Electronic Colloquium on Computational Complexity, Report No. 150 (2021)

# Extractors: Low Entropy Requirements Colliding With Non-Malleability

Eldon Chung* Maciej Obremski† Divesh Aggarwal‡

November 7, 2021

**Abstract**

The known constructions of negligible error (non-malleable) two-source extractors can be broadly classified in three categories:

- Constructions where one source has min-entropy rate about 1/2, the other source can have small min-entropy rate, but the extractor doesn't guarantee non-malleability.
- Constructions where one source is uniform, and the other can have small min-entropy rate, and the extractor guarantees non-malleability when the uniform source is tampered.
- Constructions where both sources have entropy rate very close to 1 and the extractor guarantees non-malleability against the tampering of both sources.

We introduce a new notion of collision resistant extractors and in using it we obtain a strong two source non-malleable extractor where we require the first source to have 0.8 entropy rate and the other source can have min-entropy polylogarithmic in the length of the source.

We show how the above extractor can be applied to obtain a non-malleable extractor with output rate $\frac{1}{2}$, which is optimal. We also show how, by using our extractor and extending the known protocol, one can obtain a privacy amplification secure against memory tampering where the size of the secret output is almost optimal.

## 1 Introduction

**Two-source extractors.** The problem of constructing efficient two-source extractors for low min-entropy sources with negligible error has been an important focus of research in pseudorandomness for more than 30 years, with fundamental connections to combinatorics and many applications in computer science. The first non-trivial construction was given by Chor and Goldreich [CG88] who showed that the inner product function is a low-error two-source extractor for $n$-bit sources with min-entropy $(1/2 + \gamma)n$, where $\gamma > 0$ is an arbitrarily small constant. A standard application of the probabilistic method shows that (inefficient) low-error two-source extractors exist for polylogarithmic min-entropy. While several attempts were made to improve the construction of [CG88] to allow for sources with smaller min-entropy, the major breakthrough results were obtained after almost two decades. Raz [Raz05] gave an explicit low-error two-source extractor where one of the sources must have min-entropy $(1/2 + \gamma)n$ for an arbitrarily small constant $\gamma > 0$, while the other source is allowed to have logarithmic min-entropy. In an incomparable result, Bourgain [Bou05] gave an explicit low-error two-source extractor for sources with min-entropy $(1/2 - \gamma)n$, where $\gamma > 0$ is a small constant. An improved analysis by Lewko [Lew19] shows that Bourgain's extractor can handle sources with min-entropy $4n/9$.

**(Seeded) non-malleable extractors.** The problem of privacy amplification against active adversaries was first considered by Maurer and Wolf [MW97]. In a breakthrough result, Dodis and Wichs [DW09] introduced the notion of seeded non-malleable extractors as a natural tool towards achieving a privacy amplification protocol in a minimal number of rounds, and with minimal entropy loss. Roughly speaking, the output of a seeded non-malleable extractor with a uniformly random seed $Y$, and a source $X$ with some min-entropy independent of $Y$, should look

*Centre for quantum technologies, National University of Singapore. eldon.chung@u.nus.edu. The ordering of the authors was randomized. A record of which can be found at https://www.aeaweb.org/journals/policies/random-author-order/search?RandomAuthorsSearch%5Bsearch%5D=PRrGREjgkzUk

†Centre for quantum technologies, National University of Singapore. obremski.math@gmail.com

‡Centre for quantum technologies and Department of Computer Science, National University of Singapore. dcsdiva@nus.edu.sg



ISSN 1433-8092

uniformly random to an adversary who can tamper the seed, and obtain the output of the non-malleable extractor on a tampered seed.

More precisely, we require that

$$\mathbf{nmExt}(X,Y), \mathbf{nmExt}(X,g(Y)), Y \approx_\varepsilon U_m, \mathbf{nmExt}(X,g(Y)), Y \ ,$$

where $X$ and $Y$ are independent sources with $X$ having sufficient min-entropy and $Y$ uniformly random, $g$ is an arbitrary tampering function with no fixed points, $U_m$ is uniform over $\{0,1\}^m$ and independent of $X, Y$, and $\approx_\varepsilon$ denotes the fact that the two distributions are $\varepsilon$-close in statistical distance (for small $\varepsilon$).

Prior works have also studied seeded extractors with weaker non-malleability guarantees such as look-ahead extractors [DW09] or affine-malleable extractors [AHL16], and used these to construct privacy amplification protocols.

**Non-malleable two-source extractors.** A natural strengthening of both seeded non-malleable extractors, and two-source extractors are two-source *non-malleable* extractors. Two-source non-malleable extractors were introduced by Cheraghchi and Guruswami [CG17]. Roughly speaking, a function $\mathbf{2NMExt} : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^m$ is said to be a non-malleable extractor if the output of the extractor remains close to uniform (in statistical distance), even conditioned on the output of the extractor inputs correlated with the original sources. In other words, we require that

$$\mathbf{2NMExt}(X,Y), \mathbf{2NMExt}(f(X),g(Y)), Y \approx_\varepsilon U_m, \mathbf{2NMExt}(f(X),g(Y)), Y \ .$$

where $X$ and $Y$ are independent sources with enough min-entropy, $f, g$ are arbitrary tampering functions such that one of $f, g$ has no fixed points.

The original motivation for studying efficient two-source non-malleable extractors stems from the fact that they directly yield explicit split-state non-malleable codes [DPW18] (provided the extractor also supports efficient preimage sampling).

The first constructions of non-malleable codes [DKO13, ADL18] relied heavily on the (limited) non-malleability of the inner-product two-source extractor. Subsequent improved constructions of non-malleable codes in the split-state model relied on both the inner-product two-source extractor [ADKO15, AO20], and on more sophisticated constructions of the two-source non-malleable extractors [CGL16, Li17, Li19a]. Soon after they were introduced, non-malleable extractors have found other applications such as non-malleable secret sharing [GK18, ADN$^+$19].

**Connections, and state-of-the-art constructions.** As one might expect, the various notions of extractors mentioned above are closely connected to each other. Li [Li12] obtained the first connection between seeded non-malleable extractors and two-source extractors based on inner products. This result shows that an improvement of Bourgain's result would immediately lead to better seeded non-malleable extractors, and a novel construction of seeded non-malleable extractors with a small enough min-entropy requirement and a small enough seed size would immediately lead to two-source extractors that only require small min-entropy. However, [Li12] could only obtain seeded non-malleable extractors for entropy rate above $1/2$.

In yet another breakthrough result, [CGL16] obtained a sophisticated construction of seeded non-malleable extractors for polylogarithmic min-entropy. Additionally, they showed that similar techniques can also be used to obtain two-source non-malleable extractors. This immediately led to improved privacy amplification protocols and improved constructions of non-malleable codes in the split-state model. Building on this result, in a groundbreaking work, Chattopadhyay and Zuckerman [CZ19] gave a construction of two-source extractors with polylogarithmic min-entropy and polynomiallly small error. All of these results have subsequently been improved in [Li16, BDT17, Coh17, Li17, Li19a].

