-1)$-th history definitely satisfies Condition (4), but the conditioning might change the distribution of $X^{(i)}$ by up to δ total-variation distance, and we need to compensate for that. We get that

$$\left| \mathbf{E}[C(X^{(\leq m)}, Y^{(\leq m)}) \mid \mathcal{E}] - \mathbf{E}[C] \right| \leq O\left(mt\varepsilon/\sqrt{N}\right).$$

From Condition (3), we see that $X' := \mathrm{sgn}(X^{\leq m})$ is $1/N^3$-close to $X^{(\leq m)}$. By Condition (1) we see that $Y^{(\leq m)} = \sqrt{\varepsilon} HX^{(\leq m)}$ and thus

$$Y' := \sqrt{\varepsilon} HX' = \sqrt{\varepsilon} HX^{(\leq m)} + \sqrt{\varepsilon} H(X' - X^{(\leq m)}) = Y^{(\leq m)} + err$$

where each coordinate of err is at most $\sqrt{\varepsilon}\sqrt{N}/N^3 \leq 1/N^2$ in absolute value. By Condition (2), we get that $Y' \in [-1, 1]^N$. We apply the next claim to get

$$\left| \mathbf{E}[C(X', Y') | \mathcal{E}] - \mathbf{E}[C(X^{(\leq m)}, Y^{(\leq m)}) | \mathcal{E}] \right| \leq 2/N.$$

Fact 14 (Folklore, See e.g. [17, Lemma 2.7])**.** *Let* $C : [-1, 1]^{2N} \to [-1, 1]$ *be a multi-linear function. Then for every* $z, z' \in [-1, 1]^{2N}$ *we have* $|C(z) - C(z')| \leq 2N \cdot \|z - z'\|_\infty$.

Then, triangle inequality gives

$$\left| \mathbf{E}[C(X', Y') | \mathcal{E}] - \mathbf{E}[C] \right| \leq 2/N + O\left(mt\varepsilon/\sqrt{N}\right) \leq O\left(mt\varepsilon/\sqrt{N}\right),$$

and since $(X', Y')|\mathcal{E}$ is δ-close in statistical distance to the distribution $(X', \mathrm{trnc}(\sqrt{\varepsilon}HX'))$ we get

$$\begin{aligned} |\,\mathbf{E}[C(X', \mathrm{trnc}(\sqrt{\varepsilon}HX'))] - \mathbf{E}[C]| &\le O\Big(mt\varepsilon/\sqrt{N}\Big) + \delta \\ &\le O\Big(mt\varepsilon/\sqrt{N}\Big) \\ &= O\Big(t\log(N)/\sqrt{N}\Big). \end{aligned}$$

Finally, we observe that X' is the uniform distribution over $\{-1, 1\}^N$ and the expectation of any multilinear polynomial with respect to $(X', \mathrm{trnc}(\sqrt{\varepsilon}HX'))$ is the same as that with respect to the Forrelation distribution $\mathcal{F}_n$. □

Proofs of the Three Claims. We will rely on the following theorem from [37] and the following lemma from [16].

Theorem 15 ([37], as restated in [17, Theorem 9]). *Let $n, t \ge 1$, $\delta \in (0, 1)$. Let $Z \in \mathbb{R}^n$ be a zero-mean multivariate Gaussian random variable with the following two properties:*

(1) For $i \in [n]$: $\mathbf{Var}[Z_i] \le \frac{1}{8\ln(n/\delta)}$.
(2) For $i, j \in [n], i \ne j$: $|\mathbf{Cov}[Z_i, Z_j]| \le \delta$.

Let $\mathcal{C}$ be a family of n-variate Boolean functions, which is closed under restrictions. Assume that $L_{1,2}(\mathcal{C}) \le t$. Then, for any $C \in \mathcal{C}$ it holds that $\Big|\mathbf{E}[C(\mathrm{trnc}(Z))] - C(\vec{0})\Big| \le O(\delta \cdot t)$.

Claim 16 ([16, Claim 3.3]]). *Let f be a multilinear function on $\mathbb{R}^n$ and $v \in (-1, 1)^n$. Let $\delta \in [0, 1]^n$ with $\delta_i \le 1 - |v_i|$. Then, there exists a distribution over random restrictions ρ such that for any $z \in \mathbb{R}^n$,*

$$f(v + \delta \odot z) - f(v) = \mathop{\mathbf{E}}_{\rho}[f_\rho(z) - f_\rho(\vec{0})].$$

We remark that the statement of [16, Claim 3.3] as stated in their paper is slightly different from the above, but the above claim is implicit in their proof.

We go on to prove the three claims. We start with the proof of Claim 13 as it is the hardest.

Proof of Claim 13. Fix a history $x^{(\le i-1)}, y^{(\le i-1)}$ and assume that $y^{(\le i-1)} \in [-1/2, 1/2]^N$, an event which happens with probability at least $1 - 1/N^2$. Let $d = (1 - |x^{(\le i-1}|)$. By definition,

$$Y^{(\le i)} = \mathrm{trnc}\Big(y^{(\le i-1)} + \mathrm{trnc}_{1/2}(\sqrt{\varepsilon}H(d \odot X^{(i)})\Big),$$

and by our assumption on $y^{(\le i-1)}$ we get that we can get rid of the outer trnc. Furthermore we observe that $\mathrm{trnc}_{1/2}(x) = \frac{1}{2}\mathrm{trnc}(2x)$ and we can thus simplify further to

$$Y^{(\le i)} = y^{(\le i-1)} + \frac{1}{2} \cdot \mathrm{trnc}\Big(2\sqrt{\varepsilon}H(d \odot X^{(i)})\Big).$$

We plug this in and apply Claim 16, to get that LHS of Claim 13

$$\begin{aligned} &\mathop{\mathbf{E}}_{X^{(i)}}\Big[C\Big(X^{(\le i)}, Y^{(\le i)}\Big) - C\Big(x^{(\le i-1)}, y^{(\le i-1)}\Big)\Big] \\ =& \mathop{\mathbf{E}}_{X^{(i)}}\Big[C\Big(x^{(\le i-1)} + d \odot \mathrm{trnc}\Big(X^{(i)}\Big),\ y^{(\le i-1)} + \\ &\qquad \frac{1}{2} \cdot \mathrm{trnc}\Big(2\sqrt{\varepsilon}H(d \odot X^{(i)})\Big)\Big) - C\Big(x^{\le(i-1)}, y^{\le(i-1)}\Big)\Big] \\ =& \mathop{\mathbf{E}}_{X^{(i)},\rho}\Big[C_\rho\Big(\mathrm{trnc}\Big(X^{(i)}\Big), \mathrm{trnc}\Big(2\sqrt{\varepsilon}H(d \odot X^{(i)})\Big)\Big) - C_\rho(0)\Big] \end{aligned}$$

for some distribution over random restrictions ρ. To apply Theorem 15, it remains is to bound the variances and co-variances of the coordinates in $\Big(X^{(i)}, 2\sqrt{\varepsilon}H(d \odot X^{(i)})\Big)$. We see that:

$$\begin{aligned} \forall j : \mathbf{Var}\Big(X_j^{(i)}\Big) &= \varepsilon \\ \forall j : \mathbf{Var}\Big((2\sqrt{\varepsilon}H(d \odot X^{(i)}))_j\Big) &= 4\varepsilon \cdot \varepsilon \sum_{\ell} H_{j,\ell}^2 \cdot d_\ell^2 \le 4\varepsilon^2 \\ \forall j \ne k : \mathbf{Cov}\Big(X_j^{(i)}, X_k^{(i)}\Big) &= 0 \\ \forall j, k : \Big|\mathbf{Cov}\Big(2\sqrt{\varepsilon}H(d \odot X^{(i)}))_j, X_k^{(i)}\Big)\Big| &= \\ \Big|2\sqrt{\varepsilon} \cdot H_{j,k} \cdot d_k \cdot \varepsilon\Big| &\le 2\varepsilon^{3/2}/\sqrt{N} \\ \forall j \ne k : \Big|\mathbf{Cov}\Big((2\sqrt{\varepsilon}H(d \odot X^{(i)}))_j, (2\sqrt{\varepsilon}H(d \odot X^{(i)}))_k\Big)\Big| &= \\ 4\varepsilon^2 \cdot \Big|\sum_{\ell} H_{j,\ell}H_{k,\ell}d_\ell^2\Big| & \end{aligned}$$

To bound the last term, we consider the history $X^{(\le i-1)}$ as a random variable. We denote by $D = (1 - |X^{(\le i-1)}|)$ and show that with high probability over the history, $4\varepsilon^2 \cdot \big|\sum_\ell H_{j,\ell}H_{k,\ell}D_\ell^2\big|$ is small. Observe that since the rows of H are orthogonal, and all entries are $\pm 1/\sqrt{N}$, then there are exactly $N/2$ indices ℓ such that $H_{j,\ell}H_{k,\ell} = 1/N$ and exactly $N/2$ indices ℓ such that $H_{j,\ell}H_{k,\ell} = -1/N$. Thus, we can pair each positive index ℓ with a negative index ℓ'. For each such pair, (ℓ, ℓ'), the expectation of $\frac{1}{N}(D_\ell^2 - D_{\ell'}^2)$ is 0 as the coordinates of $X^{(\le i-1)}$ are i.i.d. Furthermore, $\frac{1}{N}(D_\ell^2 - D_{\ell'}^2)$ is bounded in $[-1/N, 1/N]$. By Hoeffding's inequality (Fact 3), we get that for any η,

$$\Pr\Bigg[\Bigg|\sum_\ell H_{j,\ell}H_{k,\ell}D_\ell^2\Bigg| \ge \eta\Bigg] \le 2\exp(-\eta^2 N).$$

