



# Seed Protecting Extractors

Gil Cohen\*      Dean Doron†      Shahar Samocha‡

November 5, 2020

## Abstract

We introduce a new type of seeded extractors we dub *seed protecting* extractors. Informally, a seeded extractor is seed protecting against a class of functions  $\mathcal{C}$ , mappings seeds to seeds, if the seed  $Y$  remains close to uniform even after observing the output  $\text{Ext}(X, A(Y))$  for every choice of  $A \in \mathcal{C}$  (or, more generally, observing the outputs corresponding to several adversaries from  $\mathcal{C}$ ).

The results of this paper are structural. We establish what we believe to be surprising relations, in fact, *equivalences* between seed protecting extractors and each of the well-studied strengthenings of seeded extractors: strong extractors, non-malleable extractors (against permutations), and two-source extractors, where each case is classified by a suitable class  $\mathcal{C}$ . Our work put forth a novel approach for constructing nonmalleable extractors against permutations. Indeed, the existing machinery developed for constructing non-malleable extractors focuses on the *output* and so it is aimed towards breaking correlations. Instead, our work suggests developing techniques for protecting the *seed*.

---

\*Department of Computer Science, Tel Aviv University, Tel Aviv, Israel. The research leading to these results has received funding from the Israel Science Foundation (grant number 1569/18) and from the Azrieli Faculty Fellowship. Email: [gil@tauex.tau.ac.il](mailto:gil@tauex.tau.ac.il).

†Department of Computer Science, Stanford University. Supported by NSF award CCF-1763311. Email: [ddoron@stanford.edu](mailto:ddoron@stanford.edu).

‡Department of Computer Science, Tel Aviv University, Tel Aviv, Israel. Email: [samocho@mail.tau.ac.il](mailto:samocho@mail.tau.ac.il).

# Contents

<b>1</b>	<b>Introduction</b>	<b>1</b>
1.1	Strong seeded extractors and nonmalleable extractors . . . . .	2
1.2	Strong, nonmalleable, and seed protecting extractors . . . . .	3
1.3	Two-source extractors as seed protecting extractors . . . . .	5
1.4	Open problems . . . . .	6
<b>2</b>	<b>Warm-up</b>	<b>7</b>
<b>3</b>	<b>Seed protecting extractors for high entropy adversaries are nonmalleable</b>	<b>10</b>
3.1	Colluding does not harm non malleability . . . . .	18
<b>4</b>	<b>Seed protecting extractors from nonmalleable extractors</b>	<b>20</b>
<b>5</b>	<b>1-seed protecting and two-source extractors</b>	<b>25</b>
5.1	Lower bounds for 1-seed protecting extractors . . . . .	28
<b>6</b>	<b>Non-explicit <math>t</math>-seed protecting extractors</b>	<b>28</b>
<b>A</b>	<b>Missing proofs</b>	<b>36</b>

# 1 Introduction

Informally, a *seeded extractor* is a function that “purifies” defective randomness using few fresh random bits. A defective random source is modelled by a distribution  $X$  that has some lower bound on its *min-entropy*. A random variable  $X$  is said to have min-entropy  $k$  if for every  $x$ ,  $\Pr[X = x] \leq 2^{-k}$ . When  $X$  is supported over  $n$ -bit strings, we call  $X$  an  $(n, k)$ -source. A function  $\text{Ext}: \{0, 1\}^n \times \{0, 1\}^d \rightarrow \{0, 1\}^m$  is a  $(k, \varepsilon)$ -seeded extractor [NZ96] if for every  $(n, k)$ -source  $X$  it holds that  $\text{Ext}(X, Y)$  is  $\varepsilon$ -close, in statistical distance, to the uniform distribution over  $m$ -bit string. Here,  $Y$  is a random variable, independent of  $X$ , that is uniformly distributed over  $d$ -bit strings. We write this as  $\text{Ext}(X, Y) \approx_\varepsilon U_m$ . Informally, using the “fresh” randomness in the, hopefully, short string  $Y$ , the function  $\text{Ext}$  extracts the randomness from  $X$  to a nearly perfect form, namely, to a distribution that is close to uniform. We refer to  $Y$  as the *seed* of the extractor.

The notion of seeded extractors can be strengthened in different ways. Three such strengthenings that emerged from the study of seeded extractors are strong seeded extractors, non-malleable extractors [DW09], and two-source extractors [CG88]. The latter is the oldest notion, in fact, two-source extractors predate the explicit definition of seeded extractors. Nevertheless, such extractors proved to be the most challenging to construct. In a span of about a decade, strong seeded extractors with nearly optimal parameters were constructed using sophisticated algebraic and combinatorial ideas (see, e.g., [Tre01, LRVW03, GUV09, DKSS13, TSU12] as well as [Sha11] and [Vad12, Chapter 6]). Nonmalleable extractors were introduced more recently, and despite their syntactic resemblance to strong seeded extractors (see Section 1.1 below for the formal definitions), their constructions required completely different techniques. Furthermore, it was the insight regarding the connection between non-malleable extractors and the seemingly unrelated two-source extractors that enabled the breakthrough work of Chattopadhyay and Zuckerman [CZ19] who constructed two-source extractors for poly-logarithmic min-entropy.

**A brief and informal summary of our contribution.** In this work, we introduce a new, very natural, variant of seeded extractors we dub *seed protecting extractors*. Informally, a seeded extractor is seed protecting against a class of functions  $\mathcal{C}$ , mapping seeds to seeds, if the seed  $Y$  remains close to uniform even after observing the output  $\text{Ext}(X, A(Y))$  for every choice of  $A \in \mathcal{C}$  (and, of course, a source  $X$  with sufficient min-entropy). See Definition 1.1 below for the formal definition. We establish what we believe to be surprising and insightful relations, in fact, *equivalences* between seed protecting extractors and strong extractors, nonmalleable extractors against permutations, and two-source extractors, where each case is classified by a suitable class  $\mathcal{C}$ .

This fresh point of view on nonmalleable extractors suggests, in particular, a novel approach for constructing such extractors as, indeed, the focus shifts from breaking output correlations to protecting the seed. We first recall the definitions of strong and nonmalleable

extractors (Section 1.1). Then, in Section 1.2, we give the definition of seed protecting extractors and present our results.

## 1.1 Strong seeded extractors and nonmalleable extractors

### Strong seeded extractors

A  $(k, \varepsilon)$ -seeded extractor  $\text{Ext}$  is called *strong* if the output distribution  $\text{Ext}(X, Y)$  is close to uniform even given the seed  $Y$  used for the extraction. This can be expressed by writing  $(\text{Ext}(X, Y), Y) \approx_\varepsilon (U_m, Y)$ . Seeded extractors and, more so, their strong counterparts have found many applications. As mentioned, in a beautiful and deep line of work, efficiently computable strong seeded extractors were constructed for any min-entropy  $k$ , having seed-length  $O(\log \frac{n}{\varepsilon})$  (see [GUV09, DKSS13, TSU12] and references therein). Furthermore, connections between strong seeded extractors and other objects of study such as list decodable codes, samplers, and expander graphs were found and enabled many applications.

### Nonmalleable extractors

A *nonmalleable extractor* is a strong seeded extractor that has the following additional property. The output of the extractor remains close to uniform even after observing the output of the extractor on any altered seed. Formally, let  $A: \{0, 1\}^d \rightarrow \{0, 1\}^d$  be an arbitrary function with no fixed points, that is,  $A(y) \neq y$  for all  $y$ . The reader should think of  $A$  as an adversarially chosen way of altering the seed. A function  $\text{Ext}: \{0, 1\}^n \times \{0, 1\}^d \rightarrow \{0, 1\}^m$  is a  $(k, \varepsilon)$ -*nonmalleable extractor* if for every  $(n, k)$ -source  $X$  and  $A$  as above,

$$(\text{Ext}(X, Y), \text{Ext}(X, A(Y)), Y) \approx_\varepsilon (U_m, \text{Ext}(X, A(Y)), Y), \quad (1.1)$$

where again  $Y$  is uniform over  $\{0, 1\}^d$  and is independent of  $X$ .

Nonmalleable extractors were introduced by Dodis and Wichs [DW09]. The original motivation for studying such extractors is for the classic problem of devising privacy amplification protocols against active adversaries. Indeed, strong seeded extractors yield a solution to the passive adversary variant. As we discuss later on, nonmalleable extractors proved key for the construction of good two-source extractors. More precisely, one requires a certain generalization obtained by considering more than one adversarial function [CRS12]. Let  $t \geq 1$  be an integer. The function  $\text{Ext}$  above is called a  $(k, \varepsilon)$   $t$ -nonmalleable extractor if for every  $t$ -tuple of functions  $A_1, \dots, A_t: \{0, 1\}^d \rightarrow \{0, 1\}^d$  with no fixed points, it holds that

$$(\text{Ext}(X, Y), \{\text{Ext}(X, A_i(Y))\}_{i=1}^t, Y) \approx_\varepsilon (U_m, \{\text{Ext}(X, A_i(Y))\}_{i=1}^t, Y).$$

In a sequence of works, nonmalleable extractors were constructed (see [DLWZ11, CRS12, Li15, Coh16a, CGL16, Coh16c, CS16, CL16, Coh16b, Li17] and references therein). The state-of-the-art construction of  $(k, \varepsilon)$ -nonmalleable extractors [Li19] has seed length  $d =$

$O(\log n) + \tilde{O}(\log \frac{1}{\varepsilon})$  for a comparable min-entropy  $k$ . All of these constructions generalize to  $t$ -nonmalleable extractors. Alternatively, a black-box reduction from  $t$ -nonmalleable extractors to nonmalleable extractors [Coh16c] can be invoked to give explicit  $t$ -nonmalleable extractors with seed length  $\text{poly}(t) \cdot d$ .

## 1.2 Strong, nonmalleable, and seed protecting extractors

As mentioned, in this work we introduce a new type of randomness extractors which we call *seed protecting extractors*. To give the formal definition, for an integer  $d$ , let  $\mathcal{A}_d$  be the set of all functions from  $\{0, 1\}^d$  to  $\{0, 1\}^d$ . When  $d$  is clear from context, we simply write  $\mathcal{A}$ .

**Definition 1.1** (seed protecting extractors). *Let  $\text{Ext}: \{0, 1\}^n \times \{0, 1\}^d \rightarrow \{0, 1\}^m$  be a  $(k, \varepsilon)$ -seeded extractor. Let  $\mathcal{C} \subseteq \mathcal{A}_d$ . We say that  $\text{Ext}$  is seed protecting against  $\mathcal{C}$  if for every  $A \in \mathcal{C}$  and every  $(n, k)$ -source  $X$  it holds that*

$$(Y, \text{Ext}(X, A(Y))) \approx_\varepsilon (U_d, \text{Ext}(X, A(Y))), \quad (1.2)$$

where  $Y$  is uniformly distributed and is independent of  $X$ .

Both nonmalleable extractors and seed protecting extractors have a certain resilience property against tempering of the seed. While nonmalleable extractors focus on the *output*, seed protecting extractors are concerned about the *seed*. This shift of focus induces inherent differences. Indeed, while fixed points trivially rule out the possibility of non malleability (hence, functions with fixed points are excluded by definition), fixed points turn out to be a non-issue for seed protecting extractors. Indeed, consider the extreme case – the identity function. Clearly, non malleability cannot be achieved against this function. However, note that to be seed protecting against the identity function precisely means to be a strong seeded extractor. In fact, the first observation we make in this preliminary discussion is that strong extractors are equivalent to seed protecting extractors against the class of permutations, which we denote by  $\Pi \subseteq \mathcal{A}_d$ .

**Claim 1.2** (strong  $\iff$  seed protecting against  $\Pi$ ). *Let  $\text{Ext}: \{0, 1\}^n \times \{0, 1\}^d \rightarrow \{0, 1\}^m$  be a  $(k, \varepsilon)$ -seeded extractor. Then,*

1. *If  $\text{Ext}$  is a  $(k, \varepsilon)$ -seed protecting extractor against  $\Pi$  then  $\text{Ext}$  is a  $(k, 2\varepsilon)$ -strong seeded extractor.*
2. *If  $\text{Ext}$  is a  $(k, \varepsilon)$ -strong seeded extractor then  $\text{Ext}$  is a  $(k, 2\varepsilon)$ -seed protecting extractor against  $\Pi$ .*

The proof of Claim 1.2 is straightforward. For completeness, we give it in Appendix A. Going back to nonmalleable extractors, by the discussion above, it is not a priori clear whether non malleability is in any way related to seed protection. Nonetheless, one of the

results of this work is an *equivalence* between the property of non malleability and seed protection, at least when focusing on permutation adversaries. By saying that  $\text{Ext}$  is a nonmalleable extractor against  $\mathcal{C} \subseteq \mathcal{A}$ , we mean that Equation (1.1) holds for every  $A \in \mathcal{C}$  (but not necessarily for other functions) that has no fixed points.

For stating our result, we generalize seed protection to several adversarial functions. This should be done with some care. Indeed, naively, one's first suggestion might require that for every two functions  $A_1, A_2 \in \mathcal{C}$ , it holds that

$$(Y, \text{Ext}(X, A_1(Y)), \text{Ext}(X, A_2(Y))) \approx_\varepsilon (U_d, \text{Ext}(X, A_1(Y)), \text{Ext}(X, A_2(Y))).$$

This definition, we observe, is moot. Indeed, consider two functions  $A_1, A_2: \{0, 1\}^d \rightarrow \{0, 1\}^d$  that according to the first bit of the seed,  $Y_1$ , decide whether to “behave” exactly the same or very differently. More concretely, sample three permutations  $\pi_0, \pi_1, \pi_2$  on  $\{0, 1\}^d$  at random, and define

$$A_1(y) = \begin{cases} \pi_0(y), & y_1 = 0; \\ \pi_1(y), & y_1 = 1. \end{cases} \quad A_2(y) = \begin{cases} \pi_0(y), & y_1 = 0; \\ \pi_2(y), & y_1 = 1. \end{cases}$$

As  $\pi_0, \pi_1, \pi_2$  were chosen at random, and thus are in “general position”, by observing  $\text{Ext}(X, A_1(Y)), \text{Ext}(X, A_2(Y))$  one can distinguish  $Y$ , in fact  $Y_1$ , from uniform by checking whether both outputs are equal.

As we prove, this “colluding” in which two, or more, adversarial functions attain the same value, is the only obstacle for seed protection against permutations (already here we stress that there are other obstacles when considering functions other than permutations, as we discuss in Section 1.3). Given  $A_1, \dots, A_t: \{0, 1\}^d \rightarrow \{0, 1\}^d$ , we say  $A_1, \dots, A_t$  are *non-colluding* if for every  $y \in \{0, 1\}^d$ , all the evaluations  $A_1(y), \dots, A_t(y)$  are distinct. We denote by  $\mathcal{X}^t \subseteq \mathcal{A}_d^t$  the set of  $t$ -tuples of functions that are non-colluding. With hindsight, we give the following generalization of seed protecting extractors to several adversarial functions.

**Definition 1.3.** *Let  $\text{Ext}: \{0, 1\}^n \times \{0, 1\}^d \rightarrow \{0, 1\}^m$  be a  $(k, \varepsilon)$ -seeded extractor. Let  $\mathcal{C} \subseteq \mathcal{A}$ . We say that  $\text{Ext}$  is  $t$ -seed protecting against  $\mathcal{C}$  if for every  $(n, k)$ -source  $X$  and  $(A_1, \dots, A_t) \in \mathcal{X}^t \cap \mathcal{C}^t$  it holds that*

$$(Y, \{\text{Ext}(X, A_i(Y))\}_{i=1}^t) \approx_\varepsilon (U_d, \{\text{Ext}(X, A_i(Y))\}_{i=1}^t).$$

*We also express this by saying that  $\text{Ext}$  is seed protecting against  $\mathcal{C}^t$ .*

The following lemma gives the easier direction, showing that nonmalleable extractors against permutations (with no fixed points) are seed protecting against (non-colluding) permutations. We refer the reader to Lemma 4.4 for a more general statement.

**Lemma 1.4.** *Let  $t \geq 1$  and assume  $\text{Ext}$  is a  $(k, \varepsilon)$ -non malleable extractor against  $\Pi^t$ . Then,  $\text{Ext}$  is a  $(k, 4t\varepsilon)$ -seed protecting extractor against  $\Pi^{t+1}$ .*

As a warm up, in Section 2, we prove Lemma 1.4 for  $t = 1$  as well as its converse which is indeed more surprising and difficult to prove (see Theorem 2.1).

