Electronic Colloquium on Computational Complexity, Revision 1 of Report No. 36 (2016)

Explicit Non-Malleable Extractors, Multi-Source Extractors and Almost Optimal Privacy Amplification Protocols

Eshan Chattopadhyay*
Department of Computer Science,
University of Texas at Austin
eshanc@cs.utexas.edu

Xin Li
Department of Computer Science
John Hopkins University
lixints@cs.jhu.edu

March 14, 2016

Abstract

We make progress in the following three problems: 1. Constructing optimal seeded non-malleable extractors; 2. Constructing optimal privacy amplification protocols with an active adversary, for any possible security parameter; 3. Constructing extractors for independent weak random sources, when the min-entropy is extremely small (i.e., near logarithmic).

For the first two problems, the best known non-malleable extractors by Chattopadhyay, Goyal and Li [CGL16], and by Cohen [Coh16a, Coh16b] all require seed length and min-entropy at least $\log^2(1/\varepsilon)$, where ε is the error of the extractor. As a result, the best known explicit privacy amplification protocols with an active adversary, which achieve 2 rounds of communication and optimal entropy loss in [Li15c, CGL16], can only handle security parameter up to $s = \Omega(\sqrt{k})$, where k is the min-entropy of the shared secret weak random source. For larger s the best known protocol with optimal entropy loss in [Li15c] requires $O(s/\sqrt{k})$ rounds of communication.

In this paper we give an explicit non-malleable extractor that only requires seed length and min-entropy $\log^{1+o(1)}(n/\varepsilon)$, which also yields a 2-round privacy amplification protocol with optimal entropy loss for security parameter up to $s = k^{1-\alpha}$ for any constant $\alpha > 0$.

For the third problem, previously the best known extractor which supports the smallest min-entropy due to Li [Li13a], requires min-entropy $\log^{2+\delta} n$ and uses $O(1/\delta)$ sources, for any constant $\delta > 0$. A very recent result by Cohen and Schulman [CS16] improves this, and constructed explicit extractors that use $O(1/\delta)$ sources for min-entropy $\log^{1+\delta} n$, any constant $\delta > 0$. In this paper we further improve their result, and give an explicit extractor that uses $O(1)$ (an absolute constant) sources for min-entropy $\log^{1+o(1)} n$.

The key ingredient in all our constructions is a generalized, and much more efficient version of the independence preserving merger introduced in [CS16], which we call *non-malleable independence preserving merger*. Our construction of the merger also simplifies that of [CS16], and may be of independent interest.

*Partially supported by NSF Grant CCF-1218723 and a Dissertation Writing Fellowship awarded by UT Austin.

ISSN 1433-8092

1 Introduction

The theory of *randomness extractors* is a broad area and a fundamental branch of the more general study of pseudorandomness. Informally, randomness extractors are functions that transform biased probability distributions (weak random sources) into almost uniform probability distributions. Here we measure the entropy of a weak random source by the standard min-entropy. A source $\mathbf{X}$ is said to have min-entropy k if for any x, $\Pr[\mathbf{X} = x] \leq 2^{-k}$. An (n, k)-source $\mathbf{X}$ is a distribution on n bits with min-entropy at least k.

It is well known that it is impossible to construct deterministic randomness extractors when the input is just one (arbitrary) weak random source, even if the min-entropy is as large as $n - 1$. A natural relaxation is then to give the extractor a short independent uniform seed, and such extractors are called *seeded extractors*. With this relaxation it is indeed possible to construct extractors that work for any weak random source with essentially any min-entropy. We now formally define such extractors.

Definition 1.1. *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 $\mathcal{D}_1 \approx_\epsilon \mathcal{D}_2$.*

Definition 1.2 ([NZ96])**.** *A function $\mathrm{Ext} : \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^m$ is a seeded extractor for min-entropy k and error ϵ if for any source $\mathbf{X}$ of min-entropy k, $|\mathrm{Ext}(\mathbf{X}, \mathbf{U}_d) - \mathbf{U}_m| \leq \epsilon$. Ext is strong if in addition $|(\mathrm{Ext}(\mathbf{X}, \mathbf{U}_d), \mathbf{U}_d) - (\mathbf{U}_m, \mathbf{U}_d)| \leq \epsilon$, where $\mathbf{U}_m$ and $\mathbf{U}_d$ are independent.*

Through a long line of research we now have explicit constructions of seeded extractors with almost optimal parameters [LRVW03, GUV09, DKSS09].

In recent years, there has been much interest in the study of two other kinds of randomness extractors. The first one, known as *non-malleable extractors* (introduced by Dodis and Wichs [DW09]), is a generalization of strong seeded extractors.

Definition 1.3 (Non-malleable extractor)**.** *A function $\mathrm{nmExt} : \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^m$ is a (k, ϵ)-non-malleable extractor if the following holds: For any (n, k)-source $\mathbf{X}$, an independent uniform seed $\mathbf{Y}$ on d bits and any function $\mathcal{A} : \{0,1\}^d \to \{0,1\}^d$ with no fixed points,*[1]

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

The second one, known as *multi-source extractors* (first studied by Chor and Goldreich [CG88]), is another natural relaxation of deterministic extractors for one weak random source, in the sense that now the input to the extractor are several (at least two) independent weak random sources. Curiously, although this problem was first studied around 30 years ago, it was not until recently that significant progress has been achieved.

The above two kinds of extractors are closely related, and in many cases techniques used for one can also be used to improve the constructions of the other. These connections have been demonstrated in a number of works (e.g., [Li12b, Li13b, Li13a, Li15d, CZ16]).

We now briefly discuss the motivations for these two kinds of extractors.

1.1 Non-malleable extractors and privacy amplification

The initial motivation for non-malleable extractors comes from the problem of privacy amplification with an active adversary. As a basic problem in information theoretic cryptography, privacy

[1] i.e., for any x, $\mathcal{A}(x) \neq x$

amplification deals with the case where two parties want to communicate with each other to convert their shared secret weak random source $\mathbf{X}$ into shared secret nearly uniform random bits. On the other hand, the communication channel is watched by an adversary Eve, who has unlimited computational power. To make this task possible, we assume two parties have local (non-shared) uniform random bits.

If Eve is passive (i.e., can only see the messages but cannot change them), this problem can be solved easily by applying the aforementioned strong seeded extractors. However, in the case where Eve is active (i.e., can arbitrarily change, delete and reorder messages), the problem becomes much more complicated. The major challenge here is to design a protocol that uses as few number of interactions as possible, and outputs a uniform random string $\mathbf{R}$ that has length as close to $H_\infty(\mathbf{X})$ as possible (the difference is called *entropy loss*). A bit more formally, we pick a security parameter s, and if the adversary Eve remains passive during the protocol then the two parties should achieve shared secret random bits that are 2^{-s}-close to uniform. On the other hand, if Eve is active, then the probability that Eve can successfully make the two parties output two different strings without being detected should be at most 2^{-s}. We refer the readers to [DLWZ14] for a formal definition.

There has been a long line of work on this problem [MW97, DKRS06, DW09, RW03, KR09, CKOR10, DLWZ14, CRS14, Li12a, Li12b, Li15c]. When the entropy rate of $\mathbf{X}$ is large, i.e., bigger than $1/2$, there are known protocols that take only one round (e.g., [MW97, DKRS06]). However these protocols all have very large entropy loss. When the entropy rate of $\mathbf{X}$ is smaller than $1/2$, [DW09] showed that no one round protocol exists; furthermore the length of $\mathbf{R}$ has to be at least $O(s)$ smaller than $H_\infty(\mathbf{X})$. Thus, the natural goal is to design a two-round protocol with such optimal entropy loss. However, all protocols before the work of [DLWZ14] either need to use $O(s)$ rounds, or need to incur an entropy loss of $O(s^2)$.

In [DW09], Dodis and Wichs showed that explicit constructions of the aforementioned non-malleable extractors can be used to give two-round privacy amplification protocols with optimal entropy loss. Using the probabilistic method, they also showed that non-malleable extractors exist when $k > 2m + 2\log(1/\varepsilon) + \log d + 6$ and $d > \log(n-k+1) + 2\log(1/\varepsilon) + 5$. However, they were not able to give explicit constructions even for min-entropy $k = n - 1$. The first explicit construction of non-malleable extractors appeared in [DLWZ14], with subsequent improvements in [CRS14, Li12a, DY13, Li12b]. All these constructions require the min-entropy of the weak source to be bigger than $0.49n$, and thus only give two-round privacy amplification protocols with optimal entropy loss for such min-entropy. Together with some other ideas, [DLWZ14] also gives poly$(1/\delta)$ round protocols with optimal entropy loss for min-entropy $k \geq \delta n$, any constant $\delta > 0$. This was subsequently improved by one of the authors in [Li12b] to obtain a two-round protocol with optimal entropy loss for min-entropy $k \geq \delta n$, any constant $\delta > 0$. In the general case, using a relaxation of non-malleable extractors called non-malleable condensers, one of the authors [Li15c] also obtained a two-round protocol with optimal entropy loss for min-entropy $k \geq C\log^2 n$, some constant $C > 1$, as long as the security parameter s satisfies $k \geq Cs^2$. For larger security parameter, the best known protocol with optimal entropy loss in [Li12b] still takes $O(s/\sqrt{k})$ rounds.

In a recent work, Chattopadhyay, Goyal and Li [CGL16] constructed explicit non-malleable extractors with error ε, for min-entropy $k = \Omega(\log^2(n/\epsilon))$ and seed-length $d = O(\log^2(n/\epsilon))$. This gives an alternative protocol matching that of [Li12b]. Subsequently, Cohen [Coh16a] improved this result, and constructed non-malleable extractors with seed length $d = O(\log(n/\epsilon)\log((\log n)/\epsilon))$ and min-entropy $k = \Omega(\log(n/\epsilon)\log((\log n)/\epsilon))$. In this work, he also gave another construction that worked for $k = n/(\log n)^{O(1)}$ with seed-length $O(\log n)$. In a follow up, Cohen [Coh16b] constructed non-malleable extractors with seed length $d = O(\log n + \log^3(1/\epsilon))$ and min-entropy $k = \Omega(d)$. However, in terms of the general error parameter ε, all of these results require min-

entropy and seed length at least $\log^2(1/\varepsilon)$, thus none of them can be used to improve the privacy amplification protocols in [Li15c].

1.2 Multi-source extractors for independent sources

As mentioned before, Chor and Goldreich [CG88] introduced the problem of designing extractors for two or more independent sources. Explicit constructions of such extractors can also be used in explicit constructions of Ramsey graphs ([BRSW12, Coh16c, CZ16]). A simple probabilistic argument shows the existence of two-source extractors for min-entropy $k \geq \log n + O(1)$. However, explicit constructions of such functions are extremely challenging.

Chor and Goldreich [CG88] proved that the inner-product function is a two-source extractor for min-entropy greather than $n/2$. It was not until 20 years later when Bourgain [Bou05] broke the entropy rate $1/2$ barrier and constructed a two-source extractor for min-entropy $0.49n$. Raz [Raz05] obtained another construction which requires one source with min-entropy more than $n/2$ and the other source with min-entropy $O(\log n)$. Recently, Chattopadhyay and Zuckerman [CZ16] improved the situation substantially by constructing two-source extractors for min-entropy $k \geq \text{polylog}(n)$, with subsequent improvements obtained by Li [Li15a] and Meka [Mek15]. The ultimate goal here is to obtain two-source extractors matching the entropy bound given by the probabilistic method. We are not able to resolve this question in the present work, but we make progress on a relaxed version of the problem, where the extractor has access to more than two sources.

If we allow the extractor to have a constant number of sources instead of just two sources, then an exciting line of work [BIW06, BKS+10, Rao09, BRSW12, RZ08, Li11, Li13b, Li13a, Li15d, Coh15] constructed extractors with excellent parameters. However, the smallest entropy these constructions can achieve is $\log^{2+\delta} n$ for any constant $\delta > 0$ [Li13a], which uses $O(1/\delta) + O(1)$ sources. In a very recent work, Cohen and Schulman [CS16] managed to break this "quadratic" barrier, and constructed extractors for $O(1/\delta) + O(1)$ sources, each having min-entropy at least $\log^{1+\delta} n$.

1.3 Our results

Our first result is a new construction of non-malleable extractors that breaks the $\log^2(1/\varepsilon)$ barrier for min-entropy and seed length. Specifically, we have the following theorem.

Theorem 1. *There exists a constant $C > 0$ s.t for all $n, k \in \mathbb{N}$ and any $\epsilon > 0$, with $k \geq \log(n/\epsilon)2^{C\sqrt{\log\log(n/\epsilon)}}$, there exists an explicit (k, ϵ)-non-malleable extractor* $\text{nmExt} : \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^m$, *where $d = \log(n/\epsilon)2^{C\sqrt{\log\log(n/\epsilon)}}$ and $m = k/2^{\sqrt{\log\log(n/\epsilon)}}$.*

We also construct a non-malleable extractor with seed-length $O(\log n)$ for min-entropy $k = \Omega(\log n)$ and $\epsilon \geq 2^{-\log^{1-\beta}(n)}$ for any $\beta > 0$. Prior to this, explicit non-malleable extarctors with seed-length $O(\log n)$ either requires min-entropy at least $n/\text{poly}(\log n)$ [Coh16a] or requires $\epsilon \geq 2^{-\log^{1/3}(n)}$ [Coh16b].

Theorem 2. *There exists a constant $C > 0$ s.t for and all $n, k \in \mathbb{N}$ with $k \geq C \log n$, any constant $0 < \beta < 1$, and any $\epsilon \geq 2^{-\log^{1-\beta}(n)}$, there exists an explicit (k, ϵ)-non-malleable extractor* $\text{nmExt} : \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^m$, *where $d = O(\log n)$ and $m = \Omega(\log(1/\epsilon))$.*

Remark 1.4. *A careful examination reveals that our seed length and min-entropy requirement are better than those of [Coh16a, Coh16b] in all cases except the case that ε is large enough (e.g., $\epsilon \geq 2^{-\log^{1/3}(n)}$), where both [Coh16b] and our results require seed length and min-entropy $O(\log n)$.*

Note that given any error parameter ε, our non-malleable extractor in Theorem 1 only requires min-entropy and seed length $\log^{1+o(1)}(n/\varepsilon)$. Using this theorem and the protocol in [DW09], we immediately obtain a two-round privacy amplification protocol with optimal entropy loss, for almost all possible security parameters.

Theorem 3. *There exists a constant $C > 0$ such that for any security parameter s with $k \geq (s + \log n)2^{C\sqrt{\log(s+\log n)}}$, there exists an explicit 2-round privacy amplification protocol for (n, k)-sources with entropy loss $O(\log n + s)$, in the presence of an active adversary.*

In particular, this gives us two-round privacy amplification protocols with optimal entropy loss for security parameter $s \leq k^{1-\alpha}$ for any constant $\alpha > 0$.

Next, we improve the entropy requirement in extractors for a constant number of independent sources. In particular, we give explicit extractors for $O(1)$ sources, each having min-entropy $\log^{1+o(1)}(n)$. More formally, we have the following theorem.

Theorem 4. *There exist two constants $C_1 > 0, C_2 > 0$ s.t for all $n, k \in \mathbb{N}$ with $k \geq 2^{C_1\sqrt{\log\log(n)}} \log n$ and any constant $\epsilon > 0$,[2] there exists an explicit function $\mathrm{Ext} : (\{0,1\}^n)^{C_2} \to \{0,1\}$, such that if $\mathbf{X}_1, \ldots, \mathbf{X}_{C_2}$ are independent (n, k) sources, then*

$$|\mathrm{Ext}(\mathbf{X}_1, \ldots, \mathbf{X}_{C_2}) - \mathbf{U}_1| \leq \epsilon.$$

1.4 Non-malleable independence preserving merger

The barrier of $\log^2(1/\varepsilon)$ in seed length and min-entropy requirement of non-malleable extractors, as well as the barrier of $\log^2 n$ in min-entropy requirement of multi-source extractors mainly come from the fact that the previous constructions rely heavily on the "alternating extraction" based techniques. In [CS16], Cohen and Schulman introduced a new object called *independence preserving merger* (IPM for short). This is the key component in their construction, which helps them to obtain the $O(1/\delta) + O(1)$ source extractor for min-entropy $k \geq \log^{1+\delta} n$. The construction of the independence preserving merger in [CS16] is fairly complicated and takes up a bulk of work.

A key component in all of our constructions is a generalized, and much more efficient version of the independence preserving merger in [CS16], which we call non-malleable independence preserving merger (NIPM for short). In addition, we believe that our construction of NIPM is simpler than the construction of IPM in [CS16]. We now define this object below.

Definition 1.5. *A $(L, t, d', \epsilon, \epsilon')$-NIPM : $\{0,1\}^{Lm} \times \{0,1\}^d \to \{0,1\}^{m_1}$ satisfies the following property. Suppose*

- *$\mathbf{X}, \mathbf{X}^1, \ldots, \mathbf{X}^t$ are r.v's, each supported on boolean $L \times m$ matrices s.t for any $i \in [L]$, $|\mathbf{X}_i - \mathbf{U}_m| \leq \epsilon$,*
- *$\{\mathbf{Y}, \mathbf{Y}^1, \ldots, \mathbf{Y}^t\}$ is independent of $\{\mathbf{X}, \mathbf{X}^1, \ldots, \mathbf{X}^t\}$, s.t $\mathbf{Y}, \mathbf{Y}^1, \ldots, \mathbf{Y}^t$ are each supported on $\{0,1\}^d$ and $H_\infty(\mathbf{Y}) \geq d - d'$,*
- *there exists an $h \in [L]$ such that $|(\mathbf{X}_h, \mathbf{X}^1_h, \ldots, \mathbf{X}^t_h) - (\mathbf{U}_m, \mathbf{X}^1_h, \ldots, \mathbf{X}^t_h)| \leq \epsilon$,*

then

$$|(L, t, d', \epsilon, \epsilon')\text{-NIPM}((\mathbf{X}, \mathbf{Y}), (L, t, d', \epsilon, \epsilon')\text{-NIPM}(\mathbf{X}^1, \mathbf{Y}^1), \ldots, (L, t, d', \epsilon, \epsilon')\text{-NIPM}(\mathbf{X}^t, \mathbf{Y}^t)$$
$$-\mathbf{U}_{m_1}, (L, t, d', \epsilon, \epsilon')\text{-NIPM}(\mathbf{X}^1, \mathbf{Y}^1), \ldots, (L, t, d', \epsilon, \epsilon')\text{-NIPM}(\mathbf{X}^t, \mathbf{Y}^t)| \leq \epsilon'.$$

[2] As in [CS16], the error can actually be slightly sub-constant.

