Condensing and Extracting Against Online Adversaries

Eshan Chattopadhyay
Cornell University, Ithaca, NY, USA

Mohit Gurumukhani
Cornell University, Ithaca, NY, USA

Noam Ringach
Cornell University, Ithaca, NY, USA

Rocco A. Servedio
Columbia University, New York, NY, USA

Abstract

We investigate the tasks of deterministically condensing and extracting randomness from Online Non-Oblivious Symbol Fixing (oNOSF) sources, a natural model of defective random sources for which it is known that extraction is impossible in many parameter regimes [AORSV, EUROCRYPT'20]. A (g, ℓ)-oNOSF source is a sequence of ℓ blocks $\mathbf{X} = (\mathbf{X}_1, \ldots, \mathbf{X}_\ell) \sim (\{0,1\}^n)^\ell$, where at least g of the blocks are *good* (are independent and have some min-entropy), and the remaining *bad* blocks are controlled by an *online adversary* where each bad block can be arbitrarily correlated with any block that appears before it.

The existence of condensers (in regimes where extraction is impossible) was recently studied in [CGR, FOCS'24]. They proved condensing impossibility results for various values of g and ℓ, and they showed the existence of condensers matching the impossibility results in the special case when n is exponential in ℓ (i.e., the setting of few blocks of large length).

In this work, not only do we construct the first explicit condensers matching the existential results of [CGR, FOCS'24], but we make a doubly exponential improvement by handling the case when n is only polylogarithmic in ℓ. We also obtain a much improved explicit construction for transforming low-entropy oNOSF sources (where the good blocks only have min-entropy, as opposed to being uniform) into uniform oNOSF sources.

As our next result, we essentially resolve the question of the existence of condensers for oNOSF sources by showing the existence of condensers in almost all parameter regimes, even when n is a large enough constant and ℓ is growing.

We find interesting connections and applications of our results on condensers to collective coin flipping and collective sampling, problems that are well-studied in fault-tolerant distributed computing. We use our condensers to provide very simple protocols for these problems.

Next, we turn to understanding the possibility of extraction from oNOSF sources. For proving lower bounds, we introduce and initiate a systematic study of a new, natural notion of the influence of functions, which we call *online influence*, and establish tight bounds on the total online influence of functions, which imply extraction lower bounds. Lastly, we give explicit extractor constructions for oNOSF sources using novel connections to leader election protocols, and we further construct the required leader election protocols. These extractor constructions achieve parameters that go beyond the standard resilient functions of [AL, Combinatorica'93].

2012 ACM Subject Classification Theory of computation → Pseudorandomness and derandomization; Theory of computation → Expander graphs and randomness extractors; Computer systems organization → Dependable and fault-tolerant systems and networks

Keywords and phrases collective coin flipping, leader election, Boolean function analysis, fault tolerant distributed computing, full information model, resilient function, pseudorandomness, condensers, adversarial sources, non-oblivious symbol fixing sources, Chor-Goldreich sources

Digital Object Identifier 10.4230/LIPIcs.CCC.2026.5

41st Computational Complexity Conference (CCC 2026).
Editor: Dana Moshkovitz; Article No. 5; pp. 5:1–5:22

Leibniz International Proceedings in Informatics
Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

Related Version *Full Version*: https://arxiv.org/abs/2411.04115

Funding *Eshan Chattopadhyay*: Supported by a Sloan Research Fellowship, NSF CAREER Award 2045576, and NSF Award CCF-2514586.
Mohit Gurumukhani: Supported by a Sloan Research Fellowship, NSF CAREER Award 2045576, and NSF Award CCF-2514586.
Noam Ringach: Supported by NSF GRFP grant DGE – 2139899, NSF CAREER Award 2045576, a Sloan Research Fellowship, and NSF Award CCF-2514586.
Rocco A. Servedio: Supported by NSF Award CCF-2106429 and NSF Award CCF-2211238.

Acknowledgements We thank Madhur Tulsiani for asking a question that motivated us to consider the model of local oNOSF sources. We thank Miranda Christ for helpful feedback on an earlier version of the manuscript. We thank the organizers of the Dagstuhl Seminar on Algebraic and Analytic Methods in Computational Complexity and Schloss Dagstuhl for providing a stimulating research environment, where discussions between R.S. and E.C. contributed to this collaboration.

1 Introduction

Randomness is extremely useful in computation with wide-ranging applications in algorithm design, cryptography, distributed computing protocols, machine learning, error-correcting codes, and much more [34, 39]. Most of these applications require access to high quality randomness. However in a lot of settings, especially arising in practice, algorithms only have access to low quality source of randomness. This motivates the notion of *condensers*: functions that transform weak random sources into strong random sources that are of *better quality*.

The standard way of measuring the amount of randomness is using min-entropy. Formally, for a source (distribution) $\mathbf{X}$ with support Ω, define its min-entropy as $H_\infty(\mathbf{X}) = \min_{x\in\Omega} \log_2(1/\Pr[\mathbf{X} = x])$. If $\Omega = \{0,1\}^n$ and $H_\infty(\mathbf{X}) \geq k$, we say that $\mathbf{X}$ is an (n,k)-source. We will also need the notion of smooth min-entropy, which measures how close a distribution is to having high entropy. Formally, for a source $\mathbf{X}$, its smooth min-entropy with parameter ε is defined as $H^\varepsilon_\infty(\mathbf{X}) = \max_{\mathbf{Y}:|\mathbf{X}-\mathbf{Y}|\leq\varepsilon}\{H_\infty(\mathbf{Y})\}$, where $|\cdot|$ denotes the statistical distance.

With this, we are ready to formally define *deterministic condensers*:

▶ **Definition 1.** *A function* $\mathsf{Cond} : \{0,1\}^n \to \{0,1\}^m$ *is a* $(k_{in}, k_{out}, \varepsilon)$-condenser for a family of distributions $\mathcal{X}$ *if for all* $\mathbf{X} \in \mathcal{X}$ *with* $\mathbf{X} \sim \{0,1\}^n$ *and* $H_\infty(\mathbf{X}) \geq k_{in}$*, we have that* $H^\varepsilon_\infty(\mathsf{Cond}(\mathbf{X})) \geq k_{out}$.

We say $\frac{k_{in}}{n}$ *is the* input entropy rate*,* $\frac{k_{out}}{m}$ *is the* output entropy rate*, and* $m - k_{out}$ *is the* entropy gap *of* Cond.

The task of the condenser is to make the output entropy rate as high as possible compared to the input entropy rate; i.e., to make the output distribution more "condensed". Related to this, it is also desirable to have as small entropy gap as possible. Condensers with entropy gap 0 are known as *randomness extractors* and have been extensively studied in theoretical computer science.

When $\mathcal{X}$ is the family of all distributions, it is folklore that no non-trivial condensing is possible.[1] So, we additionally assume that $\mathcal{X}$ is a structured family of sources.[2] Since extractors are the highest quality condensers, a significant amount of work has focused on constructing extractors for many interesting families of sources [38, 11, 17, 30]. However, for many natural family of sources, one can provably show that no extractor can exist.

In this work, we focus on one natural family of sources where it is known that extraction is impossible (for many interesting parameter regimes): online non-oblivious symbol fixing sources (oNOSF sources).[3] Formally:

▶ **Definition 2.** *A (g, ℓ, n, k)-oNOSF source $\mathbf{X} = (\mathbf{X}_1, \ldots, \mathbf{X}_\ell)$ with ℓ blocks is such that each block $\mathbf{X}_i$ is over $\{0,1\}^n$, g of the blocks are independent sources with min-entropy k ("good blocks"), and each "bad block" is an arbitrary function of the blocks with an index smaller than it. When $k = n$, we will call such sources uniform (g, ℓ, n)-oNOSF sources, and when n is clear from context, we will simply call them uniform (g, ℓ)-oNOSF sources.*

Our results at a glance

The previous work of [10] gave a condenser impossibility result for oNOSF sources and showed the existence of a condenser matching that result as long as the block length n was exponential in the number of blocks ℓ. We construct explicit condensers for oNOSF sources that match the results of [10]; in fact, we only require n to be polylogarithmic in ℓ, providing a doubly exponential improvement over the (existential) result of [10]. Next, we essentially resolve the existence question for oNOSF source condensers by showing that good condensers exist even when n is a (large) constant and ℓ grows. To go with these results, we obtain an improved construction for transforming low-entropy oNOSF sources into uniform oNOSF sources. Moreover, we find new applications of our results on condensers to collective coin flipping and collective sampling, and use these connections to provide simple protocols for these problems. In the complementary direction, we construct explicit extractors for uniform oNOSF sources by explicitly constructing the required leader election protocols; the results of which are summarized in Tables 1 and 2. Also in the context of extractors for oNOSF sources, we introduce the new, natural notion of *online influence* for Boolean functions and show extraction lower bounds for oNOSF sources by establishing tight bounds on the total online influence of functions.

On the Utility of Condensing for oNOSF sources

We note that condensers (and sources with high min-entropy rate) are very useful: the condensed distribution can be used to efficiently simulate randomized algorithms with small overhead, perform one-shot simulations for randomized protocols, cryptography, interactive proofs, and much more. For details on these applications and more, see [1, 15, 10, 14].

[1] Assuming $m \leq n$ (wlog this holds since $|\mathsf{Cond}(\{0,1\}^n)| \leq 2^n$), $m - k_{out} \geq (n - k_{in}) - \log(1/(1-\varepsilon))$ and hence the output entropy rate cannot be more than the input entropy rate without incurring extremely large error (> 0.999).

[2] A different route, that has been widely studied, is to assume access to a short independent seed. In this work, we will limit ourselves to the *deterministic or seedless setting*.

[3] These sources are in contrast to non-oblivious symbol fixing (NOSF) sources where bad blocks can be arbitrary functions of all the good blocks and oblivious symbol fixing sources (OSF) where bad blocks do not depend on any good blocks. NOSF sources were introduced in [30] and OSF sources were introduced in [12] with applications in leakage-resilient cryptography, and have been well-studied.

Practical applications to blockchains and cryptography

oNOSF sources are inspired by real-time randomness generation settings such as in blockchains where the adversary has some probability of corrupting a block. Moreover, it is known that non-corrupted blocks have some amount of min-entropy [7]. In fact, several works have attempted to use Bitcoin or Ethereum as a source of randomness in cryptographic protocols [7, 6, 35, 9]. However, the authors of [6] showed that even when the adversary has a small, constant probability of corrupting a block, randomness extraction is impossible from Bitcoin.[4] Our results show that in this setting, it is still possible to get a condensed source with a high min-entropy rate. It is known that such sources are still useful for cryptographic protocols, such as hedged public-key enryption [4]. Further, there are natural cryptographic settings, such as creating a Common Reference String, that are widely used in various cryptographic protocols where oNOSF sources naturally arise [1].