### 1.3 Two-source extractors as seed protecting extractors

So far we have discussed seed protection only against permutations. This sufficed for characterizing both strong and nonmalleable extractors against permutations. But, what about other adversarial functions? Is it the case that seed protection is achievable against any single function? (of course, colluding is irrelevant in such setting). The quick answer is no. Surprisingly, our next result is a characterization we obtain for two-source extractors as 1-seed protecting extractors (namely, seed protecting extractors with a single adversarial function) against a suitable family. In particular, known impossibility results on two-source extractors translate to impossibility results on 1-seed protecting extractors.

Before recalling the formal definition of two-source extractors and describing this family, we believe it is instructive to first consider an extreme case and ask whether one can seed-protect against an adversarial function  $A$  that, unlike a permutation, is allowed to “focus” on seeds of its choice. The ultimate case is where  $A$  has image of size one. However, in such case,  $A(y)$  gives no information about the seed  $y$ , and so seed protecting trivially follows. What about image of size two? We have the following easy claim that establishes impossibility of seed protection against such functions. Let  $\mathcal{T} \subseteq \mathcal{A}_d$  be the set of all functions  $A: \{0, 1\}^d \rightarrow \{0, 1\}^d$  with image of size precisely two.

**Claim 1.5.** *Let  $\text{Ext}: \{0, 1\}^n \times \{0, 1\}^d \rightarrow \{0, 1\}$  be a  $(k, \varepsilon)$ -seeded extractor. Then, for  $k \leq n - 1$  and  $\varepsilon < \frac{1}{6}$ ,  $\text{Ext}$  is not  $(k, \varepsilon)$ -seed protecting against  $\mathcal{T}$ .*

We give the easy proof of Claim 1.5 in Appendix A. We next recall the definition of a two-source extractor or, more generally, of unbalanced two-source extractors, and then present our characterization of two-source extractors as seed protecting extractors. A  $(k_1, k_2, \varepsilon)$ -two-source extractor is a function  $\text{Ext}: \{0, 1\}^{n_1} \times \{0, 1\}^{n_2} \rightarrow \{0, 1\}^m$  such that for every  $(n_1, k_1)$ -source  $X$  and an independent  $(n_2, k_2)$ -source  $Y$  it holds that  $\text{Ext}(X, Y) \approx_\varepsilon U_m$ . The existence of a two-source extractor for min-entropies  $k_1 = \log n_2 + O(\log \frac{1}{\varepsilon})$  and  $k_2 = \log n_1 + O(\log \frac{1}{\varepsilon})$  with  $m = k_1 + k_2 - O(\log \frac{1}{\varepsilon})$  output bits was established by [CG88] but the problem of explicitly constructing a  $(k, k, \varepsilon)$ -two-source extractor with  $n_1 = n_2 = n$  even for min-entropy as high as  $k = 0.49n$  remained open for three decades [CG88, Bou05, Raz05].

Over the last few years, there has been remarkable progress on this problem. In particular, in a breakthrough work, Chattopadhyay and Zuckerman [CZ19] obtained a  $(k, k, \frac{1}{n})$ -two-source extractor  $\text{Ext}: \{0, 1\}^n \times \{0, 1\}^n \rightarrow \{0, 1\}$  for min-entropy as low as  $k = \text{poly}(\log n)$ . A subsequent line of work [BADTS17, Coh17, Li19] improved the entropy requirement even further to  $k = \tilde{O}(\log n)$ . Constructing two-source extractors for min-entropy  $O(\log n)$  (or, more ambitiously,  $\log(n) + O(1)$ ) is highly motivated by the problem of constructing explicit Ramsey graphs [BKS<sup>+</sup>10, BRSW12, Coh16d, Coh17]. A second important open problem is constructing two-source extractors with low error. Current techniques do not yield explicit two-source extractors when  $\varepsilon = o(1/n)$ .

Let  $\Delta \geq 0$  be a parameter. Define  $\mathcal{F}_\Delta$  to be the subset of  $\mathcal{A}_d$  containing all functions

$A: \{0, 1\}^d \rightarrow \{0, 1\}^d$  such that  $H_\infty(A(U_d)) \geq d - \Delta$ . For example, note that  $\mathcal{F}_0 = \Pi$ . Our main result here is proving an equivalence of two-source extractors and seed protecting extractors for a certain class.

**Theorem 1.6** (two-source extractors as seed protecting ones). *Let  $\text{Ext}: \{0, 1\}^n \times \{0, 1\}^d \rightarrow \{0, 1\}^m$ .*

1. *If  $\text{Ext}$  is  $(k_1, \varepsilon)$ -seed protecting extractor against  $\mathcal{F}_{d-k_2}$  then  $\text{Ext}$  is a  $(k_1, k_2, 3\varepsilon)$ -two-source extractor.*
2. *If  $\text{Ext}$  is a  $(k_1, k_2, \varepsilon)$ -two-source extractor which is strong in the second source <sup>1</sup> then  $\text{Ext}$  is  $(k_1, 2\varepsilon)$ -seed protecting against  $\mathcal{F}_{d-k_2}$ .*

Theorem 1.6 is proven in Section 5 (see Lemma 5.1 and Lemma 5.3 for the proof of each direction, respectively). By invoking a known lower bound result on the amount of min-entropy required for two-source extractors, Theorem 1.6 in particular implies that seed protection cannot be achieved against adversaries that are allowed to have small image. Claim 1.5 gives a direct proof of that for an extreme case of image size two. We find it insightful that the natural notion of seed protection gives a characterization of the three most well-studied types of randomness extractors: strong, two-source, and nonmalleable (against permutations).

Our main result gives a reduction from nonmalleable extractors against  $\mathcal{F}_\Delta$  to seed protecting extractors against  $\mathcal{F}_\Delta$ .

**Theorem 1.7.** *Let  $t \geq 1$  be an integer, and  $\Delta \geq \max(1, \log t)$ . Let  $\text{Ext}: \{0, 1\}^n \times \{0, 1\}^d \rightarrow \{0, 1\}^m$  be a  $(k, \varepsilon)$ -seed protecting extractor against  $\mathcal{F}_\Delta^{t+1} \cap \mathcal{X}^{t+1}$ . Assume further that  $d = \Omega(\log t)$ . Then,  $\text{Ext}$  is  $(k', \varepsilon')$ -nonmalleable against  $\mathcal{F}_\Delta^t$  with  $k' = k + mt + \log \frac{1}{\varepsilon}$  and  $\varepsilon' = O(\varepsilon^{1/3})$ .*

We prove Theorem 1.7 in Section 3.

## 1.4 Open problems

For which other classes  $\mathcal{C}$  do seed protecting extractors against  $\mathcal{C}$  exist? Can we get full-fledged non malleability (i.e., against general adversaries with no fixed points) from seed protecting extractors against these prospective  $\mathcal{C}$ -s? More generally, extending the connection between seed protecting and nonmalleable extractors is an intriguing open question left for future research.

---

<sup>1</sup>Note that this strongness requirement has the undesired effect of breaking the equivalence. However, one can always assume that a two-source extractor is strong in each of its sources provided one is willing to increase the error by a multiplicative factor of  $2^{O(m)}$ . See also a remark in the footnote of [Raz05] just prior to Definition 1.3.



Also, note that [Theorem 1.7](#) incurs  $tm$  entropy loss. Recall that nonmalleable extractors must satisfy  $k \geq (t + 1)m$ , as the  $t + 1$  outputs must be independent for a proper choice of adversaries. On the other hand, intuitively, this requirement is unnecessary for seed protecting extractors, and it seems that the only requirement should be  $k \geq m$  (we ignore the additive error dependence for simplicity). Having said that, we do not know how to formalize the intuition above regarding the entropy loss of seed protecting extractors. Indeed, in [Section 6](#) we prove the existence of seed protecting extractors via a probabilistic argument, and our proof technique requires  $k \geq tm$ . We leave the question of understanding the entropy loss of seed protecting extractors to future research.

## 2 Warm-up

As a warm-up, in this section we give a proof sketch for the equivalence between nonmalleable extractors and seed protecting extractors for permutations. For simplicity we focus on the case  $t = 1$ . The case  $t > 1$  follows by similar ideas but is somewhat more involved.

**Theorem 2.1** ( $\Pi$  nonmalleability  $\iff \Pi^2$  seed protection). *Let  $\text{Ext} : \{0, 1\}^n \times \{0, 1\}^d \rightarrow \{0, 1\}^m$ .*

1. *If  $\text{Ext}$  is  $(k, \varepsilon)$ -seed protecting against  $\Pi^2 \cap \mathcal{X}^2$  then  $\text{Ext}$  is  $(k', 14\varepsilon^{1/3})$ -nonmalleable against  $\Pi$ , where  $k' = k + 2m + O(\log(1/\varepsilon))$ .*
2. *If  $\text{Ext}$  is  $(k, \varepsilon)$ -nonmalleable against  $\Pi$  then  $\text{Ext}$  is  $(k, 3\varepsilon)$ -seed protecting extractor against  $\Pi^2 \cap \mathcal{X}^2$ .*

*Proof.* We start with the first and more difficult item.

### Proof sketch of the first item

Set  $\delta = 14\varepsilon^{1/3}$ . Assume towards a contradiction that  $\text{Ext}$  is not nonmalleable against  $\Pi$ . Consider then a source  $X \sim \{0, 1\}^n$  and adversarial permutation  $A \in \Pi$  with no fixed points for which

$$\text{SD}\left(\left(\text{Ext}(X, Y), \text{Ext}(X, A(Y)), Y\right), \left(U_m, \text{Ext}(X, A(Y)), Y\right)\right) > \delta,$$

where  $Y \sim \{0, 1\}^d$  is uniform and independent of  $X$ . That is,

$$\mathbf{E}_{y \sim Y} \left[ \text{SD}\left(\left(\text{Ext}(X, y), \text{Ext}(X, A(y))\right), \left(U_m, \text{Ext}(X, A(y))\right)\right) \right] > \delta. \quad (2.1)$$

For every  $y, y_1 \in \{0, 1\}^d$  we define the distributions

$$\begin{aligned} \mathcal{D}_{y, y_1} &= (\text{Ext}(X, y), \text{Ext}(X, y_1)), \\ \mathcal{I}_{y_1} &= (U_m, \text{Ext}(X, y_1)). \end{aligned}$$

Define the function  $T: \{0, 1\}^d \times \{0, 1\}^d \rightarrow [0, 1]$  by  $T(y, y_1) = \text{SD}(\mathcal{D}_{y, y_1}, \mathcal{I}_{y_1})$ . With this notation, Equation (2.1) can be written as  $\mathbf{E}_{y \sim Y} [T(y, A(y))] > \delta$ . By an averaging argument, there exists a set  $H \subseteq \{0, 1\}^d$  of size  $|H| = \frac{\delta}{2} \cdot 2^d$  such that  $T(y, A(y)) > \frac{\delta}{2}$  for every  $y \in H$ . Based on the fact that **Ext** is strong, we prove that there exists a subset  $B_1 \subseteq \{0, 1\}^d$  of density  $2\varepsilon^{1/3}$  such that for every  $y \notin B_1$ ,  $\mathbf{E}_{y_1 \sim U_d} [T(y, y_1)] \leq \varepsilon^{2/3}$ . We remark that this is where one pays  $2m + O(\log(1/\varepsilon))$  in the entropy loss. We choose to skip the proof of this fact (see Claim 3.4).

A main part of the proof is extending  $A|_H$ , the restriction of  $A$  to  $H$ , to a new permutation  $\widehat{A}$  over  $\{0, 1\}^d$  such that for almost every  $y$  outside of  $H$  it holds that  $T(y, \widehat{A}(y))$  is small, in particular, bounded by  $\varepsilon^{1/3}$ . This is done via a greedy algorithm. We arrange the elements of  $\{0, 1\}^d \setminus (H \cup B_1)$  in some order  $y_1, \dots, y_\ell$ . By an averaging argument, for every  $y \notin B_1$ , there are at most  $\varepsilon^{1/3}$  fraction of seeds  $y_1$  for which  $T(y, y_1) \geq \varepsilon^{1/3}$ . Denote this set by  $B(y)$ . We proceed iteratively, starting from  $i = 1$ , and choose an element  $z_i \notin B(y_i)$ , also different from  $y_i$ , that has not been assigned already as an image of (the partially defined)  $\widehat{A}$ , and set  $\widehat{A}(y_i) = z_i$ . This can be done for most  $y_i$ -s. When  $i$  gets very close to  $\ell$  we may have to assign the remaining images in any way, but which will still guarantee that  $\widehat{A}$  is a permutation. At any rate, for simplicity, let us assume that for all elements  $y_1, \dots, y_\ell$  we have that  $\widehat{A}(y_i) \notin B(y_i) \cup \{y_i\}$ .

Define the random variables  $\mathcal{D}_{\widehat{A}} = \mathcal{D}_{Y, \widehat{A}(Y)}$  and  $\mathcal{I}_{\widehat{A}} = \mathcal{I}_{\widehat{A}(Y)}$ , where  $Y$  is uniformly distributed over  $\{0, 1\}^d$ . Using the fact that **Ext** is seed protecting, we prove the following.

**Claim 2.2.** *There exists a set  $B_2 \subseteq \{0, 1\}^d$  of density at most  $\sqrt{\varepsilon}$  such that for every  $y \in \{0, 1\}^d \setminus B_2$ ,  $\text{SD}(\mathcal{D}_{\widehat{A}}, \mathcal{D}_{y, \widehat{A}(y)}) \leq \sqrt{\varepsilon}$ .*

*Proof.* Denote

$$\widehat{Z}(y) = \text{Ext}(X, \widehat{A}_1(y)).$$

With this notation, we have that

$$\begin{aligned} \mathcal{D}_{\widehat{A}} &= (\text{Ext}(X, Y), \widehat{Z}(Y)), \\ \mathcal{D}_{y, \widehat{A}(y)} &= (\text{Ext}(X, y), \widehat{Z}(y)). \end{aligned}$$

By construction,  $\widehat{A}$  is a permutation with no fixed points (more importantly, it does not collude with the identity function). Observe that as **Ext** is seed protecting against  $\Pi^2 \cap \mathcal{X}^2$  with error  $\varepsilon$ ,

$$\mathbf{E}_{y \sim U_d} [\text{SD}(\mathcal{D}_{y, \widehat{A}(y)}, \mathcal{D}_{\widehat{A}})] \leq \varepsilon.$$

By Markov's inequality, the set  $B_2 \subseteq \{0, 1\}^d$  of all  $y$ -s satisfying  $\text{SD}((\mathcal{D}_{y, \widehat{A}(y)}, \mathcal{D}_{\widehat{A}})) \geq \sqrt{\varepsilon}$  has density at most  $\sqrt{\varepsilon}$ , as stated. □

Similarly to the proof of Claim 2.2, we prove,

**Claim 2.3.** *There exists a set  $B_3 \subseteq \{0, 1\}^d$  of density at most  $\sqrt{\varepsilon}$  such that for every  $y \in \{0, 1\}^d \setminus B_3$ ,  $\text{SD}(\mathcal{I}_{\hat{A}}, \mathcal{I}_{\hat{A}(y)}) \leq \sqrt{\varepsilon}$ .*

Write  $B = B_1 \cup B_2 \cup B_3$ . Recall that  $|H| = \frac{\delta}{2} \cdot 2^d = 7\varepsilon^{1/3} \cdot 2^d$ . By the above claims we can bound  $|B| < 7\varepsilon^{1/3} \cdot 2^d$ , and so there exists  $y_h \in H \setminus B$ . Take  $y_\ell \in \{0, 1\}^d \setminus (H \cup B)$ . By Claim 2.2, since  $y_\ell, y_h \notin B_2$ ,  $\text{SD}(\mathcal{D}_{y_h, \hat{A}(y_h)}, \mathcal{D}_{\hat{A}}) \leq \sqrt{\varepsilon}$  and  $\text{SD}(\mathcal{D}_{y_\ell, \hat{A}(y_\ell)}, \mathcal{D}_{\hat{A}}) \leq \sqrt{\varepsilon}$ . Hence,

$$\text{SD}\left(\mathcal{D}_{y_\ell, \hat{A}(y_\ell)}, \mathcal{D}_{y_h, \hat{A}(y_h)}\right) \leq 2\sqrt{\varepsilon}. \quad (2.2)$$

By Claim 2.3 and since  $y_\ell, y_h \notin B_3$ ,  $\text{SD}(\mathcal{I}_{\hat{A}(y_h)}, \mathcal{I}_{\hat{A}}) \leq \sqrt{\varepsilon}$  and  $\text{SD}(\mathcal{I}_{\hat{A}(y_\ell)}, \mathcal{I}_{\hat{A}}) \leq \sqrt{\varepsilon}$ . Thus,

$$\text{SD}\left(\mathcal{I}_{\hat{A}(y_\ell)}, \mathcal{I}_{\hat{A}(y_h)}\right) \leq 2\sqrt{\varepsilon}. \quad (2.3)$$

Now, since  $y_\ell \in \{0, 1\}^d \setminus (H \cup B_1)$ ,

$$\text{SD}\left(\mathcal{D}_{y_\ell, \hat{A}(y_\ell)}, \mathcal{I}_{\hat{A}(y_\ell)}\right) \leq \varepsilon^{1/3}. \quad (2.4)$$

By Equations (2.2) to (2.4) and the triangle inequality,  $\text{SD}(\mathcal{D}_{y_h, \hat{A}(y_h)}, \mathcal{I}_{\hat{A}(y_h)}) \leq 5\varepsilon^{1/3}$ . However,  $y_h \in H$  and so

$$\text{SD}\left(\mathcal{D}_{y_h, \hat{A}(y_h)}, \mathcal{I}_{\hat{A}(y_h)}\right) = T\left(y_h, \hat{A}(y_h)\right) = T(y_h, A(y_h)) > \frac{\delta}{2},$$

contradicting our choice of  $\delta$ . This proves the first item.

