Electronic Colloquium on Computational Complexity, Report No. 70 (2018)

Non-Malleable Extractors and Codes in the Interleaved Split-State Model and More

Eshan Chattopadhyay[*]
Cornell University and IAS
eshanc@ias.edu

Xin Li[†]
Department of Computer Science,
John Hopkins University
lixints@cs.jhu.edu

April 12, 2018

Abstract

We present explicit constructions of non-malleable codes with respect to the following tampering classes. (i) Linear functions composed with split-state adversaries: In this model, the codeword is first tampered by a split-state adversary, and then the whole tampered codeword is further tampered by a linear function. (ii) Interleaved split-state adversary: Here the codeword is partitioned in an unknown (but fixed) way, and then tampered by a split-state adversary. (iii) Bounded communication split-state model: In this model, the split-state adversaries are allowed to participate in a communication protocol (with bounded communication budget) to tamper the codeword. Our results are the first explicit constructions of non-malleable codes in any of these tampering models.

We derive all our non-malleable codes from explicit constructions of seedless non-malleable extractors. We believe that our results on seedless non-malleable extractors and the techniques developed are of independent interest. Using our techniques, we also give an improved extractor for an unknown interleaving of two independent sources.

[*] Partially supported by NSF Grant CCF-1412958 and the Simons Foundation
[†] Partially supported by NSF Grant CCF-1617713.

ISSN 1433-8092

1 Introduction

1.1 Non-malleable Codes

Non-malleable codes were introduced by Dziembowski, Pietrzak and Wichs [DPW10] as a relaxation of error correcting codes, with the motivation of being able to handle more complex tamperings of the codeword. Traditional notions of error correction can only provide meaningful guarantees when the tampered codeword is close in hamming distance to actual codeword, where as in practice the adversarial functions acting on codewords could be of arbitrary complexity. Non-malleable codes bridge this gap, and informally provide the guarantee that either the codeword decodes back to the original message or decodes to a message that is independent of the original message. This captures the intuition that an adversary cannot change the codeword in a way such that the tampered codeword decodes back to a message of her choice.

The original intended use of non-malleable codes is to tamper-resilient cryptography. Subsequently, non-malleable codes have also found uses in non-malleable commitments [GPR16] and other areas of cryptography [CMTV15]. Further, interesting connections were found to non-malleable extractors [CG14]. Various components developed in constructing non-malleable codes make use of sophisticated ideas from combinatorics [ADL14, CZ14], and some of these components have found applications in constructing extractors for independent sources [Li17]. This makes it particularly interesting to study non-malleable codes on its own right, and possibly find more connections to other well studied objects.

We need to introduce some notions before formally defining non-malleable codes.

Definition 1.1. *For any function $f : S \to S$, f has a fixed point at $s \in S$ if $f(s) = s$. We say f has no fixed points in $T \subseteq S$, if $f(t) \neq t$ for all $t \in T$. f has no fixed points if $f(s) \neq s$ for all $s \in S$.*

Definition 1.2 (Tampering functions)**.** *For any $n > 0$, let $\mathcal{F}_n$ denote the set of all functions $f : \{0,1\}^n \to \{0,1\}^n$. Any subset of $\mathcal{F}_n$ is a family of tampering functions.*

We use statistical distance to measure distance between distributions.

Definition 1.3. *The statistical distance between two distributions $\mathcal{D}_1$ and $\mathcal{D}_2$ over some universal set Ω is defined as $|\mathcal{D}_1 - \mathcal{D}_2| = \frac{1}{2}\sum_{d\in\Omega} |\mathbf{Pr}[\mathcal{D}_1 = d] - \mathbf{Pr}[\mathcal{D}_2 = d]|$. We say $\mathcal{D}_1$ is ϵ-close to $\mathcal{D}_2$ if $|\mathcal{D}_1 - \mathcal{D}_2| \leq \epsilon$ and denote it by $\mathcal{D}_1 \approx_\epsilon \mathcal{D}_2$.*

We are now almost ready to formally define non-malleable codes. We need to define the following function.

$$\text{copy}(x, y) = \begin{cases} x & \text{if } x \neq \mathit{same}^\star \\ y & \text{if } x = \mathit{same}^\star \end{cases}$$

We follow the treatment in [DPW10] and first define coding schemes before introducing non-malleable codes.

Definition 1.4 (Coding schemes)**.** *Let* $\text{Enc} : \{0,1\}^k \to \{0,1\}^n$ *and* $\text{Dec} : \{0,1\}^n \to \{0,1\}^k \cup \{\perp\}$ *be functions such that* Enc *is a randomized function (i.e., it has access to private randomness) and* Dec *is a deterministic function. We say that* (Enc, Dec) *is a coding scheme with block length n and message length k if for all $s \in \{0,1\}^k$,* $\Pr[\text{Dec}(Enc(s)) = s] = 1$*, where the probability is taken over the randomness in* Enc.

Definition 1.5 (Non-malleable codes). *A coding scheme $\mathcal{C} = (\mathrm{Enc}, \mathrm{Dec})$ with block length n and message length k is a non-malleable code with respect to a family of tampering functions $\mathcal{F} \subset \mathcal{F}_n$ and error ϵ if for every $f \in \mathcal{F}$ there exists a random variable D_f on $\{0,1\}^k \cup \{same^\star\}$ which is independent of the randomness in* Enc *such that for all messages $s \in \{0,1\}^k$, it holds that*

$$|\mathrm{Dec}(f(\mathrm{Enc}(s))) - \mathrm{copy}(D_f, s)| \leq \epsilon.$$

The rate of $\mathcal{C}$ is given by k/n.

We define some tampering function families that we are concerned with in this paper. We use the notation that for any permutation $\pi : [n] \to [n]$ and any string $x \in [r]^n$, let $y = x_\pi$ denote the length n string such that $y_{\pi(i)} = x_i$.

- The family of 2-split-state functions $2\mathrm{SS} \subset \mathcal{F}_{2n}$: Any $f \in 2\mathrm{SS}$ comprises of two functions $f_1 : \{0,1\}^n \to \{0,1\}$ and $f_2 : \{0,1\}^n \to \{0,1\}$, and for any $x, y \in \{0,1\}^n$, $f(x,y) = f_1(x) \circ f_2(x)$.
- The family of linear functions $\mathrm{Lin} \subset \mathcal{F}_n$: Any $f \in \mathrm{Lin}$ is a linear function from $\{0,1\}^n$ to $\{0,1\}^n$.
- The family of interleaved 2-split-state $2\mathrm{ISS} \subset \mathcal{F}_{2n}$: Any $f \in 2\mathrm{SS}$ comprises of two functions $f_1 : \{0,1\}^n \to \{0,1\}$ and $f_2 : \{0,1\}^n \to \{0,1\}$, and a permutation $\pi : [2n] \to [2n]$ such that for any $z = x \circ y$, where $x, y \in \{0,1\}^n$, let x' be the first n bits of z_π and y' be the last n bits of z_π. Then, $f(z) = f_1(x') \circ f_2(y')$. This model extends the split-state model and captures the model of split-state tampering where the codeword is partitioned into two halves in an unknown way (and then tampered using a 2-split-state adversary). Constructing non-malleable codes with respect to such adversaries was raised by Cheraghchi and Guruswami [CG14].
- The family of bounded communication 2-split-state functions $(2,t,\ell) - \mathrm{CSS}$: Consider the following natural extension of the 2-split-state model where the two tampering functions are allowed to participate in a communication protocol. Let $c = (x,y)$ be a codeword in $\{0,1\}^{2n}$, where x is the first n bits of C and y is the remaining n bits of c. Let Alice and Bob be two tampering agents who can communicate, with Alice having access to x and Bob having access y. Alice and Bob run a communication protocol with parameters t, ℓ runs for ℓ rounds, with each round comprising Alice sending Bob t bits (that depend on x and the transcript of the communication so far) and Bob sends back t bits (that depend on y and the transcript of the communication so far) to Alice. Finally, Alice outputs $x' \in \{0,1\}^n$ and Bob outputs $y' \in \{0,1\}^n$, and the tampered codeword is $c' = (x', y')$.
- For any tampering function families $\mathcal{F}, \mathcal{G} \subset \mathcal{F}_n$, define the composed family $\mathcal{F} \circ \mathcal{G} \subset \mathcal{F}_n$ to be the set of all functions of the form $f \circ g$, where $f \in \mathcal{F}$ and $g \in \mathcal{G}$.

The following are our main results on non-malleable codes.

Theorem 1. *There exists a constant $\delta > 0$ such that for all integers $n > 0$ there exists an efficient non-malleable code with respect to* 2ISS *with rate $1/n^\delta$ and error 2^{-n^δ}.*

Theorem 2. *There exists a constant $\delta > 0$ such that for all integers $n > 0$ there exists an efficient non-malleable code with respect to* $\mathrm{Lin} \circ 2\mathrm{SS}$ *with rate $1/n^\delta$ and error 2^{-n^δ}.*

Theorem 3. *There exists a constant $\delta > 0$ such that for all integers $n, t, \ell > 0$ with $t \cdot \ell \leq \delta n$, there exists an efficient non-malleable code with respect to* $(2,t,\ell) - \mathrm{CSS}$ *with rate* $\log\log n/\log n$ *and error $2^{-n \log\log n/\log n}$.*

Prior to our work, no such efficient non-malleable code construction was known (for any rate) with respect to the tampering classes $2\mathrm{SS}, 2\mathrm{ISS}$ or $(2,t,\ell) - \mathrm{CSS}$.

Relevant prior work on non-malleable codes There has been a lot of exciting progress on explicit constructions of non-malleable codes, and we do not attempt to provide a comprehensive survey of them. In particular, we focus on relevant explicit constructions in the information theoretic model. By a very successful line of work [DKO13,ADL14,CG14,CZ14,ADKO15,CGL16,Li17,Li18], we now have explicit constructions of non-malleable codes with respect to 2-split-state adversaries with rate $\Omega(\log\log n/\log n)$. A recent work of Kanukurthi, Obbattu, and Sruthi [KOS17] gave explicit constructions of non-malleable codes in the 4-split-state model that almost achieve optimal rates. The number of states required in this construction was improved to 3 by Gupta, Maji and Wang [GMW17].

Recently, there has been more progress towards handling tampering functions that have more global access to the bits of the codeword. A work of Agrawal, Gupta, Maji, Pandey and Prabhakaran [AGM$^+$15] gave explicit constructions of non-malleable codes with respect to tampering functions that permute or flip bits. Ball, Dachman-Soled, Kulkarni and Tal Malkin [BDKM16] gave explicit construction of non-malleable codes against t-local functions for $t \leq n^{1-\epsilon}$. A recent work of Chattopadhyay and Li [CL17] gave explicit constructions of non-malleable codes with respect to linear functions and small depth circuits. The rate of the non-malleable code was exponentially improved by a recent work of Ball, Dachman-Soled, Guo, Malkin, and Tan [BDG$^+$18]. Our explicit non-malleable code for Lin $\circ$ 2SS is another step towards handling more global tampering of the codeword.

1.2 Seedless non-malleable extractors

Our results on non-malleable codes are based on new constructions of seedless non-malleable extractors. We believe these constructions should be of independent interest. We begin by recalling basics notions from the area of randomness extraction before introducing seedless non-malleable extractors.

The area of randomness extraction is motivated by the problem of purifying imperfect (or defective) sources of randomness. The concern stems from the fact that naturally occurring sources of randomness often produce low quality bits of randomness, while for most applications, one requires bits that are uniform and independent bits. The standard way of measuring the randomness of a source is using min-entropy.

Definition 1.6. *The min-entropy of a source* $\mathbf{X}$ *is defined to be:* $H_\infty(\mathbf{X}) = \min_x(-\log(\Pr[\mathbf{X} = x]))$*. The min-entropy rate of a source* $\mathbf{X}$ *on* $\{0,1\}^n$ *is* $H_\infty(\mathbf{X})/n$*. Any source* $\mathbf{X}$ *on* $\{0,1\}^n$ *with min-entropy at least* k *is called an* (n,k)*-source.*

It turns out that it is impossible to extract from a single random source. To bypass this difficulty, a particularly useful and well studied notion is that of a seeded extractor that takes in some additional amount of randomness to extract from the weak source.

Definition 1.7. *A function* $\mathrm{Ext} : \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^m$ *is a* (k,ϵ)*-seeded extractor if for any source* $\mathbf{X}$ *of min-entropy* k*,* $|\mathrm{Ext}(\mathbf{X},\mathbf{U}_d) - \mathbf{U}_m| \leq \epsilon$*.* Ext *is called a strong seeded extractor if* $|(\mathrm{Ext}(\mathbf{X},\mathbf{U}_d),\mathbf{U}_d) - (\mathbf{U}_m,\mathbf{U}_d)| \leq \epsilon$*, where* $\mathbf{U}_m$ *and* $\mathbf{U}_d$ *are independent.*

Further, if for each $s \in \mathbf{U}_d$*,* $\mathrm{Ext}(\cdot,s) : \{0,1\}^n \to \{0,1\}^m$ *is a linear function, then* Ext *is called a linear seeded extractor.*

A significantly stronger notion is that of a seeded non-malleable extractor introduced by Dodis and Wichs [DW09] in the context of achieving privacy amplification in the presence of an active adversary. Informally, such an extractor satisfies a stronger property that for most pairs of seeds, the output of the extractor are pair-wise independent and uniform. A seedless variant of non-malleable extractors were introduced by Cheraghchi and Guruswami [CG14] as a way of efficiently constructing non-malleable codes. Apart from applications to non-malleable codes, such extractors are of independent interest and have applications to constructions of extractors for independent sources [Li17].

We now define seedless non-malleable extractors. For simplicity, the definition presented here assumes that the tampering functions has no fixed points. See Section 3 for a more formal definition.

Definition 1.8 (Seedless non-malleable extractors)**.** *Let $\mathcal{F} \subset \mathcal{F}_n$ be a family of tampering functions such that no function in $\mathcal{F}$ has any fixed points. A function* $\mathrm{nmExt} : \{0,1\}^n \to \{0,1\}^m$ *is a seedless non-malleable extractor with respect to $\mathcal{F}$ and a class of sources $\mathcal{X}$ with error ϵ if for every distribution $\mathbf{X} \in \mathcal{X}$ and every tampering function $f \in \mathcal{F}$,*

$$|\mathrm{nmExt}(\mathbf{X}), \mathrm{nmExt}(f(\mathbf{X})) - \mathbf{U}_m, \mathrm{nmExt}(f(\mathbf{X}))| \leq \epsilon.$$

Further, we say that nmExt *is ϵ'-invertible, if there exists an efficient sampling algorithm $\mathcal{A}$ that takes as input $y \in \{0,1\}^m$, and outputs a sample from a distribution that is ϵ'-close to the uniform distribution on the set* $\mathrm{nmExt}^{-1}(y)$*.*

The following theorem was proved by Cheraghchi and Guruswami [CG14].

Theorem 1.9 ([CG14])**.** *Let* $\mathrm{nmExt} : \{0,1\}^n \to \{0,1\}^m$ *be an efficient seedless non-malleable extractor that works for min-entropy n with error ϵ with respect to a class of tampering functions $\mathcal{F}$ acting on $\{0,1\}^n$. Further suppose* nmExt *is ϵ'-invertible.*

Then there exists an efficient construction of a non-malleable code with respect to the tampering family $\mathcal{F}$ with block length $= n$, relative rate $\frac{m}{n}$ and error $2^m\epsilon + \epsilon'$.

The following are our main results on explicit constructions of seedless non-malleable extractors.

Theorem 4. *For all $n > 0$ there exists an efficiently computable seedless $(n, n^{\Omega(1)}, 2^{-n^{\Omega(1)}})$-non-malleable extractor with respect to that* 2ISS *is $2^{-n^{\Omega(1)}}$-invertible.*

Theorem 5. *For all $n > 0$ there exists an efficiently computable seedless $(n, n^{\Omega(1)}, 2^{-n^{\Omega(1)}})$-non-malleable extractor with respect to* $\mathrm{Lin} \circ \mathrm{SS}$ *that is $2^{-n^{\Omega(1)}}$-invertible.*

Theorem 6. *There exists $\delta > 0$ such for all integers $n, t, \ell > 0$ with $t \cdot \ell \leq \delta n$, there exists an efficiently computable seedless $(n, \log\log n / \log n, 2^{-n^{\Omega(1)}})$-non-malleable extractor with respect to $(2, t, \ell) - \mathrm{CSS}$ that is $2^{-n \log\log n / \log n}$-invertible.*

We give the first explicit construction of seedless non-malleable extractors with respect to the tampering classes $2\mathrm{ISS}, \mathrm{Lin} \circ 2\mathrm{SS}$ and $(2, t, \ell) - \mathrm{CSS}$. The non-malleable extractors with respect to $2\mathrm{ISS}, \mathrm{Lin} \circ 2\mathrm{SS}$ are fundamentally new constructions. The non-malleable extractor with respect to the tampering family $(2, t, \ell) - \mathrm{CSS}$ is obtained by showing a reduction to seedless non-malleable extractors for 2SS, where excellent constructions are known (e.g., a recent construction of Li [Li18]).

Relevant prior work on seedless non-malleable extractors The problem of constructing seedless non-malleable extractors was raised by Guruswami and Cheraghchi [CG14] as a way to construct non-malleable codes. The first such construction was given by Chattopadhyay and Zuckerman [CZ14] with respect to the class of 10-split-state adversaries. Subsequently, a series of works starting with the work of Chattopadhyay, Goyal and Li [CGL16] gave explicit seedless non-malleable extractors for 2-split-state adversaries. The only other known construction of seedless non-malleable extractors (with respect to a different tampering class) is from a work of Chattopadhyay and Li [CL17]. They constructed explicit seedless non-malleable extractors with respect to Lin and with respect to small depth circuits. We note that constructing seedless non-malleable extractors with respect to 2ISS was posed as an open problem in [CG14].

1.3 Extractors for interleaved sources

Our techniques yield improved explicit constructions of extractors for interleaved sources. Interleaved sources generalize the problem of extracting from independent sources in the following way: we assume that the extractor gets a sample that is an unknown (but fixed) interleaving of samples from a few independent sources. Raz and Yehudayoff [RY11] showed that constructing explicit extractors for such interleaved sources have applications in communication complexity and proving lower bounds for arithmetic circuits. In subsequent work, Chattopadhyay and Zuckerman [CZ16b] showed that extractors for interleaved sources can be used to construct extractors for certain samplable sources, extending a line of work initiated by Trevisan and Vadhan [TV00]. We now define interleaved sources formally.

Definition 1.10 (Interleaved Sources)**.** *Let $\mathbf{X}_1, \ldots, \mathbf{X}_r$ be arbitrary independent sources on $\{0,1\}^n$ and let $\pi : [rn] \to [rn]$ be any permutation. Then $Z = (\mathbf{X}_1 \circ \ldots \circ \mathbf{X}_r)_t$ is an r-interleaved source.*

Our main result is an explicit extractor that works for 2-interleaved sources with both sources having min-entropy at least $2n/3$. The extractor outputs $\Omega(n)$ bits that are $2^{-n^{\Omega(1)}}$-close to uniform. More formally, we have the following result.

Theorem 7. *For any constant $\delta > 0$ and all integers $n > 0$, there exists an efficiently computable function $\mathrm{i}\ell\mathrm{Ext} : \{0,1\}^{2n} \to \{0,1\}^m$, $m = \Omega(n)$, such that for any two independent sources $\mathbf{X}$ and $\mathbf{Y}$, each on n bits with min-entropy at least $(2/3+\delta)n$, and any permutation $\pi : [2n] \to [2n]$, we have*

$$|\mathrm{i}\ell\mathrm{Ext}((\mathbf{X} \circ \mathbf{Y})_\pi) - \mathbf{U}_m| \leq 2^{-n^{\Omega(1)}}.$$

Relevant prior work on interleaved extractors Raz and Yehudayoff [RY11] gave explicit extractors for 2-interleaved sources that works when both the sources have min-entropy at least $(1-\delta)n$, for a tiny δ that results out of sum-product estimates in additive combinatorics. They can output $\Omega(n)$ bits with exponentially small error. Subsequently, Chattopadhyay and Zuckerman constructed extractors for 2-interleaved sources when one of source has entropy $(1-\gamma)n$ for a small constant γ and the other source has entropy $\Omega(\log n)$. They achieve output length of $O(\log n)$ bits with error $1/n^{O(1)}$.

There is a much better result known (in terms of the min-entropy one can handle) when one has access to an interleaving of more sources. For a large enough constant C, Chattopadhyay and Li [CL16] gave an explicit extractor for C-interleaved sources with each source having entropy $k \geq \mathrm{poly}(\log n)$. They achieve error $1/n^{O(1)}$ and can output $k^{\Omega(1)}$ bits.

1.4 Open questions

Non-malleable codes for composition of function classes We gave efficient constructions of non-malleable codes for the tampering class Lin $\circ$ 2SS. Many natural questions remain to be answered. For instance, one open problem is to efficiently construct non-malleable codes for the tampering class $2\mathrm{SS} \circ \mathrm{Lin}$. It looks like one needs substantially new ideas to give such constructions. More generally, for what other interesting classes of functins $\mathcal{F}$ and $\mathcal{G}$ can we construct non-malleable codes for the composed class $\mathcal{F} \circ \mathcal{G}$? Is it possible to efficiently construct non-malleable codes for the tampering class $\mathcal{F} \circ \mathcal{G}$ if we have efficient non-malleable codes for the classes $\mathcal{F}$ and $\mathcal{G}$?

Other applications for seedless non-malleable extractors The explicit seedless non-malleable extractors that we construct satisfy strong pseudorandom properties and appear to be objects with strong combinatorial properties. A natural question is to find more applications of these non-malleable extractors in explicit constructions of other interesting combinatorial objects.

Improved seedless extractors We construct an extractor for 2-interleaved sources that works for min-entropy rate $2/3$. It is easy to verify that there exists extractors for sources with min-entropy as low as $C \log n$, and a natural question here is to come up with such explicit constructions. Given the success in constructing 2-source extractors for low min-entropy [CZ16a, Li18], we are hopeful that more progress can be made on this problem.

1.5 Organization

We present an overview of our constructions and techniques in Section 2. We use Section 3 to introduce some background and notation. We present a new advice correlation breaker in Section 4. We present the construction of a seedless non-malleable extractor with respect to 2ISS in Section 5. We present our seedless non-malleable extractor construction with respect to $\mathrm{Lin} \circ 2\mathrm{SS}$ in Section 6. The new advice correlation breaker from Section 4 is a crucial ingredient in this construction. We use Section 7 to present our non-malleable extractor construction with respect to $(2, t, \ell) - \mathrm{CSS}$. We present efficient sampling algorithms for our seedless non-malleable extractor constructions in Section 8. We use Section 9 to present an explicit construction of an extractor for interleaved sources.

2 Overview of Constructions and techniques

Our results on non-malleable codes are derived from explicit constructions of invertible seedless non-malleable extractors (see Theorem 3.16). Thus we focus on the explicit constructions of seedless non-malleable extractors with respect to the relevant classes. We conclude by discussing the explicit extractor for interleaved sources.

Seedless non-malleable extractors with respect to 2ISS The setup is as follows. We want to construct a non-malleable extractor $\mathrm{nmExt} : \{0,1\}^{2n} \to \{0,1\}^m$, $m = n^{\Omega(1)}$ such that the following hold: Let $\mathbf{X}$ and $\mathbf{Y}$ be independent (n,k)-sources with $k \geq n - n^{\delta}$ for a small constant $\delta > 0$. Let $f : \{0,1\}^n \to \{0,1\}^n$ and $g : \{0,1\}^n \to \{0,1\}^n$ be two arbitrary functions and let $\pi : [2n] \to [2n]$ be an arbitrary partition. Further, assume that f has no fixed points[1], i.e., $\forall x \in \{0,1\}^n$, $f(x) \neq x$. Then,

$$\mathrm{nmExt}((\mathbf{X}, \mathbf{Y})_{\pi}), \mathrm{nmExt}((f(\mathbf{X}) \circ g(\mathbf{Y}))_{\pi}) \approx_{\epsilon} \mathbf{U}_m, \mathrm{nmExt}((f(\mathbf{X}) \circ g(\mathbf{Y}))_{\pi}),$$

[1] We can assume this without loss of generality. See Section 5 for the more details.

where $\epsilon = 2^{-n^{\Omega(1)}}$.

The high level idea is to use framework introduced by Chattopadhyay, Goyal and Li [CGL16] for constructing non-malleable extractors. This involves two two steps: (a) explicit construction of an advice generator, and (b) explicit construction of an advice correlation breaker. We now explain these steps in more details tailored to our setting.

For simplicity, we use introduce some notation. Let $\mathbf{Z} = (\mathbf{X} \circ \mathbf{Y})_\pi$. We use $\mathbf{Z}'$ to denote the random variable $(f(\mathbf{X}) \circ g(\mathbf{Y}))_\pi$. Further, for any function ν, if $\mathbf{Q} = \nu(\mathbf{Z})$, then we use $\mathbf{Q}'$ to denote $\nu(\mathbf{Z}')$. We use the notation $\text{Slice}(x, \ell)$ to denote a slice (or prefix) of size ℓ taken from a string x,

The advice generator $\text{advGen} : \{0,1\}^{2n} \to \{0,1\}^a$ satisfies the guarantee that $\text{advGen}(\mathbf{Z}) \neq \text{advGen}(\mathbf{Z}')$ with high probability. Further, we require a to be small (n^γ, for small γ). We construct advGen in the following way. Take a large enough slice $\mathbf{Z}_1$ (say of length $n^{2\delta}$) from the source $\mathbf{Z}$. Let $\mathbf{Z}_2$ be the remaining part of Z after slicing off Z_1. Recalling that we can sample using weak sources (by a result of Zuckerman [Zuc97]), we now encode $\mathbf{Z}$ using a good linear error correcting code and sample n^γ coordinates from $\mathbf{Z}_2$ using a sampler (that takes $\mathbf{Z}_1$ as input). The output of the advice generator is $\mathbf{Z}_1$ concatenated with the sampled bits from encoding of $\mathbf{Z}_2$.