Practical applications to fault-tolerant distributed computing

One common scenario in distributed computing is that of many agents (e.g., servers in a network) attempting to collectively take a decision using several rounds of communication over a common broadcast channel in the presence of computationally unbounded adversarial agents, which render cryptographic primitives ineffective. Protocols for collective coin flipping, leader election, and collective sampling are prime examples of this scenario that have been intensively studied ([5, 19, 13, 3, 18] and many more), and already connected to the extractor literature [31, 32]. In Section 3, we explain how condensing or extracting from oNOSF sources can be viewed as a variant of these protocols. As a consequence, our new results on condensers provide a new protocol for collective sampling and impossibility results for these protocols can be translated into lower bounds against extractors and condensers for oNOSF sources.

Organization

The remainder of our introduction is structured as follows. We give an overview of previous work in Section 1.1 before presenting our main existential and explicit condenser results in Section 1.2. In Section 1.3, we present our results on the limits of extraction from oNOSF sources. Later on, in Section 3, we explain how our results on condensers have implications for collective coin flipping and sampling protocols.

1.1 Previous Work

Extractors

The study of extractors for oNOSF sources was initiated by [1].[5] Their results include the following:

- It is impossible to extract from uniform oNOSF sources when the fraction of good blocks is 0.99.
- An explicit transformation from $(g, \ell, n, 0.9n)$-oNOSF source into a source over $(\{0,1\}^{O(n)})^{\ell-1}$ where $g-1$ of the blocks are uniform and independent.
- An explicit transformation from $(g, \ell, n, 0.1n)$-oNOSF source into a source over $(\{0,1\}^{O(n)})^{100\ell}$ where $g-1$ of the blocks are uniform and independent.

[4] This mirrors our extraction impossibility result for oNOSF sources.
[5] In [1], these sources were called SHELA (Somewhere Honest Entropic Look Ahead) sources.

Even though the output entropy rate is only slightly more than the input-entropy rate in the second result and smaller in the third result, the fact that a lot of the blocks are truly uniform is very useful, and they find interesting cryptographic applications of these "somewhere-extractors".

Before our work, the best known extractors for oNOSF sources could be obtained by using resilient functions or equivalently, extractors for NOSF sources (non-online version of oNOSF sources) constructed by [2, 11, 33, 26, 27] ; these require $g \geq \ell - \frac{\ell}{(\log \ell)^2}$.

Condensers

oNOSF sources were further studied by [10], where they obtained the following results regarding condensers:

- When $n \geq k \geq \ell$, there exist functions that can transform a (g, ℓ, n, k)-oNOSF source into a uniform $(g-1, \ell-1, O(k/\ell))$-oNOSF source (this function can be made explicit with slightly worse dependence on output length).
- When $n \geq 2^{\omega(\ell)}$ and $g > 0.5\ell$, there exists condenser $\mathsf{Cond} : (\{0,1\}^n)^\ell \to \{0,1\}^{m=O(n\cdot\ell/g)}$ such that for any uniform (g, ℓ, n)-oNOSF source $\mathbf{X}$, $H^\varepsilon_\infty(\mathsf{Cond}(\mathbf{X})) \geq m - O(\log(n/\varepsilon))$.[6] Their result is not explicit.
- It is impossible to condense from uniform $(0.5\ell, \ell, n)$-oNOSF sources with output entropy rate more than 0.5.[7]

We also mention a related family of sources, namely adversarial Chor-Goldreich sources. Uniform oNOSF sources can be seen as a special case of adversarial Chor-Goldreich sources where the good blocks are uniform. Constructing condensers where the output entropy rate is g/ℓ for adversarial Chor-Goldreich sources is already a challenging task, although such condensers in various parameter regimes have been recently constructed [15, 22]. The paper of [16] recently constructed condensers for a related, more general model.

1.2 This Work: New Condenser Constructions

Previous works only showed the existence of condensers for oNOSF sources when $n \geq 2^{\omega(\ell)}$. We vastly improve on this result in two ways. First, we construct explicit condensers that work even when $n \geq \text{polylog}(\ell)$ and provide an explicit transformation from low-entropy oNOSF sources to uniform oNOSF sources that works even when the min-entropy of a block k is only $\text{polylog}(n)$. Second, we show that condensers for oNOSF sources exist when n is just a large constant, only leaving open the question of the existence of such condensers for when n is a very small constant (e.g., $n = 1$). We also discover surprising connections between condensers for oNOSF sources and protocols for natural problems in distributed computing, such as collective coin flipping and collective sampling. Lastly, we initiate the study of *online influence* of Boolean functions, a natural generalization of influence that captures the one-sided nature of our online adversary to help us analyze the setting of $n = 1$. We now discuss our results in detail below.

1.2.1 Explicit Condensers

We construct the first explicit condensers for oNOSF sources. Our ultimate result is founded on a baseline construction that itself is an explicit condenser for oNOSF sources that matches the existential results of [10] and works for any block length $n = 2^{\Omega(\ell)} \log(1/\varepsilon)$ as long as at least 51% of blocks are good.

[6] They get a tradeoff for $g \leq 0.5\ell$ as well
[7] They get impossibility for other smaller g as well

▶ **Theorem 3** (Theorem 16 restated). *For all $\varepsilon > 0$ and $n, \ell \in \mathbb{N}$ where $n \geq 2^{\Omega(\ell)} \log(1/\varepsilon)$, there exists an explicit condenser $\mathsf{Cond} : (\{0,1\}^n)^\ell \to \{0,1\}^m$ such that for any $(g = 0.51\ell, \ell, n)$-oNOSF source $\mathbf{X}$, we have that $H^\varepsilon_\infty(\mathsf{Cond}(\mathbf{X})) \geq m - 2^{O(\ell)} \log(1/\varepsilon)$ where $m = 0.0001\ell n$.*

Surprisingly, we are able to improve upon this baseline to obtain explicit condensers that work for oNOSF sources where the block length n is only at least $\mathrm{poly}(\log(\ell)/\varepsilon)$.

▶ **Theorem 4** (Informal version of Theorem 13). *For all $\varepsilon > 0$ and $n, \ell \in \mathbb{N}$ where $n \geq \mathrm{poly}(\log(\ell)/\varepsilon)$, there exists an explicit condenser $\mathsf{Cond} : (\{0,1\}^n)^\ell \to \{0,1\}^m$ such that for any $(g = 0.51\ell, \ell, n)$-oNOSF source $\mathbf{X}$, we have that $H^\varepsilon_\infty(\mathsf{Cond}(\mathbf{X})) \geq m - \mathrm{poly}(\log(\ell)/\varepsilon) \cdot \log(n)$ where $m = 0.001\ell n - O(\ell \log(\ell) \log(1/\varepsilon))$.*

Since condensing when $g = 0.5\ell$ is impossible, both results are tight. We note that neither result completely subsumes the other. Our baseline construction in Theorem 3 has an exponential dependence of n on ℓ instead of the polylogarithmic dependence achieved in Theorem 4; however, the latter result requires the dependence $n \geq \mathrm{poly}(1/\varepsilon)$ compared to $n \geq \log(1/\varepsilon)$ for the baseline construction.

Using our new results regarding transforming oNOSF sources to uniform oNOSF sources, we also obtain explicit condensers for $(0.51\ell, \ell, n, k)$-oNOSF sources for the same parameter regime:

▶ **Corollary 5.** *For all $n, \ell, k \in \mathbb{N}$ where $n \geq \mathrm{poly}(\ell)$ and $k \geq \mathrm{polylog}(n)$, there exists an explicit condenser $\mathsf{Cond} : (\{0,1\}^n)^\ell \to \{0,1\}^m$ such that for any $(g = 0.51\ell, \ell, n, k)$-oNOSF source $\mathbf{X}$, we have that $H^\varepsilon_\infty(\mathsf{Cond}(\mathbf{X})) \geq m - \mathrm{polylog}(\ell) \cdot \log(n)$ where $m = 0.001\ell n - O(\ell \log(\ell) \log\log(\ell))$ and $\varepsilon = \mathrm{poly}(1/\log(\ell))$.*

We can also extend our result to explicitly condense from uniform (g, ℓ, n)-oNOSF sources in the same parameter regime so that the output entropy rate is $1/\lfloor \ell/g \rfloor - o(1)$, which is tight according to the impossibility result of [10].

Previously, [10] showed how to existentially condense from uniform (g, ℓ, n)-oNOSF sources when $n = 2^{\Omega(\ell)}$. However, they relied on the existence of a very strong pseudorandom object: "output-light" low-error two-source extractors. Such extractors, even without the output-lightness requirement, are extremely hard to construct and it is a major open problem to obtain such extractors. We are able to construct explicit condensers by creating new tools that allow us to use an oNOSF source to sample indices within an oNOSF source, and stitching them together so that the base pseudorandom object we rely on are seeded extractors that we know how to explicitly construct with near optimal parameters.

1.2.2 Transforming Low-Entropy oNOSF sources to uniform oNOSF sources

We show how to existentially, as well as explicitly, with a slight loss in parameters, transform (g, ℓ, n, k)-oNOSF sources into uniform $(0.99g, \ell - 1, n)$-oNOSF sources. Formally, we show:

▶ **Theorem 6.** *For all ℓ, n, k, ε where $n = \mathrm{poly}(\log(\ell)), k = O(\log(\ell/\varepsilon))$, there exists a function f such that f transforms $(0.51\ell, \ell, n, k)$-oNOSF sources into uniform $(0.509\ell, \ell, m)$-oNOSF sources with error ε where $m = \Omega(k)$.*

Our construction can also be made explicit with slightly worse dependence on m and ε. See the full version of our paper for the full tradeoff.

Previously, [10] provided such a transformation only for $n \geq k \geq \Omega(\ell)$. Hence, our transformation makes a major improvement on their parameters. Such an improvement allows us to obtain better condensers for low-entropy oNOSF sources in the regime $n = \text{poly}(\log(\ell/\varepsilon))$ (see Theorem 8).

1.2.3 Existential Condensers

We show how to condense from uniform (g, ℓ, n)-oNOSF sources for almost all settings of ℓ and n when $g \geq 0.51\ell$. In particular, we show:

▶ **Theorem 7.** *For all ℓ, ε where $\ell \geq O(\log(1/\varepsilon))$, and $n = 10^4$, there exists a condenser $\mathsf{Cond} : (\{0,1\}^n)^\ell \to \{0,1\}^m$ such that for any uniform $(0.51\ell, \ell, n)$-oNOSF source $\mathbf{X}$, we have $H^\varepsilon_\infty(\mathsf{Cond}(\mathbf{X})) \geq 0.99m$ where $m = \Omega(\ell + \log(1/\varepsilon))$. Furthermore, when $n = \omega(1)$, the output entropy rate becomes $1 - o(1)$.*

This is tight since [10] showed it is impossible to condense uniform $(0.5\ell, \ell, n)$-oNOSF sources beyond output entropy rate 0.5.