### Proof sketch of the second item

Moving on to the second item, let  $A_1, A_2 \in \Pi$  be non colluding. Let  $X$  be an  $(n, k)$ -source, and let  $Y \sim \{0, 1\}^d$  be a uniform random variable, independent of  $X$ . Denote

$$Z(y) = (\text{Ext}(X, A_1(y)), \text{Ext}(X, A_2(y))).$$

As  $A_1^{-1}$  is a permutation,  $A_1^{-1}(Y)$  distributes the same as  $Y$  does. Thus,

$$\text{SD}((U_d, Z(Y)), (Y, Z(Y))) = \text{SD}((U_d, Z(A_1^{-1}(Y))), (A_1^{-1}(Y), Z(A_1^{-1}(Y)))).$$

By the data-processing inequality,<sup>2</sup> we can apply  $A_1$  on the prefix of both random variables without increasing the statistical distance; The above equation then becomes

$$\text{SD}((U_d, Z(Y)), (Y, Z(Y))) = \text{SD}((U_d, Z(A_1^{-1}(Y))), (Y, Z(A_1^{-1}(Y)))). \quad (2.5)$$

---

<sup>2</sup>By this we refer to the fact that for any random variables  $X, Y \sim \Omega_1$ , and every  $f: \Omega_1 \rightarrow \Omega_2$ , possibly randomized,  $\text{SD}(f(X), f(Y)) \leq \text{SD}(X, Y)$ . Equality is attained when  $f$  is injective.

Define  $P = A_2 \circ A_1^{-1}$ . Then,

$$Z(A_1^{-1}(Y)) = (\text{Ext}(X, Y), \text{Ext}(X, P(Y))).$$

Note that  $P$  is a permutation. Furthermore, observe that as  $(A_1, A_2) \in \mathcal{X}^2$ ,  $P$  has no fixed points. Indeed, assuming towards a contradiction that  $P(y) = y$  for some  $y \in \{0, 1\}^d$ , we get that  $A_1^{-1}(y) = A_2^{-1}(y)$ , which is impossible. By the non malleability of  $\text{Ext}$ , we know that

$$\text{SD}((Y, Z(A_1^{-1}(Y))), (Y, U_m, \text{Ext}(X, P(Y)))) \leq \varepsilon,$$

Thus, by the triangle inequality, we get

$$\begin{aligned} \text{SD}((U_d, Z(A_1^{-1}(Y))), (Y, Z(A_1^{-1}(Y)))) &\leq \text{SD}((U_d, Z(A_1^{-1}(Y))), (U_d, U_m, \text{Ext}(X, P(Y)))) + \\ &\quad \text{SD}((U_d, U_m, \text{Ext}(X, P(Y))), (Y, U_m, \text{Ext}(X, P(Y)))) + \\ &\quad \text{SD}((Y, U_m, \text{Ext}(X, P(Y))), (Y, Z(A_1^{-1}(Y)))) \\ &\leq 3\varepsilon. \end{aligned} \tag{2.6}$$

The proof then follows by Equation (2.5).  $\square$

### 3 Seed protecting extractors for high entropy adversaries are nonmalleable

In this section we prove Theorem 1.7, showing that a seed protecting extractor with adversarial entropy parameter  $\Delta$  is non-malleable against roughly the same adversarial function class.

**Definition 3.1** (non-colluding functions). *We say that a tuple  $(A_1, \dots, A_t) \in \mathcal{A}_d^t$  do not collude, if for every  $y \in \{0, 1\}^d$ ,  $A_1(y), \dots, A_t(y)$  are pairwise distinct. When  $d$  is clear from context, we denote by  $\mathcal{X}^t$  the set of  $t$ -tuples of non-colluding functions from  $\{0, 1\}^d$  to  $\{0, 1\}^d$ .*

We prove the following slight restatement of Theorem 1.7.

**Theorem 3.2.** *Let  $t \geq 1$  be an integer, and  $\Delta \geq 0$ . Let  $\text{Ext}: \{0, 1\}^n \times \{0, 1\}^d \rightarrow \{0, 1\}^m$  be a  $(k, \varepsilon)$ -seeded extractor with  $d \geq 2 \log t + \log \frac{1}{\varepsilon} + 2$  and  $\varepsilon \leq 10^{-4}$ . Assume that  $\text{Ext}$  is seed protecting against  $\mathcal{F}_{\max(\Delta, \log t, 1)}^{t+1} \cap \mathcal{X}^{t+1}$ . Then,  $\text{Ext}$  is nonmalleable against  $(\mathcal{F}_\Delta \cap \mathcal{N})^t \cap \mathcal{X}^t$  for min-entropy  $k + mt + \log \frac{1}{\varepsilon}$  and error guarantee  $14\varepsilon^{1/3}$ .*

Note that the non malleability guaranteed by Theorem 3.2 is with respect to  $(\mathcal{F}_\Delta \cap \mathcal{N})^t \cap \mathcal{X}^t$ . That is, non-colluding is still required. In Section 3.1 we show how to get rid of this requirement in a “black-box” fashion.

*Proof of Theorem 3.2.* Assume towards a contradiction that  $\text{Ext}$  is not nonmalleable against  $(\mathcal{F}_\Delta \cap \mathcal{N})^t$  for min-entropy  $k' = k + mt + \log(1/\varepsilon)$ . Then, there exists an  $(n, k')$  source  $X$  and functions  $A_1, \dots, A_t \in \mathcal{F}_\Delta \cap \mathcal{N}$  with  $(A_1, \dots, A_t) \in \mathcal{X}^t$ , such that

$$\text{SD}\left(\left(\text{Ext}(X, Y), \text{Ext}(X, A_1(Y)), \dots, \text{Ext}(X, A_t(Y)), Y\right), \left(U_m, \text{Ext}(X, A_1(Y)), \dots, \text{Ext}(X, A_t(Y)), Y\right)\right) > \delta,$$

for  $\delta = 14\varepsilon^{1/3}$ , where  $Y \sim \{0, 1\}^d$  is uniform and independent of  $X$ . That is,

$$\mathbf{E}_{y \sim Y} \left[ \text{SD}\left(\left(\text{Ext}(X, y), \text{Ext}(X, A_1(y)), \dots, \text{Ext}(X, A_t(y))\right), \left(U_m, \text{Ext}(X, A_1(y)), \dots, \text{Ext}(X, A_t(y))\right)\right) \right] > \delta. \quad (3.1)$$

For  $y, y_1, \dots, y_t \in \{0, 1\}^d$  define the distributions

$$\begin{aligned} \mathcal{D}_{y, y_1, \dots, y_t} &= (\text{Ext}(X, y), \text{Ext}(X, y_1), \dots, \text{Ext}(X, y_t)), \\ \mathcal{I}_{y_1, \dots, y_t} &= (U_m, \text{Ext}(X, y_1), \dots, \text{Ext}(X, y_t)). \end{aligned}$$

Define the function  $T: (\{0, 1\}^d)^{t+1} \rightarrow [0, 1]$  as follows. For  $y, y_1, \dots, y_t \in \{0, 1\}^d$ ,

$$T(y, y_1, \dots, y_t) = \text{SD}(\mathcal{D}_{y, y_1, \dots, y_t}, \mathcal{I}_{y_1, \dots, y_t}).$$

With this notation, Equation (3.1) can be written as  $\mathbf{E}_{y \sim Y} [T(y, A_1(y), \dots, A_t(y))] > \delta$ . By an averaging argument, there exists a set  $H \subseteq \{0, 1\}^d$  of size  $|H| = (\delta/2) \cdot 2^d$  such that for every  $y \in H$ ,

$$T(y, A_1(y), \dots, A_t(y)) > \frac{\delta}{2}.$$

Let  $Y_1, \dots, Y_t$  be independent random variables, that are jointly independent of  $X$ , and each  $Y_i$  is uniformly distributed over  $\{0, 1\}^d$ . Denote

$$Z = \text{Ext}(X, Y_1) \circ \dots \circ \text{Ext}(X, Y_t).$$

For  $z = (z_1, \dots, z_t) \in (\{0, 1\}^m)^t$  define the random variable  $X_z = X \mid \{Z = z\}$ .

**Claim 3.3.** *There exists a set  $B' \subseteq (\{0, 1\}^m)^t$  such that:*

1.  $\Pr[Z \in B'] \leq \varepsilon$ , and,
2. For every  $z \notin B'$ ,  $H_\infty(X_z) \geq H_\infty(X) - tm - \log(1/\varepsilon) \geq k$ .

*Proof.* Fix  $z \in (\{0, 1\}^m)^t$  and observe that

$$H_\infty(X_z) \geq H_\infty(X) - \log\left(\frac{1}{\Pr[Z = z]}\right). \quad (3.2)$$

Define  $B' = \{z : \Pr[Z = z] \leq 2^{-mt}\varepsilon\}$ . By Equation (3.2), for every  $z \notin B'$ , Item 2 holds. As  $B' \subseteq \{0, 1\}^{mt}$ ,

$$\Pr[Z \in B'] = \sum_{z \in B'} \Pr[Z = z] \leq |B'| \cdot 2^{-mt}\varepsilon \leq \varepsilon,$$

and so Item 1 follows as well.  $\square$

**Claim 3.4.** *There exists a subset  $B_1 \subseteq \{0, 1\}^d$  of size  $|B_1| \leq 2\varepsilon^{1/3} \cdot 2^d$  such that for every  $y \notin B_1$ ,*

$$\mathbf{E}_{(y_1, \dots, y_t) \sim U_{td}} [T(y, y_1, \dots, y_t)] \leq \varepsilon^{2/3}.$$

*Proof.* Recall the definition of  $X_z$  and  $B'$  from Claim 3.3. Fix  $z \notin B'$ . Let  $Y$  be uniform over  $\{0, 1\}^d$  and independent of  $(X, Y_1, \dots, Y_t)$ . Note that conditioned on the event  $Z = z$ , the random variables  $X_z, Y$  are independent, and, furthermore,  $Y$  is uniformly distributed over  $\{0, 1\}^d$ . In addition, as  $z \notin B'$ ,  $H_\infty(X_z) \geq k$ . Thus, as  $\text{Ext}$  is a strong  $(k, \varepsilon)$  seeded extractor,

$$(\text{Ext}(X_z, Y), Y) \approx_\varepsilon (U_m, Y).$$

Let  $Z'$  be the distribution obtained by sampling  $z \sim Z$  conditioned on  $z \notin B'$ . Then,

$$\begin{aligned} T(Y, Y_1, \dots, Y_t) &= \text{SD}((\text{Ext}(X, Y), Z, Y), (U_m, Z, Y)) \\ &= \mathbf{E}_{z \sim Z} [\text{SD}((\text{Ext}(X_z, Y), Y), (U_m, Y))] \\ &\leq \Pr[Z \in B'] + \mathbf{E}_{z' \sim Z'} [\text{SD}((\text{Ext}(X_{z'}, Y), Y), (U_m, Y))] \leq 2\varepsilon. \end{aligned}$$

By Markov's inequality, there exists a subset  $B_1 \subseteq \{0, 1\}^d$  of size  $|B_1| \leq 2\varepsilon^{1/3} \cdot 2^d$  such that for every  $y \notin B_1$ ,

$$T(y, Y_1, \dots, Y_t) \leq \varepsilon^{2/3}.$$

Thus, as  $Y_1, \dots, Y_t$  are independent, we get that for every  $y \notin B_1$ ,

$$\mathbf{E}_{(y_1, \dots, y_t) \sim U_{td}} [T(y, y_1, \dots, y_t)] \leq \varepsilon^{2/3},$$

concluding the proof of the claim.  $\square$

**Proposition 3.5.** *There exist  $(\hat{A}_1, \dots, \hat{A}_t) \in \mathcal{F}_{\max(\Delta, \log t, 1)}^t \cap \mathcal{X}^t$  and  $B_2 \subseteq \{0, 1\}^d$  of size  $|B_2| \leq 3\varepsilon^{1/3} \cdot 2^d + t$  such that*

1. For every  $y \in H$ ,  $\hat{A}_j(y) = A_j(y)$ , and,
2. For every  $y \in \{0, 1\}^d \setminus (H \cup B_2)$  it holds that  $T(y, \hat{A}_1(y), \dots, \hat{A}_t(y)) \leq \varepsilon^{1/3}$ .

*Proof.* Denote  $\beta = 2^{-d} \cdot |B_1 \setminus H|$ . By [Claim 3.4](#),  $\beta \leq 2\varepsilon^{1/3}$ . Moreover, by Markov's inequality, for every  $y \notin B_1$ , there exists  $B(y) \subseteq (\{0, 1\}^d)^t$  of size at most  $|B(y)| \leq \varepsilon^{1/3} \cdot 2^{dt}$  such that for every  $(y_1, \dots, y_t) \notin B(y)$ ,

$$T(y, y_1, \dots, y_t) \leq \varepsilon^{1/3}.$$

Let  $L = \{0, 1\}^d \setminus (H \cup B_1)$ . Fix an (arbitrary) ordering of the elements in  $L$  and denote them by  $y^1, y^2, \dots, y^{|L|}$ . Let  $c$  to be the least integer larger than  $\max(\varepsilon^{1/3} \cdot 2^d, t)$ , and set  $\ell = |L| - c$ . Denote

$$B_2 = (B_1 \setminus H) \cup \{y^{\ell+1}, \dots, y^{|L|}\},$$

observing that indeed

$$|B_2| \leq |B_1| + |L| - \ell = |B_1| + c \leq 3\varepsilon^{1/3} \cdot 2^d + t.$$

We define a family of functions

$$\left\{ \widehat{A}_{j,m} : 1 \leq j \leq t, 0 \leq m \leq \ell \right\},$$

where  $\widehat{A}_{j,0}: H \rightarrow \{0, 1\}^d$  and for  $m \geq 1$ ,

$$\widehat{A}_{j,m}: H \cup \{y^1, \dots, y^m\} \rightarrow \{0, 1\}^d.$$

The above functions are constructed via the following algorithm which proceeds iteratively on  $m$ .

### The construction algorithm for the $\widehat{A}_{j,m}$ functions

1. For every  $j \in [t]$ , set  $\widehat{A}_{j,0} = A_j|_H$ .
2. For  $m = 1, \dots, \ell$ , we will show in [Claim 3.6](#) below that there exists  $(y_1^m, \dots, y_t^m) \in (\{0, 1\}^d)^t \setminus B(y^m)$  such that  $y^m, y_1^m, \dots, y_t^m$  are pairwise distinct; furthermore, for every  $j \in [t]$ ,  $|\widehat{A}_{j,m-1}^{-1}(y_j^m)| < t$ . Under these assumptions, for every  $j \in [t]$  and  $y \in H \cup \{y^1, \dots, y^m\}$ , set

$$\widehat{A}_{j,m}(y) = \begin{cases} y_j^m & y = y^m; \\ \widehat{A}_{j,m-1}(y) & \text{otherwise.} \end{cases}$$

**Claim 3.6.** *The underlying assumption of Step 2 in the algorithm above holds for every  $m \in [\ell]$ .*

*Proof.* We begin by setting notation. For every  $m \in [\ell]$  and  $j \in [t]$ , we define the set  $G_j^m \subseteq \{0, 1\}^d \setminus \{y^m\}$  of elements whose preimage is of size strictly less than  $t$  with respect to the function  $\widehat{A}_{j,m-1}$ . Formally,

$$G_j^m = \left\{ y \in \{0, 1\}^d \setminus \{y^m\} : \left| \widehat{A}_{j,m-1}^{-1}(y) \right| < t \right\}.$$

With this notation, the hypothesis underlying Step 2 holds at iteration  $m$  if there exists an element in  $(G_1^m \times \cdots \times G_t^m) \setminus B(y^m)$  with pairwise distinct entries. To establish this, we start by bounding the size of  $G_j^m$  from below for every fixed  $j \in [t]$ .