The proof that this indeed works is as follows. We start out by observing that the interesting case is when $\mathbf{Z}_1 \mathbf{Z}_1'$. Indeed, the proof is trivial otherwise. Assume without loss of generality that there are more bits of $\mathbf{X}$ in this slice $\mathbf{Z}_1$ than bits from $\mathbf{Y}$. We fix the bits from $\mathbf{Y}$ in $\mathbf{Z}_1$ and it is now a deterministic function of $\mathbf{X}$. We also fix the bits of $\mathbf{X}$ in $\mathbf{Z}$ that are not in $\mathbf{Z}_1$. We claim that $\mathbf{Z}_1$ has min-entropy at least $n^{2\delta}/2 - n^\delta$. This is direct from the fact that $\mathbf{X}$ has min-entropy at least $n - n^\delta$ and $\mathbf{Z}_1$ contains at least $n^{2\delta}/2$ bits from $\mathbf{X}$. We now fix $\mathbf{Y}$. This fixes the random variable $\mathbf{Z}_2$. Now since f has no fixed points and $\mathbf{Z}_1 = \mathbf{Z}_1'$, it must be the case that $\mathbf{Z}_2 \neq \mathbf{Z}_2'$. Hence, once we encode it using a good error correcting code, the encoded strings differ on $\Omega(1)$ fraction of the coordinates. Thus, with probability $1 - 2^{-n^{\Omega(1)}}$, at least one of the sampled bits from the encodings must differ. This completes the proof of correctness of the advice generator.

Next, we move on to the construction of the advice correlation breaker. This is a relaxed notion of non-malleable extractors where we also supply it with an additional advice[2]. More formally, we construct a function $\text{ACB} : \{0,1\}^{2n} \times \{0,1\}^a \to \{0,1\}^m$ such that

$$\text{ACB}(\mathbf{Z}, w), \text{ACB}(\mathbf{Z}', w') \approx_\epsilon \mathbf{U}_m, \text{ACB}(\mathbf{Z}', w'),$$

for any fixed strings $w, w' \in \{0,1\}^a$ and $w \neq w'$.

We sketch some high level ideas for in the construction of ACB and refer the reader to Section 5 for more details. The idea is to construct a use an advice correlation breaker from a previous work of Chattopadhyay and Li [CL16]. Informally, they show the following: Suppose $\mathbf{X}$ is a weak source that is independent of random variables $\mathbf{Y}^1, \mathbf{Y}^2, \ldots, \mathbf{Y}^r$ and $\mathbf{Z}$. Suppose $\mathbf{Y}^1$ is uniform. Further, let $id^1, \ldots, id^r$ be fixed advice strings such that id^1 is distinct from id^j, $j \in [2, r]$. For appropriate parameters, they construct a function ACB_1 such that

$$\begin{aligned}\text{ACB}_1(\mathbf{X}+\mathbf{Z}, \mathbf{Y}^1, id^1), \text{ACB}_1(\mathbf{X}+\mathbf{Z}, \mathbf{Y}^2, id^2), \ldots, \text{ACB}(\mathbf{X}+\mathbf{Z}, \mathbf{Y}^r, id^r) \approx \\ \mathbf{U}_m, \text{ACB}_1(\mathbf{X}+\mathbf{Z}, \mathbf{Y}^2, id^2), \ldots, \text{ACB}_1(\mathbf{X}+\mathbf{Z}, \mathbf{Y}^r, id^r).\end{aligned}$$

A very informal sketch of our construction is as follows. We first take a slice of $\mathbf{Z}$ and convert it into a somewhere random source of appropriate dimensions (with longer rows than columns) using linear seeded extractors. The idea then is to use ACB_1 with the original source $\mathbf{Z}$ and each row

[2] see Section 4 for more details on advice correlation breakers

of the somewhere random source (assuming, magically that we have access to advice strings). The final output would then be a bit-wise XOR of the outputs of the advice correlation breaker (used on each row of the matrix).

We show that this can indeed be made to work. Further, the advice for each row can be generated by using the advice generator sketched above (with the row number concatenated to it). This completes the sketch of the seedless non-malleable extractor for interleaved sources.

Note that it is far from obvious how to efficiently sample from the pre-image of this non-malleable extractor. This is an important problem, since the encoder of the corresponding non-malleable code is exactly this sampler. We use Section 8 to suitably modify our extractors to support efficient sampling. We briefly sketch some high level ideas involved in efficiently sampling from the pre-image of this extractor. A crucial observation is the fact that we can use smaller disjoint slices of $\mathbf{Z}$ to carry out the various steps outlined in the construction. In particular, for the steps where we use the entire source $\mathbf{Z}$ (in getting a somewhere random source of the right dimensions and the advice correlation breaker step) it can be carried out with a large enough slice from $\mathbf{Z}$. Note that this is problematic deterministically (since then we would need a slice of length more than n to ensure we have bits from both $\mathbf{X}$ and $\mathbf{Y}$). We get around this by pseudorandomly sampling a enough coordinates from $\mathbf{Z}$ (by first taking small slice of $\mathbf{Z}$ and using a sampler that works for weak sources). We now use an elegant trick introduced by Li [Li17] where the output of the non-malleable extractor described above (with the modifications that we have specified) is now used as a seed to a linear seeded extractor applied on an even larger pseudorandom slice of $\mathbf{Z}$. The linear seeded extractor that we use has the property that for any fixing of the seed, the rank of the linear map corresponding to the linear seeded extractor is the same. Further, note that one can efficiently algorithm to sample from this subspace. The final idea is to use a Reed-Solomon code to encode the source $\mathbf{Z}$ in the construction of the advice generator. This allows us to argue that the rank of the linear restriction imposed on the free variables of $\mathbf{Z}$ does not depend on the value of the bits fixed so far.

Seedless non-malleable extractors with respect to $\mathrm{Lin} \circ 2\mathrm{SS}$ We construct a seedless non-malleable extractor $\mathrm{nmExt} : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^m$, $m = n^{\Omega(1)}$ such that the following hold: Let $\mathbf{X}$ and $\mathbf{Y}$ be independent uniform sources, each on n bits. Let $L : \{0,1\}^{2n} \to \{0,1\}^{2n}$ be a linear function and let $f : \{0,1\}^n \to \{0,1\}^n$, $g : \{0,1\}^n \to \{0,1\}^n$ be two arbitrary functions. Then,

$$\mathrm{nmExt}(\mathbf{X},\mathbf{Y}), \mathrm{nmExt}(L(f(\mathbf{X}),g(\mathbf{Y}))) \approx_\epsilon \mathbf{U}_m, \mathrm{nmExt}(L(f(\mathbf{X}),g(\mathbf{Y}))),$$

where $\epsilon = 2^{-n^{\Omega(1)}}$. Notice that such an extractor is not possible to construct in general, and we need some guarantees on the fixed point of the composition of functions L and (f,g). For simplicity, we mostly ignore these issues now. We mention a reduction below which takes care ofthis problem and we refer the reader to Section 6 for more details.

Our first step is to reduce the problem to constructing non-malleable extractors with the following guarantee. Let $\mathbf{X}$ and $\mathbf{Y}$ to be independent $(n, n-n^{\delta})$-sources and f_1, f_2, g_1, g_2 to satisfy the following condition:

- $\forall x \in \mathit{support}(\mathbf{X})$ and $y \in \mathit{support}(\mathbf{Y})$, $f_1(x) + g_1(y) \neq x$ or
- $\forall x \in \mathit{support}(\mathbf{X})$ and $y \in \mathit{support}(\mathbf{Y})$, $f_2(x) + g_2(y) \neq y$.

Then,

$$|\mathrm{nmExt}(\mathbf{X},\mathbf{Y}),\mathrm{nmExt}(f_1(\mathbf{X})+g_1(\mathbf{Y}),f_2(\mathbf{X})+g_2(\mathbf{Y}))-\\ \mathbf{U}_m,\mathrm{nmExt}(f_1(\mathbf{X})+g_1(\mathbf{Y}),f_2(\mathbf{X})+g_2(\mathbf{Y}))|\leq 2^{-n^{\Omega(1)}}.$$

The reduction can be seen in the following way: Define $\overline{f(x)} = L(f(x), 0^n)$ and $\overline{g(y)} = L(0^n, y)$. Thus, $L(f(x), g(y)) = \overline{f(x)} + \overline{g(y)}$. Define functions $L_1 : \{0,1\}^{2n} \to \{0,1\}^n$ and $L_2 : \{0,1\}^{2n} \to \{0,1\}^n$ such that $L(f(x), g(y)) = L_1(x, y), L_2(x, y)$. Since $L(f(x), g(y)) = \overline{f(x)} + \overline{g(y)}$, it follows that there exists functions $f_1, g_1, f_2, g_2 \in \mathcal{F}_n$ such that for all $x, y \in \{0,1\}^n$, the following hold:

- $L_1(x, y) = f_1(x) + g_1(y)$, and
- $L_2(x, y) = f_2(x) + g_2(y)$.

Thus, $L(f(x), g(y)) = f_1(x)+g_1(y), f_2(x)+g_2(y)$. The loss of entropy in $\mathbf{X}$ and $\mathbf{Y}$ in the reduction (from uniform to $n - n^\delta$) is because of the fact that we have handle issues related to fixed points of the tampering functions and we ignore it for the proof sketch here.

The idea now is to use the framework of advice generators and advice correlation breakers as before to construct the non-malleable extractor. It turns out that we have to work harder than before for constructing both the components.

We start out with the construction of the advice generator. We discuss the proof while describing the construction to provide more intuition for the steps involved in the construction. Without loss of generality, suppose that $\forall x \in \mathit{support}(\mathbf{X})$ and $y \in \mathit{support}(\mathbf{Y})$, $f_1(x) + g_1(y) \neq x$. Let $n_0 = n^\delta$. We take two slices from $\mathbf{X}$, say $\mathbf{X}_1$ and $\mathbf{X}_2$ of lengths $n_1 = 50n_0$ and $n_2 = 5n_0$. Similarly, we take slices from $\mathbf{Y}_1$ and $\mathbf{Y}_2$. Now using a good two-source extractor for high min-entropy (say, the inner product function IP on an appropriate field), compute $\mathbf{R}_1 = \mathrm{IP}(\mathbf{X}_1, \mathbf{Y}_1)$ and $\mathbf{R}_2 = \mathrm{IP}(\mathbf{X}_2, \mathbf{Y}_2)$. Next, use a good linear error correcting code to encode X and sample n^γ coordinates (let $\mathbf{T}$ denote this set) from this encoding using $\mathbf{R}_1$. Here $\gamma > 0$ is an appropriately chosen small constant. Let the sampled bits be the random variable $\mathbf{W}_{1,x}$. Similarly sample coordinates $\mathbf{W}_{1,y}$ from an encoding of $\mathbf{Y}$ using $\mathbf{R}_1$. Finally, let $\mathbf{W}_{2,x}$ be the output of a linear seeded extractor (with output length n^γ) on $\mathbf{X}$ with $\mathbf{R}_2$ as the seed and $\mathbf{W}_{2,y}$ be the output of the linear seeded extractor on $\mathbf{Y}$ with $\mathbf{R}_2$ as the seed. The output of the advice generator is $\mathbf{X}_1 \circ \mathbf{X}_2 \circ \mathbf{Y}_1 \circ \mathbf{Y}_2 \circ \mathbf{W}_{1,x} \circ \mathbf{W}_{2,x} \circ \mathbf{W}_{1,y} \circ \mathbf{W}_{2,y}$.

The intuition that this works is as follows. The lemma is direct if either $\mathbf{X}_1 \neq \mathbf{X}_1'$ or $\mathbf{Y}_1 \neq \mathbf{Y}_1'$. Thus, assume $\mathbf{X}_1 = \mathbf{X}_1'$ and $\mathbf{Y}_1 = \mathbf{Y}_1'$. Similarly, the lemma is direct if either $\mathbf{X}_2 \neq \mathbf{X}_2'$ or $\mathbf{Y}_2 \neq \mathbf{Y}_2'$. Thus, assume $\mathbf{X}_2 = \mathbf{X}_2'$ and $\mathbf{Y}_2 = \mathbf{Y}_2'$. It follows that $\mathbf{R}_1 = \mathbf{R}_1'$, $\mathbf{R}_2 = \mathbf{R}_2'$ and hence $\mathbf{T} = \mathbf{T}'$. Since E is a linear code and LExt is a linear seeded extractor, the following hold:

$$\mathbf{W}_{1,x} - \mathbf{W}_{1,x}' = (E(\mathbf{X} - f_1(\mathbf{X}) - g_1(\mathbf{Y})))_{\mathbf{T}},\\ \mathbf{W}_{2,x} - \mathbf{W}_{2,x}' = \mathrm{LExt}(\mathbf{X} - f_1(\mathbf{X}) - g_1(\mathbf{Y}), \mathbf{R}_2).$$

The idea is the following: Either (i) we can fix $g_1(\mathbf{Y})$ and claim that $\mathbf{Y}_1$ still has enough min-entropy or (ii) claim that $g_1(\mathbf{Y})$ has enough min-entropy conditioned on $\mathbf{Y}_2$. Let us first discuss why these this is enough. Suppose we are in the first case. Then, we can fix $\mathbf{X}_1$ and $\mathbf{R}_1$ becomes a deterministic function of $\mathbf{Y}$. Further, it is uniform since IP is a strong two-source extractor. Now, we can fix $\mathbf{X}$ and by the fixed point guarantees(recall $\forall x \in \mathit{support}(\mathbf{X})$ and $y \in \mathit{support}(\mathbf{Y})$, $f_1(x)+g_1(y) \neq x$), it follows that $\mathbf{W}_{1,x} - \mathbf{W}_{1,x}' \neq \vec{0}$. Now supose we are in the second case. We fix $\mathbf{Y}_2$, and it follows that $\mathbf{R}_2$ is uniform and a deterministic function of $\mathbf{X}$. Further, $g_1(\mathbf{Y})$ has enough min-entropy. Thus, $\mathrm{LExt}(g_1(\mathbf{Y}), \mathbf{R}_2)$ is close to uniform and we can fix $\mathbf{R}_2$ and subsequently $\mathbf{X}$.

It follows that $\mathbf{W}_{2,x} - \mathbf{W}'_{2,x}$ is close uniform and hence $\vec{0}$ with probability $1 - 2^{-n^{\Omega(1)}}$ probability, which completes the proof. The fact that always we are either in case (i) or (ii) requires work and relies on a convex combination argument based on the pre-image size of the function g_1.

We now discuss the other component in the construction, which is the advice correlation breaker. We construct a function $\mathrm{ACB} : \{0,1\}^{2n} \times \{0,1\}^a \to \{0,1\}^m$ such that

$$\begin{aligned}\mathrm{ACB}(\mathbf{X}, \mathbf{Y}, w), \mathrm{ACB}(f_1(\mathbf{X}) + g_1(\mathbf{Y}), f_2(\mathbf{X}) + g_2(\mathbf{Y}), w') &\approx_\epsilon \\ \mathbf{U}_m, \mathrm{ACB}(f_1(\mathbf{X}) + g_1(\mathbf{Y}), f_2(\mathbf{X}) + g_2(\mathbf{Y}), w'),&\end{aligned}$$

for any fixed strings $w, w' \in \{0,1\}^a$ and $w \neq w'$. The construction of this relies on the method of alternating extraction and uses the flip-flop primitive introduced by Cohen [Coh16]. In particular, we use it in a way similar to [CL17], and show that the construction works even in this more general setting. We refer the reader to Section 4 for more details.

Finally, the non-malleable extractor is constructed by using the above advice correlation breaker function with the advice being supplied by the advice generator discussed above. As before, it is not at all clear how to efficiently sample from the pre-image of this extractor. We show in Section 8 that using similar ideas as before and a by careful choice of the error correcting code that we use to encode the sources (we use a dual BCH code to ensure a good trade-off between distance and dual distance of the code) in the construction of the advice generator, we can efficiently sample from the pre-image of the extractor.

Non-malleable extractors for $(2, t, \ell)-$CSS We show that any 2-source non-malleable extractor that works for min-entropy $n - 2\delta n$ can be used as non-malleable extractor with respect to $(2, t, \ell) -$ CSS for $t\ell \leq \delta n$. The tampering function $h_{t,\ell}$ that is based on the communication protocol can be phrased in terms of functions in the following way: there exist deterministic functions $f_i : \{0,1\}^n \times \{0,1\}^{(2i-2)t} \to \{0,1\}^t$ and $g_i : \{0,1\}^n \times \{0,1\}^{(2i-1)t} \to \{0,1\}^t$ for $i = 1, \ldots, \ell$, and $f : \{0,1\}^n \times \{0,1\}^{2\ell t} \to \{0,1\}^n$ and $g : \{0,1\}^n \times \{0,1\}^{2\ell t} \to \{0,1\}^n$ such that the communication protocol between Alice and Bob corresponds to computing the following random variables: $\mathbf{S}_1 = f_1(\mathbf{X}), \mathbf{R}_1 = g_1(\mathbf{Y}, \mathbf{S}_1), \mathbf{S}_2 = f_2(\mathbf{X}, \mathbf{S}_1, \mathbf{R}_1), \ldots, \mathbf{S}_i = f_i(\mathbf{X}, \mathbf{S}_1, \ldots, \mathbf{S}_{i-1}, \mathbf{R}_1, \ldots, \mathbf{R}_{i-1}), \mathbf{R}_i = g_i(\mathbf{Y}, \mathbf{S}_1, \ldots, \mathbf{S}_i, \mathbf{R}_{i,}, \ldots, \mathbf{R}_{i-1}), \ldots, \mathbf{R}_\ell = g_\ell(\mathbf{Y}, \mathbf{S}_1, \ldots, \mathbf{S}_\ell, \mathbf{R}_1, \ldots, \mathbf{R}_{\ell-1})$.

Finally, $\mathbf{X}' = f(\mathbf{X}, \mathbf{R}_1, \ldots, \mathbf{R}_\ell, \mathbf{S}_1, \ldots, \mathbf{S}_\ell)$ and $\mathbf{Y}' = g(\mathbf{Y}, \mathbf{R}_1, \ldots, \mathbf{R}_\ell, \mathbf{S}_1, \ldots, \mathbf{S}_\ell)$ correspond to the output of Alice and the output of Bob respectively. Thus, $h_{t,\ell}(\mathbf{X}, \mathbf{Y}) = (\mathbf{X}', \mathbf{Y}')$.

Similar to the way one argues about alternating extraction protocols, we fix random variables as follows: Fix $\mathbf{S}_1$, and it follows that $\mathbf{R}_1$ is now a deterministic function of $\mathbf{Y}$. We fix $\mathbf{R}_1$, and thus $\mathbf{S}_2$ is now a deterministic function of $\mathbf{X}$. Thus, continuing in this we way, we fix all the random variables $\mathbf{S}_1, \ldots, \mathbf{S}_\ell$ and $\mathbf{R}_1, \ldots, \mathbf{R}_\ell$ while maintaining that $\mathbf{X}$ and $\mathbf{Y}$ remain independent sources. Further, invoking Lemma 3.1, with probability at least $1 - 2^{-\Omega(n)}$, both $\mathbf{X}$ and $\mathbf{Y}$ have min-entropy at least $n - \ell \cdot t - \delta n \geq n - 2\delta n$.

Note that now, $\mathbf{X}' = \eta(\mathbf{X})$ for some deterministic function η and $\mathbf{Y}' = \nu(\mathbf{X})$ for some deterministic function ν. Thus, any invertible 2-source non-malleable extractor for min-entropy $n - 2\delta n$ with error ϵ can be used. Our result follows by using such a construction from a recent work of Li [Li18].

Extractors for interleaved sources We construct an explicit extractor $\mathrm{i}\ell\mathrm{Ext} : \{0,1\}^{2n} \to \{0,1\}^m$, $m = \Omega(n)$ that satisfies the following: Let $\mathbf{X}$ and $\mathbf{Y}$ be independent (n, k)-sources with $k \geq (2/3 + \delta)n$, for any constant $\delta > 0$. Let $\pi : [2n] \to [2n]$ be any permutation. Then,

$$|\mathrm{i}\ell\mathrm{Ext}((\mathbf{X} \circ \mathbf{Y})_\pi) - \mathbf{U}_m| \leq \epsilon.$$

We present our construction and also explain the proof along the way. This gives more intuition to the different steps of the construction. Let $\mathbf{Z} = (\mathbf{X} \circ \mathbf{Y})_\pi$. We start by taking a large enough slice $\mathbf{Z}_1$ from $\mathbf{Z}$ (say, of length $(2/3 + \delta/2)n$). Let $\mathbf{X}$ have more bits in this slice than $\mathbf{Y}$. Let $\mathbf{X}_1$ be the bits of $\mathbf{X}$ in $\mathbf{Z}_1$ and $\mathbf{X}_2$ be the remaining bits of $\mathbf{X}$. Similarly define $\mathbf{Y}_1$ and $\mathbf{Y}_2$. Notice that $\mathbf{X}_1$ has linear entropy and also that it $\mathbf{X}_2$ has linear entropy conditioned on $\mathbf{X}_1$. We fix $\mathbf{Y}_1$ and use a condenser (from the work of Barak et al. [BRSW12] and Zuckerman [Zuc07]) to condense $\mathbf{Z}_1$ into a matrix with a constant number such that at least one of the row has entropy rate at least 0.9. Notice that this matrix is a deterministic function of $\mathbf{X}$. The next step is to $\mathbf{Z}$ and each row of the matrix as a seed to a linear seeded extractor get longer rows. This requires some care for the choice of the linear seeded extractor since the seed has some deficiency in entropy. After this step, we use the advice correlation breaker from [CL16] on Z and each row of the somewhere random source with the row number as the advice (similar to as done before in the construction of seedless non-malleable extractors for 2ISS), and compute the bit-wise XOR of the different outputs that we produce. Let $\mathbf{V}$ denote this random variable. Finally, to output $\Omega(n)$ bits we use a linear seeded extractor on $\mathbf{Z}$ with $\mathbf{V}$ as the seed. The correctness of various steps in the proof exploit the fact that $\mathbf{Z}$ can be written as the bit-wise sum of two independent sources, and the fact that we use linear seeded extractors. We refer the reader to Section 9 for more details.

3 Background and notation

We use $\mathbf{U}_m$ to denote the uniform distribution on $\{0,1\}^m$.
For any integer $t > 0$, $[t]$ denotes the set $\{1, \ldots, t\}$.
For a string y of length n, and any subset $S \subseteq [n]$, we use y_S to denote the projection of y to the coordinates indexed by S.
We use bold capital letters for random variables and samples as the corresponding small letter, e.g., $\mathbf{X}$ is a random variable, with x being a sample of $\mathbf{X}$.
For strings $x, y \in \{0,1\}^n$, we use $x + y$ to denote the bit-wise xor of the two strings.

3.1 A probability lemma

The following result on min-entropy was proved by Maurer and Wolf [MW97].

Lemma 3.1. *Let $\mathbf{X}, \mathbf{Y}$ be random variables such that the random variable $\mathbf{Y}$ takes at ℓ values. Then*

$$\mathbf{Pr}_{y \sim \mathbf{Y}}[H_\infty(\mathbf{X}|\mathbf{Y} = y) \geq H_\infty(\mathbf{X}) - \log \ell - \log(1/\epsilon)] > 1 - \epsilon.$$

3.2 Conditional Min-Entropy

Definition 3.2. *The average conditional min-entropy of a source $\mathbf{X}$ given a random variable $\mathbf{W}$ is defined as*

$$\widetilde{H}_\infty(\mathbf{X}|\mathbf{W}) = -\log\left(\mathbf{E}_{w \sim W}\left[\max_x \Pr[\mathbf{X} = x|\mathbf{W} = w]\right]\right) = -\log\left(\mathbf{E}\left[2^{-H_\infty(\mathbf{X}|\mathbf{W}=w)}\right]\right).$$

We recall some results on conditional min-entropy from the work of Dodis et al. [DORS08].

Lemma 3.3 ([DORS08])**.** *For any $\epsilon > 0$,*

$$\mathbf{Pr}_{w \sim \mathbf{W}}\left[H_\infty(\mathbf{X}|\mathbf{W} = w) \geq \widetilde{H}_\infty(\mathbf{X}|\mathbf{W}) - \log(1/\epsilon)\right] \geq 1 - \epsilon.$$

Lemma 3.4 ([DORS08]). *If a random variable* $\mathbf{Y}$ *has support of size* 2^ℓ*, then* $\widetilde{H}_\infty(\mathbf{X}|\mathbf{Y}) \geq H_\infty(\mathbf{X}) - \ell$*.*

We require extractors that can extract uniform bits when the source only has sufficient conditional min-entropy.

Definition 3.5. *A* (k,ϵ)*-seeded average case seeded extractor* $\mathrm{Ext} : \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^m$ *for min-entropy* k *and error* ϵ *satisfies the following property: For any source* $\mathbf{X}$ *and any arbitrary random variable* $\mathbf{Z}$ *with* $\widetilde{H}_\infty(\mathbf{X}|\mathbf{Z}) \geq k$*,*

$$\mathrm{Ext}(\mathbf{X},\mathbf{U}_d),\mathbf{Z} \approx_\epsilon \mathbf{U}_m,\mathbf{Z}.$$

It was shown in [DORS08] that any seeded extractor is also an average case extractor.

Lemma 3.6 ([DORS08]). *For any* $\delta > 0$*, if* Ext *is a* (k,ϵ)*-seeded extractor, then it is also a* $(k+\log(1/\delta),\epsilon+\delta)$*-seeded average case extractor.*

3.3 Samplers and extractors

Zuckerman [Zuc97] showed that seeded extractors can be used as samplers given access to weak sources. This connection is best presented by a graph theoretic representation of seeded extractors. A seeded extractor $\mathrm{Ext} : \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^m$ can be viewed as an unbalanced bipartite graph G_{Ext} with 2^n left vertices (each of degree 2^d) and 2^m right vertices. Let $\mathcal{N}(x)$ denote the set of neighbors of x in G_{Ext}.