The research over the past few years has shown that non-malleable two-source extractors, seeded non-malleable extractors, two-source extractors, non-malleable codes, and privacy amplification protocols are strongly connected to each other in the sense that improved construction of one of these objects has led to improvements in the construction of others. Some results have made these connections formal by transforming a construction of one object into a construction of another object. For instance, in addition to the connections already mentioned, Ben-Aroya et al. [BCD$^+$18] adapt the approach of [CZ19] to show explicit *seeded* non-malleable extractors with improved seed length lead to explicit low-error two-source extractors for low min-entropy.

Also, [AOR$^+$20] showed that some improvement in the parameters of non-malleable two-source extractor constructions from [CGL16, Li17, Li19a] leads to explicit low-error two-source extractors for min-entropy $\delta n$ with a very small constant $\delta > 0$.

**Application to Privacy Amplification.** In [AOR+20], the authors introduce an extension of privacy amplification against active adversaries where, Eve as the active adversary is additionally allowed to *fully corrupt* the internal memory of one of the honest parties, Alice and Bob, before the execution of the protocol.

Informally, in the initial phase we assume that Alice and Bob share a secret $W$ with sufficient min-entropy, and that they have access to local independent randomness $A$ and $B$, respectively. We say $(W, A)$ (resp. $(W, B)$) is Alice's *state* (resp. Bob's). Before the execution of the privacy amplification protocol between Alice and Bob, we allow Eve to specify a tampering function $F$ and one of Alice and Bob to be corrupted (e.g., by infecting either Alice's or Bob's storage device with a virus). If Alice is chosen, then Alice's state $(W, A)$ is replaced by $(\widetilde{W}, \widetilde{A}) = F(W, A)$. Eve does not learn the output of $F$, and Alice and Bob do not know whether (or which) state was corrupted.

The goal of the privacy amplification protocol is twofold:

1. **If Eve is passive:** If Eve does not tamper either of Alice's or Bob's states nor does she tamper any of the messages between Alice and Bob, it is required that Alice and Bob agree on a shared $m$-bit string $S$ such that, if $C$ denotes Eve's view of the protocol, then
$$S, C \approx U_m, C, \tag{1}$$
where $U_m$ is independent of $C$, and $\approx$ denotes some notion of computational or statistical indistinguishability.
2. **If Eve is active:** In this case, with high probability there either one of Alice or Bob detects Eve's tampering and aborts the protocol (i.e., outputs $\perp$), or they end up with a shared $m$-bit string $S$ satisfying (1).

It was shown in [AOR+20] that two-source non-malleable extractors are natural tools for designing such privacy amplification protocols. However, they required two-source non-malleable extractors with one source having a small entropy rate $\delta$ (where $\delta$ is a constant close to 0), and all known constructions of non-malleable two-source extractors mentioned above have entropy rate very close to 1.

**Best of all worlds.** Notice that the seeded non-malleable extractor, and the two-source extractors can be seen as special case of a two-source non-malleable extractor. With this view, the known constructions of negligible error (non-malleable) two-source extractors can be broadly classified in three categories:

- Constructions where one source has min-entropy rate about 1/2, the other source can have small min-entropy rate, but the extractor doesn't guarantee non-malleability.
- Constructions where one source is uniform, and the other can have small min-entropy rate, and the extractor guarantees non-malleability when the uniform source is tampered.
- Constructions where both sources have entropy rate very close to 1 and the extractor guarantees non-malleability against the tampering of both sources.

The main focus of this work is the question whether we can have one construction that subsumes all the above constructions.

**Question 1.** *Is there an explicit construction of a two-source non-malleable extractor which requires two sources of length $n_1$ and $n_2$, and min-entropy requirement $cn_1$ (for some constant $c < 1$), and $\text{poly}\log n_2$, respectively, that guarantees non-malleability against the tampering of both sources, and for which the error is negligible? In particular, can we obtain a construction with parameters suitable for application to privacy amplification with tamperable memory [AOR+20]?*

In this work, we make progress towards answering this question.

**Our Contributions and Organization of the Paper.**

- In Section 2, we give an overview of our technical details.
- In Section 3, we give mathematical preliminaries needed in the paper.
- In Section 4, we give a generic transformation that, takes in (1) a non-malleable two-source extractor which requires sources with high min-entropy, and (2) a two-source extractor which requires sources with smaller min-entropy and an additional collision-resistance property, and constructs a two-source non-malleable extractor with min-entropy requirement comparable to (but slightly worse) that of the two-source extractor used by the construction.

- In Section 5.1, we give a generic transformation that converts any seeded extractor (two-source extractor where one of the source is uniformly distributed) to a collision-resistant seeded extractor with essentially the same parameters.
- In Section 5.2, we show that the two-source extractor from [Raz05] is collision resistant.
- In Section 6, we apply our generic transformation from Section 5.1 to the seeded extractor from [RRV99] to obtain a collision-resistant seeded extractor. We then use the generic transformation from Section 4 along with the non-malleable extractor from [Li19a] to obtain a two-source non-malleable extractor, where one of the source is uniform and the other has min-entropy polylogarithmic in the length of the sources.
- In Section 7, we apply the generic transformation from Section 4 to the non-malleable extractor from Section 6, and the two-source extractor from [Raz05] to obtain a two-source non-malleable extractor where one source is required to have polylogarithmic min-entropy and the source is required to have min-entropy rate greater than 0.8.
- In Section 8, we use a generic transformation from [AKO+21] to obtain a non-malleable two-source extractor where the length of the output is $1/2 - o(1)$ times the length of the input. Notice that via the probabilistic method, it can be shown that the output length of this construction is optimal. [1]
- In Appendix A, we sketch the details of the privacy amplification protocol that uses our non-malleable two-source extractor. We extend the protocol by [AOR+20] to obtain a secret of optimal size while maintaining security against a memory tampering adversary.

# 2 Technical overview

## 2.1 Collision Resistant Extractors

At the core of our non-malleable extractor compiler is a new object we call a *collision resistant extractor*. An extractor is an object that takes as input two sources of randomness $X$ and $Y$ (in case of the seeded extractors $Y$ but uniform) and guarantees that, as long as $X$ and $Y$ are independent and have sufficient min-entropy, the output $\texttt{ext}(X, Y)$ will be uniform (even given $Y$ [2]). A *collision resistant extractor* $\mathbf{C}$ has the added property that for all fixed-point-free functions $f$ (i.e. $f(x) \neq x$ for all $x$) the probability that $\mathbf{C}(X, Y) = \mathbf{C}(f(X), Y))$ is negligible [3].

