Bounded Indistinguishability for Simple Sources

Andrej Bogdanov ✉

Department of Computer Science and Engineering and Institute of Theoretical Computer Science and Communications, The Chinese University of Hong Kong

Krishnamoorthy Dinesh ✉

Institute of Theoretical Computer Science and Communications, The Chinese University of Hong Kong

Yuval Filmus ✉

The Henry and Marylin Taub Faculty of Computer Science, Technion, Israel

Yuval Ishai ✉

The Henry and Marylin Taub Faculty of Computer Science, Technion, Israel

Avi Kaplan ✉

The Henry and Marylin Taub Faculty of Computer Science, Technion, Israel

Akshayaram Srinivasan ✉

School of Technology and Computer Science, Tata Institute of Fundamental Research, Mumbai, India

Abstract

A pair of sources $\boldsymbol{X}, \boldsymbol{Y}$ over $\{0,1\}^n$ are *k-indistinguishable* if their projections to any k coordinates are identically distributed. Can some AC^0 function distinguish between two such sources when k is big, say $k = n^{0.1}$? Braverman's theorem (Commun. ACM 2011) implies a negative answer when $\boldsymbol{X}$ is uniform, whereas Bogdanov et al. (Crypto 2016) observe that this is not the case in general.

We initiate a systematic study of this question for natural classes of *low-complexity* sources, including ones that arise in cryptographic applications, obtaining positive results, negative results, and barriers. In particular:

- There exist $\Omega(\sqrt{n})$-indistinguishable $\boldsymbol{X}, \boldsymbol{Y}$, samplable by degree-$O(\log n)$ polynomial maps (over $\mathbb{F}_2$) and by $\mathsf{poly}(n)$-size decision trees, that are $\Omega(1)$-distinguishable by OR.
- There exists a function f such that all $f(d,\epsilon)$-indistinguishable $\boldsymbol{X}, \boldsymbol{Y}$ that are samplable by degree-d polynomial maps are ϵ-indistinguishable by OR for all sufficiently large n. Moreover, $f(1,\epsilon) = \lceil \log(1/\epsilon) \rceil + 1$ and $f(2,\epsilon) = O(\log^{10}(1/\epsilon))$.
- Extending (weaker versions of) the above negative results to AC^0 distinguishers would require settling a conjecture of Servedio and Viola (ECCC 2012). Concretely, if every pair of $n^{0.9}$-indistinguishable $\boldsymbol{X}, \boldsymbol{Y}$ that are samplable by linear maps is ϵ-indistinguishable by AC^0 circuits, then the binary inner product function can have at most an ϵ-correlation with $\mathsf{AC}^0 \circ \oplus$ circuits.

Finally, we motivate the question and our results by presenting applications of positive results to low-complexity secret sharing and applications of negative results to leakage-resilient cryptography.

2012 ACM Subject Classification Theory of Computation → Computational Complexity and Cryptography; Theory of Computation → Circuit Complexity

Keywords and phrases Pseudorandomness, bounded indistinguishability, complexity of sampling, constant-depth circuits, secret sharing, leakage-resilient cryptography

Digital Object Identifier 10.4230/LIPIcs.CVIT.2016.23

Related Version A full version of the paper is available at [11].

Funding *Andrej Bogdanov*: Supported by Hong Kong Research Grants Council GRF CUHK 14207618 and CUHK 14209419.
Yuval Filmus: Supported by the European Union's Horizon 2020 research and innovation programme under grant agreement No 802020-ERC-HARMONIC.
Yuval Ishai: Supported by ERC Project NTSC (742754), NSF-BSF grant 2015782, BSF grant

2018393, and a grant from the Ministry of Science and Technology, Israel and Department of Science and Technology, Government of India.
Avi Kaplan: Supported by the European Union's Horizon 2020 research and innovation programme under grant agreement No 802020-ERC-HARMONIC, and ERC Project NTSC (742754).

Acknowledgements We thank Chin Ho Lee, Igor Oliveira, Rahul Santhanam, Amir Shpilka, Justin Thaler, and Emanuele Viola for useful feedback. Special thanks go to Chin Ho Lee, who suggested [11, Conjecture 2], and Justin Thaler, who suggested the construction in [11, Appendix A].

1 Introduction

A pair of sources $\boldsymbol{X}, \boldsymbol{Y}$ over $\{0,1\}^n$ are *k-indistinguishable* if their projections to any k coordinates are identically distributed. Can some AC^0 function distinguish between two such sources when k is big, say $k = n^{0.1}$? Braverman's theorem [15, 56] implies a negative answer when $\boldsymbol{X}$ is uniform, or equivalently when $\boldsymbol{X}, \boldsymbol{Y}$ are *k-independent*. What about the general case?

The above question was posed by Bogdanov et al. [13], who observed a tight connection[1] (via LP duality) with the *approximate degree* of the distinguisher. Using this connection, positive answers can be derived from the literature on the approximate degree of AC^0 functions [44, 45, 53, 7, 1, 51, 17, 18, 19, 20, 21, 22, 52]. In particular, there exist $\sqrt{n}$-indistinguishable sources that can be $\Omega(1)$-distinguished by the OR function [43] and $n^{1-\delta}$-indistinguishable sources that can be $\Omega(1)$-distinguished by an AC^0 function for every $\delta > 0$ [22]. On the other hand, upper bounds on approximate degree imply limitations on the indistinguishability threshold k. In particular, the $\sqrt{n}$ threshold for OR distinguishers is known to be asymptotically tight, whereas the $n^{1-\delta}$ threshold for AC^0 distinguishers is only conjectured to be tight.

The study of the bounded indistinguishability question in [13] was motivated by the following "win-win" connection with cryptography. If the answer to the question turns out to be positive, namely there exist k-indistinguishable $\boldsymbol{X}, \boldsymbol{Y}$ that can be distinguished in AC^0, this implies *secret-sharing schemes*[2] where the secret can be reconstructed in AC^0. This is surprising in light of the fact that standard secret-sharing schemes, such as Shamir's scheme [50], use a *linear* function to reconstruct the secret. On the flip side, a negative answer is motivated by the goal of protecting cryptographic applications against leakage of partial information on their internal state. Concretely, in any application that was designed to protect against *local* leakage of k bits, a negative answer implies automatic protection against *global* AC^0 leakage. Such applications abound in the vast literature on secure multiparty computation (MPC), originating from [66, 34, 9, 23], and leakage-resilient circuits, originating from [36]. Braverman's theorem does not apply here because the process of computing on secret-shared data, while respecting k-indistinguishability by design, inevitably creates local dependencies. Obtaining provable resilience to AC^0 leakage turned out to be a challenging task that has led to more intricate constructions and analysis [31, 48, 12].

On the downside, both kinds of "win" come with a caveat. In the secret-sharing application, schemes arising from the approximate degree literature minimize reconstruction complexity

[1] The connection with approximate degree breaks down over non-binary alphabets [13]. Here we restrict the attention to the binary case, which suffices for our motivating applications.

[2] Here we refer to a relaxation of standard threshold secret sharing that allows for a gap between the secrecy and the reconstruction thresholds and for a small error probability. Bogdanov et al. [13] present general techniques for narrowing the gap and making the error probability negligible by increasing the share size, while keeping reconstruction in AC^0.

at the expense of a high *sharing complexity*, of generating the shares. The question of simultaneously minimizing the complexity of sharing and reconstruction remained largely open. For the leakage-resilience application, a general protection even against benign leakage by an OR function (capturing so-called "selective failure" attacks, discussed below) requires $k \gg \sqrt{n}$. Viewing n as the total number of wires in a circuit, existing constructions of leakage-resilient circuits (such as [36]) are far from achieving this k-local secrecy threshold, rendering the generic "security upgrade" guarantee essentially useless in the context of natural applications.

Towards tackling both of the above challenges, we take a more fine-grained view of bounded indistinguishablity, asking the following main question:

Can some AC^0 function distinguish between *simple* k-indistinguishable sources?

To make the question precise, we need to specify a class $\mathcal{F}$ of samplers that define a "simple" source. We also consider distinguisher classes $\mathcal{C}$ that are strict subclasses of AC^0, such as depth 1 (OR) or depth 2 (DNF) distinguishers. Given $\mathcal{F}$ and $\mathcal{C}$, the goal is to understand the achievable tradeoff between the threshold k and the distinguishing advantage ϵ.

Braverman's theorem resolves the analogous question for *k-independent* sources. As k-independent sources can be sampled both linearly and locally, the fooling ability of such sources does not depend on their complexity. In contrast, in this work we demonstrate that the fooling power of k-indistinguishable sources is significantly affected by their complexity.