For an element  $y$  not to be contained in  $G_j^m$  there must be at least  $t$  elements whose image under  $\widehat{A}_{j,m-1}$  is  $y$ . At the beginning of the  $m^{\text{th}}$  iteration,  $m-1$  elements have been assigned an image at Step 2 and additional  $|H| = \frac{\delta}{2} \cdot 2^d$  elements were assigned at Step 1. Hence,

$$\begin{aligned} |G_j^m| &\geq |\{0, 1\}^d \setminus \{y^m\}| - \frac{|H| + m - 1}{t} \\ &\geq 2^d - 1 - \frac{|H| + \ell - 1}{t}. \end{aligned} \quad (3.3)$$

As  $\ell = |L| - c$  and since  $L \cap H = \emptyset$  we have that

$$|H| + \ell = |H| + |L| - c \leq |H \cup L| - c \leq 2^d - c,$$

and so

$$|G_j^m| \geq \left(1 - \frac{1}{t}\right) 2^d + \frac{c+1}{t} - 1.$$

Thus, as  $y^m \notin B_1$ ,

$$|(G_1^m \times \cdots \times G_t^m) \setminus B(y^m)| \geq \left( \left(1 - \frac{1}{t}\right) 2^d + \frac{c+1}{t} - 1 \right)^t - \varepsilon^{1/3} \cdot 2^d. \quad (3.4)$$

Let  $\text{NE} \subseteq (\{0, 1\}^d)^t$  be the set of vectors  $v \in (\{0, 1\}^d)^t$  such that  $v_i \neq v_j$  for every pair of distinct  $i, j \in [t]$ . With this notation, to prove that the assumption underlying Step 2 holds at step  $m$ , one must show that

$$((G_1^m \times \cdots \times G_t^m) \setminus B(y^m)) \cap \text{NE} \neq \emptyset. \quad (3.5)$$

To this end, note that  $|(\{0, 1\}^d)^t \setminus \text{NE}| \leq \binom{t}{2} 2^{(t-1)d}$ . Thus, by Equation (3.4), it suffices to show that

$$\left( \left(1 - \frac{1}{t}\right) 2^d + \frac{c+1}{t} - 1 \right)^t > \varepsilon^{1/3} \cdot 2^d + \binom{t}{2} 2^{(t-1)d}. \quad (3.6)$$

For  $t = 1$ , Equation (3.6) is equivalent to  $c > \varepsilon^{1/3} \cdot 2^d$  which readily follows by the definition of  $c$ . Consider then  $t \geq 2$ . By definition,  $c \geq t$  and so  $\frac{c+1}{t} - 1 > 0$ . Note further that  $(1 - \frac{1}{t})^t \geq \frac{1}{4}$ . Therefore, to satisfy Equation (3.6), it suffices to establish that

$$\frac{1}{4} \cdot 2^{dt} \geq \varepsilon^{1/3} \cdot 2^d + \binom{t}{2} 2^{(t-1)d}.$$

It is straightforward to verify that the above equation follows per our assumption  $d \geq 2 \log t + 2$ . □



We turn to extend the functions  $\widehat{A}_{1,\ell}, \dots, \widehat{A}_{t,\ell}$  to the domain  $\{0, 1\}^d$ . To this end, let  $D = \{0, 1\}^d \setminus (H \cup \{y^1, \dots, y^\ell\})$  and denote its elements by  $y^{\ell+1}, \dots, y^{\ell+e}$ . For  $m = 1, \dots, e$  we define the function

$$\widehat{A}_{j,\ell+m}: D \cup \{y^{\ell+1}, \dots, y^{\ell+m}\} \rightarrow \{0, 1\}^d$$

using the following iterative algorithm.

**The algorithm for extending  $\widehat{A}_{j,\ell}$  to  $\widehat{A}_j$**

1. For  $m = 1, \dots, e$ , we will show in [Claim 3.7](#) below that there exist pairwise distinct  $y_1^{\ell+m}, \dots, y_t^{\ell+m} \in \{0, 1\}^d \setminus \{y^{\ell+m}\}$  such that for every  $j \in [t]$ ,  $|\widehat{A}_{j,\ell+m-1}^{-1}(y_j^{\ell+m})| \leq 1$ . Under these assumptions, for every  $j \in [t]$  and  $y \in H \cup \{y^1, \dots, y^{\ell+m}\}$ , set

$$\widehat{A}_{j,\ell+m}(y) = \begin{cases} y_j^{\ell+m} & y = y^{\ell+m}; \\ \widehat{A}_{j,\ell+m-1}(y) & \text{otherwise.} \end{cases}$$

2. For  $j \in [t]$ , set  $\widehat{A}_j = \widehat{A}_{j,e}$ .

**Claim 3.7.** *The underlying assumption in Step 1 of the algorithm above holds.*

*Proof.* Fix  $m \in [e]$ . For every  $j \in [t]$ , the number of elements  $z$  for which  $|\widehat{A}_{j,\ell+m-1}^{-1}(z)| \geq 2$  is bounded above by  $\frac{1}{2} \cdot 2^d$ . Thus, when setting  $\widehat{A}_{j,\ell+m}(y^{\ell+m})$  one has at least  $2^d/2$  choices for an image with respect to this restriction. Recall that we also need to guarantee that

$$y^{\ell+m}, \widehat{A}_{1,\ell+m}(y^{\ell+m}), \dots, \widehat{A}_{t,\ell+m}(y^{\ell+m})$$

are pairwise distinct. This can be achieved as  $\frac{1}{2} \cdot 2^d + t + 1 < 2^d$  per our assumption  $d \geq 2 \log t + 2$ .  $\square$

**Analyzing the  $\widehat{A}$  functions.** First, note that the domain of each  $\widehat{A}_1, \dots, \widehat{A}_t$  is  $\{0, 1\}^d$ . Recall that each of  $A_1, \dots, A_t$  has no fixed points by assumption and, furthermore, are non-colluding. Thus,  $\widehat{A}_1, \dots, \widehat{A}_t$  have no fixed points and are non-colluding when restricted to  $H$ . Moreover, by construction, the functions  $\widehat{A}_1, \dots, \widehat{A}_t$  are defined to have no fixed points and to be non-colluding outside of  $H$  as well. Thus,  $(\text{id}, \widehat{A}_1, \dots, \widehat{A}_t) \in \mathcal{X}^{t+1}$ , where  $\text{id}: \{0, 1\}^d \rightarrow \{0, 1\}^d$  is the identity function.

We turn to show that  $\widehat{A}_j \in \mathcal{F}_{\max(\Delta, \log t, 1)}$  for every  $j \in [t]$ . Recall that  $A_j \in \mathcal{F}_\Delta$ . Both algorithms above assure that for any  $j \in [t]$ , and  $y \notin \text{Im}(\widehat{A}_j|_H)$  it holds that,  $|\widehat{A}_j^{-1}(y)| \leq \max(t, 2)$ . Observe that  $f \in \mathcal{F}_{\log t}$  if and only if for every  $y \in \text{Im}(f)$ ,  $|f^{-1}(y)| \leq t$ , and so it holds that

$$\widehat{A}_j \in \mathcal{F}_\Delta \cup \mathcal{F}_{\log \max(t, 2)} = \mathcal{F}_{\max(\Delta, \log t, 1)}.$$

This concludes the proof of [Proposition 3.5](#).  $\square$

We turn back to the proof of [Theorem 3.2](#). Define the random variables

$$\begin{aligned}\mathcal{D}_{\widehat{A}} &= \mathcal{D}_{Y, \widehat{A}(Y)}, \\ \mathcal{I}_{\widehat{A}} &= \mathcal{I}_{\widehat{A}(Y)},\end{aligned}$$

where  $Y$  is uniformly distributed over  $\{0, 1\}^d$  and  $\widehat{A}(Y) = (\widehat{A}_1(Y), \dots, \widehat{A}_t(Y))$ .

**Claim 3.8.** *There exists a set  $B_3 \subseteq \{0, 1\}^d$  of size  $|B_3| \leq \sqrt{\varepsilon} \cdot 2^d$  such that for every  $y \in \{0, 1\}^d \setminus B_3$ ,*

$$\text{SD}\left(\mathcal{D}_{\widehat{A}}, \mathcal{D}_{y, \widehat{A}(y)}\right) \leq \sqrt{\varepsilon}.$$

*Proof.* Denote

$$\widehat{Z}(y) = \left(\text{Ext}(X, \widehat{A}_1(y)), \dots, \text{Ext}(X, \widehat{A}_t(y))\right).$$

With this notation,

$$\begin{aligned}\mathcal{D}_{\widehat{A}} &= \left(\text{Ext}(X, Y), \widehat{Z}(Y)\right), \\ \mathcal{D}_{y, \widehat{A}(y)} &= \left(\text{Ext}(X, y), \widehat{Z}(y)\right).\end{aligned}$$

By [Proposition 3.5](#),  $\widehat{A}_1, \dots, \widehat{A}_t \in \mathcal{F}_{\max(\Delta, \log t, 1)}$ ; moreover, note that  $\text{id} \in \mathcal{F}_{\max(\Delta, \log t, 1)}$ . Observe that as  $\text{Ext}$  is seed protecting against  $\mathcal{F}_{\max(\Delta, \log t, 1)}^{t+1}$ , and since  $(\text{id}, \widehat{A}_1, \dots, \widehat{A}_t) \in \mathcal{X}^{t+1}$ , it holds that

$$\mathbf{E}_{y \sim U_d} \left[ \text{SD}\left(\left(\text{Ext}(X, y), \widehat{Z}(y)\right), \left(\text{Ext}(X, Y), \widehat{Z}(Y)\right)\right) \right] \leq \varepsilon. \quad (3.7)$$

Let  $B_3 \subseteq \{0, 1\}^d$  be the set of all  $y$ -s satisfying

$$\text{SD}\left(\left(\text{Ext}(X, y), \widehat{Z}(y)\right), \left(\text{Ext}(X, Y), \widehat{Z}(Y)\right)\right) \geq \sqrt{\varepsilon}.$$

By Markov's inequality, it follows that  $|B_3| \leq \sqrt{\varepsilon} \cdot 2^d$ , as stated. □

**Claim 3.9.** *There exists a set  $B_4 \subseteq \{0, 1\}^d$  of size  $|B_4| \leq \sqrt{\varepsilon} \cdot 2^d$  such that for every  $y \in \{0, 1\}^d \setminus B_4$ ,*

$$\text{SD}\left(\mathcal{I}_{\widehat{A}}, \mathcal{I}_{\widehat{A}(y)}\right) \leq \sqrt{\varepsilon}.$$

*Proof.* Note that for every  $y \in \{0, 1\}^d$  it holds that

$$\text{SD}\left(\mathcal{I}_{\widehat{A}}, \mathcal{I}_{\widehat{A}(y)}\right) = \text{SD}\left(\widehat{Z}(Y), \widehat{Z}(y)\right).$$

By [Equation \(3.7\)](#),

$$\mathbf{E}_{y \sim U_d} \left[ \text{SD}\left(\mathcal{I}_{\widehat{A}}, \mathcal{I}_{\widehat{A}(y)}\right) \right] \leq \varepsilon.$$

Let  $B_4 \subseteq \{0, 1\}^d$  be the set of all  $y$ -s satisfying

$$\text{SD}(\mathcal{I}_{\hat{A}}, \mathcal{I}_{\hat{A}(y)}) \geq \sqrt{\varepsilon}.$$

By Markov's inequality, it follows that  $|B_4| \leq \sqrt{\varepsilon} \cdot 2^d$ , as stated.  $\square$

We are now ready to complete the proof. Write  $B = B_1 \cup B_2 \cup B_3 \cup B_4$ . Recall that

$$|H| = \frac{\delta}{2} \cdot 2^d = 7\varepsilon^{1/3} \cdot 2^d.$$

By the above claims and using our hypothesis on  $d$ ,

$$|B| \leq (5\varepsilon^{1/3} + 2\sqrt{\varepsilon}) \cdot 2^d + t < 7\varepsilon^{1/3} \cdot 2^d,$$

and so there exists  $y_h \in H \setminus B$ . On the other hand,

$$|H \cup B| \leq \left( \frac{\delta}{2} + 5\varepsilon^{1/3} + 2\sqrt{\varepsilon} \right) 2^d + t < 2^d,$$

where the last inequality follows as  $\varepsilon \leq 10^{-4}$  and, again, using our hypothesis on  $d$ . Hence, there exists  $y_\ell \in \{0, 1\}^d \setminus (H \cup B)$ .

By [Claim 3.8](#), since  $y_\ell, y_h \notin B_3$ ,

$$\begin{aligned} \text{SD}(\mathcal{D}_{y_h, \hat{A}(y_h)}, \mathcal{D}_{\hat{A}}) &\leq \sqrt{\varepsilon}, \\ \text{SD}(\mathcal{D}_{y_\ell, \hat{A}(y_\ell)}, \mathcal{D}_{\hat{A}}) &\leq \sqrt{\varepsilon}, \end{aligned}$$

and so

$$\text{SD}(\mathcal{D}_{y_\ell, \hat{A}(y_\ell)}, \mathcal{D}_{y_h, \hat{A}(y_h)}) \leq 2\sqrt{\varepsilon}. \quad (3.8)$$

By [Claim 3.9](#) and since  $y_\ell, y_h \notin B_4$ ,

$$\begin{aligned} \text{SD}(\mathcal{I}_{\hat{A}(y_h)}, \mathcal{I}_{\hat{A}}) &\leq \sqrt{\varepsilon}, \\ \text{SD}(\mathcal{I}_{\hat{A}(y_\ell)}, \mathcal{I}_{\hat{A}}) &\leq \sqrt{\varepsilon}. \end{aligned}$$

Thus,

$$\text{SD}(\mathcal{I}_{\hat{A}(y_\ell)}, \mathcal{I}_{\hat{A}(y_h)}) \leq 2\sqrt{\varepsilon}. \quad (3.9)$$

Now, since  $y_\ell \in \{0, 1\}^d \setminus (H \cup B_2)$ , by [Item 2 of Proposition 3.5](#),

$$\text{SD}(\mathcal{D}_{y_\ell, \hat{A}(y_\ell)}, \mathcal{I}_{\hat{A}(y_\ell)}) \leq \varepsilon^{1/3}. \quad (3.10)$$

By [Equations \(3.8\) to \(3.10\)](#) and the triangle inequality,

$$\text{SD}(\mathcal{D}_{y_h, \hat{A}(y_h)}, \mathcal{I}_{\hat{A}(y_h)}) \leq 5\varepsilon^{1/3}.$$

However,  $y_h \in H$  and so

$$\begin{aligned} \text{SD} \left( \mathcal{D}_{y_h, \widehat{A}(y_h)}, \mathcal{I}_{\widehat{A}(y_h)} \right) &= T \left( y_h, \widehat{A}(y_h) \right) \\ &= T(y_h, A(y_h)) > \frac{\delta}{2}, \end{aligned}$$

contradicting our choice of  $\delta$ . □

Observe that for  $\Delta = 0$  and  $t = 1$ , [Theorem 2.1](#) shows that seed protection against permutations is enough, and one does not need to devise an extractor against  $\mathcal{F}_1$ . For a general  $t > 1$  however, we suspect it is not true, and one needs to handle  $\mathcal{F}_\Delta$  for  $\Delta > 0$  to get non malleability against permutations. We note however, that if one is willing to tolerate “smoothness” (in the sense of [Definitions 4.1](#) and [4.3](#) below), or a slight error degradation, we can get non malleability against permutations from seed protecting extractors against permutations, as long as  $t$  is small enough. We omit the details.

### 3.1 Colluding does not harm non malleability

[Theorem 3.2](#) established non malleability against  $(\mathcal{F}_\Delta \cap \mathcal{N})^t \cap \mathcal{X}^t$ . However, in sharp contrast to seed protecting extractors, colluding cannot help adversaries in breaking nonmalleable extractors. Intuitively this should be clear, as redundant information should not help the adversary in distinguishing  $\text{Ext}(X, Y)$  from uniform. Here we make it formal.