Readers might notice the resemblance to the collision resistant hashing families and the leftover hash lemma. The leftover hash lemma states that if the probability that $h(x_0, Y) = h(x_1, Y)$ is sufficiently small then $h(.,.)$ is an extractor. Obremski and Skorski ([OS18]) showed that the inverse is almost true — there exists a 'core' of inputs on which every extractor has to fulfill the small collision probability property. This inverse leftover hash lemma is sadly not constructive and not efficient (the description of the core might be exponential), and thus we are unable to use it to obtain an efficient *collision resistant extractor*.

We show that Raz's extractor ([Raz05]) is a *collision resistant extractor* with essentially the same parameters. We obtain this result by carefully modifying the original proof. The proof techniques are similar and we do not discuss the details in this section.

We also show a generic transform that turns any seeded extractor (a two-source extractor where one source is uniform) into a *collision resistant extractor* with a slight increase in the size of the seed.

### 2.1.1 General Compiler for Seeded Extractors

We first construct a collision-resistant extractor $h$ with a short output based on the Nisan-Widgerson generator or Trevisan's extractor. Given the input $X$ and the seed $Z$ function $h$ will output $\hat{X}(Z_1) \circ \hat{X}(Z_2) \circ \cdots \circ \hat{X}(Z_t)$ where $\texttt{EC}$ is an error-correcting code of appropriate minimum distance, $\hat{X} = \texttt{EC}(X)$, and $Z = Z_1 \circ Z_2 \circ \cdots \circ Z_t$, and $\hat{X}(Z_i)$ denotes $Z_i$-th bit of $\hat{X}$. Proof that this is an extractor follows directly from Nisan-Widgerson generator properties, while the collision resistance follows from the large distance of the error-correcting code.

We can now use any seeded extractor and the collision resistant extractor mentioned above to obtain a collision resistant seeded extractor with output size comparable to the seeded extractor. Consider seeded extractors that

[1] The main drawback of this construction compared to the construction from 7 is that this is not a strong two-source non-malleable extractor, and hence cannot be used in most applications.

[2] This property is often referred to as strong extraction

[3] This notion might somewhat resemble various non-malleability notions, however in case of the non-malleability one would expect $\mathbf{C}(f(X), Y))$ to be independent of $\mathbf{C}(X, Y)$, here we only expect that those two outputs don't collide

take as input a random source $X$ and a short but uniform source $S$ and output $\texttt{ext}(X,S)$ which is uniform (even given $S$ [2]). Let us require on input a slightly longer uniform seed $S \circ Z$ (where $\circ$ denotes concatenation), and consider the following extractor: $\mathbf{C}(X, S \circ Z) = \texttt{ext}(X,S) \circ h(X,Z)$, where $h$ is either a collision resistant hash function or a collision resistant extractor.

The proof follows quite easily. Function $h$ ensures that collisions indeed happen with negligible probability, the only thing left to show is that $\mathbf{C}(X, S \circ Z)$ is uniform. First notice that by the definition the seeded extractor $\texttt{ext}(X,S)$ is uniform, so we only have to show that $h(X,Z)$ is uniform even given $\texttt{ext}(X,S)$. Observe that $Z$ is uniform and independent given $X, S$, so it suffices to show that $X$ has some remaining entropy given $\texttt{ext}(X,S), S$, then $h(X,Z)$ will be uniform (either by leftover hash lemma, if $h$ is a collision resistant hash function, or by the definition of collision resistant extractor). This last step can be ensured simply by setting $\texttt{ext}$ to extract fewer bits than the entropy of $X$, thus a slight penalty in the parameters. Also notice that $h$ above can be a fairly bad extractor in terms of the rate or the output size and seed size. We can make the output and the seed of $h$ very small and thus the parameters of $\mathbf{C}$ will be dominated by the parameters of $\texttt{ext}$.

## 2.2 Our Non-Malleable Extractor Compiler

Our compiler takes as an input two objects, one is a collision resistant extractor (as discussed in the previous section), the other object is a strong two-source non-malleable extractor. A right-strong [4] non-malleable extractor gives the guarantee that $\texttt{ext}(X,Y)$ is uniform even given $\texttt{ext}(f(X), g(Y))$ and $Y$ (or $X$ in case of a left-strong non-malleable extractor) for any tampering functions $f, g$ where at least one of them are fixed-point-free. When we refer to a non-malleable extractor as strong without specifying if it's left-strong or right-strong we mean that the non-malleable extractor is both left-strong and right-strong. The construction is as follows: For a collision resistant extractor $\mathbf{C}$, and a strong non-malleable extractor $\mathbf{E}$ we consider following extractor:

$$\mathbf{2NMExt}(X, Y_\ell \circ Y_r) := \mathbf{E}(Y_\ell \circ Y_r, \mathbf{C}(X, Y_\ell)) \ . \tag{2}$$

We will show that **2NMExt** inherits the best of both worlds — strong non-malleability of $\mathbf{E}$ and the good entropy requirements of $\mathbf{C}$.

There are two main issues to handle:

**Issue of the independent tampering.** Notice that the definition of the non-malleable extractor guarantees that $\texttt{ext}(X,Y)$ is uniform given $\texttt{ext}(X',Y')$ only if the sources are tampered independently (i.e. $X'$ is a function of only $X$, and $Y'$ is a function of only $Y$).

To leverage the non-malleability of $\mathbf{E}$, we need to ensure that the tampering $X \to X'$ and $Y_\ell \circ Y_r \to Y'_\ell \circ Y'_r$ translates to the independent tampering of $Y_\ell \circ Y_r \to Y'_\ell \circ Y'_r$ and $\mathbf{C}(X, Y_\ell) \to \mathbf{C}(X', Y'_\ell)$. The problem is that both tamperings depend on $Y_\ell$. To alleviate this issue we will simply reveal $Y_\ell$ and $Y'_\ell$ (notice that $Y'_\ell$ can depend on $Y_r$ thus revealing $Y_\ell$ alone is not sufficient). Once $Y_\ell = y_\ell$ and $Y'_\ell = y'_\ell$ are revealed the tampering $y_\ell \circ Y_r \to y'_\ell \circ Y'_r$ and $\mathbf{C}(X, y_\ell) \to \mathbf{C}(X', y'_\ell)$ becomes independent since right tampering depends only on $X$, which is independent of $Y_\ell \circ Y_r$ and remains independent of $Y_r$ even after we reveal $Y_\ell$ and $Y'_\ell$ (this extra information only lowers the entropy of $Y_r$).

**Issue of the fixed points (or why we need collision resistance).** Non-malleable extractors guarantee that $\texttt{ext}(X,Y)$ is uniform given $\texttt{ext}(X',Y')$ if and only if $(X,Y) \neq (X',Y')$.