We present an explicit construction of an NIPM which requires seed length $d = \log(m/\epsilon)L^{o(1)}$ for the case $t = 1$. More formally, we have the following theorem.

Theorem 5. *For all integers $m, L > 0$, any $\epsilon > 0$, there exists an explicit $(L, 1, 0, \epsilon, \epsilon')$-NIPM : $\{0,1\}^{mL} \times \{0,1\}^d \to \{0,1\}^{m'}$, where $d = 2^{O(\sqrt{\log L})} \log(m/\epsilon), m' = \frac{m}{2^{\sqrt{\log L}}} - 2^{O(\sqrt{\log L})} \log(m/\epsilon)$ and $\epsilon' = O(\epsilon L)$.*

We have a more general version of the above theorem presented in Section 4.3 which works for general t. This is crucial for us to obtain our results on extractors for independent sources with near logarithmic min-entropy.

Using our NIPM, we construct a standard IPM introduced in the work of Cohen and Schulman [CS16]. We first define an IPM.

Definition 1.6. *A $(L, k, t, \epsilon, \epsilon')$-IPM : $\{0,1\}^{Lm} \times \{0,1\}^n \to \{0,1\}^{m_1}$ satisfies the following property. Suppose*

- *$\mathbf{X}, \mathbf{X}^1, \ldots, \mathbf{X}^t$ are r.v's, each supported on boolean $L \times m$ matrices s.t for any $i \in [L]$, $|\mathbf{X}_i - \mathbf{U}_m| \leq \epsilon$,*
- *$\mathbf{Y}$ is an (n, k)-source, independent of $\{\mathbf{X}, \mathbf{X}^1, \ldots, \mathbf{X}^t\}$.*
- *there exists an $h \in [L]$ such that $|(\mathbf{X}_h, \mathbf{X}^1_h, \ldots, \mathbf{X}^t_h) - (\mathbf{U}_m, \mathbf{X}^1_h, \ldots, \mathbf{X}^t_h)| \leq \epsilon$,*

then

$$|(L,k,t,\epsilon,\epsilon')\text{-IPM}(\mathbf{X},\mathbf{Y}), (L,k,t,\epsilon,\epsilon')\text{-IPM}(\mathbf{X}^1,\mathbf{Y}), \ldots, (L,k,t,\epsilon,\epsilon')\text{-NIPM}(\mathbf{X}^t,\mathbf{Y}) - \mathbf{U}_{m_1}, (L,k,t,\epsilon,\epsilon')\text{-IPM}(\mathbf{X}^1,\mathbf{Y}), \ldots, (L,k,t,\epsilon,\epsilon')\text{-IPM}(\mathbf{X}^t,\mathbf{Y})| \leq \epsilon'$$

Theorem 6. *For all integers $m, L > 0$, any $\epsilon > 0$, and any $k \geq 2^{O(\sqrt{\log L})} \log(m/\epsilon)$, there exists an explicit $(L, k, 1, \epsilon, \epsilon')$-IPM : $\{0,1\}^{mL} \times \{0,1\}^n \to \{0,1\}^{m'}$, with $m' = \frac{1}{2^{\sqrt{\log L}}}(m - O(\log(n/\epsilon))) - 2^{O(\sqrt{\log L})} \log(m/\varepsilon)$ and $\epsilon' = O(\epsilon L)$.*

As in the case of NIPM, we in fact construct an IPM for general t. The construction of IPM from NIPM is relatively straightforward, and using this explicit IPM we derive our improved results on extractors for independent sources.

We note that there are several important differences between our IPM and the construction in [CS16]. First, we only require that there exists at least *one* "good" row $\mathbf{X}_h$ in the matrix (i.e., $\mathbf{X}_h$ is uniform even given $\mathbf{X}^1_h, \ldots, \mathbf{X}^t_h$). In contrast, the IPM in [CS16] requires that 0.99 fraction of the rows are good. Second, the construction of IPM in [CS16] offers a trade-off between the number of additional sources required and the min-entropy requirement of each source. In particular, they construct an IPM using b additional sources, each having min-entropy $k = \Omega(L^{1/b} \log(n/\epsilon))$. In contrast, we use just *one* additional source with min-entropy $k = \Omega(L^{o(1)} \log(m/\varepsilon))$, and works as long as $m \geq O(\log(n/\epsilon)) + L^{o(1)} \log(m/\varepsilon)$. In typical applications, we will have $m \approx k < n$, so it suffices to set $k = L^{o(1)} \log(n/\varepsilon)$. For all applications in this paper, we will choose $L = O(\log(n/\varepsilon))$ and thus we get $k = \log^{1+o(1)}(n/\varepsilon)$. The fact that our IPM uses only one additional source improves significantly upon the IPM in [CS16] and is crucial for us to obtain an $O(1)$ source extractor for min-entropy $k = \log^{1+o(1)} n$.

2 Outline of Constructions

Here we give an informal and high level description of our constructions. We start with our non-malleable independence preserving merger (NIPM) with a uniform (or high entropy rate) seed.

2.1 Non-malleable independence preserving merger with uniform seed

For simplicity we start by describing the case of only one tampering adversary. Here, we have two correlated random variables $\mathbf{X} = (\mathbf{X}_1, \ldots, \mathbf{X}_L)$ and $\mathbf{X}' = (\mathbf{X}'_1, \ldots, \mathbf{X}'_L)$, each of them is an $L \times m$ matrix. We have another two correlated random variables $\mathbf{Y}, \mathbf{Y}'$. We assume the following conditions: $(\mathbf{X}, \mathbf{X}')$ is independent of $(\mathbf{Y}, \mathbf{Y}')$, each $\mathbf{X}_i$ is uniform and there exists a $j \in [L]$ such that $\mathbf{X}_j$ is uniform even conditioned on $\mathbf{X}'_j$, and $\mathbf{Y}$ is uniform. Our goal is to construct a function NIPM such that $\text{NIPM}(\mathbf{X}, \mathbf{Y})$ is uniform conditioned on $\text{NIPM}(\mathbf{X}', \mathbf{Y}')$, i.e., using $\mathbf{Y}$ we can merge $\mathbf{X}$ into a uniform random string which keeps the independence property over $\mathbf{X}'$ even with a tampered seed $\mathbf{Y}'$.

Our starting point is the following simple observation. Let $(\mathbf{X}, \mathbf{X}')$ be two correlated weak sources and $(\mathbf{R}, \mathbf{R}')$ be two correlated random variables such that $(\mathbf{X}, \mathbf{X}')$ is independent of $(\mathbf{R}, \mathbf{R}')$. Let $\mathbf{R}$ be uniform and take any strong seeded extractor Ext, consider $\mathbf{Z} = \text{Ext}(\mathbf{X}, \mathbf{R})$ and $\mathbf{Z}' = \text{Ext}(\mathbf{X}', \mathbf{R}')$. Assume the length of the output of Ext is small enough. Then $\mathbf{Z}$ is close to uniform given $\mathbf{Z}'$ if either of the following two conditions holds: $\mathbf{R}$ is uniform given $\mathbf{R}'$ or $\mathbf{X}$ has sufficient min-entropy conditioned on $\mathbf{X}'$. Indeed, in the first case, we can first fix $\mathbf{R}'$, and argue that conditioned on this fixing, $\mathbf{Z}'$ is a deterministic function of X'. We can now further fix $\mathbf{Z}'$, and conditioned on this fixing, $\mathbf{X}$ still has enough entropy left (since the length of $\mathbf{Z}'$ is small). Note that at this point $\mathbf{R}$ is still uniform and independent of X, thus $\mathbf{Z} = \text{Ext}(\mathbf{X}, \mathbf{R})$ is close to uniform given $\mathbf{Z}'$. In the second case, we can first fix $\mathbf{X}'$, and conditioned on this fixing $\mathbf{X}$ still has enough entropy left. Now since Ext is a strong extractor, we know that $\mathbf{Z} = \text{Ext}(\mathbf{X}, \mathbf{R})$ is close to uniform even given $\mathbf{R}$. Since we have already fixed $\mathbf{X}'$ and $(\mathbf{R}, \mathbf{R}')$ is independent of $(\mathbf{X}, \mathbf{X}')$, this means that $\mathbf{Z}$ is also close to uniform even given $\mathbf{R}'$ and $\mathbf{X}'$, which gives us $\mathbf{Z}' = \text{Ext}(\mathbf{X}', \mathbf{R}')$.

Now we can describe our basic NIPM. The construction is actually simple in the sense that it is essentially an alternating extraction process between $\mathbf{X}$ and $\mathbf{Y}$, except that in each alternation we use a *new* row from $\mathbf{X}$. Specifically, we first take a small slice $\mathbf{S}_1$ from $\mathbf{X}_1$, and apply a strong seeded extractor to obtain $\mathbf{R}_1 = \text{Ext}(\mathbf{Y}, \mathbf{S}_1)$; we then use $\mathbf{R}_1$ to extract from $\mathbf{X}_2$ and obtain $\mathbf{S}_2 = \text{Ext}(\mathbf{X}_2, \mathbf{R}_1)$. Now we continue and obtain $\mathbf{R}_2 = \text{Ext}(\mathbf{Y}, \mathbf{S}_2)$ and $\mathbf{S}_3 = \text{Ext}(\mathbf{X}_3, \mathbf{R}_2)$... .The final output of our merger will be $\mathbf{S}_L = \text{Ext}(\mathbf{X}_L, \mathbf{R}_{L-1})$.

To see why this construction works, first assume that the length of each $\mathbf{S}_i, \mathbf{R}_i$ is small enough. Let j be the first index in $[L]$ such that $\mathbf{X}_j$ is uniform even conditioned on $\mathbf{X}'_j$. Then, we can fix all the intermediate random variables $\mathbf{S}_1, \mathbf{S}'_1, \mathbf{R}_1, \mathbf{R}'_1, \mathbf{S}_2, \mathbf{S}'_2, \mathbf{R}_2, \mathbf{R}'_2 \ldots \mathbf{S}_{j-1}, \mathbf{S}'_{j-1}$, and conditioned on these fixings we know that: 1. $(\mathbf{R}_{j-1}, \mathbf{R}'_{j-1})$ are deterministic functions of $(\mathbf{Y}, \mathbf{Y}')$, and thus independent of $(\mathbf{X}, \mathbf{X}')$; 2. $\mathbf{R}_{j-1}$ is close to uniform; 3. $\mathbf{X}_j$ still has enough entropy conditioned on $\mathbf{X}'_j$. Now, by the first case we discussed above, this implies that $\mathbf{S}_j$ is close to uniform given $\mathbf{S}'_j$. From this point on, by using the second case we discussed above and an inductive approach, we can argue that for all subsequent $t \geq j$, we have that $\mathbf{R}_t$ is close to uniform given $\mathbf{R}'_t$ and $\mathbf{S}_t$ is close to uniform given $\mathbf{S}'_t$. Thus the final output $\mathbf{S}_L$ is close to uniform given $\mathbf{S}'_L$.

Note that this construction can work even if $\mathbf{Y}$ is a very weak random source instead of being uniform or having high min-entropy rate. However this basic approach will require the min-entropy of Y to be at least $O(L \log(m/\epsilon))$, which is pretty large if L is large. We next describe a way to reduce this entropy requirement, in the case where $\mathbf{Y}$ is uniform or has high min-entropy rate.

The idea is that, rather than merging the L rows in one step, we merge them in a sequence of steps, with each step merging all the blocks of some ℓ rows. Thus, it will take us roughly $\frac{\log L}{\log \ell}$ steps to merge the entire matrix. Now first assume that $\mathbf{Y}$ is uniform, then in each step we will not use the entire $\mathbf{Y}$ to do the alternating extraction and merging, but just use a *small slice* of $\mathbf{Y}$ for this purpose. That is, we will first take a small slice $\mathbf{Y}_1$ and use this slice to merge L/ℓ blocks of $\mathbf{X}$, where each block has ℓ rows; we then take another slice $\mathbf{Y}_2$ of $\mathbf{Y}$ and use this slice to merge L/ℓ^2 new blocks, where each block has ℓ rows, and so on. The advantage of this approach is that now the entropy consumed in each merging step is contained in the slice $\mathbf{Y}_i$ (and $\mathbf{Y}'_i$), and won't affect the rest of $\mathbf{Y}$ much.

As we discussed before, we need to make sure that each slice $\mathbf{Y}_i$ has min-entropy $O(\ell \log(m/\epsilon))$ conditioned on the fixing of all previous $(\mathbf{Y}_j, \mathbf{Y}'_j)$. As a result, we need to set $|\mathbf{Y}_{i+1}| \geq 2|\mathbf{Y}_i| + O(\ell \log(m/\epsilon))$. It suffices to take $|\mathbf{Y}_i| = c^i \ell \log(m/\epsilon)$ for some constant $c > 2$. We know that the whole merging process is going to take roughly $\frac{\log L}{\log \ell}$ steps, so the total length (or min-entropy) of $\mathbf{Y}$ is something like $c^{\frac{\log L}{\log \ell}} \ell \log(m/\epsilon)$. We just need to choose a proper ℓ to minimize this quantity. A simple calculation shows that the best ℓ is roughly such that $\log \ell = \sqrt{\log L}$, which gives us a seed length of $2^{O(\sqrt{\log L})} \log(m/\epsilon)$.

It is not difficult to see that this argument also extends to the case where $\mathbf{Y}$ is not perfectly uniform but has high min-entropy rate (e.g., $1 - o(1)$) where we can still start with a small slice of $\mathbf{Y}$, and the case where we have $t+1$ correlated matrices $\mathbf{X}, \mathbf{X}^1, \ldots, \mathbf{X}^t$ and t tampered seeds $\mathbf{Y}^1, \ldots, \mathbf{Y}^t$ of $\mathbf{Y}$.

2.2 Non-malleable extractor with almost optimal seed

The above NIPM is already enough to yield our construction of a non-malleable extractor with almost optimal seed length. Specifically, given an (n, k) source $\mathbf{X}$, an independent seed $\mathbf{Y}$, and a tampered seed $\mathbf{Y}'$, we follow the approach of one of the authors' previous work [CGL16] by first obtaining an advice of length $L = O(\log(n/\epsilon))$. Let the advice generated by $(\mathbf{X}, \mathbf{Y})$ be S and the advice generated by $\mathbf{X}, \mathbf{Y}'$ be S'. We have that with probability $1-\epsilon$, $S \neq S'$. Further, conditioned on (S, S') and some other random variables, we have that $\mathbf{X}$ is still independent of $(\mathbf{Y}, \mathbf{Y}')$ and $\mathbf{Y}$ has high min-entropy rate.

Now we take a small slice $\mathbf{Y}_1$ of $\mathbf{Y}$, and use $\mathbf{X}$ and $\mathbf{Y}_1$ to generate a random matrix $\mathbf{V}$ with L rows, where the i'th row is obtained by doing a flip-flop alternating extraction (introduced in [Coh15]) using the i'th bit of S. Similarly a matrix $\mathbf{V}'$ is generated using $\mathbf{X}'$ and $\mathbf{Y}_1$. The flip-flop alternating extraction guarantees that each row in $\mathbf{V}$ is close to uniform, and moreover if the i'th bit of S and S' are different, then $\mathbf{V}_i$ is close to uniform even given $\mathbf{V}'_i$. Note that conditioned on the fixing of $(\mathbf{Y}_1, \mathbf{Y}'_1)$, we have that $(\mathbf{V}, \mathbf{V}')$ are deterministic functions of $\mathbf{X}$, and are thus independent of $(\mathbf{Y}, \mathbf{Y}')$. Furthermore $\mathbf{Y}$ still has high min-entropy rate.

At this point we can just use our NIPM and $\mathbf{Y}$ to merge $\mathbf{V}$ into a uniform string $\mathbf{Z}$, which is guaranteed to be close to uniform given $\mathbf{Z}'$ (obtained from $(\mathbf{V}', \mathbf{Y}')$). The seed length of $\mathbf{Y}$ will be $O(\log(n/\epsilon)) + 2^{O(\sqrt{\log\log(n/\epsilon)})} \log(k/\epsilon)$. A careful analysis shows that the final error will be $O(\epsilon \log(n/\epsilon))$. Thus we need to set the error parameter ϵ slightly smaller in order to achieve a desired final error ϵ', but that does not affect the seed length much. Altogether this gives us a seed length and entropy requirement of $2^{O(\sqrt{\log\log(n/\epsilon)})} \log(n/\epsilon)$.

2.3 Independence preserving merger with weak random seed

We now use our previous NIPM to construct a standard independence preserving merger with weak random seed, an object introduced in [CS16]. Suppose we are given $(\mathbf{X}, \mathbf{X}')$ as described above and an independent random variable $\mathbf{Y}$. Here $\mathbf{Y}$ can be a very weak source, so our first step is to convert it to a uniform (or high min-entropy rate) seed.