Using our new results regarding transforming oNOSF sources to uniform oNOSF sources, we also obtain condensers for $(0.51\ell, \ell, n, k)$-oNOSF sources when $n \geq \text{poly}(\log(\ell))$,

▶ **Theorem 8.** *For all ℓ, n, ε where $n = \text{poly}(\log(\ell/\varepsilon)), k = \Omega(\log(\ell/\varepsilon))$, there exists a condenser $\mathsf{Cond} : (\{0,1\}^n)^\ell \to \{0,1\}^m$ such that for any $(0.51\ell, \ell, n, k)$-oNOSF source $\mathbf{X}$, we have $H^\varepsilon_\infty(\mathsf{Cond}(\mathbf{X})) \geq m - O(m/\log(m)) - O(\log(1/\varepsilon))$ where $m = \Omega(k)$.*

We sketch the proof of both of these theorems in Section 2.1 We can also extend our result to condense from uniform (g, ℓ, n)-oNOSF sources for all g, ℓ and constant n where the output entropy rate is $1/\lfloor \ell/g \rfloor - 0.001$. This is tight since [10] showed it is impossible to condense such sources beyond output entropy rate $1/\lfloor \ell/g \rfloor$.

Previously, [10] showed how to existentially condense from uniform (g, ℓ, n)-oNOSF sources when $g \geq 0.51\ell$, provided $n \geq 2^{\omega(\ell)}$. As n gets smaller, condensing becomes harder since a uniform (g, ℓ, n)-oNOSF source is also a uniform $(g \cdot n/1000, \ell \cdot n/1000, 1000)$-oNOSF source. Hence, we greatly improve the parameters while using different and much simpler techniques.

1.3 Extraction from oNOSF Sources

Next we discuss our positive and negative results on the limits of extraction from oNOSF sources. Our upper bound results (explicit extractors) are based on a novel connection to leader election and coin-flipping protocols; to instantiate this connection and give explicit extractors, we construct novel protocols for these distributed problems. Our lower bounds are based on a new notion of influence of functions, namely *online influence*, that we introduce and analyze.

Extraction Lower bounds via Online Influence

For simplicity, we focus on the case of $n = 1$, which leads to interesting new questions about Boolean functions. We refer to such uniform $(g, \ell, 1)$-oNOSF sources as (g, ℓ)-oNOBF sources; oNOBF stands for online non-oblivious bit-fixing sources. We ask what is the exact tradeoff between g, ℓ, and ε for extracting from oNOBF sources. Towards this, we introduce the notion of online influence.

▶ **Definition 9** (Online influence). *For a function $f : \{0,1\}^\ell \to \{0,1\}$, the* online influence *of the i-th bit is*

$$\mathbf{oI}_i[f] = \mathop{\mathbb{E}}_{x\sim\mathbf{U}_{i-1}}\left[\left|\mathop{\mathbb{E}}_{y\sim\mathbf{U}_{\ell-i}}[f(x,1,y)] - \mathop{\mathbb{E}}_{y\sim\mathbf{U}_{\ell-i}}[f(x,0,y)]\right|\right]$$

and the total online influence *is* $\mathbf{oI}[f] = \sum_{i=1}^{\ell} \mathbf{oI}_i[f]$.

We establish new structural results on online influence, including a Poincaré-style inequality and use them to obtain the following extraction lower bound.

▶ **Theorem 10.** *For $\varepsilon < 0.01$, there do not exist extractors for $(0.97\ell, \ell)$-oNOBF sources with error at most ε.*

A similar extraction lower bound was shown in [1] using different techniques.

Explicit Extractors via Leader Election Protocols

Here we present our explicit constructions of extractors for oNOBF and oNOSF sources. The following are our main results.

▶ **Theorem 11.** *There exists an explicit function $\mathsf{Ext} : \{0,1\}^\ell \to \{0,1\}$ such that for any (g,ℓ)-oNOBF source $\mathbf{X}$ where $g \geq \ell - \ell/(C\log(\ell))$, we have $\mathsf{Ext}(\mathbf{X}) \approx_{\varepsilon=1/100} \mathbf{U}_1$, where C is a large constant.*

▶ **Theorem 12.** *There exists an explicit function $\mathsf{Ext} : (\{0,1\}^n)^\ell \to \{0,1\}^n$ such that for any (g,ℓ,n)-oNOSF source $\mathbf{X}$ where $g \geq \ell - \ell/(C\log^*(\ell))$ and $n \geq \log(\ell)$, we have $\mathsf{Ext}(\mathbf{X}) \approx_{\varepsilon=1/100} \mathbf{U}_n$, where C is a large constant.*

It is instructive to contrast our results with the non-online setting (where adversarial bits may depend on any good bit), called NOSF sources and NOBF sources. For both these sources, the current best extractors require $g \geq \ell - \frac{\ell}{(\log \ell)^2}$, which is much more than what Theorem 11 and Theorem 12 require.

We contrast the results for both settings in Tables 1 and 2. In these tables, we are providing known upper and lower bounds on the value of $b(\ell)$, defined as the maximum number of bad symbols for which extraction is still possible with a small constant error – so lower bounds correspond to best known constructions of such functions and upper bounds refers to the best known limitation of such functions. We write "$O(\ell)$" to mean "$c\ell$ for some small universal constant $c < 1$".

To interpret our results in terms of (online) influence of coalitions, it will be useful to extend the definition of online influence to subsets of coordinates. We formally do so in the full version of the paper. Intuitively, we're measuring the influence of the exact same adversary as in an oNOSF source. Using this connection, we observe that online-resilient functions are equivalent to extractors for uniform oNOSF source sources (with one bit output). Thus, our explicit extractor results immediately imply explicit online-resilient functions. We present this connection in the full version of the paper.

Our main technique for Theorems 11 and 12 is a new generic way to transform leader election and coin flipping protocols into extractors for oNOBF and oNOSF sources. The general idea of constructing an extractor is to simulate an appropriate leader election

[8] Recall that this lower bound is for (g,ℓ,n)-oNOSF sources with $n \geq \log(\ell)$.

Table 1 $b(\ell)$ bounds in the non-online setting.

Source	Lower bound	Upper bound
NOBF	$\Omega\left(\frac{\ell}{\log^2 \ell}\right)$, [2]	$O\left(\frac{\ell}{\log \ell}\right)$, [28]
NOSF	$\Omega\left(\frac{\ell}{\log^2 \ell}\right)$, [2]	$O(\ell)$, [8]

Table 2 $b(\ell)$ bounds in the online setting.

Source	Lower bound	Upper bound
oNOBF	$\Omega\left(\frac{\ell}{\log \ell}\right)$, [Theorem 11]	$O(\ell)$, Theorem 10 or [1]
oNOSF	$\Omega\left(\frac{\ell}{\log^* \ell}\right)$, [Theorem 12] [8]	$O(\ell)$, [1]

protocol with the source at hand (oNOBF or oNOSF), and output according to the chosen leader. To instantiate this transformation, we revisit previous leader election protocols. Our leader election protocols provide a slightly stronger than usual guarantee: a good player is elected as the leader with probability close to 1. This contrasts with the usual guarantee in leader election protocols, where a good leader is chosen with only a non-trivial (constant) probability. We give more connections to distributed computing in Section 3 where we delineate applications of our results to collection coin flipping and collective sampling. For further details, see the full version of our paper.

2 Proof Overview

Our proof overview begins by outlining our new explicit result for condensers in Section 2.1 that is able to handle polylogarithmic block length. Next, we present our transformation of low-entropy oNOSF sources to uniform oNOSF sources in Section 2.2 before discussing our existential results for condensers that can handle constant block length in Section 2.3. We present the main ideas behind our results regarding online influence and extractor lower bounds in Section 2.4. In Section 2.5, we overview our extractor constructions for oNOBF and oNOSF sources that are based on a general transformation from leader election protocols. We refer the reader to the full version of this paper for more details and for formal proofs of all our results.

2.1 Explicit Condensers for Uniform oNOSF Sources

We sketch here our constructions (as well as proof ideas) of explicit condensers for uniform $(0.51\ell, \ell, n)$-oNOSF sources.[9] The goal will be to construct explicit condensers that work with as few good sources as possible while minimizing the block length n. In particular, we will show:

▶ **Theorem 13.** *For all $\varepsilon > 0$ and $n, \ell \in \mathbb{N}$ where $n \geq \left(\frac{\log(\ell)}{\varepsilon}\right)^{\Omega(1)}$, there exists an explicit condenser $\mathsf{Cond} : (\{0,1\}^n)^\ell \to \{0,1\}^m$ such that for any $(g = 0.51\ell, \ell, n)$-oNOSF source $\mathbf{X}$, we have that $H^\varepsilon_\infty(\mathsf{Cond}(\mathbf{X})) \geq m - \left(\frac{\log(\ell)}{\varepsilon}\right)^{O(1)} \cdot \log(n)$ where $m = 0.001 \cdot \ell n - O\left(\ell \log(\ell) \log(1/\varepsilon)\right)$.*

[9] Since all sources are uniform here, we will not explicitly mention this again.

We will require two main tools to show this. The first one uses ideas from the leader election literature and allows us to sample an $O(\log(\ell))$ sized committee starting from ℓ players while essentially maintaining the fraction of bad players. Formally:

▶ **Lemma 14.** *For all $\varepsilon_s > 0$, $n, \ell \in \mathbb{N}$, and constant $\varepsilon_a > 0$ where $n \geq \Omega(\log(\ell)\log(1/\varepsilon_s))$, there exists an explicit function* $\mathsf{oNOSFSamp} : (\{0,1\}^n)^\ell \to [\ell]^D$ *where $D \leq O(\log(\ell/\varepsilon_s))$ with the following property.*[10] *For all $S \subset [\ell]$ and (g, ℓ, n)-oNOSF sources $\mathbf{X}$, we have that*

$$\Pr_{x \sim \mathbf{X}}\left[\left|\frac{|\mathsf{oNOSFSamp}(x) \cap S|}{D} - \frac{|S|}{\ell}\right| \geq \varepsilon_a\right] \leq \varepsilon_s$$

At a high level, to construct $\mathsf{oNOSFSamp}$, we slightly modify the committee selection procedure from [36] and instantiate it with a seeded extractor with near optimal dependence on the seed [40].

Our second tool is a seeded condenser for general min-entropy sources $\mathbf{X}$ that uses an oNOSF source $\mathbf{Y}$ as the seed, where the bad bits in $\mathbf{Y}$ can depend on $\mathbf{X}$.