By taking $\eta := 1/\sqrt{\varepsilon N}$, we get that this probability is smaller than $2\exp(-1/\varepsilon) = 2/N^{100}$. To summarize, we see that with probability at least $1 - 2/N^2$, the history satisfies $Y^{(\le i-1)} \in [-1/2, 1/2]^N$ and $\big|\sum_\ell H_{j,\ell}H_{k,\ell}D_\ell^2\big| < 1/\sqrt{\varepsilon N}$. This makes the co-variances of $(X^{(i)}, 2\sqrt{\varepsilon}H(d \odot X^{(i)}))$ smaller than $\delta := \varepsilon/\sqrt{N}$ and the variances smaller than $\varepsilon \le 1/(8\ln(N/\delta))$, and hence Theorem 15 gives

$$\begin{aligned} \forall \rho : \mathop{\mathbf{E}}_{X^{(i)}}\Big[C_\rho\Big(\mathrm{trnc}(X^{(i)}), \mathrm{trnc}(2\sqrt{\varepsilon}H(d \odot X^{(i)}))\Big) - C_\rho(0)\Big] &\le \\ O(t \cdot \delta) = O(t\varepsilon/\sqrt{N})\ . & \end{aligned}$$

□

Proof of Claim 11. For $i = 1, \ldots, m$, let $\mathcal{E}_i$ be the event that $Y^{(\le i)}$ satisfy the conditions of the claim, i.e., $Y^{(\le i)} = \sqrt{\varepsilon}HX^{(\le i)}$ and $Y^{(\le i)} \in [-1/2, 1/2]^N$.

We prove by induction on i that $\Pr[\mathcal{E}_1, \ldots, \mathcal{E}_i] \ge 1 - i/N^{10}$. The claim surely holds for $i = 0$. For $i \ge 1$, conditioned on $\mathcal{E}_1, \ldots, \mathcal{E}_{i-1}$, $X^{(i)}$ is still completely random, and by the concentration of multivariate Gaussians, the i-th step size is small with high probability. More precisely, $\sqrt{\varepsilon}H(D \odot X^{(i)})$ gives N independent Gaussians with zero-mean and variance $\le \varepsilon^2$. They are all in the range $[-1/2, 1/2]$ with a probability of at least $1 - 2N \cdot \exp(-\Omega(1/\varepsilon^2)) \ge 1 - \mathrm{negl}(N)$. Furthermore $X^{(i)} \in [-1, 1]^N$ with with probability at least $1 - 2N\exp(-1/2\varepsilon) \ge 1 - 1/N^{40}$. Let $\mathcal{E}_i'$ be the event that all coordinates of $\sqrt{\varepsilon}H(D \odot X^{(i)})$ are between $-1/2$ and $1/2$ and all coordinates of $X^{(i)}$ are between −1 and 1. Under this event, we get that the truncations do nothing, and we have

$$X^{(\le i)} = X^{(\le i-1)} + D \odot X^{(i)}$$
$$Y^{(\le i)} = Y^{(\le i-1)} + \sqrt{\varepsilon} H(D \odot X^{(i)}).$$

Thus, under $\mathcal{E}_1, \dots, \mathcal{E}_{i-1}, \mathcal{E}'_i$, we have

$$Y^{(\le i)} = \sqrt{\varepsilon} H X^{(\le i)}$$

which concludes the proof of the first property.

As for the second property, observe that without any conditioning, $X^{(\le i)}$ is a collection of N i.i.d. zero-mean bounded random variables in $[-1, 1]$. This means that we can apply Hoeffding's inequality (Fact 3) to conclude that

$$\forall j \in [N] : \quad \Pr[|(\sqrt{\varepsilon} H X^{(\le i)})_j| \ge 1/2] \le 2 \cdot \exp(-1/(8\varepsilon)).$$

Finally, we observe that if both the events $Y^{(\le i)} = \sqrt{\varepsilon} H X^{(\le i)}$ and $(\sqrt{\varepsilon} H X^{(\le i)}) \in [-1/2, 1/2]^N$ happen, then the event $\mathcal{E}_i$ happens. Taking a union bound over the bad events, we get that

$$\begin{aligned}\Pr[\neg \mathcal{E}_i \mid \mathcal{E}_1, \dots, \mathcal{E}_{i-1}] &\le \mathrm{negl}(N) + 1/N^{40} + 2N \cdot \exp(-1/(8\varepsilon)) \\ &\le 1/N^{10} ,\end{aligned}$$

which, in turn, implies that $\Pr[\mathcal{E}_1, \dots, \mathcal{E}_i] \ge 1 - i/N^{10}$. □

To prove Claim 12 we rely on the following Claim from [16].

Claim 17 ([16, Claim 3.5])**.** *Let $A_1, \dots, A_m \in [-1, 1]$ be independent symmetric random variables with $\mathbf{E}[A_i^2] \ge p$. For $i = 1, \dots, m$ define $B_i = B_{i-1} + (1 - |B_{i-1}|)A_i$, where $B_0 = 0$. Then, $\mathbf{E}[B_m^2] \ge 1 - q$ for $q = 3\exp(-mp/16)$.*

Proof of Claim 12. Fix $j \in [N]$. We see that the sequences $A_1 = \mathrm{trnc}(X_j^{(1)}), \dots, A_m = \mathrm{trnc}(X_j^{(m)})$ and $B_1 = X_j^{(\le 1)}, \dots, B_m = X_j^{(\le m)}$ satisfy $B_i = B_{i-1} + (1 - |B_{i-1}|)A_i$. Additionally, $A_1, \dots, A_m$ are independent, symmetric random variables with

$$\begin{aligned}\mathbf{E}[A_i^2] &= \mathbf{E}\left[(X_j^{(i)})^2\right] - \mathbf{E}\left[\left((X_j^{(i)})^2 - 1\right) \cdot \mathbb{1}\left\{|X_j^{(i)}| \ge 1\right\}\right] \\ &\ge \varepsilon - 1/N^{50} \ge \varepsilon/2 .\end{aligned}$$

Thus, we get that $\mathbf{E}[1 - |B_m|] \le \mathbf{E}[1 - B_m^2] \le q$ for $q = 3\exp(-m\varepsilon/32) \le 1/N^6$, and in particular $\Pr[1 - |B_m| \ge 1/N^3] \le 1/N^3$. Taking union bound over all N coordinates completes the proof. □

4 CONSTRUCTION OF THE ORACLE

The oracle used in our construction of pseudorandom states is simple to describe: it consists of a uniformly random oracle A, and an oracle B that answers all NP queries to A or B. Formally, we construct the oracle as follows.

Definition 18. *For a language $A : \{\pm 1\}^* \to \{\pm 1\}$, we define a language $\mathcal{O}[A]$ as follows. We construct an oracle B inductively: for each $\ell \in \mathbb{N}$ and $x \in \{\pm 1\}^\ell$, view x as an encoding of a pair $\langle M, y\rangle$ such that*

(1) $\langle M, y\rangle$ takes less than ℓ bits to specify,[6]
(2) M is an NP oracle machine and y is an input to M,
(3) M is syntactically restricted to run in less than ℓ steps, and to make queries to A and B on strings of length at most $\lfloor\sqrt{\ell}\rfloor$.

Then we define $B(x) \coloneqq M(y)$. Finally, let $\mathcal{O}[A] = (A, B)$.

Oracles such as those defined in Definition 18 always collapse NP to P, as shown below.

Proposition 19. *For any language $A : \{\pm 1\}^* \to \{\pm 1\}$, $\mathsf{P}^{\mathcal{O}[A]} = \mathsf{NP}^{\mathcal{O}[A]}$.*

Proof. Given an $\mathsf{NP}^{\mathcal{O}[A]}$ machine M and input y, a polynomial time algorithm can decide $M(y)$ by taking $x = \langle M, y\rangle$ and querying $B(x)$. □

Similar oracle constructions appeared in [4, 11]. Morally speaking, queries to $\mathcal{O}[A]$ are roughly equivalent in power to queries to PH^A. Indeed, any PH^A language can be decided in $\mathsf{P}^{\mathcal{O}[A]}$, by a simple extension of Proposition 19. A partial converse also holds: via the well-known connection between between PH algorithms and AC^0 circuits [20], each bit of $\mathcal{O}[A]$ can be computed by an exponential-sized AC^0 circuit depending on A.

We next define the quantum states that we use to construct pseudorandom ensembles relative to our oracles, which are based on t-Forrelation states.