To do this, our observation is that since we know that each row in $\mathbf{X}$ is uniform, we can just take a small slice $\mathbf{W}$ of the first row $\mathbf{X}_1$, and apply a strong seeded extractor to $\mathbf{Y}$ to obtain $\mathbf{Z} = \text{Ext}(\mathbf{Y}, \mathbf{W})$, which is guaranteed to be close to uniform. However by doing this we also created a correlated $\mathbf{Z}' = \text{Ext}(\mathbf{Y}, \mathbf{W}')$ where $\mathbf{W}'$ is a slice of $\mathbf{X}'_1$. Note that conditioned on the fixing of $(\mathbf{W}, \mathbf{W}')$ we have $(\mathbf{X}, \mathbf{X}')$ is independent of $(\mathbf{Z}, \mathbf{Z}')$, each row of $\mathbf{X}$ still has high min-entropy, and the "good" row $\mathbf{X}_j$ still has high min-entropy even given $\mathbf{X}'_j$. We now take a small slice $\mathbf{V}$ of $\mathbf{Z}$, and use it to extract from each row of $\mathbf{X}$ to obtain another matrix $\overline{\mathbf{X}}$. Similarly we also have a slice $\mathbf{V}'$ from $\mathbf{Z}'$ and obtain $\overline{\mathbf{X}'}$. We can now argue that conditioned on the fixing of $(\mathbf{V}, \mathbf{V}')$, $(\overline{\mathbf{X}}, \overline{\mathbf{X}'})$ is independent of $(\mathbf{Z}, \mathbf{Z}')$, each row of $\overline{\mathbf{X}}$ is close to uniform, and the "good" row $\overline{\mathbf{X}}_j$ is close to uniform even given $\overline{\mathbf{X}'}_j$. Moreover $\mathbf{Z}$ still has high min-entropy rate.

Thus, we have reduced this case to the case of an independence preserving merger with a tampered high min-entropy rate seed. We can therefore apply our NIPM to finish the construction. It is also not difficult to see that our construction can be extended to the case where we have $\mathbf{X}, \mathbf{X}^1, \ldots, \mathbf{X}^t$ instead of having just $\mathbf{X}$ and $\mathbf{X}'$.

2.4 Improved multi-source extractor

We can now apply our independence preserving merger with weak random seed to improve the multi-source extractor construction in [CS16]. Our construction follows the framework of that in [CS16], except that we replace their independence preserving merger with ours. Essentially, the key step in the construction of [CS16], and the only step which takes $O(1/\delta)$ independent $(n, \log^{1+\delta} n)$ sources (if we only aim at achieving constant or slightly sub-constant error) is to merge a matrix with $O(\log n)$ rows using $(n, \log^{1+\delta} n)$ sources. For this purpose and since the error of the merger needs to be $1/\text{poly}(n)$, the independence preserving merger in [CS16] uses two additional sources in each step to reduce the number of rows by a factor of $\log^{\delta} n$. Thus altogether it takes $2/\delta$ sources. Our merger as described above, in contrast, only requires *one* extra independent source with min-entropy at least $O(\log n) + 2^{O(\sqrt{\log \log n})} \log n = \log^{1+o(1)} n$. Therefore, we obtain a multi-source extractor for an absolute constant number of $(n, \log^{1+o(1)} n)$ sources, which outputs one bit with constant (or slightly sub-constant) error.

Organization We introduce some preliminaries in Section 3. We present our constructions of non-malleable independence preserving mergers and independence preserving mergers in Section 4. We use Section 5 to present the construction of our almost-optimal non-malleable extractor. Finally, we present our results on multi-source extractors in Section 6.

3 Preliminaries

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.
For a string y of length m, define the string $\text{Slice}(y, w)$ to be the prefix of length w of y.
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 $\mathbf{X}$.

3.1 Conditional Min-Entropy

Definition 3.1. *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 3.2 ([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 3.3 ([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 3.4. *A (k,ϵ)-seeded average case seeded extractor $\text{Ext} : \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^m$ for min-entropy k and error ϵ satisfies the following property: For any source $\mathbf{X}$ and any arbitrary random variable $\mathbf{Z}$ with $\tilde{H}_\infty(\mathbf{X}|\mathbf{Z}) \geq k$,*

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

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

Lemma 3.5 ([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.*

3.2 Some Probability Lemmas

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

Lemma 3.6. *Let $\mathbf{X}, \mathbf{Y}$ be random variables such that the random variable $\mathbf{Y}$ takes at ℓ values. Then*

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

Lemma 3.7 ([BIW06])**.** *Let $\mathbf{X}_1, \ldots, \mathbf{X}_\ell$ be independent random variables on $\{0,1\}^m$ such that $|\mathbf{X}_i - \mathbf{U}_m| \leq \epsilon$. Then, $|\sum_{i=1}^\ell \mathbf{X}_i - \mathbf{U}_m| \leq \epsilon^\ell$.*

3.3 Seeded Extractors

We use optimal constructions of strong-seeded extractors.

Theorem 3.8 ([GUV09])**.** *For any constant $\alpha > 0$, and all integers $n, k > 0$ there exists a polynomial time computable strong-seeded extractor $\text{Ext} : \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^m$ with $d = c_{3.8}(\log n + \log(1/\epsilon))$ and $m = (1-\alpha)k$.*

4 Non-Malleable Independence Preserving Mergers

In our proofs, we repeatedly condition on random variables with small support and account for entropy loss by implicitly using Lemma 3.3.

4.1 ℓ-Non-Malleable Independence Preserving Merger

In this section, we construct an explicit function NIPM that uses a (weak) seed $\mathbf{Y}$ to merge ℓ correlated r.v's $\mathbf{X}_1, \ldots, \mathbf{X}_\ell, \mathbf{X}'_1, \ldots, \mathbf{X}'_\ell$ in a way such that such that if for some i, $\mathbf{X}_i|\mathbf{X}'_i$'s is close to uniform on average, then this property is transferred to the output of NIPM. As discussed in the introduction, a recent work by Cohen and Schulman [CS16] introduces a similar object in the context of constructing multi-source extractors with nearly logarithmic min-entropy. However there are some important differences. To carry out the independence preserving merging, [CS16] uses access to multiple independent sources which are themselves not tampered. Here we allow access to an independent weak seed $\mathbf{Y}$ which is further subject to being tampered ($\mathbf{Y}'$ being the tampered seed).

The following is the main result of this section.

Theorem 4.1. *There exist constants $c_{4.1}, c'_{4.1} > 0$ such that for all integers $m, d, k_1, \ell > 0$ and any $\epsilon > 0$, with $m \geq d \geq k_1 > c_{4.1}\ell \log(n/\epsilon)$, there exists an explicit function ℓ-NIPM : $(\{0,1\}^m)^\ell \times \{0,1\}^d \to \{0,1\}^{m_1}$, $m_1 = 0.9(m - c_{4.1}\ell \log(m/\epsilon))$, such that if the following conditions hold:*

- *$\mathbf{X}_1, \ldots, \mathbf{X}_\ell$ are r.v's s.t for all $i \in [\ell]$, $|\mathbf{X}_i - \mathbf{U}_m| \leq \epsilon_1$, and $\mathbf{X}'_1, \ldots, \mathbf{X}'_\ell$ are r.v's with each $\mathbf{X}'_i$ supported on $\{0,1\}^m$.*
- *$\{\mathbf{Y}, \mathbf{Y}'\}$ is independent of $\{\mathbf{X}_1, \ldots, \mathbf{X}_t, \mathbf{X}'_1, \ldots, \mathbf{X}'_t\}$, s.t the r.v's $\mathbf{Y}, \mathbf{Y}'$ are both supported on $\{0,1\}^d$ and $H_\infty(\mathbf{Y}) \geq k_1$.*
- *there exists an $h \in [t]$ such that $|(\mathbf{X}_h, \mathbf{X}'_h) - (\mathbf{U}_m, \mathbf{X}'_h)| \leq \epsilon$,*

then

$$|\ell\text{-NIPM}((\mathbf{X}_1, \ldots, \mathbf{X}_\ell), \mathbf{Y}), \ell\text{-NIPM}((\mathbf{X}'_1, \ldots, \mathbf{X}'_\ell), \mathbf{Y}'), \mathbf{Y}, \mathbf{Y}' - \mathbf{U}_{m_1}, \ell\text{-NIPM}((\mathbf{X}'_1, \ldots, \mathbf{X}'_\ell), \mathbf{Y}'), \mathbf{Y}, \mathbf{Y}'| \leq c'_{4.1}\ell\epsilon$$

Our construction of NIPM uses the method of alternating extraction and extends it in a new way. Briefly we recall the method of alternating extraction which was introduced by Dziembowski and Pietrzak [DP07], and has been useful in a variety of extractor constructions [DW09, Li13a, Li15d, Coh15, CGL16, Li15b, CL16, Coh16a, Coh16b].

Alternating Extraction Assume that there are two parties, Quentin with a source $\mathbf{Q}$ and Wendy with a source $\mathbf{W}$. The alternating extraction 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 $\mathbf{R}_1$ using $\mathbf{W}$, and sends $\mathbf{R}_1$ 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 $\mathbf{S}_2$ from $\mathbf{Q}$ using $\mathbf{S}_1$, 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 r.v's is generated:

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

ℓ-Alternating Extraction We extend the above technique by letting Quentin have access to ℓ sources $\mathbf{Q}_1, \ldots, \mathbf{Q}_\ell$ (instead of just $\mathbf{Q}$) and ℓ strong-seeded extractors $\{\mathrm{Ext}_{q,i} : i \in [\ell]\}$ such that in the i'th round of the protocol, he uses $\mathbf{Q}_i$ to produce the r.v $\mathbf{S}_i = \mathrm{Ext}_{q,i}(\mathbf{Q}_i, \mathbf{R}_i)$. More formally, the following sequence of r.v's is generated: $\mathbf{S}_1 = \mathrm{Slice}(\mathbf{Q}_1, d), \mathbf{R}_1 = \mathrm{Ext}_w(\mathbf{W}, \mathbf{S}_1), \mathbf{S}_2 = \mathrm{Ext}_{q,2}(\mathbf{Q}_2, \mathbf{R}_1), \ldots, \mathbf{R}_{\ell-1} = \mathrm{Ext}_w(\mathbf{Q}_{\ell-1}, \mathbf{S}_{\ell-1}), \mathbf{S}_\ell = \mathrm{Ext}_{q,\ell}(\mathbf{Q}_\ell, \mathbf{R}_\ell)$. Define the look-ahead extractor

$$\ell\text{-laExt}((\mathbf{Q}_1, \ldots, \mathbf{Q}_\ell), \mathbf{W}) = \mathbf{S}_\ell.$$

We are now ready to prove Theorem 4.1.

Proof of Theorem 4.1. We instantiate the ℓ-look-ahead extractor described above with the following strong seeded extractors: Let $\mathrm{Ext}_1 : \{0,1\}^m \times \{0,1\}^{d_1} \to \{0,1\}^{d_1}$, $\mathrm{Ext}_2 : \{0,1\}^d \times \{0,1\}^{d_1} \to \{0,1\}^{d_1}$ and $\mathrm{Ext}_3 : \{0,1\}^m \times \{0,1\}^{d_1} \to \{0,1\}^{m_1}$ be explicit strong-seeded from Theorem 3.8 designed to extract from min-entropy $m/2, k_1/4, m - c_{4.1}\ell \log(m/\epsilon)$ respectively, each with error ϵ. Thus $d_1 = c_{3.8} \log(m/\epsilon)$.

We think of each $\mathbf{X}_i$ being uniform, and add back an error $\epsilon_1 \ell$ in the end.

For each $i \in [\ell - 1]$, let $\mathrm{Ext}_{q,i} = \mathrm{Ext}_1$, $\mathrm{Ext}_{q,\ell} = \mathrm{Ext}_3$ and $\mathrm{Ext}_w = \mathrm{Ext}_2$.

Define

$$\mathrm{NIPM}((\mathbf{X}_1, \ldots, \mathbf{X}_\ell), \mathbf{Y}) = \mathrm{laExt}((\mathbf{X}_1, \ldots, \mathbf{X}_\ell), \mathbf{Y}).$$

For any random variable $\mathbf{V} = f((\mathbf{X}_1, \ldots, \mathbf{X}_\ell), \mathbf{Y})$ (where f is an arbitrary deterministic function), let $\mathbf{V}' = f((\mathbf{X}'_1, \ldots, \mathbf{X}'_\ell), \mathbf{Y}')$.

We first prove the following claim.

Claim 4.2. *For any $j \in [h-1]$, conditioned on the r.v's $\{\mathbf{S}_i : i \in [j-1]\}, \{\mathbf{S}'_i : i \in [j-1]\}$, $\{\mathbf{R}_i : i \in [j-1]\}, \{\mathbf{R}'_i : i \in [j-1]\}$ the following hold:*

- *$\mathbf{S}_j$ is $2(j-1)\epsilon$-close to $\mathbf{U}_{d_1}$,*
- *$\mathbf{S}_j, \mathbf{S}'_j$ are deterministic functions of $\{\mathbf{X}_j, \mathbf{X}'_j\}$,*
- *for each $i \in [t]$, $\mathbf{X}_i$ has average conditional min-entropy at least $m - 2(j-1)d_1 - \log(1/\epsilon)$,*
- *$\mathbf{Y}$ has average conditional min-entropy at least $k_1 - 2(j-1)d_1 - \log(1/\epsilon)$,*
- *$\{\mathbf{X}_1, \ldots, \mathbf{X}_\ell, \mathbf{X}'_1, \ldots, \mathbf{X}'_\ell\}$ is independent of $\{\mathbf{Y}, \mathbf{Y}'\}$.*

Further, conditioned on the r.v's $\{\mathbf{S}_i : i \in [j]\}, \{\mathbf{S}'_i : i \in [j]\}, \{\mathbf{R}_i : i \in [j-1]\}, \{\mathbf{R}'_i : i \in [j-1]\}$ the following hold:

- *$\mathbf{R}_j$ is $(2j-1)\epsilon$-close to $\mathbf{U}_d$,*
- *$\mathbf{R}_j, \mathbf{R}'_j$ are deterministic functions of $\{\mathbf{Y}, \mathbf{Y}'\}$,*
- *for any $i \in [\ell]$, $\mathbf{X}_i$ has average conditional min-entropy at least $m - 2jd_1 - \log(1/\epsilon)$,*
- *$\mathbf{Y}$ has average conditional min-entropy at least $k_1 - 2(j-1)d_1 - \log(1/\epsilon)$,*
- *$\{\mathbf{X}_1, \ldots, \mathbf{X}_\ell, \mathbf{X}'_1, \ldots, \mathbf{X}'_\ell\}$ is independent of $\{\mathbf{Y}, \mathbf{Y}'\}$.*

Proof. We prove the above by induction on j. The base case when $j = 1$ is direct. Thus suppose $j > 1$. Fix the r.v's $\{\mathbf{S}_i : i \in [j-1]\}, \{\mathbf{S}'_i : i \in [j-1]\}, \{\mathbf{R}_i : i \in [j-2]\}, \{\mathbf{R}'_i : i \in [j-2]\}$. Using inductive hypothesis, it follows that

- $\mathbf{R}_{j-1}$ is $(2j-3)\epsilon$-close to $\mathbf{U}_d$,
- $\mathbf{R}_{j-1}, \mathbf{R}'_{j-1}$ are deterministic functions of $\{\mathbf{Y}, \mathbf{Y}'\}$,
- for any $i \in [t]$, $\mathbf{X}_i$ has average conditional min-entropy at least $m - 2(j-1)d_1 - \log(1/\epsilon)$,
- $\mathbf{Y}$ has average conditional min-entropy at least $k_1 - 2(j-2)d_1 - \log(1/\epsilon)$,
- $\{\mathbf{X}_1, \ldots, \mathbf{X}_\ell, \mathbf{X}'_1, \ldots, \mathbf{X}'_\ell\}$ is independent of $\{\mathbf{Y}, \mathbf{Y}'\}$.

Now since $\mathbf{S}_j = \mathrm{Ext}_1(\mathbf{X}_j, \mathbf{R}_{j-1})$, it follows that $\mathbf{S}_j$ is $2(j-1)\epsilon$-close to $\mathbf{U}_{d_1}$ on average conditioned on $\mathbf{R}_{j-1}$. We thus fix $\mathbf{R}_{j-1}$. Further, we also fix $\mathbf{R}'_{j-1}$ without affecting the distribution of $\mathbf{S}_j$. Thus $\mathbf{S}_j, \mathbf{S}'_j$ are now a deterministic function of $\mathbf{X}_j, \mathbf{X}'_j$. It follows that after these fixings, the average conditional min-entropy of $\mathbf{Y}$ is at least $k_1 - 2(j-2)d_1 - \log(1/\epsilon) - 2d_1 = k_1 - 2(j-1)d_1 - \log(1/\epsilon)$.

Next, we have $\mathbf{R}_j = \mathrm{Ext}_2(\mathbf{Y}, \mathbf{S}_j)$, and thus fixing $\mathbf{S}_j$, it follows that $\mathbf{R}_j$ is $(2j-1)\epsilon$-close to uniform on average. Further, since $\mathbf{R}_j$ is now a deterministic function of $\mathbf{Y}$, we fix $\mathbf{S}'_j$. As a result of these fixings, each $\mathbf{X}_i$ loses conditional min-entropy at most $2d_1$ on average. Since at each point, we either fix a r.v that is a deterministic function of either $\{\mathbf{X}_1, \ldots, \mathbf{X}_\ell, \mathbf{X}'_1, \ldots, \mathbf{X}_\ell\}$ or $\{\mathbf{Y}, \mathbf{Y}'\}$ it follows that $\{\mathbf{X}_1, \ldots, \mathbf{X}_\ell, \mathbf{X}'_1, \ldots, \mathbf{X}'_\ell\}$ remain independent of $\{\mathbf{Y}, \mathbf{Y}'\}$. This completes the inductive step, and hence the proof follows. □

We now proceed to prove the following claim.