▶ **Lemma 15.** *There exists a constant C_{2Cond} such that for all $n_x, k, n_y, t \in \mathbb{N}$ with $\varepsilon > 0$ and $n_y \geq (C_{\mathsf{2Cond}})^t \log(tn_x/\varepsilon)$, there exists an explicit condenser* $\mathsf{2Cond} : \{0,1\}^{n_x} \times (\{0,1\}^{n_y})^t \to \{0,1\}^m$ *where $m = \frac{1}{3}(k - (C_{\mathsf{2Cond}})^t \log(tn_x/\varepsilon))$ so that the following holds: For all (n_x, k)-sources $\mathbf{X}$ and $(g = 1, \ell = t)$-oNOSF sources $\mathbf{Y} \sim (\{0,1\}^{n_y})^t$ such that the good blocks in $\mathbf{Y}$ are independent of $\mathbf{X}$ and the bad blocks in $\mathbf{Y}$ can depend on $\mathbf{X}$, we have that $H^\varepsilon_\infty(\mathsf{2Cond}(\mathbf{X}, \mathbf{Y})) \geq m - (C_{\mathsf{2Cond}})^t \log(tn_x/\varepsilon)$.*

We will sketch how to construct this in Section 2.1.6. Using these tools, we are ready to present our explicit condenser. In fact, we will provide sketches of five different constructions of explicit condensers with increasingly better parameter dependence; the fifth (and final) one is the construction given by Theorem 13. The parameters they will vary in are the fraction of good blocks (i.e., g/ℓ) and the block length n. As we will see, each construction will build on ideas from the previous construction.

2.1.1 Construction 1: 51% good and $n \geq 2^{\Omega(\ell)}$

We here construct the following condenser:

▶ **Theorem 16.** *For all $\varepsilon > 0$ and $n, \ell \in \mathbb{N}$ where $n \geq 2^{\Omega(\ell)} \log(1/\varepsilon)$, there exists an explicit condenser* $\mathsf{Cond} : (\{0,1\}^n)^\ell \to \{0,1\}^m$ *such that for any $(g = 0.51\ell, \ell, n)$-oNOSF source $\mathbf{X}$, we have that $H^\varepsilon_\infty(\mathsf{Cond}(\mathbf{X})) \geq m - 2^{O(\ell)} \log(1/\varepsilon)$ where $m = 0.0001 \cdot n\ell$.*

Proof sketch. Let $\gamma = 0.01$ and $\ell' = \ell/2$. We decompose the input $\mathbf{X}$ into two equal sized parts so that $\mathbf{X} = (\mathbf{X}_1, \mathbf{X}_2)$ where both $\mathbf{X}_1, \mathbf{X}_2 \sim (\{0,1\}^n)^{\ell/2} \equiv (\{0,1\}^n)^{\ell'}$. Since $\mathbf{X}$ has $(0.5 + \gamma)\ell$ good players, we infer that each of $\mathbf{X}_1, \mathbf{X}_2$ has at least $\gamma\ell = (2\gamma) \cdot \ell'$ good players. In particular, we use the fact that $H_\infty(\mathbf{X}_1) \geq (2\gamma) \cdot (\ell n/2)$ and that $\mathbf{X}_2$ is a $(g = (2\gamma)\ell/2, \ell/2, n)$-oNOSF source. With this, we let $\mathsf{2Cond}$ be the condenser from our second tool Lemma 15 and let our final output be $\mathsf{2Cond}(\mathbf{X}_1, \mathbf{X}_2)$. Note that here $t = \ell$ and so, this requires $n \geq (C_{\mathsf{2Cond}})^\ell \log(\ell n/\varepsilon)$, an inequality that we indeed satisfy. The guarantees from Lemma 15 provide us with the desired claim. ◀

[10] Even though the output domain of $\mathsf{oNOSFSamp}$ is a vector, we will abuse notation and often treat it as a set.

Each of the subsequent constructions will use a similar construction idea as above. However, they will try to decrease t as much as possible, where t is the number of players in the oNOSF source when applying 2Cond from Lemma 15. Note that any reduction results in a decrease in the block length requirement n.

2.1.2 Construction 2: 67% good and $n \geq \text{poly}(\ell)$

Our next construction requires a slightly larger fraction of good blocks. However, the block length required is exponentially improved.

▶ **Theorem 17.** *For all $\varepsilon > 0$ and $n, \ell \in \mathbb{N}$ where $n \geq \left(\frac{\ell}{\varepsilon}\right)^{\Omega(1)}$, there exists an explicit condenser $\mathsf{Cond} : (\{0,1\}^n)^\ell \to \{0,1\}^m$ such that for any $(g = 0.67\ell, \ell, n)$-oNOSF source $\mathbf{X}$, we have that $H^\varepsilon_\infty(\mathsf{Cond}(\mathbf{X})) \geq m - \left(\frac{\ell}{\varepsilon}\right)^{O(1)} \log(n)$ where $m = 0.001 \cdot \ell n$.*

Proof sketch. Let $\gamma = 0.67 - (2/3)$. Let $\ell' = \ell/3$. We decompose the input $\mathbf{X}$ into three equal sized parts so that $\mathbf{X} = (\mathbf{X}_1, \mathbf{X}_2, \mathbf{X}_3)$ where all $\mathbf{X}_1, \mathbf{X}_2, \mathbf{X}_3 \sim (\{0,1\}^n)^{\ell'}$. Since $\mathbf{X}$ has $((2/3) + \gamma)\ell$ good players, we easily see that each $\mathbf{X}_i$ is a $(g = 3\gamma\ell', \ell', n)$-oNOSF source.

We use $\mathbf{X}_1$ to sample a $O(\log(\ell))$ sized committee from $\mathbf{X}_3$. To do so, we use $\mathsf{oNOSFSamp}_{1\to 3} : (\{0,1\}^n)^{\ell'} \to (\{0,1\}^{\ell'})^D$ from Lemma 14 with $S \subset [\ell']$ being the set of good players from $\mathbf{X}_3$, the approximation factor $\varepsilon_a = \gamma$ and sampling error $\varepsilon_s = \varepsilon/3$. Let $\mathcal{C}_3 \subset [\ell'], |\mathcal{C}_3| \leq D_3 = O(\log(\ell'/\varepsilon)) = O(\log(\ell/\varepsilon))$ be the committee of players thus obtained. The approximation property of the sampler guarantees us that out of $\geq 3\gamma\ell'$ good players in $\mathbf{X}_3$, at least $2\gamma\,|\mathcal{C}_3|$ many good players will be in $\mathcal{C}_3$ with probability $1 - \varepsilon/3$. Let $\mathbf{Y}_3$ be the $(2\gamma D_3, D_3, n)$-oNOSF source obtained by restricting the players in $\mathbf{X}_3$ to the committee $\mathcal{C}_3$. We finally use 2Cond from Lemma 15 and output $\mathsf{2Cond}(\mathbf{X}_2, \mathbf{Y}_3)$. Here, the parameter t in Lemma 15 will be set to $D \leq O(\log(\ell/\varepsilon))$, and hence, Lemma 15 would only require that $n \geq (C_{\mathsf{2Cond}})^t \log(\ell n/\varepsilon) = \left(\frac{\ell}{\varepsilon}\right)^{O(1)}$, a condition that we do meet. We carefully compute the remaining parameters to infer the claim. ◀

2.1.3 Construction 3: 76% good and $n \geq \text{poly}(\log(\ell))$

We build on our previous construction and show how to condense when the block length requirement is again exponentially decreased. This comes at a cost of slightly larger fraction of good blocks.

▶ **Theorem 18.** *For all $\varepsilon > 0$ and $n, \ell \in \mathbb{N}$ where $n \geq \left(\frac{\log(\ell)}{\varepsilon}\right)^{\Omega(1)}$, there exists an explicit condenser $\mathsf{Cond} : (\{0,1\}^n)^\ell \to \{0,1\}^m$ such that for any $(g = 0.76\ell, \ell, n)$-oNOSF source $\mathbf{X}$, we have that $H^\varepsilon_\infty(\mathsf{Cond}(\mathbf{X})) \geq m - \left(\frac{\log(\ell)}{\varepsilon}\right)^{O(1)} \log(n)$ where $m = 0.001 \cdot \ell n$.*

Proof sketch. Let $\gamma = 0.01$. Let $\ell' = \ell/4$. We decompose the input $\mathbf{X}$ into four equal sized parts such that $\mathbf{X} = (\mathbf{X}_1, \mathbf{X}_2, \mathbf{X}_3, \mathbf{X}_4)$ and conclude that each $\mathbf{X}_i$ is a $(g = 4\gamma\ell', \ell', n)$-oNOSF source. However here, we claim something stronger. Call $i \in [\ell']$ a totally good index if it corresponds to a good player across each of the four blocks. Since $\mathbf{X}$ has $(3/4 + \gamma) \cdot (4\ell')$ good players, there must be $\geq 4\gamma\ell'$ totally good indices.

We first use $\mathbf{X}_1$ to sample a $D_2 = O(\log(\ell/\varepsilon))$ sized committee $\mathcal{C}_2 \subset [\ell']$ using the sampler from Lemma 14 such that $\mathcal{C}_2$ will have at least 3γ fraction of totally good indices. We let $\mathbf{Y}_2$ be the $(g = 3\gamma D_2, D_2, n)$-oNOSF source obtained by restricting $\mathbf{X}_2$ to indices from $\mathcal{C}_2$.

Second, we use $\mathbf{Y}_2$ to sample a $D_4 = O(\log(\log(\ell)/\varepsilon))$ sized committee $\mathcal{C}_4 \subset \mathcal{C}_2$ such that $\mathcal{C}_4$ has at least 2γ fraction of totally good indices. We let $\mathbf{Y}_4$ be the $(g = 2\gamma D_4, D_4, n)$-oNOSF source obtained by restricting $\mathbf{X}_4$ to indices from $\mathcal{C}_4$.

Third and last, we use $\mathsf{2Cond}$ from Lemma 15 and output $\mathsf{2Cond}(\mathbf{X}_3, \mathbf{Y}_4)$. Here, the parameter t in Lemma 15 will be set to $D_4 \leq O(\log(\log(\ell)/\varepsilon))$, and hence, Lemma 15 would only require that $n \geq (C_{\mathsf{2Cond}})^t \log(\ell n/\varepsilon) = \left(\frac{\log(\ell)}{\varepsilon}\right)^{O(1)}$, a condition that we do meet. We carefully compute the remaining parameters to infer the claim. ◀

2.1.4 Construction 4: 67% good and $n \geq \mathbf{poly}(\log(\ell))$

Our next construction maintains a similar guarantee as before on the block length and decreases the requirement on the fraction of good blocks.

▶ **Theorem 19.** *For all $\varepsilon > 0$ and $n, \ell \in \mathbb{N}$ where $n \geq \left(\frac{\log(\ell)}{\varepsilon}\right)^{\Omega(1)}$, there exists an explicit condenser $\mathsf{Cond} : (\{0,1\}^n)^\ell \to \{0,1\}^m$ such that for any $(g = 0.67\ell, \ell, n)$-oNOSF source $\mathbf{X}$, we have that $H^\varepsilon_\infty(\mathsf{Cond}(\mathbf{X})) \geq m - \left(\frac{\log(\ell)}{\varepsilon}\right)^{O(1)} \log(n)$ where $m = 0.001 \cdot \ell n$.*

Proof sketch. Let $\gamma = 0.67 - (2/3)$. Let $\ell' = \ell/3$. We decompose $\mathbf{X} = (\mathbf{X}_1, \mathbf{X}_2, \mathbf{X}_3)$ so that each $\mathbf{X}_i$ is a $(g = 3\gamma\ell', \ell', n)$-oNOSF source with $3\gamma\ell'$ totally good indices.