Definition 20 (t-Forrelation states)**.** *For a t-tuple of functions $F = (f^1, f^2, ..., f^t)$ where $f^i : \{\pm 1\}^n \to \{\pm 1\}$, we denote by $|\Phi_F\rangle$ the state:*

$$|\Phi_F\rangle \coloneqq U_{f^t} \cdot H \cdot U_{f^{t-1}} \cdot H \cdots H \cdot U_{f^1} |+^n\rangle .$$

where U_{f^i} is the unitary phase oracle corresponding to f^i and H is the n-qubit Hadamard transform. We call any such state a t-Forrelation state.

The pseudorandom state ensembles we consider consist of random t-Forrelation states where the phase oracles are specified by the random oracle A.

Definition 21 (State ensemble relative to A)**.** *Fix a security parameter κ and $t \ge 1$. We define an ensemble of n-qubit states for some $\kappa + 1 \le n \le \mathrm{poly}(\kappa)$. For each $k \in \{0, 1\}^\kappa$ and $i \in [t]$, define $f_k^i : \{\pm 1\}^n \to \{\pm 1\}$ by $f_k^i(x) = A(x, k, i)$.*[7] *Letting $F_k = (f_k^1, f_k^2, \dots, f_k^t)$ we choose:*

$$|\varphi_k\rangle \coloneqq |\Phi_{F_k}\rangle ,$$

and take the ensemble to be $\{|\varphi_k\rangle\}_{k \in \{0,1\}^\kappa}$.

The main goal of the remainder of this work will be to show that when A is a random oracle, then with probability 1 over A, the set $\{|\varphi_k\rangle\}_{k \in \{0,1\}^\kappa}$ forms a secure pseudorandom state ensemble relative to $\mathcal{O}[A]$. We emphasize that our proofs will show security for *any* function $n(\kappa)$ that satisfies $\kappa + 1 \le n \le \mathrm{poly}(\kappa)$.

5 SINGLE-COPY SECURITY

Throughout this section, we fix $t = 2$ in Definition 21. Additionally, we will always denote (f_k^1, f_k^2) by (f_k, g_k), so that:

$$|\varphi_k\rangle = U_{g_k} \cdot H \cdot U_{f_k} |+^n\rangle .$$

The goal of this section is to prove, relative to $\mathcal{O}[A]$, the pseudorandomness of the ensemble $\{|\varphi_k\rangle\}_{k \in \{0,1\}^\kappa}$ defined in Definition 21.

[6] Note that there are $2^\ell - 1$ such possible $\langle M, y\rangle$, which is why we take an encoding in $\{\pm 1\}^\ell$.

[7] In a slight abuse of notation, k and i correspond to their binary representations over $\{\pm 1\}^\kappa$ and $\{\pm 1\}^{\lceil \log t\rceil}$, respectively, in $A(x, k, i)$.

Theorem 22. *With probability* 1 *over a random oracle A, the ensemble $\{|\varphi_k\rangle\}_{k\in\{0,1\}^\kappa}$ is single-copy pseudorandom relative to $O[A]$.*

5.1 Construction of Hybrids

We will prove Theorem 22 via a hybrid argument. Each hybrid below defines a security challenge for the quantum adversary. The security challenge consists of a state $|\psi\rangle$ and an oracle A that are sampled by the hybrid (note that $|\psi\rangle$ may in general depend on A). The adversary is given a single copy of $|\psi\rangle$ as input, and can make queries to $O[A]$.

For convenience, in each of these hybrids we only specify the part of A that corresponds to the functions $\{(f_k, g_k)\}_{k\in\{0,1\}^\kappa}$ that are used to construct the states with security parameter κ. Recall that $f_k(x) = A(x, k, 1)$ and $g_k(x) = A(x, k, -1)$. Otherwise, the rest of A is always sampled uniformly at random.

Ultimately, we wish to show the indistinguishability of the following two challenges:

Hybrid H_0*:* Sample $k^* \sim \{0,1\}^\kappa$. For each $k \in \{0,1\}^\kappa$, sample $f_k, g_k : \{\pm1\}^n \to \{\pm1\}$ uniformly at random. The adversary gets $|\psi\rangle = |\varphi_{k^*}\rangle$ as input.

Hybrid H_4*:* For each $k \in \{0,1\}^\kappa$, sample $f_k, g_k : \{\pm1\}^n \to \{\pm1\}$ uniformly at random. The adversary gets a Haar-random state $|\psi\rangle$ as input.

Hybrid H_0 corresponds to sampling a state from the PRS ensemble, whereas Hybrid H_4 corresponds to sampling a Haar-random state. We will interpolate between these hybrids by changing how we sample either the oracle A or the state $|\psi\rangle$ in each step.

In the first intermediate hybrid, we observe that the uniform distribution over (f_k, g_k) can also be generated by first sampling a Forrelated (f'_k, g'_k), and then multiplying g'_k pointwise with a uniformly random function. This motivates the next hybrid, which we shall show is equivalent to H_0.

Hybrid H_1*:* Sample $k^* \sim \{0,1\}^\kappa$. For each $k \in \{0,1\}^\kappa$, sample $f'_k, g'_k : \{\pm1\}^n \to \{\pm1\}$ as follows:

- If $k = k^*$, draw $(f'_k, g'_k) \sim \mathcal{F}_n$.
- If $k \neq k^*$, draw f'_k, g'_k uniformly at random.

Additionally, sample a random function $h : \{\pm1\}^n \to \{\pm1\}$. For each $k \in \{0,1\}^\kappa$, set $f_k = f'_k$ and $g_k = g'_k \cdot h$ (i.e. XOR in the ±1 domain). The adversary gets $|\psi\rangle = |\varphi_{k^*}\rangle$ as input.

From the results of [4] (and Theorem 9 about the Forrelation distribution $\mathcal{F}_n$), we know that no efficient quantum algorithm that queries the oracle $O[A]$ can distinguish the distribution of $\{f'_k, g'_k\}_k$ where a random pair k^* is Forrelated from the uniform distribution $\{f'_k, g'_k\}_k$. So, one expects that if one samples f'_{k^*}, g'_{k^*} to be uniformly random instead, no quantum algorithm should be able to detect this. However, we cannot use the result of [4] as a black box, because in our setting the quantum algorithm also gets an input state that is correlated with the distribution of the oracle.

To handle this issue, we first show that we can replace the input state with a state that is not correlated with the oracle, so that afterwards we can apply the result of [4]. Ultimately, we will argue using the definition of $\mathcal{F}_n$ that, from the viewpoint of the algorithm, the replaced state looks like a mixture of $|\varphi_{k^*}\rangle$ and a maximally mixed state in the orthogonal subspace.

Hybrid H_2*:* The distribution of $f_k, g_k, h : \{\pm1\}^n \to \{\pm1\}$ is the same as the Hybrid H_1, but the adversary instead receives the state $|\psi\rangle = |\Phi_h\rangle$ as the input (recall that $|\Phi_h\rangle = U_h |+^n\rangle$).

Since in Hybrid H_2, the input state is independent of the oracle, we can apply the result of [4] and switch the distribution of f'_{k^*}, g'_{k^*} as discussed before. This gives us the next hybrid.

Hybrid H_3*:* The distribution of f_k, g_k is chosen as in the Hybrid H_2 except that f'_{k^*}, g'_{k^*} are chosen to be uniformly random functions as opposed to being sampled from $\mathcal{F}_n$. The adversary receives the same input state $|\psi\rangle = |\Phi_h\rangle$ as in the Hybrid H_2.

Note that the distribution of f_k, g_k is uniformly random in H_3, and $|\Phi_h\rangle$ is a random phase state independent of the oracle. The result of [15] will imply that we can replace $|\Phi_h\rangle$ with a Haar random state, as in H_4.[8]

5.2 Security Proof

We now proceed to the formal security proof. For a fixed quantum adversary $\mathcal{A}$ and $i \in \{0,1,2,3,4\}$, we denote:

$$p_i(\mathcal{A}) := \Pr_{(|\psi\rangle, A)\sim \mathsf{H}_i}\left[\mathcal{A}^{O[A]}(1^\kappa, |\psi\rangle) = 1\right],$$

as the probability that the algorithm accepts on a particular hybrid. We successively analyze the hybrids in numerical order.

Claim 23. *For all $\mathcal{A}$, $p_0(\mathcal{A}) = p_1(\mathcal{A})$.*

Proof. This follows from the fact that H_0 and H_1 are identically distributed, as we now argue. It suffices to show that the oracle A chosen in H_1 is uniformly random. This holds by observing that if we sample $(f, g) \sim \mathcal{F}_n$ and $h : \{\pm1\}^n \to \{\pm1\}$ uniformly at random, then $(f, g\cdot h)$ is a uniformly random pair of functions, because by Definition 8, the marginal distribution of f is uniformly random. □

For the next pair of hybrids, it will be helpful to first establish two statistical lemmas about the Fourier spectrum of the f_k's.