Useful classes of simple sources. We will be mainly interested in sources that can be sampled by *low-degree* polynomial maps over $\mathbb{F}_2$. Beyond the complexity-theoretic interest in such sources (see, e.g., [46, 29, 30, 10, 39]), they are also motivated by the two kinds of cryptographic applications discussed above. In the context of secret sharing, positive answers for *degree 1* sources (also referred to as linear or affine sources) would give rise to *linear* secret-sharing schemes with AC^0 reconstruction. Linear schemes have the useful feature of supporting local addition of shared secrets. Perhaps more surprisingly, *degree 2* (quadratic) sources are also naturally motivated by cryptographic applications. We observe that many existing MPC protocols from the literature (including the most efficient ones [26]) can be brought to a form where, for every fixed input, the full transcript is a degree 2 function of the randomness. This holds regardless of the complexity of the function being computed. If for quadratic sources we can get negative answers for much smaller values of k than for general sources, this would enable strong leakage-resilience guarantees for natural applications.

We also consider the minimal *depth* and *locality* required for sampling the sources. A positive result from [13] shows that OR can distinguish between a pair of k-indistinguishable AC^0-*samplable* sources. However, a direct implementation of this sampler has depth 9. How low can the depth be? Considering *locality*, can AC^0 distinguish between NC^0-samplable sources? Positive answers to the above questions are motivated by the goal of simultaneously minimizing the complexity of sharing and reconstructing secrets.

Useful classes of distinguishers. As random parity-0 and parity-1 strings are $(n-1)$-wise indistinguishable but samplable by essentially the simplest possible closed-under-projection class $\mathcal{F}$ of linear 2-local sources,[3] it is sensible to restrict attention to distinguisher classes $\mathcal{C}$ that cannot compute parities, such as AC^0 or some subclass of it. The simplest subclasses are depth 1 OR distinguishers (disjunction of a subset of the source bits and their negations) and depth 2 DNF distinguishers. Positive results for OR give rise to *visual* secret-sharing

---

[3] The sampler for parity-b strings of length n is $r_1, r_1 \oplus r_2, \ldots, r_{n-2} \oplus r_{n-1}, r_{n-1} \oplus b$.

schemes [43], where the secret can be reconstructed by overlaying transparencies. Negative results for OR and DNF are motivated by securing computations against *selective failure* attacks, where there are multiple events that can trigger failure and only the existence of failure is leaked to the attacker. Beyond this direct motivation, OR leakage comes up naturally in MPC protocols based on garbled circuits [40, 35]. DNF leakage can capture stronger selective failure attacks. See [13, 12] for further discussion.

1.1 Overview of results

We now give a detailed account of our main results, for the classes of source samplers $\mathcal{F}$ and distinguishers $\mathcal{C}$ discussed above. The results can be classified into three types: positive (distinguishability), negative (indistinguishability), and barriers. They are summarized in Table 1.

Some of our results merely require that one of the sources $\boldsymbol{X}, \boldsymbol{Y}$ be simple and allow the other to be of arbitrary complexity. For given parameters k, ϵ, we say that

- $\mathcal{F}$ *weakly ϵ-fools* $\mathcal{C}$ if for every k-indistinguishable pair $\boldsymbol{X}, \boldsymbol{Y}$ with $\boldsymbol{X} \in \mathcal{F}$ *and* $\boldsymbol{Y} \in \mathcal{F}$ and every $C \in \mathcal{C}$, $|\Pr[C(\boldsymbol{X}) = 1] - \Pr[C(\boldsymbol{Y}) = 1]| \leq \epsilon$. We refer to this as $\mathsf{MAIN}(k, \epsilon)$.
- $\mathcal{F}$ *strongly ϵ-fools* $\mathcal{C}$ if for every k-indistinguishable pair $\boldsymbol{X}, \boldsymbol{Y}$ with $\boldsymbol{X} \in \mathcal{F}$ *or* $\boldsymbol{Y} \in \mathcal{F}$ and every $C \in \mathcal{C}$, $|\Pr[C(\boldsymbol{X}) = 1] - \Pr[C(\boldsymbol{Y}) = 1]| \leq \epsilon$. We refer to this as $\mathsf{GENERAL}(k, \epsilon)$.

In this terminology, Braverman's theorem states that for $k = \mathsf{polylog}(n)$, the uniform distribution strongly $o(1)$-fools AC^0. We say that $\mathcal{C}$ *distinguishes* $\mathcal{F}$ if $\mathcal{F}$ does not fool $\mathcal{C}$.

	Source ($\mathcal{F}$)	Distinguisher ($\mathcal{C}$)	Statement: Result	Statement: Ref.
Positive	Symmetric, AC^0	OR	$\neg\mathsf{MAIN}(\Theta_\epsilon(\sqrt{n}), 1-\epsilon)$	[13]
Positive	Mixture of IID, Poly-size decision trees, Degree $O(\log n)$	OR	$\neg\mathsf{MAIN}(\Theta_\epsilon(\sqrt{n}), 1-\epsilon)$	Theorem 3
Negative	Linear	$O(1)$-local DNF	$\mathsf{GENERAL}(O(\log \frac{1}{\epsilon}), \epsilon)$	
Negative	Degree $O(1)$	OR	$\mathsf{MAIN}(O_\epsilon(1), \epsilon)$	
Negative	Quadratic	Unambiguous DNF	$\mathsf{GENERAL}(\mathsf{poly}(\log \frac{n}{\epsilon}), \epsilon)$	
Negative	Quadratic	OR	$\mathsf{GENERAL}(\mathsf{poly}(\log \frac{1}{\epsilon}), \epsilon)$	
Negative	Depth 1	Arbitrary	$\mathsf{MAIN}(O(\log\log(n/\epsilon)), \epsilon)$	Theorem 1
Barrier	Linear	AC^0	$\mathsf{MAIN}(n/\log n, \epsilon) \Rightarrow \mathsf{IPAP}(\epsilon)$	
Barrier	Linear (LDPC)	AC^0	No NC^0 reduction to k-independence	
Barrier	NC^0	AC^0	$\mathsf{MAIN}(n^{\Omega(1)}, 1/3) \Rightarrow$ [11, Conjecture 7]	

Table 1 Our main results for sources in class $\mathcal{F}$ and distinguishers of type $\mathcal{C}$. A positive result gives a value of k such that there exist $\mathcal{F}$-samplable, k-indistinguishable distributions that are ϵ-distinguished by $\mathcal{C}$. A negative result gives a value of k for which any $\mathcal{F}$-samplable, k-indistinguishable distributions ϵ-fool $\mathcal{C}$. A barrier typically shows that proving a (stronger) negative result would settle a natural conjecture, implying a conditional difficulty to do so. All distinguishers are $\mathsf{poly}(n)$ sized. LDPC refers to uniform distributions over two distinct cosets of a good (linear) low-density parity-check code. Due to space limitations, only a few results are formally stated. The precise statements of negative results appear in [11, Section 6] and barriers in [11, Section 4.2, Section 7.2, Section 8.2].

Positive results. In [11, Section 5] we show the existence of an $O_\epsilon(\sqrt{n})$-indistinguishable pair of sources that are $(1-\epsilon)$-distinguishable by OR and samplable by (a) decision trees of size polynomial in n, and (b) polynomials of degree $O(\log n)$ (Theorem 3) thereby showing that OR ϵ-distinguishes the sources described in (a) as well as in (b). Part (a) improves on the aforementioned result of Bogdanov et al., by weakening the circuit class from AC^0 to decision trees. Moreover, these sources implement an evolving visual secret sharing scheme [38] of very low informational and computational complexities (see [11, Section 5.5]).

Our positive result for degree-$O(\log n)$ sources is obtained by applying a suitable randomized encoding technique [47, 54, 6] to sources sampled by decision trees. In [11, Section 8] we consider other applications of this technique, showing that a (hypothetical) positive result for $o(\log\log n)$-local sources implies a positive result for 4-local sources. We also put forward a natural conjecture ([11, Conjecture 7]) on the complexity of randomized encoding of AC^0 functions that may be viewed as a barrier to negative results.

Negative results. In contrast to Theorem 3, we show that constant-degree sources are indistinguishable by OR (see Table 1):

1. $O(\log(n/\epsilon))$-indistinguishable linear sources strongly ϵ-fool polysize unambiguous DNFs and ORs of $O(1)$-local functions. ([11, Lemma 6.2] + [11, Lemma 6.8])
2. $O(\log^{10}(n/\epsilon))$-indistinguishable quadratic sources strongly ϵ-fool polysize unambiguous DNFs. (Theorem 4 + [11, Lemma 6.8])
3. $O_{d,\epsilon}(1)$-indistinguishable degree-d sources weakly ϵ-fool OR. ([11, Corollary 6.15] + [11, Corollary 6.6.])

In applications to leakage-resilient cryptography, it is desirable to make the adversary's advantage ϵ a negligible function of the instance size n. The first two negative results allow a low indistinguishability parameter k even when ϵ must vanish exponentially with n. In particular, the first result implies that all linear secret-sharing schemes are automatically immune to selective failure attacks (see [13, Section 3.3]). The second result implies the same kinds of immunity for efficient MPC protocols, as it turns out that the joint view of the parties in such protocols can be sampled by quadratic polynomial maps (see [11, Section 9.1]).