Claim 4.3. *Conditioned on the r.v's $\{\mathbf{S}_i : i \in [h-1]\}, \{\mathbf{S}'_i : i \in [h]\}, \{\mathbf{R}_i : i \in [h-1]\}, \{\mathbf{R}'_i : i \in [h]\}$ the following hold:*

- *$\mathbf{S}_h$ is $2(h-1)\epsilon$-close to $\mathbf{U}_d$,*
- *$\mathbf{S}_h$ is a deterministic function of $\mathbf{X}_h$,*
- *for each $i \in [t]$, $\mathbf{X}_i$ has average conditional min-entropy at least $m - 2hd_1 - \log(1/\epsilon)$,*
- *$\mathbf{Y}$ has average conditional min-entropy at least $k_1 - 2hd_1 - \log(1/\epsilon)$,*
- *$\{\mathbf{X}_1, \ldots, \mathbf{X}_\ell, \mathbf{X}'_1, \ldots, \mathbf{X}'_\ell\}$ is independent of $\{\mathbf{Y}, \mathbf{Y}'\}$.*

Proof. We fix the r.v's $\{\mathbf{S}_i : i \in [h-1]\}, \{\mathbf{S}'_i : i \in [h-1]\}, \{\mathbf{R}_i : i \in [h-2]\}, \{\mathbf{R}'_i : i \in [h-2]\}$, and using Claim 4.2 the following hold:

- $\mathbf{R}_{h-1}$ is $(2h-3)\epsilon$-close to $\mathbf{U}_d$,
- $\mathbf{R}_{h-1}, \mathbf{R}'_{h-1}$ are deterministic functions of $\{\mathbf{Y}, \mathbf{Y}'\}$,
- for any $i \in [t]$, $\mathbf{X}_i$ has average conditional min-entropy at least $m - 2(h-1)d_1 - \log(1/\epsilon)$,
- $\mathbf{Y}$ has average conditional min-entropy at least $k_1 - 2(h-2)d_1 - \log(1/\epsilon)$,
- $\{\mathbf{X}_1, \ldots, \mathbf{X}_\ell, \mathbf{X}'_1, \ldots, \mathbf{X}'_\ell\}$ is independent of $\{\mathbf{Y}, \mathbf{Y}'\}$.

Next we claim that $\mathbf{X}_h$ has average conditional min-entropy at least $m - 2(h-1)d_1 - \log(1/\epsilon)$ even after fixing $\mathbf{X}'_h$. We know that before fixings any other r.v, we have $\mathbf{X}_h | \mathbf{X}'_h$ is ϵ-close to uniform on average. Since while computing the average conditional min-entropy, the order of fixing does

not matter, we can as well think of first fixing of $\mathbf{X}'_h$ and then fixing the r.v's $\{\mathbf{S}_i : i \in [h-1]\}$, $\{\mathbf{S}'_i : i \in [h-1]\}, \{\mathbf{R}_i : i \in [h-2]\}, \{\mathbf{R}'_i : i \in [h-2]\}$. Thus, it follows that the average conditional min-entropy of $\mathbf{X}_h$ is at least $m - 2(h-1)d_1 - \log(1/\epsilon)$.

We now show that even after fixing the r.v's $\mathbf{X}'_h, \mathbf{R}_{h-1}, \mathbf{R}'_{h-1}$, the r.v $\mathbf{S}_h$ is $2(h-1)\epsilon$-close to uniform on average. Fix $\mathbf{X}'_h$ and by the above argument $\mathbf{X}_h$ has average conditional min-entropy at least $m - 2(h-1)d_1 - \log(1/\epsilon)$. Since $\mathbf{S}_h = \mathrm{Ext}_1(\mathbf{X}_h, \mathbf{R}_{h-1})$, it follows that $\mathbf{S}_h$ is $2(h-1)\epsilon$-close to uniform on average even conditioned on $\mathbf{R}_{h-1}$. We fix $\mathbf{R}_{h-1}$, and thus $\mathbf{S}_h$ is a deterministic function of $\mathbf{X}_h$. Note that $\mathbf{S}'_h = \mathrm{Ext}_1(\mathbf{X}'_h, \mathbf{R}'_{h-1})$ is now a deterministic function of $\mathbf{R}'_h$ (and thus $\mathbf{Y}'$). Thus, we can fix $\mathbf{R}'_h$ (which also fixes $\mathbf{S}'_h$) without affecting the distribution of $\mathbf{S}_h$.

Observe that after the r.v's $\mathbf{R}_{h-1}, \mathbf{R}'_{h-1}$ are fixed, $\mathbf{S}'_h$ is a deterministic function of $\mathbf{X}'_h$. We only fix $\mathbf{S}'_h$ and do not fix $\mathbf{X}'_h$, and note that $\mathbf{S}_h$ is still $2(h-1)\epsilon$-close to uniform. Further after these fixings, each $\mathbf{X}_i$ has average conditional min-entropy at least $m - 2hd_1 - \log(1/\epsilon)$, and $\mathbf{Y}$ has average conditional min-entropy at least $k_1 - 2hd_1 - \log(1/\epsilon)$. □

By our construction of NIPM, Theorem 4.1 is direct from the following claim.

Claim 4.4. *For any $j \in [h, \ell]$, conditioned on the r.v's $\{\mathbf{S}_i : i \in [j-1]\}, \{\mathbf{S}'_i : i \in [j]\}, \{\mathbf{R}_i : i \in [j-1]\}, \{\mathbf{R}'_i : i \in [j]\}$ the following hold:*

- *$\mathbf{S}_j$ is $2(j-1)\epsilon$-close to $\mathbf{U}_d$,*
- *$\mathbf{S}_j$ is a deterministic function of $\mathbf{X}_j$*
- *for each $i \in [\ell]$, $\mathbf{X}_i$ has average conditional min-entropy at least $m - 2jd_1 - \log(1/\epsilon)$,*
- *$\mathbf{Y}$ has average conditional min-entropy at least $k_1 - 2jd_1 - \log(1/\epsilon)$,*
- *$\{\mathbf{X}_1, \ldots, \mathbf{X}_\ell, \mathbf{X}'_1, \ldots, \mathbf{X}'_\ell\}$ is independent of $\{\mathbf{Y}, \mathbf{Y}'\}$.*

Further, conditioned on the r.v's $\{\mathbf{S}_i : i \in [j]\}, \{\mathbf{S}'_i : i \in [j+1]\}, \{\mathbf{R}_i : i \in [j-1]\}, \{\mathbf{R}'_i : i \in [j]\}$ the following hold:

- *$\mathbf{R}_j$ is $(2j-1)\epsilon$-close to $\mathbf{U}_d$,*
- *$\mathbf{R}_j$ is a deterministic function of $\mathbf{Y}$,*
- *for any $i \in [\ell]$, $\mathbf{X}_i$ has average conditional min-entropy at least $m - 2(j+1)d_1 - \log(1/\epsilon)$,*
- *$\mathbf{Y}$ has average conditional min-entropy at least $k_1 - 2(j+1)d_1 - \log(1/\epsilon)$,*
- *$\{\mathbf{X}_1, \ldots, \mathbf{X}_\ell, \mathbf{X}'_1, \ldots, \mathbf{X}'_\ell\}$ is independent of $\{\mathbf{Y}, \mathbf{Y}'\}$.*

Proof. We prove this by induction on j. For the base case, when $j = h$, fix the r.v's $\{\mathbf{S}_i : i \in [h-1]\}$, $\{\mathbf{S}'_i : i \in [h]\}, \{\mathbf{R}_i : i \in [h-1]\}, \{\mathbf{R}'_i : i \in [h]\}$. Using Claim 4.3, it follows that

- $\mathbf{S}_h$ is $2(h-1)\epsilon$-close to $\mathbf{U}_d$,
- $\mathbf{S}_h$ is a deterministic function of $\mathbf{X}_h$,
- for each $i \in [\ell]$, $\mathbf{X}_i$ has average conditional min-entropy at least $m - 2hd_1 - \log(1/\epsilon)$,
- $\mathbf{Y}$ has average conditional min-entropy at least $k_1 - 2hd_1 - \log(1/\epsilon)$,

- $\{\mathbf{X}_1, \ldots, \mathbf{X}_\ell, \mathbf{X}'_1, \ldots, \mathbf{X}'_\ell\}$ is independent of $\{\mathbf{Y}, \mathbf{Y}'\}$.

Noting that $\mathbf{R}_h = Ext_2(\mathbf{Y}, \mathbf{S}_h)$, we fix $\mathbf{S}_h$ and $\mathbf{R}_h$ is $2h\epsilon$-uniform on average after this fixing. We note that $\mathbf{R}_h$ is now a deterministic function of $\mathbf{Y}$. Since $\mathbf{R}'_h$ is fixed, $\mathbf{S}'_{h+1}$ is a deterministic function of $\mathbf{X}'_{h+1}$, and we fix it without affecting the distribution of $\mathbf{R}_h$. The average conditional min-entropy of each $\mathbf{X}_i$ after these fixings is at least $m - 2(h+1)d_1 - \log(1/\epsilon)$. Further, we note that our fixings preserve the independence between $\{\mathbf{X}_1, \ldots, \mathbf{X}_\ell, \mathbf{X}'_1, \ldots, \mathbf{X}'_\ell\}$ and $\{\mathbf{Y}, \mathbf{Y}'\}$. This completes the proof of the base case.

Now suppose $j > h$. Fix the r.v's $\{\mathbf{S}_i : i \in [j-1]\}, \{\mathbf{S}'_i : i \in [j]\}, \{\mathbf{R}_i : i \in [j-2]\}$, $\{\mathbf{R}'_i : i \in [j-1]\}$. Using inductive hypothesis, it follows that

- $\mathbf{R}_{j-1}$ is $(2j-3)\epsilon$-close to $\mathbf{U}_d$,
- $\mathbf{R}_{j-1}$ is a deterministic function of $\mathbf{Y}$,
- for any $i \in [t]$, $\mathbf{X}_i$ has average conditional min-entropy at least $m - 2jd_1 - \log(1/\epsilon)$,
- $\mathbf{Y}$ has average conditional min-entropy at least $k_1 - 2jd_1 - \log(1/\epsilon)$,
- $\{\mathbf{X}_1, \ldots, \mathbf{X}_\ell, \mathbf{X}'_1, \ldots, \mathbf{X}'_\ell\}$ is independent of $\{\mathbf{Y}, \mathbf{Y}'\}$.

Using the fact that $\mathbf{S}_j = \mathrm{Ext}_1(\mathbf{X}_j, \mathbf{R}_{j-1})$, we fix $\mathbf{R}_{j-1}$ and $\mathbf{S}_j$ is $(2j-2)\epsilon$-close to uniform on average after this fixing. Further, $\mathbf{S}_j$ is a deterministic function of $\mathbf{X}_j$. Since $\mathbf{S}'_j$ is fixed, it follows that $\mathbf{R}'_j$ is a deterministic function of $\mathbf{Y}$ and we fix it without affecting the distribution of $\mathbf{S}_j$. We note that after these fixings, $\mathbf{Y}$ has average conditional min-entropy at least $k_1 - 2(j+1)d_1 - \log(1/\epsilon)$. Further, we note that our fixings preserve the independence between $\{\mathbf{X}_1, \ldots, \mathbf{X}_\ell, \mathbf{X}'_1, \ldots, \mathbf{X}'_\ell\}$ and $\{\mathbf{Y}, \mathbf{Y}'\}$.

Now, we fix $\mathbf{S}_j$ and it follows that $\mathbf{R}_j$ is a deterministic function of $\mathbf{Y}$ and is $(2j-1)\epsilon$-close to uniform on average. Further, since $\mathbf{R}'_j$ is fixed, it follows that $\mathbf{S}'_{j+1}$ is a deterministic function of $\mathbf{X}_{j+1}$ and we fix it without affecting the distribution of $\mathbf{R}_j$. The average conditional min-entropy of each $\mathbf{X}_i$ after these fixings is at least $m - 2(j+1)d_1 - \log(1/\epsilon)$. Further, we note that our fixings preserve the independence between $\{\mathbf{X}_1, \ldots, \mathbf{X}_\ell, \mathbf{X}'_1, \ldots, \mathbf{X}'_\ell\}$ and $\{\mathbf{Y}, \mathbf{Y}'\}$.

This completes the proof of inductive step, and hence the claim follows. □

□

4.2 (ℓ, t)-Non-Malleable Independence Preserving Merger

In this section, we generalize the construction of NIPM from Section 4 to handle multiple adversaries.

We first introduce some notation. For a random variable $\mathbf{V}$ supported on $a \times b$ matrices, we use $\mathbf{V}_i$ to denote the random variable corresponding to the i'th row of $\mathbf{V}$. Our main result in this section is the following theorem.

Theorem 4.5. *There exists constant $c_{4.5}, c'_{4.5} > 0$ such that for all integers $m, d, k_1, \ell, t > 0$ and any $\epsilon > 0$, with $m \geq d \geq k_1 > c_{4.5}(t+1)\ell \log(m/\epsilon)$, there exists an explicit function t-NIPM : $\{0,1\}^{m\ell} \times \{0,1\}^d \to \{0,1\}^{m_1}$, $m_1 = 0.9(m - c_{4.5}(t+1)\ell \log(m/\epsilon))$ such that if the following conditions hold:*

- $\mathbf{X}, \mathbf{X}^1, \ldots, \mathbf{X}^t$ *are r.v's, each supported on boolean* $\ell \times m$ *matrices s.t for any* $i \in [\ell]$, $|\mathbf{X}_i - \mathbf{U}_m| \leq \epsilon$,
- $\{\mathbf{Y}, \mathbf{Y}^1, \ldots, \mathbf{Y}^t\}$ *is independent of* $\{\mathbf{X}, \mathbf{X}^1, \ldots, \mathbf{X}^t\}$, *s.t* $\mathbf{Y}, \mathbf{Y}^1, \ldots, \mathbf{Y}^t$ *are each supported on* $\{0,1\}^d$ *and* $H_\infty(\mathbf{Y}) \geq k_1$.
- *there exists an* $h \in [\ell]$ *such that* $|(\mathbf{X}_h, \mathbf{X}_h^1, \ldots, \mathbf{X}_h^t) - (\mathbf{U}_m, \mathbf{X}_h^1, \ldots, \mathbf{X}_h^t)| \leq \epsilon$,

then

$$|(\ell,t)\text{-NIPM}((\mathbf{X},\mathbf{Y}),(\ell,t)\text{-NIPM}(\mathbf{X}^1,\mathbf{Y}^1),\ldots,(\ell,t)\text{-NIPM}(\mathbf{X}^t,\mathbf{Y}^t),\mathbf{Y},\mathbf{Y}^1,\ldots,\mathbf{Y}^t$$
$$-\mathbf{U}_{m_1},(\ell,t)\text{-NIPM}(\mathbf{X}^1,\mathbf{Y}^1),\ldots,(\ell,t)\text{-NIPM}(\mathbf{X}^t,\mathbf{Y}^t),\mathbf{Y},\mathbf{Y}^1,\ldots,\mathbf{Y}^t| \leq c'_{4.5}\ell\epsilon.$$

Proof. We instantiate the ℓ-look-ahead extractor described in Section 4.1 with the following strong-seeded extractors: Let $\text{Ext}_1 : \{0,1\}^m \times \{0,1\}^{d_1} \to \{0,1\}^{d_1}$, $\text{Ext}_2 : \{0,1\}^d \times \{0,1\}^{d_1} \to \{0,1\}^{d_1}$ and $\text{Ext}_3 : \{0,1\}^m \times \{0,1\}^{d_1} \to \{0,1\}^{m_1}$ be explicit strong-seeded from Theorem 3.8 designed to extract from min-entropy $k_1 = m/2, k_2 = d/2, k_3 = m - c_{4.5}(t+1)\log(m/\epsilon)$ respectively with error ϵ. Thus $d_1 = c_{3.8}\log(m/\epsilon)$.

For each $i \in [\ell - 1]$, let $\text{Ext}_{q,i} = \text{Ext}_1$, $\text{Ext}_{q,\ell} = \text{Ext}_3$ and $\text{Ext}_w = \text{Ext}_2$.

Define

$$t\text{-NIPM}((\mathbf{X}_1,\ldots,\mathbf{X}_\ell),\mathbf{Y}) = \ell\text{-laExt}((\mathbf{X}_1,\ldots,\mathbf{X}_\ell),\mathbf{Y}).$$

For any random variable $\mathbf{V} = f((\mathbf{X}_1,\ldots,\mathbf{X}_t),\mathbf{Y})$ (where f is an arbitrary deterministic function), let $\mathbf{V}^i = f((\mathbf{X}_1^i,\ldots,\mathbf{X}_\ell^i),\mathbf{Y}^i)$. The proof of correctness of the construction is similar in structure to Theorem 4.1, but requires more care to handle t adversaries.

We think of each $\mathbf{X}_i$ being uniform, and add back an error $\epsilon_1\ell$ in the end.

We begin by proving the following claim.

Claim 4.6. *For any* $j \in [h-1]$, *conditioned on the r.v's* $\{\mathbf{S}_i : i \in [j-1]\}, \{\mathbf{S}_i^g : i \in [j-1], g \in [t]\}$, $\{\mathbf{R}_i : i \in [j-1]\}, \{\mathbf{R}_i^g : i \in [j-1], g \in [t]\}$ *the following hold:*

- $\mathbf{S}_j$ *is* $2(j-1)\epsilon$*-close to* $\mathbf{U}_d$,
- $\mathbf{S}_j, \{\mathbf{S}_j^g : g \in [t]\}$ *are deterministic functions of* $\mathbf{X}, \{\mathbf{X}_j^g : g \in [t]\}$,
- *for each* $i \in [\ell]$, $\mathbf{X}_i$ *has average conditional min-entropy at least* $m-(t+1)(j-1)d_1-\log(1/\epsilon)$,
- $\mathbf{Y}$ *has average conditional min-entropy at least* $k_1 - 2(t+1)(j-1)d_1 - \log(1/\epsilon)$,
- $\{\mathbf{X}, \mathbf{X}^1, \ldots, \mathbf{X}^t\}$ *is independent of* $\{\mathbf{Y}, \mathbf{Y}^1, \ldots, \mathbf{Y}^t\}$.