For the first step, we again use $\mathbf{X}_1$ along with a sampler from Lemma 14 to obtain $\mathcal{C}_2 \subset [\ell']$ with $D_2 = |\mathcal{C}_2| \leq O(\log(\ell/\varepsilon)$ and a subsource of $\mathbf{X}_2$ restricted to $\mathcal{C}_2$ - Y_2 that is a $(g = 2\gamma D_2, D_2, n)$-oNOSF source. For the second step, we again use $\mathbf{Y}_2$ to sample a $D_3 = O(\log(\log(\ell)/\varepsilon))$ sized committee $\mathcal{C}_3 \subset \mathcal{C}_2$ such that $\mathcal{C}_3$ has $\geq \gamma$ fraction of totally good indices. We let $\mathbf{Y}_3$ be the $(g = \gamma D_3, D_3, n)$-oNOSF source obtained by restricting $\mathbf{X}_3$ to indices from $\mathcal{C}_3$. Third and last, we use $\mathsf{2Cond}$ from Lemma 15 and output $\mathsf{2Cond}(\mathbf{X}_2, \mathbf{Y}_3)$. Again the parameter t in Lemma 15 will be set to $D_3 \leq O(\log(\log(\ell)/\varepsilon))$ and would only require that $n \geq \left(\frac{\log(\ell)}{\varepsilon}\right)^{O(1)}$.

Analyzing this construction requires more care since we use $\mathbf{X}_2$ to both sample from $\mathbf{X}_3$ and as a source for $\mathsf{2Cond}$. We use the chain rule for min-entropy to argue that most fixings of $\mathbf{Y}_2 = y_2$ will leave $\mathbf{X}_2$ with lot of entropy (since sampler requires few random bits) and observe that such a fixing still leaves $\mathbf{X}_3$ as oNOSF source with the same parameters. Also since for most fixings of $\mathbf{Y}_2 = y_2$, the committee $\mathcal{C}_3$ has γ fraction of good players, we obtain our claim. ◀

2.1.5 Construction 5: 51% good and $n \geq \mathbf{poly}(\log(\ell))$

We lastly construct the condenser promised in our main result (Theorem 13).

Proof sketch of Theorem 13. Let $\gamma = 0.01$. Let $\ell' = \ell/2$. We decompose $\mathbf{X} = (\mathbf{X}_1, \mathbf{X}_2)$ so that each $\mathbf{X}_i$ is a $(g = 2\gamma\ell', \ell', n)$-oNOSF source with $2\gamma\ell'$ totally good indices.

For the first step, we let $\mathbf{X}'_1$ be the $(2\gamma\ell', \ell', n'_1)$-oNOSF source obtained by taking a prefix of length n'_1 from each source where we set $n'_1 \ll n$ but also n'_1 is long enough to be used by the sampler from Lemma 14. We use $\mathbf{X}'_1$ with such a sampler to obtain a committee $\mathcal{C}_{1\to2} \subset [\ell']$ with $D_{1\to2} = |\mathcal{C}_{1\to2}| \leq O(\log(\ell/\varepsilon)$ and a subsource of $\mathbf{X}_2$ restricted to $\mathcal{C}_{1\to2}$, which we call $\mathbf{Y}_{1\to2}$, that is a $(g = (3/2)\gamma D_{1\to2}, D_{1\to2}, n)$-oNOSF source.

We argue that: 1) most fixings of $\mathbf{X}'_1$ are such that they leave $\mathbf{X}_1$ with high entropy, and 2) that the committee $\mathcal{C}_{1\to2}$ obtained will have $3\gamma/2$ fraction of good players. We obtain this using the chain rule for min-entropy and by guarantees of the sampler. We condition on such a fixing from here on.

For the second step, we use $\mathbf{Y}_{1\to2}$ to sample a $D_{2\to2} = O(\log(\log(\ell)/\varepsilon))$ sized committee $\mathcal{C}_{2\to2} \subset \mathcal{C}_{1\to2}$ such that $\mathcal{C}_{2\to2}$ has $\geq \gamma$ fraction of totally good indices. We let $\mathbf{Y}_{2\to2}$ be the $(g = \gamma D_{2\to2}, D_{2\to2}, n)$-oNOSF source obtained by restricting $\mathbf{X}_2$ to indices from $\mathcal{C}_{2\to2}$.

Lastly, we use 2Cond from Lemma 15 and output $\mathsf{2Cond}(\mathbf{X}_1, \mathbf{Y}_{2\to 2})$. The parameter t in Lemma 15 will be set so that it would only require that $n \geq \left(\frac{\log(\ell)}{\varepsilon}\right)^{O(1)}$. We must be a bit careful about the error parameter $\varepsilon_{\mathsf{2Cond}}$ for 2Cond and we will choose it to be extremely small.

Analyzing this construction requires care since we use $\mathbf{X}_2$ both to sample from within $\mathbf{X}_2$ itself and also as a seed for 2Cond. We cannot use the chain rule since a fixing of $\mathbf{Y}_{1\to 2}$ will destroy the structure of the source $\mathbf{X}_2$. We first see that the sampler guarantees that no matter how the adversary behaves, with probability $1 - \varepsilon/4$, the sampler will succeed in selecting a committee $\mathcal{C}_{2\to 2}$ with γ fraction of good players. We pay $\varepsilon/4$ in error and now assume that the sampler always succeeds in doing so. We then compare two scenarios: one scenario Opt where the bits in $\mathbf{Y}_{1\to 2}$ are all uniform and independent of all other bits and another scenario Adv where the bits in $\mathbf{Y}_{1\to 2}$ are all controlled by an adversary (guarantees on this latter scenario suffice for our claim). Let the total number of bits in $\mathbf{Y}_{1\to 2}$ be equal to $b_{1\to 2}$. Under scenario Opt, we easily see that we succeed and with error $\varepsilon_{\mathsf{2Cond}}$ will have high entropy - say k. We compare this to scenario Adv and use the fact that the adversary can only control few bits, to conclude that in scenario Adv, with error $\varepsilon_{\mathsf{2Cond}} \cdot 2^{b_{1\to 2}}$, the output will have entropy $k - b_{1\to 2}$. Since we carefully chose $\varepsilon_{\mathsf{2Cond}}$ to be small enough and $b_{1\to 2}$ is small since we only use $\mathbf{Y}_{1\to 2}$ as source for the sampler, the output will still have small error and will have high-entropy as desired. ◀

2.1.6 Construction of 2Cond

We now sketch how to construct our desired 2Cond.

Proof sketch of Lemma 15. Let $\mathbf{X}$ and $\mathbf{Y} = (\mathbf{Y}_1, \ldots, \mathbf{Y}_t)$ be the two sources. For $i \in [t]$, let $n_i \approx C^{t-i+1} \log(tn_x/\varepsilon)$ where C is a large constant. For $i \in [t]$, let $\mathbf{Z}_i$ be the length n_i prefix of the block $\mathbf{Y}_i$. Our final construction will be the parity of the outputs of seeded extractors applied with source $\mathbf{X}$ and seeds $\mathbf{Z}_i$. More formally, we output

$$\bigoplus_{i=1}^{t} \mathsf{sExt}_i(\mathbf{X}, \mathbf{Z}_i),$$

where sExt_i is any explicit near optimal seeded extractor such a from [25].

We proceed to sketch the analysis. We are guaranteed that there exists at least one $j \in [t]$ from $\mathbf{Y}$ that is good. We first condition on fixing blocks $\mathbf{Z}_1, \ldots, \mathbf{Z}_{j-1}$. Since these blocks can depend on $\mathbf{X}$, we apply the chain rule for min-entropy and conclude $\mathbf{X}$ will only lose some small amounts of entropy (the amount will be very small since these blocks are tiny compared to the amount entropy in $\mathbf{X}$). Moreover, since the adversary is online, $\mathbf{Z}_j$ remains uniform even after this fixing. We now view our construction as

$$g(\mathbf{X}) \oplus \bigoplus_{i=j}^{t} \mathsf{sExt}_i(\mathbf{X}, \mathbf{Z}_i)$$

where g is the fixed function obtained by fixing $\mathbf{Y}_1, \ldots, \mathbf{Y}_{j-1}$.

We now compare two scenarios: (1) Where all of $\mathbf{Z}_j, \ldots, \mathbf{Z}_t$ are uniform (2) Only $\mathbf{Z}_j$ is uniform and $\mathbf{Z}_{j+1}, \ldots, \mathbf{Z}_t$ are arbitrarily controlled by an adversary and can even depend on $\mathbf{X}$:

In the first scenario, we further condition on fixing $\mathbf{Z}_{j+1}, \ldots, \mathbf{Z}_t$. Since in this scenario $\mathbf{Z}_i$ are independent and random, $\mathbf{X}$ retains the same entropy and $\mathbf{Y}_j$ remains uniform. So our overall output is of the form $h(\mathbf{X}) \oplus \mathsf{sExt}_j(\mathbf{X}, \mathbf{Z}_j)$ for some fixed function h. We condition

on fixing output $h(\mathbf{X})$. Since the number of output bits $m \ll H_\infty(\mathbf{X})$, we apply the chain rule to infer that $\mathbf{X}$ still has lots of entropy when we do this fixing. Now the output is just $z \oplus \mathsf{sExt}_j(\mathbf{X}, \mathbf{Z}_j)$ where z is a fixed string, and hence is uniform.

The second scenario is more realistic and, in the worst case, this is what can actually happen. We then use the result that if an adversary controls few bits in the input distribution, then they cannot make the output of the condenser too bad. With this, since we carefully chose geometrically decreasing lengths of $\mathbf{Z}_i$ to help control the error, we indeed obtain that the output will be condensed. ◀

2.2 Converting Low-Entropy oNOSF Sources to Uniform oNOSF Sources

They key part of our proof for condensing from low-entropy oNOSF sources is a transformation from low-entropy oNOSF sources to uniform oNOSF sources. Here, we sketch the proof for our transformation in Theorem 6 and compare it to that of [10]. Both these transformations rely on two-source extractors as a basic primitive.