The issue in our compiler is clear: If $Y_\ell \circ Y_r$ do not change, and $X$ is tampered to be $X' \neq X$ but $\mathbf{C}(X', Y_\ell) = \mathbf{C}(X, Y_\ell)$ then

$$\mathbf{2NMExt}(X, Y_\ell \circ Y_r) = \mathbf{E}(Y_\ell \circ Y_r, \mathbf{C}(X, Y_\ell)) = \mathbf{E}(Y_\ell \circ Y_r, \mathbf{C}(X', Y_\ell)) = \mathbf{2NMExt}(X', Y_\ell \circ Y_r) \ . \tag{3}$$

To mitigate this problem, we require $\mathbf{C}$ to be collision resistant, which means the probability that $\mathbf{C}(X, Y_\ell) = \mathbf{C}(X', Y_\ell)$ is negligible thereby resolving this issue. It is also possible to use $\mathbf{C}$ without the collision resilience property, this gives a weaker notion of non-malleable extractor — for further discussion please see Section 2.3.

[4] Notice that unlike many results in the literature, we need to distinguish between left strong and right strong for our extractor since the construction is inherently not symmetric.

**Is 2NMExt strong?** Here we briefly argue that if **E** is strong (i.e. both left and right strong) then **2NMExt** will also be strong. To argue that compiled extractor is left-strong, we notice that revealing $X$ on top of $Y_\ell$ and $Y'_\ell$ (which we had to reveal to maintain independence of tampering) translates to revealing $\mathbf{C}(X, Y_\ell)$ which reveals right input of **E** (revealing of $Y_\ell$ and $Y'_\ell$ is irrelevant since $Y_r$ maintains high enough entropy). As for the right-strongness, revealing $Y_r$ on top of $Y_\ell$ and $Y'_\ell$ translates to revealing of the left input of **E**, notice that $\mathbf{C}(X, Y_\ell)$ remains uniform given $Y_\ell$ by the strong extraction property of **C**.

For our construction, we will apply the compiler twice. First, we will use a collision resistant seeded extractor and the Li's extractor [Li19b]. This gives us a strong non-malleable extractor **FNMExt** for the first source with poly-logarithmic entropy, and the second source being uniform. We will refer to this object as a *fully non-malleable seeded extractor*. Then, we will then apply our compiler to Raz's extractor [Raz05] and **FNMExt** which will produce an extractor **nmRaz** that is a strong non-malleable extractor for the first source with poly-logarithmic entropy and the second source with entropy rate[5] 0.8.

### 2.2.1 Compiling Seeded Extractor with Li's Extractor

In this section we will apply our compiler the collision resistant seeded extractor **crTre** and strong non-malleable extractor **Li** from [Li19b], yielding the following construction:

$$\mathbf{FNMExt}(X, Y_\ell \circ Y_r) = \mathbf{Li}(Y_\ell \circ Y_r, \mathbf{crTre}(X, Y_\ell)). \tag{4}$$

The extractor $\mathbf{Li}(0.99, 0.99)$ requires both sources to have a high entropy rate of $99\%$[6], while the extractor $\mathbf{crTre}(\text{poly-log}, \text{uniform})$ requires first source to have poly-logarithmic entropy, and the second source to be uniform. Let us analyse the entropy requirements of the extractor **FNMExt**: Since part of the construction is $\mathbf{crTre}(X, Y_\ell)$ we require $Y_\ell$ to be uniform, which means that whole $Y_\ell \circ Y_r$ has to be uniform. On the other hand $X$ has to only have a poly-logarithmic entropy. The output of $\mathbf{crTre}(X, Y_\ell)$ will be uniform which will fulfill the 0.99 entropy rate requirement of **Li**. There is a small caveat: While $Y_\ell \circ Y_r$ is uniform one has to remember that we had to reveal $Y_\ell$ and $Y'_\ell$ to ensure independent tampering, therefore we only have to make sure that $Y_\ell$ is very short so $Y_\ell \circ Y_r$ will have over 0.99 entropy rate even given $Y_\ell$ and $Y'_\ell$. This is possible since **crTre** requires only a very short seed length. Thus we get that $\mathbf{FNMExt}(\text{poly-log}, \text{uniform})$ requires first source to have poly-logarithmic entropy, while the second source is uniform.

### 2.2.2 Compiling Raz's Extractor with the Above

Now we will compile Raz's extractor [Raz05] with above obtained **FNMExt**. The result will be:

$$\mathbf{nmRaz}(X, Y_\ell \circ Y_r) = \mathbf{FNMExt}(Y_\ell \circ Y_r, \mathbf{Raz}(X, Y_\ell)). \tag{5}$$

As we discussed above $\mathbf{FNMExt}(\text{poly-log}, \text{uniform})$ requires first source to have poly-logarithmic entropy, while the second source has to be uniform, $\mathbf{Raz}(\text{poly-log}, 0.5)$ requires first source to have poly-logarithmic entropy while second source has to have over 0.5 entropy rate. Therefore we require $Y_\ell$ to have an entropy rate above 0.5 and it is sufficient if $X$ has poly-logarithmic entropy. As for requirements enforced by **FNMExt**, since the output of **Raz** will be uniform we only have check if $Y_\ell \circ Y_r$ has poly-logarithmic entropy given $Y_\ell$ and $Y'_\ell$. Given that $Y'_\ell$ can not lower the entropy of $Y_r$ by more then its size $|Y'_\ell|$ we have two equations:

$$H_\infty(Y_r) > |Y_\ell|$$
$$H_\infty(Y_\ell) > 0.5|Y_\ell|$$

which implies

$$H_\infty(Y_\ell \circ Y_r) > 2|Y_\ell|$$
$$H_\infty(Y_\ell \circ Y_r) > |Y_r| + 0.5|Y_\ell|$$

which asserts that $\frac{H_\infty(Y_\ell \circ Y_r)}{|Y_\ell \circ Y_r|} > 0.8$. Therefore $\mathbf{nmRaz}(\text{poly-log}, 0.8)$ requires first source to have poly-logarithmic entropy, while second source has to have entropy rate above 0.8.

[5] Entropy rate is a ratio of min-entropy of the random variable to its length: $\frac{H_\infty(X)}{|X|}$

[6] This is a simplification, formally speaking there exist a constant $\delta$ such that sources are required to have entropy rate above $1 - \delta$. The reader may think of $\delta = 0.01$.

Finally notice that **Raz** has a relatively short output (shorter than both inputs) but that is not a problem since **FNMExt** can have its first input much longer than the second input. We can adjust the output size of **crTre** to accommodate the input size requirements of **Li** (this extractor requires both inputs to have the same length). We stress however that taking into consideration all inputs requirements both in terms of entropy and in terms of sizes is not trivial and our construction is tuned towards seeded-extractors and the Raz's extractor.