Lemma 24. *With probability* 1 *over A, for all sufficiently large κ, $k \in \{0,1\}^\kappa$, and $i \in \{0,1\}^n$, we have that:*

$$\left|\hat{f}_k(i)\right| \leq \frac{1}{\sqrt{\varepsilon 2^n}},$$

where ε is given in Definition 8.

Proof. Fix $\kappa \in \mathbb{N}$. Note that for any fixed k, i, the Fourier coefficient $\hat{f}_k(i)$ is a sum of 2^n independent $\pm\frac{1}{2^n}$ random variables. Hence, by Fact 3 it holds that:

$$\Pr_A\left[\left|\hat{f}_k(i)\right| > \frac{1}{\sqrt{\varepsilon 2^n}}\right] \leq 2\exp\left(-\frac{\frac{2}{\varepsilon 2^n}}{2^n \cdot \frac{4}{4^n}}\right) = 2\exp\left(-\frac{1}{2\varepsilon}\right),$$

[8] Actually, because we only consider single-copy security, we will not require the full strength of [15]. In particular, we will be able to use the simpler observation that a single copy of either a Haar-random state or a random phase state equals the maximally mixed state.

and therefore, by a union bound:

$$\begin{aligned}\Pr_A\left[\exists k \in \{0,1\}^\kappa, i \in \{0,1\}^n : \left|\hat{f}_k(i)\right| > \frac{1}{\sqrt{\varepsilon 2^n}}\right] &\le 2^{n+\kappa+1}\exp\left(-\frac{1}{2\varepsilon}\right)\\ &\le 2^{n+\kappa+1-1/2\varepsilon}\\ &= 2^{\kappa+1-49n}\\ &\le \mathrm{negl}(\kappa),\end{aligned}$$

where we have used the fact that $\varepsilon = \frac{1}{100n}$ and $n > \kappa$.

By the Borel–Cantelli Lemma, because $\sum_{\kappa=1}^{\infty} \mathrm{negl}(\kappa) \le O(1)$, we conclude that with probability 1 over A, $\left|\hat{f}_k(i)\right| > \frac{1}{\sqrt{\varepsilon 2^n}}$ for at most finitely many k, i. Hence, the lemma. □

Lemma 25. *With probability* 1 *over* A,

$$\sum_{i \in \{\pm 1\}^n} \left|\frac{1}{2^n} - \mathop{\mathbf{E}}_{k \sim \{0,1\}^\kappa}\left[\hat{f}_k(i)^2\right]\right| \le \mathrm{negl}(\kappa).$$

Proof. For notational simplicity, let

$$q_{\kappa,A} = \sum_{i \in \{\pm 1\}^n} \left|\frac{1}{2^n} - \mathop{\mathbf{E}}_{k \sim \{0,1\}^\kappa}\left[\hat{f}_k(i)^2\right]\right|.$$

Applying Lemma 5, we have that for an absolute constant $C > 0$,

$$\mathop{\mathbf{E}}_A\left[q_{\kappa,A}\right] \le \sum_{i \in \{\pm 1\}^n} C 2^{-n-\kappa/2} = C 2^{-\kappa/2}.$$

Hence, by Markov's inequality:

$$\Pr_A\left[q_{\kappa,A} \ge \sqrt{C} 2^{-\kappa/4}\right] \le \sqrt{C} 2^{-\kappa/4}.$$

By the Borel–Cantelli Lemma, because $\sum_{\kappa=1}^{\infty} \sqrt{C} 2^{-\kappa/4} \le O(1)$, we conclude that with probability 1 over A, $q_{\kappa,A} \ge \sqrt{C} 2^{-\kappa/4}$ for at most finitely many $\kappa \in \mathbb{N}$. This is to say that $q_{\kappa,A} \le \mathrm{negl}(\kappa)$ with probability 1 over A. □

For a given oracle A, let ρ_A denote the mixed state obtained by conditionally averaging over all possible states $|\psi\rangle$ such that $(|\psi\rangle, A)$ was sampled from H_1, i.e. the 2-Forrelation state $|\varphi_{k^*}\rangle$. That is, we define:

$$\rho_A \coloneqq \mathop{\mathbf{E}}_{\mathsf{H}_1}\left[|\psi\rangle\langle\psi| \mid A\right]. \tag{5}$$

Likewise, define σ_A analogously for H_2, i.e. the phase state $|\Phi_h\rangle$:

$$\sigma_A \coloneqq \mathop{\mathbf{E}}_{\mathsf{H}_2}\left[|\psi\rangle\langle\psi| \mid A\right]. \tag{6}$$

Note that the above mixed states are the input states from the viewpoint of any algorithm $\mathcal{A}$ that operates on hybrids H_1 and H_2, respectively, after fixing the oracle A.

Lemma 26. *Let* $\tau_A = \varepsilon\rho_A + (1-\varepsilon)\frac{I}{2^n}$*, where* $\varepsilon = \frac{1}{100n}$ *is as in Definition 8. Then with probability* 1 *over* A, $\mathrm{TD}(\sigma_A, \tau_A) \le \mathrm{negl}(\kappa)$.

Proof. First, it will be convenient to compute more explicit forms for ρ_A and σ_A. Letting $\{(f_k, g_k)\}_{k \in \{0,1\}^\kappa}$ be the functions sampled in A, we can write:

$$\rho_A = \mathop{\mathbf{E}}_{k^* \sim \{0,1\}^\kappa}\left[U_{g_{k^*}} H U_{f_{k^*}} |+^n\rangle\langle +^n| U_{f_{k^*}} H U_{g_{k^*}}\right].$$

Hence, it follows that individual entries of ρ_A are given by:

$$\langle i|\rho_A|j\rangle = \mathop{\mathbf{E}}_{k^* \sim \{0,1\}^\kappa}\left[g_{k^*}(i) g_{k^*}(j) \hat{f}_{k^*}(i) \hat{f}_{k^*}(j)\right], \tag{7}$$

where we have used the fact that $\langle i| H U_f |+^n\rangle = \hat{f}(i)$ for any Boolean function f.

Analogously, σ_A may be expressed as:

$$\sigma_A = \mathop{\mathbf{E}}_{k^* \sim \{0,1\}^\kappa}\left[\mathop{\mathbf{E}}_{\mathcal{F}_n}\left[U_{g_{k^*}} U_g |+^n\rangle\langle +^n| U_g U_{g_{k^*}} \middle| f = f_{k^*}\right]\right],$$

where the inner expectation denotes that we conditionally average over $(f, g) \sim \mathcal{F}_n$ conditioned on the event $f = f_{k^*}$. This is identically distributed as σ_A since $h = g_{k^*} \cdot g$. It follows that the entries of σ_A are:

$$\langle i|\sigma_A|j\rangle = \mathop{\mathbf{E}}_{k^* \sim \{0,1\}^\kappa}\left[\frac{g_{k^*}(i) g_{k^*}(j)\, \mathbf{E}_{\mathcal{F}_n}\left[g(i)g(j) \mid f = f_{k^*}\right]}{2^n}\right]. \tag{8}$$

Our strategy for bounding the expected distance between σ_A and τ_A will be to consider the diagonal and off-diagonal entries separately.

Fix $i \ne j$. Recall from Lemma 24 that with probability 1 over A, for all sufficiently large κ, for all $k \in \{0,1\}^\kappa$ and $i \in \{0,1\}^n$, $\left|\hat{f}_k(i)\right| \le \frac{1}{\sqrt{\varepsilon 2^n}}$. This implies that $\mathrm{trnc}\left(\sqrt{\varepsilon 2^n}\hat{f}(i)\right) = \sqrt{\varepsilon 2^n}\hat{f}(i)$ and $\mathrm{trnc}\left(\sqrt{\varepsilon 2^n}\hat{f}(j)\right) = \sqrt{\varepsilon 2^n}\hat{f}(j)$, and therefore:

$$\mathop{\mathbf{E}}_{\mathcal{F}_n}\left[g(i)g(j) \mid f\right] = \varepsilon 2^n \hat{f}(i)\hat{f}(j). \tag{9}$$

By substituting (9) into (8) and comparing with (7), it follows that $\langle i|\sigma_A|j\rangle = \varepsilon\langle i|\rho_A|j\rangle = \langle i|\tau_A|j\rangle$ for every $i \ne j$ (i.e. in this case, the off-diagonal entries of σ_A and τ_A are exactly equal). Therefore, with probability 1 over A, for sufficiently large κ we have:

$$\mathrm{TD}(\sigma_A, \tau_A) = \mathrm{TVD}(\mathrm{diag}(\sigma_A), \mathrm{diag}(\tau_A)).$$

We bound this quantity via:

$$\begin{aligned}\mathrm{TVD}(\mathrm{diag}(\sigma_A), \mathrm{diag}(\tau_A)) &= \mathrm{TVD}(\mathrm{diag}(I/2^n), \mathrm{diag}(\tau_A))\\ &= \varepsilon\mathrm{TVD}(\mathrm{diag}(I/2^n), \mathrm{diag}(\rho_A))\\ &= \frac{\varepsilon}{2}\sum_{i \in \{\pm 1\}^n}\left|\frac{1}{2^n} - \mathop{\mathbf{E}}_{k \sim \{0,1\}^\kappa}\left[\hat{f}_k(i)^2\right]\right|\\ &\le \mathrm{negl}(\kappa),\end{aligned}$$

where in the first line we observe that (8) always evaluates to $\frac{1}{2^n}$ on the diagonal, in the second line we use the fact that τ_A is a convex combination of ρ_A and $\frac{I}{2^n}$, in the third line we expand the TVD as a sum, and in the last line we appeal to Lemma 25, which holds with probability 1 over A.