Further, conditioned on the r.v's $\{\mathbf{S}_i : i \in [j]\}, \{\mathbf{S}_i^g : i \in [j], g \in [t]\}, \{\mathbf{R}_i : i \in [j-1]\}, \{\mathbf{R}_i^g : i \in [j-1], g \in [t]\}$ *the following hold:*

- $\mathbf{R}_j$ *is* $(2j-1)\epsilon$*-close to* $\mathbf{U}_d$,
- $\mathbf{R}_j, \{\mathbf{R}_j^g : g \in [t]\}$ *are deterministic functions of* $\mathbf{Y}, \{\mathbf{Y}^g : g \in [t]\}$,
- *for any* $i \in [\ell]$, $\mathbf{X}_i$ *has average conditional min-entropy at least* $m - (t+1)jd_1 - \log(1/\epsilon)$,
- $\mathbf{Y}$ *has average conditional min-entropy at least* $k_1 - (t+1)(j-1)d_1 - \log(1/\epsilon)$,

- $\{\mathbf{X}, \mathbf{X}^1, \ldots, \mathbf{X}^t\}$ *is independent of* $\{\mathbf{Y}, \mathbf{Y}^1, \ldots, \mathbf{Y}^t\}$.

Proof. In the course of the proof, we always maintain the property that the r.v's being fixed are either a deterministic function of $\{\mathbf{X}, \mathbf{X}^1, \ldots, \mathbf{X}^t\}$ or $\{\mathbf{Y}, \mathbf{Y}^1, \ldots, \mathbf{Y}^t\}$, and thus ensure $\{\mathbf{X}, \mathbf{X}^1, \ldots, \mathbf{X}^t\}$ is independent of $\{\mathbf{Y}, \mathbf{Y}^1, \ldots, \mathbf{Y}^t\}$.

We prove the claim by induction on j. The base case when $j = 1$ is direct. Thus suppose $j > 1$.

Fix the r.v's $\{\mathbf{S}_i : i \in [j-1]\}, \{\mathbf{S}_i^g : i \in [j-1], g \in [t]\}, \{\mathbf{R}_i : i \in [j-2]\}, \{\mathbf{R}_i^g : i \in [j-2], g \in [t]\}$. Using inductive hypothesis, it follows that

- $\mathbf{R}_{j-1}$ is $(2j-3)\epsilon$-close to $\mathbf{U}_{d_1}$,
- $\mathbf{R}_{j-1}, \mathbf{R}'_{j-1}$ are deterministic functions of $\{\mathbf{Y}, \mathbf{Y}'\}$,
- for any $i \in [\ell]$, $\mathbf{X}_i$ has average conditional min-entropy at least $m - (j-1)d_1 - \log(1/\epsilon)$,
- $\mathbf{Y}$ has average conditional min-entropy at least $k_1 - (j-2)d_1 - \log(1/\epsilon)$,
- $\{\mathbf{X}, \mathbf{X}^1, \ldots, \mathbf{X}^t\}$ is independent of $\{\mathbf{Y}, \mathbf{Y}^1, \ldots, \mathbf{Y}^t\}$.

Now since $\mathbf{S}_j = \mathrm{Ext}_1(\mathbf{X}_j, \mathbf{R}_{j-1})$, it follows that $\mathbf{S}_j$ is $2(j-1)\epsilon$-close to $\mathbf{U}_{d_1}$ on average conditioned on $\mathbf{R}_{j-1}$. We thus fix $\mathbf{R}_{j-1}$, and $\mathbf{S}_j$ is now a deterministic function of $\mathbf{X}$. Next, we fix $\{\mathbf{R}_{j-1}^g : g \in [t]\}$ without affecting the distribution of $\mathbf{S}_j$. Thus $\mathbf{S}_j, \mathbf{S}'_j$ are now a deterministic function of $\mathbf{X}, \mathbf{X}^1, \ldots, \mathbf{X}^t$. It follows that after these fixings, the average conditional min-entropy of $\mathbf{Y}$ is at least $k_1 - (j-2)(t+1)d_1 - \log(1/\epsilon) - (t+1)d_1 = k_1 - (j-1)(t+1)d_1 - \log(1/\epsilon)$.

Next, we have $\mathbf{R}_j = \mathrm{Ext}_2(\mathbf{Y}, \mathbf{S}_j)$, and thus fixing $\mathbf{S}_j$, it follows that $\mathbf{R}_j$ is $(2j-1)\epsilon$-close to uniform on average. Further, since $\mathbf{R}_j$ is now a deterministic function of $\mathbf{Y}$, we fix $\{\mathbf{S}_j^g : g \in [t]\}$. As a result of these fixings, each $\mathbf{X}_i$ loses conditional min-entropy at most $2(t+1)d_1$ on average. This completes the inductive step, and hence the proof follows. □

Claim 4.7. *Conditioned on the r.v's* $\{\mathbf{S}_i : i \in [h-1]\}, \{\mathbf{S}_i^g : i \in [h], g \in [t]\}, \{\mathbf{R}_i : i \in [h-1]\}$, $\{\mathbf{R}_i^g : i \in [h], g \in [t]\}$ *the following hold:*

- $\mathbf{S}_h$ *is* $2(h-1)\epsilon$*-close to* $\mathbf{U}_d$,
- $\mathbf{S}_h$ *is a deterministic function of* $\mathbf{X}_h$,
- *for each* $i \in [t]$, $\mathbf{X}_i$ *has average conditional min-entropy at least* $m - (t+1)hd_1 - \log(1/\epsilon)$,
- $\mathbf{Y}$ *has average conditional min-entropy at least* $k_1 - (t+1)hd_1 - \log(1/\epsilon)$,
- $\{\mathbf{X}, \mathbf{X}^1, \ldots, \mathbf{X}^t\}$ *is independent of* $\{\mathbf{Y}, \mathbf{Y}^1, \ldots, \mathbf{Y}^t\}$.

Proof. We fix the r.v's $\{\mathbf{S}_i : i \in [h-1]\}, \{\mathbf{S}_i^g : i \in [h-1], g \in [t]\}, \{\mathbf{R}_i : i \in [h-2]\}, \{\mathbf{R}_i^g : i \in [h-2], g \in [t]\}$, and using Claim 4.6 the following hold:

- $\mathbf{R}_{h-1}$ is $(2h-3)\epsilon$-close to $\mathbf{U}_d$,
- $\mathbf{R}_{h-1}, \{\mathbf{R}_{h-1}^g : g \in [t]\}$ are deterministic functions of $\mathbf{Y}, \{\mathbf{Y}^g : g \in [t]\}$,
- for any $i \in [\ell]$, $\mathbf{X}_i$ has average conditional min-entropy at least $m - (t+1)(h-1)d_1 - \log(1/\epsilon)$,
- $\mathbf{Y}$ has average conditional min-entropy at least $k_1 - (t+1)(h-2)d_1 - \log(1/\epsilon)$,

- $\{\mathbf{X}, \mathbf{X}^1, \ldots, \mathbf{X}^t\}$ is independent of $\{\mathbf{Y}, \mathbf{Y}^1, \ldots, \mathbf{Y}^t\}$.

Next we claim that $\mathbf{X}_h$ has average conditional min-entropy at least $m-(h-1)(t+1)d_1-\log(1/\epsilon)$ even after fixing $\{\mathbf{X}_h^g : g \in [t]\}$. Before fixings any other r.v, we have $\mathbf{X}_h|\{\mathbf{X}_h^g : g \in [t]\}$ is ϵ-close to uniform on average. Since while computing the average conditional min-entropy, the order of fixing does not matter, we can as well think of first fixing of $\{\mathbf{X}_h^g : g \in [t]\}$ and then fixing the r.v's $\{\mathbf{S}_i : i \in [h-1]\}, \{\mathbf{S}'_i : i \in [h-1]\}, \{\mathbf{R}_i : i \in [h-2]\}, \{\mathbf{R}'_i : i \in [h-2]\}$. Thus, it follows that the average conditional min-entropy of $\mathbf{X}_h$ is at least $m-(t+1)(h-1)d_1-\log(1/\epsilon)$.

We now prove that even after fixing the r.v's $\{\mathbf{X}_h^g : g \in [t]\}, \mathbf{R}_{h-1}, \{\mathbf{R}_{h-1}^g : g \in [t]\}$, the r.v $\mathbf{S}_h$ is $2(h-1)\epsilon$-close to uniform on average. Fix $\{\mathbf{X}_h^g : g \in [t]\}$ and by the above argument $\mathbf{X}_h$ has average conditional min-entropy at least $m-(t+1)(h-1)d_1-\log(1/\epsilon)$. Since $\mathbf{S}_h = \mathrm{Ext}_1(\mathbf{X}_h, \mathbf{R}_{h-1})$, it follows that $\mathbf{S}_h$ is $2(h-1)\epsilon$-close to uniform on average conditioned on $\mathbf{R}_{h-1}$. We fix $\mathbf{R}_{h-1}$, and thus $\mathbf{S}_h$ is now a deterministic function of $\mathbf{X}_h$. Note that $\mathbf{S}_h^g = \mathrm{Ext}_1(\mathbf{X}_h^g, \mathbf{R}_{h-1}^g)$ is now a deterministic function of $\mathbf{R}_h^g$ (and thus $\mathbf{Y}^g$). Thus, we can fix $\{\mathbf{R}_h^g : g \in [t]\}$ (which also fixes $\{\mathbf{S}_h^g : g \in [t]\}$) without affecting the distribution of $\mathbf{S}_h$.

Observe that once the r.v's $\mathbf{R}_{h-1}, \{\mathbf{R}_{h-1}^g : g \in [t]\}$ are fixed, $\{\mathbf{S}_h^g : g \in [t]\}$ is a deterministic function of $\{\mathbf{X}_h^g : g \in [t]\}$. We fix $\{\mathbf{S}_h^g : g \in [t]\}$ and do not fix $\{\mathbf{X}_h^g : g \in [t]\}$, and note that $\mathbf{S}_h$ is still $2(h-1)\epsilon$-close to uniform. Further after these fixings, each $\mathbf{X}_i$ has average conditional min-entropy at least $m-(t+1)hd_1-\log(1/\epsilon)$, and $\mathbf{Y}$ has average conditional min-entropy at least $k_1-(t+1)hd_1-\log(1/\epsilon)$. □

Theorem 4.5 follows directly from the following claim.

Claim 4.8. *For any $j \in [h, \ell]$, conditioned on the r.v's $\{\mathbf{S}_i : i \in [j-1]\}, \{\mathbf{S}_i^g : i \in [j], g \in [t]\}$, $\{\mathbf{R}_i : i \in [j-1]\}, \{\mathbf{R}_i^g : i \in [j], g \in [t]\}$ the following hold:*

- *$\mathbf{S}_j$ is $2(j-1)\epsilon$-close to $\mathbf{U}_d$,*
- *$\mathbf{S}_j$ is a deterministic function of $\mathbf{X}_j$*
- *for each $i \in [\ell]$, $\mathbf{X}_i$ has average conditional min-entropy at least $m-(t+1)(j+1)d_1-\log(1/\epsilon)$,*
- *$\mathbf{Y}$ has average conditional min-entropy at least $k_1-(t+1)jd_1-\log(1/\epsilon)$,*
- *$\{\mathbf{X}, \mathbf{X}^1, \ldots, \mathbf{X}^t\}$ is independent of $\{\mathbf{Y}, \mathbf{Y}^1, \ldots, \mathbf{Y}^t\}$.*

Further, conditioned on the r.v's $\{\mathbf{S}_i : i \in [j]\}, \{\mathbf{S}_i^g : i \in [j+1], g \in [t]\}, \{\mathbf{R}_i : i \in [j-1]\}$, $\{\mathbf{R}_i^g : i \in [j], g \in [t]\}$ the following hold:

- *$\mathbf{R}_j$ is $(2j-1)\epsilon$-close to $\mathbf{U}_d$,*
- *$\mathbf{R}_j$ is a deterministic function of $\mathbf{Y}$,*
- *for any $i \in [\ell]$, $\mathbf{X}_i$ has average conditional min-entropy at least $m-(t+1)(j+1)d_1-\log(1/\epsilon)$,*
- *$\mathbf{Y}$ has average conditional min-entropy at least $k_1-(t+1)jd_1-\log(1/\epsilon)$,*
- *$\{\mathbf{X}, \mathbf{X}^1, \ldots, \mathbf{X}^t\}$ is independent of $\{\mathbf{Y}, \mathbf{Y}^1, \ldots, \mathbf{Y}^t\}$.*

Proof. We prove this by induction on j. For the base case, when $j=h$, fix the r.v's $\{\mathbf{S}_i : i \in [h-1]\}$, $\{\mathbf{S}_i^g : i \in [h], g \in [t]\}, \{\mathbf{R}_i : i \in [h-1]\}, \{\mathbf{R}_i^g : i \in [h], g \in [t]\}$. Using Claim 4.7, it follows that

- $\mathbf{S}_h$ is $2(h-1)\epsilon$-close to $\mathbf{U}_d$,
- $\mathbf{S}_h$ is a deterministic function of $\mathbf{X}_h$,
- for each $i \in [\ell]$, $\mathbf{X}_i$ has average conditional min-entropy at least $m - (t+1)hd_1 - \log(1/\epsilon)$,
- $\mathbf{Y}$ has average conditional min-entropy at least $d - (t+1)hd_1 - \log(1/\epsilon)$,
- $\{\mathbf{X}, \mathbf{X}^1, \ldots, \mathbf{X}^t\}$ is independent of $\{\mathbf{Y}, \mathbf{Y}^1, \ldots, \mathbf{Y}^t\}$.

Noting that $\mathbf{R}_h = \mathrm{Ext}_2(\mathbf{Y}, \mathbf{S}_h)$, we fix $\mathbf{S}_h$ and $\mathbf{R}_h$ is $2h\epsilon$-uniform on average after this fixing. We note that $\mathbf{R}_h$ is now a deterministic function of $\mathbf{Y}$. Since $\{\mathbf{R}_h^g : g \in [t]\}$ is fixed, $\{\mathbf{S}_{h+1}^g : g \in [t]\}$ is a deterministic function of $\{\mathbf{X}_{h+1}^g : g \in [t]\}$, and we fix it without affecting the distribution of $\mathbf{R}_h$. The average conditional min-entropy of each $\mathbf{X}_i$ after these fixings is at least $m-(t+1)(h+1)d_1-\log(1/\epsilon)$.

Now suppose $j > h$. Fix the r.v's $\{\mathbf{S}_i : i \in [j-1]\}, \{\mathbf{S}_i^g : i \in [j], g \in [t]\}, \{\mathbf{R}_i : i \in [j-2]\}$, $\{\mathbf{R}_i^g : i \in [j-1], g \in [t]\}$. By inductive hypothesis, the following hold:

- $\mathbf{R}_{j-1}$ is $(2j-3)\epsilon$-close to $\mathbf{U}_d$,
- $\mathbf{R}_{j-1}$ is a deterministic function of $\mathbf{Y}$,
- for any $i \in [\ell]$, $\mathbf{X}_i$ has average conditional min-entropy at least $m - (t+1)jd_1 - \log(1/\epsilon)$,
- $\mathbf{Y}$ has average conditional min-entropy at least $k_1 - (t+1)(j-1)d_1 - \log(1/\epsilon)$,
- $\{\mathbf{X}, \mathbf{X}^1, \ldots, \mathbf{X}^t\}$ is independent of $\{\mathbf{Y}, \mathbf{Y}^1, \ldots, \mathbf{Y}^t\}$.

Using the fact that $\mathbf{S}_j = \mathrm{Ext}_1(\mathbf{X}_j, \mathbf{R}_{j-1})$, we fix $\mathbf{R}_{j-1}$ and $\mathbf{S}_j$ is $(2j-2)\epsilon$-close to uniform on average after this fixing. Further, $\mathbf{S}_j$ is a deterministic function of $\mathbf{X}_j$. Since $\{\mathbf{S}_j^g : g \in [t]\}$ is fixed, it follows that $\{\mathbf{R}_j^g : g \in [t]\}$ is a deterministic function of $\mathbf{Y}$ and we fix it without affecting the distribution of $\mathbf{S}_j$. We note that after these fixings, $\mathbf{Y}$ has average conditional min-entropy at least $k_1 - (t+1)jd_1 - \log(1/\epsilon)$.

Now, we fix $\mathbf{S}_j$ and it follows that $\mathbf{R}_j$ is a deterministic function of $\mathbf{Y}$ and is $(2j-1)\epsilon$-close to uniform on average. Further, since $\{\mathbf{R}_j^g : g \in [t]\}$ is fixed, it follows that $\{\mathbf{S}_{j+1}^g : g \in [t]\}$ is a deterministic function of $\mathbf{X}_{j+1}$ and we fix it without affecting the distribution of $\mathbf{R}_j$. The average conditional min-entropy of each $\mathbf{X}_i$ after these fixings is at least $m - (t+1)jd_1 - \log(1/\epsilon)$.

This completes proof of the inductive step, and the claim now follows. □

□

4.3 A Recursive Non-Malleable Independence Preserving Merger

In this section, we show a recursive way of applying the (ℓ, t)-NIPM constructed in the previous section in order to achieve better trade-off between parameters. This object is crucial in obtaining our near optimal non-malleable extractor construction.

Notation: For an $a \times b$ matrix $\mathbf{V}$, and any $S \subseteq [a]$, let $\mathbf{V}_S$ denote the matrix obtained by restricting $\mathbf{V}$ to the rows indexed by S.

Our main result in this section is the following theorem.