**Lemma 3.10.** *Let  $\text{Ext}: \{0, 1\}^n \times \{0, 1\}^d \rightarrow \{0, 1\}^m$  be a  $(k, \varepsilon)$ -nonmalleable extractor against  $\mathcal{N}^t \cap \mathcal{X}^t$  (i.e., non-colluding functions with no fixed points), so that  $d \geq \log(t + 2)$ . Then,  $\text{Ext}$  is  $(k, \varepsilon)$ -nonmalleable against  $\mathcal{N}^t$  (i.e., a  $t$ -nonmalleable extractor).*

*Proof.* Let  $A_1, \dots, A_t \in \mathcal{A}_d \cap \mathcal{N}$  be any adversarial functions with no fixed points. Fix an  $(n, k)$ -source  $X$  and let  $Y \sim \{0, 1\}^d$  be a uniform random variable, independent of  $X$ .

We define the tuple of non-colluding functions  $A'_1, \dots, A'_t$  as follows. Let  $\mathbf{B} \subseteq \{0, 1\}^d$  be the set of  $y$ -s in which a colluding occurs. Namely, for each  $y \in \mathbf{B}$  there exist distinct  $i, j \in [t]$  for which  $A_i(y) = A_j(y)$ . Note that it is possible that different set of functions collude separately, say  $A_i(y) = A_j(y) = z$  and  $A_{i'}(y) = A_{j'}(y) = z'$  for  $z \neq z'$ . Given  $y \in \{0, 1\}^d$ , let  $B(y) \subseteq [t]$  be the set of “redundant” adversaries for  $y$ . Formally,

$$B(y) = \{i \in [t] : \text{there exists } j < i \text{ such that } A_j(y) = A_i(y)\}.$$

Note that if  $y \notin \mathbf{B}$ ,  $B(y)$  is empty. Also, given  $y \in \mathbf{B}$ , we denote by  $I(y) = \{A_1(y), \dots, A_t(y)\}$ , and take  $E_1(y), \dots, E_t(y)$  to be the first  $t$  elements in  $\{0, 1\}^d \setminus (I(y) \cup \{y\})$  in some fixed order. As  $d \geq \log(t + 2)$ , we can indeed do so. For every  $i \in [t]$ , we define

$$A'_i(y) = \begin{cases} A_i(y) & y \notin \mathbf{B}, \\ A_i(y) & y \in \mathbf{B} \wedge i \notin B(y), \\ E_i(y) & \text{otherwise.} \end{cases}$$

It then follows that  $(A'_1, \dots, A'_t) \in \mathcal{X}^t$ .

Denote  $Z(y) = (\text{Ext}(X, A_1(y)), \dots, \text{Ext}(X, A_t(y)))$ , and likewise,

$$Z'(y) = (\text{Ext}(X, A'_1(y)), \dots, \text{Ext}(X, A'_t(y))).$$

We further define  $Z_{\text{reduce}}(y)$  to be joint distribution of the  $\text{Ext}(X, A_i(y))$  for  $i$ -s which are not in  $B(y)$ . Namely,

$$Z_{\text{reduce}}(y) = \bigcirc_{i \in [t] \setminus B(y)} \text{Ext}(X, A_i(y)).$$

We record the following two easy claims.

**Claim 3.11.** *For every  $y \in \{0, 1\}^d$ , it holds that*

$$\begin{aligned} \text{SD}((\text{Ext}(X, y), Z(y)), (U_m, Z(y))) &= \\ \text{SD}((\text{Ext}(X, y), Z_{\text{reduce}}(y)), (U_m, Z_{\text{reduce}}(y))). \end{aligned}$$

*Proof.* The claim follows from the following observation: For every three random variables  $A, B$ , and  $C$ , it holds that  $\text{SD}((A, B, C, C), (U, B, C, C)) = \text{SD}((A, B, C), (U, B, C))$ , where  $U$  is uniform over the support of  $A$  and independent of all other random variables.  $\square$

**Claim 3.12.** *For every  $y \in \{0, 1\}^d$  it holds that*

$$\begin{aligned} \text{SD}((\text{Ext}(X, y), Z_{\text{reduce}}(y)), (U_m, Z_{\text{reduce}}(y))) &\leq \\ \text{SD}((\text{Ext}(X, y), Z'(y)), (U_m, Z'(y))). \end{aligned}$$

*Proof.* The claim readily follows from the data processing inequality, observing that  $Z'(y) = (Z_{\text{reduce}}(y), A)$  for some random variable  $A$ .  $\square$

We can now finish the proof. As  $\text{Ext}$  is non malleable against non-colluding functions, we know that

$$\text{SD}((\text{Ext}(X, Y), Z'(Y), Y), (U_m, Z'(Y), Y)) \leq \varepsilon.$$

But

$$\text{SD}((\text{Ext}(X, Y), Z'(Y), Y), (U_m, Z'(Y), Y)) = \mathbf{E}_{y \sim U_d} [\text{SD}((\text{Ext}(X, y), Z'(y)), (U_m, Z'(y)))],$$

so combining the above with [Claim 3.11](#) and [Claim 3.12](#), it follows that

$$\begin{aligned} \text{SD}((\text{Ext}(X, Y), Z(Y), Y), (U_m, Z(Y), Y)) &= \mathbf{E}_{y \sim U_d} [\text{SD}((\text{Ext}(X, y), Z(y)), (U_m, Z(y)))] \\ &= \mathbf{E}_{y \sim U_d} [\text{SD}((\text{Ext}(X, y), Z_{\text{reduce}}(y)), (U_m, Z_{\text{reduce}}(y)))] \\ &\leq \mathbf{E}_{y \sim U_d} [\text{SD}((\text{Ext}(X, y), Z'(y)), (U_m, Z'(y)))] \\ &\leq \varepsilon, \end{aligned}$$

as desired.  $\square$

The above lemma can be adapted to cases when the non malleability is against more restricted family of functions. In particular, we will need the following lemma.

**Lemma 3.13.** *Let  $\text{Ext}: \{0, 1\}^n \times \{0, 1\}^d \rightarrow \{0, 1\}^m$  be a  $(k, \varepsilon)$ -nonmalleable extractor against  $(\mathcal{F}_\Delta \cap \mathcal{N})^t \cap \mathcal{X}^t$  for  $\Delta \geq 1$ , so that  $d \geq \log t + 3$ . Then,  $\text{Ext}$  is  $(k, \varepsilon)$ -nonmalleable against  $(\mathcal{F}_\Delta \cap \mathcal{N})^t$ .*

*Proof.* Inspecting the proof of Lemma 3.10, we just need to make sure that  $A'_1, \dots, A'_t$  stay inside the family  $\mathcal{F}_\Delta$ . For every  $i \in [t]$ , let  $\mathbf{C}_i \subseteq \{0, 1\}^d$  be the set of seeds we re-wired. Namely,

$$\mathbf{C}_i = \left\{ y \in \{0, 1\}^d : y \in \mathbf{B} \wedge i \in B(y) \right\}.$$

Recall that if  $y \in \mathbf{C}_i$  then  $A'_i(y) = E_i(y)$ . We will modify the definition of  $E_i$  to guarantee that  $A'_i \in \mathcal{F}_\Delta$ , while still satisfying  $(A'_1, \dots, A'_t) \in \mathcal{X}^t \cap \mathcal{N}^t$ .

Let  $\mathbf{G}_1(y) = \{0, 1\}^d \setminus (I(y) \cup \{y\})$  be the set of “safe” seeds. In Lemma 3.10 we simply set  $E_i(y)$  to be the  $i$ -th element of  $\mathbf{G}_1(y)$ . Now, we need to be just a bit more careful. Let

$$\mathbf{G}_2 = \left\{ z \in \{0, 1\}^d : |A_i^{-1}(z)| < 2^\Delta \right\}.$$

By an averaging argument,  $|\mathbf{G}_2| \geq 2^{d-\Delta}$ . Thus,

$$|\mathbf{G}_1(y) \cap \mathbf{G}_2| \geq 2^d - t - 1 - 2^{d-\Delta} \geq t,$$

and we can set  $E_i(y)$  to be the  $i$ -th element of  $\mathbf{G}_1(y) \cap \mathbf{G}_2$ . Both properties now hold.  $\square$

Combining Theorem 3.2 and Lemma 3.13, we get our main result.

**Corollary 3.14.** *Let  $t \geq 1$  be an integer, and  $\Delta \geq 1$ . Let  $\text{Ext}: \{0, 1\}^n \times \{0, 1\}^d \rightarrow \{0, 1\}^m$  be a  $(k, \varepsilon)$ -seeded extractor with  $d \geq 2 \log t + \log \frac{1}{\varepsilon} + 2$  and  $\varepsilon \leq 10^{-4}$ . Assume that  $\text{Ext}$  is seed protecting against  $\mathcal{F}_{\max(\Delta, \log t)}^{t+1} \cap \mathcal{X}^{t+1}$ . Then,  $\text{Ext}$  is nonmalleable against  $(\mathcal{F}_\Delta \cap \mathcal{N})^t$  for min-entropy  $k + mt + \log \frac{1}{\varepsilon}$  and error guarantee  $14\varepsilon^{1/3}$ .*

## 4 Seed protecting extractors from nonmalleable extractors

In this section, we show that non malleability against permutations implies seed protection for the class of permutations. We also prove a similar claim for a more restricted kind of permutations –  $t$ -cliques, which we define below. For the sake of generality, we consider the “smooth” variants of these classes.

**Definition 4.1** (smooth permutations). *Given  $A \in \mathcal{A}_d$  and  $\tau \in [0, 1]$ , we say that  $A \in \Pi_\tau$  if there exists a set  $G \subseteq \{0, 1\}^d$  with  $|G| \geq (1 - \tau) \cdot 2^d$  such that  $A|_G$  is injective.*

To describe our next family of structured adversaries, we introduce the following notation. We say that a function  $A \in \mathcal{A}$  is  $\tau$ -close to an involution if for all but  $\tau$ -fraction of  $y \in \{0, 1\}^d$  it holds that  $A(A(y)) = y$  and  $A(y) \neq y$ . That is, the directed graph induced by the function  $A$  has, but for one component of density  $\tau$ , an involution structure (i.e., a perfect matching). More generally, for  $t \geq 1$ , we formalize what it means for an adversarial function to be  $\tau$ -close to  $(t + 1)$ -cliques, or clusters. Fix functions  $A_1, \dots, A_t \in \mathcal{A}$ . For  $y \in \{0, 1\}^d$ , we define the neighborhood of  $y$  by  $\Gamma(y) = \{y, A_1(y), \dots, A_t(y)\}$ . We say that  $(A_1, \dots, A_t) \in \mathcal{M}_\tau^t$  if there exists  $G \subseteq \{0, 1\}^d$  with  $|G| \geq (1 - \tau) \cdot 2^d$  such that for every  $y \in G$  it holds that  $\Gamma(\Gamma(y)) = \Gamma(y)$ , and  $|\Gamma(y)| = t + 1$ . So, intuitively, but for a density- $\tau$  component, the vertices are partitioned to cliques, or clusters, of size  $t + 1$ . In fact, we consider a more structured variant, which we now formally define.

**Definition 4.2** (*t-cliques*). *Given  $A_1, \dots, A_t \in \mathcal{A}_d$  and  $p \geq t$ , we say  $(A_1, \dots, A_t) \in \mathcal{M}^t[p]$  if there exists a partition  $\{0, 1\}^d = C_1 \uplus \dots \uplus C_\ell$ , each  $t \leq |C_i| \leq p$ , such that the following holds. For every  $i \in [\ell]$  let  $c_i = |C_i|$  and denote  $C_i = \{y^0, \dots, y^{c_i-1}\}$ , and  $A_1(y^j) = z^j$ . Then,*

1.  $A_1$  restricted to  $C_i$  is a permutation. That is,  $\{y^0, \dots, y^{c_i-1}\} = \{z^0, \dots, z^{c_i-1}\}$ .
2. For any integers  $j \in [c_i]$  and  $2 \leq r \leq t$ ,  $A_r(y^j) = z^{j+r-1 \bmod c_i}$ .

Note, in particular, that  $\mathcal{M}^t[p] \subset \Pi^t$ . For brevity, we denote  $\mathcal{M}^t[t] = \mathcal{M}^t$ .

**Definition 4.3** (*smooth t-cliques*). *For positive integers  $p \geq t$ , and  $\tau \in [0, 1]$ , we define the set  $\mathcal{M}_\tau^t[p] \subseteq \mathcal{A}_d^t$  as follows. A tuple  $\mathbf{A} = (A_1, \dots, A_t) \in \mathcal{M}_\tau^t[p]$  if there exists  $G \subseteq \{0, 1\}^d$  with  $|G| \geq (1 - \tau) \cdot 2^d$  such that*

$$(A_1|_G, \dots, A_t|_G) \in \mathcal{M}^t[p]$$

where by the latter we mean formally that there exists a partition  $G = C_1 \uplus \dots \uplus C_\ell$ , each  $t \leq |C_i| \leq p$ , such that the conditions of [Definition 4.2](#) are met. For brevity, we denote  $\mathcal{M}_\tau^t[t] = \mathcal{M}_\tau^t$ .

We begin with permutations.

**Lemma 4.4.** *Let  $\text{Ext}: \{0, 1\}^n \times \{0, 1\}^d \rightarrow \{0, 1\}^m$  be a  $(k, \varepsilon)$ -nonmalleable extractor against  $(\Pi \cap \mathcal{N})^t$  (i.e., permutations with no fixed points), and fix any  $\tau \geq 0$ . Then,  $\text{Ext}$  is  $(k, \varepsilon')$ -seed protecting against  $\Pi_\tau^{t+1} \cap \mathcal{X}^{t+1}$  for  $\varepsilon' = 2(t + 1)(\tau + \varepsilon)$ .*

*Proof.* Let  $A_1, \dots, A_{t+1} \in \Pi_\tau$  be non-colluding. Let  $X$  be an  $(n, k)$ -source, and let  $Y \sim \{0, 1\}^d$  be a uniform random variable, independent of  $X$ . For each  $i \in [t + 1]$ , let  $G_i \subseteq \{0, 1\}^d$  be such that  $A_i|_{G_i}$  is injective. Writing  $G = G_1 \cap \dots \cap G_{t+1}$ , we have that  $|G| \geq (1 - (t + 1)\tau) \cdot 2^d$ . For each  $i \in [t + 1]$ , denote by  $\tilde{A}_i \in \Pi$  the permutation that is obtained by keeping the

function's value on  $G$  and completing it to a permutation on  $\{0, 1\}^d$  in such a way that  $\tilde{A}_1, \dots, \tilde{A}_{t+1}$  do not collide. Observe that it is possible to do so as long as  $|\{0, 1\}^d \setminus G| \geq t+1$ , which certainly holds.<sup>3</sup> In what follows, we denote

$$\begin{aligned} Z_1(Y) &= (\text{Ext}(X, A_1(Y)), \dots, \text{Ext}(X, A_{t+1}(Y))), \\ \tilde{Z}_1(Y) &= (\text{Ext}(X, \tilde{A}_1(Y)), \dots, \text{Ext}(X, \tilde{A}_{t+1}(Y))). \end{aligned}$$

First, note that

$$\text{SD}((Y, Z_1(Y)), (Y, \tilde{Z}_1(Y))) \leq \Pr[Y \notin G] \leq (t+1)\tau. \quad (4.1)$$

Next, as  $\tilde{A}_1^{-1}$  is a permutation,  $\tilde{A}_1^{-1}(Y)$  distributes the same as  $Y$  does. Thus,

$$\text{SD}((U_d, \tilde{Z}_1(Y)), (Y, \tilde{Z}_1(Y))) = \text{SD}((U_d, \tilde{Z}_1(\tilde{A}_1^{-1}(Y))), (\tilde{A}_1^{-1}(Y), \tilde{Z}_1(\tilde{A}_1^{-1}(Y)))). \quad (4.2)$$

By the data-processing inequality, we can apply  $\tilde{A}_1$  on the prefix of both random variables without increasing the statistical distance; Equation (4.2) becomes

$$\text{SD}((U_d, \tilde{Z}_1(Y)), (Y, \tilde{Z}_1(Y))) = \text{SD}((U_d, \tilde{Z}_1(\tilde{A}_1^{-1}(Y))), (Y, \tilde{Z}_1(\tilde{A}_1^{-1}(Y)))). \quad (4.3)$$

For  $i \in [t]$ , define  $P_i = \tilde{A}_{i+1} \circ \tilde{A}_1^{-1}$ . Then,

$$\begin{aligned} \tilde{Z}_1(\tilde{A}_1^{-1}(Y)) &= \left( \text{Ext}(X, Y), \text{Ext}\left(X, \tilde{A}_2(\tilde{A}_1^{-1}(Y))\right), \dots, \text{Ext}\left(X, \tilde{A}_{t+1}(\tilde{A}_1^{-1}(Y))\right) \right) \\ &= (\text{Ext}(X, Y), \text{Ext}(X, P_1(Y)), \dots, \text{Ext}(X, P_t(Y))). \end{aligned}$$

Note that for every  $i \in [t]$ ,  $P_i$  is a permutation. Furthermore, observe that as  $(\tilde{A}_1, \dots, \tilde{A}_{t+1}) \in \mathcal{X}^{t+1}$ ,  $P_i$  has no fixed points. Indeed, assuming towards a contradiction that  $P_i$  satisfies  $P_i(y) = y$  for some  $y \in \{0, 1\}^d$ , we get that  $\tilde{A}_1^{-1}(y) = \tilde{A}_{i+1}^{-1}(y)$ , which is impossible since  $\tilde{A}_1(z) \neq \tilde{A}_{i+1}(z)$  for any  $z \in \{0, 1\}^d$ . By the non malleability of  $\text{Ext}$ , we know that

$$\text{SD}((Y, \tilde{Z}_1(\tilde{A}_1^{-1}(Y))), (Y, U_m, Z_2(Y))) \leq \varepsilon,$$

for  $Z_2(Y) = (\text{Ext}(X, P_1(Y)), \dots, \text{Ext}(X, P_t(Y)))$ , and the same is true without conditioning on  $Y$ . Thus, by the triangle inequality, we get

$$\begin{aligned} \text{SD}((U_d, \tilde{Z}_1(\tilde{A}_1^{-1}(Y))), (Y, \tilde{Z}_1(\tilde{A}_1^{-1}(Y)))) &\leq \text{SD}((U_d, \tilde{Z}_1(\tilde{A}_1^{-1}(Y))), (U_d, U_m, Z_2(Y))) + \\ &\quad \text{SD}((U_d, U_m, Z_2(Y)), (Y, U_m, Z_2(Y))) + \\ &\quad \text{SD}((Y, U_m, Z_2(Y)), (Y, \tilde{Z}_1(\tilde{A}_1^{-1}(Y)))) \\ &\leq 2\varepsilon + \text{SD}((U_d, U_m, Z_2(Y)), (Y, U_m, Z_2(Y))). \end{aligned} \quad (4.4)$$

---

<sup>3</sup>Otherwise,  $\tau < 2^{-d}$  which implies  $\tau = 0$  and we can simply take  $\tilde{A}_i = A_i$  for each  $i \in [t+1]$ .