□

We defer the proof of the following corollary to the full version [30].

Corollary 27. *For all* $\mathcal{A}$, $\varepsilon p_1(\mathcal{A}) + (1-\varepsilon)p_3(\mathcal{A}) - p_2(\mathcal{A}) \le \mathrm{negl}(\kappa)$.

This next theorem was essentially proved in [4, Section 4.2], with some minor differences in language and choice of parameters. Most of these differences stem from the fact that [4] considered a decision problem called OR ∘ Forrelation, whereas here we consider a distinguishing task. We defer its proof to the appendix of the full version [30].

Theorem 28. *For all polynomial-time quantum adversaries* $\mathcal{A}$, $p_2(\mathcal{A}) - p_3(\mathcal{A}) \le \mathrm{negl}(\kappa)$.

Corollary 29. *For all polynomial-time quantum adversaries $\mathcal{A}$, $p_1(\mathcal{A}) - p_2(\mathcal{A}) \leq \mathrm{negl}(\kappa)$.*

Proof. Recall from Corollary 27 that

$$\varepsilon p_1(\mathcal{A}) + (1-\varepsilon)\, p_3(\mathcal{A}) - p_2(\mathcal{A}) \leq \mathrm{negl}(\kappa).$$

Adding $(1-\varepsilon)\,(p_2(\mathcal{A}) - p_3(\mathcal{A}))$ to both sides and applying Theorem 28 gives

$$\varepsilon\,(p_1(\mathcal{A}) - p_2(\mathcal{A})) \leq \mathrm{negl}(\kappa).$$

Multiplying through by $\frac{1}{\varepsilon}$ yields

$$p_1(\mathcal{A}) - p_2(\mathcal{A}) \leq \frac{\mathrm{negl}(\kappa)}{\varepsilon} \leq \mathrm{negl}(\kappa),$$

because $\frac{1}{\varepsilon} \leq O(n) \leq \mathrm{poly}(\kappa)$. □

Finally, we prove indistinguishability of the remaining two hybrids.

Claim 30. *For all $\mathcal{A}$, $p_3(\mathcal{A}) = p_4(\mathcal{A})$.*

Proof. Observe that

$$p_3(\mathcal{A}) = \Pr_A\left[\mathcal{A}^{O[A]}\left(1^\kappa, \frac{I}{2^n}\right) = 1\right].$$

To complete the proof, notice that

$$\begin{aligned} p_4(\mathcal{A}) &= \Pr_{A, |\psi\rangle \sim \mu_{\mathrm{Haar}}^n}\left[\mathcal{A}^{O[A]}(1^\kappa, |\psi\rangle) = 1\right] \\ &= \Pr_A\left[\mathcal{A}^{O[A]}\left(1^\kappa, \frac{I}{2^n}\right) = 1\right] \end{aligned}$$

as well, which follows from the fact that

$$\mathop{\mathbf{E}}_{|\psi\rangle \sim \mu_{\mathrm{Haar}}^n}\left[|\psi\rangle\langle\psi|\right] = \frac{I}{2^n}.$$ □

We can now show that the distinguishing advantage of any efficient adversary is negligible when averaged over the random oracle A.

Theorem 31. *Let $\mathcal{A}$ be a polynomial-time quantum adversary. Then:*

$$\mathop{\mathbf{E}}_A\left[\Pr_{k^* \sim \{0,1\}^\kappa}\left[\mathcal{A}^{O[A]}(1^\kappa, |\varphi_{k^*}\rangle) = 1\right] - \Pr_{|\psi\rangle \sim \mu_{\mathrm{Haar}}^n}\left[\mathcal{A}^{O[A]}(1^\kappa, |\psi\rangle) = 1\right]\right]$$
$$\leq \mathrm{negl}(\kappa).$$

Proof. Observe that the quantity that we wish to bound is exactly $p_0(\mathcal{A}) - p_4(\mathcal{A})$. From Claim 23, Corollary 29, Theorem 28, and Claim 30, we know that $p_i(\mathcal{A}) - p_{i+1}(\mathcal{A}) \leq \mathrm{negl}(\kappa)$ for every $i \in \{0,1,2,3\}$. Summing these bounds then gives the desired result. □

Using techniques similar to Yao's distinguisher/predictor lemma [43], this also yields a bound on the absolute advantage of any adversary. The rough idea is that $\mathcal{A}$ can try to guess the sign of its own distinguishing advantage.

Corollary 32. *Let $\mathcal{A}$ be a polynomial-time quantum adversary. Then:*

$$\mathop{\mathbf{E}}_A\left|\Pr_{k^* \sim \{0,1\}^\kappa}\left[\mathcal{A}^{O[A]}(1^\kappa, |\varphi_{k^*}\rangle) = 1\right] - \Pr_{|\psi\rangle \sim \mu_{\mathrm{Haar}}^n}\left[\mathcal{A}^{O[A]}(1^\kappa, |\psi\rangle) = 1\right]\right|$$
$$\leq \mathrm{negl}(\kappa).$$

Proof. We assume that $\mathcal{A}$ outputs a bit in $\{\pm 1\}$. For an oracle A, let

$$a(A) := \Pr_{k^* \sim \{0,1\}^\kappa}\left[\mathcal{A}^{O[A]}(1^\kappa, |\varphi_{k^*}\rangle) = 1\right]$$

and

$$b(A) := \Pr_{|\psi\rangle \sim \mu_{\mathrm{Haar}}^n}\left[\mathcal{A}^{O[A]}(1^\kappa, |\psi\rangle) = 1\right]$$

so that the quantity we need to bound is $\mathbf{E}_A\,|a(A) - b(A)|$. Consider an adversary $\mathcal{B}(1^\kappa, |\psi\rangle)$ that does the following:

(1) Toss a coin $c \in \{\pm 1\}$.
(2) If $c = 1$, then execute $\mathcal{A}\left(1^\kappa, \mathbf{E}_{k \sim \{0,1\}^\kappa}[|\varphi_k\rangle\langle\varphi_k|]\right)$ once and call the output d. Otherwise, if $c = -1$, then execute $\mathcal{A}\left(1^\kappa, \frac{I}{2^n}\right)$ and call the output d.
(3) Output $c \cdot d \cdot \mathcal{A}(1^\kappa, |\psi\rangle)$.

Observe that $\mathcal{B}$ runs in polynomial time. Also note that $c \cdot d$ is sampled to be 1 with probability $\frac{1+a(A)-b(A)}{2}$ and -1 with probability $\frac{1-a(A)+b(A)}{2}$. As a result, we may compute:

$$\begin{aligned} &\mathop{\mathbf{E}}_A\left[\Pr_{k^* \sim \{0,1\}^\kappa}\left[\mathcal{B}^{O[A]}\,(1^\kappa, |\varphi_{k^*}\rangle) = 1\right] - \Pr_{|\psi\rangle \sim \mu_{\mathrm{Haar}}^n}\left[\mathcal{B}^{O[A]}\,(1^\kappa, |\psi\rangle) = 1\right]\right] \\ &\quad = \mathop{\mathbf{E}}_A\left[\Pr[cd = 1]\,(a(A) - b(A)) + \Pr[cd = -1]\,(b(A) - a(A))\right] \\ &\quad = \mathop{\mathbf{E}}_A\left[(a(A) - b(A))^2\right]. \end{aligned} \tag{10}$$

To complete the proof, we bound the quantity:

$$\begin{aligned} \mathop{\mathbf{E}}_A |a(A) - b(A)| &\leq \sqrt{\mathop{\mathbf{E}}_A\left[(a(A) - b(A))^2\right]} \\ &\leq \sqrt{\mathrm{negl}(\kappa)} \\ &\leq \mathrm{negl}(\kappa), \end{aligned}$$

where in the first line we applied Jensen's inequality, and in the second line we substituted (10) and applied Theorem 31. □

Now, we have all of the tools needed to show that $\{|\varphi_k\rangle\}_{k \in \{0,1\}^\kappa}$ is pseudorandom. Due to space constraints, we defer this proof to the full version [30].