Given a (g, ℓ, n, k)-oNOSF source $\mathbf{X} = \mathbf{X}_1, \ldots, \mathbf{X}_\ell$, [10] uses excellent existential two-source extractors to define output blocks $\mathbf{O}_i = 2\mathsf{Ext}(\mathbf{X}_1 \circ \cdots \circ \mathbf{X}_{i-1}, \mathbf{X}_i)$ for $i \in \{2, \ldots, \ell\}$ and define their transformation as $f(\mathbf{X}) = \mathbf{O}_2, \ldots, \mathbf{O}_\ell$. They show that $\mathbf{O}_i$ is a good block if: (1) $\mathbf{X}_i$ is a good block and (2) at least one block amongst $\mathbf{X}_1, \ldots, \mathbf{X}_{i-1}$ is a good block. They showed that such a good block will be uniform and independent of the blocks $\mathbf{O}_2, \ldots, \mathbf{O}_{i-1}$ and argued there will be $g - 1$ such good output blocks. This indeed shows their output is a uniform $(g - 1, \ell - 1, m)$-oNOSF source. However, each of their output blocks has length $m = O\left(\frac{k}{\ell}\right) \leq O\left(\frac{n}{\ell}\right)$, and so they were not able to handle the case of $n = o(\ell)$. We improve on their construction by using a "sliding window" based technique to obtain a much better transformation that can even handle $n = \mathrm{poly}(\log(\ell))$.

▶ **Theorem 20.** *Let $d, g, g_{out}, \ell, n, m, k, \varepsilon$ be such that $g_{out} \leq g - \frac{\ell - g + 2}{d}, n \geq k \geq \log(nd - k) + md + 2\log(2g_{out}/\varepsilon)$. Then, there exists a function $f : (\{0,1\}^n)^\ell \to (\{0,1\}^m)^{\ell-1}$ such that for any (g, ℓ, n, k)-oNOSF source $\mathbf{X}$, there exists uniform $(g_{out}, \ell - 1, m)$-oNOSF source $\mathbf{Y}$ for which $|f(\mathbf{X}) - \mathbf{Y}| \leq \varepsilon$.*

The parameter d in our theorem statement above is the width of our sliding window. When we set $d = \ell$ we recover the analysis of [10]. The true advantage of our transformation emerges when d is very small compared to ℓ. For instance, when $g = 0.51\ell, n = \mathrm{poly}(\log(\ell))$ and $k = \mathrm{poly}(\log(\ell))$, we set d to be a large constant and conclude that the output distribution is a uniform $(0.509\ell, \ell, \mathrm{poly}(\log(\ell))$-NOSF source.

Proof sketch of Theorem 20. Define $\mathbf{O}_i = 2\mathsf{Ext}(\mathbf{X}_{i-d} \circ \cdots \circ \mathbf{X}_{i-1}, \mathbf{X}_i)$. We call $\mathbf{O}_i$ a good output block when $\mathbf{X}_i$ is good and there is at least one good block amongst $\{\mathbf{X}_{i-d}, \ldots, \mathbf{X}_{i-1}\}$.

We first compute the number of good output blocks g_{out}. Let $j_1, \ldots, j_g$ be the indices of the good input blocks in $\mathbf{X}$ and $d_i = j_{i+1} - j_i$ be the gap between the i-th good block and the next $(i+1)$-th good block. If the gap d_i is at most d, then $\mathbf{O}_{i+1}$ must be a good output block. So, g_{out} is the number of i such that $d_i \leq d$. Since $g \geq 0.51\ell$, such large gaps cannot appear too often and we compute that $g_{out} \geq g - \frac{\ell - g + 2}{d}$ as desired.

Next, we show that the good output blocks are indeed uniform conditioned on all previous output blocks. With this, we will obtain that the output distribution will be uniform $(g_{out}, \ell - 1, m)$-oNOSF source as desired. Let i be the index of a good output block. We want to show that $\mathbf{O}_i$ is uniform conditioned on $\mathbf{O}_1, \ldots, \mathbf{O}_{i-1}$. To do this, we first observe that any input block contributes to at most $d + 1$ good output blocks. This means

that$(\mathbf{X}_{i-d} \circ \cdots \circ \mathbf{X}_{i-1})$, which has min-entropy at least k, loses at most $d \cdot m$ min-entropy conditioned on fixing $\mathbf{O}_1, \ldots, \mathbf{O}_{i-1}$. Moreover, $\mathbf{X}_i$ still remains uniform and independent of $(\mathbf{X}_{i-d} \circ \cdots \circ \mathbf{X}_{i-1})$ when fixing these previous output blocks. Hence, the output of the two-source extractor will indeed be uniform as desired. ◀

We can make Theorem 20 explicit by using the explicit two-source extractors at a slight cost of dependence on m and ε.

2.3 Existence of oNOSF Condensers for All ℓ and n

Here we sketch the proof of Theorem 7. This result states that when $g = 0.51\ell$ and $n = 1000$, there exists a condenser Cond for uniform (g, ℓ, n)-oNOSF sources so that the output entropy rate is 0.99, the number of output bits is $m = O(\ell + \log(1/\varepsilon))$, and the error of the condenser is ε where $\varepsilon \leq 2^{-\Omega(\ell)}$ is arbitrary.

Our construction uses amazing seeded condensers with $1 \cdot \log(1/\varepsilon)$ dependence on seed length. We slightly modify our source and then apply such seeded condenser. Here is a proof sketch:

Proof sketch for Theorem 7. Let $\mathbf{X} = (\mathbf{X}_1, \ldots, \mathbf{X}_\ell)$ be such a source. Let $\mathbf{Y}_1 \sim (\{0,1\}^n)^{0.5\ell}$ be the source obtained by concatenating the first 0.5ℓ blocks of $\mathbf{X}$. Since 0.51ℓ blocks are good, there exist at least 0.01ℓ uniform blocks in $\mathbf{Y}_1$. We treat $\mathbf{Y}_1$ as a single distribution over $n\ell$ bits with min-entropy $\geq 0.01\ell n$. Let $\mathbf{Y}_2 \sim \{0,1\}^{0.5\ell}$ be the source obtained by concatenating 1 bit from each of the last 0.5ℓ blocks of $\mathbf{X}$. Once again, since 0.51ℓ blocks are good, there exist at least 0.01ℓ uniform bits in $\mathbf{Y}_2$. We will use the following seeded condenser:

▶ **Theorem 21.** *For all d, ε such that $d \geq \log(\ell n/\varepsilon) + O(1)$, there exists a seeded condenser $\mathsf{sCond} : \{0,1\}^{0.5\ell n} \times \{0,1\}^d \to \{0,1\}^m$ such that for all $\mathbf{X} \sim \{0,1\}^{0.5\ell n}$ with $H_\infty(\mathbf{X}) \geq 0.01\ell n$, we have $H^\varepsilon_\infty(\mathsf{sCond}(\mathbf{X}, \mathbf{U}_d)) \geq 0.01\ell n + d$ where $m = 0.01\ell n + d + \log(1/\varepsilon) + O(1)$.*

Our condenser Cond will output $\mathsf{sCond}(\mathbf{Y}_1, \mathbf{Y}_2)$. Observe that not only is $\mathbf{Y}_2$ not uniform, there could be as many as 0.49ℓ "bad bits" in $\mathbf{Y}_2$ that can depend on $\mathbf{Y}_1$. To remedy this, we use the well known fact that the behavior of such adversarial $\mathbf{Y}_2$ cannot be far worse than the behavior if $\mathbf{Y}_2$ were uniform. Concretely, suppose if $\mathbf{Y}_2$ were uniform and the output entropy and error were k and ε. Then for the actual $\mathbf{Y}_2$, the output entropy will be $k - 0.49\ell$ and error will be $\varepsilon \cdot 2^{0.49\ell}$.

For us, it means the following: let $\varepsilon_{\mathsf{sCond}}, k_{\mathsf{sCond}}$ be such that $H^{\varepsilon_{\mathsf{sCond}}}_\infty(\mathsf{sCond}(\mathbf{Y}_1, \mathbf{U}_{0.5\ell})) \geq k_{\mathsf{sCond}}$. Then, it must be that $H^{2^{0.49\ell} \cdot \varepsilon_{\mathsf{sCond}}}_\infty(\mathsf{sCond}(\mathbf{Y}_1, \mathbf{Y}_2)) \geq k_{\mathsf{sCond}} - 0.49\ell$. So, for our final error to be some ε, we need to have $\varepsilon_{\mathsf{sCond}} = \varepsilon \cdot 2^{-0.49\ell}$. For seeded condensers to exist, we need $0.5\ell \geq \log(\ell n/\varepsilon_{\mathsf{sCond}}) + O(1)$ and we check that such an inequality can indeed be satisfied if $\varepsilon \geq 2^{-0.01\ell}$.

Hence, we finally obtain that our seeded condenser will output $0.01\ell n + O(\ell)$ bits and will have output entropy $m - \Delta$ where $\Delta = O(\ell)$. Hence, if n is a large enough constant, our output entropy rate, $\frac{m-\Delta}{m}$, will be ≥ 0.99 as desired. ◀

▶ Remark 22. Here (in the inequality $0.5\ell \geq 1 \cdot \log(\ell n/\varepsilon_{\mathsf{sCond}})$) we crucially used the fact that there exist seeded condensers with seed length dependence $1 \cdot \log(1/\varepsilon)$. Currently, we do not have explicit constructions with this dependence. We also could not have used a seeded extractor since for them, the seed length dependence is $2 \cdot \log(1/\varepsilon)$. For that to work, we would need to assume $g \geq 0.76\ell$.

2.4 Online Influence and Extractor Lower Bounds

In this subsection, we provide a brief overview of our results regarding online influence and sketch how they imply extractor lower bounds against oNOBF sources. We also contrast this with the established notion of influence for Boolean functions. For any function $f : \{0,1\}^n \to \{0,1\}$, define the function $e(f)(x) = (-1)^{f(x)}$.

A Poincaré inequality and extractor lower bounds

One fundamental inequality about regular influence is the Poincaré inequality which states that $\mathrm{Var}(f) \leq \mathbf{I}[f]$. We prove a similar result for online influence.

▶ **Theorem 23.** *For any $f : \{0,1\}^\ell \to \{0,1\}$, we have $\mathrm{Var}(e(f)) \leq \mathbf{oI}[f] \leq \sqrt{\ell \,\mathrm{Var}(e(f))}$.*

It is not hard to derive extractor lower bounds for oNOBF sources from the above result. The high level idea is to collect bits with high online influence, which is guaranteed by the first inequality in the above theorem (using an averaging argument) to form a *coalition of coordinates* that has enough online influence to bias the claimed extractor.

The proof of Theorem 23 is based on techniques from the Fourier analysis of Boolean functions. The following key result implies Theorem 23.

▶ **Lemma 24.** *For any $f : \{0,1\}^\ell \to \{0,1\}$ and $i \in [\ell]$,*

$$\mathbf{oI}_i(f)^2 \leq \sum_{\substack{S \subseteq [i] \\ S \ni i}} \widehat{f}(S)^2 \leq \mathbf{oI}_i(f).$$

Influence vs Online Influence

It is not hard to see that $\mathbf{oI}_i[f] \leq \mathbf{I}_i[f]$ for all $i \in [\ell]$, with equality always holding for $i = \ell$ as an adversarial online bit in the last index can see every good bit. Moreover, we observe that for monotone functions, the notion of online influence is equivalent to regular influence, so any separation between the two notions must come from non-monotone functions.