We continue in the same manner. Observing that  $P_1^{-1}(Y)$  distributes the same as  $Y$  does, and using the data-processing inequality, we have

$$\text{SD}((U_{d+m}, Z_2(Y)), (Y, U_m, Z_2(Y))) = \text{SD}((U_{d+m}, Z_2(P_1^{-1}(Y))), (Y, U_m, Z_2(P_1^{-1}(Y)))). \quad (4.5)$$

For  $i \in [t-1]$  define the permutation  $Q_i = P_{i+1} \circ P_1^{-1}$ . Similarly to the above argument,

$$\begin{aligned} Z_2(P_1^{-1}(Y)) &= (\text{Ext}(X, Y), \text{Ext}(X, P_2(P_1^{-1}(Y))), \dots, \text{Ext}(X, P_t(P_1^{-1}(Y)))) \\ &= (\text{Ext}(X, Y), \text{Ext}(X, Q_1(Y)), \dots, \text{Ext}(X, Q_{t-1}(Y))). \end{aligned}$$

This time, the fact that every  $Q_i$  has no fixed points follows from the fact that  $\tilde{A}_2(z) \neq \tilde{A}_{i+2}(z)$  for any  $z \in \{0, 1\}^d$ . Using the non malleability, together with Equations (4.3) to (4.5), we get

$$\begin{aligned} \text{SD}((U_d, \tilde{Z}_1(Y)), (Y, \tilde{Z}_1(Y))) &\leq 2\varepsilon + \text{SD}((U_d, U_m, Z_2(Y)), (U_d, U_{2m}, Z_3(Y))) + \\ &\quad \text{SD}((U_d, U_{2m}, Z_3(Y)), (Y, U_{2m}, Z_3(Y))) + \\ &\quad \text{SD}((Y, U_{2m}, Z_3(Y)), (Y, U_m, Z_2(Y))) \\ &\leq 4\varepsilon + \text{SD}((U_d, U_{2m}, Z_3(Y)), (Y, U_{2m}, Z_3(Y))), \end{aligned}$$

for  $Z_3(Y) = (\text{Ext}(X, Q_1(Y)), \dots, \text{Ext}(X, Q_{t-1}(Y)))$ . We continue this process inductively, and eventually obtain

$$\text{SD}((U_d, \tilde{Z}_1(Y)), (Y, \tilde{Z}_1(Y))) \leq 2(t+1)\varepsilon + \text{SD}((U_d, U_{(t+1)m}), (Y, U_{(t+1)m})) = 2(t+1)\varepsilon. \quad (4.6)$$

Combining Equations (4.1) and (4.6), we get

$$\begin{aligned} \text{SD}((U_d, Z_1(Y)), (Y, Z_1(Y))) &\leq \text{SD}((Y, Z_1(Y)), (Y, \tilde{Z}_1(Y))) + \\ &\quad \text{SD}((Y, \tilde{Z}_1(Y)), (U_d, \tilde{Z}_1(Y))) + \\ &\quad \text{SD}((U_d, \tilde{Z}_1(Y)), (U_d, Z_1(Y))) \\ &\leq (t+1)(2\varepsilon + \tau) + \text{SD}(\tilde{Z}_1(Y), Z_1(Y)). \end{aligned}$$

To bound the last term of the above inequality, note that

$$\text{SD}(\tilde{Z}_1(Y), Z_1(Y)) \leq \text{SD}((Y, \tilde{Z}_1(Y)), (Y, Z_1(Y))) \leq (t+1)\tau,$$

where the last inequality follows by Equation (4.1). This concludes the proof.  $\square$

Next, we prove a similar lemma for  $t$ -cliques.

**Lemma 4.5.** *Let  $\text{Ext}: \{0, 1\}^n \times \{0, 1\}^d \rightarrow \{0, 1\}^m$  be a  $(k, \varepsilon)$ -nonmalleable extractor against  $\mathcal{M}^t \cap \mathcal{N}^t$ , and fix any  $\tau \geq 0$ . Then,  $\text{Ext}$  is a  $(k, \varepsilon')$ -seed protecting extractor against  $\mathcal{M}_\tau^{t+1} \cap \mathcal{X}^{t+1}$  for  $\varepsilon' = 2(t+1)\varepsilon + 2\tau$ .*

*Proof.* Given non colluding  $\mathbf{A} = (A_1, \dots, A_{t+1}) \in \mathcal{M}_\tau^{t+1}$ , an  $(n, k)$ -source  $X$  and a uniform  $Y \sim \{0, 1\}^d$  independent of  $X$ , the proof proceeds similarly to [Lemma 4.4](#). Let  $G \subseteq \{0, 1\}^d$  be the set defined in [Definition 4.3](#) with respect to  $(A_1, \dots, A_{t+1}) \in \mathcal{M}_\tau^{t+1}$ , and recall that  $|G| \leq \tau \cdot 2^d$ . We define

$$\tilde{\mathbf{A}} = (\tilde{A}_1, \dots, \tilde{A}_{t+1}) \in \mathcal{M}^{t+1}$$

by setting  $\tilde{A}_i$  to agree with  $A_i$  on  $G$  for every  $i$ . Completing  $\tilde{A}_i|_G$  to functions on  $\{0, 1\}^d$  while maintaining the  $\mathcal{M}^{t+1}$  property can be done by arbitrarily selecting  $t + 1$  inputs that were not assigned yet, iteratively, and assigning them to form a clique.<sup>4</sup> Note that by the definition of  $\mathcal{M}^{t+1}$ , the functions in  $\tilde{\mathbf{A}}$  do not collude.

Define, inductively, the following set of functions. For  $i \in [t + 1]$ ,  $P_i^{(0)} = \tilde{A}_i$ . For every  $j \in [t]$  and  $i \in [t + 1 - j]$ , we define

$$P_i^{(j)} = P_{i+1}^{(j-1)} \circ (P_1^{(j-1)})^{-1}. \quad (4.7)$$

Next, define, exactly as in [Lemma 4.4](#),

$$\tilde{Z}_1(Y) = \left( \text{Ext} \left( X, P_1^{(0)}(Y) \right), \dots, \text{Ext} \left( X, P_{t+1}^{(0)}(Y) \right) \right).$$

Moreover, for every  $j \in [t + 1]$ , we define

$$Z_{j+1}(Y) = \left( \text{Ext} \left( X, P_1^{(j)}(Y) \right), \dots, \text{Ext} \left( X, P_{t-j+1}^{(j)}(Y) \right) \right).$$

The crux of the proof is establishing the following inequality for every  $j \geq 2$ .

$$\text{SD}((U_d, \tilde{Z}_1(Y)), (Y, \tilde{Z}_1(Y))) \leq 2(j - 1)\varepsilon + \text{SD}((U_d, U_{(j-1)m}, Z_j(Y)), (Y, U_{(j-1)m}, Z_j(Y))). \quad (4.8)$$

Following the same reasoning as in [Lemma 4.4](#), [Equation \(4.8\)](#) holds if the following conditions are met:

1. For every  $j \geq 0$ ,  $(P_1^{(j)})^{-1}(Y)$  distributes the same as  $Y$  does.
2. For every  $j \geq 1$  and  $i \leq t + 1 - j$ ,  $P_i^{(j)}$  has no fixed points.
3. For every  $j \geq 0$  it holds that  $(P_1^{(j)}, \dots, P_{t-j+1}^{(j)}) \in \mathcal{M}^{t-j+1}[t + 1]$ . Note that a nonmalleable extractor against  $\mathcal{M}^{t+1}$  is also nonmalleable against  $\mathcal{M}^{t'}[t + 1]$  for any  $t' \leq t + 1$ .

---

<sup>4</sup>Formally, choose  $y_1, \dots, y_{t+1}$  that were not assigned by  $\tilde{A}_1$  yet, namely, with no preimage in  $\tilde{A}_1|_G$ . Assign  $y_1 \rightarrow y_1, \dots, y_{t+1} \rightarrow y_{t+1}$  in  $\tilde{A}_1$ ,  $y_1 \rightarrow y_2, y_2 \rightarrow y_3, \dots, y_{t+1} \rightarrow y_1$  in  $\tilde{A}_2$ , and so on. Note that when  $t + 1$  does not divide  $2^d$ , we can make some cliques larger. We do not address this issue formally and it does not affect the statement.

Item 1 readily holds, since each  $\tilde{A}_i$  is a permutation, and permutations are closed under inversion and composition. To see that Item 2 holds, fix some  $j \in [t]$  and  $i \in [t+1-j]$  and consider  $P_i^{(j)}$ . Assume towards a contradiction that  $P_i^{(j)}(y) = y$  for some  $y \in \{0,1\}^d$ . Thus,

$$P_{i+1}^{(j-1)} \left( \left( P_1^{(j-1)} \right)^{-1} (y) \right) = y,$$

so

$$\left( P_1^{(j-1)} \right)^{-1} (y) = \left( P_{i+1}^{(j-1)} \right)^{-1} (y),$$

which means there exists  $z \in \{0,1\}^d$  such that  $P_{i+1}^{(j-1)}(z) = P_1^{(j-1)}(z)$ . But due to Item 3 which we now prove,  $(P_1^{(j-1)}, \dots, P_{t-j+2}^{(j-1)}) \in \mathcal{M}^{t-j+2}$ , so in particular they do not collude, so we have a contradiction. Indeed, what is left is to prove Item 3.

**Claim 4.6.** *For every  $j \geq 0$  it holds that  $(P_1^{(j)}, \dots, P_{t-j+1}^{(j)}) \in \mathcal{M}^{t-j+1}[t+1]$ .*

*Proof.* Starting from  $(t+1)$ -cliques in the 0-th level, in general, the  $j$ -th level will also form  $(t+1)$ -cliques. We will prove this by induction on  $j$ . For  $j = 0$ , it follows by our construction. Assuming that it holds for some  $j \geq 0$ , we inspect the  $(j+1)$ -th level.

We characterize the cliques in the  $j$ -th level as follows. We can partition the domain (and codomain) to  $\{0,1\}^d = C_1 \uplus \dots \uplus C_\ell$ . By definition, a full characterization of  $P_1^{(j)}, \dots, P_{t-j+1}^{(j)}$  can be given by a permutation  $\phi_i: C_i \rightarrow C_i$ , for each  $i \in [\ell]$ . Indeed, for any  $y \in C_i$  for some  $i \in [\ell]$ ,  $P_1^{(j)}(y) = \phi_i(y)$ , and for  $r \geq 2$ ,  $P_r^{(j)} = \phi_i^r$ . Namely,  $\phi_i$  generates the permutations  $P_1^{(j)}, \dots, P_{t-j+1}^{(j)}$  restricted to  $C_i$ . We claim that this structure is preserved for the next level, with the same clique structure. Indeed, for each  $i \in [\ell]$  observe that the permutation  $\phi_i$  is also a generator for  $P_1^{(j+1)}, \dots, P_{t-j}^{(j+1)}$  restricted to  $C_i$  as, by Equation (4.7) applied with  $i = 1$ ,

$$P_1^{(j+1)} = P_2^{(j)} \circ \left( P_1^{(j)} \right)^{-1} = \phi_i^2 \circ \phi_i^{-1} = \phi_i.$$

Recalling that  $P_r^{(j+1)} = P_{r+1}^{(j)} \circ \left( P_1^{(j)} \right)^{-1}$ , we see that indeed computing  $P_r^{(j+1)}(y)$  amounts to finding the  $i$  for which  $y \in C_i$  and computing  $\phi_i^r(y)$ . Thus, the  $(j+1)$ -th level belong to  $\mathcal{M}^{t-j}[t+1]$ . □

□

## 5 1-seed protecting and two-source extractors

In this section we prove Theorem 1.6. We prove each direction separately in Lemma 5.1 and Lemma 5.3 below.

**Lemma 5.1.** *Let  $\text{Ext}: \{0,1\}^n \times \{0,1\}^d \rightarrow \{0,1\}^m$  be a  $(k_1, \varepsilon)$  1-seed protecting extractor against  $\mathcal{F}_{d-k_2}$  for  $k_2 \leq d-1$ . Then,  $\text{Ext}$  is a  $(k_1, k_2, 3\varepsilon)$  two-source extractor.*

*Proof.* Assume towards a contradiction that  $\text{Ext}$  is not such a two-source extractor, and let  $X_1, X_2$  with  $H_\infty(X_1) \geq k_1$  and  $H_\infty(X_2) \geq k_2$  be such that

$$\text{SD}(\text{Ext}(X_1, X_2), U_m) > 3\varepsilon,$$

and we can assume without loss of generality that both  $X_1$  and  $X_2$  are flat sources. Let  $Y$  be the uniform distribution over  $\{0, 1\}^d$ , independent of  $(X_1, X_2)$ . Recall that  $\text{Ext}$  is a  $(k_1, \varepsilon)$  extractor, so

$$\text{SD}(\text{Ext}(X_1, Y), U_m) \leq \varepsilon.$$

Order the  $y$ -s according to  $\text{SD}(\text{Ext}(X_1, y), U_m)$ , and let  $G_1 \subseteq \{0, 1\}^d$  be the  $2^{d-1}$  bottom ones (i.e., for which  $\text{SD}(\text{Ext}(X_1, y), U_m)$  is smaller). As  $G_1$  can be indexed using  $d-1$  bits, there exists an injection  $A_0: \{0, 1\}^{d-1} \rightarrow \{0, 1\}^d$  that maps to  $G_1$  uniformly, and satisfies

$$\text{SD}(\text{Ext}(X_1, A_0(Y')), U_m) \leq \varepsilon, \tag{5.1}$$

where  $Y'$  is the uniform distribution over  $\{0, 1\}^{d-1}$ , independent of all other variables.