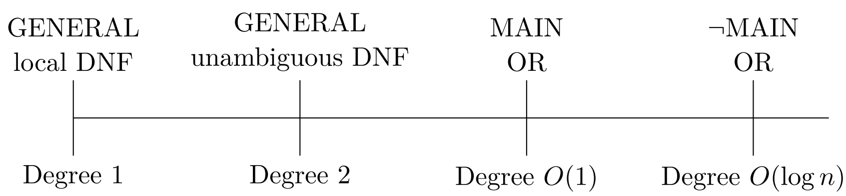


Figure 1 Main results in terms of degree for different classes of distinguishers.

As decision trees can be expressed by depth 2 AND/OR formulas (both CNFs and DNFs) of the same size, our positive result leaves open the fooling power of depth 1 sources. We obtain a strong negative result for such sources (see Figure 2) in Theorem 1 which is as follows:

▶ **Theorem 1.** *If $\boldsymbol{X}, \boldsymbol{Y}$ are two $(\log\log(n/\epsilon)+2)$-indistinguishable depth 1 sources then the statistical distance between $\boldsymbol{X}$ and $\boldsymbol{Y}$ is at most ϵ.*

This result is optimal not only in terms of the depth, but also in terms of the indistinguishability parameter, at least for constant ϵ (see a matching positive result in [11, Lemma 6.39]).

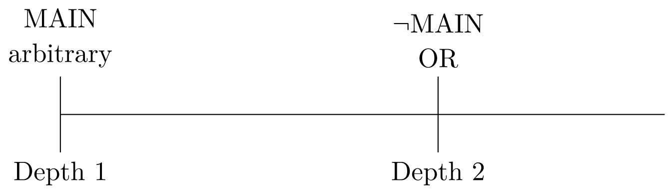


Figure 2 Main results in terms of depth for different classes of distinguishers.

Barriers for linear sources. The basic building block of MPC protocols and other cryptographic applications is *linear* secret sharing. It is thus especially important to understand the consequences of bounded indistinguishability for linear sources. We believe that it is plausible to conjecture the following:

▶ **Conjecture 2.** *k-indistinguishable linear pairs of sources on n bits $o(1)$-fool AC^0 when $k = \mathsf{polylog}(n)$.*

When one of the sources is uniform, this is implied by Braverman's theorem [15, 56]. When the distinguisher is the OR function, it follows from our first negative result. In [11, Section 4.2] we show, however, that proving Conjecture 2 for any $k = o(n/\log n)$ requires first proving the "IPAP conjecture" (Inner Product by AC^0 over Parities) of Servedio and Viola [49], which states that the binary inner product function on n inputs (IP) cannot be computed by $\mathsf{AC}^0 \circ \oplus$ circuits, i.e. bounded-depth AND/OR circuits with a bottom layer of PARITY gates. While a number of partial results have been obtained in support of IPAP [25, 24, 16], it currently remains out of reach.

While IP is known not to be computable by the subclass $\mathsf{DNF} \circ \oplus$ of $\mathsf{AC}^0 \circ \oplus$ [49, 2], its approximability on a constant fraction of inputs remains open [25]. Proving even the special case of Conjecture 2 when the class of distinguishers is restricted to DNFs requires resolving this problem.

One possible approach for making progress on Conjecture 2 (and therefore also IPAP) is to find, for every pair of k-indistinguishable linear sources, an AC^0 reduction that maps them to some pair of *k'-independent* sources. In [11, Section 7.2], we rule out the existence of NC^0 reductions of this type in general. However, in [11, Section 7.1] we give examples of linear NC^0 reductions to bounded independence for specific k-indistinguishable pairs of sources that describe the views of MPC protocols. The results of [12] are also proved via reductions of this type.

The examples in [11, Section 7.1] are related to the study of the complexity of distributions [5, 33, 59, 41, 8, 28, 60, 61, 62, 63, 64], intimately related to the study of extractors [58]. However, this line of study focuses on the complexity of sampling distributions given uniform sources, whereas we allow arbitrary k-independent sources.

On the gap between IPAP and Conjecture 2: predicting parity from parities. While a positive resolution of the IPAP conjecture is necessary to prove Conjecture 2, it is unclear if it is sufficient. Towards bridging this gap, in [11, Section 4.2] we show that Conjecture 2 is implied by $\mathsf{PREDICTION}_\oplus(\mathsf{AC}^0, \Omega(1/n))$, where $\mathsf{PREDICTION}_\oplus(\mathcal{C}, \epsilon)$ is the following statement (see [11, Conjecture 5]):

> A class-$\mathcal{C}$ circuit on n inputs that is given as advice some set S of linear functions of its inputs, under the constraint that no $\mathsf{polylog}(n)$ of the functions in S XOR to the parity of all inputs, cannot predict parity on a $(1+\epsilon)/2$ fraction of inputs.

In the other direction, $\mathsf{PREDICTION}_{\oplus}(\mathsf{AC}^0, \Omega(1))$ implies the average-case IPAP conjecture (see Figure 3). As additional evidence towards Conjecture 2, we prove that $\mathsf{PREDICTION}_{\oplus}(\text{size-}s\ \mathsf{DNF}, 1 - \Omega(1/s))$ holds for $s = \mathsf{poly}(n)$, thereby strengthening a result of Cohen and Shinkar [25] (see [11, Corollary 4.6]).

To give a bit more intuition on the distinction between Conjecture 2 and the IPAP conjecture: Refuting Conjecture 2 is equivalent to showing that some (polynomial-length) $\mathbb{F}_2$-linear encoding of n input bits can be used by an AC^0 circuit to nontrivially predict the parity of *some* subset of these bits. (Here "nontrivially" means that the target parity is not spanned by polylogarithmically many outputs of the encoding.) In contrast, refuting the IPAP conjecture requires proving the existence of a single encoding as above that enables AC^0 circuits to predict the parity of *every* subset. The equivalence between the two conjectures is open even if we replace "predict" by "exactly compute."

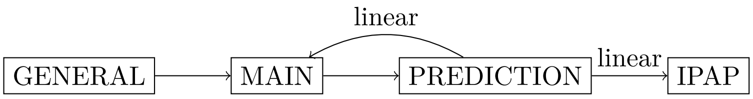


Figure 3 Relations between indistinguishability, prediction, and the IPAP conjecture.

Applications to leakage-resilient cryptography. We already discussed applications to low-complexity secret sharing. In [11, Section 9] we consider applications to *leakage-resilient circuit compilers* (LRCC) [36], which protect sensitive computations against leakage from the internal wires of the computation. More concretely, an LRCC transforms a circuit C into a randomized circuit $\widehat{C}$ mapping an encoded input to an encoded output, such that revealing the output of a leakage function applied to wires of $\widehat{C}$ reveals essentially nothing about the input. Much of the work in this area focuses on obtaining efficient constructions for *local* leakage, confined to a small subset of k wires. Following [42], Faust et al. [31] considered the global leakage model where the leakage function acts on all the wires but is restricted to a low complexity class such as AC^0. LRCC constructions in this model, such as those of Rothblum [48] and Bogdanov et al. [12], are complex to analyze and incur a significant overhead, compiling a circuit C to $\widehat{C}$ of size $\tilde{O}(\lambda^2|C|)$ for a security error parameter $2^{-\lambda}$. In contrast, the best known LRCC constructions in the local leakage model based on efficient MPC protocols [27, 26] can be quite efficient and only incur a polylogarithmic overhead in the local leakage parameter k. A natural question is whether this gap is inherent.

We show that one can bridge the efficiency gap between the local leakage and the global leakage models assuming our main conjecture holds for *quadratic* sources. Specifically, assuming this conjecture, we give a construction of LRCC against AC^0 circuits with $|\widehat{C}| = |C| \cdot \mathsf{polylog}(\lambda)$ (plus additive terms that only depend on the depth of C). As an additional application, we use the same conjecture for *linear* sources to show that a construction of LRCC from [36, 12] for the class of circuits that only contain XOR gates satisfies a stronger security property. Namely, we show that security against AC^0 leakage is retained even when the output decoder is not implemented by a trusted hardware. We also show how to improve the efficiency of this construction by relying on a high-rate variant of Shamir's secret-sharing scheme [32].

Summary of unconditional applications. While several of the cryptographic applications presented in this work depend on unproven conjectures, others can be based on theorems we prove unconditionally. For convenience, we summarize applications of the latter kind below.