We exactly exhibit such a separation via the address function $\mathrm{Addr}_\ell : \{0,1\}^{\log \ell + \ell} \to \{0,1\}$ which considers its first $\log \ell$ bits as an index in $\{1, \ldots, \ell\}$ and then outputs the value of the chosen index. It is easy to show that the first $\log \ell$ bits of Addr_ℓ have no online influence, while the remaining bits have online influence of $O\left(\frac{1}{\ell}\right)$. This is in contrast to the well known result of [28] showing that, for a balanced function such as Addr_ℓ, there must exist a bit with influence at least $\Omega\left(\frac{\log \ell}{\ell}\right)$.

2.5 Extractors via Leader Election Protocols

We sketch our main idea for constructing an extractor for oNOBF sources. Similar ideas work more generally for extracting from oNOSF sources. As mentioned above, we use a novel connection to leader election protocols to construct extractors.

Suppose π is an $(r-1)$-round leader election protocol over ℓ players where in each round, each player sends 1 bit and with the guarantee that if there are at most $\delta\ell$ bad players, then a good player is chosen as leader with probability $1 - \epsilon$. Suppose $\mathbf{X}$ is an $(g, \ell r)$-oNOBF source, where $g \geq lr - \delta\ell$. We simply partition the bits of $\mathbf{X}$ into chunks $\mathbf{X}_1, \mathbf{X}_2, \ldots, \mathbf{X}_r$, where each X_i is on ℓ bits, and simulate the protocol π by using the j'th bit of $\mathbf{X}_i$ as the message of the j'th player in round i, for all $1 \leq j \leq \ell$ and $1 \leq i \leq r-1$. At the end of this simulation suppose $j^* \in [\ell]$ is the chosen leader. Then we output the j^*'th bit of $\mathbf{X}_r$ as the output of the extractor.

Briefly, the reason that the above is a valid simulation of π is the fact that the value of any bad bit in this online setting just depends on bits that appear before it, which is allowed in the leader election protocol (where in round i, the message of a bad player can be any function of the messages in the same round or previous rounds). The correctness of the extractor now follows from the fact that since the number of bad players (i.e., bad bits in $\mathbf{X}$) is at most $\delta\ell$, the guarantee of the protocol ensures that the chosen leader $j^* \in [\ell]$ is a good player with probability at least $1 - \epsilon$, and in this case the j^*'th bit of $\mathbf{X}_r$ must be uniform.

We note here that in the usual definition of leader election protocols, the requirement is to select a good leader with constant probability, which is a weaker guarantee than what we need to instantiate the above plan. It turns out that we can combine leader election protocols from prior works, in particular from [18] and [3], to construct protocols with the stronger guarantee we require.

3 Application to Collective Coin Flipping and Collective Sampling

We now discuss applications of our results on condensers for oNOSF sources to fault-tolerant distributed computing. Condensing from oNOSF sources can be viewed as a special case of coin flipping and collective sampling protocols in the full information model that arise in fault-tolerant distributed computing.

3.1 Background

Say there are ℓ players who have a common broadcast channel and want to jointly perform a task such as collectively flipping a coin. Some b players out of them are "bad" and want to deter the task. We assume the bad players are computationally unbounded so cryptographic primitives are of no use. We further assume that each player has private access to uniform randomness. [5] initiated the study of this model and aptly termed this task as "collective coin flipping."

The simplest way to collectively flip a coin would be for all the players to initially agree on a function $f : \{0,1\}^\ell \to \{0,1\}$, then synchronously broadcast one random bit r_i, and to finally agree on the output being $f(r_1, \ldots, r_\ell)$. However, synchronizing broadcasts is hard, and it could be that the bad players set their output as function of the bits of the good players. [28] showed that no function f can handle more than $O\left(\frac{\ell}{\log \ell}\right)$ corruptions.

One way to allow for more corruptions (almost linear) among players is to consider "protocols" that allow more rounds of communication. In particular, a protocol can be thought of as a tree where each vertex represents a "round" where in every round the following happens: all good players sends their bits, then all bad players send their bits as a function of the bits of the good players, and they jointly compute a function of these bits. Depending on the outcome of the function, everyone branches on one branch in this tree. Furthermore, every leaf is labeled with final outcomes (say 0 or 1) and, once a leaf is reached, that is the outcome that everybody agrees on. [20] initiated the study of protocols where the outcomes are from a larger range and where the bad players are trying to minimize the largest probability of any outcome. They called this problem "collective sampling."

3.1.1 Known Results

[5] showed that for protocols with outcomes $\{0,1\}$, b bad players can always ensure that some outcome occurs with probability at least $\frac{1}{2} + \frac{b}{2\ell}$. [3] first constructed a protocol that can handle a linear number of corruptions. Follow-up works tried to reduce the number of rounds in this protocol where, in some settings, players were allowed to send more than one bit per round [36, 18].

[20] showed that for all collective sampling protocols and all outcomes, there exists a way for b bad players to coordinate and ensure that an outcome that happens without corruption with probability p, now happens with probability $p^{1-(b/n)} \geq p\left(1 + \frac{b}{n}\log(1/p)\right)$. Nearly matching collective sampling protocols were constructed by [20, 37, 24]. For an overview of further results and bounds, see [13].

3.2 Connection to oNOSF Sources

The problem of extracting or condensing from oNOSF sources can be seen as special cases or variants of collective coin flipping and collective sampling that provide very simple protocols. For instance, suppose one has an extractor or condenser f for uniform (g, ℓ, n)-oNOSF sources. Then, consider a protocol where all ℓ players take turns and output n random bits. The agreed final outcome is f applied on these ℓn bits. This leads to protocols that are structurally much simpler since players don't have to carefully compute whose turn it is to go in various rounds and can obliviously prepare for their turn.

The above protocol can also be viewed as a relaxed version of a 1-round protocol where instead of everyone providing their output asynchronously, they take turns and provide outputs one after another in a simple sequential manner.

3.2.1 Previous Results Interpreted in oNOSF source context

Previous impossibility results can be interpreted in the context of extracting / condensing from uniform oNOSF sources. For instance, collective coin flipping impossibility results of [5] imply extraction impossibility results for uniform (g, ℓ, n)-oNOSF sources when $n = 1$. They imply:

▶ **Corollary 25.** *There does not exist an $\frac{b}{2\ell}$-extractor for uniform $(g, \ell, 1)$-oNOSF sources.*

Similarly, we observe that the notion of collective sampling is equivalent to 0-error condensing. Hence, lower bounds of [20] imply 0-error condensing lower bounds for uniform (g, ℓ, n)-oNOSF sources when $n = 1$. Formally:

▶ **Corollary 26.** *There does not exist a condenser $\mathsf{Cond} : \{0,1\}^\ell \to \{0,1\}^m$ for uniform $(g, \ell, 1)$-oNOSF sources that can guarantee output smooth min-entropy (with parameter $\varepsilon = 0$) more than $k = \frac{g}{\ell} \cdot m$.*

3.2.2 ε-Collective Sampling

Since collective sampling lower bounds show that for any protocol, 0-error condensing beyond rate g/ℓ is impossible, one can naturally ask whether condensing with small error ε is possible. We call this problem *ε-collective sampling*, where the goal is to output a distribution which is ε-close to a distribution where every output has small probability.

Interpreted this way, this is exactly what protocols arising out of our condensers for uniform oNOSF sources provide: Using Theorem 7, when each player has access to 10^4 random bits, there exists a simple protocol that can handle 0.49ℓ corrupt players such that the players can collectively sample a distribution over $m = O(\ell)$ bits which is $2^{-\Omega(\ell)}$-close to having entropy $0.99m$. As far as we are aware, such a protocol is not implied by any other previous protocol. Most previous protocols are obtained through *leader election* protocols, which do not seem useful here since the leader has access to only constant number of bits.

We similarly obtain explicit protocols using Theorem 4 for the case when each player has access to $n \geq \text{poly}(\log(\ell)/\varepsilon)$ many bits.

3.2.3 Collective Coin Flipping and Sampling with Weak Random Sources

A natural extension to collective coin flipping and sampling in the full information model is when all players only have access to weak source of randomness (that are independent from each other) instead of true uniform randomness. This question was first studied by [21]. [29] used network extractor protocol to transform weak random sources of each player into independent private random sources. This way, after using the network extraction protocol, players can follow the usual collective coin flipping / sampling protocol. [23] improved the network extraction protocol using two-source non-malleable extractors.

Using our (g, ℓ, n, k)-oNOSF source condensers, we obtain alternative, simple ε-collective sampling protocols in the setting where players have access to weak sources of randomness. We obtain such an existential protocol using Theorem 8, and explicit protocol using Corollary 5.

4 Open Problems

We list here some interesting open problems left by our work:

- While we obtain explicit condensers for almost all parameter regimes, it remains open to construct them when the bock length is constant, matching the parameters of our existential results. As we show, one way of achieving this would be to explicitly construct a seeded condenser with dependence on seed length being $1 \cdot \log(1/\varepsilon)$.
- All our condensers have entropy gap much larger than a constant. It will be interesting to show there exist condensers with constant entropy gap (for any values of n, ℓ) for uniform oNOSF sources. A slightly weaker but equally interesting question is to construct seeded extractors for uniform oNOSF sources with constant seed length.
- Show that there exist non-trivial condensers for oNOBF sources or show no such condenser exists. We conjecture that no condenser exists with output entropy rate larger than the input entropy rate for such sources.
- Construct ε-collective sampling protocols with fewer rounds than the ones obtained using uniform oNOSF source condensers. It will also be interesting to explicitly construct such protocols when the number of players are very large compared to the number of bits each player has access to. Further, proving lower bounds for ε-collective sampling protocols is a natural direction to explore.
- Determine the exact threshold for extracting from oNOBF sources and oNOSF sources. Our lower bounds show extraction is impossible when $g \leq 0.99\ell$ while our constructions using leader election protocols require $g \geq \ell - \Omega\left(\frac{\ell}{\log \ell}\right)$ for oNOBF sources and $g \geq \ell - \Omega\left(\frac{\ell}{\log^*(\ell)}\right)$ for (g, ℓ, n)-oNOSF sources where $n \geq \log(\ell)$. Using the connection between extractors and leader election protocols, lower bounds for extraction imply lower bounds for leader election protocols. In particular, matching lower bounds for extraction would imply all current leader election protocols are tight, a long standing open problem.

References

1 Divesh Aggarwal, Maciej Obremski, João Ribeiro, Luisa Siniscalchi, and Ivan Visconti. How to Extract Useful Randomness from Unreliable Sources. In Anne Canteaut and Yuval Ishai, editors, *Advances in Cryptology – EUROCRYPT 2020*, Lecture Notes in Computer Science, pages 343–372, Cham, 2020. Springer International Publishing. doi:10.1007/978-3-030-45721-1_13.