## 2.3 Weaker Variant of Non-Malleable Extractors

As we have already mentioned in the paragraph *Issue of the fixed points* one can consider this compiler without using a collision resistant extractor. Indeed Goyal, Srinivasan and Zhu [GSZ21] did consider the following construction

$$\mathbf{2NMExt}(X, Y_\ell \circ Y_r) := \mathbf{Li}(\mathbf{C}(X, Y_\ell), Y_r), \tag{6}$$

where $\mathbf{C}$ is either a seeded extractor (not collision resistant) or Raz extractor. The notion of non-malleability **2NMExt** achieves is weaker than the standard definition of two-source non-malleable extractor. Namely in this variant $\mathtt{ext}(X, Y)$ and $\mathtt{ext}(X', Y')$ are equal (even if $(X, Y) \neq (X', Y')$) or they are independent[7]. As Goyal, Srinivasan and Zhu note, this weaker notion indeed has a multitude of applications. Below we highlight the limitations of the weaker variant compared to the standard notion. First, using the result by Aggarwal, Kanukurthi, Obbattu, Obremski and Sekar [AKO+21] we show that our strong non-malleable extractor can be compiled into (non-strong) non-malleable extractor with output rate[8] 1/2 (which is optimal).

Then we give the application to the *Privacy Amplification with Tamperable Memory* introduced by Aggarwal, Obremski, Ribeiro, Simkin and Siniscalchi in [AOR+20]. The original protocol can be extended to give an optimal size output.

Both applications work only with the standard notion of non-malleable extractors and not with the weaker variant considered by [GSZ21].

## 2.4 Instantiation of the Rate Compiler

In [AKO+21] the authors give a compiler that turns any left-strong non-malleable extractor into a non-malleable extractor with optimal output rate of $\frac{1}{2}$. The construction looks as follows:

$$\mathbf{2NMExt}(X, Y) = \mathtt{SExt}(X, \mathtt{ext}(X, Y)),$$

where $\mathtt{SExt}$ is a seeded extractor from [GUV09] with output size equal $\frac{1}{2}H_\infty(X)$, and $\mathtt{ext}$ is a left-strong non-malleable extractor.

We will briefly discuss the idea behind that construction. Let $X'$ be a tampering of $X$, and $Y'$ be a tampering of $Y$. We need to argue that if $X \neq X' \vee Y \neq Y'$ then $\mathbf{2NMExt}(X, Y)$ remains uniform even given $\mathbf{2NMExt}(X', Y')$. If $X \neq X' \vee Y \neq Y'$ then left-strong non-malleable extractor $\mathtt{ext}(X, Y)$ is uniform even given $\mathtt{ext}(X', Y'), X$. The final idea crucially relies on the fact that $\mathtt{SExt}$ extracts only half of the entropy of $X$: we can reveal $\mathtt{ext}(X', Y')$ and then $\mathtt{SExt}(X', \mathtt{ext}(X', Y'))$ becomes a leakage from $X$ (i.e. it is just a deterministic function of $X$ with a small output). We get that $\tilde{H}_\infty(X|\mathtt{ext}(X', Y'), \mathtt{SExt}(X', \mathtt{ext}(X', Y'))) \approx \frac{1}{2}H_\infty(X)$ (size of $\mathtt{ext}(X', Y')$ is tiny so it's asymptotically irrelevant). Moreover by the left-strong property of $\mathtt{ext}$ we get that $X$ and $\mathtt{ext}(X, Y)$ remain independent given $\mathtt{ext}(X', Y'), \mathtt{SExt}(X', \mathtt{ext}(X', Y'))$, this means that $\mathtt{SExt}(X, \mathtt{ext}(X, Y))$ is uniform given $\mathtt{ext}(X', Y'), \mathtt{SExt}(X', \mathtt{ext}(X', Y'))$ which gives the result.

Notice that this reduction crucially relies on the fact that if $X \neq X' \vee Y \neq Y'$ then $\mathtt{ext}(X, Y)$ is independent of $\mathtt{ext}(X', Y')$. In a weaker non-malleability version it would be possible to tamper $X \neq X'$ and $Y \neq Y'$ such that $\mathtt{ext}(X, Y) = \mathtt{ext}(X', Y')$, then we would have no guarantee about relation between $\mathtt{SExt}(X, \mathtt{ext}(X, Y))$ and $\mathtt{SExt}(X', \mathtt{ext}(X, Y))$.

## 2.5 Application to Privacy Amplification with Tamperable Memory

Imagine Alice and Bob sharing some random but not uniform string $W$, they would like to "upgrade" their random string $W$ to uniformly random string. However Eve is fully controlling a channel between Alice and Bob and can

[7] In other words this is an extractor that is also a non-malleable randomness encoder.

[8] The output rate of the extractor is the size of the extractors output divided by the entropy of the inputs: for $\mathtt{ext}(X, Y)$ the rate of $\mathtt{ext}$ is $\frac{|\mathtt{ext}|}{H_\infty(X)+H_\infty(Y)}$.

arbitrarily tamper with the messages sent. The Privacy Amplification (PA) protocol guarantees that either Alice and Bob will end up with the same uniform string (unknown to Eve), or at least one of them will abort[9].

In [AOR+20] the authors consider a stronger version of PA which they call a *privacy amplification resilient against memory-tampering active adversaries*. In their model, Alice and Bob have access to a shared string $W$ and their local sources of (not necessarily uniform) randomness $A$ and $B$ respectively. At the beginning of the protocol Eve can select one party, say Alice, and corrupt her memory $F(W, A) = (\tilde{W}, \tilde{A})$ (or $F(W, B) = (\tilde{W}, \tilde{B})$ if Eve decides to corrupt Bob). If Eve did not corrupt the memory of any of the parties then the standard PA guarantees follow. On the other hand if Eve decides to corrupt one of the parties then either Alice and Bob agree on a uniformly random string (unknown to Eve) or the non-corrupted party will detect the tampering.

In the [AOR+20] protocol Alice and Bob exchange the random strings $A$ and $B$ and then locally compute $R = \mathbf{2NMExt}(A \circ B, W)$. They then split $R$ into 3 parts, Alice sends the first part to Bob to prove she has gotten the right output, Bob then sends the second part to Alice to do the same. If this phase was successful then last part of $R$ is the shared uniform string. Figure 1 illustrates the protocol.

| Alice | | Bob |
|---|---|---|
| Memory: $(W, A)$ | | Memory: $(W, B)$ |
| | $A \longrightarrow A'$ | |
| | $B' \longleftarrow B$ | |
| $R_A = \mathbf{2NMExt}(A \circ B', W)$ | | $R_B = \mathbf{2NMExt}(A' \circ B, W)$ |
| | $[R_A]_\alpha \longrightarrow [R_A]'_\alpha$ | |
| | $[R_B]'_{\alpha\cdot 2\alpha} \longleftarrow [R_B]_{\alpha:2\alpha}$ | |
| If $[R_A]_{\alpha\cdot 2\alpha} = [R_B]'_{\alpha:2\alpha}$ | | If $[R_B]_\alpha = [R_A]'_\alpha$ |
| then $S_A = [R_A]_{2\alpha:}$ | | then $S_B = [R_B]_{2\alpha:}$ |
| Otherwise $S_A = \perp$ | | Otherwise $S_B = \perp$ |

Figure 1: Verbatim from [AOR+20]. Privacy amplification protocol against memory-tampering active adversaries. In the above, for an $n$-bit string $x$ we define $[x]_i = (x_1, x_2, \ldots, x_i)$, $[x]_{i:j} = (x_{i+1}, \ldots, x_j)$, and $[x]_{j:} = (x_{j+1}, \ldots, x_n)$.