- Low-complexity secret sharing. Our positive results imply secret-sharing schemes with secrecy threshold $k = \Omega(\sqrt{n})$, reconstruction by OR[4] (with small constant error probability), and sharing by (depth-2) polynomial-size decision trees or degree-$O(\log n)$ $\mathbb{F}_2$-polynomials ([11, Section 5.2] and [11, Section 5.3] respectively). This improves over similar results in [13] in which sharing is done by higher depth AC^0 circuits. We show that our schemes are depth-optimal by ruling out similar schemes with *depth-1* sharing. Concretely, we show that the highest achievable secrecy threshold for schemes with depth-1 sharing is $k = \Theta(\log \log n)$ (see [11, Section 6.5]). Finally, our results imply the first *evolving* visual secret-sharing scheme in the sense of [38] (see [11, Section 5.5]).

- Leakage-resilient cryptography. Our negative results imply that k-indistinguishability of degree-1 or degree-2 sources with $k \geq \mathsf{polylog}(n)$ suffices for protecting against low-depth leakage classes, including depth-1 AC^0 and unambiguous DNF. The latter capture natural kinds of selective failure attacks. We further show that degree-2 sources suffice in the context of efficient leakage-resilient circuit compilers. In particular, all of the applications discussed above and in [11, Section 9] apply unconditionally to leakage by depth-1 AC^0 and unambiguous DNF.

1.2 Open questions

Our results suggest many open questions. We would like to single out the following.

▶ **Open Question 1.** What is the smallest possible degree d for which there are $\Theta(\sqrt{n})$-indistinguishable degree d sources which OR can $\Omega(1)$-distinguish?

Our results show that $d = \omega(1)$ and $d = O(\log n)$.

▶ **Open Question 2.** Are the GENERAL and MAIN conjectures equivalent? Is the PREDICTION conjecture for linear sources implied by IPAP?

We are mainly interested in the case of AC^0 distinguishers. GENERAL trivially implies MAIN, and PREDICTION for linear sources implies IPAP, so the open question is asking for the converse directions. We are able to show that MAIN and PREDICTION are equivalent for linear sources (for general sources, we only know that MAIN implies PREDICTION). A positive answer to the latter question roughly amounts to showing that if linear preprocessing can help AC^0 circuits nontrivially predict *some* parity of n bits then there is universal linear preprocessing that helps predict *all* parities. This implication is open even for exact computation.

▶ **Open Question 3.** Is there a pair of $n^{\Omega(1)}$-indistinguishable sources, samplable in NC^0, which can be $\Omega(1)$-distinguished in AC^0?

A positive answer would imply an extreme form of low-complexity secret sharing, where secrets are shared by NC^0 circuits and reconstructed by AC^0 circuits. Our positive results imply weaker secret-sharing schemes with sharing by polynomial-size decision trees. In [11, Section 8] we show that a negative answer to the question would imply a natural conjecture on low-complexity randomized encodings of functions. Another reason why settling Open Question 3 in the negative may be challenging is the difficulty of ruling out local sampling (up to a small statistical error) even for some simple and explicit distributions [63].

[4] Alternatively, allowing AC^0 reconstruction, an amplification technique from [13] can be used to obtain near-threshold schemes with negligible reconstruction error and the same sharing complexity.

2 Technical Overview of Our Results

In this section we outline the proofs of some of our main results. For a detailed discussion, see the full version [11]. In Section 2.1 we describe our construction of $\Omega(\sqrt{n})$-indistinguishable sources that are samplable by sources of degree $O(\log n)$ and are $\Omega(1)$-distinguished by OR. In Section 2.2 we describe our various indistinguishability results. Finally, in Section 2.3 we outline the proof of the equivalence of MAIN and PREDICTION for linear sources, and the proof that LDPC sources cannot be reduced to bounded independence using local maps.

2.1 OR can distinguish logarithmic degree sources

Bogdanov et al. [13] showed that there exists a pair $\boldsymbol{X}, \boldsymbol{Y}$ of $\sqrt{n}$-indistinguishable sources over $\{0,1\}^n$ which OR distinguishes, by appealing to LP duality. Explicit constructions appear in other works, for example Špalek [55] and Bun and Thaler [17]. However, except for a construction of AC^0-sampleable sources from [13], the corresponding distributions do not satisfy natural notions of computational simplicity. As our first result, we show how to reduce $\boldsymbol{X}, \boldsymbol{Y}$ to sources samplable by polynomial size decision trees, as well as to sources of degree $O_\epsilon(\log n)$, proving the following.

▶ **Theorem 3.** **(a)** *For any $\epsilon > 0$ there exists a pair $\boldsymbol{X}, \boldsymbol{Y}$ of $\Theta_\epsilon(\sqrt{n})$-indistinguishable sources over $\{0,1\}^n$ samplable by decision trees of size $O_\epsilon(n^3 \log^2 n)$ that the OR function $\mathsf{OR}(x) = x_1 \vee \cdots \vee x_n$ can $(1-\epsilon)$-distinguish.* **(b)** *For any $\epsilon > 0$ there exists a pair $\boldsymbol{X}, \boldsymbol{Y}$ of $\Theta_\epsilon(\sqrt{n})$-indistinguishable sources over $\{0,1\}^n$ of degree $O_\epsilon(\log n)$ that the OR function $\mathsf{OR}(x) = x_1 \vee \cdots \vee x_n$ can $(1-\epsilon)$-distinguish.*

We convert an arbitrary pair of $\sqrt{n}$-indistinguishable distributions which OR can distinguish into a similar pair samplable by simple sources using a sequence of reductions:

Arbitrary sources $\Longrightarrow$ *Mixtures of iid* $\Longrightarrow$ *Decision trees* $\Longrightarrow$ $O(\log n)$ *degree*

Each of these reductions preserves indistinguishability (possibly modifying n) while having only a small effect on the distinguishing advantage of OR.

Mixtures of i.i.d. A distribution on $\{0,1\}^n$ is a *mixture of iid* if we can sample it using a two-step process:

1. Sample a bias $p \in [0,1]$ according to some distribution on $[0,1]$.
2. Sample n iid bits with bias p.

Given an arbitrary source $\boldsymbol{X}_0$ over $\{0,1\}^m$, we construct a mixture of iid $\boldsymbol{X}_1$ using *erase-all-subscripts symmetrization* [21]: Sample $x \sim \boldsymbol{X}_0$, and then sample n uniform bits chosen from x.

If $\boldsymbol{X}_0, \boldsymbol{Y}_0$ are k-indistinguishable and we construct $\boldsymbol{X}_1, \boldsymbol{Y}_1$ in this fashion, then $\boldsymbol{X}_1, \boldsymbol{Y}_1$ are still k-indistinguishable. If $\boldsymbol{X}_0, \boldsymbol{Y}_0$ are ϵ-distinguished by OR then this means that $|\Pr[\boldsymbol{X}_0 = \mathbf{0}] - \Pr[\boldsymbol{Y}_0 = \mathbf{0}]| \geq \epsilon$. Since

$$\Pr[\boldsymbol{X}_0 = \mathbf{0}] \leq \Pr[\boldsymbol{X}_1 = \mathbf{0}] \leq \Pr[\boldsymbol{X}_0 = \mathbf{0}] + \left(1 - \frac{1}{m}\right)^n,$$

if we choose $n = \Theta(m \log(1/\epsilon))$ then $\boldsymbol{X}_1, \boldsymbol{Y}_1$ are $\Omega(\epsilon)$-distinguished by OR. We can choose $\boldsymbol{X}_0, \boldsymbol{Y}_0$ to be k-indistinguishable for $k = \Theta(\sqrt{m}) = \Theta(\sqrt{n})$.

Decision trees The next step is to show that we can approximately sample $\boldsymbol{X}_1, \boldsymbol{Y}_1$ using decision trees whose randomness derives from a supply of unbiased random bits. If we had access to biased random bits, then this would be immediate, and we can simulate biased random bits using unbiased random bits with some small failure probability. In order to maintain k-indistinguishability, in case of failure we output the constant vector $\mathbf{0}$. In this way we construct a pair of sources $\boldsymbol{X}_2, \boldsymbol{Y}_2$ which are k-indistinguishable and are $\Omega(\epsilon)$-distinguished by OR.

How large are the decision trees used to sample $\boldsymbol{X}_2, \boldsymbol{Y}_2$? This depends both on the failure probability and on the *complexity* of $\boldsymbol{X}_1, \boldsymbol{Y}_1$, as measured in the bit complexity of the probabilities used to define these mixtures of iid. Taking a close look at the construction of Bun and Thaler [17], we show that if we use it as our starting point $\boldsymbol{X}_0, \boldsymbol{Y}_0$ then the resulting $\boldsymbol{X}_1, \boldsymbol{Y}_1$ are low complexity, and so $\boldsymbol{X}_2, \boldsymbol{Y}_2$ are samplable using polynomial size decision trees for any constant failure probability.