Denote  $G_2 = \text{Supp}(X_2)$  and recall that  $|G_2| = 2^{k_2}$ . Again, since  $k_2 \leq d-1$ , we can define an injection  $A_1: \{0, 1\}^{d-1} \rightarrow \{0, 1\}^d$  so that  $A_1(U_{d-1}) = U_{G_2}$ , and then

$$\text{SD}(\text{Ext}(X_1, A_1(Y')), U_m) > 3\varepsilon. \tag{5.2}$$

Next, define  $A \in \mathcal{A}_d$  such that

$$A(y) = A_{y_1}(y_{[2:n]}).$$

**Claim 5.2.** *It holds that  $A \in \mathcal{F}_{d-k_2}$ .*

*Proof.* Let  $Z = A(U_d)$ . Clearly,  $\text{Supp}(Z) \subseteq G_1 \cup G_2$ . If  $z \in G_1$ ,

$$\begin{aligned} \Pr_{y \sim U_d} [A(y) = z] &= \frac{1}{2} \cdot \Pr_{y \sim U_d} [A_0(y_{[2:n]}) = z] + \frac{1}{2} \cdot \Pr_{y \sim U_d} [A_1(y_{[2:n]}) = z] \\ &= \frac{1}{2} \cdot \frac{1}{|G_1|} + \frac{1}{2} \cdot \frac{\mathbf{1}_{z \in G_2}}{|G_2|} \leq 2^{-k_2}. \end{aligned}$$

The same bound applies for  $z \in G_2$  in a similar manner. □

We will now show that using  $A$ , an adversary can learn the first bit of the seed, in contradiction to the fact that  $\text{Ext}$  is seed protecting. Define

$$R_{Y_1} \triangleq \text{Ext}(X_1, A_{Y_1}(Y_{[2:d]})),$$

and note that by Equation (5.1), Equation (5.2) and the triangle inequality, it holds that  $\text{SD}(R_0, R_1) > 2\varepsilon$ . Then,

$$\begin{aligned} \text{SD}((Y, \text{Ext}(X_1, A(Y))), (U_d, \text{Ext}(X_1, A(Y)))) &\geq \text{SD}((Y_1, \text{Ext}(X_1, A(Y))), (U_1, \text{Ext}(X_1, A(Y)))) \\ &= \text{SD}((Y_1, R_{Y_1}), (U_1, R_{Y_1})). \end{aligned}$$

Finally, observe that

$$\begin{aligned}
\text{SD}((Y_1, R_{Y_1}), (U_1, R_{Y_1})) &= \frac{1}{2} \sum_r \left| \Pr[Y_1 = 1 \wedge R_1 = r] - \frac{1}{2} \Pr[R_{Y_1} = r] \right| \\
&\quad + \frac{1}{2} \sum_r \left| \Pr[Y_1 = 0 \wedge R_0 = r] - \frac{1}{2} \Pr[R_{Y_1} = r] \right| \\
&= \frac{1}{4} \sum_r |\Pr[R_0 = r] - \Pr[R_1 = r]| \\
&= \frac{1}{2} \cdot \text{SD}(R_0, R_1) \\
&> \varepsilon,
\end{aligned}$$

which is a contradiction to that  $\text{Ext}$  is 1-seed protecting per our hypothesis. □

The other direction also holds.

**Lemma 5.3.** *Let  $\text{Ext}: \{0, 1\}^n \times \{0, 1\}^d \rightarrow \{0, 1\}^m$  be a  $(k_1, k_2, \varepsilon)$  two-source extractor which is strong in the second source. Then,  $\text{Ext}$  is a  $(k_1, 2\varepsilon)$  1-seed protecting against  $\mathcal{F}_{d-k_2}$ .*

*Proof.* Assume towards a contradiction that  $\text{Ext}$  is not 1-seed protecting, so there exists an  $(n, k_1)$ -source  $X_1$  and  $A \in \mathcal{F}_{d-k_2}$  such that

$$\text{SD}((\text{Ext}(X_1, A(Y)), Y), \text{Ext}(X_1, A(Y), Y')) > 2\varepsilon,$$

where  $Y, Y' \sim \{0, 1\}^d$  are uniform and independent random variables, also independent of  $X_1$ . By the triangle inequality, it follows that at least one of the following holds:

1.  $\text{SD}((\text{Ext}(X_1, A(Y)), Y'), (U_m, Y)) > \varepsilon,$
2.  $\text{SD}((\text{Ext}(X_1, A(Y)), Y), (U_m, Y)) > \varepsilon.$

First assume the first inequality holds. As  $Y'$  is independent of  $X_1$  and  $Y$ ,

$$\begin{aligned}
\text{SD}((\text{Ext}(X_1, A(Y)), Y'), (U_m, Y)) &= \text{SD}(\text{Ext}(X_1, A(Y)) \times Y', U_m \times Y) \\
&= \text{SD}(\text{Ext}(X_1, A(Y)) \times Y', U_m \times Y') \\
&= \text{SD}(\text{Ext}(X_1, A(Y)), U_m).
\end{aligned}$$

As  $A \in \mathcal{F}_{d-k_2}$ ,  $H_\infty(A(Y)) \geq k_2$  and by the fact that  $\text{Ext}$  is a two-source extractor, it follows that  $\text{SD}(\text{Ext}(X_1, A(Y)), U_m) \leq \varepsilon$ , contradicting [Item 1](#).

Next, assume that the second inequality holds. We have that

$$\begin{aligned} \text{SD}((\text{Ext}(X_1, A(Y)), A(Y)), (U_m, A(Y))) &= \mathbf{E}_{z \sim A(Y)} [\text{SD}(\text{Ext}(X_1, z), U_m)] \\ &= \mathbf{E}_{y \sim Y} [\text{SD}(\text{Ext}(X_1, A(y)), U_m)] \\ &= \text{SD}((\text{Ext}(X_1, A(Y)), Y), (U_m, Y)) > \varepsilon. \end{aligned}$$

But since  $\text{Ext}$  is a strong  $(k_1, k_2, \varepsilon)$  two-source extractor,

$$\text{SD}((\text{Ext}(X_1, A(Y)), A(Y)), (U_m, A(Y))) \leq \varepsilon,$$

in contradiction. □

## 5.1 Lower bounds for 1-seed protecting extractors

In light of the above result, lower bounds for (unbalanced) two-source extractors imply lower bounds for 1-seed protecting extractors. We use the following standard lower bound.<sup>5</sup>

**Theorem 5.4.** *Let  $\text{Ext}: \{0, 1\}^n \times \{0, 1\}^d \rightarrow \{0, 1\}^m$  be a  $(k_1, k_2, \varepsilon)$  two-source extractor which is strong in the second source. Then,  $m \leq k_1 - 2 \log \frac{1}{\varepsilon} - O(1)$ ,  $k_2 \geq \log(n - k_1) + 2 \log \frac{1}{\varepsilon} - O(1)$  and  $k_1 \geq \log(d - k_2) + 2 \log \frac{1}{\varepsilon} - O(1)$ .*

We can thus conclude:

**Corollary 5.5.** *Let  $\text{Ext}: \{0, 1\}^n \times \{0, 1\}^d \rightarrow \{0, 1\}^m$  be a  $(k, \varepsilon)$  1-seed protecting against  $\mathcal{F}_\Delta$  for some  $\Delta > 0$ . Then,  $m \leq k - 2 \log \frac{1}{\varepsilon} - O(1)$ ,  $d \geq \log(n - k) + \Delta + 2 \log \frac{1}{\varepsilon} - O(1)$  and  $k \geq \log \Delta + 2 \log \frac{1}{\varepsilon} - O(1)$ .*

The fact that no 1-seed protecting extractors against  $\mathcal{F}_\Delta$  exist for  $\Delta$  approaching  $d$  can be established in a more straightforward way. Indeed, in [Claim 1.5](#) we showed why  $\Delta = d - 1$  is unattainable.

## 6 Non-explicit $t$ -seed protecting extractors

In this section we prove the existence of a seed protecting extractor via a probabilistic argument.

---

<sup>5</sup>The lower bound for  $m = 1$  and any nontrivial  $\varepsilon$  follows from bounds on strong dispersers and their connection to Ramsey graphs [[RTS00](#), [BADTS20](#)]. The entropy loss and the  $2 \log \frac{1}{\varepsilon}$  factor in  $d$  and  $k$  follows from lower bounds on strong seeded extractors [[RTS00](#)].

**Theorem 6.1.** Let  $n, k, m, d, t \in \mathbb{N}$ ,  $\Delta \geq 0$  and  $\varepsilon > 0$  be such that

$$k \geq tm + 2\Delta + 2 \log \frac{1}{\varepsilon} + O(\log d + \log t).$$

Then, there exists a  $(k, \varepsilon)$ -seed protecting extractor  $\text{Ext}: \{0, 1\}^n \times \{0, 1\}^d \rightarrow \{0, 1\}^m$  against  $\mathcal{F}_\Delta^t \cap \mathcal{X}^t$  with

$$d = \log(n - k) + 2\Delta + 2 \log \frac{1}{\varepsilon} + O(\log d + \log t).$$

**Remark.** Theorem 6.1 tells us we cannot take  $\Delta$  to be smaller than  $\frac{d}{2}$ , meaning we are at the *weak seeds* regime. In contrast, for  $t = 1$ , we know from the equivalence to two-source extractors (see Lemma 5.3) that we can take  $\Delta$  to be much larger, roughly  $d - \log n$ . An interesting open problem is whether there is a real barrier going from  $t = 1$  to larger  $t$ -s or whether it is a mere artifact of our proof.

*Proof.* Choose  $\text{Ext}: \{0, 1\}^n \times \{0, 1\}^d \rightarrow \{0, 1\}^m$  uniformly at random. Fix an  $(n, k)$  source  $X$ . It is well-known [CG88] that one can assume  $X$  is flat, that is, it is uniformly distributed over a set of size  $2^k$ . Also, fix non-colluding functions  $A_1, \dots, A_t \in \mathcal{F}_\Delta$ . Let  $Y \sim \{0, 1\}^d$  be uniform and independent of  $X$ . Write  $N = 2^n$ ,  $K = 2^k$ ,  $D = 2^d$ , and

$$Z(x, y) = (\text{Ext}(x, A_1(y)), \dots, \text{Ext}(x, A_t(y))),$$

observing that for every fixed  $x$  and  $y$ ,  $Z$  is a random variable whose randomness comes from  $\text{Ext}$ . We want to bound the probability that

$$\text{SD}((Y, Z(X, Y)), (U_d, Z(X, Y))) > \varepsilon.$$

Fix  $T: \{0, 1\}^{d+mt} \rightarrow \{0, 1\}$  and for each  $y \in [D]$ , denote by  $T_y: \{0, 1\}^{mt} \rightarrow \{0, 1\}$  the corresponding restriction of  $T$ . Then, we want to bound the probability over  $\text{Ext}$  that

$$\mathbf{E}_{w \sim [D]} \left[ \mathbf{E}_X [T_w(Z(X, w))] \right] - \mathbf{E}_{w \sim [D]} \left[ \mathbf{E}_{X, Y} [T_w(Z(X, Y))] \right] > \varepsilon.$$

Write the expression on the left hand side as

$$\mathbf{E}_{x \sim X, w \sim [D]} \left[ T_w(Z(x, w)) - \mathbf{E}_Y [T_w(Z(x, Y))] \right],$$

and define

$$Q(x, w) = T_w(Z(x, w)) - \mathbf{E}_Y [T_w(Z(x, Y))].$$

First, we argue,

**Claim 6.2.** For any  $x \in \{0, 1\}^n$  and  $w \in [D]$  it holds that  $\mathbf{E}[Q(x, w)] = 0$ .

*Proof.* By our assumption on  $A_1, \dots, A_t$ , the values  $A_1(w), \dots, A_t(w)$  are distinct, so  $Z(x, w)$  is uniform over  $\{0, 1\}^{mt}$ , and thus  $\mathbf{E}[T_w(Z(x, w))] = \mu(T_w)$ . The claim now follows from the linearity of expectation.  $\square$

Write

$$Q(x, w) = (T_w(Z(x, w)) - \mu(T_w)) - \left( \mathbf{E}_Y [T_w(Z(x, Y))] - \mu(T_w) \right) \triangleq Q_1(x, w) - Q_2(x, w),$$

each  $Q_i(x, w)$  being a random variable with expectation zero. We handle each term separately.

**Handling  $Q_1$ .** Define the random variable

$$\mathbf{Q}_1 = \mathbf{E}_{x \sim X, w \sim [D]} [Q_1(x, w)].$$

Unfortunately, the random variables  $Q_1(x, w)$ , for  $x \in X$  and  $w \in [D]$ , are not independent. In particular, it may be the case that  $Q_1(x, w_1)$  and  $Q_1(x, w_2)$  query the same input to  $\text{Ext}$ . The next observation will help us overcome this issue.

**Claim 6.3.** *Assume there exists a subset  $V \subseteq [D]$  such that  $\{A_i(w)\}_{i \in [t], w \in V}$  are all distinct, and enumerate  $\{Q_1(x, w)\}_{x \in X, w \in V} = Q_1, \dots, Q_{s=K|V|}$  arbitrarily. Then, for every  $i \in [s]$ ,*

$$\mathbf{E}[Q_i \mid Q_1, \dots, Q_{i-1}] = 0.$$

*Proof.* Fix  $i \in [s]$ . First note that for  $x_a \neq x_b$ ,  $Q_a = Q_1(x_a, w_a)$  and  $Q_b = Q_1(x_b, w_b)$  are independent. Assume that  $Q_i = Q_1(x, w)$  and let  $\{i_1, \dots, i_\ell\} \subseteq [i-1]$  be the indices that correspond to the same  $x$ , i.e., each  $Q_{i_j} = Q_1(x, w_j)$  for some  $w_j \neq w$ . Thus,

$$\mathbf{E}[Q_i \mid Q_1, \dots, Q_{i-1}] = \mathbf{E}[Q_i \mid Q_{i_1}, \dots, Q_{i_\ell}].$$

Next, fix all values of  $\text{Ext}$  queried by the  $Q_{i_j}$ -s. Keeping the notation  $Q_{i_j} = Q_1(x, w_j)$ , this means we fix every  $\text{Ext}(x, A_r(w_j))$  for  $j \in [\ell]$  and  $r \in [t]$ . These fixings do not affect  $Q_i$ , by our assumption on  $V$ . Thus, under these fixings,  $\mathbf{E}[Q_i] = 0$ , as desired.  $\square$

We now argue that we can partition  $[D]$  to a bounded number of such  $V$ -s.

**Lemma 6.4.** *There exists a partition  $[D] = V_1 \cup \dots \cup V_L$  for  $L = O(dt^2 2^\Delta)$  such that for every  $i \in [L]$ ,  $\{A_j(w)\}_{j \in [t], w \in V_i}$  are all distinct.*

*Proof.* Let  $G' = (W = [D], U = [D], E_0)$  be the bipartite graph in which each  $w \in W$  is connected to  $A_1(w), \dots, A_t(w)$ . Thus,  $G'$  is left-regular with degree  $t$  and its right-degree is bounded by  $t \cdot 2^\Delta$ . Let  $G = (V = [D], E)$  be the two-step walk graph of  $G'$ . Namely,  $(x, y) \in E$  if and only if there exists a path  $x \sim z \sim y$  in  $G'$ , where  $x, y \in W$  and  $z \in U$ . Note that the maximal degree in  $G$  is at most  $t^2 \cdot 2^\Delta$ . We will repeatedly use the following standard claim, which can be shown by a simple greedy algorithm.



**Claim 6.5.** *Let  $G$  be an undirected graph over  $n$  vertices with maximal degree  $\delta$ . Then, the size of the largest independent set in  $G$  is at least  $\frac{n}{\delta+1}$ .*

The crucial observation is that an independent set in  $G$  corresponds to a valid partition. To see this, take any  $w_1, w_2 \in V$  such that  $(w_1, w_2) \notin E$ . By definition, there are no  $r_1, r_2 \in [t]$  such that  $A_{r_1}(w_1) = A_{r_2}(w_2)$ . In light of this observation, we can greedily define  $V_1, \dots, V_L$  in the following manner.

1. Set  $G_0 \leftarrow G$ ,  $i \leftarrow 0$  and  $\delta = t^2 2^\Delta$ .
2. As long as  $G_i$  has more than  $2\delta$  vertices,
  - Let  $V_{i+1}$  be the largest independent set in  $G_i$ .
  - Remove  $V_{i+1}$  and all its adjacent edges and denote the resulting graph by  $G_{i+1}$ . Set  $i \leftarrow i + 1$ .
3. The graph  $G_i$  has  $b \leq 2\delta$  vertices. Put each of these vertices in a separate set.
4. The resulting partition is  $V_1, \dots, V_i, \dots, V_{L=i+b}$ .