Theorem 3.7 ([Zuc97]). *Let* $\mathrm{Ext} : \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^m$ *be a seeded extractor for min-entropy* k *and error* ϵ*. Let* $D = 2^d$*. Then for any set* $R \subseteq \{0,1\}^m$*,*

$$|\{x \in \{0,1\}^n : ||\mathcal{N}(x) \cap R| - \mu_R D| > \epsilon D\}| < 2^k,$$

where $\mu_R = |R|/2^m$*.*

Theorem 3.8 ([Zuc97]). *Let* $\mathrm{Ext} : \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^m$ *be a seeded extractor for min-entropy* k *and error* ϵ*. Let* $\{0,1\}^d = \{r_1,\ldots,r_D\}$*,* $D = 2^d$*. Define* $\mathrm{Samp}(x) = \{\mathrm{Ext}(x,r_1),\ldots,\mathrm{Ext}(x,r_D)\}$*. Let* $\mathbf{X}$ *be an* $(n,2k)$*-source. Then for any set* $R \subseteq \{0,1\}^m$*,*

$$\mathbf{Pr}_{\mathbf{x}\sim\mathbf{X}}[||\mathrm{Samp}(\mathbf{x}) \cap R| - \mu_R D| > \epsilon D] < 2^{-k},$$

where $\mu_R = |R|/2^m$*.*

3.4 Explicit extractors from prior work

We recall an optimal construction of strong-seeded extractors.

Theorem 3.9 ([GUV09]). *For any constant* $\alpha > 0$*, and all integers* $n,k > 0$ *there exists a polynomial time computable strong-seeded extractor* $\mathrm{Ext} : \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^m$ *with* $d = O(\log n + \log(1/\epsilon))$ *and* $m = (1-\alpha)k$*.*

The following are explicit constructions of linear seeded extractors.

Theorem 3.10 ([Tre01, RRV02]). *For every* $n,k,m \in \mathbb{N}$ *and* $\epsilon > 0$*, with* $m \leq k \leq n$*, there exists an explicit strong linear seeded extractor* $\mathrm{LExt} : \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^m$ *for min-entropy* k *and error* ϵ*, where* $d = O\left(\log^2(n/\epsilon)/\log(k/m)\right)$*.*

A drawback of the above construction is that the seeded length is $\omega(\log n)$ for sub-linear min-entropy. A construction of Li [Li15] achieves $O(\log n)$ seed length for even polylogarithmic min-entropy.

Theorem 3.11 ([Li15]). *There exists a constant $c > 1$ such that for every $n, k \in \mathbb{N}$ with $c \log^8 n \leq k \leq n$ and any $\epsilon \geq 1/n^2$, there exists a polynomial time computable linear seeded extractor* $\mathrm{LExt} : \{0, 1\}^n \times \{0,1\}^d \to \{0,1\}^m$ *for min-entropy k and error ϵ, where $d = O(\log n)$ and $m \leq \sqrt{k}$.*

A different construction achieves seed length $O(\log(n/\epsilon))$ for high entropy sources.

Theorem 3.12 ([CGL16, Li17]). *For all $\delta > 0$ there exist $\alpha, \gamma > 0$ such that for all integers $n > 0$, $\epsilon \geq 2^{-\gamma n}$, there exists an efficiently computable linear strong seeded extractor* $\mathrm{LExt} : \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^{\alpha d}$, *$d = O(\log(n/\epsilon))$ for min-entropy δn. Further, for any $y \in \{0,1\}^d$, the linear map $\mathrm{LExt}(\cdot, y)$ has rank αd.*

The above theorem is stated in [Li17] for $\delta = 0.9$, but it is straightforward to see that the proof extends for any constant $\delta > 0$.

We use a property of linear seeded extractors proved by Rao [Rao09].

Lemma 3.13 ([Rao09]). *Let* $\mathrm{Ext} : \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^m$ *be a linear seeded extractor for min-entropy k with error $\epsilon < \frac{1}{2}$. Let X be an affine (n,k)-source. Then*

$$\Pr_{u \sim U_d}[|\mathrm{Ext}(X, u) - U_m| > 0] \leq 2\epsilon.$$

We recall a two-source extractor construction for high entropy sources based on the inner product function.

Theorem 3.14 ([CG88]). *For all $m, r > 0$, with $q = 2^m, n = rm$, let $\mathbf{X}, \mathbf{Y}$ be independent sources on $\mathbb{F}_q^r$ with min-entropy k_1, k_2 respectively. Let* IP *be the inner product function over the field $\mathbb{F}_q$. Then, we have:*

$$|\mathrm{IP}(\mathbf{X}, \mathbf{Y}), \mathbf{X} - \mathbf{U}_m, \mathbf{X}| \leq \epsilon, \quad |\mathrm{IP}(\mathbf{X}, \mathbf{Y}), \mathbf{Y} - \mathbf{U}_m, \mathbf{Y}| \leq \epsilon$$

where $\epsilon = 2^{-(k_1+k_2-n-m)/2}$.

3.5 Non-malleable codes via seedless non-malleable extractors

We first recall the definition of a general seedless non-malleable extractor with respect to a class of tampering functions.

Definition 3.15 (Seedless Non-Malleable Extractor). *A function* $\mathrm{nmExt} : \{0,1\}^n \to \{0,1\}^m$ *is a (k, ε)-seedless non-malleable extractor with respect to a class $\mathcal{X}$ of sources over $\{0,1\}^n$ and a class $\mathcal{F}$ of tampering functions acting on $\{0,1\}^n$, if for every $\mathbf{X} \in \mathcal{X}$ with min-entropy k and every $f \in \mathcal{F}$, there is a distribution $\mathcal{D}$ over $\{0,1\}^m \cup \{same^\star\}$ such that for an independent $\mathbf{Y}$ sampled from D, we have*

$$(\mathrm{nmExt}(\mathbf{X}), \mathrm{nmExt}(f(\mathbf{X}))) \approx_\varepsilon (U_m, \mathrm{copy}(\mathbf{Y}, U_m)),$$

where the second U_m is the same random variable as the first one.

The following connection was discovered between non-malleable codes and seedless non-malleable extractors by Cheraghchi and Guruswami [CG14].

Theorem 3.16. *Let* nmExt $: \{0,1\}^n \to \{0,1\}^m$ *be a polynomial time computable seedless non-malleable extractor that works for min-entropy n with error ϵ with respect to a class of tampering functions $\mathcal{F}$ acting on $\{0,1\}^n$. Further suppose there is a sampling algorithm* Samp *that on any input $z \in \{0,1\}^m$ runs in time* $\text{poly}(n)$ *and samples from a distribution that is ϵ'-close to uniform on the set* $\text{nmExt}^{-1}(s)$.

Then there exists an efficient construction of a non-malleable code with respect to the tampering family $\mathcal{F}$ with block length $= n$, relative rate $\frac{m}{n}$ and error $2^m\epsilon + \epsilon'$.

The non-malleable code is define in the following way: For any message $s \in \{0,1\}^m$, the encoder of the non-malleable code outputs $\text{Samp}(s)$. For any codeword $c \in \{0,1\}^n$, the decoder outputs $\text{nmExt}(c)$.

4 Advice correlation breakers

We use a primitive called 'correlation breaker' in our construction. Consider a situation where we have arbitrarily correlated random variables $\mathbf{Y}^1, \ldots, \mathbf{Y}^r$, where each $\mathbf{Y}^i$ is on ℓ bits. Further suppose $\mathbf{Y}^1$ is a 'good' random variable (typically, we assume $\mathbf{Y}^1$ is uniform or has almost full min-entropy). A correlation breaker CB is an explicit function that takes some additional resource $\mathbf{X}$, where $\mathbf{X}$ is typically additional randomness (an (n,k)-source) that is independent of $\{\mathbf{Y}^1, \ldots, \mathbf{Y}^r\}$. Thus using $\mathbf{X}$, the task is to break the correlation between $\mathbf{Y}^1$ and the random variables $\mathbf{Y}^2, \ldots, \mathbf{Y}^r$, i.e., $\text{CB}(\mathbf{Y}^1, \mathbf{X})$ is independent of $\{\text{CB}(\mathbf{Y}^2, \mathbf{X}), \ldots, \text{CB}(\mathbf{Y}^r, \mathbf{X})\}$. A weaker notion is that of an advice correlation breaker that takes in some advice for each of the $\mathbf{Y}^i$'s as an additional resource in breaking the correlations. This primitive was implicitly constructed in [CGL16] and used in explicit constructions of non-malleable extractors, and has subsequently found many applications in explicit constructions of extractors for independent sources and non-malleable extractors.

We recall an explicit advice correlation breaker constructed in [CL16]. This correlation breaker works even with the weaker guarantee that the 'helper source' $\mathbf{X}$ is now allowed to be correlated to the sources random variables $\mathbf{Y}^1, \ldots, \mathbf{Y}^r$ in a structured way. Concretely, we assume the source to be of the form $\mathbf{X} + \mathbf{Z}$, where $\mathbf{X}$ is assumed to be an (n,k)-source that is uncorrelated with $\mathbf{Y}^1, \ldots, \mathbf{Y}^r, \mathbf{Z}$. We now state the result more precisely.

Theorem 4.1 ([CL16])**.** *For all integers $n, n_1, n_2, k, k_1, k_2, t, d, h, \lambda$ and any $\epsilon > 0$, such that $d = O(\log^2(n/\epsilon))$, $k_1 \geq 2d + 8tdh + \log(1/\epsilon)$, $n_1 \geq 2d + 10tdh + (4ht+1)n_2^2 + \log(1/\epsilon)$, and $n_2 \geq 2d + 3td + \log(1/\epsilon)$, let*

- *$\mathbf{X}$ be an (n, k_1)-source, $\mathbf{X}'$ a r.v on n bits, $\mathbf{Y}^1$ be an $(n_1, n_1 - \lambda)$-source, $\mathbf{Z}, \mathbf{Z}'$ are r.v's on n bits, and $\mathbf{Y}^2, \ldots, \mathbf{Y}^t$ be r.v's on n_1 bits each, such that $\{\mathbf{X}, \mathbf{X}'\}$ is independent of $\{\mathbf{Z}, \mathbf{Z}', \mathbf{Y}^1, \ldots, \mathbf{Y}^t\}$,*
- *$id^1, \ldots, id^t$ be bit-strings of length h such that for each $i \in \{2, t\}$, $id^1 \neq id^i$.*

Then there exists an efficient algorithm $\text{ACB} : \{0,1\}^{n_1} \times \{0,1\}^n \times \{0,1\}^h \to \{0,1\}^{n_2}$ *which satisfies the following: let*

- $\mathbf{Y}_h^1 = \text{ACB}(\mathbf{Y}^1, \mathbf{X} + \mathbf{Z}, id^1)$,
- $\mathbf{Y}_h^i = \text{ACB}(\mathbf{Y}^i, \mathbf{X}' + \mathbf{Z}', id^i)$, $i \in [2, t]$

Then,

$$\mathbf{Y}_h^1, \mathbf{Y}_h^2, \ldots, \mathbf{Y}_h^t, \mathbf{X}, \mathbf{X}' \approx_{O((h+2^\lambda)\epsilon)} \mathbf{U}_{n_2}, \mathbf{Y}_h^2, \ldots, \mathbf{Y}_h^t, \mathbf{X}, \mathbf{X}'.$$

4.1 A new advice correlation breaker

We build a new correlation breaker that is crucial in our non-malleable extractor constructions. Consider the following situation: $\mathbf{X}, \mathbf{Y}$ are independent (n, k)-sources and $\mathbf{X}^1, \mathbf{X}^2, \mathbf{Y}^1, \mathbf{Y}^2$ are arbitrary random variables (each on n bits) such that $\{\mathbf{X}, \mathbf{X}^1, \mathbf{X}^2\}$ is independent of $\{\mathbf{Y}, \mathbf{Y}^1, \mathbf{Y}^2\}$. The task is to build a function $f : \{0,1\}^n \times \{0,1\}^n \times \{0,1\}^h \to \{0,1\}^m$ such that $f(\mathbf{X}, \mathbf{Y}), f(\mathbf{X}^1 + \mathbf{Y}^1, \mathbf{X}^2 + \mathbf{Y}^2) \approx \mathbf{U}_m, f(\mathbf{X}^1 + \mathbf{Y}^1, \mathbf{X}^2 + \mathbf{Y}^2)$. As is the case with previous constructions, we actually consider the weaker notion when the function f takes as input an advice string as well.

The following is our main result.

Theorem 4.2. *There exist constants $\delta, \delta_1, \delta_2 > 0$ such that for all integers n, λ, h, λ and any $0 < \epsilon < 2^{-n^{\delta_1}}$, with $\lambda \leq n^{\delta}$, $h < n^{1/10}$, there exists an efficient algorithm* ACB $: \{0,1\}^n \times \{0,1\}^n \times \{0,1\}^h \to \{0,1\}^{n_1}$, *$n_1 = n^{\delta_2}$, which satisfies the following: let $\mathbf{X}, \mathbf{Y}$ be $(n, n - \lambda)$-sources, $\mathbf{X}', \mathbf{X}'', \mathbf{Y}', \mathbf{Y}''$ be arbitrary random variables on n bits such that $\{\mathbf{X}, \mathbf{X}^1, \mathbf{X}^2\}$ is independent of $\{\mathbf{Y}, \mathbf{Y}^1, \mathbf{Y}^2\}$, id, id' be bit-strings of length h such that $id \neq id'$. Then,*

$$|\mathrm{ACB}(\mathbf{X}, \mathbf{Y}, id), \mathrm{ACB}(\mathbf{X}^1 + \mathbf{Y}^1, \mathbf{X}^2 + \mathbf{Y}^2, id') - \mathbf{U}_m, \mathrm{ACB}(\mathbf{X}^1 + \mathbf{Y}^1, \mathbf{X}^2 + \mathbf{Y}^2, id')| \leq O((h + 2^{\lambda})\epsilon).$$

We use the rest of the section to prove the above theorem. The construction of the function ACB is based on the using alternating extraction, and uses the flip-flop primitive introduced by Cohen [Coh15].

We first define the method of alternating extraction. Assume that there are two parties, Quentin with a source $\mathbf{Q}$ and a uniform seed $\mathbf{S}_0$, and Wendy with a source $\mathbf{W}$. The protocol is an interactive process between Quentin and Wendy, and starts off with Quentin sending the seed $\mathbf{S}_0$ to Wendy. Wendy uses $\mathbf{S}_0$ and a strong seeded extractor Ext_w to extract a seed $\mathbf{R}_0$ using $\mathbf{W}$, and sends $\mathbf{R}_0$ back to Quentin. This constitutes a round of the alternating extraction protocol. In the next round, Quentin uses a strong extractor Ext_q to extract a seed $\mathbf{S}_1$ from $\mathbf{Q}$ using $\mathbf{S}_0$, and sends it to Wendy and so on. The protocol is run for h steps, where h is an input parameter. Thus, the following sequence of random variables is generated:

$$\mathbf{S}_0, \mathbf{R}_0 = \mathrm{Ext}_w(\,\mathbf{S}_0), \mathbf{S}_1 = \mathrm{Ext}_q(\mathbf{Q}, \mathbf{R}_0), \ldots, \mathbf{S}_u = \mathrm{Ext}_q(\mathbf{Q}, \mathbf{R}_{h-1}), \mathbf{R}_h = \mathrm{Ext}_w(\mathbf{W}, \mathbf{S}_h).$$

The look-ahead extractor is defined as follows:

$$\mathrm{laExt}(\mathbf{W}, (\mathbf{Q}, \mathbf{S}_0)) = \mathbf{R}_1, \ldots, \mathbf{R}_h.$$

The flip-flop primitive is presented in Algorithm 1 uses alternating extraction. We construct the advice correlation breaker in Algorithm 2, and the basic idea is to chain together several flip-flop steps.

We setup some ingredients for Algorithm 1.

1. Let $d = O(\log^2(n/\epsilon))$, $n_1 = n^{100\delta}$, $k = 2d$ and $k_1 = 2n_1$.
2. Let $\mathrm{LExt}_1 : \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^d$, $\mathrm{LExt}_2 : \{0,1\}^{n_1} \times \{0,1\}^d \to \{0,1\}^d$ be (k, ϵ)-strong linear seeded extractors.
3. Let $\mathrm{LExt}_3 : \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^{n_1}$ be a (k_1, ϵ)-strong linear seeded extractor.
4. Let $\mathrm{laExt} : \{0,1\}^n \times \{0,1\}^{n_1+d} \to \{0,1\}^{2d}$ be a look-ahead extractor for an alternating extraction protocol run for 2 rounds using $\mathrm{LExt}_1, \mathrm{LExt}_2$ as the seeded extractors.

```
Algorithm 1: flip-flop$(y^i, x, y, b)$
Input: Bit strings $y^i, x, y$ of length $n_1, n, n$ respectively, and a bit $b$.
Output: Bit string $y^{i+1}$ of length $n_1$.

Let $s_0^i = \text{Slice}(y^i, d)$, $\text{laExt}(x, (y^i, s_0^i)) = r_0^i, r_1^i$
Let $\overline{y_1^i} = \text{LExt}_3(y, r_b^i)$
Let $\overline{s_0^i} = \text{Slice}(\overline{y_1^i}, d)$, $\text{laExt}(w, (\overline{y_1^i}, \overline{s_0^i})) = \overline{r_0^i}, \overline{r_1^i}$
Output $y^{i+1} = \text{LExt}_3(y, \overline{r_{1-b}^i})$
```

```
Algorithm 2: ACB$(x, y, id)$
Input: Bit strings $x, y, id$ of length $n, n, h$ respectively.
Output: Bit string $y^{h+1}$ of length $n_1$.

Let $z^1 = \text{Slice}(y, n_1)$
for $j = 1$ to $h$ do
    $z^{j+1} = \text{flip-flop}(z^j, x, y, id[j])$
end
Output $z^{h+1}$.
```

We use the following notation: if $\mathbf{W} = g(\mathbf{X}, \mathbf{Y}, id)$ (for some function g), then we use to $\mathbf{W}'$ or $(\mathbf{W})'$ to denote the random variable $g(\mathbf{X}^1 + \mathbf{Y}^1, \mathbf{X}^2 + \mathbf{Y}^2, id')$.

Let $\ell \in [h]$ be the smallest index such that $id(\ell) \neq id'(\ell)$. The existence of such an ℓ is guaranteed by the fact that $id \neq id'$.

For $i \in [h]$, define $k_{x,i} = k_{y,i} = n - n^{\delta} - i(d + n_1) - \log(1/\epsilon)$.

The proof of correctness of our construction follows by combining Claim 4.3, Claim 4.4, and Claim 4.5. The first claim shows that we can condition random variables appropriately till the $(\ell - 1)$'th iteration of Algorithm 2. The second claim shows that we 'gain independence' in the ℓ'th iteration, i.e., $\mathbf{Z}^{\ell+1}$ is uniform even conditioned on $(\mathbf{Z}^{\ell+1})'$. The final claim shows that this gain of independence continues for the next iterations. The proof of these claims goes via careful conditioning of random variables, and crucially uses the fact that we use linear seeded extractors in the alternating extraction game. We prove the lemma for $\lambda = 0$. When $\lambda > 0$, this adds a term of $2^{\lambda}\epsilon$ to the overall error analyis[3].

Claim 4.3. *For all $i \leq \ell$, conditioned on the random variables $\{\mathbf{S}_a^j : a \in \{0,1\}, j \in [i-1]\}$, $\{\mathbf{R}_a^j : a \in \{0,1\}, j \in [i-1]\}$, $\{\overline{\mathbf{S}_a^j} : a \in \{0,1\}, j \in [i-1]\}$, $\{\overline{\mathbf{R}^j} : a \in \{0,1\}, j \in [i-1]\}$, $\{\mathbf{S}_a^j : a \in \{0,1\}, j \in [i-1]\}$, $\{(\mathbf{R}_a^j)' : a \in \{0,1\}, j \in [i-1]\}$, $\{(\overline{\mathbf{S}_a^j})' : a \in \{0,1\}, j \in [i-1]\}$, $\{(\overline{\mathbf{R}^j})' : a \in \{0,1\}, j \in [i-1]\}$, $\{\mathbf{Z}^j : j \in [i-1]\}$, $\{\overline{\mathbf{Z}^j} : j \in [i-1]\}$, $\{(\mathbf{Z}^j)' : j \in [i-1]\}$, $\{(\overline{\mathbf{Z}^j})' : j \in [i-1]\}$, the following hold:*

- *$\{\mathbf{X}, \mathbf{X}^1, \mathbf{X}^2\}$ is independent of $\{\mathbf{Y}, \mathbf{Y}^1, \mathbf{Y}^2\}$,*
- *$\widetilde{H}_{\infty}(\mathbf{X}) \geq k_{x,i-1}$, $\widetilde{H}_{\infty}(\mathbf{Y}) \geq k_{y,i-1}$.*
- *$\mathbf{Z}^i$ is $O((i-1)\epsilon)$-close to uniform, and is a deterministic function of $\mathbf{Y}$.*

[3] this follows from the fact that a (k, ϵ)-strong seeded extractor with seed-length d also works for when supplied with a seed with min-entropy $d - \lambda$, but has error $2^{\lambda\epsilon}$.

Proof. We prove this by induction on i. The base case for $i = 1$ is direct. Assume the claim to be true for $i < \ell$, and we prove it for $i + 1$. Fix the random variables: $\{\mathbf{S}^j_a : a \in \{0,1\}, j \in [i-1]\}$, $\{\mathbf{R}^j_a : a \in \{0,1\}, j \in [i-1]\}, \{\overline{\mathbf{S}^j_a} : a \in \{0,1\}, j \in [i-1]\}, \{\overline{\mathbf{R}^j} : a \in \{0,1\}, j \in [i-1]\}, \{\mathbf{S}^j_a : a \in \{0, 1\}, j \in [i-1]\}, \{(\mathbf{R}^j_a)' : a \in \{0,1\}, j \in [i-1]\}, \{(\overline{\mathbf{S}^j_a})' : a \in \{0,1\}, j \in [i-1]\}, \{(\overline{\mathbf{R}^j})' : a \in \{0, 1\}, j \in [i-1]\}, \{\mathbf{Z}^j : j \in [i-1]\}, \{\overline{\mathbf{Z}^j} : j \in [i-1]\}, \{(\mathbf{Z}^j)' : j \in [i-1]\}, \{\overline{(\mathbf{Z}^j)}' : j \in [i-1]\}$. By induction hypothesis, we have that

- $\{\mathbf{X}, \mathbf{X}^1, \mathbf{X}^2\}$ is independent of $\{\mathbf{Y}, \mathbf{Y}^1, \mathbf{Y}^2\}$,
- $\widetilde{H}_\infty(\mathbf{X}) \geq k_{x,i-1}$, $\widetilde{H}_\infty(\mathbf{Y}) \geq k_{y,i-1}$.
- $\mathbf{Z}^i$ is $O(i\epsilon)$-close to uniform, and is a deterministic function of $\mathbf{Y}$.

Note that $(\mathbf{Z}^i)' = \mathrm{LExt}_3(\mathbf{X}^2 + \mathbf{Y}^2, (\overline{\mathbf{R}^{i-1}_{1-b'}})') = \mathbf{X}^3 + \mathbf{Y}^3$, where $\mathbf{X}^3$ and $\mathbf{Y}^3$ are random variables each on n_1 bits such that $\{\mathbf{X}, \mathbf{X}^1, \mathbf{X}^2, \mathbf{X}^3\}$ is independent of $\{\mathbf{Y}, \mathbf{Y}^1, \mathbf{Y}^2, \mathbf{Y}^3\}$. This follows from the fact that we have fixed $(\overline{\mathbf{R}^{i-1}_{1-b'}})'$ and that LExt_3 is a linear seeded extractor. Fix the $\mathbf{X}^3$, and it follows that $\mathbf{X}$ has conditional min-entropy at least $k_{x,i-1} - n_1$.

We note that $id(i) = id'(i)$ since $i < \ell$. We split the proof according to the value of $id(i)$.

Case 1: Suppose $id(i) = 0$. We have, $\mathbf{R}^i_0 = \mathrm{LExt}_1(\mathbf{X}, \mathbf{S}^i_0)$ and $(\mathbf{R}^0_i)' = \mathrm{LExt}(\mathbf{X}^1, (\mathbf{S}^i_0)') + \mathrm{LExt}(\mathbf{Y}^1, (\mathbf{S}^i_0)')$. We fix $\mathbf{S}^i_0$, and use the fact that LExt_1 is a strong extractor to conclude that $\mathbf{R}^i_0$ is close to uniform. Further, we fix $(\mathbf{S}^i_0)'$ without affecting $\mathbf{R}^i_0$ which is now a deterministic function of $\mathbf{X}$. Since $(\mathbf{R}^i_0)'' = \mathrm{LExt}_1(\mathbf{X}^1, (\mathbf{S}^i_0)'') + \mathrm{LExt}_1(\mathbf{Y}^1, (\mathbf{S}^i_0)')$, we fix $\mathrm{LExt}_1(\mathbf{Y}^1, (\mathbf{S}^i_0)')$ and this does not affect the distribution of $\mathbf{R}^i_0$. Further note that $(\mathbf{R}^i_0)'$ is now a deterministic function of $\mathbf{X}$. At this point note that $\mathbf{X}$ has conditional min-entropy at least $k_{x,i-1} - n_1$ and $\mathbf{Y}$ has conditional min-entropy at least $k_{y,i-1} - 3d$.