6 IMPLICATIONS FOR THE STANDARD MODEL

We now make a few remarks about how the security proof above can be ported to the nonoracular setting. In particular, we argue that our security proof gives a way to instantiate real-world pseudorandom states without assuming the existence of one-way functions. We do so by considering the following security property of a (nonoracular) set of functions $F = \{(f_k, g_k)\}_{k \in \{0,1\}^\kappa}$:

Property 33. *Let $F = \{(f_k, g_k)\}_{k \in \{0,1\}^\kappa}$ be a set of pairs of functions $f_k, g_k : \{\pm 1\}^n \to \{\pm 1\}$ keyed by k, for some $\kappa + 1 \leq n \leq \mathrm{poly}(\kappa)$. We assume F satisfies the following:*

(i) (Efficient computation) For all k, f_k and g_k can be evaluated in time $\mathrm{poly}(\kappa)$.
(ii) (Smoothness of Fourier spectrum of f_k) For all sufficiently large κ, $k \in \{0,1\}^\kappa$, and $i \in \{0,1\}^n$, we have that:

$$\left|\hat{f}_k(i)\right| \leq \frac{1}{\sqrt{\varepsilon 2^n}}, \tag{11}$$

where ε is given in Definition 8. Additionally, we have:

$$\sum_{i\in\{\pm1\}^n}\left|\frac{1}{2^n}-\mathop{\mathbf{E}}_{k\in\{0,1\}^\kappa}\left[\hat{f}_k(i)^2\right]\right|\leq \mathrm{negl}(\kappa). \tag{12}$$

(iii) (Hardness of shifted Forrelation) Let $h\sim\mathcal{H}_\kappa$ denote that we sample h as follows. First, we choose $k\sim\{0,1\}^\kappa$. Then, we sample a function $g:\{\pm1\}^n\to\{\pm1\}$ by sampling $g(x)$ with bias $\sqrt{\varepsilon 2^n}\hat{f}_k(x)$, independently for each $x\in\{\pm1\}^n$. Equivalently, we sample from the conditional probability distribution $g\sim\mathcal{F}_n\mid f=f_k$. Finally, we let $h=g_k\cdot g$.

For any polynomial-time quantum adversary $\mathcal{A}$ with quantum query access to h, we require that:

$$\left|\Pr_{h\sim\mathcal{H}_\kappa}\left[\mathcal{A}^h\left(1^\kappa\right)=1\right]-\Pr_{h:\{\pm1\}^n\to\{\pm1\}}\left[\mathcal{A}^h\left(1^\kappa\right)=1\right]\right|\leq\mathrm{negl}(\kappa). \tag{13}$$

The high level intuition of (iii) is that an efficient quantum algorithm on input a shift function h (via oracle access) cannot approximate the maximum shifted Forrelation value:

$$\max_{k\in\{0,1\}^\kappa}\left|\langle +^n|\Phi_{(f_k,g_k\cdot h)}\rangle\right|;$$

or equivalently, the algorithm is not able to distinguish a uniformly random h from h such that for some k, f_k and $g_k\cdot h$ are noticeably Forrelated.

6.1 Usefulness of Property 33

In light of our proofs in Section 5, we observe that Property 33 simultaneously:

(a) Suffices to construct n-qubit single-copy pseudorandom states,
(b) Holds for a random oracle, and thus plausibly holds for existing cryptographic hash functions like SHA-3, and
(c) Is independent of P vs. NP in the black-box setting.

We briefly sketch why this is the case. To establish (a), we note that the same general hybrid argument suffices to establish the single-copy pseudorandomness of the ensemble

$$\{|\varphi_k\rangle := |\Phi_{(f_k,g_k)}\rangle\}_{k\in\{0,1\}^\kappa},$$

assuming F satisfies Property 33. Consider a sequence of hybrids where in H_1, the adversary receives $|\varphi_k\rangle$ for a random k; in H_2, the adversary receives $|\Phi_h\rangle$ for $h\sim\mathcal{H}_\kappa$; in H_3, the adversary receives $|\Phi_h\rangle$ for a uniformly random h; and in H_4, the adversary receives a Haar-random state $|\psi\rangle$. Then, Item ii of Property 33 serves as a substitute for Lemma 24 and Lemma 25, and implies via the same argument as Lemma 26 that H_2 is statistically indistinguishable from a non-negligible mixture of H_1 and H_3. Item iii of Property 33 implies that H_2 and H_3 are computationally indistinguishable, because $|\Phi_h\rangle$ can be prepared efficiently with a single query to h. Finally, H_3 and H_4 are statistically indistinguishable, just because

$$\mathop{\mathbf{E}}_{|\psi\rangle\sim\mu^n_{\mathrm{Haar}}}\left[|\psi\rangle\langle\psi|\right]=\mathop{\mathbf{E}}_{h:\{\pm1\}^n\to\{\pm1\}}\left[|\Phi_h\rangle\langle\Phi_h|\right]=\frac{I}{2^n},$$

as observed in Claim 30. Together, these imply that H_1 and H_4 are computationally indistinguishable, which proves the pseudorandomness of the ensemble.

On the other hand, (b) and (c) can be established simultaneously by showing that Property 33 holds relative to $\mathcal{O}[A]$, with probability 1 over a random oracle A. This is because A is a sub-oracle of $\mathcal{O}[A]$, so if Property 33 holds relative to $\mathcal{O}[A]$, then it certainly holds relative to A alone, because the functions f_k and g_k depend only on A. Additionally, we know that $\mathsf{P}^A\neq\mathsf{NP}^A$ with probability 1 over A [13], whereas $\mathsf{P}^{\mathcal{O}[A]}=\mathsf{NP}^{\mathcal{O}[A]}$, by Proposition 19.

Item i clearly holds relative to $\mathcal{O}[A]$, by Definition 21, whereas (ii) was shown to hold with probability 1 in Lemma 24 and Lemma 25. Finally, (iii) was essentially established in the proof of Theorem 28 in the full version [30].

6.2 Further Remarks

A few additional comments are in order. First, we emphasize that (iii) is the only computational hardness property assumed in Property 33. Indeed, (ii) is merely a *statistical* property of the functions f_k. Thus, we could gain confidence that (ii) holds for a specific F by verifying on small values of κ, or we might even be able to prove that it holds unconditionally for certain instantiations of F. Furthermore, this statistical property as stated is sufficient but perhaps not necessary for our proofs to go through. For instance, we believe that one could relax (11) to only hold with overwhelming probability over uniformly chosen $k\in\{0,1\}^\kappa$.

One might object that the security property (iii) is impractical and unrealistic, because there is no way to efficiently simulate quantum query access to a random $h\sim\mathcal{H}_\kappa$. In the language of Naor [36] and Gentry and Wichs [21], Property 33 is not *falsifiable*, because the security property cannot (apparently) be modeled as an interactive game between an adversary and an efficient challenger, in which the challenger can decide whether the adversary won the game. However, we emphasize that efficient simulation is not actually necessary for a security property to be useful! Indeed, it is quite common for cryptographic security reductions to proceed via a hybrid argument in which one or more of the hybrids has no efficient simulation, as we have done here. We also note that exactly the same criticism could be leveled against the definition of pseudorandom states itself, because Haar-random quantum states cannot be prepared in polynomial time. And yet, we know that pseudorandom states *are* useful for instantiating a wide variety of cryptographic schemes [6, 28, 33].

7 CONJECTURED MULTI-COPY SECURITY

In this section, we outline a plausible path towards proving that our oracle construction remains secure in the multi-copy case, assuming a strong conjecture about t-Forrelation states. To motivate this conjecture, it will be helpful to identify the step in our proof of single-copy security that breaks down in the multi-copy case. The key step appears to be Lemma 26, which essentially states that the view of the adversary under H_2 is equivalent to a probabilistic mixture of its views under H_1 and H_3. This relies on the fact that, for a given A and k^*, the state $|\Phi_h\rangle$ sampled in H_2 will have $\mathbf{E}_{\mathsf{H}_2}\left[|\langle\Phi_h|\varphi_{k^*}\rangle|\mid A,k^*\right]=\delta$ for some non-negligible δ. Unfortunately, this does not appear to hold in the multi-copy case: the expected overlap between T copies of the states $\mathbf{E}_{\mathsf{H}_2}\left[\left|\langle\Phi_h|^{\otimes T}|\varphi_{k^*}\rangle^{\otimes T}\right|\mid A,k^*\right]$ could be much smaller, typically on the order of δ^T, which can quickly become negligible for $T=\mathrm{poly}(\kappa)$. Thus, the correlation between $|\Phi_h\rangle$ and $|\varphi_{k^*}\rangle$ is too small to directly prove indistinguishability in the multi-copy case.

Note, however, that we have *not* demonstrated multi-copy insecurity of our construction from Section 5. Rather, it just appears that proving multi-copy security would require different ideas.

Our Conjecture. To overcome this issue, we conjecture the existence of "Forrelation-like" distributions with much stronger correlation properties. The formal statement of our conjecture is the following:

Conjecture 34. *For some $t = \mathrm{poly}(n)$, for every t-tuple $G = (g^1, g^2, ..., g^t)$ where $g^i : \{\pm1\}^n \to \{\pm1\}$, there exists a distribution $\mathcal{D}_G$ over t-tuples of functions $F = (f^1, f^2, ..., f^t)$ where $f^i : \{\pm1\}^n \to \{\pm1\}$ such that:*

(i) (AC^0-pseudorandomness) For every $C \in \mathsf{AC}^0[2^{\mathrm{poly}(n)}, O(1)]$,

$$\left|\mathop{\mathbf{E}}_{F\sim\mathcal{D}_G}\left[C\left(\mathrm{tt}(f^1),\mathrm{tt}(f^2),\ldots,\mathrm{tt}(f^t)\right)\right] - \mathop{\mathbf{E}}_{z\sim\{\pm1\}^{t2^n}}[C(z)]\right| \le \mathrm{negl}(n).$$

(ii) (Statistical closeness to $|\Phi_G\rangle$)

$$\mathop{\mathbf{E}}_{F\sim\mathcal{D}_G}\left[\mathrm{TD}(|\Phi_F\rangle, |\Phi_G\rangle)\right] \le \mathrm{negl}(n).$$

(iii) (Compound distribution is uniform) If G is a uniformly random t-tuple of functions, then sampling $F \sim \mathcal{D}_G$ yields a uniformly random t-tuple of functions (averaged over G).