Since one of the sources of randomness might be faulty, even if the original $A, B$ were uniform, one requires a left-strong non-malleable extractor **2NMExt** to remain secure for the first source with entropy below 0.5, the construction of such an extractor prior to this work was unknown[10].

There are two remarks that we should make now:

The first remark is that the above protocol could work with a weaker notion of non-malleability introduced in [GSZ21]. As we have discussed, one can achieve this notion by compiling standard extractors with non-malleable extractors (instead of collision resistant extractors with non-malleable extractors).

The second remark is that the above protocol obtains very short output compared to entropy of $W$, whereas ideally we would like to obtain something close to entropy of $W$. This is not achievable with the current generation of non-malleable extractors (including the one introduced in this paper). Using the [GSZ21] notion of non-malleability would not have an impact on output rate of the extractor since the bottleneck is caused by the non-malleable extractor not by the collision resistant extractor. We also remark that the extractor achieved in Section 2.4 can not be applied here since it is not strong.

If Alice and Bob have access to uniform randomness, one can extend this protocol to output almost as many bits as $W$'s entropy (see Figure 2). This is only possible if we use the standard notion of non-malleable extractors. After the execution of the [AOR+20] protocol we have the additional guarantee (see proof of Theorem 6, point (b)) that if $S_A \neq \perp$ and $S_B \neq \perp$ then we know that $S_A = S_B$ and are close to uniform and moreover Eve did not tamper with $W$ of either of the parties (this is only achieved with standard notion of non-malleability). If Alice and Bob have access to some extra uniform bits (if $A$ and $B$ were uniform to start with then we could cut them in half $A = A_1 \circ A_2$ and $B = B_1 \circ B_2$, use the first half to run the original protocol by [AOR+20] and save the other half for later) then we can continue the protocol: Alice will send $A_2, \sigma_A$ to Bob, where $\sigma_A$ is a Message Autentication Code of $A_2$ with first half of $S_A$ as a key. Bob will do the same: send $B_2, \sigma_B$ to Alice using other half of $S_B$ as a MAC key. There is a one final problem, we know that one of $A_2$ or $B_2$ is uniform but we don't know which (Eve could have left $W$ unchanged but could have tampered with random coins $A$ and $B$), moreover one of them might

[9] If one of the parties, say Alice, aborts but Bob generates random string $R_B$ then we require $R_B$ to be uniform and unknown to Eve.

[10] Authors of [AOR+20] proceed to construct a computational non-malleable extractors with parameters that would allow for this protocol to go through.

depend on $W$. Notice that $A_2$ and $B_2$ will remain independent, and one of them is independent of $W$ and uniform. Therefore $A_2 + B_2$ is uniform and independent of $W$. Now all we have to do is plug in $W$ and $A_2 + B_2$ into seeded extractor $\texttt{SExt}(W, A_2 + B_2)$ and we can extract almost whole entropy out of $W$ (and the output remains hidden from the view of Eve).

| Alice | | Bob |
|---|---|---|
| Memory: $(W, A_1, A_2)$ | | Memory: $(W, B_1, B_2)$ |
| | $A_1 \longrightarrow A_1'$ | |
| | $B_1' \longleftarrow B_1$ | |
| $R_A = \mathbf{2NMExt}(A_1 \circ B_1', W)$ | | $R_B = \mathbf{2NMExt}(A_1' \circ B_1, W)$ |
| | $[R_A]_\alpha \longrightarrow [R_A]'_\alpha$ | |
| | $[R_B]'_{\alpha\cdot 2\alpha} \longleftarrow [R_B]_{\alpha:2\alpha}$ | |
| If $[R_A]_{\alpha\cdot 2\alpha} = [R_B]'_{\alpha:2\alpha}$ then $S_A^1 = [R_A]_{2\alpha:3\alpha}$ and $S_A^2 = [R_A]_{3\alpha:4\alpha}$ | | If $[R_B]_\alpha = [R_A]'_\alpha$ then $S_B^1 = [R_B]_{2\alpha:3\alpha}$ and $S_B^2 = [R_B]_{3\alpha:4\alpha}$ |
| Otherwise Abort | | Otherwise Abort |
| | If the parties did not Abort we know that $S_A^1 = S_B^1$ and $S_A^2 = S_B^2$, and we know that $W$ has not been tampered with | |
| $\sigma_A = \texttt{MAC}(A_2, S_A^1)$ | $A_2, \sigma_A \longrightarrow A_2', \sigma_A'$ | $\texttt{Verify}(A_2', \sigma_A', S_B^1)$ |
| $\texttt{Verify}(B_2', \sigma_B', S_A^2)$ | $B_2', \sigma_B' \longleftarrow B_2, \sigma_B$ | $\sigma_B = \texttt{MAC}(B_2, S_B^2)$ |
| If verify successful | | If verify successful |
| Output: | | Output: |
| $\texttt{SExt}(W, A_2 + B_2')$ | | $\texttt{SExt}(W, A_2' + B_2)$ |
| Else Abort | | Else Abort |

Figure 2: Extension of the original PA protocol. $R$ is split into 4 parts instead of 3. Here $\texttt{MAC}$ is a standard information theoretic message authentication code (MAC). And $\texttt{SExt}$ is any seeded extractor. When party Aborts it stops responding and the final output is $\perp$.

For formal definitions and the full proof we refer to the Appendix A.

# 3 Preliminaries

## 3.1 Random Variables, Statistical Distance and Entropy

For any set $S$, we denote by $U_S$ the uniform distribution over the set $S$. For any positive integer $m$, we shorthand $U_{\{0,1\}^m}$ by $U_m$. For any random variable $X$, we denote the support of $X$ by $\mathbf{supp}(X)$. Also, for any random variable $X$ and event $E$, we denote by $X|_E$ the random variable $X'$ such that for all $x \in \mathbf{supp}(X)$, $\Pr[X' = x] = \Pr[X = x|E]$. The min-entropy of a random variable $X$ is defined to be $-\log_2 \max_{x \in \mathbf{supp}(X)} \Pr[X = x]$.