Next, we have, $\overline{\mathbf{Z}^i} = \mathrm{LExt}_3(\mathbf{Y}, \mathbf{R}^i_0)$ and $\overline{\mathbf{Z}^i}' = \mathrm{LExt}_3(\mathbf{X}^2, (\mathbf{R}^i_0)') + \mathrm{LExt}_3(\mathbf{Y}^2, (\mathbf{R}^i_0)'))$. Fix $\mathbf{R}^i_0$, and $\overline{\mathbf{Z}^i}$ remains close to uniform and is now a deterministic function of $\mathbf{Y}$. Thus we fix the random variable $(\mathbf{R}^i_0)'$ without affecting $\overline{\mathbf{Z}^i}$. Note that after this conditioning, $\overline{\mathbf{Z}^i}' = \mathbf{X}^4 + \mathbf{Y}^4$, where $\mathbf{X}^4$ and $\mathbf{Y}^4$ are random variables each on n_1 bits such that $\{\mathbf{X}, \mathbf{X}^1, \mathbf{X}^2, \mathbf{X}^3, \mathbf{X}^4\}$ is independent of $\{\mathbf{Y}, \mathbf{Y}^1, \mathbf{Y}^2, \mathbf{Y}^3, \mathbf{Y}^4\}$. Fix the random variable $\mathbf{X}^4$, and note that $\mathbf{X}$ has conditional min-entropy at least $k_{x,i-1} - 2n_1$. For convenience of notation, let the source $\mathbf{Y}^4$ denote $x^4 + \mathbf{Y}^4$. This does not affect any part of the argument that follows. Continuing with the argument, we have $\overline{\mathbf{R}^i_0} = \mathrm{LExt}_1(\mathbf{X}, \overline{\mathbf{S}^i_0})$ and $(\overline{\mathbf{R}^0_i})' = \mathrm{LExt}(\mathbf{X}^1, \overline{(\mathbf{S}^i_0)}') + \mathrm{LExt}(\mathbf{Y}^1, \overline{(\mathbf{S}^i_0)}')$. We fix $\overline{\mathbf{S}^i_0}$ and use the fact that LExt_1 is a strong seeded extractor to conclude that $\overline{\mathbf{R}^i_0}$ is to uniform. Note that $\overline{\mathbf{R}^i_0}$ is now a deterministic function of $\mathbf{X}$. Next fix $(\overline{\mathbf{S}^0_i})'$ which is deterministic function of $\mathbf{Y}$. We also fix the random variable $\mathrm{LExt}(\mathbf{Y}^1, \overline{(\mathbf{S}^i_0)}')$ without affecting the distribution of $\overline{\mathbf{R}^i_0}$. Thus, $(\overline{\mathbf{R}^0_i})'$ is now a deterministic function of $\mathbf{X}$. Next, $\overline{\mathbf{S}^1_i} = \mathrm{LExt}_2(\overline{\mathbf{Z}^i}, \overline{\mathbf{R}^i_0})$ and $(\overline{\mathbf{S}^1_i})' = \mathrm{LExt}_2(\mathbf{Y}^4, \overline{\mathbf{R}^i_0}')$. Using arguments as before, we fix $\overline{\mathbf{R}^i_0}, \overline{\mathbf{R}^i_0}'$, and the random variable $\overline{\mathbf{S}^1_i}$ is close to uniform and deterministic function of $\mathbf{Y}$. Further, $(\overline{\mathbf{S}^1_i})'$ is a deterministic function of $\mathbf{Y}$. Next, we have $\overline{\mathbf{R}^i_1} = \mathrm{LExt}_1(\mathbf{X}, \overline{\mathbf{S}^1_i})$ and $\overline{\mathbf{R}^i_1}' = \mathrm{LExt}_1(\mathbf{X}^1, (\overline{\mathbf{S}^1_i})') + \mathrm{LExt}_1(\mathbf{Y}^1, (\overline{\mathbf{S}^1_i})')$. Fix $\overline{\mathbf{S}^1_i}$, and $\overline{\mathbf{R}^i_1}$ is close to uniform and a deterministic function of $\mathbf{X}$. Further fix the random variables $(\overline{\mathbf{S}^1_i})'$ and $\mathrm{LExt}_1(\mathbf{Y}^1, (\overline{\mathbf{S}^1_i})')$. Note that the distribution of $\overline{\mathbf{R}^i_1}$ is not affected. Further, $(\overline{\mathbf{R}^i_1})'$ is a deterministic function of $\mathbf{X}$. Finally, we have $\mathbf{Z}^{i+1} = \mathrm{LExt}_3(\mathbf{Y}, \overline{\mathbf{R}^i_1})$ and $(\mathbf{Z}^{i+1})' = \mathrm{LExt}_3(\mathbf{X}^2, (\overline{\mathbf{R}^i_1})') + \mathrm{LExt}_3(\mathbf{Y}^2, (\overline{\mathbf{R}^i_1})')$. Fix the random variables $\overline{\mathbf{R}^i_1}, (\overline{\mathbf{R}^i_1})'$, and it follows that $\mathbf{Z}^{i+1}$ is close to uniform and is a deterministic function of $\mathbf{Y}$. After all these conditioning, it can be verified that $\mathbf{X}$ has conditional min-entropy at least $k_{x,i} - 10n_1 - 10d$ and $\mathbf{Y}$ has conditional min-entropy at least $k_{y,i} - 10n_1 - 10d$.

Case 2: Suppose $id(i) = 1$. Since $\mathbf{X}^3$ is fixed, $(\mathbf{Z}^i)'$ is a deterministic function of $\mathbf{Y}$. We have $\mathbf{R}_0^i = \mathrm{LExt}_1(\mathbf{X}, \mathbf{S}_0^i)$ and $(\mathbf{R}_i^0)' = \mathrm{LExt}(\mathbf{X}^1, (\mathbf{S}_0^i)') + \mathrm{LExt}(\mathbf{Y}^1, (\mathbf{S}_0^i)')$. We fix $\mathbf{S}_0^i$ and since LExt_1 is a strong seeded extractor, it follows that $\mathbf{R}_0^i$ close is to uniform. $\mathbf{R}_0^i$ is now a deterministic function of $\mathbf{X}$, and we fix $(\mathbf{S}_i^0)'$ which is deterministic function of $\mathbf{Y}$. We also fix the random variable $\mathrm{LExt}(\mathbf{Y}^1, (\mathbf{S}_0^i)')$ without affecting the distribution of $\mathbf{R}_0^i$. Thus, $(\mathbf{R}_i^0)'$ is now a deterministic function of $\mathbf{X}$. $\mathbf{S}_i^1 = \mathrm{LExt}_2(\mathbf{Z}^i, \mathbf{R}_0^i)$ and $(\mathbf{S}_i^1)' = \mathrm{LExt}_2(x^3 + \mathbf{Y}^3, \mathbf{R}_0^{i\prime})$. We now fix $\mathbf{R}_0^i, \mathbf{R}_0^{i\prime}$, and the random variable $\mathbf{S}_i^1$ is close to uniform and is a deterministic function of $\mathbf{Y}$. Further, $(\mathbf{S}_i^1)'$ is a deterministic function of $\mathbf{Y}$. We now have $\mathbf{R}_1^i = \mathrm{LExt}_1(\mathbf{X}, \mathbf{S}_i^1)$ and $(\mathbf{R}_1^i)' = \mathrm{LExt}_1(\mathbf{X}^1, (\mathbf{S}_i^1)') + \mathrm{LExt}_1(\mathbf{Y}^1, (\mathbf{S}_i^1)')$. Fix $\mathbf{S}_i^1$, and $\mathbf{R}_1^i$ is close to uniform and a deterministic function of $\mathbf{X}$. Further fix the random variables $(\mathbf{S}_i^1)'$ and $\mathrm{LExt}_1(\mathbf{Y}^1, (\mathbf{S}_i^1)')$. Note that the distribution of $\overline{\mathbf{R}_1^i}$ is not affected. Further, $(\mathbf{R}_1^i)'$ is a deterministic function of $\mathbf{X}$. Finally, we have $\overline{\mathbf{Z}^i} = \mathrm{LExt}_3(\mathbf{Y}, \mathbf{R}_1^i)$ and $(\overline{\mathbf{Z}^i})' = \mathrm{LExt}_3(\mathbf{X}^2, (\mathbf{R}_1^i)') + \mathrm{LExt}_3(\mathbf{Y}^2, (\mathbf{R}_1^i)')$. Fix the random variables $\mathbf{R}_1^i, (\mathbf{R}_1^i)'$, and it follows that $\overline{\mathbf{Z}^i}$ is close to uniform and is a deterministic function of $\mathbf{Y}$. Thus, $(\overline{\mathbf{Z}^i})' = \mathbf{X}^4 + \mathbf{Y}^4$ where $\mathbf{X}^4$ and $\mathbf{Y}^4$ are random variables each on n_1 bits such that $\{\mathbf{X}, \mathbf{X}^1, \mathbf{X}^2, \mathbf{X}^3, \mathbf{X}^4\}$ is independent of $\{\mathbf{Y}, \mathbf{Y}^1, \mathbf{Y}^2, \mathbf{Y}^3, \mathbf{Y}^4\}$. We fix $\mathbf{X}^4$, and $(\overline{\mathbf{Z}^{i+1}})'$ is now a deterministic function of $\mathbf{Y}$.

Continuing, we have $\overline{\mathbf{R}_0^i} = \mathrm{LExt}_1(\mathbf{X}, \overline{\mathbf{S}_0^i})$ and $(\overline{\mathbf{R}_0^i})' = \mathrm{LExt}_1(x^4 + \mathbf{Y}^4, \overline{\mathbf{S}_0^i}')$. We fix $\overline{\mathbf{S}_0^i}$ and $(\overline{\mathbf{S}_0^i})'$, and it follows that $\overline{\mathbf{R}_0^i}$ is close to uniform. Further, $\overline{\mathbf{R}_0^i}$ and $(\overline{\mathbf{R}_0^i})'$ are now deterministic functions of $\mathbf{X}$. We fix $\overline{\mathbf{R}_0^i}, (\overline{\mathbf{R}_0^i})'$, and it follows that $\mathbf{Z}^{i+1} = \mathrm{LExt}(\mathbf{Y}, \overline{\mathbf{R}_0^i})$ is close to uniform. Further, $\mathbf{Z}^{i+1}$ is a deterministic function of $\mathbf{Y}$. Finally, it can be verified that after all these conditioning, $\mathbf{X}$ has conditional min-entropy at least $k_{x,i} - 10n_1 - 10d$ and $\mathbf{Y}$ has conditional min-entropy at least $k_{y,i} - 10n_1 - 10d$. This completes the proof of the claim. □

Claim 4.4. *Conditioned on the random variables* $\{\mathbf{S}_a^j : a \in \{0,1\}, j \in [\ell]\}, \{\mathbf{R}_a^j : a \in \{0,1\}, j \in [\ell]\}, \{\overline{\mathbf{S}_a^j} : a \in \{0,1\}, j \in [\ell]\}, \{\overline{\mathbf{R}^j} : a \in \{0,1\}, j \in [\ell]\}, \{\mathbf{S}_a^j : a \in \{0,1\}, j \in [\ell]\}, \{(\mathbf{R}_a^j)' : a \in \{0,1\}, j \in [\ell]\}, \{(\overline{\mathbf{S}_a^j})' : a \in \{0,1\}, j \in [\ell]\}, \{(\overline{\mathbf{R}^j})' : a \in \{0,1\}, j \in [\ell]\}, \{\mathbf{Z}^j : j \in [\ell]\}, \{\overline{\mathbf{Z}^j} : j \in [\ell]\}, \{(\mathbf{Z}^j)' : j \in [\ell]\}, \{(\overline{\mathbf{Z}^j})' : j \in [\ell+1]\}$, *the following hold:*

- $\{\mathbf{X}, \mathbf{X}^1, \mathbf{X}^2\}$ *is independent of* $\{\mathbf{Y}, \mathbf{Y}^1, \mathbf{Y}^2\}$,
- $\widetilde{H}_\infty(\mathbf{X}) \geq k_{x,\ell}$, $\widetilde{H}_\infty(\mathbf{Y}) \geq k_{y,\ell}$.
- $\mathbf{Z}^{\ell+1}$ *is* $O(\ell\epsilon)$*-close to uniform, and is a deterministic function of* $\mathbf{Y}$*.*

Proof. Fix the random variables: $\{\mathbf{S}_a^j : a \in \{0,1\}, j \in [\ell-1]\}, \{\mathbf{R}_a^j : a \in \{0,1\}, j \in [\ell-1]\}, \{\overline{\mathbf{S}_a^j} : a \in \{0,1\}, j \in [\ell-1]\}, \{\overline{\mathbf{R}^j} : a \in \{0,1\}, j \in [\ell-1]\}, \{\mathbf{S}_a^j : a \in \{0,1\}, j \in [\ell-1]\}, \{(\mathbf{R}_a^j)' : a \in \{0,1\}, j \in [\ell-1]\}, \{(\overline{\mathbf{S}_a^j})' : a \in \{0,1\}, j \in [\ell-1]\}, \{(\overline{\mathbf{R}^j})' : a \in \{0,1\}, j \in [\ell-1]\}, \{\mathbf{Z}^j : j \in [\ell-1]\}, \{\overline{\mathbf{Z}^j} : j \in [\ell-1]\}, \{(\mathbf{Z}^j)' : j \in [\ell-1]\}, \{(\overline{\mathbf{Z}^j})' : j \in [\ell-1]\}$. By Claim 4.3, we have

- $\{\mathbf{X}, \mathbf{X}^1, \mathbf{X}^2\}$ is independent of $\{\mathbf{Y}, \mathbf{Y}^1, \mathbf{Y}^2\}$,
- $\widetilde{H}_\infty(\mathbf{X}) \geq k_{x,\ell-1}$, $\widetilde{H}_\infty(\mathbf{Y}) \geq k_{y,\ell-1}$.
- $\mathbf{Z}^\ell$ is $O(\ell\epsilon)$-close to uniform, and is a deterministic function of $\mathbf{Y}$.

Note that $(\mathbf{Z}^\ell)' = \mathrm{LExt}_3(\mathbf{X}^2 + \mathbf{Y}^2, (\overline{\mathbf{R}^{\ell-1}_{1-id(\ell)'}})') = \mathbf{X}^3 + \mathbf{Y}^3$, where $\mathbf{X}^3$ and $\mathbf{Y}^3$ are random variables each on n_1 bits such that $\{\mathbf{X}, \mathbf{X}^1, \mathbf{X}^2, \mathbf{X}^3\}$ is independent of $\{\mathbf{Y}, \mathbf{Y}^1, \mathbf{Y}^2, \mathbf{Y}^3\}$. This follows from the fact that we have fixed $(\overline{\mathbf{R}^{i-1}_{1-id(\ell)'}})'$ and that LExt_3 is a linear seeded extractor. Fix the random variable $\mathbf{X}^3$, and it follows that $\mathbf{X}$ has conditional min-entropy at least $k_{x,\ell-1} - n_1$.

We note that $id(\ell) \neq id'(\ell)$. We split the proof according to the value of $id(\ell)$.

Case 1**:** Suppose $id(\ell) = 0$. We have, $\mathbf{R}_0^\ell = \text{LExt}_1(\mathbf{X}, \mathbf{S}_0^\ell)$ and $(\mathbf{R}_\ell^0)' = \text{LExt}(\mathbf{X}^1, (\mathbf{S}_0^\ell)') + \text{LExt}(\mathbf{Y}^1, (\mathbf{S}_0^\ell)')$. We fix $\mathbf{S}_0^\ell$, and use the fact that LExt_1 is a strong extractor to conclude that $\mathbf{R}_0^\ell$ is close to uniform. Further, we fix $(\mathbf{S}_0^\ell)'$ without affecting $\mathbf{R}_0^\ell$ which is now a deterministic function of $\mathbf{X}$. Since $(\mathbf{R}_0^\ell)'' = \text{LExt}_1(\mathbf{X}^1, (\mathbf{S}_0^\ell)'') + \text{LExt}_1(\mathbf{Y}^1, (\mathbf{S}_0^\ell)')$, we fix $\text{LExt}_1(\mathbf{Y}^1, (\mathbf{S}_0^\ell)')$ and this does not affect the distribution of $\mathbf{R}_0^\ell$. Further note that $(\mathbf{R}_0^\ell)'$ is now a deterministic function of $\mathbf{X}$. Note that $(\mathbf{S}_1^\ell)' = \text{LExt}_2(x^3 + \mathbf{Y}^3, (\mathbf{R}_0^\ell)')$ and $(\mathbf{R}_1^i)' = \text{LExt}_1(\mathbf{X}^1, (\mathbf{S}_1^\ell)') + \text{LExt}_1(\mathbf{Y}^1, (\mathbf{S}_1^\ell)')$.

Next, we have, $\overline{\mathbf{Z}^\ell} = \text{LExt}_3(\mathbf{Y}, \mathbf{R}_0^\ell)$ and $(\overline{\mathbf{Z}^\ell})' = \text{LExt}_3(\mathbf{X}^2, (\mathbf{R}_1^\ell)') + \text{LExt}_3(\mathbf{Y}^2, (\mathbf{R}_1^\ell)'))$. Fix $\mathbf{R}_0^\ell$, and $\overline{\mathbf{Z}^\ell}$ remains close to uniform and is now a deterministic function of $\mathbf{Y}$. We now fix the random variables $\text{LExt}_3(\mathbf{X}^2, (\mathbf{R}_1^\ell)'), (\mathbf{R}_0^\ell)'$ noting that they are deterministic functions of $\mathbf{X}$. Further note that $(\mathbf{S}_1^\ell)'$ and $(\overline{\mathbf{S}_0^\ell})'$ are now deterministic functions of $\mathbf{Y}$. Continuing with the argument, we have $\overline{\mathbf{R}_0^i} = \text{LExt}_1(\mathbf{X}, \overline{\mathbf{S}_0^i})$ and $(\overline{\mathbf{R}_0^\ell})' = \text{LExt}(\mathbf{X}^1, \overline{(\mathbf{S}_0^\ell)}') + \text{LExt}(\mathbf{Y}^1, \overline{(\mathbf{S}_0^\ell)}')$. We fix $\overline{\mathbf{S}_0^i}$ and use the fact that LExt_1 is a strong seeded extractor to conclude that $\overline{\mathbf{R}_0^i}$ is to uniform. Note that $\overline{\mathbf{R}_0^\ell}$ is now a deterministic function of $\mathbf{X}$. Fix $(\mathbf{S}_1^\ell)'$ and $(\overline{\mathbf{S}_0^\ell})'$ which are deterministic functions of $\mathbf{Y}$. We also fix the random variables $\text{LExt}(\mathbf{Y}^1, (\mathbf{S}_1^\ell)'), \text{LExt}(\mathbf{Y}^1, \overline{(\mathbf{S}_0^\ell)}')$ without affecting the distribution of $\overline{\mathbf{R}_0^\ell}$. Thus, $(\mathbf{R}_1^\ell)'$ and $(\overline{\mathbf{R}_0^\ell})'$ are now deterministic function of $\mathbf{X}$. Next, we have $\overline{\mathbf{S}_1^\ell} = \text{LExt}_2(\overline{\mathbf{Z}^\ell}, \overline{\mathbf{R}_0^\ell})$. We fix $\overline{\mathbf{R}_0^i}$,, and the random variable $\overline{\mathbf{S}_1^\ell}$ is close to uniform and is a deterministic function of $\mathbf{Y}$. We now fix $(\mathbf{R}_i^1)', (\overline{\mathbf{R}_0^\ell})'$ recalling that they are deterministic functions of $\mathbf{X}$. We have, $(\mathbf{Z}^{\ell+1})' = \text{LExt}_3(\mathbf{X}^2, (\overline{\mathbf{R}_0^\ell})') + \text{LExt}_3(\mathbf{Y}^2, (\overline{\mathbf{R}_0^\ell})')$. Fix the random variable $\text{LExt}_3(\mathbf{X}^2, (\overline{\mathbf{R}_0^\ell})')$, and this does not affect the distribution of $\overline{\mathbf{S}_1^\ell}$. Thus, $(\mathbf{Z}^{\ell+1})'$ is now a deterministic function of $\mathbf{Y}$. Next, we have $\overline{\mathbf{R}_1^\ell} = \text{LExt}_1(\mathbf{X}, \overline{\mathbf{S}_1^\ell})$. Fix $\overline{\mathbf{S}_1^\ell}$; it follows that $\overline{\mathbf{R}_1^\ell}$ is close to uniform and a deterministic function of $\mathbf{X}$. We now fix $(\mathbf{Z}^{\ell+1})'$ which is a deterministic function of $\mathbf{Y}$. Finally, we have $\mathbf{Z}^{\ell+1} = \text{LExt}_3(\mathbf{Y}, \overline{\mathbf{R}_1^\ell})$. Fix the random variables $\overline{\mathbf{R}_1^\ell}$, and it follows that $\mathbf{Z}^{\ell+1}$ is close to uniform and is a deterministic function of $\mathbf{Y}$. After all these conditioning, it can be verified that $\mathbf{X}$ has conditional min-entropy at least $k_{x,\ell} - 10n_1 - 10d$ and $\mathbf{Y}$ has conditional min-entropy at least $k_{y,\ell} - 10n_1 - 10d$.

Case 2: Suppose $id(\ell) = 1$. Since $\mathbf{X}^3$ is fixed, $(\mathbf{Z}^\ell)'$ is a deterministic function of $\mathbf{Y}$. We have, $\mathbf{R}_0^\ell = \text{LExt}_1(\mathbf{X}, \mathbf{S}_0^\ell)$ and $(\mathbf{R}_0^\ell)' = \text{LExt}_1(\mathbf{X}^1, (\mathbf{S}_0^i)') + \text{LExt}_1(\mathbf{Y}^1, (\mathbf{S}_0^i)')$. By arguments as before, we fix $\mathbf{S}_0^\ell$ and $(\mathbf{S}_0^i)'$, and $\mathbf{R}_0^\ell$ is close to uniform and a deterministic function of $\mathbf{X}$. Further, fix $\text{LExt}_1(\mathbf{Y}^1, (\mathbf{S}_0^i)')$, and thus $(\mathbf{R}_0^\ell)'$ is now a deterministic function of $\mathbf{X}$. Continuing, we fix $\mathbf{R}_0^\ell, (\mathbf{R}_0^\ell)'$, and the random variable $\mathbf{S}_1^\ell = \text{LExt}_2(\mathbf{Y}, \mathbf{R}_0^\ell)$ is close uniform and is a deterministic function of $\mathbf{Y}$. Recall that $(\overline{\mathbf{Z}^\ell})' = \text{LExt}_3(\mathbf{X}^2, (\mathbf{R}_0^\ell)') + \text{LExt}_3(\mathbf{Y}^2, (\mathbf{R}_0^\ell)')$. Thus we fix $\text{LExt}_3(\mathbf{X}^2, (\mathbf{R}_0^\ell)')$ as well, and $(\overline{\mathbf{Z}^\ell})'$ is now a deterministic function of $\mathbf{Y}$. Next, we have $\mathbf{R}_1^\ell = \text{LExt}_1(\mathbf{X}, \mathbf{S}_1^\ell)$. We fix $\mathbf{S}_1^\ell$ and we have $\mathbf{R}_1^\ell$ is close to uniform and a deterministic function of $\mathbf{X}$. We fix also fix $(\overline{\mathbf{Z}^\ell})'$ which is a deterministic function of $\mathbf{Y}$. Recall that $(\mathbf{R}_0^\ell)' = \text{LExt}_1(\mathbf{X}^1, (\overline{\mathbf{S}_0^\ell})') + \text{LExt}_1(\mathbf{Y}^1, (\overline{\mathbf{S}_0^\ell})')$, where we have fixed $(\overline{\mathbf{S}_0^\ell})'$. Next we fix $\text{LExt}_1(\mathbf{Y}^1, (\overline{\mathbf{S}_0^\ell})')$ and note that this does not affect the distribution of $\mathbf{R}_1^\ell$. Thus $(\mathbf{R}_0^\ell)'$ is now a deterministic function of $\mathbf{X}$.

Next, we have that $\overline{\mathbf{Z}^\ell} = \text{LExt}_3(\mathbf{Y}, \mathbf{R}_1^\ell)$. We fix $\mathbf{R}_1^\ell$ and it follows that $\overline{\mathbf{Z}^\ell}$ is a deterministic function of $\mathbf{Y}$ and is close to uniform. We fix $(\mathbf{R}_0^\ell)'$ which is a deterministic function of $\mathbf{X}$. Observe that $(\overline{\mathbf{S}_1^\ell})' = \text{LExt}_2((\overline{\mathbf{Z}^\ell})', (\mathbf{R}_0^\ell)')$ is fixed. Next, noting that $(\overline{\mathbf{R}_1^\ell})' = \text{LExt}_2(\mathbf{X}^1, (\overline{\mathbf{S}_1^\ell})') + \text{LExt}_2(\mathbf{Y}^1, (\overline{\mathbf{S}_1^\ell})')$, we fix $\text{LExt}_2(\mathbf{X}^1, (\overline{\mathbf{S}_1^\ell})')$ and thus $(\overline{\mathbf{R}_1^\ell})'$ is now a deterministic function of $\mathbf{Y}$. Continuing, we fix $\overline{\mathbf{S}_0^\ell}$, and we have that $\overline{\mathbf{R}_0^\ell} = \text{LExt}_1(\mathbf{X}, \overline{\mathbf{S}_0^\ell})$ is close to uniform and is a deterministic function of $\mathbf{X}$. We fix the random variables $(\overline{\mathbf{R}_1^\ell})', \text{LExt}_3(\mathbf{Y}^2, (\overline{\mathbf{R}_1^\ell})')$ noting that $(\overline{Z^{\ell+1}})' = \text{LExt}_3(\mathbf{X}^2,$

$(\overline{\mathbf{R}_1^\ell})')$+LExt$_3(\mathbf{Y}^2, (\overline{\mathbf{R}_1^\ell})')$ is now a deterministic function of $\mathbf{X}$. Finally, note that $\mathbf{Z}^{\ell+1} = \text{LExt}_3(\mathbf{Y}, \overline{\mathbf{R}_0^\ell})$. We fix $\overline{\mathbf{R}_0^\ell}$ and it follows that $\mathbf{Z}^{\ell+1}$ is close to uniform and is a determistic function of $\mathbf{Y}$. We fix $(\overline{Z^{\ell+1}})'$ noting that it is a deterministic function of $\mathbf{X}$ and hence does not affect the distribution of $\mathbf{Z}^{\ell+1}$. Finally, it can be verified that after all these conditioning, $\mathbf{X}$ has conditional min-entropy at least $k_{x,i} - 10n_1 - 10d$ and $\mathbf{Y}$ has conditional min-entropy at least $k_{y,i} - 10n_1 - 10d$. This completes the proof of the claim. □

The following claim can be proved using arguments that are very similar to the ones used in the proof of Claim 4.3 and Claim 4.4, and we skip the proof.