Theorem 4.9. *For all integers $m, \ell, L, t > 0$, any $\epsilon > 0$, $r = \lceil \frac{\log L}{\log \ell} \rceil$ and any $d = (c_{4.5}\ell \log(m/\epsilon) + d')(t+2)^{r+1}$, there exists an explicit function (L,ℓ,t)-NIPM : $\{0,1\}^{mL} \times \{0,1\}^d \to \{0,1\}^{m'}$, $m' = (0.9)^r(m - c_{4.5}\ell(t+1)r\log(m/\epsilon))$, such that if the following conditions hold:*

- *$\mathbf{X}, \mathbf{X}^1, \ldots, \mathbf{X}^t$ are r.v's, each supported on boolean $L \times m$ matrices s.t for any $i \in [L]$, $|\mathbf{X}_i - \mathbf{U}_m| \leq \epsilon$,*
- *$\{\mathbf{Y}, \mathbf{Y}^1, \ldots, \mathbf{Y}^t\}$ is independent of $\{\mathbf{X}, \mathbf{X}^1, \ldots, \mathbf{X}^t\}$, s.t $\mathbf{Y}, \mathbf{Y}^1, \ldots, \mathbf{Y}^t$ are each supported on $\{0,1\}^d$ and $H_\infty(\mathbf{Y}) \geq d - d'$,*
- *there exists an $h \in [\ell]$ such that $|(\mathbf{X}_h, \mathbf{X}^1_h, \ldots, \mathbf{X}^t_h) - (\mathbf{U}_m, \mathbf{X}^1_h, \ldots, \mathbf{X}^t_h)| \leq \epsilon$,*

then

$$|(L,\ell,t)\text{-NIPM}((\mathbf{X},\mathbf{Y}), (L,\ell,t)\text{-NIPM}(\mathbf{X}^1,\mathbf{Y}^1), \ldots, (L,\ell,t)\text{-NIPM}(\mathbf{X}^t,\mathbf{Y}^t), \mathbf{Y}, \mathbf{Y}^1, \ldots, \mathbf{Y}^t$$
$$-\mathbf{U}_{m_1}, (L,\ell,t)\text{-NIPM}(\mathbf{X}^1,\mathbf{Y}^1), \ldots, (L,\ell,t)\text{-NIPM}(\mathbf{X}^t,\mathbf{Y}^t), \mathbf{Y}, \mathbf{Y}^1, \ldots, \mathbf{Y}^t| \leq 2c'_{4.5}L\epsilon.$$

Proof. We set up parameters and ingredients required in our construction.

- For $i \in [r]$, let $L_i = \lceil \frac{L}{\ell^i} \rceil$.
- Let $d_1 = d' + \log(1/\epsilon) + c_{4.5}(t+1)\ell\log(m/\epsilon)$. For $i \in [r]$, let $d_i = (t+2)d_{i-1}$.
- Let $m_0 = m$. For $i \in [r]$, define $m_i = 0.9^i(m - ic_{4.5}(t+1)\ell\log(m/\epsilon))$
- For each $i \in [r]$, let (ℓ,t)-NIPM$_i$: $\{0,1\}^{\ell m_i} \times \{0,1\}^{d_i} \to \{0,1\}^{m_{i+1}}$ be an instantiation of the function from Theorem 4.5 with error parameter ϵ.

Algorithm 1: (L,ℓ,t)-NIPM(x,y)

Input: x is a boolean $L \times m$ matrix, and y is a bit string of length d.
Output: A bit string of length m_r.

```
Let x[0] = x.
for i = 1 to r do
    Let y[i] = Slice(y, d_i)
    Let x[i] be a L_i × m_i matrix, whose j'th row x[i]_j = (ℓ,t)-NIPM_i(x[i−1]_{[(j−1)ℓ+1, jℓ]}, y[i])
end
Ouput x[r].
```

We prove the following claim from which it is direct that the function (L,ℓ,t)-NIPM computed by Algorithm 1 satisfies the conclusion of Theorem 4.9. Let $\epsilon_0 = \epsilon$, and for $i \in [r]$, let $\epsilon_i = \ell\epsilon_{i-1} + c'_{4.5}\ell\epsilon$.

Claim 4.10. *For all $i \in [r]$, conditioned on the r.v's $\{\mathbf{Y}[j] : j \in [i]\}, \{\mathbf{Y}^g[j] : j \in [i], g \in [t]\}$, the following hold:*

- *$\mathbf{X}[i], \mathbf{X}^1[i], \ldots, \mathbf{X}^t[i]$ are r.v's, each supported on boolean $L_i \times m_i$ matrices s.t for any $j \in [L_i]$, $|\mathbf{X}[i]_j - \mathbf{U}_{m_i}| \leq (c'_{4.5}\ell)^i\epsilon$,*
- *$\{\mathbf{Y}, \mathbf{Y}^1, \ldots, \mathbf{Y}^t\}$ is independent of $\{\mathbf{X}[i], \mathbf{X}[i]^1, \ldots, \mathbf{X}[i]^t\}$.*
- *there exists an $h_i \in [L_i]$ such that $\mathbf{X}[i]_h | \{\mathbf{X}[i]^1_h, \ldots, \mathbf{X}[i]^t_h\}$ is ϵ_i-close to $\mathbf{U}_{m_i}$ on average,*

- $\mathbf{Y}$ *has average conditional min-entropy at least* $d - d_{i+1} + c_{4.5}(t+1)\ell\log(m/\epsilon)$.

Proof. We prove this claim by an induction on i. The base case, when $i = 0$, is direct. Thus suppose $i \geq 1$. Fix the *r.v*'s $\{\mathbf{Y}[j] : j \in [i-1]\}, \{\mathbf{Y}^g[j] : j \in [i-1], g \in [t]\}$. By inductive hypothesis, it follows that

- $\mathbf{X}[i-1], \mathbf{X}^1[i-1], \ldots, \mathbf{X}^t[i-1]$ are r.v's each supported on boolean $L_{i-1} \times m_{i-1}$ matrices s.t for any $j \in [L_{i-1}]$, $|\mathbf{X}[i-1]_j - \mathbf{U}_{m-1}| \leq (c'_{4.5}\ell)^{i-1}\epsilon$,
- $\{\mathbf{Y}[i-1], \mathbf{Y}^1[i-1], \ldots, \mathbf{Y}^t[i-1]\}$ is independent of $\{\mathbf{X}[i-1], \mathbf{X}[i-1]^1, \ldots, \mathbf{X}[i-1]^t\}$.
- $h_i \in [L_i]$ such that $\mathbf{X}[i-1]_h | \{\mathbf{X}[i-1]^1_h, \ldots, \mathbf{X}[i-1]^t_h\}$ is ϵ_{i-1}-close to $\mathbf{U}_{m_{i-1}}$ on average,
- $\mathbf{Y}$ has average conditional min-entropy at least $d - d_i + c_{4.5}(t+1)\ell\log(m/\epsilon)$.

Thus the r.v $\mathbf{Y}[i] = \text{Slice}(\mathbf{Y}, d_i)$ has average conditional min-entropy at least $c_{4.5}(t+1)\ell\log(n/\epsilon)$. Let $h_i \in [\ell(h_i - 1) + 1, \ell h_i]$, for some $h_i \in [L_i]$. By Claim 4.6, it follows that conditioned on the r.v's $\mathbf{Y}[i], \{\mathbf{Y}^g[i] : g \in [t]\}$, for any $j \in [L_i]$, $|\mathbf{X}[i]_j - \mathbf{U}_m| \leq \ell\epsilon_{i-1} + c'_{4.5}\ell\epsilon = \epsilon_i$.

Further, using Theorem 4.5, conditioned on $\mathbf{Y}[i], \{\mathbf{Y}^g[i] : g \in [t]\}, \{\mathbf{X}^g[i]_{h_i} : g \in [t]\}$, the r.v $\mathbf{X}[i]_{h_i}$ is $\ell\epsilon_{i-1} + c'_{4.5}\ell\epsilon$-close to uniform on average.

Thus, we fix the r.v's $\mathbf{Y}[i], \{\mathbf{Y}^g[i] : g \in [t]\}$, and note that $\mathbf{Y}$ still has average conditional min-entropy at least $d - d_i + c_{4.5}(t+1)\ell\log(m/\epsilon) - (t+1)d_i \geq d - d_{i+1} + c_{4.5}(t+1)\ell\log(m/\epsilon)$. This completes the proof of the inductive step, and the theorem follows. □

□

4.4 An Independence Preserving Merger Using a Weak Source

In this section, we show a way of using the (L, ℓ, t)-NIPM constructed in the Section 4.3 to merge the r.v's $\mathbf{X}, \mathbf{X}^1, \ldots, \mathbf{X}^t$, each supported on boolean $L \times m$ matrices, with the guarantee that there is some $h \in [L]$ s.t $\mathbf{X}_h$ is uniform on average conditioned on $\{\mathbf{X}^g_h : g \in [t]\}$ using an independent (n, k)-source $\mathbf{Y}$ (instead of a seed as in the previous section). We note that our construction provides a direct improvement in terms of parameters over [CS16], and further uses just 1 independent source. In Section 6, we use this new merger to improve upon the results on multi-source extractors obtained in [CS16].

We use the following notation, as introduced before.

Notation: For an $a \times b$ matrix $\mathbf{V}$, and any $S \subseteq [a]$, let $\mathbf{V}_S$ denote the matrix obtained by restricting $\mathbf{V}$ to the rows indexed by S.

Our main result in this section is the following theorem. We reuse the constants $c_{4.5}, c'_{4.5}$ from Theorem 4.5.

Theorem 4.11. *For all integers* $m, \ell, L, t > 0$, *any* $\epsilon > 0$, $r = \lceil \frac{\log L}{\log \ell} \rceil$ *and any* $k \geq 2c_{4.5}\ell\log(m/\epsilon)(t+2)^{r+2}$, *there exists an explicit function* (L, ℓ, t)-IPM $: \{0,1\}^{mL} \times \{0,1\}^n \to \{0,1\}^{m''}$, $m'' = 0.9^{r+1}(m - c_{4.5}\ell(t+1)r\log(m/\epsilon) - c_{3.8}(t+2)\log(n/\epsilon)))$, *such that if the following conditions hold:*

- $\mathbf{X}, \mathbf{X}^1, \ldots, \mathbf{X}^t$ *are r.v's, each supported on boolean* $L \times m$ *matrices s.t for any* $i \in [L]$, $|\mathbf{X}_i - \mathbf{U}_m| \leq \epsilon$,
- $\mathbf{Y}$ *is an* (n, k)*-source, independent of* $\{\mathbf{X}, \mathbf{X}^1, \ldots, \mathbf{X}^t\}$.

- *there exists an* $h \in [\ell]$ *such that* $|(\mathbf{X}_h, \mathbf{X}_h^1, \ldots, \mathbf{X}_h^t) - (\mathbf{U}_m, \mathbf{X}_h^1, \ldots, \mathbf{X}_h^t)| \leq \epsilon$,

then

$$|(L,\ell,t)\text{-IPM}(\mathbf{X},\mathbf{Y}), (L,\ell,t)\text{-IPM}(\mathbf{X}^1,\mathbf{Y}), \ldots, (L,\ell,t)\text{-NIPM}(\mathbf{X}^t,\mathbf{Y}) \\ -\mathbf{U}_{m''}, (L,\ell,t)\text{-IPM}(\mathbf{X}^1,\mathbf{Y}), \ldots, (L,\ell,t)\text{-IPM}(\mathbf{X}^t,\mathbf{Y})| \leq 3c'_{4.5} L\epsilon.$$

Proof. We set up parameters and ingredients required in our construction.

- Let $d = 0.8k, d' = c_{3.8}\log(m/\epsilon), d_1 = c_{3.8}\log(n/\epsilon)$.
- Let $\text{Ext}_1 : \{0,1\}^n \times \{0,1\}^{d_1} \to \{0,1\}^d$ be a (k,ϵ)-strong-seeded extractor from Theorem 3.8.
- Let $\text{Ext}_2 : \{0,1\}^m \times \{0,1\}^{d'} \to \{0,1\}^{m'}$, $m' = 0.9(m - c_{3.8}(t+1)\log(n/\epsilon))$, be a $(m - c_{3.8}(t+1)\log(n/\epsilon), \epsilon)$-strong-seeded extractor from Theorem 3.8.
- Let (L,ℓ,t)-NIPM : $\{0,1\}^{Lm'} \times \{0,1\}^d \to \{0,1\}^{m''}$ be the function from Theorem 4.9 with error parameter ϵ.

Algorithm 2: (L,ℓ,t)-IPM(x,y)

Input: x is a boolean $L \times m$ matrix, and y is a bit string of length n.
Output: A bit string of length m''.

1 Let $w = \text{Slice}(x_1, d_1)$
2 Let $z = \text{Ext}_1(y, w)$.
3 Let $v = \text{Slice}(z, d')$.
4 Let $\overline{v}$ be a $L \times m'$-matrix, whose i'th row is given by $\overline{v}_i = \text{Ext}_2(x_i, v)$.
5 Output $\overline{z} = (L,\ell,t)$-NIPM$(\overline{v}, z)$.

We begin by proving the following claim.

Claim 4.12. *Conditioned on* $\mathbf{W}, \{\mathbf{W}^g : g \in [t]\}$, *the following hold:*

- $\mathbf{Z}$ *is* ϵ*-close to* $\mathbf{U}_d$,
- $\mathbf{Z}, \{\mathbf{Z}^g : g \in [t]\}$ *is independent of* $\mathbf{X}, \{\mathbf{X}^g : g \in [t]\}$,
- *For each* $i \in [L]$, $\mathbf{X}_i$ *has average conditional min-entropy at least* $m - (t+2)\log(n/\epsilon)$,
- $\mathbf{X}_h | \{\mathbf{X}_h^g : g \in [t]\}$ *has average conditional min-entropy at least* $m - (t+2)d_1\log(n/\epsilon)$.

Proof. Since Ext_1 is a strong extractor, we can fix $\mathbf{W}$, and $\mathbf{Z}$ is ϵ-close to $\mathbf{U}_d$ on average. Further, $\mathbf{Z}$ is now a deterministic function of $\mathbf{X}_1$. Thus, we can fix $\{\mathbf{W}^1, \ldots, \mathbf{W}^t\}$, without affecting the distribution of $\mathbf{Z}$. Since $\mathbf{W}^i$ is on d_1 bits, and without any prior conditioning since $\mathbf{X} | \{\mathbf{X}_h^g : g \in [t]\}$ is ϵ-close to uniform on average, it follows that conditioned on $\{\mathbf{X}_h^g : g \in [t]\}, \mathbf{W}, \{\mathbf{W}^g : g \in [t]\}$, the r.v $\mathbf{X}_h$ has average conditional min-entropy $m - (t+1)d_1\log(n/\epsilon) - \log(1/\epsilon)$. □

Claim 4.13. *Conditioned on* $\mathbf{W}, \{\mathbf{W}^g : g \in [t]\}, \mathbf{V}, \{\mathbf{V}^g : g \in [t]\}$, *the following hold:*

- $\{\mathbf{Z}, \mathbf{Z}^1, \ldots, \mathbf{Z}^t\}$ *is independent of* $\{\mathbf{X}, \mathbf{X}^1, \ldots, \mathbf{X}^t\}$,

- $\{\overline{\mathbf{V}}, \overline{\mathbf{V}}^1, \ldots, \overline{\mathbf{V}}^t\}$ *is a deterministic function of* $\{\mathbf{X}, \mathbf{X}^1, \ldots, \mathbf{X}^t\}$,
- *For each* $i \in [L]$, $\overline{\mathbf{V}}_i$ *is* 2ϵ*-close to uniform,*
- $\overline{\mathbf{V}}_h | \{\overline{\mathbf{V}}_h^g : g \in [t]\}$ *is* 2ϵ*-close to uniform on average.*
- $\mathbf{Z}$ *has average conditional min-entropy at least* $d - (t+2)\log(m/\epsilon)$.

Proof. Fix $\mathbf{W}, \{\mathbf{W}^g : g \in [t]\}$. Thus, by Claim 4.12, we have

- $\mathbf{Z}$ is ϵ-close to $\mathbf{U}_d$,
- $\mathbf{Z}, \{\mathbf{Z}^g : g \in [t]\}$ is independent of $\mathbf{X}, \{\mathbf{X}^g : g \in [t]\}$,
- For each $i \in [L]$, $\mathbf{X}_i$ has average conditional min-entropy at least $m - (t+2)\log(n/\epsilon)$,
- $\mathbf{X}_h | \{\mathbf{X}_h^g : g \in [t]\}$ has average conditional min-entropy at least $m - (t+2)\log(n/\epsilon)$.

Since each $\mathbf{X}_i$ has average conditional min-entropy at least $m - (t+2)\log(n/\epsilon)$, it follows that each $\overline{\mathbf{V}}_i$ is 2ϵ-close to uniform and Ext_2 is a strong extractor, it follows that $\overline{\mathbf{V}}_i$ is 2ϵ-close to $\mathbf{U}_d$ on average even conditioned on $\{\mathbf{V}, \mathbf{V}^1, \ldots, \mathbf{V}^t\}$. After this fixing, $\mathbf{Z}$ has average conditional min-entropy at least $d - (t+2)\log(n/\epsilon)$.

We now prove that $\overline{\mathbf{V}}_h | \{\overline{\mathbf{V}}_h^g : g \in [t]\}$ is 2ϵ-close to uniform on average. First, we fix the r.v's $\mathbf{W}, \{\mathbf{W}^g : g \in [t]\}$ (at this point no other r.v's are fixed). As before, we have $\mathbf{X}_h | \{\mathbf{X}_h^g : g \in [t]\}$ has average conditional min-entropy $k_x \geq m - (t+2)\log(n/\epsilon)$. Thus, we fix $\{\mathbf{X}_h^g : g \in [t]\}$. Now since Ext_2 is a strong extractor, $\overline{\mathbf{V}}_h$ is uniform on average even conditioned on $\mathbf{V}$. We fix $\mathbf{V}$, and thus $\overline{\mathbf{V}}_h$ is a deterministic function of $\mathbf{X}_h$. Further, $\{\overline{\mathbf{V}}_h^g : g \in [t]\}$ is a deterministic function of $\{\mathbf{V}^g : g \in [t]\}$, and hence a deterministic function of $\mathbf{Z}, \{\mathbf{Z}^g : g \in [t]\}$. Thus, we can fix $\{\overline{\mathbf{V}}_h^g : g \in [t]\}$ without affecting the distribution of $\overline{\mathbf{V}}_h$. This completes the proof of our claim. □

The correctness of the function IPM is direct from the next claim.