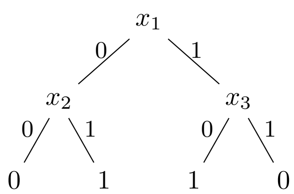
Logarithmic degree The final step is converting $\boldsymbol{X}_2, \boldsymbol{Y}_2$ to a pair of distributions $\boldsymbol{X}_3, \boldsymbol{Y}_3$ samplable by sources of degree $O(\log n)$. The idea is to used a *randomized encoding* inspired by the Razborov–Smolensky [47, 54] lower bound technique. (See [11, Section 8] for a more general perspective using the randomized encoding framework of [6].)

Razborov and Smolensky approximate the AND function on ℓ bits to error 2^{-d} using the degree-d $\mathbb{F}_2$ polynomial

$$\prod_{i=1}^{d} \left(1 + \sum_{j=1}^{\ell} r_{i,j}(1 + x_j)\right).$$

Here $x_1, \ldots, x_\ell$ are the inputs, and $r_{i,j}$ are random bits. When $x_1 = \cdots = x_\ell = 1$, this expression always equals 1, and otherwise each factor is a random bit, and so the expression equals 0 with probability $1 - 2^{-d}$.

A decision tree can be written as an "unambiguous" sum of conjunctions, that is, at most one conjunction can be true. For example, the decision tree



can be expressed as

$$(1 - x_1)(1 - x_3) + x_1 x_2.$$

We have one conjunction per leaf labeled 1, and the conjunction corresponds to the path leading to the leaf.

We convert the decision tree into a polynomial by replacing each conjunction with its Razborov–Smolensky encoding. If the decision tree has size s then we need the error to be $O(\epsilon/s)$, and so the resulting degree is $\log(s/\epsilon)$. When s is polynomial, this is $O(\log(n/\epsilon))$.

We note that when attempting to apply the Razborov–Smolensky encoding to a general AC^0 circuit, rather than a decision tree or an unambiguous DNF, not only does the degree of the encoding grow to $\mathsf{polylog}(n)$, but there is also an encoding *privacy error*. The latter results in an approximate notion of k-indistinguishability in which the k-projections have $2^{-\mathsf{polylog}(n)}$ statistical distance. This relaxed notion, studied in [14], is qualitatively weaker than the perfect notion we consider in this work. In particular, it may totally break down when the projection set is chosen in an adaptive fashion. See [11, Section 8] for more details.

2.2 Fooling OR and DNFs

In this section we describe our various negative results, as described in Table 1. Most of these results are proved via the notion of *predictability*, which we first explain. We then briefly outline the proofs of the remaining negative results.

2.2.1 Predictability

Let $\boldsymbol{X}$ be a source over $\{0,1\}^n$. We say that a subset S of coordinates *ϵ-predicts* $\boldsymbol{X}$ if

$$\Pr[\boldsymbol{X}|_S = 0 \text{ and } \boldsymbol{X} \neq 0] \leq \epsilon.$$

Roughly speaking, this means that in order to know the value of OR on $\boldsymbol{X}$, it suffices to peek at the coordinates in S.

If $\boldsymbol{X}, \boldsymbol{Y}$ are each ϵ-predicted by a subset of k coordinates, then the union of the two subsets ϵ-predicts both sources. Hence if $\boldsymbol{X}, \boldsymbol{Y}$ are $2k$-indistinguishable, then they ϵ-fool OR.

A more surprising observation is that if $\boldsymbol{Y}$ is ϵ/n-predicted by a subset S of k coordinates and $\boldsymbol{X}, \boldsymbol{Y}$ are $(k+1)$-indistinguishable, then S also ϵ-predicts $\boldsymbol{X}$; this is because for any coordinate $i \notin S$,

$$\Pr[\boldsymbol{Y}|_S = 0 \text{ and } \boldsymbol{Y}_i \neq 0] \leq \frac{\epsilon}{n}.$$

Accordingly, we define two notions of predictability for classes of sources:

- $\mathcal{F}$ is *weakly predictable* if for every $\epsilon > 0$, any source from $\mathcal{F}$ is ϵ-predicted by a subset of $C(\epsilon)$ coordinates.
- $\mathcal{F}$ is *strongly predictable* if for every $\epsilon > 0$, any source from $\mathcal{F}$ is ϵ-predicted by a subset of $\mathsf{polylog}(1/\epsilon)$ coordinates.

Strongly predictable sources in fact fool not only OR, but also *unambiguous DNFs*. An unambiguous DNF is a disjunction of conjunctions, with the promise that no two conjunctions can be satisfied simultaneously. As explained in Section 2.1, a decision tree of size s can be converted to an unambiguous disjunction of at most s conjunctions. Writing the unambiguous DNF as a sum of ANDs (over the reals!), it suffices to (ϵ/s)-fool each AND in order to ϵ-fool the entire DNF. Consequently (since fooling ANDs and ORs is the same), $\mathsf{polylog}(ns/\epsilon)$-indistinguishable sources ϵ-fool unambiguous DNFs as long as one of the sources belongs to a strongly predictable class of sources which is closed under input negation.

2.2.2 Applying predictability

Our main results are:

- Constant degree sources are weakly predictable. This also includes sources of constant locality.
- Quadratic sources (i.e., degree 2 sources) are strongly predictable.

We also show that linear sources fool *local DNFs*, which are disjunctions of local functions. The proof is very similar to the proof that local sources fool OR, and so we do not describe it here.

Linear sources. We prove predictability using the structure vs randomness paradigm. As an example, consider the class of linear sources, in which each output bit is an affine combination of input bits. For ease of exposition, we consider the special case in which each output bit is a *linear* combination of inputs bits (i.e., we disallow $x_1 = r_1 \oplus r_2 \oplus 1$). We will show that every linear source $\boldsymbol{X}$ is ϵ-predicted by a subset of $\log(1/\epsilon)$ coordinates.

The source $\boldsymbol{X}$ is *pseudorandom* if it has rank at least $\log(1/\epsilon)$. In this case, any subset S of $\log(1/\epsilon)$ linearly independent coordinates ϵ-predicts $\boldsymbol{X}$, since $\Pr[\boldsymbol{X}|_S = 0] \leq \epsilon$.

The source $\boldsymbol{X}$ is *structured* if it has rank at most $\log(1/\epsilon)$. In this case, we choose a subset S such that $\{\boldsymbol{X}_i\}_{i \in S}$ spans $\boldsymbol{X}_1, \ldots, \boldsymbol{X}_n$. This subset 0-predicts $\boldsymbol{X}$ since if $\boldsymbol{X}|_S = 0$ then $\boldsymbol{X} = 0$.

Local sources. A more sophisticated example is that of s-local sources, that is, sources where every output bit $\boldsymbol{X}_i$ depends on at most s input bits, forming a set J_i. Suppose that we are given such a source $\boldsymbol{X}$.

The source $\boldsymbol{X}$ is *pseudorandom* if we can find $2^s \log(1/\epsilon)$ coordinates which depend on disjoint sets of inputs. A short calculation shows that the probability that all these coordinates equal zero is at most ϵ.

Otherwise, the source $\boldsymbol{X}$ is *structured*: we can find a "hitting set" T of size $s2^s \log(1/\epsilon)$ for $J_1, \ldots, J_n$. For each setting of the input bits in T, the source simplifies to an $(s-1)$-local source, and we can find an ϵ-predicting set by induction. Putting all of these sets together, we obtain an ϵ-predicting set for the original source.

A very similar argument appears in work of Trevisan [57], in the context of deterministic approximate counting of solutions to k-CNFs, and in recent work of Akmal and Williams [3], in the context of threshold counting of solutions to k-CNFs. See Williams [65] for deterministic approximate counting of solutions to systems of polynomial equations, a topic related to our next example, constant degree sources.

Constant-degree sources. We handle degree d sources using a similar argument. We need to find a pseudorandomness condition for a set S of coordinates which will guarantee that $\Pr[\boldsymbol{X}|_S = 0] \leq \epsilon$. Such a condition is supplied by higher-order Fourier analysis: if all linear combinations of $\{\boldsymbol{X}_i\}_{i \in S}$ have high *rank* (a notion we explain below) and S is large enough, then $\Pr[\boldsymbol{X}|_S = 0] \leq \epsilon$ (pseudorandom case).

Otherwise (structured case), we choose a maximal set T such that all linear combinations of $\{\boldsymbol{X}_i\}_{i \in T}$ have high rank. By the definition of rank, this implies that each $i \notin T$ simplifies, modulo $\{\boldsymbol{X}_i\}_{i \in T}$, to a function depending on a bounded number of degree $d-1$ polynomials, and we can complete the proof by induction.

Quadratic sources. The arguments for local sources and for constant degree sources result in a very bad dependence between ϵ and the size $C(\epsilon)$ of the ϵ-fooling subset of coordinates. In the case of quadratic sources, we are able to use Dickson's structure theorem for quadratic polynomials, via a series of careful reductions, to obtain the much better dependence $C(\epsilon) = O(\log^{10}(1/\epsilon))$.