Claim 4.5. *For all $i \in [\ell+1, h+1]$, conditioned on the random variables $\{\mathbf{S}_a^j : a \in \{0,1\}, j \in [i-1]\}$, $\{\mathbf{R}_a^j : a \in \{0,1\}, j \in [i-1]\}, \{\overline{\mathbf{S}_a^j} : a \in \{0,1\}, j \in [i-1]\}, \{\overline{\mathbf{R}^j} : a \in \{0,1\}, j \in [i-1]\}, \{\mathbf{S}_a^j : a \in \{0, 1\}, j \in [i-1]\}, \{(\mathbf{R}_a^j)' : a \in \{0,1\}, j \in [i-1]\}, \{(\overline{\mathbf{S}_a^j})' : a \in \{0,1\}, j \in [i-1]\}, \{(\overline{\mathbf{R}^j})' : a \in \{0,1\}, j \in [i-1]\}, \{\mathbf{Z}^j : j \in [i-1]\}, \{\overline{\mathbf{Z}^j} : j \in [i-1]\}, \{(\mathbf{Z}^j)' : j \in [i-1]\}, \{\overline{(\mathbf{Z}^j)'} : j \in [i]\}$, the following hold:*

- *$\{\mathbf{X}, \mathbf{X}^1, \mathbf{X}^2\}$ is independent of $\{\mathbf{Y}, \mathbf{Y}^1, \mathbf{Y}^2\}$,*
- *$\widetilde{H}_\infty(\mathbf{X}) \geq k_{x,i-1}$, $\widetilde{H}_\infty(\mathbf{Y}) \geq k_{y,i-1}$.*
- *$\mathbf{Z}^i$ is $O((i-1)\epsilon)$-close to uniform, and is a deterministic function of $\mathbf{Y}$.*

5 Non-malleable extractors in the interleaved model

Our main result in this section is a non-malleable extractor for 2-interleaved sources.

Theorem 5.1. *For all integers $n > 0$ with there exists an efficiently computable function $\text{i}\ell\text{NM} : \{0,1\}^{2n} \to \{0,1\}^m$, $m = n^{\Omega(1)}$, such that the following holds: Let $\mathbf{X}$ and $\mathbf{Y}$ be independent uniform sources on n bits each, and let $\mathbf{Z} = (\mathbf{X} \circ \mathbf{Y})_\pi$ be an interleaving of $\mathbf{X}$ and $\mathbf{Y}$, where $\pi : [2n] \to [2n]$ is permutation. Let $f, g \in \mathcal{F}_n$ be arbitrary functions. Then, there exists a distribution $\mathcal{D}_{f,g}$ on $\{0,1\}^m \cup \{same^\star\}$ that is independent of $\mathbf{X}$ and $\mathbf{Y}$ such that*

$$|\text{i}\ell\text{NM}((\mathbf{X} \circ \mathbf{Y})_\pi), \text{i}\ell\text{NM}((f(\mathbf{X}) \circ g(\mathbf{Y}))_\pi) - \text{copy}(\mathcal{D}_{f,g}, \mathbf{U}_m)| \leq 2^{-n^{\Omega(1)}}.$$

We impose constraint that at least one of tampering functions has no fixed points and prove the following theorem.

Theorem 5.2. *There exists a small constant $\delta > 0$ such that for all positive integers n, k with $n \geq k \geq n - n^\delta$ there exists an efficiently computable function $\text{i}\ell\text{NM} : \{0,1\}^{2n} \to \{0,1\}^m$, $m = n^{\Omega(1)}$, such that the following holds: Let $\mathbf{X}$ and $\mathbf{Y}$ be independent (n,k)-sources, and let $\mathbf{Z} = (\mathbf{X} \circ \mathbf{Y})_\pi$ be an interleaving of $\mathbf{X}$ and $\mathbf{Y}$, where $\pi : [2n] \to [2n]$ is permutation. Let $f : \{0,1\}^n \to \{0,1\}^n$ and $g : \{0,1\}^n \to \{0,1\}^n$ be arbitrary functions such that at least one of f and g does not have any fixed points. Then,*

$$|\text{i}\ell\text{NM}((\mathbf{X} \circ \mathbf{Y})_\pi), \text{i}\ell\text{NM}((f(\mathbf{X}) \circ g(\mathbf{Y}))_\pi) - \mathbf{U}_m, \text{i}\ell\text{NM}((f(\mathbf{X}) \circ g(\mathbf{Y}))_\pi)| \leq 2^{-n^{\Omega(1)}}.$$

Theorem 5.1 is can be derived from Theorem 5.2 in the following way: Let $\Gamma_1 = \{x \in \{0,1\}^n : f(x) = x\}$ and $\Gamma_2 = \{0,1\}^n \setminus \Gamma_1$. Further, let $\Delta_1 = \{y \in \{0,1\}^n : g(y) = y\}$ and $\Delta_2 = \{0,1\}^n \setminus \Delta_1$. Let $\mathbf{X}_i$ be flat on Γ_i for $i = 1, 2$ and $\mathbf{Y}_i$ be flat on Δ_i for $i = 1, 2$.

Clearly, $((\mathbf{X}\circ\mathbf{Y})_\pi,(f(\mathbf{X})\circ g(\mathbf{Y}))_\pi)$ is a convex combination of $((\mathbf{X}_i\circ\mathbf{Y}_j)_\pi,(f(\mathbf{X}_i)\circ g(\mathbf{Y}_j))_\pi)$, for $i=1,2$ and $j=1,2$. If the weight of any of these distributions in the convex combination is less that 2^{-n^δ}, we ignore it in and add an error of 2^{-n^δ} to our analysis. Thus, we can assume that the entropy of each of the sources $\mathbf{X}_1,\mathbf{X}_2,\mathbf{Y}_1,\mathbf{Y}_2$ is at least $n-n^\delta$. Note that $((\mathbf{X}_1\circ\mathbf{Y}_1)_\pi, (f(\mathbf{X}_1)\circ g(\mathbf{Y}_1))_\pi)=((\mathbf{X}_1\circ\mathbf{Y}_1)_\pi,(\mathbf{X}_1\circ\mathbf{Y}_1)_\pi)$, and in each of the other convex combinations it holds that at least one f or g has no fixed points. Thus, Theorem 5.1 is now direct using Theorem 5.2.

The rest of the Section is used to prove Theorem 5.2. Our extractor construction uses the framework developed in [CGL16] for constructing non-malleable extractors. Very informally, the framework is the following: The first step is to produce a short string that (with high probability) is different from the corresponding tampered string. This is produced by a primitive called as an advice generator. The next step is to use a primitive called as an advice correlation breaker, which informally, breaks correlations between random variables using the short string produced in the previous step as 'advice'.

We use the following notation for the rest of this section: We use $\mathbf{Z}'$ to denote the random variable $(f(\mathbf{X})\circ g(\mathbf{Y}))_\pi$. Further, for any function ν, if $\mathbf{Q}=\nu(\mathbf{Z})$, then we use $\mathbf{Q}'$ to denote $\nu(\mathbf{Z}')$.

5.1 An explicit advice generator

A key ingredient in our construction is an explicit advice generator. This primitive has been extensively used in recent constructions of non-malleable extractors. Informally, the advice generator on input $\mathbf{Z}$ produces a short string $\mathbf{W}$ such that the corresponding tampered variable $\mathbf{W}'=\mathrm{advGen}(\mathbf{Z}')$ is different from $\mathbf{W}$ with high probability. In particular, we prove the following.

Lemma 5.3. *There exist a constant $C>0$ such that for any $\delta>0$ and positive integers n,k with $n\geq k\geq n-n^\delta$ there exists an efficiently computable function $\mathrm{advGen}:\{0,1\}^{2n}\rightarrow\{0,1\}^{n_4}$, $n_4=n^{\delta_2}$, $\delta_2=C\delta$, such that the following holds: Let $\mathbf{X}$ and $\mathbf{Y}$ be independent (n,k)-sources, and let $\mathbf{Z}=(\mathbf{X}\circ\mathbf{Y})_\pi$ be an arbitrary interleaving of $\mathbf{X}$ and $\mathbf{Y}$, where $\pi:[2n]\rightarrow[2n]$ is a permutation. Let $f:\{0,1\}^n\rightarrow\{0,1\}^n$ and $g:\{0,1\}^n\rightarrow\{0,1\}^n$ be arbitrary tampering functions such that at least one of f and g does not have any fixed points. Then, with probability at least $1-2^{-n^{\Omega(1)}}$ over the fixing of the random variables $\mathrm{advGen}(\mathbf{Z}),\mathrm{advGen}(\mathbf{Z}')$,*

- $\mathrm{advGen}(\mathbf{Z})\neq\mathrm{advGen}(\mathbf{Z}')$,
- $\{\mathbf{X},\mathbf{X}'\}$ *independent of* $\{\mathbf{Y},\mathbf{Y}'\}$,
- $H_\infty(\mathbf{X})\geq k-3n_4$, $H_\infty(\mathbf{Y})\geq k-3n_4$.

We prove the above lemma in the rest of this subsection. We claim that the function advGen computed by Algorithm 3 satisfies the above lemma. We first set up some parameters and ingredients.

- Let $E:\{0,1\}^{2n}\rightarrow\{0,1\}^{n_1}$ be the encoding function of a linear error correcting code $\mathcal{C}$ with constant rate α_1 and constant distance β_1.
- Let $n_2=n^{\delta_1}$, where $\delta_1=2\delta$.
- Let $\mathrm{Ext}_1:\{0,1\}^{n_2}\times\{0,1\}^{d_1}\rightarrow\{0,1\}^{\log(n_1-n_2)}$ be a $(n_2/8,\beta_1/10)$-seeded extractor instantiated using Theorem 3.9. Thus $d_1=C_3\log n_2$, for some constant C_3.

- Let $\mathrm{Samp} : \{0,1\}^{n_2} \to [n_1 - n_2]^{n_3}$ be the sampler obtained from Theorem 3.8 using Ext_1. Thus $n_3 = 2^{d_1} = n^{C_3\delta_1}$.

```
Algorithm 3: advGen($z$)
Input: Bit-string $z = (x \circ y)_\pi$ of length $2n$, where $x$ and $y$ are each $n$ bit-strings, and
$\pi : [2n] \to [2n]$ is a permutation.
Output: Bit string $w$ of length $n_4 = n_2 + n_3$.

Let $z_1 = \mathrm{Slice}(z, n_2)$. Let $z_2$ be the remaining part of $z$.
Let $v = E(z_2)$.
Let $T = \mathrm{Samp}(z_1)$.
Output $w = z_1 \circ v_T$.
```

Lemma 5.4. *With probability at least* $1 - 2^{-n^{\Omega(1)}}$, $\mathbf{W} \neq \mathbf{W}'$.

Proof. Let $\mathbf{X}_1$ be the bits of $\mathbf{X}$ in $\mathbf{Z}_1$ and $\mathbf{X}_2$ be the bits of $\mathbf{X}$ in remaining part of $\mathbf{Z}$. Define $\mathbf{Y}_1$ and $\mathbf{Y}_2$ similarly. Without loss of generality, suppose $|\mathbf{X}_1| \geq |\mathbf{Y}_1|$. If $\mathbf{Z}_1 \neq \mathbf{Z}_1'$, then clearly $\mathbf{W} \neq \mathbf{W}'$. Thus suppose $\mathbf{Z}_1 = \mathbf{Z}_1'$.

Fix the random variable $\mathbf{Y}_1$. Thus $\mathbf{Z}_1$ is now a deterministic function of $\mathbf{X}$. Next we fix the random variable $\mathbf{X}_2$. Note that since $H_\infty(\mathbf{X}) \geq n - n^\delta$, it follows by Lemma 3.1 that with probability at least $1 - 2^{-n^\delta}$ over the fixing of $\mathbf{X}_2$, $H_\infty(\mathbf{X}_1) \geq n_2/2$. Further fix the random variables $\mathbf{Y}_2, \mathbf{Y}_2'$ noting it does not affect the distribution of $\mathbf{X}_2$. Note that this fixes $\mathbf{Z}_2$ and $\mathbf{Z}_2'$. Assume without loss of generality that the function f has no fixed points. Since $\mathbf{X} \neq \mathbf{X}'$ and $\mathbf{X}_1 = \mathbf{X}_1'$, it follows that $\mathbf{X}_2 \neq \mathbf{X}_2$ and hence $\mathbf{Z}_2 \neq \mathbf{Z}_2$.

Now, using the fact E is an encoding function of a code with constant distance, it follows that there exists a subset $S \subset [n_1]$, $|S| \geq \beta(n_1 - n_2)$ such that for any $i \in S$, $(\mathbf{Z}_2)_i \neq (\mathbf{Z}_2')_i$. It now follows from Theorem 3.8 that with probability at least $1 - 2^{-n_2/4}$, $|\mathrm{Samp}(\mathbf{Z}_1) \cap S| \geq \beta(n_1 - n_2)/2 > 1$. It follows that with probability at least $1 - 2^{-n^{\Omega(1)}}$, $\mathbf{V}_\mathbf{T} \neq \mathbf{V}_{\mathbf{T}'}$. This completes the proof. □

5.2 The extractor construction

We are now ready to present the construction of iℓNM that satisfies the requirements of Theorem 5.2. We first set up some parameters and ingredients. We are now ready to present the construction of iℓNM that satisfies the requirements of Theorem 5.2. We first set up some parameters and ingredients.

- Let $\delta > 0$ be a small enough constant.
- Let $\mathrm{advGen} : \{0,1\}^{2n} \to \{0,1\}^{n_1}$ be the advice generator from Lemma 5.3 using $\delta_{5.3} = \delta$. Thus $n_1 = n^{\delta_1}$, where $\delta_1 = C_{5.3}\delta_{5.3}$.
- Let $n_2 = n^{\delta_2}$, where $\delta_2 = 2\delta_1$.
- Let $\mathrm{LExt}_1 : \{0,1\}^{n_2} \times \{0,1\}^d \to \{0,1\}^{d_1}$, $d_1 = \sqrt{n_2}$, be a linear-seeded extractor instantiated from Theorem 3.10 set to extract from entropy $k_1 = n_2/10$ with error $\epsilon_1 = 1/10$. Thus $d = C_1 \log n_2$, for some constant C_1. Let $D = 2^d = n^{\delta_3}$, $\delta_3 = 2C_1\delta_1$.
- Set $\delta' = 20C_{5.3}C_1\delta$.

- Let $\mathrm{LExt}_2 : \{0,1\}^{2n} \times \{0,1\}^{d_1} \to \{0,1\}^{n_4}$, $n_4 = n^{8\delta_3}$ be a linear-seeded extractor instantiated from Theorem 3.10 set to extract from entropy $k_2 = 0.9k$ with error $\epsilon_2 = 2^{-\Omega(\sqrt{d_1})} = 2^{-n^{\Omega(1)}}$, such that the seed length of the extractor LExt_2 (by Theorem 3.10) is d_1.
- Let $\mathrm{ACB} : \{0,1\}^{n_{1,acb}} \times \{0,1\}^{n_{acb}} \times \{0,1\}^{h_{acb}} \to \{0,1\}^{n_{2,acb}}$, be the advice correlation breaker from Theorem 4.1 set with the following parameters: $n_{acb} = 2n, n_{1,acb} = n_4, n_{2,acb} = m = O(n^{2\delta_3}), t_{acb} = 2D, h_{acb} = n_1 + d, \epsilon_{acb} = 2^{-n^{\delta_1}}$, $d_{acb} = O(\log^2(n/\epsilon_{acb})), \lambda_{acb} = 0$. It can be checked that by our choice of parameters, the conditions required for Theorem 4.1 indeed hold for $k_{1,acb} \geq n^{2\delta_3}$.

Algorithm 4: iℓNM(z)

Input: Bit-string $z = (x \circ y)_\pi$ of length $2n$, where x and y are each n bit-strings, and $\pi : [2n] \to [2n]$ is a permutation.
Output: Bit string of length m.

```
Let $w = \mathrm{advGen}(z)$.
Let $z_1 = \mathrm{Slice}(z, n_2)$.
Let $v$ be a $D \times n_3$ matrix, with its $i$'th row $v_i = \mathrm{LExt}_1(z_1, i)$.
Let $r$ be a $D \times n_4$ matrix, with its $i$'th row $r_i = \mathrm{LExt}_2(z, v_i)$.
Let $s$ be a $D \times m$ matrix, with its $i$'th row $s_i = \mathrm{ACB}(r_i, z, w \circ i)$.
Output $\oplus_{i=1}^{D} s_i$.
```

We now prove that the function iℓNM computed by Algorithm 4 satisfies the conclusion of Theorem 5.2. Let $\mathbf{X}_1$ be the bits of $\mathbf{X}$ in $\mathbf{Z}_1$ and $\mathbf{X}_2$ be the remaining bit of $\mathbf{X}$. Define $\mathbf{Y}_1$ and $\mathbf{Y}_2$ similarly. Without loss of generality suppose that $|\mathbf{X}_1| \geq |\mathbf{Y}_1|$. Define $\overline{\mathbf{X}} = (\mathbf{X} \circ 0^n)_\pi$ and $\overline{\mathbf{Y}} = (\mathbf{Y} \circ 0^n)_\pi$. Further, let $\overline{\mathbf{X}_1} = \mathrm{Slice}(\overline{\mathbf{X}}, n_2)$ and $\overline{\mathbf{Y}_1} = \mathrm{Slice}(\overline{\mathbf{Y}}, n_2)$. It follows that $\mathbf{Z} = \overline{\mathbf{X}} + \overline{\mathbf{Y}}$, and $\mathbf{Z}_1 = \overline{\mathbf{X}_1} + \overline{\mathbf{Y}_1}$ (recall that we use the + operation to denote bitwise xor).

Claim 5.5. *Conditioned on the random variables* $\mathbf{W}, \mathbf{W}', \mathbf{Y}_1, \mathbf{Y}'_1$, $\{\mathrm{LExt}_2(\overline{\mathbf{X}}, \mathrm{LExt}_1(\overline{\mathbf{X}_1} + \overline{\mathbf{Y}_1}, i))\}_{i=1}^{D}$, $\{\mathrm{LExt}_2(\overline{\mathbf{X}}', \mathrm{LExt}_1(\overline{\mathbf{X}}'_1 + \overline{\mathbf{Y}}'_1, i))\}_{i\in[D]}$, $\mathbf{X}_1$ *and* $\mathbf{X}'_1$, *the following hold:*

- *the matrix* $\mathbf{R}$ *is* $2^{-n^{\Omega(1)}}$*-close to a somewhere random source,*
- $\mathbf{R}$ *and* $\mathbf{R}'$ *are deterministic functions of* $\mathbf{Y}$*,*
- $H_\infty(\mathbf{X}) \geq n - n^{\delta'}$, $H_\infty(\mathbf{Y}) \geq n - n^{\delta'}$.

Proof. Fix the random variables $\mathbf{W}, \mathbf{W}'$. By Lemma 5.3, it follows that $\{\mathbf{X}, \mathbf{X}'\}$ remains independent of $\{\mathbf{Y}, \mathbf{Y}'\}$, and with probability at least $1 - 2^{-n^{\Omega(1)}}$, $H_\infty(\mathbf{X}) \geq k - 3n_1$ and $H_\infty(\mathbf{Y}) \geq k - 3n_1$. It follows that with probability at least $1 - 2^{-n^{\Omega(1)}}$, $H_\infty(\mathbf{X}_1) \geq \frac{n_2}{2} - 3n_1 - 2n^\delta \geq \frac{n_2}{2} - 5n_1 \geq 0.4n_2$.

Now, by construction, we have that for any $j \in [D]$,

$$\begin{aligned} \mathbf{R}_j &= \mathrm{LExt}_2(\mathbf{Z}, \mathrm{LExt}_1(\mathbf{Z}_1, j)) \\ &= \mathrm{LExt}_2(\overline{\mathbf{X}} + \overline{\mathbf{Y}}, \mathrm{LExt}_1(\overline{\mathbf{X}_1} + \overline{\mathbf{Y}_1}, j)) \\ &= \mathrm{LExt}_2(\overline{\mathbf{X}}, \mathrm{LExt}_1(\overline{\mathbf{X}_1} + \overline{\mathbf{Y}_1}, j)) + \mathrm{LExt}_2(\overline{\mathbf{Y}}, \mathrm{LExt}_1(\overline{\mathbf{X}_1} + \overline{\mathbf{Y}_1}, j)) \end{aligned}$$

Fix the random variables $\mathbf{Y}_1, \mathbf{Y}'_1$. Note that after these fixings, $\overline{\mathbf{Y}}$ has min-entropy at least $n - 3n_1 - n_2 > 0.9k$. Now, since LExt_2 is a strong seeded extractor for entropy $0.9k$, it follows that there exists a set $T \subset \{0,1\}^{d_1}$, $|T| \geq (1 - \sqrt{\epsilon_2})2^{d_1}$, such that for any $j \in [T]$, $|\mathrm{LExt}_2(\overline{\mathbf{Y}}, j) - \mathbf{U}_{n_4}| \leq \sqrt{\epsilon_2}$.

Now viewing LExt_1 as a sampler (see Section 3.3) using the weak source $\overline{\mathbf{X}}_{1,y_1} = \overline{\mathbf{X}}_1 + \overline{y_1}$, it follows by Theorem 3.8 that

$$\Pr[|\{\mathrm{LExt}_1(\overline{\mathbf{X}}_{1,y_1}, i) : i \in \{0,1\}^d\} \cap T| > (1 - \sqrt{\epsilon_2} - \epsilon_1)D] \geq 1 - 2^{0.2n_2} = 1 - 2^{-n^{\Omega(1)}}.$$

We fix $\overline{\mathbf{X}}_1$, and it follows that with probability at least $1 - 2^{-n^{\Omega(1)}}$, $\{\mathrm{LExt}_1(\overline{\mathbf{X}}_{1,y_1}, i) : i \in \{0,1\}^d\} \cap T \neq \emptyset$, and thus there exists a $j \in [D]$ such that $\mathrm{LExt}_2(\overline{\mathbf{Y}}, \mathrm{LExt}_1(\overline{\mathbf{X}_1} + \overline{\mathbf{Y}_1}, j))$ is $2^{-n^{\Omega(1)}}$-close to $\mathbf{U}_{n_2}$ and is a deterministic function of $\mathbf{Y}$.

We now fix the random variables $\overline{\mathbf{X}}_1'$, $\{\mathrm{LExt}_2(\overline{\mathbf{X}}, \mathrm{LExt}_1(\overline{\mathbf{X}_1}+\overline{\mathbf{Y}_1}, i))\}_{i=1}^D$, $\{\mathrm{LExt}_2(\overline{\mathbf{X}}', \mathrm{LExt}_1(\overline{\mathbf{X}_1}'+\overline{\mathbf{Y}_1}', i))\}_{i=1}^D$, and note that $\mathrm{LExt}_2(\overline{\mathbf{Y}}, \mathrm{LExt}_1(\overline{\mathbf{X}_1} + \overline{\mathbf{Y}_1}, j))$ continues to be $2^{-n^{\Omega(1)}}$-close to $\mathbf{U}_{n_2}$. It follows that $\mathbf{R}_j$ is $2^{-n^{\Omega(1)}}$-close to $\mathbf{U}_{n_2}$. Further, for any $i \in [D]$, the random variables $\mathbf{R}_i$ and $\mathbf{R}_i'$ are deterministic functions of $\mathbf{Y}$. Finally, note that $\{\mathbf{X}, \mathbf{X}'\}$ remain independent after these conditionings, and $H_\infty(\mathbf{X}) \geq n - 3n_1 - 2n_2 - 2Dn_4 \geq n - n^{10\delta_3}$ and $H_\infty(\mathbf{Y}) \geq n - 3n_1 - n_2 > n - n^{\delta_3}$. □

Theorem 5.2 is direct from the next claim.