Claim 4.14. *Conditioned on* $\{\overline{\mathbf{Z}}^g : g \in [t]\}\}$, *the r.v* $\overline{\mathbf{Z}}$ *is* $3L\epsilon$*-close to uniform on average.*

Proof. Fix the r.v's $\mathbf{W}, \{\mathbf{W}^g : g \in [t]\}, \mathbf{V}, \{\mathbf{V}^g : g \in [y]\}$. We observe that the following hold:

- $\mathbf{Z}, \{\mathbf{Z}^g : g \in [t]\}$ is independent of $\mathbf{Y}, \{\mathbf{Y}^g : g \in [t]\}$,
- For each $i \in [L]$, $\overline{\mathbf{V}}_i$ is 2ϵ-close to uniform,
- $\overline{\mathbf{V}}_h | \{\overline{\mathbf{V}}_h^g : g \in [t]\}$ is 2ϵ-close to uniform on average.
- $\mathbf{Z}$ has average conditional min-entropy at least $d - (t+2)\log(m/\epsilon)$.

The claim is now direct from Theorem 4.9 by observing that by our choice of parameters, the following hold:

- $d \geq (c_{4.5}\ell \log(m/\epsilon) + d'')(t+2)^{r+1}$, where $d'' = (t+2)\log(m/\epsilon)$,
- $\mathbf{Z}$ has average conditional min-entropy at least $d - d''$,
- $m'' \leq 0.9^r(m' - c_{4.5}\ell(t+1)r\log(m/\epsilon))$.

This completes the proof of the claim, and hence Theorem 4.11 follows. □

□

5 Explicit Almost-Optimal Non-Malleable Extractor

We present an explicit construction of a non-malleable extractor with min-entropy requirement $k = (\log(n/\epsilon))^{1+o(1)}$ and seed-length $d = (\log(n/\epsilon))^{1+o(1)}$. We also show a way of setting parameters that allows for $O(\log n)$ seed-length for large enough error. The following are the main results of this section.

Theorem 5.1. *There exist a constant $C_{5.1} > 0$ s.t for all $n, k \in \mathbb{N}$ and any $\epsilon > 0$, with $k \geq \log(n/\epsilon)2^{C_{5.1}\sqrt{\log\log(n/\epsilon)}}$, there exists an explicit (k,ϵ)-non-malleable extractor* $\mathrm{nmExt} : \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^m$, *where $d = \log(n/\epsilon)2^{C_{5.1}\sqrt{\log\log(n/\epsilon)}}$ and $m = k/2^{\sqrt{\log\log(n/\epsilon)}}$.*

Theorem 5.2. *There exist a constant $C_{5.2} > 0$ s.t for constant $\beta > 0$ and all $n, k \in \mathbb{N}$ and any $\epsilon > 2^{-\log^{1-\beta}(n)}$, with $k \geq C_{5.2}\log n$, there exists an explicit (k,ϵ)-non-malleable extractor* $\mathrm{nmExt} : \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^m$, *where $d = O(\log n)$ and $m = \Omega(\log(1/\epsilon))$.*

We derive both the above theorems from the following theorem.

Theorem 5.3. *There exist constants $\delta_{5.3}, C_{5.3} > 0$ s.t for all $n, k \in \mathbb{N}$ and any error parameter $\epsilon_1 > 0$, with $k \geq \log(k/\epsilon_1)2^{C_{5.3}\sqrt{\log\log(n/\epsilon_1)}} + C_{5.3}\log(n/\epsilon_1)$, there exists an explicit (k,ϵ')-non-malleable extractor* $\mathrm{nmExt} : \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^m$, *where $d = \log(k/\epsilon)2^{C_{5.3}\sqrt{\log\log(n/\epsilon_1)}} + C_{5.3}\log(n/\epsilon_1)$, $m = \delta_{5.3}k/2^{\sqrt{\log\log(n/\epsilon_1)}}$ and $\epsilon' = C_{5.3}\epsilon_1\log(n/\epsilon_1)$.*

We first show how to derive Theorem 5.1 and Theorem 5.2 from Theorem 5.3.

Proof of Theorem 5.1. Let $\mathrm{nmExt} : \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^m$ be the function from Theorem 5.3 set to extract from min-entropy k, where we set the parameter $\epsilon_1 = \epsilon/2C_{5.3}n$. It follows that the error of nmExt is

$$C_{5.3}\epsilon_1\log(n/\epsilon_1) = \frac{\epsilon}{2n}(\log n + \log(2C_{5.3}n) + \log(1/\epsilon)) < \epsilon.$$

Further note that for this setting of ϵ_1, the min-entropy required and seed length are $\log(n/\epsilon)2^{C_{5.1}\sqrt{\log\log(n/\epsilon)}} + C_{5.1}\log(n/\epsilon)$, for some constant $C_{5.1}$. □

Proof of Theorem 5.2. Let $\mathrm{nmExt} : \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^m$ be the function from Theorem 5.3 set to extract from min-entropy $2C_{5.3}\log(n/\epsilon_1)$, where we set the parameter $\epsilon_1 = \epsilon/2C_{5.3}\log n$. Thus, the error of nmExt is

$$\epsilon_1\log(n/\epsilon_1) \leq \frac{\epsilon}{2\log n}(\log n + \log(1/\epsilon) + \log(2C_{5.3}\log n)) < \epsilon.$$

For this setting of parameters, we note that the seed-length required by nmExt is bounded by $\log((\log^2 n)/\epsilon)2^{C_{5.3}\sqrt{\log\log(n\log n/\epsilon)}} + C_{5.3}\log(n\log n/\epsilon) = O(\log n)$. □

We spend the rest of the section proving Theorem 5.3. We recall some explicit constructions from previous work.

The following flip-flop function was constructed by Cohen [Coh15] using alternating extraction. Subsequently, Chattopadhyay, Goyal and Li [CGL16], used this in constructing non-malleable extractors. Informally, the flip-flop function uses an independent source $\mathbf{X}$ to break the correlation between two r.v's $\mathbf{Y}$ and $\mathbf{Y}'$, given an advice bit. We now describe this more formally.

Theorem 5.4 ([Coh15, CGL16]). *There exist constants $C_{5.4}, \delta_{5.4} > 0$ such that for all $n > 0$ and any $\epsilon > 0$, there exists an explicit function* flip-flop $: \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^m$, $m = \delta_{5.4} k$, *satisfying the following: Let $\mathbf{X}$ be an (n,k)-source, and $\mathbf{Y}$ be an independent weak seed on d bits with entropy $d - \lambda$, $\lambda < d/2$. Let $\mathbf{Y}'$ be a r.v on d bits independent of $\mathbf{X}$, and let b, b' be bits s.t. $b \neq b'$. If $k, d \geq C_{5.4} \log(n/\epsilon)$, then*

$$|\text{flip-flop}(\mathbf{X}, \mathbf{Y}, b), \text{flip-flop}(\mathbf{X}, \mathbf{Y}', b'), \mathbf{Y}, \mathbf{Y}' - \mathbf{U}_m, \text{flip-flop}(\mathbf{X}, \mathbf{Y}', b'), \mathbf{Y}, \mathbf{Y}'| \leq \epsilon.$$

We now recall an explicit function advGen from [CGL16]. Informally, advGen takes as input a source $\mathbf{X}$ and a seed $\mathbf{Y}$ and produces a short string such that for any r.v $\mathbf{Y}' \neq \mathbf{Y}$, advGen$(\mathbf{X}, \mathbf{Y}) \neq$ advGen$(\mathbf{X}, \mathbf{Y})$. We record this property more formally.

Theorem 5.5 ([CGL16]). *There exists a constant $c_{5.5}, C_{5.5} > 0$ such that for all $n > 0$ and any $\epsilon > 0$, there exists an explicit function* advGen $: \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^L$, $L = c_{5.5} \log(n/\epsilon)$ *satisfying the following: Let $\mathbf{X}$ be an (n,k)-source, and $\mathbf{Y}$ be an independent uniform seed on d bits. Let $\mathbf{Y}'$ be a r.v on d bits independent of $\mathbf{X}$, s.t $\mathbf{Y}' \neq \mathbf{Y}$. If $k, d \geq C_{5.5} \log(n/\epsilon)$, then*

- *with probability at least $1 - \epsilon$,* advGen$(\mathbf{X}, \mathbf{Y}) \neq$ advGen$(\mathbf{X}, \mathbf{Y}')$,
- *there exists a function f such that conditioned on* advGen$(\mathbf{X}, \mathbf{Y})$, advGen$(\mathbf{X}, \mathbf{Y}')$, $f(\mathbf{X})$,
  - $\mathbf{X}$ *remains independent of* $\mathbf{Y}, \mathbf{Y}'$,
  - $\mathbf{X}$ *has average conditional min-entropy at least* $k - C_{5.5} \log(n/\epsilon)$,
  - $\mathbf{Y}$ *has average conditional min-entropy at least* $d - C_{5.5} \log(n/\epsilon)$

We are now ready to prove Theorem 5.3.

Proof of Theorem 5.3. We set up parameters and ingredients required in our construction.

- Let advGen $: \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^L$, $L = c_{5.5} \log(n/\epsilon_1)$, be the function from Theorem 5.5 with error parameter ϵ_1.
- Let $d_1 = (C_{5.5} + C_{5.4} + 1) \log(n/\epsilon_1)$.
- Let flip-flop $: \{0,1\}^n \times \{0,1\}^{d_1} \to \{0,1\}^{m'}$, $m' = \delta_{5.4} k$, be the function from Theorem 5.4 with error parameter ϵ_1.
- $d_2 = c_{3.8} \log(d/\epsilon_1), d_3 = c_{3.8} \log(m'/\epsilon_1)$.
- Let $\text{Ext}_1 : \{0,1\}^n \times \{0,1\}^{d_2} \to \{0,1\}^{d'}$, $d' = 0.9d - 2d_1 - C_{5.5} \log(n/\epsilon_1)$ be a $(d - 2d_1 - C_{5.5} \log(n/\epsilon_1), \epsilon_1)$-strong-seeded extractor from Theorem 3.8.
- Let $\text{Ext}_2 : \{0,1\}^{m'} \times \{0,1\}^{d_3} \to \{0,1\}^{m''}$, $m'' = 0.9m' - 2d_2$, be a $(m' - 2d_2 - \log(1/\epsilon_1), \epsilon_1)$-strong-seeded extractor from Theorem 3.8.
- Let $\ell = 2^{\sqrt{\log L}}$.
- Let $(L, \ell, 1)$-NIPM $: \{0,1\}^{Lm''} \times \{0,1\}^{d'} \to \{0,1\}^m$ be the function from Theorem 4.9, $m = 0.9^r m' - 2c_{4.5} \ell(t+1) r \log(m/\epsilon_1)$ with error parameter ϵ_1.

Algorithm 3: nmExt(x, y)

Input: x, y are bit string of length n, d respectively.
Output: A bit string of length m.

Let $w = \text{advGen}(x, y)$.
Let $y = y_1 \circ y_2$, where $y_1 = \text{Slice}(y, d_1)$.
Let v be a $L \times m'$ matrix, whose i'th row $v_i = \text{flip-flop}(x, y_1, w_i)$ (w_i is the i'th bit of the string w).
Let $\overline{v_1} = \text{Slice}(v_1, d_2)$
Let $\overline{y} = \text{Ext}_1(y, \overline{v_1}) = \overline{y_1} \circ \overline{y_2}$, where $\overline{y_1} = \text{Slice}(\overline{y}, d_3)$.
Let z be a $L \times m''$ matrix, whose i'th row $z_i = \text{Ext}_2(v_i, \overline{y_1})$
Output $\overline{z} = (L, \ell, 1)\text{-NIPM}(z, \overline{y})$.

We prove in the following claims that the function nmExt constructed in Algorithm 2 satisfies the conclusion of Theorem 5.3. Let $\mathcal{A}$ be the adversarial function tampering the seed $\mathbf{Y}$, and let $\mathbf{Y}' = \mathcal{A}(\mathbf{Y})$. Since $\mathcal{A}$ has no fixed points, it follows that $\mathbf{Y} \neq \mathbf{Y}'$.

Notation: For any random variable $\mathbf{H} = g(\mathbf{X}, \mathbf{Y})$ (where g is an arbitrary deterministic function), let $\mathbf{H}' = g(\mathbf{X}, \mathbf{Y}')$.

Claim 5.6. *With probability at least* $1 - \epsilon$, $\mathbf{W} \neq \mathbf{W}'$.

Proof. Follows directly from Theorem 5.5. □

Let f be the function guaranteed by Theorem 5.5.

Claim 5.7. *Conditoned on the r.v's* $\mathbf{W}, \mathbf{W}', \mathbf{Y}_1, \mathbf{Y}_1', f(\mathbf{X})$, *the following hold:*

- *for each* $i \in [L]$, $\mathbf{V}_i$ *is* ϵ_1*-close to uniform,*
- *there exists an* $h \in [L]$ *such that conditioned on* $\mathbf{V}_h'$, *the r.v* $\mathbf{V}_h$ *is* ϵ_1*-close to uniform on average,*
- $\{\mathbf{V}, \mathbf{V}'\}$ *is independent of* $\{\mathbf{Y}, \mathbf{Y}'\}$.
- $\mathbf{Y}$ *has average conditional min-entropy at least* $d - C_{5.5} \log(n/\epsilon_1) - 2d_1$.

Proof. Fix the r.v's $\mathbf{W}, \mathbf{W}', f(\mathbf{X})$ such that $\mathbf{W} \neq \mathbf{W}'$. It follows from Theorem 5.5 that after this conditioning,

- $\mathbf{X}$ is independent of $\mathbf{Y}, \mathbf{Y}'$,
- $\mathbf{X}$ has average conditional min-entropy at least $k - C_{5.5} \log(n/\epsilon_1)$,
- $\mathbf{Y}$ has average conditional min-entropy at least $d - C_{5.5} \log(n/\epsilon_1)$

Thus $\mathbf{Y}_1 = \text{Slice}(\mathbf{Y}, d_1)$ has average conditional min-entropy at least $2C_{5.4} \log(n/\epsilon_1)$. The claim now follows by applying Theorem 5.4. □

Claim 5.8. *Conditioned on the r.v's* $\mathbf{W}, \mathbf{W}', \overline{\mathbf{V}_1}, \overline{\mathbf{V}_1}', \mathbf{Y}_1, \mathbf{Y}_1' \overline{\mathbf{Y}_1}, \overline{\mathbf{Y}_1}', f(\mathbf{X})$, *the following hold:*

- $\overline{\mathbf{Y}}$ *has average conditional min-entropy at least* $d' - 2d_3 - \log(1/\epsilon)$.

- *for each* $i \in [L]$, $\mathbf{Z}_i$ *is* $3\epsilon_1$*-close to uniform on average.*
- *there exists* $h \in [L]$ *such that further conditioned on* $\mathbf{Z}'_i$, $\mathbf{Z}_i$ *is* $3\epsilon_1$*-close to uniform on average.*
- $\{\overline{\mathbf{Y}}, \overline{\mathbf{Y}}'\}$ *is independent of* $\{\mathbf{Z}, \mathbf{Z}'\}$.

Proof. Fix the r.v's $\mathbf{W}, \mathbf{W}', \mathbf{Y}_1, \mathbf{Y}'_1, f(\mathbf{X})$. By Claim 5.7, we have

- for each $i \in [L]$, $\mathbf{V}_i$ is ϵ_1-close to uniform,
- there exists an $h \in [L]$ such that conditioned on $\mathbf{V}'_h$, the r.v $\mathbf{V}_h$ is ϵ_1-close to uniform on average,
- $\{\mathbf{V}, \mathbf{V}'\}$ is independent of $\{\mathbf{Y}, \mathbf{Y}'\}$.
- $\mathbf{Y}$ has average conditional min-entropy at least $d - C_{5.5}\log(n/\epsilon_1) - 2d_1$.

Using the fact that Ext_1 is a strong extractor, it follows that we can fix $\overline{\mathbf{V}_1}$, and $\overline{\mathbf{Y}}$ is $2\epsilon_1$-close to uniform on average. Further, $\overline{\mathbf{Y}}$ is a deterministic function of $\mathbf{Y}$. Thus, we fix $\overline{\mathbf{V}_1}'$ without affecting the distribution of $\overline{\mathbf{Y}}$. Now, using the fact that Ext_2 is a strong extractor, we can fix $\overline{\mathbf{Y}_1}$, and we have for each $i \in [L]$, $\mathbf{Z}_i$ is $3\epsilon_1$-close to uniform on average. Next we can fix $\overline{\mathbf{Y}_1}'$ without affecting $\mathbf{V}$.

We prove that conditioned on $\mathbf{Z}'_i$, the r.v $\mathbf{Z}_i$ is $3\epsilon_1$-close to uniform on average in the following way. For this argument, as above we fix all r.v's but do not yet fix $\overline{\mathbf{Y}_1}, \overline{\mathbf{Y}_1}'$. Instead, we first fix $\mathbf{V}'_h$, and $\mathbf{V}_h$ has average conditional min-entropy at least $m' - 2d_2$. We now fix $\overline{\mathbf{Y}_1}$, and as before we have $\mathbf{Z}_h$ is $3\epsilon_1$-close. At this point, $\mathbf{Z}'_h$ is a deterministic function of $\overline{\mathbf{Y}_1}'$, and hence we can fix it without affecting the distribution of $\mathbf{Z}_h$. This completes the proof. □

Claim 5.9. *Conditioned on* $\overline{\mathbf{Z}}'$, *the r.v* $\overline{\mathbf{Z}}$ *is* $O(\epsilon_1 \log(n/\epsilon_1))$*-close to uniform on average.*

Proof. Fix the r.v's $\mathbf{W}, \mathbf{W}', \overline{\mathbf{V}_1}, \overline{\mathbf{V}_1}', \mathbf{Y}_1, \mathbf{Y}'_1\overline{\mathbf{Y}_1}, \overline{\mathbf{Y}_1}', f(\mathbf{X})$. By Claim 5.8, the following hold:

- $\overline{\mathbf{Y}}$ has average conditional min-entropy at least $d' - 2d_3 - \log(1/\epsilon_1)$.
- for each $i \in [L]$, $\mathbf{Z}_i$ is $3\epsilon_1$-close to uniform on average.
- there exists $h \in [L]$ such that further conditioned on $\mathbf{Z}'_i$, the r.v $\mathbf{Z}_i$ is $3\epsilon_1$-close to uniform on average.
- $\{\overline{\mathbf{Y}}, \overline{\mathbf{Y}}'\}$ is independent of $\{\mathbf{Z}, \mathbf{Z}'\}$.