▶ **Theorem 4.** *The class of quadratic sources is $(O(\log^{10}(1/\epsilon)), \epsilon)$-predictable.*

2.2.3 Other negative results

We prove two other negative results: the prediction variant holds for linear sources and DNF distinguishers, and depth 1 sources fool arbitrary distinguishers.

PREDICTION **holds for linear sources and DNF distinguishers.** Given a DNF ϕ and a linear source $\boldsymbol{X}$, our goal is to show that if no k coordinates of $\boldsymbol{X}$ span some target parity π, then ϕ cannot compute π, even with a small error.

If T is any term of ϕ, then the probability that T is satisfied is $2^{-\operatorname{rank}(T)}$, where the rank of T is the rank of the span of the corresponding coordinates of $\boldsymbol{X}$. If T has large rank then it is unlikely to be satisfied, so we can drop all of these terms, obtaining a narrow DNF ψ.

We now apply Jackson's lemma [37], according to which ψ must correlate with some Fourier character χ_S, where S is a subset of the set of variables appearing in some term of ψ. Since all terms in ψ are narrow and ψ computes π (with small error), this implies that π has nontrivial correlation with, and so is equal to, a linear combination of a small number of coordinates in $\boldsymbol{X}$, which contradicts our initial assumption.

Depth 1 sources fool arbitrary distinguishers. Let $\boldsymbol{X}, \boldsymbol{Y}$ be k-indistinguishable depth 1 sources, that is, each coordinate is an AND or OR of literals. Since we allow arbitrary distinguishers, we can assume that each coordinate is an AND of literals.

Wide conjunctive coordinates are hardly ever 1, so allowing for a small error, we can replace them with constant 0 coordinates. We are left with only narrow coordinates, say of width at most $\log(n/\epsilon)$. Applying a result of Amano et al. [4], if $k = \log\log(n/\epsilon) + 2$ then the two truncated sources are identically distributed, completing the proof.

2.3 Other results

MAIN and PREDICTION are equivalent for linear sources. To prove the equivalence between [11, Conjecture 9] ($\mathsf{MAIN}_\oplus(\mathsf{AC}^0)$) and $\mathsf{PREDICTION}_\oplus(\mathsf{AC}^0)$, we consider an equivalent formulation of $\mathsf{PREDICTION}_\oplus(\mathsf{AC}^0)$, which we call $\mathsf{COSET}_\oplus(\mathsf{AC}^0)$. This is the special case of $\mathsf{MAIN}_\oplus(\mathsf{AC}^0)$ in which the two k-indistinguishable sources arise from a single source by fixing the first bit of the seed. The resulting sources are uniformly distributed on two cosets of the same linear subspace, hence the name. The equivalence of the two formulations is a simple exercise (see [11, Section 4]).

Two linear sources are k-indistinguishable if they satisfy the same affine constraints of width k or less. This suggests the following strategy for proving $\mathsf{MAIN}_\oplus$ (with parameters k, ϵ) given $\mathsf{COSET}_\oplus$ (with parameters k, δ): Given two k-indistinguishable linear sources $\boldsymbol{X}, \boldsymbol{Y}$, construct the "free k-indistinguishable source" $\boldsymbol{Z}$ given by all affine constraints of width at most k satisfied by $\boldsymbol{X}$. This is the most general linear source which is k-indistinguishable from $\boldsymbol{X}$. Moreover, we obtain exactly the same source if we apply the same construction to $\boldsymbol{Y}$. Therefore it suffices to show that $\boldsymbol{X}, \boldsymbol{Z}$ fool $\mathcal{C}$.

The idea is to construct a sequence of hybrids $\boldsymbol{Z}_0, \ldots, \boldsymbol{Z}_t$, where $\boldsymbol{Z}_0 = \boldsymbol{Z}$, $\boldsymbol{Z}_t = \boldsymbol{X}$, and $\boldsymbol{Z}_{i+1}$ is obtained from $\boldsymbol{Z}_i$ by imposing one more affine constraint. We can also define $\boldsymbol{W}_{i+1}$ in the same way, by imposing the opposite constraint (for example, $x_1 \oplus x_2 = 1$ rather than $x_1 \oplus x_2 = 0$). By construction, $\boldsymbol{Z}_{i+1}, \boldsymbol{W}_{i+1}$ are cosets, and so $\mathsf{COSET}_\oplus(\mathsf{AC}^0)$ shows that they δ-fool $\mathcal{C}$. On the other hand, $\boldsymbol{Z}_i$ is a $\frac{1}{2}$-$\frac{1}{2}$ mixture of $\boldsymbol{Z}_{i+1}, \boldsymbol{W}_{i+1}$, and so $\boldsymbol{Z}_i, \boldsymbol{Z}_{i+1}$ $\delta/2$-fool $\mathcal{C}$.

In total, $\boldsymbol{X}, \boldsymbol{Z}$ $t\delta/2$-fool $\mathcal{C}$, and so $\boldsymbol{X}, \boldsymbol{Y}$ $t\delta$-fool $\mathcal{C}$. Clearly $t \le n$, and so it suffices to take $\delta = \epsilon/n$.

LDPC codes cannot be reduced to bounded independence using local maps. An LDPC code is a code whose parity-check matrix is sparse: every message bit appears in exactly D parity checks (this is one of several common definitions). If we choose a $\theta n \times n$ parity-check matrix at random, then the bipartite graph corresponding to the parity-check matrix will be an expander, and so the corresponding code will have linear minimum distance, say at least γn.

A simple sensitivity argument shows that for large n, such a code C cannot be generated using B-local maps from the uniform distribution over m bits: The $n \times m$ binary matrix describing which input bits each output bit depends on contains at most Bn ones, and so there must be some input bit affecting at most Bn/m output bits. Flipping this bit results in flipping at most Bn/m input bits. Since the minimum distance of C is at least γn, this shows that $m \leq B/\gamma$. On the other hand, m must be at least the rate $(1-\theta)n$ of the code, and we obtain a contradiction for $n > B/\gamma(1-\theta)$.

Does the picture change if we are allowed to reduce to an arbitrary k-independent distribution $\boldsymbol{z}$? Let P be the parity-check matrix of C, and let F denote the B-local reduction. Thus $PF(z) = 0$ for all z in the support of $\boldsymbol{z}$. Since every column of P contains D many ones, the average row of P contains D/θ many ones, and so the typical entry of $PF(z)$ depends on at most BD/θ many bits of $\boldsymbol{z}$. If $BD/\theta \ll k$ then the projection of $\boldsymbol{z}$ to these coordinates will have full support due to k-independence, and so $PF(z) = 0$ for *all* z. Thus F also works as a reduction to the uniform distribution, allowing us to apply the earlier lower bound.

References

1. Scott Aaronson and Yaoyun Shi. Quantum lower bounds for the collision and the element distinctness problems. *J. ACM*, 51(4):595–605, 2004. doi:10.1145/1008731.1008735.
2. Adi Akavia, Andrej Bogdanov, Siyao Guo, Akshay Kamath, and Alon Rosen. Candidate weak pseudorandom functions in $\mathsf{AC}^0 \circ \mathsf{MOD}_2$. In *Innovations in Theoretical Computer Science, ITCS'14, Princeton, NJ, USA, January 12-14, 2014*, pages 251–260, 2014. doi:10.1145/2554797.2554821.
3. Shyan Akmal and Ryan Williams. Majority-3sat (and related problems) in polynomial time, 2021. arXiv:2107.02748.
4. Kazuyuki Amano, Kazuo Iwama, Akira Maruoka, Kenshi Matsuo, and Akihiro Matsuura. Inclusion-exclusion for k-cnf formulas. *Inf. Process. Lett.*, 87(2):111–117, 2003. doi:10.1016/S0020-0190(03)00259-X.
5. A. Ambainis, L.J. Schulman, A. Ta-Shma, U. Vazirani, and A. Wigderson. The quantum communication complexity of sampling. In *Proceedings 39th Annual Symposium on Foundations of Computer Science (Cat. No.98CB36280)*, pages 342–351, 1998. doi:10.1109/SFCS.1998.743480.
6. Benny Applebaum, Yuval Ishai, and Eyal Kushilevitz. Cryptography in NC^0. *SIAM J. Comput.*, 36(4):845–888, 2006.
7. Robert Beals, Harry Buhrman, Richard Cleve, Michele Mosca, and Ronald de Wolf. Quantum lower bounds by polynomials. *J. ACM*, 48(4):778–797, 2001. doi:10.1145/502090.502097.
8. Chris Beck, Russell Impagliazzo, and Shachar Lovett. Large deviation bounds for decision trees and sampling lower bounds for ac0-circuits. In *2012 IEEE 53rd Annual Symposium on Foundations of Computer Science*, pages 101–110, 2012. doi:10.1109/FOCS.2012.82.
9. Michael Ben-Or, Shafi Goldwasser, and Avi Wigderson. Completeness theorems for non-cryptographic fault-tolerant distributed computation (extended abstract). In *Proceedings of the 20th Annual ACM Symposium on Theory of Computing, May 2-4, 1988, Chicago, Illinois, USA*, pages 1–10, 1988. doi:10.1145/62212.62213.
10. Eli Ben-Sasson and Ariel Gabizon. Extractors for polynomial sources over fields of constant order and small characteristic. *Theory Comput.*, 9:665–683, 2013. doi:10.4086/toc.2013.v009a021.
11. Andrej Bogdanov, Krishnamoorthy Dinesh, Yuval Filmus, Yuval Ishai, Avi Kaplan, and Akshayaram Srinivasan. Bounded indistinguishability for simple sources. *Electron. Colloquium Comput. Complex.*, 2021. URL: https://eccc.weizmann.ac.il/report/2021/093.
12. Andrej Bogdanov, Yuval Ishai, and Akshayaram Srinivasan. Unconditionally secure computation against low-complexity leakage. In *Advances in Cryptology - CRYPTO 2019 - 39th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 18-22, 2019, Proceedings, Part II*, volume 11693 of *Lecture Notes in Computer Science*, pages 387–416, 2019. doi:10.1007/978-3-030-26951-7_14.