2 Miklós Ajtai and Nathan Linial. The influence of large coalitions. *Combinatorica*, 13(2):129–145, 1993. doi:10.1007/BF01303199.

3 Noga Alon and Moni Naor. Coin-flipping games immune against linear-sized coalitions. *SIAM J. Comput.*, 22(2):403–417, 1993. doi:10.1137/0222030.

4 Mihir Bellare, Zvika Brakerski, Moni Naor, Thomas Ristenpart, Gil Segev, Hovav Shacham, and Scott Yilek. Hedged Public-Key Encryption: How to Protect against Bad Randomness. In Mitsuru Matsui, editor, *Advances in Cryptology – ASIACRYPT 2009*, pages 232–249, Berlin, Heidelberg, 2009. Springer. doi:10.1007/978-3-642-10366-7_14.

5 Michael Ben-Or and Nathan Linial. Collective Coin Flipping. *Advances In Computing Research*, 5:91–115, 1989. URL: https://www.cs.huji.ac.il/~nati/PAPERS/coll_coin_fl.pdf.

6 Iddo Bentov, Ariel Gabizon, and David Zuckerman. Bitcoin Beacon, 2016. arXiv:1605.04559 [cs]. doi:10.48550/arXiv.1605.04559.

7 Joseph Bonneau, Jeremy Clark, and Steven Goldfeder. On Bitcoin as a public randomness source, 2015. Publication info: Preprint. MINOR revision. URL: https://eprint.iacr.org/2015/1015.

8 Jean Bourgain, Jeff Kahn, Gil Kalai, Yitzhak Katznelson, and Nathan Linial. The influence of variables in product spaces. *Israel Journal of Mathematics*, 77(1):55–64, 1992. doi:10.1007/BF02808010.

9 Benedikt Bünz, Steven Goldfeder, and Joseph Bonneau. Proofs-of-delay and randomness beacons in ethereum. *IEEE Security and Privacy on the blockchain (IEEE S&B)*, 2017.

10 Eshan Chattopadhyay, Mohit Gurumukhani, and Noam Ringach. On the existence of seedless condensers: Exploring the terrain. In *Proceedings of the 65th Annual IEEE Symposium on Foundations of Computer Science (FOCS)*, 2024. To appear.

11 Eshan Chattopadhyay and David Zuckerman. Explicit two-source extractors and resilient functions. *Annals of Mathematics*, 189(3):653–705, 2019. doi:10.4007/annals.2019.189.3.1.

12 Benny Chor, Oded Goldreich, Johan Hasted, Joel Freidmann, Steven Rudich, and Roman Smolensky. The bit extraction problem or t-resilient functions. In *Proceedings of the 26th Annual Symposium on Foundations of Computer Science*, SFCS '85, pages 396–407, USA, 1985. IEEE Computer Society. doi:10.1109/SFCS.1985.55.

13 Yevgeniy Dodis. Fault-tolerant leader election and collective coin-flipping in the full information model, 2006.

14 Yevgeniy Dodis, Krzysztof Pietrzak, and Daniel Wichs. Key derivation without entropy waste. In Phong Q. Nguyen and Elisabeth Oswald, editors, *Advances in Cryptology - EUROCRYPT 2014 - 33rd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Copenhagen, Denmark, May 11-15, 2014. Proceedings*, volume 8441 of *Lecture Notes in Computer Science*, pages 93–110. Springer, 2014. doi:10.1007/978-3-642-55220-5_6.

15 Dean Doron, Dana Moshkovitz, Justin Oh, and David Zuckerman. Almost Chor-Goldreich Sources and Adversarial Random Walks. In *Proceedings of the 55th Annual ACM Symposium on Theory of Computing*, STOC 2023, pages 1–9, New York, NY, USA, June 2023. Association for Computing Machinery. doi:10.1145/3564246.3585134.

16 Dean Doron, Dana Moshkovitz, Justin Oh, and David Zuckerman. Online Condensing of Unpredictable Sources via Random Walks. In Srikanth Srinivasan, editor, *40th Computational Complexity Conference (CCC 2025)*, volume 339 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 30:1–30:17, Dagstuhl, Germany, 2025. Schloss Dagstuhl – Leibniz-Zentrum für Informatik. doi:10.4230/LIPIcs.CCC.2025.30.

17 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.

18 Uriel Feige. Noncryptographic selection protocols. In *40th Annual Symposium on Foundations of Computer Science, FOCS '99, 17-18 October, 1999, New York, NY, USA*, pages 142–153. IEEE Computer Society, 1999. doi:10.1109/SFFCS.1999.814586.

19 O. Goldreich, S. Goldwasser, and N. Linial. Fault-tolerant computation in the full information model. In *[1991] Proceedings 32nd Annual Symposium of Foundations of Computer Science*, pages 447–457, 1991. doi:10.1109/SFCS.1991.185405.

20 Oded Goldreich, Shafi Goldwasser, and Nathan Linial. Fault-tolerant computation in the full information model. *SIAM J. Comput.*, 27(2):506–544, 1998. doi:10.1137/S0097539793246689.

21 Shafi Goldwasser, Madhu Sudan, and Vinod Vaikuntanathan. Distributed computing with imperfect randomness. In Pierre Fraigniaud, editor, *Distributed Computing, 19th International Conference, DISC 2005, Cracow, Poland, September 26-29, 2005, Proceedings*, volume 3724 of *Lecture Notes in Computer Science*, pages 288–302. Springer, 2005. doi:10.1007/11561927_22.

22 Jesse Goodman, Xin Li, and David Zuckerman. Improved condensers for chor-goldreich sources. In *Proceedings of the 65th Annual IEEE Symposium on Foundations of Computer Science (FOCS)*, 2024. To appear.

23 Vipul Goyal, Akshayaram Srinivasan, and Chenzhi Zhu. Multi-source non-malleable extractors and applications. In Anne Canteaut and François-Xavier Standaert, editors, *Advances in Cryptology - EUROCRYPT 2021 - 40th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zagreb, Croatia, October 17-21, 2021, Proceedings, Part II*, volume 12697 of *Lecture Notes in Computer Science*, pages 468–497. Springer, 2021. doi:10.1007/978-3-030-77886-6_16.

24 Ronen Gradwohl, Salil P. Vadhan, and David Zuckerman. Random selection with an adversarial majority. In Cynthia Dwork, editor, *Advances in Cryptology - CRYPTO 2006, 26th Annual International Cryptology Conference, Santa Barbara, California, USA, August 20-24, 2006, Proceedings*, volume 4117 of *Lecture Notes in Computer Science*, pages 409–426. Springer, 2006. doi:10.1007/11818175_25.

25 Venkatesan Guruswami, Christopher Umans, and Salil Vadhan. Unbalanced expanders and randomness extractors from Parvaresh–Vardy codes. *Journal of the ACM*, 56(4):20:1–20:34, 2009. doi:10.1145/1538902.1538904.

26 Peter Ivanov, Raghu Meka, and Emanuele Viola. Efficient resilient functions. In Nikhil Bansal and Viswanath Nagarajan, editors, *Proceedings of the 2023 ACM-SIAM Symposium on Discrete Algorithms, SODA 2023, Florence, Italy, January 22-25, 2023*, pages 2867–2874. SIAM, 2023. doi:10.1137/1.9781611977554.CH108.

27 Peter Ivanov and Emanuele Viola. Resilient functions: Optimized, simplified, and generalized. *CoRR*, abs/2406.19467, 2024. doi:10.48550/arXiv.2406.19467.

28 J. Kahn, G. Kalai, and N. Linial. The influence of variables on Boolean functions. In *[Proceedings 1988] 29th Annual Symposium on Foundations of Computer Science*, pages 68–80, 1988. doi:10.1109/SFCS.1988.21923.

29 Yael Tauman Kalai, Xin Li, Anup Rao, and David Zuckerman. Network extractor protocols. In *49th Annual IEEE Symposium on Foundations of Computer Science, FOCS 2008, October 25-28, 2008, Philadelphia, PA, USA*, pages 654–663. IEEE Computer Society, 2008. doi:10.1109/FOCS.2008.73.

30 Jesse Kamp and David Zuckerman. Deterministic Extractors for Bit-Fixing Sources and Exposure-Resilient Cryptography. *SIAM Journal on Computing*, 36(5):1231–1247, January 2007. doi:10.1137/S0097539705446846.

31 Xin Li. Extractors for a Constant Number of Independent Sources with Polylogarithmic Min-Entropy. In *Proceedings of the 2013 IEEE 54th Annual Symposium on Foundations of Computer Science*, FOCS '13, pages 100–109, USA, 2013. IEEE Computer Society. doi:10.1109/FOCS.2013.19.

32 Xin Li. New independent source extractors with exponential improvement. In *Proceedings of the forty-fifth annual ACM symposium on Theory of Computing*, STOC '13, pages 783–792, New York, NY, USA, 2013. Association for Computing Machinery. doi:10.1145/2488608.2488708.

33 Raghu Meka. Explicit Resilient Functions Matching Ajtai-Linial. In *Proceedings of the 2017 Annual ACM-SIAM Symposium on Discrete Algorithms (SODA)*, Proceedings, pages 1132–1148. Society for Industrial and Applied Mathematics, 2017. doi:10.1137/1.9781611974782.73.

34 Rajeev Motwani and Prabhakar Raghavan. *Randomized algorithms*. Cambridge University Press, 1995. doi:10.1017/CBO9780511814075.

35 Cécile Pierrot and Benjamin Wesolowski. Malleability of the blockchain's entropy. *Cryptography Commun.*, 10(1):211–233, 2018. doi:10.1007/s12095-017-0264-3.

36 Alexander Russell and David Zuckerman. Perfect information leader election in log* n+o (1) rounds. *J. Comput. Syst. Sci.*, 63(4):612–626, 2001. doi:10.1006/JCSS.2001.1776.

37 Saurabh Sanghvi and Salil P. Vadhan. The round complexity of two-party random selection. *SIAM J. Comput.*, 38(2):523–550, 2008. doi:10.1137/050641715.

38 Luca Trevisan and Salil P. Vadhan. Extracting randomness from samplable distributions. In *41st Annual Symposium on Foundations of Computer Science, FOCS 2000, 12-14 November 2000, Redondo Beach, California, USA*, pages 32–42. IEEE Computer Society, 2000. doi:10.1109/SFCS.2000.892063.

39 Salil P. Vadhan. Pseudorandomness. *Foundations and Trends® in Theoretical Computer Science*, 7(1–3):1–336, 2012. doi:10.1561/0400000010.

40 David Zuckerman. Linear Degree Extractors and the Inapproximability of Max Clique and Chromatic Number. *Theory of Computing*, 3:103–128, August 2007. Number: 6. doi:10.4086/toc.2007.v003a006.