**Definition 1** (Statistical Distance)**.** *Let $X, Y \in S$ be random variables. The* statistical distance *between $X$ and $Y$ is defined by*

$$\Delta(X;Y) := \frac{1}{2}\sum_{a \in S} |\Pr[X = a] - \Pr[Y = a]|$$

*or equivalently,*

$$\Delta(X;Y) := \max_{A \subseteq S} |\Pr[X \in S] - \Pr[Y \in S]|.$$

*We shorthand the statement $\Delta(X;Y) \leq \varepsilon$ by $X \approx_\varepsilon Y$ and we sometimes write this as $X$ is $\varepsilon$-close to $Y$.*

For any random variables $A, B, C$, and event $E$, we shorthand $\Delta(A, C; B, C)$ by $\Delta(A; B\,|C)$, and $\Delta(A|_E; B|_E)$ by $\Delta(A; B\,|E)$ i.e.,

$$\Delta(A; B\,|C) = \Delta(A, C; B, C)\ ,$$

and

$$\Delta\left(A;B\,|E\right)=\Delta\left(A|_E;B|_E\right)\ .$$

The following lemma is immediate from the definitions and triangle inequality.

**Lemma 1.** *Let $A,B,C$ be random variables such that $A,B\in S$ and $\mathbf{supp}(C)=T$ with $T=T_1\cup T_2, T_1\cap T_2=\emptyset$. Then:*

1. $\Delta\left(A;B\,|C\right)\leq\sum_{c\in T}\Pr[C=c]\Delta\left(A;B\,|C=c\right)$
2. $\Delta\left(A;B\,|C\right)\leq\Pr[C\in T_1]\Delta\left(A;B\,|C\in T_1\right)+\Pr[C\in T_2]\Delta\left(A;B\,|C\in T_2\right)$

We will need the following standard lemmas.

**Lemma 2** (Lemma 10 of [ADKO15] )**.** *Let $X_1,\ldots,X_m$ be binary random variables and for any non-empty $\tau\subseteq[m]$, $|\Pr[\bigoplus_{i\in\tau}X_i=0]-\frac{1}{2}|\leq\varepsilon$, then $\Delta\left(X_1,\ldots,X_m;U_m\right)\leq\varepsilon\cdot 2^{\frac{m}{2}}$.*

**Lemma 3.** *Let $X,Y$ be random variables. Further let $f_I$ be a family of functions $f$ indexed by set $I$ and let $S$ be a random variable supported on $I$ that is independent of both $X$ and $Y$. Then $f_S$ can be thought of as a randomised function such that $f_S(x)=f_s(x)$ with probability $\Pr[S=s]$.*

*Then it holds that:*

$$\Delta\left(f_S(X);f_S(Y)\right)\leq\Delta\left(X;Y\right).$$

**Lemma 4** (Lemma 4 of [DDV10], Lemma 9 of [ADKO15])**.** *Let $A,B$ be independent random variables and consider a sequence $V_1,\ldots,V_i$ of random variables, where for some function $\phi$, $V_i=\phi_i(C_i)=\phi(V_1,\ldots,V_{i-1},C_i)$ with each $C_i\in\{A,B\}$. Then $A$ and $B$ are independent conditioned on $V_1,\ldots,V_i$. That is, $I(A;B|V_1,\ldots,V_i)=0$.*

**Definition 2.** *Call a sequence of variables $Z_1,\ldots,Z_N$ $(k,\varepsilon)$-biased against linear tests if for any non-empty $\tau\subseteq[N]$ such that $|\tau|\leq k$, $|\Pr[\bigoplus_{i\in\tau}Z_i=0]-\frac{1}{2}|\leq\varepsilon$.*

**Lemma 5** (Theorem 2 of [AGHP90])**.** *Let $N=2^t-1$ and let $k$ be an odd integer. Then it is possible to construct $N$ random variables $Z_i$ with $i\in[N]$ which are $(k,\varepsilon)$-biased against linear tests using a seed of size at most $2\lceil\log(1/\varepsilon)+\log\log N+\log k\rceil+1$ bits.*

## 3.2 Min-entropy

**Definition 3** (Min-entropy)**.** *Given a distribution $X$ over $\mathcal{X}$, the* min-entropy of $X$*, denoted by $H_\infty(X)$, is defined as*

$$H_\infty(X)=-\log\left(\max_{x\in\mathcal{X}}\Pr[X=x]\right).$$

**Definition 4** (Average min-entropy)**.** *Given distributions $X$ and $Z$, the* average min-entropy of $X$ given $Z$*, denoted by $\tilde{H}_\infty(X|Z)$, is defined as*

$$\tilde{H}_\infty(X|Z)=-\log\left(\mathbb{E}_{z\leftarrow Z}\left[\max_{x\in\mathcal{X}}\Pr[X=x|Z=z]\right]\right).$$

**Lemma 6** ([DORS08])**.** *Given arbitrary distributions $X$ and $Z$ such that $|\mathbf{supp}(Z)|\leq 2^\lambda$, we have*

$$\tilde{H}_\infty(X|Z)\geq H_\infty(X,Z)-\lambda\geq H_\infty(X)-\lambda\ .$$

**Lemma 7** ([MW97])**.** *For arbitrary distributions $X$ and $Z$, it holds that*

$$\Pr_{z\leftarrow Z}[H_\infty(X|Z=z)\geq\tilde{H}_\infty(X|Z)-s]\geq 1-2^{-s}.$$

**Definition 5** ($(n,k)$-sources)**.** *We say that a random variable $X$ is an* $(n,k)$-source *if $\mathbf{supp}(X)\subseteq\{0,1\}^n$ and $H_\infty(X)\geq k$. Additionally, we say that $X$ is a* flat $(n,k)$-source *if for any $a\in\mathbf{supp}(X)$, $\Pr[X=a]=2^{-k}$, i.e., $X$ is uniform over its support.*

$X\sim(n,k)$ denotes the fact that $X$ is an $(n,k)$-source. Further, we call $X$ $(n,k)$-flat if $X\sim(n,k)$ and is flat. We say that $X$ is $\varepsilon$-close to a flat distribution if there exists a set $S$ such that $X\approx_\varepsilon U_S$.