13 Andrej Bogdanov, Yuval Ishai, Emanuele Viola, and Christopher Williamson. Bounded indistinguishability and the complexity of recovering secrets. In *Advances in Cryptology - CRYPTO 2016 - 36th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 14-18, 2016, Proceedings, Part III*, volume 9816 of *Lecture Notes in Computer Science*, pages 593–618, 2016. doi:10.1007/978-3-662-53015-3_21.

14 Andrej Bogdanov and Christopher Williamson. Approximate bounded indistinguishability. In *44th International Colloquium on Automata, Languages, and Programming (ICALP 2017)*, pages 53:1–53:11, 2017.

15 Mark Braverman. Poly-logarithmic independence fools bounded-depth boolean circuits. *Commun. ACM*, 54(4):108–115, 2011. doi:10.1145/1924421.1924446.

16 Mark Bun, Robin Kothari, and Justin Thaler. Quantum algorithms and approximating polynomials for composed functions with shared inputs. In *Proceedings of the Thirtieth Annual ACM-SIAM Symposium on Discrete Algorithms, SODA 2019, San Diego, California, USA, January 6-9, 2019*, pages 662–678, 2019. doi:10.1137/1.9781611975482.42.

17 Mark Bun and Justin Thaler. Dual lower bounds for approximate degree and markov-bernstein inequalities. In *Automata, Languages, and Programming - 40th International Colloquium, ICALP 2013, Riga, Latvia, July 8-12, 2013, Proceedings, Part I*, volume 7965 of *Lecture Notes in Computer Science*, pages 303–314, 2013. doi:10.1007/978-3-642-39206-1_26.

18 Mark Bun and Justin Thaler. Dual polynomials for collision and element distinctness. *Theory Comput.*, 12:Paper No. 16, 34, 2016. doi:10.4086/toc.2016.v012a016.

19 Mark Bun and Justin Thaler. Approximate degree and the complexity of depth three circuits. In *Approximation, randomization, and combinatorial optimization. Algorithms and techniques*, volume 116 of *LIPIcs. Leibniz Int. Proc. Inform.*, pages Art. No. 35, 18. Schloss Dagstuhl. Leibniz-Zent. Inform., Wadern, 2018.

20 Mark Bun and Justin Thaler. The large-error approximate degree of AC^0. In *Approximation, randomization, and combinatorial optimization. Algorithms and techniques*, volume 145 of *LIPIcs. Leibniz Int. Proc. Inform.*, pages Art. No. 55, 16. Schloss Dagstuhl. Leibniz-Zent. Inform., Wadern, 2019.

21 Mark Bun and Justin Thaler. Guest column: Approximate degree in classical and quantum computing. *SIGACT News*, 51(4):48–72, 2020. doi:10.1145/3444815.3444825.

22 Mark Bun and Justin Thaler. A nearly optimal lower bound on the approximate degree of AC^0. *SIAM J. Comput.*, 49(4), 2020. doi:10.1137/17M1161737.

23 David Chaum, Claude Crépeau, and Ivan Damgård. Multiparty unconditionally secure protocols (extended abstract). In *Proceedings of the 20th Annual ACM Symposium on Theory of Computing, May 2-4, 1988, Chicago, Illinois, USA*, pages 11–19, 1988. doi:10.1145/62212.62214.

24 Mahdi Cheraghchi, Elena Grigorescu, Brendan Juba, Karl Wimmer, and Ning Xie. $\mathsf{AC}^0 \circ \mathsf{MOD}_2$ lower bounds for the boolean inner product. In *43rd International Colloquium on Automata, Languages, and Programming, ICALP 2016, July 11-15, 2016, Rome, Italy*, volume 55 of *LIPIcs*, pages 35:1–35:14, 2016. doi:10.4230/LIPIcs.ICALP.2016.35.

25 Gil Cohen and Igor Shinkar. The complexity of DNF of parities. In *Proceedings of the 2016 ACM Conference on Innovations in Theoretical Computer Science, Cambridge, MA, USA, January 14-16, 2016*, pages 47–58, 2016. doi:10.1145/2840728.2840734.

26 Ivan Damgård, Yuval Ishai, and Mikkel Krøigaard. Perfectly secure multiparty computation and the computational overhead of cryptography. In *Advances in Cryptology - EUROCRYPT 2010, 29th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Monaco / French Riviera, May 30 - June 3, 2010. Proceedings*, volume 6110 of *Lecture Notes in Computer Science*, pages 445–465, 2010. doi:10.1007/978-3-642-13190-5_23.

27 Ivan Damgård and Jesper Buus Nielsen. Scalable and unconditionally secure multiparty computation. In *Advances in Cryptology - CRYPTO 2007, 27th Annual International Cryptology*

Conference, Santa Barbara, CA, USA, August 19-23, 2007, Proceedings, volume 4622 of *Lecture Notes in Computer Science*, pages 572–590, 2007. doi:10.1007/978-3-540-74143-5_32.

28 Anindya De and Thomas Watson. Extractors and lower bounds for locally samplable sources. *ACM Trans. Comput. Theory*, 4(1), March 2012. URL: https://doi-org.ezlibrary.technion.ac.il/10.1145/2141938.2141941, doi:10.1145/2141938.2141941.

29 Zeev Dvir, Ariel Gabizon, and Avi Wigderson. Extractors and rank extractors for polynomial sources. *Comput. Complex.*, 18(1):1–58, 2009. doi:10.1007/s00037-009-0258-4.

30 Zeev Dvir, Dan Gutfreund, Guy N. Rothblum, and Salil P. Vadhan. On approximating the entropy of polynomial mappings. In Bernard Chazelle, editor, *Innovations in Computer Science - ICS 2011, Tsinghua University, Beijing, China, January 7-9, 2011. Proceedings*, pages 460–475. Tsinghua University Press, 2011. URL: http://conference.iiis.tsinghua.edu.cn/ICS2011/content/papers/28.html.

31 Sebastian Faust, Tal Rabin, Leonid Reyzin, Eran Tromer, and Vinod Vaikuntanathan. Protecting circuits from computationally bounded and noisy leakage. *SIAM J. Comput.*, 43(5):1564–1614, 2014. doi:10.1137/120880343.

32 Matthew K. Franklin and Moti Yung. Communication complexity of secure computation (extended abstract). In S. Rao Kosaraju, Mike Fellows, Avi Wigderson, and John A. Ellis, editors, *Proceedings of the 24th Annual ACM Symposium on Theory of Computing, May 4-6, 1992, Victoria, British Columbia, Canada*, pages 699–710. ACM, 1992. doi:10.1145/129712.129780.

33 Oded Goldreich, Shafi Goldwasser, and Asaf Nussboim. On the implementation of huge random objects. *SIAM Journal on Computing*, 39(7):2761–2822, 2010. arXiv:https://doi.org/10.1137/080722771, doi:10.1137/080722771.

34 Oded Goldreich, Silvio Micali, and Avi Wigderson. How to play any mental game or A completeness theorem for protocols with honest majority. In *Proceedings of the 19th Annual ACM Symposium on Theory of Computing, 1987, New York, New York, USA*, pages 218–229, 1987. doi:10.1145/28395.28420.

35 Yuval Ishai, Eyal Kushilevitz, Rafail Ostrovsky, Manoj Prabhakaran, and Amit Sahai. Efficient non-interactive secure computation. In Kenneth G. Paterson, editor, *Advances in Cryptology - EUROCRYPT 2011 - 30th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Tallinn, Estonia, May 15-19, 2011. Proceedings*, volume 6632 of *Lecture Notes in Computer Science*, pages 406–425. Springer, 2011. doi:10.1007/978-3-642-20465-4_23.