Claim 6.5 guarantees that at each iteration,  $V_{i+1}$  contains at least  $1 - \frac{1}{\delta+1}$  fraction of the remaining vertices. Let  $j$  be the smallest integer for which

$$\left(1 - \frac{1}{\delta+1}\right)^j \cdot 2^d \leq 2\delta.$$

One can verify that  $j = O(\delta d)$ , so overall  $L \leq j + 2\delta = O(dt^2 2^\Delta)$ , as desired.  $\square$

In light of the above lemma and Claim 6.3, we can define, for each  $i \in [L]$ ,

$$\mathbf{S}_i = \sum_{x \in X, w \in V_i} Q_1(x, w),$$

so  $\mathbf{Q}_1 = \frac{1}{KD} \sum_{i \in [L]} \mathbf{S}_i$ . Note that every sequence in  $\mathbf{S}_i$  is a martingale, and also, that  $|Q_1(x, w)| \leq 1$  with probability 1. Thus, using Azuma's inequality,

$$\begin{aligned} \Pr \left[ |\mathbf{Q}_1| > \frac{\varepsilon}{2} \right] &= \Pr \left[ \left| \sum_{i \in [L]} \mathbf{S}_i \right| > \frac{\varepsilon}{2} KD \right] \leq \sum_{i \in [L]} \Pr \left[ |\mathbf{S}_i| > \frac{\varepsilon}{2L} KD \right] \\ &\leq \sum_{i \in [L]} 2 \exp \left( -\frac{\left(\frac{\varepsilon}{2L} KD\right)^2}{2K|V_i|} \right) \leq 2L \cdot e^{-\frac{KD}{8L^2} \varepsilon^2}. \end{aligned} \tag{6.1}$$

**Handling  $Q_2$ .** Similarly, we define  $\mathbf{Q}_2 = \mathbf{E}_{x \sim X, w \sim [D]}[Q_2(x, w)]$ , but we write it as

$$\mathbf{Q}_2 = \mathbf{E}_{x \sim X, y \sim Y} \left[ \mathbf{E}_{w \sim [D]} [T_w(Z(x, y))] - \mu(T) \right],$$

i.e., we switched the order of  $w$  and  $y$ . Now, define

$$Q'_2(x, y) = \mathbf{E}_{w \sim [D]} [T_w(Z(x, y))] - \mu(T),$$

so  $\mathbf{Q}_2 = \mathbf{E}_{x \sim X, y \sim [D]}[Q'_2(x, y)]$ . We follow the same reasoning as before: For arbitrary  $y_1 \neq y_2$ ,  $Q'_2(x, y_1)$  may depend on  $Q'_2(x, y_2)$ , but with the same partitioning we can overcome the dependencies. Also, for any  $x \in \{0, 1\}^n$  and  $y \in [D]$  it holds that

$$\mathbf{E} \left[ \mathbf{E}_{w \sim [D]} [T_w(Z(x, y))] \right] = \mu(T),$$

so overall,

$$\Pr \left[ |\mathbf{Q}_2| > \frac{\varepsilon}{2} \right] \leq 2L \cdot e^{-\frac{KD}{8L^2}\varepsilon^2} \quad (6.2)$$

as well.

**Putting it altogether.** Combining Equations (6.1) and (6.2), we get

$$\Pr \left[ \mathbf{E}_{x \sim X, w \sim [D]} [Q(x, w)] > \varepsilon \right] \leq 4L \cdot e^{-\frac{KD}{8L^2}\varepsilon^2} \leq 2^{-c_1 \frac{KD}{d^2 t^4 2^{2\Delta}} \varepsilon^2 + \log d + 2 \log t + c_2}$$

for some universal constants  $c_1, c_2 > 0$ . To complete our analysis, we require **Ext** to work for any  $X, A_1, \dots, A_t$  and  $T$ . By the union bound, the probability for a random **Ext** to fail, denote it by  $p$ , is as given by

$$\begin{aligned} p &\leq \binom{N}{K} D^{tD} 2^{DM^t} 2^{-c_1 \frac{KD}{d^2 t^4 2^{2\Delta}} \varepsilon^2 + \log d + 2 \log t + c_2} \\ &\leq 2^{K \log \left( \frac{N\varepsilon}{K} \right) + tDd + DM^t - c_1 \frac{KD}{d^2 t^4 2^{2\Delta}} \varepsilon^2 + \log d + 2 \log t + c_2} \\ &\leq 2^{K(n-k+2) + tDd + DM^t + \log d + 2 \log t + c_2 - c_1 \frac{KD}{d^2 t^4 2^{2\Delta}} \varepsilon^2}. \end{aligned}$$

To prove that  $p < 1$  (in fact, we will show that  $p \ll 1$ ) it is sufficient to argue that:

1.  $K(n - k + 2) \leq \frac{c_1}{4} \frac{KD}{d^2 t^4 2^{2\Delta}} \varepsilon^2$ , and,
2.  $D(td + M^t) + \log d + 2 \log t + c_2 \leq \frac{c_1}{4} \frac{KD}{d^2 t^4 2^{2\Delta}} \varepsilon^2$ , or,  $D(4td + M^t) \leq \frac{c_1}{4} \frac{KD}{d^2 t^4 2^{2\Delta}} \varepsilon^2$ .

Item 1 is true whenever

$$D \geq \frac{4}{c_1} \cdot \frac{(n - k + 2)d^2 t^4 2^{2\Delta}}{\varepsilon^2}.$$

Item 2 it true whenever

$$K \geq \frac{4}{c_1} \cdot \frac{(4td + M^t)d^2 t^4 2^{2\Delta}}{\varepsilon^2}.$$

The bounds on  $d$  and  $k$  follow from the above two inequalities. □

## References

- [BADTS17] Avraham Ben-Aroya, Dean Doron, and Amnon Ta-Shma. An efficient reduction from two-source to non-malleable extractors: achieving near-logarithmic min-entropy. In *STOC'17—Proceedings of the 49th Annual ACM SIGACT Symposium on Theory of Computing*, pages 1185–1194. ACM, New York, 2017.
- [BADTS20] Avraham Ben-Aroya, Dean Doron, and Amnon Ta-Shma. Near-optimal erasure list-decodable codes. In *35th Computational Complexity Conference (CCC 2020)*. Schloss Dagstuhl-Leibniz-Zentrum für Informatik, 2020.
- [BKS<sup>+</sup>10] B. Barak, G. Kindler, R. Shaltiel, B. Sudakov, and A. Wigderson. Simulating independence: new constructions of condensers, Ramsey graphs, dispersers, and extractors. *J. ACM*, 57(4):Art. 20, 52, 2010.
- [Bou05] J. Bourgain. More on the sum-product phenomenon in prime fields and its applications. *Int. J. Number Theory*, 1(1):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. *Ann. of Math. (2)*, 176(3):1483–1543, 2012.
- [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'16—Proceedings of the 48th Annual ACM SIGACT Symposium on Theory of Computing*, pages 285–298. ACM, New York, 2016.
- [CL16] Eshan Chattopadhyay and Xin Li. Explicit non-malleable extractors, multi-source extractors and almost optimal privacy amplification protocols. In *57th Annual IEEE Symposium on Foundations of Computer Science—FOCS 2016*, pages 158–167. IEEE Computer Soc., Los Alamitos, CA, 2016.
- [Coh16a] Gil Cohen. Local correlation breakers and applications to three-source extractors and mergers. *SIAM J. Comput.*, 45(4):1297–1338, 2016.
- [Coh16b] Gil Cohen. Making the most of advice: new correlation breakers and their applications. In *57th Annual IEEE Symposium on Foundations of Computer Science—FOCS 2016*, pages 188–196. IEEE Computer Soc., Los Alamitos, CA, 2016.

- [Coh16c] Gil Cohen. Non-malleable extractors—new tools and improved constructions. In *31st Conference on Computational Complexity*, volume 50 of *LIPICs. Leibniz Int. Proc. Inform.*, pages Art. No. 8, 29. Schloss Dagstuhl. Leibniz-Zent. Inform., Wadern, 2016.
- [Coh16d] Gil Cohen. Two-source dispersers for polylogarithmic entropy and improved Ramsey graphs. In *STOC'16—Proceedings of the 48th Annual ACM SIGACT Symposium on Theory of Computing*, pages 278–284. ACM, New York, 2016.
- [Coh17] Gil Cohen. Towards optimal two-source extractors and Ramsey graphs. In *STOC'17—Proceedings of the 49th Annual ACM SIGACT Symposium on Theory of Computing*, pages 1157–1170. ACM, New York, 2017.
- [CRS12] Gil Cohen, Ran Raz, and Gil Segev. Non-malleable extractors with short seeds and applications to privacy amplification. In *2012 IEEE 27th Conference on Computational Complexity—CCC 2012*, pages 298–308. IEEE Computer Soc., Los Alamitos, CA, 2012.
- [CS16] Gil Cohen and Leonard J. Schulman. Extractors for near logarithmic min-entropy. In *57th Annual IEEE Symposium on Foundations of Computer Science—FOCS 2016*, pages 178–187. IEEE Computer Soc., Los Alamitos, CA, 2016.
- [CZ19] Eshan Chattopadhyay and David Zuckerman. Explicit two-source extractors and resilient functions. *Ann. of Math. (2)*, 189(3):653–705, 2019.
- [DKSS13] Zeev Dvir, Swastik Kopparty, Shubhangi Saraf, and Madhu Sudan. Extensions to the method of multiplicities, with applications to Kakeya sets and mergers. *SIAM J. Comput.*, 42(6):2305–2328, 2013.
- [DLWZ11] Yevgeniy Dodis, Xin Li, Trevor D. Wooley, and David Zuckerman. Privacy amplification and non-malleable extractors via character sums. In *2011 IEEE 52nd Annual Symposium on Foundations of Computer Science—FOCS 2011*, pages 668–677. IEEE Computer Soc., Los Alamitos, CA, 2011.
- [DW09] Yevgeniy Dodis and Daniel Wichs. Non-malleable extractors and symmetric key cryptography from weak secrets. In *STOC'09—Proceedings of the 2009 ACM International Symposium on Theory of Computing*, pages 601–610. ACM, New York, 2009.
- [GUV09] Venkatesan Guruswami, Christopher Umans, and Salil Vadhan. Unbalanced expanders and randomness extractors from Parvaresh-Vardy codes. *J. ACM*, 56(4):Art. 20, 34, 2009.

- [Li15] Xin Li. Three-source extractors for polylogarithmic min-entropy. In *2015 IEEE 56th Annual Symposium on Foundations of Computer Science—FOCS 2015*, pages 863–882. IEEE Computer Soc., Los Alamitos, CA, 2015.
- [Li17] Xin Li. Improved non-malleable extractors, non-malleable codes and independent source extractors. In *STOC’17—Proceedings of the 49th Annual ACM SIGACT Symposium on Theory of Computing*, pages 1144–1156. ACM, New York, 2017.
- [Li19] Xin Li. Non-malleable extractors and non-malleable codes: partially optimal constructions. In *34th Computational Complexity Conference*, volume 137 of *LIPICs. Leibniz Int. Proc. Inform.*, pages Art. No. 28, 49. Schloss Dagstuhl. Leibniz-Zent. Inform., Wadern, 2019.
- [LRVW03] Chi-Jen Lu, Omer Reingold, Salil Vadhan, and Avi Wigderson. Extractors: Optimal up to constant factors. In *Proceedings of the thirty-fifth annual ACM symposium on Theory of computing*, pages 602–611, 2003.
- [NZ96] Noam Nisan and David Zuckerman. Randomness is linear in space. *J. Comput. System Sci.*, 52(1):43–52, 1996.
- [Raz05] Ran Raz. Extractors with weak random seeds. In *STOC’05: Proceedings of the 37th Annual ACM Symposium on Theory of Computing*, pages 11–20. ACM, New York, 2005.
- [RTS00] Jaikumar Radhakrishnan and Amnon Ta-Shma. Bounds for dispersers, extractors, and depth-two superconcentrators. *SIAM Journal on Discrete Mathematics*, 13(1):2–24, 2000.
- [Sha11] Ronen Shaltiel. An introduction to randomness extractors. In *Automata, languages and programming. Part II*, volume 6756 of *Lecture Notes in Comput. Sci.*, pages 21–41. Springer, Heidelberg, 2011.
- [Tre01] Luca Trevisan. Extractors and pseudorandom generators. *J. ACM*, 48(4):860–879, 2001.
- [TSU12] Amnon Ta-Shma and Christopher Umans. Better condensers and new extractors from Parvaresh-Vardy codes. In *2012 IEEE 27th Conference on Computational Complexity—CCC 2012*, pages 309–315. IEEE Computer Soc., Los Alamitos, CA, 2012.
- [Vad12] Salil P Vadhan. *Pseudorandomness*, volume 7. Now, 2012.

## A Missing proofs

*Proof of Claim 1.2.* For the first item, a seed protecting extractor against  $\Pi$  can be seen to be a strong seeded-extractor by taking  $A$  to be the identity function. Indeed, with this choice, since  $\text{Ext}$  is a seeded-extractor, the right hand side of Equation (1.2) is  $\varepsilon$ -close to  $U_{d+m}$ , and so  $(Y, \text{Ext}(X, Y)) \approx_{2\varepsilon} (Y, U_m)$ . For the other direction, as  $\text{Ext}$  is  $(k, \varepsilon)$ -strong we have that  $(Y, \text{Ext}(X, Y)) \approx_\varepsilon (Y, U_m)$ . Thus, for any  $A \in \Pi_d$ , it holds that

$$(A(Y), \text{Ext}(X, A(Y))) \approx_\varepsilon (A(Y), U_m).$$

By the data processing inequality, one can apply any function to the first component  $A(Y)$  of both sides and maintain the  $\varepsilon$ -closeness. In particular, by applying  $A^{-1}$  we get

$$(Y, \text{Ext}(X, A(Y))) \approx_\varepsilon (Y, U_m). \quad (\text{A.1})$$

Now,  $(Y, U_m)$  has the same distribution as  $U_{d+m}$ , and  $\text{Ext}(X, A(Y)) \approx_\varepsilon U_m$ . This, together with Equation (A.1), implies that  $(Y, \text{Ext}(X, A(Y))) \approx_{2\varepsilon} (U_d, \text{Ext}(X, A(Y)))$ , completing the proof.  $\square$

*Proof of Claim 1.5.* Fix an arbitrary  $w \in \{0, 1\}^d$  and assume without loss of generality that  $\Pr[\text{Ext}(U_n, w) = 0] \geq \frac{1}{2}$ . Define  $X$  to be the random variable that is uniformly distributed over all  $x \in \{0, 1\}^n$  such that  $\text{Ext}(x, w) = 0$ . Since  $\text{Ext}$  is a  $(k, \varepsilon)$ -seeded-extractor for min-entropy  $k$  and as  $H_\infty(X) \geq n - 1 \geq k$ , we have that  $\text{Ext}(X, Y) \approx_\varepsilon U_1$ . Equivalently,

$$\Pr[\text{Ext}(X, Y) = 1] \geq \frac{1}{2} - \varepsilon.$$

By an averaging argument, there exists  $z \in \{0, 1\}^d$  such that

$$\Pr[\text{Ext}(X, z) = 1] \geq \frac{1}{2} - \varepsilon.$$

Note that  $w \neq z$ . Define the function  $A : \{0, 1\}^d \rightarrow \{0, 1\}^d$  by

$$A(y) = \begin{cases} w & y_1 = 0, \\ z & y_1 = 1, \end{cases}$$

and note that  $A \in \mathcal{T}$ . Denote  $Z = \text{Ext}(X, Y)$  and  $Z' = \text{Ext}(X, A(y))$ . We turn to show that

$$\gamma = \text{SD}((Y, Z'), (U_d, Z')) \geq \frac{1}{4} - \frac{\varepsilon}{2}.$$

To see this, note that

$$\gamma \geq \text{SD}((Y_1, Z'), (U_1, Z')) \geq \Pr[Z' = Y_1] - \Pr[Z' = U_1]. \quad (\text{A.2})$$

We have that

$$\begin{aligned}\Pr[Z' = Y_1] &= \frac{1}{2} \Pr[Z' = Y_1 \mid Y_1 = 0] + \frac{1}{2} \Pr[Z' = Y_1 \mid Y_1 = 1] \\ &= \frac{1}{2} (\Pr[\text{Ext}(X, w) = 0] + \Pr[\text{Ext}(X, z) = 1]) \\ &\geq \frac{1}{2} \left(1 + \frac{1}{2} - \varepsilon\right) \\ &= \frac{3 - 2\varepsilon}{4}.\end{aligned}$$

On the other hand,  $\Pr[Z' = U_1] = \frac{1}{2}$ , and so by Equation (A.2),

$$\gamma \geq \frac{3 - 2\varepsilon}{4} - \frac{1}{2} \geq \frac{1}{4} - \frac{\varepsilon}{2}.$$

Thus, as we assume  $\varepsilon < \frac{1}{6}$ , we get that  $\gamma > \frac{1}{6}$  which concludes the proof.  $\square$