Claim 5.6. *There exists $j \in [D]$ such that*

$$\mathbf{S}_j, \{\mathbf{S}_i\}_{i \in [D] \setminus j} \approx_{2^{-n^{\Omega(1)}}} \mathbf{U}_m, \{\mathbf{S}_i\}_{i \in [D] \setminus j}.$$

Proof. Fix the random variables: $\mathbf{W}, \mathbf{W}', \mathbf{Y}_1, \mathbf{Y}_1'$, $\{\mathrm{LExt}_2(\overline{\mathbf{X}}, \mathrm{LExt}_1(\overline{\mathbf{X}}_1 + \overline{\mathbf{Y}}_1, i))\}_{i=1}^D$, $\{\mathrm{LExt}_2(\overline{\mathbf{X}}', \mathrm{LExt}_1(\overline{\mathbf{X}}_1' + \overline{\mathbf{Y}}_1', i))\}_{i \in [D]}$, $\mathbf{X}_1$ and $\mathbf{X}_1'$. By Lemma 5.3, we have that with probability at least $1 - 2^{-n^{\Omega(1)}}$, $\mathbf{W} \neq \mathbf{W}'$. Further, by Claim 5.5 we have that $\mathbf{R}$ and $\mathbf{R}'$ are deterministic functions of $\mathbf{Y}$, and with probability at least $1 - 2^{-n^{\Omega(1)}}$, there exists $j \in [D]$ such that $\mathbf{R}_j$ is $2^{-n^{\Omega(1)}}$-close to uniform, and $H_\infty(\overline{\mathbf{X}}) \geq \frac{1}{2}n_{acb} - n^{\delta'} > n^{2\delta_3}$. Recall that $\mathbf{Z} = \overline{\mathbf{X}} + \overline{\mathbf{Y}}$ and $\mathbf{Z}' = \overline{\mathbf{X}}' + \overline{\mathbf{Y}}'$. It now follows by Theorem 4.1 that

$$\begin{aligned}\mathrm{ACB}(\mathbf{R}_j, \mathbf{Z}, \mathbf{W} \circ j), \{\mathrm{ACB}(\mathbf{R}_i, \overline{\mathbf{X}} + \overline{\mathbf{Y}}, \mathbf{W} \circ i)\}_{i \in [D] \setminus j}, \{\mathrm{ACB}(\mathbf{R}_i', \overline{\mathbf{X}}' + \overline{\mathbf{Y}}', \mathbf{W}' \circ i)\}_{i \in [D]} \approx_{2^{-n^{\Omega(1)}}} \\ \mathbf{U}_m, \{\mathrm{ACB}(\mathbf{R}_i, \overline{\mathbf{X}} + \overline{\mathbf{Y}}, \mathbf{W} \circ i)\}_{i \in [D] \setminus j}, \{\mathrm{ACB}(\mathbf{R}_i', \overline{\mathbf{X}}' + \overline{\mathbf{Y}}', \mathbf{W}' \circ i)\}_{i \in [D]}\end{aligned}$$

This completes the proof of the claim. □

6 NM extractors for linear composed with split-state adversaries

The main result of this section is an explicit non-malleable extractor against the tampering family $\mathrm{Lin} \circ 2\mathrm{SS} \subset \mathcal{F}_{2n}$.

Theorem 6.1. *For all integers $n > 0$ there exists an explicit function $\mathrm{nmExt} : \{0,1\}^{2n} \to \{0,1\}^m$, $m = n^{\Omega(1)}$, such that the following holds: For any linear function $h : \{0,1\}^{2n} \to \{0,1\}^{2n}$, and arbitrary functions $f, g \in \mathcal{F}_n$, and independent uniform sources $\mathbf{X}$ and $\mathbf{Y}$ each on n bits, there exists a distribution $\mathcal{D}_{h,f,g}$ on $\{0,1\}^m \cup \{same^\star\}$, such that*

$$|\mathrm{nmExt}(\mathbf{X}, \mathbf{Y}), \mathrm{nmExt}(h(f(\mathbf{X}), g(\mathbf{Y}))) - \mathbf{U}_m, \mathrm{copy}(\mathcal{D}_{h,f,g}, \mathbf{U}_m)| \leq 2^{-n^{\Omega(1)}}.$$

Our first step is to show that in order to prove Theorem 6.1 it is enough to construct a non-malleable extractor satisfying Theorem 6.2.

Theorem 6.2. *There exists a $\delta > 0$ such that for all integers $n, k > 0$ with $n \geq k \geq n - n^{\delta}$, there exists an explicit function* $\mathrm{nmExt} : \{0,1\}^{2n} \to \{0,1\}^m$*, $m = n^{\Omega(1)}$, such that the following holds: Let $\mathbf{X}$ and $\mathbf{Y}$ to be independent $(n, n - n^{\delta})$-sources and f_1, f_2, g_1, g_2 to satisfy the following condition:*

- *$\forall x \in support(\mathbf{X})$ and $y \in support(\mathbf{Y})$, $f_1(x) + g_1(y) \neq x$ or*
- *$\forall x \in support(\mathbf{X})$ and $y \in support(\mathbf{Y})$, $f_2(x) + g_2(y) \neq y$.*

Then,

$$|\mathrm{nmExt}(\mathbf{X}, \mathbf{Y}), \mathrm{nmExt}(f_1(\mathbf{X}) + g_1(\mathbf{Y}), f_2(\mathbf{X}) + g_2(\mathbf{Y})) - \mathbf{U}_m, \mathrm{nmExt}(f_1(\mathbf{X}) + g_1(\mathbf{Y}), f_2(\mathbf{X}) + g_2(\mathbf{Y}))| \leq 2^{-n^{\Omega(1)}}.$$

Proof of Theorem 6.1 assuming Theorem 6.2. Define $\overline{f(x)} = h(f(x), 0^n)$ and $\overline{g(y)} = h(0^n, y)$. Thus, $h(f(x), g(y)) = \overline{f(x)} + \overline{g(y)}$. Define functions $h_1 : \{0,1\}^{2n} \to \{0,1\}^n$ and $h_2 : \{0,1\}^{2n} \to \{0,1\}^n$ such that $h(f(x), g(y)) = h_1(x, y), h_2(x, y)$. Since $h(f(x), g(y)) = \overline{f(x)} + \overline{g(y)}$, it follows that there exists functions $f_1, g_1, f_2, g_2 \in \mathcal{F}_n$ such that for all $x, y \in \{0,1\}^n$, the following hold:

- $h_1(x, y) = f_1(x) + g_1(y)$, and
- $h_2(x, y) = f_2(x) + g_2(y)$.

Thus, $h(f(x), g(y)) = f_1(x) + g_1(y), f_2(x) + g_2(y)$.

Now, the idea is to show that $((\mathbf{X}, \mathbf{Y}), (f_1(\mathbf{X}) + g_1(\mathbf{Y}), f_2(\mathbf{X}) + g_2(\mathbf{Y})))$ is $2^{-n^{\Omega(1)}}$-close to a convex combination of $((\mathbf{X}, \mathbf{Y}), (\mathbf{X}, \mathbf{Y}))$ and distributions of the form $((\mathbf{X}', \mathbf{Y}'), (\eta_1(\mathbf{X}) + \nu_1(\mathbf{Y}), \eta_2(\mathbf{X}) + \nu_2(\mathbf{Y})))$, where $\mathbf{X}'$ and $\mathbf{Y}'$ are independent $(n, n - n^{\delta})$-sources and $\eta_1, \eta_2, \nu_1, \nu_2$ are deterministic functions satisfying the condition that:

- $\forall x \in support(\mathbf{X}')$ and $y \in support(\mathbf{Y}')$, $\eta_1(x) + \nu_1(y) \neq x$ or
- $\forall x \in support(\mathbf{X}')$ and $y \in support(\mathbf{Y}')$, $\eta_2(x) + \nu_2(y) \neq y$.

Theorem 6.1 is then direct from from Theorem 6.2.

Let $n_0 = n^{\delta}$. For any $y \in \{0,1\}^n$ and any function $\eta : \{0,1\}^n \to \{0,1\}^n$, let $\eta^{-1}(y)$ denote the set $\{z \in \{0,1\}^n : \eta(z) = y\}$. We partition $\{0,1\}^n$ into the following two sets:

$$\Gamma_1 = \{y \in \{0,1\}^n : |g_1^{-1}(g_1(y))| \geq 2^{n-n_0}\}, \qquad \Gamma_2 = \{0,1\}^n \setminus \Gamma_1.$$

Let $\mathbf{Y}_1$ be uniform on Γ_1 and $\mathbf{Y}_2$ be uniform on Γ_2. Clearly, $\mathbf{Y}$ is a convex combination of $\mathbf{Y}_1$ and $\mathbf{Y}_2$ with weights $w_i = |\Gamma_1|/2^n$, $i = 1, 2$. If $w_i \leq 2^{-n_0/2}$, we ignore the corresponding source and add an error of $2^{-n_0/2}$ to the extractor. Thus, suppose $w_i \geq 2^{-n_0/2}$ for $i = 1, 2$. Thus, $\mathbf{Y}_1$ and $\mathbf{Y}_2$ each have min-entropy at least $n - n_0/2$.

We claim that $g_1(\mathbf{Y}_2)$ has min-entropy at least $n_0/2$. This can be seen in the following way. For any $y \in \Gamma_2$, $|g_1^{-1}(g_1(y))| \leq 2^{n-n_0}$, and hence it follows $g_1(\mathbf{Y}_2)$ has min-entropy at least $(n - n_0/2) - (n - n_0) = n_0/2$. Thus, clearly for any $x \in \{0,1\}^n$, $x + g_1(\mathbf{Y}_2) \neq x$ with probability at least $1 - 2^{-n_0/2}$. We add a term of $2^{-n^{\Omega(1)}}$ to the error and assume that $\mathbf{X} + g_1(\mathbf{Y}_2) \neq \mathbf{X}$. Thus, $(\mathbf{X}, \mathbf{Y}_2), (f_1(\mathbf{X}) + g_1(\mathbf{Y}_2), f_1(\mathbf{X}) + g_1(\mathbf{Y}_2))$ is indeed $2^{-n^{\Omega(1)}}$close to a convex combination of distributions of the required form.

Next, we claim that for any fixing of $g_1(\mathbf{Y}_1)$, the random variable $\mathbf{Y}_1$ has min-entropy at least $n - n_0$. This is direct from the fact that for any $y \in \Gamma_2$, $|g_1^{-1}(g_1(y))| > 2^{n-n_0}$. We fix $g_1(\mathbf{Y}_1) = g$, and let $f_{1,g}(x) = f_1(x) + g$. Thus, $f_{1,g}(\mathbf{X}) = f_1(\mathbf{X}) + g_1(\mathbf{Y}_1)$. We now partition $\{0,1\}^n$ according to the fixed points of $f_{1,g}$. Let

$$\Delta_1 = \{x : f_1'(x) = x\}, \qquad \Delta_2 = \{0,1\}^n \setminus \Delta_1.$$

Let $\mathbf{X}_1$ be a flat distribution on Δ_1 and $\mathbf{X}_2$ be a flat distribution on Δ_2. If $|\Delta_1| < 2^{n-n_0/2}$, we ignore the distribution $\mathbf{X}_1$ and add an error of $2^{n-n_0/2}$ to the analyis of the non-malleable extractor. Further, it is direct from definition that $f_1(\mathbf{X}_2) + g \neq \mathbf{X}_2$. We now handle to case when $\Delta_1 > 2^{n-n_0/2}$. Note that in this case, $H_1(\mathbf{X}_1) \geq n - n_0/2$. The idea is now to partition Δ_1 into two sets based on the pre-image size of f_2 similar to the way we partioned the support of $\mathbf{Y}$ based on the pre-image size of g_1. Define the sets

$$\Delta_{11} = \{x \in \Delta_1 : |f_2^{-1}(f_2(x)) \cap \Delta_1| \geq 2^{n-n_0}\}, \qquad \Delta_{12} = \Delta_1 \setminus \Delta_{11}.$$

Let $\mathbf{X}_{11}$ be flat on Δ_{11} and $\mathbf{X}_{12}$ be flat on Δ_{12}. Clearly, $\mathbf{X}_1$ is a convex combination of the sources $\mathbf{X}_{11}$ and $\mathbf{X}_{12}$. If Δ_{11} or Δ_{12} is smaller than $2^{n-3n_0/4}$, we ignore the corresponding distribution and add an error of $2^{-n_0/4}$ to the error analysis of the non-malleable extractor. Thus suppose $\Delta_{1i} \geq 2^{n-3n_0/4}$ for $i = 1, 2$. Thus, $\mathbf{X}_{11}$ and $\mathbf{X}_{12}$ both have min-entropy at least $n - 3n_0/4$.

We claim that $f_2(\mathbf{X}_{12})$ has min-entropy at least $n_0/4$. This can be seen in the following way. For any $x \in \Delta_{12}$, $|f_2^{-1}(f_2(x)) \cap \Delta_1| \leq 2^{n-n_0}$, and hence it follows $f_2(\mathbf{X}_{12})$ has min-entropy at least $(n - 3n_0/4) - (n - n_0) = n_0/4$. Thus, clearly $f_2(\mathbf{X}_{12}) + g_2(\mathbf{Y}_1) \neq \mathbf{Y}_1$ with probability at least $1 - 2^{-n_0/4}$. As before, we add an error of $2^{-n^{\Omega(1)}}$ to the error, and assume that $f_2(\mathbf{X}_{12}) + g_2(\mathbf{Y}_1) \neq \mathbf{Y}_1$. Thus, $(\mathbf{X}_{12}, \mathbf{Y}_1), (f_1(\mathbf{X}_{12}) + g_1(\mathbf{Y}_2), f_1(\mathbf{X}_{12}) + g_1(\mathbf{Y}_2))$ is indeed $2^{-n^{\Omega(1)}}$-close to a convex combination of distributions of the required form.

Next, we claim that for any fixing of $f_2(\mathbf{X}_{11})$, the random variable $\mathbf{X}_{11}$ has min-entropy at least $n - n_0$. This is direct from the fact that for any $x \in \Delta_1$, $|f_2^{-1}(f_1(x)) \cap \Delta_1| > 2^{n-n_0}$. We fix $f_2(\mathbf{X}_{11}) = \lambda$, and let $g_{2,\lambda}(y) = \lambda + g_2(y)$. Thus, $g_{2,\lambda}(\mathbf{Y}) = f_1(\mathbf{X}) + g_1(\mathbf{Y}_1)$. We now partition Γ_1 according to the fixed points of $f_{1,g}$. Let

$$\Gamma_{11} = \{y : g_{2,\lambda}(y) = y\}, \qquad \Gamma_{12} = \{0,1\}^n \setminus \Gamma_{11}.$$

Let $\mathbf{Y}_{11}$ be a flat distribution on Γ_{11} and $\mathbf{Y}_{12}$ be a flat distribution on Γ_{12}. It follows from definition that $(f_1(\mathbf{X}_{11}) + g_1(\mathbf{Y}_{11}), f_2(\mathbf{X}_{11}) + g_2(\mathbf{Y}_{11})) = (\mathbf{X}_{11}, \mathbf{Y}_{11})$. Further, $f_2(\mathbf{X}_{11}) + g_2(\mathbf{Y}_{12}) \neq \mathbf{Y}_{12}$, and hence $(\mathbf{X}_{11}, \mathbf{Y}_{12})$ is $2^{-n^{\Omega(1)}}$-close to a convex combination of distributions of the required form. This completes the proof. □

In the rest of the section, we prove the following Theorem 6.2. We use the following notation: if $\mathbf{W} = h(\mathbf{X}, \mathbf{Y})$ (for some function h), then we use to $\mathbf{W}'$ or $(\mathbf{W})'$ to denote the random variable $h(f_1(\mathbf{X}) + g_1(\mathbf{Y}), f_2(\mathbf{X}) + g_2(\mathbf{Y}))$. In Section 6.1 we construct a new advice generator, and present the non-malleable extractor construction in Section 6.2.

6.1 A new advice generator

Lemma 6.3. *There exist a constant $C > 0$ and an efficiently computable function* advGen : $\{0,1\}^n \times \{0,1\}^n \to \{0,1\}^{n_5}$, *$n_5 = Cn^{\delta}$, such that with probability at least $1 - 2^{-n^{\Omega(1)}}$ over the fixing of the random variables* $\{\text{advGen}(\mathbf{X}, \mathbf{Y}), \text{advGen}(f_1(\mathbf{X}) + g_1(\mathbf{Y}), f_2(\mathbf{X}) + g_2(\mathbf{Y}))\}$, *the following hold:*

- $\mathrm{advGen}(\mathbf{X},\mathbf{Y}) \neq \mathrm{advGen}(f_1(\mathbf{X})+g_1(\mathbf{Y}), f_2(\mathbf{X})+g_2(\mathbf{Y}))$,
- $\mathbf{X}$ *and* $\mathbf{Y}$ *are independent,*
- $H_\infty(\mathbf{X}) \geq n - 3Cn^\delta$*,* $H_\infty(\mathbf{Y}) \geq n - 3Cn^\delta$*.*

We prove the above lemma in the rest of this subsection. We claim that the function advGen computed by Algorithm 3 satisfies the above lemma. We first set up some parameters and ingredients.

- Let $n_0 = n^\delta, n_1 = 50n_0, n_2 = 5n_0$.
- Let $\mathrm{IP}_1 : \{0,1\}^{n_1} \times \{0,1\}^{n_1} \to \{0,1\}^{n_0}$ be a two-source extractor instantiated from Theorem 3.14.
- Let $\mathrm{IP}_2 : \{0,1\}^{n_2} \times \{0,1\}^{n_2} \to \{0,1\}^{n_0}$ be a two-source extractor instantiated from Theorem 3.14.
- Let $\mathrm{LExt} : \{0,1\}^{n} \times \{0,1\}^{n_2} \to \{0,1\}^{n_0}$ be a linear seeded extractor instantiated from Theorem 3.14 set to extract from min-entropy n_2 and error $2^{\Omega(\sqrt{n_2})}$.
- Let $E : \{0,1\}^n \to \{0,1\}^{n_3}$ be the encoding function of a linear error correcting code $\mathcal{C}$ with constant rate α and constant distance β.
- Let $\mathrm{Samp} : \{0,1\}^{n_0} \to [n_3]^{n_4}$, $n_4 = n_0/\log n_3$ be a sampler that splits its input bit-string of length n_0 into $\log n_3$ sized strings and outputs the corresponding elements from $[n_3]$.

```
Algorithm 5: advGen($x, y$)
Input: Bit-string $x$ and $y$ are each $n$ bit-strings.
Output: Bit string $v$ of length $n_5 = 2n_1 + 2n_0 + 2n_4$.
Let $x_1 = \mathrm{Slice}(x, n_1), y_1 = \mathrm{Slice}(y, n_1), x_2 = \mathrm{Slice}(x, n_2), y_2 = \mathrm{Slice}(y, n_2)$.
Let $r_1 = \mathrm{IP}(x_1, y_1)$ and $r_2 = \mathrm{IP}(x_2, y_2)$.
Let $T = \mathrm{Samp}(r_1)$.
Let $w_{1,x} = (E(x))_T$ and $w_{1,y} = (E(y))_T$.
Let $w_{2,x} = \mathrm{LExt}(x, r_2)$ and $w_{2,y} = \mathrm{LExt}(y, r_2)$.
Output $v = x_1 \circ y_1 \circ x_2 \circ y_2 \circ w_{1,x} \circ w_{1,y} \circ w_{2,x} \circ w_{2,y}$.
```

Lemma 6.4. *With probability at least* $1 - 2^{-n^{\Omega(1)}}$*,* $\mathbf{V} \neq \mathbf{V}'$*.*

Proof. We prove the lemma assuming $f_1(\mathbf{X}) + g_1(\mathbf{Y}) \neq \mathbf{X}$. The proof in the other case (i.e., $f_2(\mathbf{X}) + g_2(\mathbf{Y}) \neq \mathbf{Y}$) is similar and we skip it.

The lemma is direct if either $\mathbf{X}_1 \neq \mathbf{X}'_1$ or $\mathbf{Y}_1 \neq \mathbf{Y}'_1$. Thus, assume $\mathbf{X}_1 = \mathbf{X}'_1$ and $\mathbf{Y}_1 = \mathbf{Y}'_1$. Similarly, the lemma is direct if either $\mathbf{X}_2 \neq \mathbf{X}'_2$ or $\mathbf{Y}_2 \neq \mathbf{Y}'_2$. Thus, assume $\mathbf{X}_2 = \mathbf{X}'_2$ and $\mathbf{Y}_2 = \mathbf{Y}'_2$. It follows that $\mathbf{R}_1 = \mathbf{R}'_1$, $\mathbf{R}_2 = \mathbf{R}'_2$ and hence $\mathbf{T} = \mathbf{T}'$. Since E is a linear code and LExt is a linear seeded extractor, the following hold:

$$\mathbf{W}_{1,x} - \mathbf{W}'_{1,x} = (E(\mathbf{X} - f_1(\mathbf{X}) - g_1(\mathbf{Y})))_{\mathbf{T}},$$
$$\mathbf{W}_{2,x} - \mathbf{W}'_{2,x} = \mathrm{LExt}(\mathbf{X} - f_1(\mathbf{X}) - g_1(\mathbf{Y}), \mathbf{R}_2).$$

Without loss of generality we can assume that $\mathbf{Y}$ is flat source on a set $\Gamma \subset \{0,1\}^n$, $|\Gamma| \geq 2^{n-n_0}$. We partition Γ into two sets Γ_a and Γ_b according to the pre-image size of the function g_1 in the following way. For any $y \in \{0,1\}^n$, let $g_1^{-1}(y)$ denote the set $\{z \in \{0,1\}^n : g_1(z) = y\}$.

Let $n_p = 15n_0$. Define

$$\Gamma_a = \{y \in \Gamma : |g_1^{-1}(g_1(y)) \cap \Gamma| \geq 2^{n-n_p}\}, \qquad \Gamma_b = \Gamma \setminus \Gamma_1.$$

Let $\mathbf{Y}_a$ be the flat source supported on Γ_a and $\mathbf{Y}_b$ be the flat source supported on Γ_b. Clearly $\mathbf{Y}$ is a convex combination of the distributions $\mathbf{Y}_a$ and $\mathbf{Y}_b$, with weights $w_a = |\Gamma_a|/|\Gamma|$ and $w_a = |\Gamma_a|/|\Gamma|$. If any of w_a or w_b is less that 2^{-n_e}, we ignore the corresponding source and add it to the error. Thus suppose both w_a and w_b are at least 2^{-n_0}. This implies that both $\mathbf{Y}_a$ and $\mathbf{Y}_b$ have min-entropy at least $n - 2n_0$.

We introduce some notation. For any random variable $\nu = \eta(\mathbf{X}, \mathbf{Y})$ (where η is an arbitrary deterministic function), we add an extra a or b to the subscript and use ν_a and ν_b to denote the random variable $\eta(\mathbf{X}, \mathbf{Y}_a)$ and ν_b to denote the random variables $\eta(\mathbf{X}, \mathbf{Y}_b)$ $\eta(\mathbf{X}, \mathbf{Y}_b)$ respectively. For example, we use $\mathbf{W}'_{1,x,a}$ to denote the random variable $E(f_1(\mathbf{X}) + g_1(\mathbf{Y}_a))_{\mathbf{T}'_a}$, where $\mathbf{T}'_a = \text{Samp}(\mathbf{R}_a)'$, and $\mathbf{R}_a = \text{IP}(\mathbf{X}, g_1(\mathbf{Y}_a))$.

We prove the following two statements:

1. $\mathbf{W}_{1,x,a} - \mathbf{W}'_{1,x,a} \neq 0$ with probability $1 - 2^{-n^{\Omega(1)}}$.

2. $\mathbf{W}_{2,x,b} - \mathbf{W}'_{2,x,b} \neq 0$ with probability $1 - 2^{-n^{\Omega(1)}}$.

It is direct that the lemma follows from the above two estimates.

We begin with the proof of (1). Consider any fixing of $g_1(\mathbf{Y}_a) = g$. By definition of $\mathbf{Y}_a$, it follows that there are at least 2^{n-n_p} strings in the support of $\mathbf{Y}_a$ such that g_1 maps each of these strings to g. Thus, it follows that after this conditioning, $\mathbf{Y}_a$ has min-entropy at least $n - n_p$. Let $\mathbf{Y}_a = \mathbf{Y}_{1,a} \circ \overline{\mathbf{Y}_{1,a}}$, i.e., $\overline{\mathbf{Y}_{1,a}}$ is the remaining bits of $\mathbf{Y}_a$ after slicing off $\mathbf{Y}_{1,a}$. Since the length of $\overline{\mathbf{Y}_{1,a}}$ is $n - n_1$, it follows that $\mathbf{Y}_{1,a}$ has min-entropy at least $(n-n_p)-(n-n_1) = n_1 - n_p = 35n_0 = 7n_1/10$. Further, $\mathbf{X}_1$ has min-entropy at least $n - n_0 - (n - n_1) = n_1 - n_0 = 49n_1/50$. It follows by Theorem 3.14 that $\mathbf{R}_a = \text{IP}(\mathbf{X}_1, \mathbf{Y}_{1,a})$ is $2^{-n^{\Omega(1)}}$-close to uniform even conditioned on $\mathbf{X}_1$. We fix $\mathbf{X}_1$ and $\mathbf{X} - f_1(\mathbf{X})$. It follows that $\mathbf{X} - f_1(\mathbf{X}) - g_1\mathbf{Y}_a$ is now a fixed non-zero string, and hence $E(\mathbf{X} - f_1(\mathbf{X}) - g_1\mathbf{Y}_a)$ has 1's in at least β fraction of its coordinates. Since $\mathbf{R}_a$ is uniform, it follows that with probability at least $1 - 2^{-n^{\Omega(1)}}$, $(\mathbf{W}_{1,x,a} - \mathbf{W}_{1,x,a})_{\mathbf{T}_a}$ is not the all zero string. Thus, $\mathbf{W}_{1,x,a} - \mathbf{W}'_{1,x,a} \neq 0$ with probability $1 - 2^{-n^{\Omega(1)}}$.