36 Yuval Ishai, Amit Sahai, and David A. Wagner. Private circuits: Securing hardware against probing attacks. In Dan Boneh, editor, *Advances in Cryptology - CRYPTO 2003, 23rd Annual International Cryptology Conference, Santa Barbara, California, USA, August 17-21, 2003, Proceedings*, volume 2729 of *Lecture Notes in Computer Science*, pages 463–481. Springer, 2003. doi:10.1007/978-3-540-45146-4_27.

37 Jeffrey C. Jackson. An efficient membership-query algorithm for learning DNF with respect to the uniform distribution. In *35th Annual Symposium on Foundations of Computer Science, Santa Fe, New Mexico, USA, 20-22 November 1994*, pages 42–53, 1994. doi:10.1109/SFCS.1994.365706.

38 Ilan Komargodski, Moni Naor, and Eylon Yogev. How to share a secret, infinitely. In *TCC (B2)*, pages 485–514. Springer, 2016. doi:10.1007/978-3-662-53644-5_19.

39 Xin Li. Improved two-source extractors, and affine extractors for polylogarithmic entropy. In *FOCS*, pages 168–177, 2016.

40 Yehuda Lindell and Benny Pinkas. An efficient protocol for secure two-party computation in the presence of malicious adversaries. In Moni Naor, editor, *Advances in Cryptology - EUROCRYPT 2007, 26th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Barcelona, Spain, May 20-24, 2007, Proceedings*, volume 4515 of *Lecture Notes in Computer Science*, pages 52–78. Springer, 2007. doi:10.1007/978-3-540-72540-4_4.

41 Shachar Lovett and Emanuele Viola. Bounded-depth circuits cannot sample good codes. In *Proceedings of the 26th Annual IEEE Conference on Computational Complexity, CCC 2011, San Jose, California, USA, June 8-10, 2011*, pages 243–251, 2011. doi:10.1109/CCC.2011.11.

42 Silvio Micali and Leonid Reyzin. Physically observable cryptography (extended abstract). In Moni Naor, editor, *Theory of Cryptography, First Theory of Cryptography Conference, TCC 2004, Cambridge, MA, USA, February 19-21, 2004, Proceedings*, volume 2951 of *Lecture Notes in Computer Science*, pages 278–296. Springer, 2004. doi:10.1007/978-3-540-24638-1_16.

43 Moni Naor and Adi Shamir. Visual cryptography. In *Advances in Cryptology - EUROCRYPT '94, Workshop on the Theory and Application of Cryptographic Techniques, Perugia, Italy, May 9-12, 1994, Proceedings*, volume 950 of *Lecture Notes in Computer Science*, pages 1–12, 1994. doi:10.1007/BFb0053419.

44 Noam Nisan and Mario Szegedy. On the degree of boolean functions as real polynomials. In *Proceedings of the 24th Annual ACM Symposium on Theory of Computing, May 4-6, 1992, Victoria, British Columbia, Canada*, pages 462–467, 1992. doi:10.1145/129712.129757.

45 Ramamohan Paturi. On the degree of polynomials that approximate symmetric boolean functions (preliminary version). In *Proceedings of the Twenty-Fourth Annual ACM Symposium on Theory of Computing*, STOC '92, page 468–474, New York, NY, USA, 1992. Association for Computing Machinery. doi:10.1145/129712.129758.

46 Anup Rao. Extractors for low-weight affine sources. In *Proceedings of the 24th Annual IEEE Conference on Computational Complexity, CCC 2009, Paris, France, 15-18 July 2009*, pages 95–101. IEEE Computer Society, 2009. doi:10.1109/CCC.2009.36.

47 Alexander A. Razborov. Lower bounds on the size of bounded depth circuits over a complete basis with logical addition. *Mathematical Notes of the Academy of Sciences of the USSR*, 41(4):333–338, 1987.

48 Guy N. Rothblum. How to compute under AC^0 leakage without secure hardware. In *Advances in Cryptology - CRYPTO 2012 - 32nd Annual Cryptology Conference, Santa Barbara, CA, USA, August 19-23, 2012. Proceedings*, volume 7417 of *Lecture Notes in Computer Science*, pages 552–569, 2012. doi:10.1007/978-3-642-32009-5_32.

49 Rocco A. Servedio and Emanuele Viola. On a special case of rigidity. *Electronic Colloquium on Computational Complexity (ECCC)*, 19:144, 2012. URL: http://eccc.hpi-web.de/report/2012/144.

50 Adi Shamir. How to share a secret. *Commun. ACM*, 22(11):612–613, 1979. URL: http://doi.acm.org/10.1145/359168.359176, doi:10.1145/359168.359176.

51 Alexander A. Sherstov. Approximating the AND-OR tree. *Theory Comput.*, 9:653–663, 2013. doi:10.4086/toc.2013.v009a020.

52 Alexander A. Sherstov. Algorithmic polynomials. *SIAM J. Comput.*, 49(6):1173–1231, 2020. doi:10.1137/19M1278831.

53 Yaoyun Shi. Lower bounds of quantum black-box complexity and degree of approximating polynomials by influence of Boolean variables. *Inform. Process. Lett.*, 75(1-2):79–83, 2000. doi:10.1016/S0020-0190(00)00069-7.

54 Roman Smolensky. Algebraic methods in the theory of lower bounds for boolean circuit complexity. In *Proceedings of the 19th Annual ACM Symposium on Theory of Computing, 1987, New York, New York, USA*, pages 77–82, 1987. doi:10.1145/28395.28404.

55 Robert Spalek. A dual polynomial for OR, 2008. arXiv:0803.4516.

56 Avishay Tal. Tight bounds on the fourier spectrum of AC^0. In *32nd Computational Complexity Conference, CCC 2017, July 6-9, 2017, Riga, Latvia*, volume 79 of *LIPIcs*, pages 15:1–15:31, 2017. doi:10.4230/LIPIcs.CCC.2017.15.

57 Luca Trevisan. A note on approximate counting for k-dnf. In Klaus Jansen, Sanjeev Khanna, José D. P. Rolim, and Dana Ron, editors, *Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques*, pages 417–425, Berlin, Heidelberg, 2004. Springer Berlin Heidelberg.

58 S. Vadhan and L. Trevisan. Extracting randomness from samplable distributions. In *2000 IEEE 41st Annual Symposium on Foundations of Computer Science*, page 32, Los Alamitos, CA, USA, nov 2000. IEEE Computer Society. URL: `https://doi.ieeecomputersociety.org/10.1109/SFCS.2000.892063`, `doi:10.1109/SFCS.2000.892063`.

59 Emanuele Viola. The complexity of distributions. In *51th Annual IEEE Symposium on Foundations of Computer Science, FOCS 2010, October 23-26, 2010, Las Vegas, Nevada, USA*, pages 202–211, 2010. `doi:10.1109/FOCS.2010.27`.

60 Emanuele Viola. Extractors for turing-machine sources. In Anupam Gupta, Klaus Jansen, José Rolim, and Rocco Servedio, editors, *Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques*, pages 663–671, Berlin, Heidelberg, 2012. Springer Berlin Heidelberg.

61 Emanuele Viola. Extractors for circuit sources. *SIAM Journal on Computing*, 43(2):655–672, 2014. `arXiv:https://doi.org/10.1137/11085983X`, `doi:10.1137/11085983X`.

62 Emanuele Viola. Quadratic maps are hard to sample. *ACM Trans. Comput. Theory*, 8(4), June 2016. `doi:10.1145/2934308`.

63 Emanuele Viola. Sampling lower bounds: Boolean average-case and permutations. *SIAM Journal on Computing*, 49(1):119–137, 2020. `arXiv:https://doi.org/10.1137/18M1198405`, `doi:10.1137/18M1198405`.

64 Emanuele Viola. Lower bounds for samplers and data structures via the cell-probe separator. *Electron. Colloquium Comput. Complex.*, 28:73, 2021. URL: `https://eccc.weizmann.ac.il/report/2021/073`.

65 R. Ryan Williams. Counting solutions to polynomial systems via reductions. In Raimund Seidel, editor, *1st Symposium on Simplicity in Algorithms (SOSA 2018)*, volume 61 of *OpenAccess Series in Informatics (OASIcs)*, pages 6:1–6:15, Dagstuhl, Germany, 2018. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik. URL: `http://drops.dagstuhl.de/opus/volltexte/2018/8307`, `doi:10.4230/OASIcs.SOSA.2018.6`.

66 Andrew Chi-Chih Yao. How to generate and exchange secrets. In *27th Annual Symposium on Foundations of Computer Science (sfcs 1986)*, pages 162–167, 1986. `doi:10.1109/SFCS.1986.25`.