Let $d'' = 2d_3 + \log(1/\epsilon_1), r = \lceil \frac{\log L}{\log \ell} \rceil = \lceil \sqrt{\log L} \rceil$. Thus $d'' = O(\log(k/\epsilon_1)), r = O(\sqrt{\log\log(n/\epsilon_1)})$, $\ell = 2^{O(\sqrt{\log\log(n/\epsilon_1)})}$. In order to use Theorem 4.9, we observe that for a large enough constant $C_{5.3}$ the following hold:

- $\overline{\mathbf{Y}}$ has conditional min-entropy at least $d - d''$,
- $d' \geq (c_{4.5}\ell \log(m''/\epsilon_1) + d'')3^{r+1}$,
- $m < (0.9)^r(m'' - c_{4.5}\ell(t+1)r\log(m/\epsilon_1))$.

Thus the conditions of Theorem 4.9 are met, and hence it follows that conditioned on $\overline{\mathbf{Z}}'$, the r.v $\overline{\mathbf{Z}}$ is $2c'_{4.5}L\epsilon_1$-close to uniform on average. Recall that $L = O(\log(n/\epsilon_1))$, and hence the claim follows. □

□

6 Improved Multi-Source Extractors

In this section, we construct extractors for a constant number of independent sources $\mathbf{X}_1, \ldots, \mathbf{X}_C$, each with min-entropy $\tilde{O}(\log n)$. In particular, this improves upon a recent result of Cohen and Schulman [CS16], where they constructed an extractor for $O(1/\delta)$ independent sources, with each having min-entropy $\log^{1+\delta}(n)$.

Our main result in this section is the following.

Theorem 6.1. *There exists a constant $C > 0$ s.t for all $n, k \in \mathbb{N}$ and any constant $\epsilon > 0$, with $k \geq 2^{C\sqrt{\log\log(n)}} \log n$, there exists an explicit function $\mathrm{Ext} : (\{0,1\}^n)^C \to \{0,1\}$, such that*

$$|\mathrm{Ext}(\mathbf{X}_1, \ldots, \mathbf{X}_C) - \mathbf{U}_1| \leq \epsilon.$$

Our starting point is the following reduction from [CS16]. Informally, a constant number of independent sources are used to transform into a sequence of matrices such that a large fraction of the matrices follow a certain t-wise independence property. For our purposes, we need to slightly modify this construction. The length of the rows (the parameter m in the following theorem) in the work of [CS16] can be set to $c\log(n/\epsilon)$, for any constant c. Using another additional source and extracting from it using each row as seed (using any optimal strong-seeded extractor), the length of each row can be made $\Omega(k)$. We state the theorem from [CS16] with this modification.

Theorem 6.2 ([CS16])**.** *There exists constants $\alpha > 0$ and and $c_{6.2}$ such that for all $n, t \in \mathbb{N}$, and for any $\epsilon, \delta > 0$, there exists an polynomial time computable function $f : (\{0,1\}^n)^C \to (\{0,1\}^{Lm})^r$, where $C = 7/\alpha, L = O(t\log n), r = n^{3/\alpha}, m = \Omega(k)$, such that the following hold: Let $\mathbf{X}_1, \ldots, \mathbf{X}_C$ be independent (n,k) sources, $k = c_{6.2}t\log(t)\log(n\log t/\epsilon)$. Then there exists a subset $S \subset [r]$, $|S| \geq r - r^{\frac{1}{2}-\alpha}$ and a sequence of $L \times m$ matrices $\mathbf{Y}^1, \ldots, \mathbf{Y}^r$ such that:*

- *$f(\mathbf{X}_1, \ldots, \mathbf{X}_C)$ is $1/r$-close to $\mathbf{Y}^1, \ldots, \mathbf{Y}^r$,*
- *for any $i \in [L]$ and $g \in S$, $\mathbf{Y}^g_i$ is ϵ-close to $\mathbf{U}_m$,*
- *for any $g \in S$, and any distinct $i_1, \ldots, i_t$ in $S \setminus \{g\}$, there exists an $h \in [L]$ such that $\mathbf{Y}^g_h | \{\mathbf{Y}^j_h : j \in [r] \setminus \{g\}\}$ is ϵ-close to uniform.*

Now composing the above theorem with our independence preserving merger from Section 4.4, we have the following result.

Theorem 6.3. *There exists a constant $\alpha > 0$ such that for all $n, t \in \mathbb{N}$, and for any $\epsilon, \delta > 0$, there exists an polynomial time computable function $\mathrm{reduce} : (\{0,1\}^n)^{C+1} \to \{0,1\}^r$, where $C = \frac{7}{\alpha} + 1, r = n^{3/\alpha}$, such that the following hold: Let $\mathbf{X}_1, \ldots, \mathbf{X}_C$ be independent (n,k) sources, $k \geq 2^{\sqrt{\log t + \log\log n}} \log(k/\epsilon)(t+2)^{O(\sqrt{\log t + \log\log n})} + c_{6.2}t\log(t)\log(n\log t/\epsilon)$, and let $\mathbf{Z} = \mathrm{reduce}(\mathbf{X}_1, \ldots, \mathbf{X}_{C+1})$. Then there exists a subset $S \subset [r]$, $|S| \geq r - r^{\frac{1}{2}-\alpha}$ such that $\mathbf{Z}_S$ is $n^{-\Omega(1)}$-close to a $(t, \gamma_{6.3})$-wise independent distribution, where $\gamma_{6.3} = O(\epsilon t \log n)$.*

Proof. Let $f : (\{0,1\}^n)^C \to (\{0,1\}^{Lm})^r$ be the function from Theorem 6.2 with $\epsilon_{6.2} = \epsilon, m = \beta k$ for some constant $\beta > 0$. Thus $L = O(t \log n)$. Let (L, ℓ, t)-IPM : $(\{0,1\}^{Lm})^t \times \{0,1\}$ be the function from Theorem 4.11, with $\ell = 2^{\sqrt{\log L}} = 2^{O(\sqrt{\log t + \log\log n})}$ and error parameter $\epsilon_{4.11} = \epsilon$. Define

$$\text{reduce}(x_1, \ldots, x_{C+1}) = (L, \ell, t)\text{-IPM}(f(x_1, \ldots, x_C), x_{C+1}).$$

We note that $k > c_{6.2} t \log(t) \log(n \log t/\epsilon)$. Thus, using Theorem 6.2, it follows that there exists a subset $S \subset [r]$, $|S| \geq r - r^{\frac{1}{2}-\alpha}$ and a sequence of $L \times m$ matrices $\mathbf{Y}^1, \ldots, \mathbf{Y}^r$ such that:

- $f(\mathbf{X}_1, \ldots, \mathbf{X}_C)$ is $1/r$-close to $\mathbf{Y}^1, \ldots, \mathbf{Y}^r$,
- for any $i \in [L]$ and $g \in S$, $\mathbf{Y}^g_i$ is ϵ-close to $\mathbf{U}_m$,
- for any $g \in S$, and any distinct $i_1, \ldots, i_t$ in $S \setminus \{g\}$, there exists an $h \in [L]$ such that $\mathbf{Y}^g_h | \{\mathbf{Y}^j_h : j \in [r] \setminus \{g\}\}$ is ϵ-close to uniform.

We now work with the sources $\mathbf{Y}^1, \ldots, \mathbf{Y}^r$, and add an error of $1/r$ in the end. The theorem is now direct using Theorem 4.11 and observing that the following hold by our setting of parameters:

- $k \geq 2c_{4.5} \ell \log(k/\epsilon)(t+2)^{\lceil \frac{\log L}{\log \ell} \rceil + 1}$,
- $m = \beta k \geq 2^{\sqrt{\log L}}(c_{4.5} \ell (t+1) r \log(m/\epsilon) + c_{3.8}(t+2)\log(n/\epsilon))$.

□

Our multi-source extractor in Theorem 6.1 is now easy to obtain using a result on the majority function.

Theorem 6.4 ([Vio14, CS16])**.** *Let $\mathbf{Z}$ be a source on r bits such that there exists a subset $S \subset [r]$, $|S| \geq r - r^{\frac{1}{2}-\alpha}$ such that $\mathbf{Z}_S$ is t-wise independent. Then,*

$$\left| \Pr[\text{Majority}(\mathbf{Z}) = 1] - \frac{1}{2} \right| \leq O\left(\frac{\log t}{t} + r^{-\alpha} \right).$$

We also recall a result about almost t-wise independent distributions.

Theorem 6.5 ([AGM03])**.** *Let $\mathcal{D}$ be a (t, γ)-wise independent distribution on $\{0,1\}^n$. Then there exists a t-wise independent distribution that is $n^t\gamma$-close to $\mathcal{D}$.*

Thus, we have the following corollary.

Corollary 6.6. *There exists a constant c such that the following holds: Let $\mathbf{Z}$ be a source on r bits such that there exists a subset $S \subset [r]$, $|S| \geq r - r^{\frac{1}{2}-\alpha}$ such that $\mathbf{Z}_S$ is (t, γ)-wise independent. Then,*

$$|\Pr[\text{Majority}(\mathbf{Z}) = 1] - \frac{1}{2}| \leq c\left(\frac{\log t}{t} + r^{-\alpha} + \gamma r^t \right).$$

Proof of Theorem 6.1. Set t to a large enough constant such that $\frac{c \log t}{t} < \epsilon/2$. Let α be the constant from Theorem 6.3, $r = n^{3/\alpha}$ and $C = \frac{7}{\alpha} + 1$. Let reduce be the function from Theorem 6.3 with parameter $t_{6.3} = t$, $r_{6.3} = r$, and the error parameter $\epsilon_{6.3}$ set such that the parameter $\gamma_{6.3} \leq \frac{1}{r^{t+1}}$. This can be ensured by setting $\epsilon = n^{-C'}$ for a large enough constant C'.

Define

$$\mathrm{Ext}(x_1, \ldots, x_C) = \mathrm{Majority}(f(x_1, \ldots, x_C)).$$

Let $\mathbf{Z} = f(\mathbf{X}_1, \ldots, \mathbf{X}_C)$. We note that with this setting of parameters, there exists some constant C'' such that any $k \geq 2^{C''\sqrt{\log \log n}} \log(n)$ is sufficient for the conclusion of Theorem 6.3 to hold. Thus, $\mathbf{Z}$ is a source on r bits such that there exists a subset $S \subset [r]$, $|S| \geq r - r^{\frac{1}{2}-\alpha}$ for which $\mathbf{Z}_S$ is (t, γ)-wise independent. Theorem 6.1 is now direct from Corollary 6.6. □

References

[AGM03] Noga Alon, Oded Goldreich, and Yishay Mansour. Almost k-wise independence versus k-wise independence. *Inf. Process. Lett.*, 88(3):107–110, 2003.

[BIW06] Boaz Barak, Russell Impagliazzo, and Avi Wigderson. Extracting randomness using few independent sources. *SIAM J. Comput.*, 36(4):1095–1118, December 2006.

[BKS+10] Boaz Barak, Guy Kindler, Ronen Shaltiel, Benny Sudakov, and Avi Wigderson. Simulating independence: New constructions of condensers, Ramsey graphs, dispersers, and extractors. *J. ACM*, 57(4), 2010.

[Bou05] J. Bourgain. More on the sum-product phenomenon in prime fields and its applications. *International Journal of Number Theory*, 01(01):1–32, 2005.

[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.

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

[CKOR10] N. Chandran, B. Kanukurthi, R. Ostrovsky, and L. Reyzin. Privacy amplification with asymptotically optimal entropy loss. In *Proceedings of the 42nd Annual ACM Symposium on Theory of Computing*, pages 785–794, 2010.

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

[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.

[Coh16a] Gil Cohen. Non-malleable extractors - new tools and improved constructions. In *CCC*, 2016.

[Coh16b] Gil Cohen. Non-malleable extractors with logarithmic seeds. Technical Report TR16-030, ECCC, 2016.

[Coh16c] Gil Cohen. Two-source dispersers for polylogarithmic entropy and improved Ramsey graphs. In *STOC*, 2016.

[CRS14] Gil Cohen, Ran Raz, and Gil Segev. Non-malleable extractors with short seeds and applications to privacy amplification. *SIAM Journal on Computing*, 43(2):450–476, 2014.

[CS16] Gil Cohen and Leonard Schulman. Extractors for near logarithmic min-entropy. Technical Report TR16-014, ECCC, 2016.

[CZ16] Eshan Chattopadhyay and David Zuckerman. Explicit two-source extractors and resilient functions. In *STOC*, 2016.

[DKRS06] Y. Dodis, J. Katz, L. Reyzin, and A. Smith. Robust fuzzy extractors and authenticated key agreement from close secrets. In *Advances in Cryptology — CRYPTO '06, 26th Annual International Cryptology Conference, Proceedings*, pages 232–250, 2006.

[DKSS09] Zeev Dvir, Swastik Kopparty, Shubhangi Saraf, and Madhu Sudan. Extensions to the method of multiplicities, with applications to Kakeya sets and mergers. In *Proceedings of the 50th Annual IEEE Symposium on Foundations of Computer Science*, pages 181–190, 2009.

[DLWZ14] Yevgeniy Dodis, Xin Li, Trevor D. Wooley, and David Zuckerman. Privacy amplification and non-malleable extractors via character sums. *SIAM Journal on Computing*, 43(2):800–830, 2014.

[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.

[DP07] Stefan Dziembowski and Krzysztof Pietrzak. Intrusion-resilient secret sharing. In *Proceedings of the 48th Annual IEEE Symposium on Foundations of Computer Science*, FOCS '07, pages 227–237, Washington, DC, USA, 2007. IEEE Computer Society.

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

[DY13] Yevgeniy Dodis and Yu Yu. Overcoming weak expectations. In *10th Theory of Cryptography Conference*, 2013.

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

[KR09] B. Kanukurthi and L. Reyzin. Key agreement from close secrets over unsecured channels. In *EUROCRYPT 2009, 28th Annual International Conference on the Theory and Applications of Cryptographic Techniques*, 2009.

[Li11] Xin Li. Improved constructions of three source extractors. In *Proceedings of the 26th Annual IEEE Conference on Computational Complexity, CCC 2011, San Jose, California, June 8-10, 2011*, pages 126–136, 2011.

[Li12a] Xin Li. Design extractors, non-malleable condensers and privacy amplification. In *Proceedings of the 44th Annual ACM Symposium on Theory of Computing*, pages 837–854, 2012.

[Li12b] Xin Li. Non-malleable extractors, two-source extractors and privacy amplification. In *Proceedings of the 53rd Annual IEEE Symposium on Foundations of Computer Science*, pages 688–697, 2012.

[Li13a] Xin Li. Extractors for a constant number of independent sources with polylogarithmic min-entropy. In *Proceedings of the 54th Annual IEEE Symposium on Foundations of Computer Science*, pages 100–109, 2013.

[Li13b] Xin Li. New independent source extractors with exponential improvement. In *Proceedings of the 45th Annual ACM Symposium on Theory of Computing*, pages 783–792, 2013.

[Li15a] Xin Li. Improved constructions of two-source extractors. Technical Report TR15-125, ECCC, 2015.

[Li15b] Xin Li. Improved two-source extractors, and affine extractors for polylogarithmic entropy. Technical Report TR15-125, ECCC, 2015.

[Li15c] Xin Li. Non-malleable condensers for arbitrary min-entropy, and almost optimal protocols for privacy amplification. In *12th Theory of Cryptography Conference*, 2015.

[Li15d] Xin Li. Three-source extractors for polylogarithmic min-entropy. In *Proceedings of the 56th Annual IEEE Symposium on Foundations of Computer Science*, 2015.

[LRVW03] Chi-Jen Lu, Omer Reingold, Salil P. Vadhan, and Avi Wigderson. Extractors: optimal up to constant factors. In *STOC*, pages 602–611, 2003.

[Mek15] Raghu Meka. Explicit resilient functions matching Ajtai-Linial. *CoRR*, abs/1509.00092, 2015.

[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.

[NZ96] Noam Nisan and David Zuckerman. Randomness is linear in space. *J. Comput. Syst. Sci.*, 52(1):43–52, 1996.

[Rao09] Anup Rao. Extractors for a constant number of polynomially small min-entropy independent sources. *SIAM J. Comput.*, 39(1):168–194, 2009.

[Raz05] Ran Raz. Extractors with weak random seeds. In *Proceedings of the 37th Annual ACM Symposium on Theory of Computing*, pages 11–20, 2005.

[RW03] Renato Renner and Stefan Wolf. Unconditional authenticity and privacy from an arbitrarily weak secret. In *Advances in Cryptology — CRYPTO '03, 23rd Annual International Cryptology Conference, Proceedings*, pages 78–95, 2003.

[RZ08] Anup Rao and David Zuckerman. Extractors for three uneven-length sources. In *Approximation, Randomization and Combinatorial Optimization. Algorithms and Techniques, 11th International Workshop, APPROX 2008, and 12th International Workshop, RANDOM 2008, Boston, MA, USA, August 25-27, 2008. Proceedings*, pages 557–570, 2008.

[Vio14] Emanuele Viola. Extractors for circuit sources. *SIAM J. Comput.*, 43(2):655–672, 2014.

ECCC ISSN 1433-8092

http://eccc.hpi-web.de