To provide some intuition, we state a weaker conjecture that is implied by Conjecture 34, and that is more directly comparable to the currently known properties of the Forrelation distribution. Note, however, that we only know how to prove multi-copy security assuming the stronger Conjecture 34; it is not clear whether the weaker conjecture below suffices.

Conjecture 35. *For some $t = \mathrm{poly}(n)$, there exists a distribution $\mathcal{D}$ over t-tuples of functions $F = (f^1, f^2, ..., f^t)$ where $f^i : \{\pm1\}^n \to \{\pm1\}$ such that:*

(i) (AC^0-pseudorandomness) For every $C \in \mathsf{AC}^0[2^{\mathrm{poly}(n)}, O(1)]$,

$$\left|\mathop{\mathbf{E}}_{F\sim\mathcal{D}}\left[C\left(\mathrm{tt}(f^1),\mathrm{tt}(f^2),\ldots,\mathrm{tt}(f^t)\right)\right] - \mathop{\mathbf{E}}_{z\sim\{\pm1\}^{t2^n}}[C(z)]\right| \le \mathrm{negl}(n).$$

(ii) (Statistical closeness to $|+^n\rangle$)

$$\mathop{\mathbf{E}}_{F\sim\mathcal{D}}\left[\langle +^n|\Phi_F\rangle\right] \ge 1 - \mathrm{negl}(n).$$

In plain words, Conjecture 35 posits the existence of a distribution that is pseudorandom against AC^0, and that samples *highly t-Forrelated* functions with high probability. If we compare to what is known about the $t = 2$ case, we know by Theorem 9 that the Forrelation distribution $\mathcal{F}_n$ is also pseudorandom against AC^0. However, $\mathcal{F}_n$ only samples functions that are *weakly Forrelated*, i.e. $\mathbf{E}_{F\sim\mathcal{F}_n}[\langle +^n|\Phi_F\rangle] = \delta$ for some non-negligible δ, rather than a δ that is close to 1. For values of $t > 2$, the current state of the art for t-fold Forrelation [9] gives a distribution over t-tuples of functions that is pseudorandom against AC^0 circuits (in fact, the pseudorandomness parameter is $2^{-\Omega(nt)}$ as opposed to $\mathrm{negl}(n)$), however the expected overlap of $|\Phi_F\rangle$ with the $|+^n\rangle$ state is roughly $2^{-\Omega(t)}$ which is not sufficient for our purposes.

We expect that it may be necessary to choose t to be some large polynomial, say $t = n^2$, in order for either Conjecture 34 or Conjecture 35 to hold. The reason is that, for small t, there could be very few Fs for which $|\Phi_F\rangle$ has large overlap with the $|+^n\rangle$ state, and so it might not be possible for a distribution over such Fs to also be pseudorandom against AC^0. In more technical terms, a counting argument suggests that random 2-Forrelation states would not form an ε-net to the set of n-qubit states with real amplitudes, at least not for small ε. However, for larger t, it seems plausible that t-Forrelation states could form an ε-net for some exponentially small ε, and proving this might be a useful first step towards establishing either of our two conjectures.

Due to space constraints, we defer a proof that Conjecture 34 implies the multi-copy security of $\{|\varphi_k\rangle\}_{k\in\{0,1\}^\kappa}$ to the full version of this text [30].

ACKNOWLEDGMENTS

We thank Scott Aaronson, Chinmay Nirkhe, and Henry Yuen for insightful discussions. Part of this work was done while the authors attended the 2022 Extended Reunion for the Quantum Wave in Computing at the Simons Institute for the Theory of Computing. WK is supported by an NDSEG Fellowship. LQ is supported by DARPA under Agreement No. HR00112020023. MS is supported by a Simons-Berkeley Postdoctoral Fellowship. AT is supported by a Sloan Research Fellowship and NSF CAREER Award CCF-2145474.

REFERENCES

[1] Scott Aaronson. 2009. On Perfect Completeness for QMA. *Quantum Info. Comput.* 9, 1 (jan 2009), 81–89. https://doi.org/10.26421/QIC9.1-2-5

[2] Scott Aaronson. 2010. BQP and the Polynomial Hierarchy. In *Proceedings of the Forty-Second ACM Symposium on Theory of Computing* (Cambridge, Massachusetts, USA) *(STOC '10)*. Association for Computing Machinery, New York, NY, USA, 141–150. https://doi.org/10.1145/1806689.1806711

[3] Scott Aaronson and Andris Ambainis. 2018. Forrelation: A Problem That Optimally Separates Quantum from Classical Computing. *SIAM J. Comput.* 47, 3 (2018), 982–1038. https://doi.org/10.1137/15M1050902

[4] Scott Aaronson, DeVon Ingram, and William Kretschmer. 2022. The Acrobatics of BQP. In *37th Computational Complexity Conference (CCC 2022) (Leibniz International Proceedings in Informatics (LIPIcs), Vol. 234)*, Shachar Lovett (Ed.). Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl, Germany, 20:1–20:17. https://doi.org/10.4230/LIPIcs.CCC.2022.20

[5] Scott Aaronson and Greg Kuperberg. 2007. Quantum Versus Classical Proofs and Advice. *Theory of Computing* 3, 7 (2007), 129–157. https://doi.org/10.4086/toc.2007.v003a007

[6] Prabhanjan Ananth, Luowen Qian, and Henry Yuen. 2022. Cryptography from Pseudorandom Quantum States. In *Advances in Cryptology – CRYPTO 2022 (Lecture Notes in Computer Science, Vol. 13507)*, Yevgeniy Dodis and Thomas Shrimpton (Eds.). Springer International Publishing, 208–236. https://doi.org/10.1007/978-3-031-15802-5_8

[7] Srinivasan Arunachalam, Sergey Bravyi, Arkopal Dutt, and Theodore J. Yoder. 2022. Optimal algorithms for learning quantum phase states. https://doi.org/10.48550/arXiv.2208.07851 arXiv:2208.07851

[8] Theodore Baker, John Gill, and Robert Solovay. 1975. Relativizations of the P=?NP Question. *SIAM J. Comput.* 4, 4 (1975), 431–442. https://doi.org/10.1137/0204037

[9] Nikhil Bansal and Makrand Sinha. 2021. k-Forrelation Optimally Separates Quantum and Classical Query Complexity. In *STOC '21: 53rd Annual ACM SIGACT Symposium on Theory of Computing, Virtual Event, Italy, June 21-25, 2021*, Samir Khuller and Virginia Vassilevska Williams (Eds.). ACM, 1303–1316. https://doi.org/10.1145/3406325.3451040

[10] James Bartusek, Andrea Coladangelo, Dakshita Khurana, and Fermi Ma. 2021. One-Way Functions Imply Secure Computation in a Quantum World. In *Advances in Cryptology – CRYPTO 2021*, Tal Malkin and Chris Peikert (Eds.). Springer International Publishing, Cham, 467–496. https://doi.org/10.1007/978-3-030-84242-0_17

[11] Richard Beigel and Alexis Maciel. 1999. Circuit lower bounds collapse relativized complexity classes. In *Proceedings. Fourteenth Annual IEEE Conference on Computational Complexity (Formerly: Structure in Complexity Theory Conference) (Cat.No.99CB36317)*. 222–226. https://doi.org/10.1109/CCC.1999.766280

[12] Charles H. Bennett and Gilles Brassard. 1984. Quantum cryptography: Public key distribution and coin tossing. In *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*. New York, NY, USA, 8.