We now prove (2). Note that by definition, for any $y_b \in \mathbf{Y}_b$, $|g_1^{-1}(g_1(Y_b))| \leq 2^{n-n_p}$. Since $\mathbf{Y}_b$ has min-entropy at least $n - 2n_0$, it follows that $g_1(\mathbf{Y}_b)$ has min-entropy at least $n - 2n_0 - (n - n_p) = n_p - 2n_0 = 13n_0$. Next, note that $\mathbf{Y}_{2,b}$ has min-entropy at least $(n - 2n_0) - (n - n_2) = n_2 - 2n_0 = 3n_2/5$ and $\mathbf{X}_{2,b}$ has min-entropy at least $(n - n_0) - (n - n_2) = 4n_2/5$. Fix $\mathbf{Y}_{2,b}$, and it follows by Theorem 3.14 that $\mathbf{R}_{2,b}$ is $2^{-n^{\Omega(1)}}$-close to uniform and is a deterministic function of $\mathbf{X}$. Now, $g_1(\mathbf{Y}_b)$ has min-entropy at least $13n_0 - n_2 - n_0 = 7n_0 > n_2$ with probability at least $1 - 2^{-n^{\Omega(1)}}$. It follows by our choice of parameters that $\text{LExt}(g_1(\mathbf{Y}_b), \mathbf{R}_{2,b})$ is $2^{-n^{\Omega(1)}}$-close to uniform. We fix $\mathbf{R}_{2,b}$, and thus $\text{LExt}(g_1(\mathbf{Y}_b), \mathbf{R}_{2,b})$ is now a deterministic function of $\mathbf{Y}$. Further, $\text{LExt}(\mathbf{X} - f_1(\mathbf{X}), \mathbf{R}_{2,b})$ is now a deterministic function of $\mathbf{X}$, and we fix it. Note that this does not affect the distribution of $\text{LExt}(g_1(\mathbf{Y}_b), \mathbf{R}_{2,b})$. It follows that $\mathbf{W}_{2,x,b} - \mathbf{W}_{2,x,b} = \text{LExt}(g_1(\mathbf{Y}_b), \mathbf{R}_{2,b}) + \text{LExt}(\mathbf{X} - f_1(\mathbf{X}), \mathbf{R}_{2,b})$ is close to uniform, and hence $\mathbf{W}_{2,x,b} - \mathbf{W}'_{2,x,b} \neq 0$ with probability $1 - 2^{-n^{\Omega(1)}}$. This completes the proof. □

The proof of Lemma 6.3 is now direct from the construction in the following way: Fix $\mathbf{X}_1$, $\mathbf{Y}_1, \text{Slice}(f_1(\mathbf{X}), n_1), \text{Slice}(f_2(\mathbf{X}), n_1), \text{Slice}(g_1(\mathbf{Y}), n_1), \text{Slice}(g_2(\mathbf{Y}), n_1)$. Note that this fixes $\mathbf{T}, \mathbf{T}'$, $\mathbf{R}_2, \mathbf{R}_2'$. Further fix the random variables $E(\mathbf{X})_T, E(\mathbf{Y})_T, E(f_1(\mathbf{X}))_{T'}, E(f_2(\mathbf{X}))_{T'}, E(g_1(\mathbf{Y}))_{T'}$, $E(f_2(\mathbf{Y}))_{T'}$. This clearly fixes $\mathbf{V}, \mathbf{V}'$ and we have maintained that $\mathbf{X}$ and $\mathbf{Y}$ are still independent sources. Further, it can be verified that with probability at least $1 - 2^{-n^{\Omega(1)}}$, $\mathbf{X}$ and $\mathbf{Y}$ each have min-entropy at least $n - 200n_0$.

6.2 The extractor construction

We are now ready to present the construction of iℓNM that satisfies the requirements of Theorem 5.2. We first set up some parameters and ingredients. We are now ready to present the construction of iℓNM that satisfies the requirements of Theorem 5.2. We first set up some parameters and ingredients.

- Let $\delta > 0$ be a small enough constant.
- Let $\text{advGen} : \{0,1\}^{2n} \to \{0,1\}^{n_1}$ be the advice generator from Lemma 6.3. Thus $n_1 = O(n^{\delta})$.
- Let $\text{ACB} : \{0,1\}^{n_{acb}} \times \{0,1\}^{n_{acb}} \times \{0,1\}^{h_{acb}} \to \{0,1\}^{n_{1,acb}}$ be the advice correlation breaker from Theorem 4.2 set with the following parameters: $n_{acb} = n, n_{1,acb} = m = n^{\delta_2}$, for some small enough $\delta_2 > 0$, $h_{acb} = n_1, \epsilon_{acb} = 2^{-n^{2\delta}}$, $d_{acb} = O(\log^2(n/\epsilon_{acb}))$, and $\lambda_{acb} = Cn^{\delta}$ for some large constant C.

```
Algorithm 6: nmExt($x, y$)
Input: Bit-strings $x, y$ each of length $n$,
Output: Bit string $v$ of length $m$.

Let $w = \text{advGen}(x, y)$.
Output $v = \text{ACB}(x, y, w)$.
```

We prove that nmExt computed by Algorithm 6 is the required construction for Theorem 6.2. The proof is almost direct. By Lemma 6.3, it follows that $\mathbf{W} \neq \mathbf{W}'$ with probability at least $1 - 2^{-n^{\Omega(1)}}$. Further, fixing $\mathbf{W}, \mathbf{W}'$, we are guaranteed that $\mathbf{X}$ and $\mathbf{Y}$ remain independent sources, each with min-entropy at least $n - O(n^{\delta})$. Using Theorem 4.2, it now follows that $|\mathbf{V}, \mathbf{V}' - \mathbf{U}_m, \mathbf{V}'| \leq 2^{-n^{\Omega(1)}}$ which completes the proof.

7 Non-malleable extractors for split-state adversaries with bounded communication

Let $\mathcal{F}_{n,t,\ell} \subset \mathcal{F}_{2n}$ be the set of all functions that can be computed by such a communication protocol with parameters t, ℓ. The following is our main result.

Theorem 7.1. *There exists a constant $\delta > 0$ such that for all integers $n, t, \ell > 0$ with $t \cdot \ell \leq \delta n$, there exists an efficiently computable function* nmExt $: \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^m$, $m = \Omega(n)$, *such that the following holds: let $\mathbf{X}$ and $\mathbf{Y}$ be uniform independent sources each on n bits, and let $h_{t,\ell}$ be an arbitrary tampering function in $\mathcal{F}_{n,t,\ell}$. Then, there exists a distribution $\mathcal{D}_h$ on $\{0,1\}^m \cup \{same^{\star}\}$ that is independent of $\mathbf{X}$ and $\mathbf{Y}$ such that*

$$|\text{nmExt}(\mathbf{X}, \mathbf{Y}), \text{nmExt}(h_{t,\ell}(\mathbf{X}, \mathbf{Y})) - \mathbf{U}_m, \text{copy}(\mathcal{D}_h, \mathbf{U}_m)| \leq 2^{-n \log\log n / \log n}.$$

Further, nmExt *is* $2^{-n\log\log n/\log n}$*-invertible.*

Proof. We show that any 2-source non-malleable extractor that works for min-entropy $n-2\delta n$ can be used as the required non-malleable extractor in the above theorem. The tampering function $h_{t,\ell}$ that is based on the communication protocol can be phrased in terms of functions in the following way: there exist deterministic functions $f_i : \{0,1\}^n \times \{0,1\}^{(2i-2)t} \to \{0,1\}^t$ and $g_i : \{0,1\}^n \times \{0,1\}^{(2i-1)t} \to \{0,1\}^t$ for $i = 1,\ldots,\ell$, and $f : \{0,1\}^n \times \{0,1\}^{2\ell t} \to \{0,1\}^n$ and $g : \{0,1\}^n \times \{0,1\}^{2\ell t} \to \{0,1\}^n$ such that the communication protocol between Alice and Bob corresponds to computing the following random variables: $\mathbf{S}_1 = f_1(\mathbf{X}), \mathbf{R}_1 = g_1(\mathbf{Y},\mathbf{S}_1), \mathbf{S}_2 = f_2(\mathbf{X},\mathbf{S}_1,\mathbf{R}_1),\ldots,$ $\mathbf{S}_i = f_i(\mathbf{X},\mathbf{S}_1,\ldots,\mathbf{S}_{i-1},\mathbf{R}_1,\ldots,\mathbf{R}_{i-1}), \mathbf{R}_i = g_i(\mathbf{Y},\mathbf{S}_1,\ldots,\mathbf{S}_i,\mathbf{R}_{i,},\ldots,\mathbf{R}_{i-1}),\ldots,\mathbf{R}_\ell = g_\ell(\mathbf{Y},\mathbf{S}_1,$ $\ldots,\mathbf{S}_\ell,\mathbf{R}_1,\ldots,\mathbf{R}_{\ell-1})$.

Finally, $\mathbf{X}' = f(\mathbf{X},\mathbf{R}_1,\ldots,\mathbf{R}_\ell,\mathbf{S}_1,\ldots,\mathbf{S}_\ell)$ and $\mathbf{Y}' = g(\mathbf{Y},\mathbf{R}_1,\ldots,\mathbf{R}_\ell,\mathbf{S}_1,\ldots,\mathbf{S}_\ell)$ correspond to the output of Alice and the output of Bob respectively. Thus, $h_{t,\ell}(\mathbf{X},\mathbf{Y}) = (\mathbf{X}',\mathbf{Y}')$.

Similar to the way we argue about alternating extraction protocols, we fix random variables as follows: Fix $\mathbf{S}_1$, and it follows that $\mathbf{R}_1$ is now a deterministic function of $\mathbf{Y}$. We fix $\mathbf{R}_1$, and thus $\mathbf{S}_2$ is now a deterministic function of $\mathbf{X}$. Thus, continuing in this we way, we fix all the random variables $\mathbf{S}_1,\ldots,\mathbf{S}_\ell$ and $\mathbf{R}_1,\ldots,\mathbf{R}_\ell$ while maintaining that $\mathbf{X}$ and $\mathbf{Y}$ remain independent sources. Further, invoking Lemma 3.1, with probability at least $1-2^{-\Omega(n)}$, both $\mathbf{X}$ and $\mathbf{Y}$ have min-entropy at least $n-\ell\cdot t-\delta n \geq n-2\delta n$.

Note that now, $\mathbf{X}' = \eta(\mathbf{X})$ for some deterministic function η and $\mathbf{Y}' = \nu(\mathbf{X})$ for some deterministic function ν. Thus, for any 2-source non-malleable extractor nmExt that works for min-entropy $n-2\delta n$ with error ϵ, we have that there exists a distribution $\mathcal{D}_{\eta,\nu}$ over $\{0,1\}^m \cup \{\mathit{same}^\star\}$ that is independent of $\mathbf{X}$ and $\mathbf{Y}$ such that

$$|\mathrm{nmExt}(\mathbf{X},\mathbf{Y}), \mathrm{nmExt}(\eta(\mathbf{X}),\nu(\mathbf{Y})) - \mathbf{U}_m, \mathrm{copy}(\mathcal{D}_{\eta,\nu},\mathbf{U}_m)| \leq \epsilon.$$

The theorem now follows by plugging in such a construction from a recent work of Li ([Li18], Theorem 1.12). We note the non-malleable construction in [Li18] is indeed $2^{-n\log\log n/\log n}$-invertible. □

8 Efficient sampling algorithms

In this section, we provide efficient sampling algorithms for the seedless non-malleable extractor constructions presented in Section 5 and Section 6. This is crucial to get efficient encoding algorithms for the corresponding non-malleable codes. We do not know how to invert the non-malleable extractor constructions in Theorem 5.1 and Theorem 6.1, but we show that the constructions can suitably modified in a way that admits efficient sampling from the pre-image of the extractor.

8.1 An invertible non-malleable extractor with respect to interleaved adversaries

The main idea is to ensure that on fixing appropriate random variables that are generated in computing the non-malleable extractor, the source is now restricted onto a known subspace of fixed dimension (i.e., the dimension does not depend on value of the fixed random variables). Once we can ensure this, sampling from the pre-image can simply be done by first uniformly sampling the fixed random variables, and then sampling the other variables uniformly from the known subspace. To carry this out, we need an efficient construction of a linear seeded extractor that has the property that for any fixing of the seed the linear map corresponding linear seeded extractor has the same rank. Such a linear seeded extractor was constructed in prior works [CGL16, Li17] (see Theorem 3.12).

We now set up some parameters and ingredients for our construction of an invertible non-malleable extractor.

- Let $\delta > 0$ be a small enough constant and C a large constant.
- Let $n_1 = n^{\delta}, n_2 = n^{C\delta}, n_3 = n^{C^2\delta}/5, n_4 = n^{C^3\delta}, n_5 = n - \sum_{i=1}^{4} n_i$. We ensure that $n_5 \geq 3n/2$.
- Let $\mathbb{F}$ be the finite field $\mathbb{F}_{2^{\log(n+1)}}$. Let $n_7 = (2n - n_1)/\log(n+1)$. Let $\mathrm{RS} : \mathbb{F}^{n_4} \to \mathbb{F}^n$ be the Reed-Solomon code encoding n_7 symbols of $\mathbb{F}$ to n symbols in $\mathbb{F}$, where we use RS to denote the code as well as the encoder. Thus, RS is a $[n, n_7, n - n_7 + 1]_n$ error correcting code.
- Let $\mathrm{Ext}_1 : \{0,1\}^{n_1} \times \{0,1\}^{d_1} \to \{0,1\}^{\log n}$ be a $(n_1/8, \beta_1/10)$-seeded extractor instantiated using Theorem 3.9. Thus $d_1 = C_1 \log n_1$, for some constant C_1.
- Let $\mathrm{Samp}_1 : \{0,1\}^{n_1} \to [n]^{n_8}$ be the sampler obtained from Theorem 3.8 using Ext_1. Thus $n_8 = 2^{d_1} = n^{C_1\delta}$. Let $\delta_1 = C_1\delta$.
- Let $\mathrm{Ext}_2 : \{0,1\}^{n_3} \times \{0,1\}^{d_2} \to \{0,1\}^{\log(n_5)}$ be a $(n_3/8, 1/100)$-seeded extractor instantiated using Theorem 3.9. Thus $d_1 = C_1 \log n_3$.
- Let $\mathrm{Samp}_2 : \{0,1\}^{n_3} \to [n_5]^{n_9}$ be the sampler obtained from Theorem 3.8 using Ext_2. Thus $n_9 = 2^{d_2} = n_3^{C_1} = n^{C_1 C^2 \delta}$. Let $\delta_2 = C_1 C^2 \delta$.
- Let $\mathrm{Ext}_3 : \{0,1\}^{n_4} \times \{0,1\}^{d_3} \to \{0,1\}^{n_5 - n_9}$ be a $(n_4/8, 1/100)$-seeded extractor instantiated using Theorem 3.9. Thus $d_3 = C_1 \log n_4$.
- Let $\mathrm{Samp}_3 : \{0,1\}^{n_4} \to [n_5 - n_9]^{n_{10}}$ be the sampler obtained from Theorem 3.8 using Ext_3. Thus $n_{10} = 2^{d_3} = n_4^{C_1} = n^{C_1 C^3 \delta}$. Let $\delta_3 = C_1 C^3 \delta$.
- Let $\mathrm{LExt}_1 : \{0,1\}^{n_2} \times \{0,1\}^{d} \to \{0,1\}^{d_4}$, $d_4 = \sqrt{n_2}$, be a linear-seeded extractor instantiated from Theorem 3.10 set to extract from entropy $k_1 = n_2/10$ with error $\epsilon_1 = 1/10$. Thus $d = C_2 \log n_2$, for some constant C_2. Let $D = 2^d = n^{\delta_4}$, $\delta_4 = 2C_2 C\delta$.
- Let $\mathrm{LExt}_2 : \{0,1\}^{n_9} \times \{0,1\}^{d_4} \to \{0,1\}^{m_1}$, $m_1 = n^{8\delta_4}$ be a linear-seeded extractor instantiated from Theorem 3.10 set to extract from entropy $k_2 = n_9/100$ with error $\epsilon_2 = 2^{-\Omega(\sqrt{d_4})} = 2^{-n^{\Omega(1)}}$, such that the seed length of the extractor LExt_2 (by Theorem 3.10) is d_4.
- Let $\mathrm{ACB} : \{0,1\}^{n_{1,acb}} \times \{0,1\}^{n_{acb}} \times \{0,1\}^{h_{acb}} \to \{0,1\}^{n_{2,acb}}$, be the advice correlation breaker from Theorem 4.1 set with the following parameters: $n_{acb} = n_9, n_{1,acb} = m_1, n_{2,acb} = n_{11} = O(n^{2\delta_4}), t_{acb} = 2D, h_{acb} = n_1 + d, \epsilon_{acb} = 2^{-n^{\delta_1}}$, $d_{acb} = O(\log^2(n/\epsilon_{acb})), \lambda_{acb} = 0$. It can be checked that by our choice of parameters, the conditions required for Theorem 4.1 indeed hold for $k_{1,acb} \geq n^{2\delta_4}$.
- Let $\mathrm{LExt}_3 : \{0,1\}^{n_{10}} \times \{0,1\}^{n_{11}} \to \{0,1\}^{m}$ be the linear seeded extractor from Theorem 3.12 set to extract from min-entropy rate 0.1 and error $\epsilon = 2^{-\Omega(n_{11})}$ (such that the seed-length is indeed m). Thus, $m = \alpha n_{11}$, for some small contant α that arises out of Theorem 3.12.

Algorithm 7: iℓNM(z)

Input: Bit-string $z = (x \circ y)_\pi$ of length $2n$, where x and y are each n bit-strings, and $\pi : [2n] \to [2n]$ is a permutation.
Output: Bit string of length m.

```
Let $z_i = z_1 \circ z_2 \circ z_3 \circ z_4 \circ z_5$, where $z_i$ is of length $n_i$.
Let $T_1 = \mathrm{Samp}_1(z_1)$.
Let $w = z_1 \circ (\mathrm{RS}(z_2 \circ z_3 \circ z_4 \circ z_5))_{T_1}$.
Let $v$ be a $D \times d_4$ matrix, with its $i$'th row $v_i = \mathrm{LExt}_1(z_2, i)$.
Let $T_2 = \mathrm{Samp}_2(z_3)$ and $T_3 = \mathrm{Samp}_3(z_4)$.
Let $\overline{z_3} = (z_5)_{T_2}$
Let $r$ be a $D \times n_4$ matrix, with its $i$'th row $r_i = \mathrm{LExt}_2(\overline{z_3}, v_i)$.
Let $s$ be a $D \times m$ matrix, with its $i$'th row $s_i = \mathrm{ACB}(r_i, \overline{z_3}, w \circ i)$.
Let $\tilde{s} = \oplus_{i=1}^{D} s_i$.
Let $z_6$ be the bits in $z_5$ outside $T_2$.
Let $\overline{z_6} = (z_6)_{T_3}$
Output $g = \mathrm{LExt}_3(\overline{z_6}, \tilde{s})$.
```

Theorem 8.1. *There exists a small constant $\delta > 0$ such that for all positive integers n, k with $n \geq k \geq n - n^\delta$, the function* i$\ell$NM $: \{0,1\}^{2n} \to \{0,1\}^m$*, computed by Algorithm 7 has the following property: Let $\mathbf{X}$ and $\mathbf{Y}$ be independent (n,k)-sources, and let $\mathbf{Z} = (\mathbf{X} \circ \mathbf{Y})_\pi$ be an interleaving of $\mathbf{X}$ and $\mathbf{Y}$, where $\pi : [2n] \to [2n]$ is permutation. Let $f : \{0,1\}^n \to \{0,1\}^n$ and $g : \{0,1\}^n \to \{0,1\}^n$ be arbitrary functions such that at least one of f and g does not have any fixed points. Then,*

$$|\mathrm{i\ell NM}((\mathbf{X} \circ \mathbf{Y})_\pi), \mathrm{i\ell NM}((f(\mathbf{X}) \circ g(\mathbf{Y}))_\pi) - \mathbf{U}_m, \mathrm{i\ell NM}((f(\mathbf{X}) \circ g(\mathbf{Y}))_\pi)| \leq 2^{-n^{\Omega(1)}}.$$

The proof of the above theorem is very similar to the proof of Theorem 5.2, and we omit the details and include a brief discussion on the differences from the construction given in Algorithm 4. One differences is that in the steps where we transform the somewhere random matrix v into a matrix with longer rows, and the subsequent step where the advice correlation breaker is applied is now done using a pseudorandomly sampled subset of coordinates from $\mathbf{Z}$ (as opposed to the entire $\mathbf{Z}$ which we did before). It is not hard to prove that this does not make a difference as long as we sample enough bits. The other difference is the final step where we use a linear seeded extractor, with $\overline{\mathbf{Z}_6}$ as the seed. As done many times in the paper, we use the sum structure of $\overline{\mathbf{Z}_6}$ (into a source that depends on $\mathbf{X}$ and a source that depends on $\mathbf{Y}$) along with the fact that LExt_3 is linear seeded to show that the output is close to uniform.

We now focus on the problem of efficiently sampling from the pre-image of this extractor. The following lemma almost immediately implies a simple sampling algorithm.

Lemma 8.2. *For any fixing of the variables $z_1, z_2, z_3, \overline{z_3}, z_4, w, g$, the set $nmExt^{-1}(g)$ is a linear subspace of fixed dimension.*

Proof. We note that fixing z_1, z_2 fixes v. Further, fixing z_3 fixes T_3 and subsequently fixing z_4 fixes T_4. Next, we fix the remaining part of w and also $\overline{z3}$. Thus, we can now compute $\tilde{s}$. Next, we sample $\overline{z_6}$ uniformly from the set $(\mathrm{LExt}_3(\cdot, \tilde{s}))^{-1}(g)$. Note that this can be done efficiently by Theorem 3.12, and further the dimension of the sub-space from which $\overline{z_6}$ is sampled does not depend on the value of $\tilde{s}$. Finally, we are left to sample the bits in z_5 not indexed by T_3. Let z_7 denote this string. Note that by our choice of parameters the length of z_7 is at least n. We think of z_7 to be in $\mathbb{F}$. Thus, there are at least $n/\log(n+1)$ free variables. The number of linear constraints imposed on the bits of z_7 by fixing w is n_8 which is much smaller than the number of $n/\log(n+1)$. Further, note that the number of linear constraints is exactly equal to the number of variables sampled from z_6 (and does not depend on the values of the fixed variables). This follows from the fact that the generator matrix of the RS code is a Vandermonde matrix, and hence any subset of columns are linearly independent. This completes the proof. $\square$

Given Lemma 8.2, the sampling algorithm is now straightforward:
Input $g \in \{0,1\}^m$; Output z that is uniform on the set $\mathrm{i}\ell\mathrm{NM}^{-1}(g)$.

1. Sample z_1, z_2, z_3, z_4, w uniformly at random.
2. Compute $\tilde{s}$ using Algorithm 7.
3. Sample z_5 uniformly from $(\mathrm{LExt}(\cdot, \tilde{s}))^{-1}(g)$.
4. Sample z_6 as discussed in Lemma 8.2.
5. Output $z = z_1 \circ z_2 \circ z_3 \circ z_4 \circ z_5 \circ z_6$.

8.2 An invertible non-malleable extractor with respect to linear composed with split-state adversaries

The modifications to the non-malleable extractor we make in this section is similar to the ones made in the previous section. One additional care we need to take is the choice of the error correcting code we use in the advice generator construction. We ensure that the linear constraints imposed by fixing the advice string does not depend on the value of the advice string. This is more subtle than before since the advice generator now comprises of a sample from an error correction of the sources as well as the output of the a linear seeded extractor on the sources. The basic idea is to remove a few sampled coordinates of the error corrected sources and show that this suffices to remove any linear dependencies. Let $L : \{0,1\}^r \to \{0,1\}^s$ be a linear map given by $L(\alpha) = M\alpha$ for some matrix M. We use con_L to denote a maximal set of linearly independent rows of M. We first set up some parameters and ingredients.

- Let $\delta > 0$ be a small enough constant.
- Let $n_0 = n^{\delta}, n_1 = 50n_0, n_2 = 5n_0, n_3 = \sqrt{n}, n_4 = n^{3/4}$. Let $n_5 = n - \sum_{i=1}^{4} n_i$. Thus, $n_5 > 9n/10$.
- Let $\mathrm{IP}_1 : \{0,1\}^{n_1} \times \{0,1\}^{n_1} \to \{0,1\}^{n_0}$ be a two-source extractor instantiated from Theorem 3.14.
- Let $\mathrm{IP}_2 : \{0,1\}^{n_2} \times \{0,1\}^{n_2} \to \{0,1\}^{n_0}$ be a two-source extractor instantiated from Theorem 3.14.
- Let $\mathrm{LExt} : \{0,1\}^n \times \{0,1\}^{n_2} \to \{0,1\}^{\sqrt{n_0}}$ be a linear seeded extractor instantiated from Theorem 3.14 set to extract from min-entropy n_2 and error $2^{\Omega(\sqrt{n_2})}$.
- Let $\mathcal{C}$ be a BCH code with parameters: $[n_b, n_b - t_b \log n_b, 2t_b]_2$, $t_b = \sqrt{n_b}/100$, where we fix n_b in the following way. Let dBCH be the dual code. From standard literature, it follows that dBCH is a $[n_b, t_b \log n_b, \frac{n_b}{2} - t_b\sqrt{n_b}]_2$-code. Set n_b such that $t_b \cdot \log n_b = \sqrt{n_b} \log n_b = n$. Let E be the encoder of dBCH.