[13] Charles H. Bennett and John Gill. 1981. Relative to a Random Oracle A, P^A != NP^A != coNP^A with Probability 1. *SIAM J. Comput.* 10, 1 (1981), 96–113. https://doi.org/10.1137/0210008

[14] Zvika Brakerski, Ran Canetti, and Luowen Qian. 2023. On the Computational Hardness Needed for Quantum Cryptography. In *14th Innovations in Theoretical Computer Science Conference (ITCS 2023) (Leibniz International Proceedings in Informatics (LIPIcs), Vol. 251)*, Yael Tauman Kalai (Ed.). Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl, Germany, 24:1–24:21. https://doi.org/10.4230/LIPIcs.ITCS.2023.24

[15] Zvika Brakerski and Omri Shmueli. 2019. (Pseudo) Random Quantum States with Binary Phase. In *Theory of Cryptography*, Dennis Hofheinz and Alon Rosen (Eds.). Springer International Publishing, Cham, 229–250. https://doi.org/10.1007/978-3-030-36030-6_10

[16] Eshan Chattopadhyay, Pooya Hatami, Kaave Hosseini, and Shachar Lovett. 2019. Pseudorandom Generators from Polarizing Random Walks. *Theory of Computing* 15, 10 (2019), 1–26. https://doi.org/10.4086/toc.2019.v015a010

[17] Eshan Chattopadhyay, Pooya Hatami, Shachar Lovett, and Avishay Tal. 2019. Pseudorandom Generators from the Second Fourier Level and Applications to AC0 with Parity Gates. In *ITCS (LIPIcs, Vol. 124)*. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 22:1–22:15. https://doi.org/10.4230/LIPIcs.ITCS.2019.22

[18] Kai-Min Chung, Siyao Guo, Qipeng Liu, and Luowen Qian. 2020. Tight Quantum Time-Space Tradeoffs for Function Inversion. In *2020 IEEE 61st Annual Symposium on Foundations of Computer Science (FOCS)*. 673–684. https://doi.org/10.1109/FOCS46700.2020.00068

[19] Whitfield Diffie and Martin Hellman. 1976. New directions in cryptography. *IEEE Transactions on Information Theory* 22, 6 (1976), 644–654. https://doi.org/10.1109/TIT.1976.1055638

[20] Merrick Furst, James B. Saxe, and Michael Sipser. 1984. Parity, circuits, and the polynomial-time hierarchy. *Mathematical Systems Theory* 17, 1 (1984), 13–27. https://doi.org/10.1007/BF01744431

[21] Craig Gentry and Daniel Wichs. 2011. Separating succinct non-interactive arguments from all falsifiable assumptions. In *Proceedings of the 43rd ACM Symposium on Theory of Computing, STOC 2011, San Jose, CA, USA, 6-8 June 2011*, Lance Fortnow and Salil P. Vadhan (Eds.). ACM, 99–108. https://doi.org/10.1145/1993636.1993651

[22] Oded Goldreich. 1990. A note on computational indistinguishability. *Inform. Process. Lett.* 34, 6 (1990), 277–281. https://doi.org/10.1016/0020-0190(90)90010-U

[23] Alex B. Grilo, Huijia Lin, Fang Song, and Vinod Vaikuntanathan. 2021. Oblivious Transfer Is in MiniQCrypt. In *Advances in Cryptology – EUROCRYPT 2021*, Anne Canteaut and François-Xavier Standaert (Eds.). Springer International Publishing, Cham, 531–561. https://doi.org/10.1007/978-3-030-77886-6_18

[24] Russell Impagliazzo. 1995. A personal view of average-case complexity. In *Proceedings of Structure in Complexity Theory. Tenth Annual IEEE Conference*. 134–147. https://doi.org/10.1109/SCT.1995.514853

[25] Russell Impagliazzo and Michael Luby. 1989. One-way functions are essential for complexity based cryptography. In *30th Annual Symposium on Foundations of Computer Science*. 230–235. https://doi.org/10.1109/SFCS.1989.63483

[26] Russell Impagliazzo and Steven Rudich. 1989. Limits on the Provable Consequences of One-Way Permutations. In *Proceedings of the Twenty-First Annual ACM Symposium on Theory of Computing* (Seattle, Washington, USA) *(STOC '89)*. Association for Computing Machinery, New York, NY, USA, 44–61. https://doi.org/10.1145/73007.73012

[27] Sandy Irani, Anand Natarajan, Chinmay Nirkhe, Sujit Rao, and Henry Yuen. 2022. Quantum Search-To-Decision Reductions and the State Synthesis Problem. In *37th Computational Complexity Conference (CCC 2022) (Leibniz International Proceedings in Informatics (LIPIcs), Vol. 234)*, Shachar Lovett (Ed.). Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl, Germany, 5:1–5:19. https://doi.org/10.4230/LIPIcs.CCC.2022.5

[28] Zhengfeng Ji, Yi-Kai Liu, and Fang Song. 2018. Pseudorandom Quantum States. In *Advances in Cryptology – CRYPTO 2018*, Hovav Shacham and Alexandra Boldyreva (Eds.). Springer International Publishing, Cham, 126–152. https://doi.org/10.1007/978-3-319-96878-0_5

[29] William Kretschmer. 2021. Quantum Pseudorandomness and Classical Complexity. In *16th Conference on the Theory of Quantum Computation, Communication and Cryptography (TQC 2021) (Leibniz International Proceedings in Informatics (LIPIcs), Vol. 197)*, Min-Hsiu Hsieh (Ed.). Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl, Germany, 2:1–2:20. https://doi.org/10.4230/LIPIcs.TQC.2021.2

[30] William Kretschmer, Luowen Qian, Makrand Sinha, and Avishay Tal. 2022. Quantum Cryptography in Algorithmica. https://doi.org/10.48550/arXiv.2212.00879 arXiv:2212.00879

[31] Hoi-Kwong Lo and H. F. Chau. 1997. Is Quantum Bit Commitment Really Possible? *Phys. Rev. Lett.* 78 (Apr 1997), 3410–3413. Issue 17. https://doi.org/10.1103/PhysRevLett.78.3410

[32] Dominic Mayers. 1997. Unconditionally Secure Quantum Bit Commitment is Impossible. *Phys. Rev. Lett.* 78 (Apr 1997), 3414–3417. Issue 17. https://doi.org/10.1103/PhysRevLett.78.3414

[33] Tomoyuki Morimae and Takashi Yamakawa. 2022. Quantum Commitments and Signatures without One-Way Functions. In *Advances in Cryptology – CRYPTO 2022 (Lecture Notes in Computer Science, Vol. 13507)*, Yevgeniy Dodis and Thomas Shrimpton (Eds.). Springer International Publishing, 269–295. https://doi.org/10.1007/978-3-031-15802-5_10

[34] Yoshifumi Nakata, Christoph Hirche, Masato Koashi, and Andreas Winter. 2017. Efficient Quantum Pseudorandomness with Nearly Time-Independent Hamiltonian Dynamics. *Phys. Rev. X* 7 (Apr 2017), 021006. Issue 2. https://doi.org/10.1103/PhysRevX.7.021006

[35] Yoshifumi Nakata, Christoph Hirche, Ciara Morgan, and Andreas Winter. 2017. Unitary 2-designs from random X- and Z-diagonal unitaries. *J. Math. Phys.* 58, 5 (2017), 052203. https://doi.org/10.1063/1.4983266

[36] Moni Naor. 2003. On Cryptographic Assumptions and Challenges. In *Advances in Cryptology - CRYPTO 2003, 23rd Annual International Cryptology Conference, Santa Barbara, California, USA, August 17-21, 2003, Proceedings (Lecture Notes in Computer Science, Vol. 2729)*, Dan Boneh (Ed.). Springer, 96–109. https://doi.org/10.1007/978-3-540-45146-4_6

[37] Ran Raz and Avishay Tal. 2019. Oracle Separation of BQP and PH. In *Proceedings of the 51st Annual ACM SIGACT Symposium on Theory of Computing* (Phoenix, AZ, USA) *(STOC 2019)*. Association for Computing Machinery, New York, NY, USA, 13–23. https://doi.org/10.1145/3313276.3316315

[38] Renato Renner. 2008. Security of Quantum Key Distribution. *International Journal of Quantum Information* 06, 01 (2008), 1–127. https://doi.org/10.1142/S0219749908003256

[39] Avishay Tal. 2017. Tight Bounds on the Fourier Spectrum of AC0. In *32nd Computational Complexity Conference (CCC 2017) (Leibniz International Proceedings in Informatics (LIPIcs), Vol. 79)*, Ryan O'Donnell (Ed.). Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik, Dagstuhl, Germany, 15:1–15:31. https://doi.org/10.4230/LIPIcs.CCC.2017.15

[40] Roman Vershynin. 2018. *High-Dimensional Probability: An Introduction with Applications in Data Science*. Cambridge University Press. https://doi.org/10.1017/9781108231596

[41] Jun Yan. 2022. General Properties of Quantum Bit Commitments (Extended Abstract). In *Advances in Cryptology – ASIACRYPT 2022*, Shweta Agrawal and Dongdai Lin (Eds.). Springer Nature Switzerland, Cham, 628–657. https://doi.org/10.1007/978-3-031-22972-5_22

[42] Jun Yan, Jian Weng, Dongdai Lin, and Yujuan Quan. 2015. Quantum Bit Commitment with Application in Quantum Zero-Knowledge Proof (Extended Abstract). In *Algorithms and Computation*, Khaled Elbassioni and Kazuhisa Makino (Eds.). Springer Berlin Heidelberg, Berlin, Heidelberg, 555–565. https://doi.org/10.1007/978-3-662-48971-0_47

[43] Andrew C. Yao. 1982. Theory and application of trapdoor functions. In *23rd Annual Symposium on Foundations of Computer Science (sfcs 1982)*. 80–91. https://doi.org/10.1109/SFCS.1982.45

Received 2022-11-07; accepted 2023-02-06