- Let $\text{Samp} : \{0,1\}^{n_0} \to [n_b]^{n_7}$, $n_7 = n_0/\log n_b$ be a sampler that splits its input bit-string of length n_0 into $\log n_b$ sized strings and outputs the corresponding elements from $[n_b]$.
- Let $\text{ACB} : \{0,1\}^{n_{acb}} \times \{0,1\}^{n_{acb}} \times \{0,1\}^{h_{acb}} \to \{0,1\}^{n_{1,acb}}$ be the advice correlation breaker from Theorem 4.2 set with the following parameters: $n_{acb} = n_3, n_{1,acb} = n_8 = n^{\delta_2}$, for some small enough $\delta_2 > 0$, $h_{acb} = n_1, \epsilon_{acb} = 2^{-n^{2\delta}}$, $d_{acb} = O(\log^2(n/\epsilon_{acb}))$, and $\lambda_{acb} = Cn^{\delta}$ for some large constant C.
- Let $\text{LExt}_1 : \{0,1\}^{n_4} \times \{0,1\}^{n_8} \to \{0,1\}^m$ be the linear seeded extractor from Theorem 3.12 set to extract from min-entropy rate 0.1 and error $\epsilon = 2^{-\Omega(n_8)}$ (such that the seed-length is indeed m). Thus, $m = \alpha n_8$, for some small contant α that arises out of Theorem 3.12.

```
Algorithm 8: nmExt(x, y)
Input: Bit-strings $x, y$ each of length $n$,
Output: Bit string $v$ of length $m$.
1  Let $x = x_1 \circ x_2 \circ x_3 \circ x_4 \circ x_5$, where $z_i$ is of length $n_i$.
2  Let $y = y_1 \circ y_2 \circ y_3 \circ y_4 \circ y_5$, where $z_i$ is of length $n_i$.
3  Let $r_1 = \text{IP}(x_1, y_1)$ and $r_2 = \text{IP}(x_2, y_2)$.
4  Let $T = \text{Samp}(r_1)$.
5  Let $g_1(x) = \text{LExt}(x, r_2)$ and $g_2(y) = \text{LExt}(y, r_2)$.
6  For any set $Q$, define $E_Q(x) = (E(x))_Q$ and $E_Q(y) = (E(y))_Q$.
7  Pick a subset $\overline{T} \subset T$ of size $n_7 - 2\sqrt{n_0}$ such that $con_{\overline{T}}$ is linearly independent of
   $con_{g_1} \cup con_{g_2}$. If there is no such set $\overline{T}$, then output $0^m$.
8  Let $w_{1,x} = (E(x))_{\overline{T}}$ and $w_{1,y} = (E(y))_{\overline{T}}$.
9  Let $w_{2,x} = g_1(x)$ and $w_{2,y} = g_2(y)$.
10 Let $v = x_1 \circ y_1 \circ x_2 \circ y_2 \circ w_{1,x} \circ w_{1,y} \circ w_{2,x} \circ w_{2,y}$.
11 Let $z = \text{ACB}(x_3, y_3, v)$.
12 Output $\tilde{z} = \text{LExt}_1(x_4, z)$.
```

The existence of the subset $\overline{T}$ is guaranteed by the fact that E has dual distance $t_b = \Omega(n/\log n)$. Thus, any Con_T is a set of size $|T| = n_7$. Further, $\text{Con}_{g_1} \cup \text{Con}_{g_2}$ is a set with cardinality at most $2\sqrt{n_0}$. Thus, indeed there exists such a set $\overline{T}$. Following the proof of Theorem 6.1, it is now direct to show that the function nmExt computed by Algorithm 8 indeed satisfies the conclusion of Theorem 6.1. An important detial to notice is that $|T \setminus \overline{T}| = 2\sqrt{n_0} = o(n_7)$ and the distance of the code computed by E is $\Omega(1)$. Thus, the fact that we discard the bits indexed by the set $T \setminus \overline{T}$ from the encoded $\mathbf{X}$ and $\mathbf{Y}$ (and thus the output of the advice generator) does not affect the proof. The rest of the proof is straightforward and we omit the details.

We now focus on the problem of efficiently sampling from the pre-image of this extractor. The following lemma almost immediately implies a simple sampling algorithm.

Lemma 8.3. *With probability at least $1 - 2^{-n^{\Omega(1)}}$ over uniformly randomly fixing $x_1, x_2, x_3, y_1, y_2, y_3, y_4, w_{1,x}, w_{1,y}, w_{2,x}, w_{2,y}$, the set $nmExt^{-1}(\tilde{z}) \subset \{0,1\}^{2n}$ is a linear subspace of fixed dimension.*

Proof. Fix x_1, y_1 and x_2, y_2. Note that this fixes r_1, r_2 and the set T. Now fix $w_{2,x}$ and $w_2(y)$. Note that by Lemma 3.13, with probability at least $1 - 2^{-n^{\Omega(1)}}$, con_{g_1} and con_{g_2} are each sets of cardinality exactly $\sqrt{n_0}$. Next fix $w_{2,x}$ and $w_{2,y}$ and a subset $\overline{T} \subset T$ satisfying Step (7) of Algorithm 8. Fix the variables x_3, y_3 and compute z using Algorithm 8. Next, sample x_4 uniformly from the set $(\mathrm{LExt}_1(\cdot, z))^{-1}(\tilde{z})$. Note that this can be done efficiently by Theorem 3.12, and further the dimension of the sub-space from which x_4 is sampled does not depend on the variables fixed so far. Now, we are left with sampling x_5, y_4, y_5. Note that (with probability $1 - 2^{-n^{\Omega(1)}}$) the number of linearly independent constraints imposed on x_5 is exactly $\sqrt{n_0} + n_7 - 2\sqrt{n_0} = n_7 - \sqrt{n_0}$, and the number of linearly independent constraints imposed on $y_4 \circ y_5$ is also $n_7 - \sqrt{n_0}$. Thus, we sample x_5 and $y_4 \circ y_5$ from the appropriate subspaces noting that the number of constraints $n_7 - \sqrt{n_0}$ is much smaller than the lengths of x_5 and $y_4 \circ y_5$. It is clear from the argument that with probability at least $1 - 2^{-n^{\Omega(1)}}$, the dimension of sub-space from which $x \circ y$ is sampled does not depend on the values of $x_1, x_2, x_3, y_1, y_2, y_3, y_4, w_{1,x}, w_{1,y}, w_{2,x}, w_{2,y}$. □

Given Lemma 8.3, the sampling algorithm is now straightforward:

Input $\tilde{z} \in \{0,1\}^m$; Output x, y that is uniform on the set $\mathrm{nmExt}^{-1}(\tilde{z})$.

1. Sample $x_1, x_2, x_3, y_1, y_2, y_3, y_4, w_{1,x}, w_{1,y}, w_{2,x}, w_{2,y}$ uniformly at random.
2. Compute z using Algorithm 8.
3. Sample x_4 uniformly from $(\mathrm{LExt}(\cdot, z))^{-1}(\tilde{z})$.
4. Pick an appropriate set $\overline{T}$ and sample x_5, y_4, y_5 as discussed in Lemma 8.3.
5. Output $x = x_1 \circ x_2 \circ x_3 \circ x_4 \circ x_5, y = y_1 \circ y_2 \circ y_3 \circ y_4 \circ y_5$.

9 Extractors for interleaved sources

Our techniques yield improved explicit constructions of extractors for interleaved sources. Our extractor works when both sources have entropy at least $2n/3$, and outputs $\Omega(n)$ bits that are $2^{-n^{\Omega(1)}}$-close to uniform.

The following is our main result.

Theorem 9.1. *For any constant $\delta > 0$ and all integers $n > 0$, there exists an efficiently computable function $\mathrm{i}\ell\mathrm{Ext} : \{0,1\}^{2n} \to \{0,1\}^m$, $m = \Omega(n)$, such that for any two independent sources $\mathbf{X}$ and $\mathbf{Y}$, each on n bits with min-entropy at least $(2/3 + \delta)n$, and any permutation $\pi : [2n] \to [2n]$, we have*

$$|\mathrm{i}\ell\mathrm{Ext}((\mathbf{X} \circ \mathbf{Y})_\pi) - \mathbf{U}_m| \le 2^{-n^{\Omega(1)}}.$$

We use the rest of the section to prove Theorem 9.1. An important ingredient in our construction is an explicit somewhere condenser for high-entropy sources constructed in the works of Barak et al. [BRSW12] and Zuckerman [Zuc07].

Theorem 9.2. *For all constants β, δ and all integers $n > 0$, there exists an efficiently computable function $\mathrm{Con} : \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^\ell$, $d = 0(1)$ and $\ell = \Omega(n)$ such that the following holds: for any $(n, \delta n)$-source $\mathbf{X}$ there exists a $y \in \{0,1\}^d$ such that $\mathrm{Con}(\mathbf{X}, y)$ is $2^{-\Omega(n)}$-close to a source with min-entropy $(1 - \beta)\ell$.*
We call such a function Con to be a $(\delta, 1 - \beta)$-condenser.

We prove that Algorithm 9 computes the required extractor. We begin by setting up some ingredients and parameters.

- Let $\kappa > 0$ be a small enough constant.

- Let $n_1 = (2/3 + \delta/2)n$ and $n_2 = n^{5\kappa}$.

- Let β be a parameter which we fix later. Let $\text{Con} : \{0,1\}^{n_1} \times \{0,1\}^d \to \{0,1\}^\ell$ be a $(\delta/4, 1-\beta)$-condenser instantiated from Theorem 9.2. Thus $\ell = n/C'$, for some constant C' that depends on δ, β. Let $D = 2^d$. Note that $D = O(1)$.

- Let $\text{LExt}_1 : \{0,1\}^{2n} \times \{0,1\}^\ell \to \{0,1\}^{n_2}$ be the linear seeded extractor from Theorem 3.12 set to extract from min-entropy rate $1/12$ and error $\epsilon_1 = 2^{-2\beta\ell}$. The seed-length is at most $3C\beta\ell$, some constant C that arises out of Theorem 3.12. We choose $\beta = min\{1/3C, \gamma\}$, where γ is the constant in Theorem 3.12. Note that the seed-length of LExt_1 is indeed at most ℓ.

- Let $\text{ACB} : \{0,1\}^{n_{1,acb}} \times \{0,1\}^{n_{acb}} \times \{0,1\}^{h_{acb}} \to \{0,1\}^{n_{2,acb}}$, be the advice correlation breaker from Theorem 4.1 set with the following parameters: $n_{acb} = 2n, n_{1,acb} = n_2, n_{2,acb} = n_3 = n^{2\kappa}$, $t_{acb} = D, h_{acb} = d, \epsilon_{acb} = 2^{-n^\kappa}, d_{acb} = O(\log^2(n/\epsilon_{acb})), \lambda_{acb} = 0$. It can be checked that by our choice of parameters, the conditions required for Theorem 4.1 indeed hold for $k_{1,acb} \geq n^{2\kappa}$.

- Let $\text{LExt}_2 : \{0,1\}^{2n} \times \{0,1\}^{n_3} \to \{0,1\}^m$, $m = \Omega(n)$, be a linear-seeded extractor instantiated from Theorem 3.10 set to extract from entropy $k_1 = n/10$ with error $\epsilon_1 = 2^{-\alpha\sqrt{n_3}}$, for an appropriately picked small constant α.

Algorithm 9: iℓExt(z)

Input: Bit-string $z = (x \circ y)_\pi$ of length $2n$, where x and y are each n bit-strings, and $\pi : [2n] \to [2n]$ is a permutation.
Output: Bit string of length m.

```
Let $z_1 = \text{Slice}(z, n_1)$.
Let $v$ be a $D \times n_2$ matrix, with its $i$'th row $v_i = \text{Con}(z_1, i)$.
Let $r$ be a $D \times n_3$ matrix, with its $i$'th row $r_i = \text{LExt}_1(z, v_i)$.
Let $s$ be a $D \times m$ matrix, with its $i$'th row $s_i = \text{ACB}(r_i, z, i)$.
Let $\tilde{s} = \oplus_{i=1}^{D} s_i$.
Output $\text{LExt}_2(z, \tilde{s})$.
```

We use the following notation: Let $\mathbf{X}_1$ be the bits of $\mathbf{X}$ in $\mathbf{Z}_1$ and $\mathbf{X}_2$ be the remaining bit of $\mathbf{X}$. Let $\mathbf{Y}_1$ be the bits of $\mathbf{Y}$ in $\mathbf{Z}_1$ and $\mathbf{Y}_2$ be the remaining bits of $\mathbf{Y}$. Without loss of generality assume $|\mathbf{X}_1| \geq |\mathbf{Y}_1|$. Define $\overline{\mathbf{X}} = (\mathbf{X} \circ 0^n)_\pi$ and $\overline{\mathbf{Y}} = (\mathbf{Y} \circ 0^n)_\pi$. Further, let $\overline{\mathbf{X}}_1 = \text{Slice}(\overline{\mathbf{X}}, n_1)$ and $\overline{\mathbf{Y}}_1 = \text{Slice}(\overline{\mathbf{Y}}, n_1)$. It follows that $\mathbf{Z} = \overline{\mathbf{X}} + \overline{\mathbf{Y}}$, and $\mathbf{Z}_1 = \overline{\mathbf{X}}_1 + \overline{\mathbf{Y}}_1$. Further, let $k_x = k_y = (2/3 + \delta)n$.

We begin by proving the following claim.

Claim 9.3. *Conditioned on the random variables $\mathbf{X}_1, \mathbf{Y}_1, \{\text{LExt}_1(\overline{\mathbf{X}}, \text{Con}(\overline{\mathbf{X}_1} + \overline{\mathbf{Y}}_1, i))\}_{i=1}^{D}$, the following hold:*

- *the matrix $\mathbf{R}$ is $2^{-\Omega(n)}$-close to a somewhere random source,*

- *$\mathbf{R}$ is a deterministic functions of $\mathbf{Y}$,*

- *$H_\infty(\mathbf{X}) \geq \delta n/4$, $H_\infty(\mathbf{Y}) \geq n/6$.*

Proof. By construction, we have that for any $j \in [D]$,

$$\begin{aligned}\mathbf{R}_j &= \mathrm{LExt}_1(\mathbf{Z}, \mathrm{Con}(\mathbf{Z}_1, j)) \\ &= \mathrm{LExt}_1(\overline{\mathbf{X}} + \overline{\mathbf{Y}}, \mathrm{Con}(\overline{\mathbf{X}_1} + \overline{\mathbf{Y}_1}, j)) \\ &= \mathrm{LExt}_2(\overline{\mathbf{X}}, \mathrm{Con}(\overline{\mathbf{X}_1} + \overline{\mathbf{Y}_1}, j)) + \mathrm{LExt}_2(\overline{\mathbf{Y}}, \mathrm{Con}(\overline{\mathbf{X}_1} + \overline{\mathbf{Y}_1}, j))\end{aligned}$$

Fix the random variables $\mathbf{Y}_1$, and $\overline{\mathbf{Y}}$ has min-entropy at least $k_y - n_1/2 \geq n/6 + 3\delta n/4$. Further, note that $\overline{\mathbf{X}_1}$ has min-entropy at least $n_1/2 - (n - k_x) \geq \delta n/4$. Now, by Theorem 9.2, we know that there exists a $j \in [D]$ such that $\mathrm{Con}(\overline{\mathbf{X}}_1 + \overline{\mathbf{Y}}_1, j)$ is $2^{-\Omega(n)}$-close to a source with min-entropy at least $(1-\beta)\ell$. Further, note that $\mathbf{V}$ is a deterministic function of $\mathbf{X}$.

Now, since LExt_1 is a strong seeded extractor set to extract from min-entropy $n/6$, it follows that

$$|\mathrm{LExt}_1(\overline{\mathbf{Y}}, \mathrm{Con}(\overline{\mathbf{X}_1} + \overline{\mathbf{Y}}_1, j)) - \mathbf{U}_{n_2}| \leq 2^{\beta\ell}\epsilon_1 + 2^{-\Omega(n)} \leq 2^{-\beta\ell+1}.$$

We now fix the random variables $\overline{\mathbf{X}}_1$ and note that $\mathrm{LExt}_1(\overline{\mathbf{Y}}, \mathrm{Con}(\overline{\mathbf{X}}_1 + \overline{\mathbf{Y}}_1, j))$ continues to be $2^{-\Omega(\ell)}$-close to $\mathbf{U}_{n_2}$. This follows from the fact that LExt_1 is a strong seeded extractor. Note that the random variables $\{\mathrm{Con}(\overline{\mathbf{X}}_1 + \overline{\mathbf{Y}}_1, i)) : i \in [D]\}$ are now fixed. Next, fix the random variables $\{\mathrm{LExt}_1(\overline{\mathbf{X}}, \mathrm{Con}(\overline{\mathbf{X}_1} + \overline{\mathbf{Y}}_1, i))\}_{i=1}^{D}$ noting that they are deterministic functions of $\mathbf{X}$. Thus $\mathbf{R}_j$ is $2^{-\Omega(n)}$-close to $\mathbf{U}_{n_2}$ and for any $i \in [D]$, the random variables $\mathbf{R}_i$ are deterministic functions of $\mathbf{Y}$. Finally, note that $\mathbf{X}$ and $\mathbf{Y}$ remain independent after these conditionings, and $H_\infty(\mathbf{X}) \geq k_x - n_1 - Dn_2$ and $H_\infty(\mathbf{Y}) \geq k_y - n_1/2$. □

The next claim almost gets us to Theorem 9.1.

Claim 9.4. *There exists $j \in [D]$ such that*

$$\mathbf{S}_j, \{\mathbf{S}_i\}_{i\in[D]\setminus j}, \mathbf{X} \approx_{2^{-n^{\Omega(1)}}} \mathbf{U}_{n_3}, \{\mathbf{S}_i\}_{i\in[D]\setminus j}, \mathbf{X}.$$

Proof. Fix the random variables: $\mathbf{X}_1, \mathbf{Y}_1, \{\mathrm{LExt}_1(\overline{\mathbf{X}}, \mathrm{Con}(\overline{\mathbf{X}_1} + \overline{\mathbf{Y}_1}, i))\}_{i=1}^{D}$. By Claim 9.3 we have that $\mathbf{R}$ is a deterministic function of $\mathbf{Y}$, and with probability at least $1 - 2^{-\Omega(n)}$, there exists $j \in [D]$ such that $\mathbf{R}_j$ is $2^{-n^{\Omega(1)}}$-close to uniform, and $H_\infty(\overline{\mathbf{X}}) \geq \delta n/4$. Recall that $\mathbf{Z} = \overline{\mathbf{X}} + \overline{\mathbf{Y}}$. It now follows by Theorem 4.1 that

$$\begin{aligned}\mathrm{ACB}(\mathbf{R}_j, \mathbf{Z}, \mathbf{W} \circ j), \{\mathrm{ACB}(\mathbf{R}_i, \overline{\mathbf{X}} + \overline{\mathbf{Y}}, \mathbf{W} \circ i)\}_{i\in[D]\setminus j}, \mathbf{X} &\approx_{2^{-n^{\Omega(1)}}} \\ \mathbf{U}_{n_3}, \{\mathrm{ACB}(\mathbf{R}_i, \overline{\mathbf{X}} + \overline{\mathbf{Y}}, \mathbf{W} \circ i)\}_{i\in[D]\setminus j}, \mathbf{X}&.\end{aligned}$$

□

It follows by Claim 9.4 that $\widetilde{\mathbf{S}}$ is $2^{-n^{\Omega(1)}}$-close to uniform even conditioned on $\mathbf{X}$. Thus, noting that $\mathrm{LExt}_2(\mathbf{Z}, \widetilde{\mathbf{S}}) = \mathrm{LExt}_2(\overline{\mathbf{X}}, \widetilde{\mathbf{S}}) + \mathrm{LExt}_2(\overline{\mathbf{Y}}, \widetilde{\mathbf{S}})$, it follows that we can fix $\widetilde{\mathbf{S}}$ and $\mathrm{LExt}_2(\overline{\mathbf{X}}, \widetilde{\mathbf{S}})$ remains $2^{-n^{\Omega(1)}}$-close to uniform and is a deterministic function of $\mathbf{X}$. Next, we fix $\mathrm{LExt}_2(\overline{\mathbf{Y}}, \widetilde{\mathbf{S}})$ without affecting the distribution of $\mathrm{LExt}_2(\overline{\mathbf{X}}, \widetilde{\mathbf{S}})$. It follows that $\mathrm{LExt}_2(\mathbf{Z}, \widetilde{\mathbf{S}})$ is $2^{-n^{\Omega(1)}}$-close to uniform. This completes the proof of Theorem 9.1.

References

[ADKO15] D. Aggarwal, Y. Dodis, T. Kazana, and M. Obremski. Non-malleable reductions and applications. To appear in STOC, 2015.

[ADL14] Divesh Aggarwal, Yevgeniy Dodis, and Shachar Lovett. Non-malleable codes from additive combinatorics. In *STOC*, 2014.

[AGM$^+$15] Shashank Agrawal, Divya Gupta, Hemanta K. Maji, Omkant Pandey, and Manoj Prabhakaran. A rate-optimizing compiler for non-malleable codes against bit-wise tampering and permutations. In *Theory of Cryptography - 12th Theory of Cryptography Conference, TCC 2015, Warsaw, Poland, March 23-25, 2015, Proceedings, Part I*, pages 375–397, 2015.

[BDG$^+$18] Marshall Ball, Dana Dachman-Soled, Siyao Guo, Tal Malkin, and Li-Yang Tan. Non-malleable codes for small-depth circuits. *Electronic Colloquium on Computational Complexity (ECCC)*, 2018.

[BDKM16] Marshall Ball, Dana Dachman-Soled, Mukul Kulkarni, and Tal Malkin. Non-malleable codes for bounded depth, bounded fan-in circuits, 2016.

[BRSW12] Boaz Barak, Anup Rao, Ronen Shaltiel, and Avi Wigderson. 2-source dispersers for $n^{o(1)}$ entropy, and Ramsey graphs beating the Frankl-Wilson construction. *Annals of Mathematics*, 176(3):1483–1543, 2012. Preliminary version in STOC '06.

[CG88] Benny Chor and Oded Goldreich. Unbiased bits from sources of weak randomness and probabilistic communication complexity. *SIAM Journal on Computing*, 17(2):230–261, 1988.

[CG14] Mahdi Cheraghchi and Venkatesan Guruswami. Non-malleable coding against bit-wise and split-state tampering. In *TCC*, pages 440–464, 2014.

[CGL16] Eshan Chattopadhyay, Vipul Goyal, and Xin Li. Non-malleable extractors and codes, with their many tampered extensions. In *STOC*, 2016.

[CL16] Eshan Chattopadhyay and Xin Li. Extractors for sumset sources. In *STOC*, 2016.

[CL17] Eshan Chattopadhyay and Xin Li. Non-malleable codes and extractors for small-depth circuits, and affine functions. In *Proceedings of the 49th Annual ACM SIGACT Symposium on Theory of Computing*, pages 1171–1184. ACM, 2017.

[CMTV15] Sandro Coretti, Ueli Maurer, Björn Tackmann, and Daniele Venturi. From single-bit to multi-bit public-key encryption via non-malleable codes. In *Theory of Cryptography Conference*, pages 532–560. Springer, 2015.

[Coh15] Gil Cohen. Local correlation breakers and applications to three-source extractors and mergers. In *Proceedings of the 56th Annual IEEE Symposium on Foundations of Computer Science*, 2015.

[Coh16] Gil Cohen. Two-source dispersers for polylogarithmic entropy and improved Ramsey graphs. In *STOC*, 2016.

[CZ14] Eshan Chattopadhyay and David Zuckerman. Non-malleable codes against constant split-state tampering. In *Proceedings of the 55th Annual IEEE Symposium on Foundations of Computer Science*, pages 306–315, 2014.

[CZ16a] Eshan Chattopadhyay and David Zuckerman. Explicit two-source extractors and resilient functions. In *STOC*, 2016.

[CZ16b] Eshan Chattopadhyay and David Zuckerman. New extractors for interleaved sources. In *CCC*, 2016.

[DKO13] Stefan Dziembowski, Tomasz Kazana, and Maciej Obremski. Non-malleable codes from two-source extractors. In *CRYPTO (2)*, pages 239–257, 2013.

[DORS08] Y. Dodis, R. Ostrovsky, L. Reyzin, and A. Smith. Fuzzy extractors: How to generate strong keys from biometrics and other noisy data. *SIAM Journal on Computing*, 38:97–139, 2008.

[DPW10] Stefan Dziembowski, Krzysztof Pietrzak, and Daniel Wichs. Non-malleable codes. In *ICS*, pages 434–452, 2010.

[DW09] Yevgeniy Dodis and Daniel Wichs. Non-malleable extractors and symmetric key cryptography from weak secrets. In *STOC*, pages 601–610, 2009.

[GMW17] Divya Gupta, Hemanta K Maji, and Mingyuan Wang. Constant-rate non-malleable codes in the split-state model. 2017.

[GPR16] Vipul Goyal, Omkant Pandey, and Silas Richelson. Textbook non-malleable commitments. In *Proceedings of the forty-eighth annual ACM symposium on Theory of Computing*, pages 1128–1141. ACM, 2016.

[GUV09] Venkatesan Guruswami, Christopher Umans, and Salil P. Vadhan. Unbalanced expanders and randomness extractors from Parvaresh–Vardy codes. *J. ACM*, 56(4), 2009.

[KOS17] Bhavana Kanukurthi, Sai Lakshmi Bhavana Obbattu, and Sruthi Sekar. Four-state non-malleable codes with explicit constant rate. In *Theory of Cryptography Conference*, pages 344–375. Springer, 2017.

[Li15] Xin Li. Improved two-source extractors, and affine extractors for polylogarithmic entropy. Technical Report TR15-125, ECCC, 2015.

[Li17] Xin Li. Improved non-malleable extractors, non-malleable codes and independent source extractors. In *Proceedings of the 49th Annual ACM SIGACT Symposium on Theory of Computing*, STOC 2017, pages 1144–1156, 2017.

[Li18] Xin Li. Pseudorandom correlation breakers, independence preserving mergers and their applications. *Electronic Colloquium on Computational Complexity (ECCC)*, 2018.

[MW97] Ueli Maurer and Stefan Wolf. Privacy amplification secure against active adversaries. In *Advances in Cryptology — CRYPTO '97*, volume 1294, pages 307–321, August 1997.

[Rao09] Anup Rao. Extractors for low-weight affine sources. In *Proceedings of the 24th Annual IEEE Conference on Computational Complexity*, 2009.

[RRV02] Ran Raz, Omer Reingold, and Salil Vadhan. Extracting all the randomness and reducing the error in Trevisan's extractors. *JCSS*, 65(1):97–128, 2002.

[RY11] Ran Raz and Amir Yehudayoff. Multilinear formulas, maximal-partition discrepancy and mixed-sources extractors. *Journal of Computer and System Sciences*, 77:167–190, 2011.

[Tre01] Luca Trevisan. Extractors and pseudorandom generators. *Journal of the ACM*, pages 860–879, 2001.

[TV00] Luca Trevisan and Salil P. Vadhan. Extracting Randomness from Samplable Distributions. In *IEEE Symposium on Foundations of Computer Science*, pages 32–42, 2000.

[Zuc97] David Zuckerman. Randomness-optimal oblivious sampling. *Random Structures and Algorithms*, 11:345–367, 1997.

[Zuc07] David Zuckerman. Linear degree extractors and the inapproximability of max clique and chromatic number. *Theory of Computing*, pages 103–128, 2007.