**Definition 6** ($\varepsilon$-smooth min-entropy)**.** *A random variable $X$ is said to have $\varepsilon$-smooth min-entropy at least $k$ if there exists $Y$ such that $\Delta\left(X;Y\right)\leq\varepsilon$, and*

$$H_\infty(Y)\geq k\ .$$

### 3.3 Extractors

**Definition 7** ((Strong) Two-Source Extractor)**.** *Call $E : \{0,1\}^{n_1} \times \{0,1\}^{n_2} \to \{0,1\}^m$ a* two-source extractor *for input lengths $n_1, n_2$, min-entropy $k_1, k_2$, output length $m$, and error $\varepsilon$ if for any two independent sources $X, Y$ with $X \sim (n_1, k_1)$, $Y \sim (n_2, k_2)$, the following holds:*

$$\Delta\left(E(X,Y); U_m\right) \leq \varepsilon$$

*If $n_2 = k_2$, we call such an extractor* seeded*. We use $E : [(n_1, k_1), (n_2, k_2) \mapsto m \sim \varepsilon]$ to denote the fact that $E$ is such an extractor.*

*Additionally, we call the extractor $E$* right strong*, if:*

$$\Delta\left(E(X,Y); U_m \,|Y\right) \leq \varepsilon\ ,$$

*and we call the extractor $E$* left strong*, if:*

$$\Delta\left(E(X,Y); U_m \,|X\right) \leq \varepsilon\ .$$

*We call an extractor $E$* strong *if it is both left strong and right strong. The extractor is said to be $\varepsilon_{Collision}$-collision resistant if $\Pr_{X,Y}[E(X,Y) = E(f(X), Y)] \leq \varepsilon_{Collision}$*

**Definition 8** (Two Source Non-malleable Extractor)**.** *Call $E : [(n_1, k_1), (n_2, k_2) \mapsto m \sim \varepsilon]$ a* two source non-malleable extractor *if additionally for any pair of functions $f : \{0,1\}^{n_1} \to \{0,1\}^{n_1}$, $g : \{0,1\}^{n_2} \to \{0,1\}^{n_2}$ such at least one of $f, g$ is fixed-point-free[11], the following holds:*

$$\Delta\left(E(X,Y); U_m \,|E(f(X), g(Y))\right) \leq \varepsilon$$

*Additionally, we call the extractor $E$ a* right strong non-malleable two-source extractor *if:*

$$\Delta\left(E(X,Y); U_m \,|E(f(X), g(Y)), Y\right) \leq \varepsilon\ ,$$

*and we call the extractor $E$ a* left strong non-malleable two-source extractor *if:*

$$\Delta\left(E(X,Y); U_m \,|E(f(X), g(Y)), X\right) \leq \varepsilon\ ,$$

One useful thing to note is that the extractor remains non-malleable even if the functions $f, g$ are randomised with shared coins (independent of $X$ and $Y$).

**Lemma 8.** *Let $E$ be a two source non-malleable extractor for $(n,k)$-sources $X, Y$ with output length $m$ and error $\varepsilon$. Let $f_S, g_S$ random functions over the shared randomness of $S$ independent of $X$ and $Y$ such that for all $s \in \mathbf{supp}(S)$, at at least one of $f_s$ or $g_s$ is fixed-point-free. Then*

$$\Delta\left(E(X,Y); U_m \,|E(f_S(X), g_S(Y))\right) \leq \varepsilon$$

**Lemma 9.** *If $\mathtt{ext} : [(n,k), (d,d) \mapsto m \sim \varepsilon]$ is a strong seeded extractor, then for any $X, W$ such that $\mathbf{supp}(X) \subseteq \{0,1\}^n$ and $\tilde{H}_\infty(X|W) \geq k + \log(1/\eta)$ with $\eta > 0$, it holds that:*

$$\Delta\left(\mathtt{ext}(X, U_d); U_m \,|U_d, W\right) \leq \varepsilon + \eta$$

We will need the following constructions of extractors.

**Lemma 10** (Theorem 6.9 of [Li19b])**.** *There exists a constant $0 < \gamma < 1$ and an explicit two-source non-malleable extractor $\mathbf{Li} : [(n, (1-\gamma)n), (n, (1-\gamma)n) \mapsto \Omega(n) \sim \varepsilon_L]$ such that $\varepsilon_L = 2^{-\Omega(n \frac{\log\log n}{\log n})}$.*

**Lemma 11** (Theorem 2 of [RRV99])**.** *For every $n, k$ there exists an explicit strong seeded extractor $\mathbf{Tre} : [(n,k), (d,d) \mapsto \Omega(k) \sim \varepsilon]$ such that $d = O(\log^2(n)\log(1/\varepsilon))$.*

**Lemma 12** (Theorem 1 of [Raz05])**.** *For any $n_1, n_2, k_1, k_2, m$ and any $0 < \delta < \frac{1}{2}$ such that:*

1. *$k_1 \geq 5\log(n_2 - k_2)$*
2. *$n_2 \geq 6\log n_2 + 2\log n_1$,*
3. *$k_2 \geq (\frac{1}{2} + \delta) \cdot n_2 + 3\log n_2 + \log n_1$,*
4. *$m = \Omega(\min\{n_2, k_1\})$,*

*there exists a strong two-source extractor $\mathbf{Raz} : [(n_1, k_1), (n_2, k_2) \mapsto m \sim \varepsilon]$, such that $\varepsilon = 2^{-\frac{3m}{2}}$.*

[11] A function $f$ is said to be fixed-point-free if for any $x$, $f(x) \neq x$

# 4 A Generic Construction of a Two-Source Non-Malleable Extractor

In this section we present a generic construction that transforms a non-malleable two-source extractor $\mathbf{E}$ into another non-malleable two-source extractor with a much smaller entropy rate requirement via a two-source extractor.

**Theorem 1.** *For any integers $n_1, n_2, n_3, n_4, k_1, k_2, k_3, k_4, m$ and $\delta_{\mathbf{E}}, \delta_{\mathbf{C}}, \varepsilon_{Collision} > 0$, $n_4 < n_1$, given an efficient construction of*

- *a strong non-malleable extractor $\mathbf{E} : [(n_1, k_1), (n_2, k_2) \mapsto m \sim \delta_{\mathbf{E}}]$,*
- *a right strong two-source extractor $\mathbf{C} : [(n_3, k_3), (n_4, k_4) \mapsto n_2 \sim \delta_{\mathbf{C}}]$ that is $\varepsilon_{Collision}$-collision resistant,*

*then for any integers $k_1^*, k_2^*$, $\varepsilon, \tau > 0$ that satisfy the following conditions, there is an efficient construction of a left and right strong non-malleable two-source extractor $\mathbf{2NMExt} : [(n_3, k_1^*), (n_1, k_2^*) \mapsto m \sim \varepsilon]$.*

$$k_1^* \geq k_3 \ ,$$

$$k_2^* \geq \log 1/\tau + \max\left(k_4 + (n_1 - n_4), k_1 + 2n_4\right) \ ,$$

*and*

$$\varepsilon \leq 3\tau + 3\delta_{\mathbf{E}} + 2\delta_{\mathbf{C}} + 2\sqrt{\varepsilon_{Collision}} \ .$$

*Proof.* Our construction is as follows: Given inputs $x \in \{0,1\}^{n_3}$ and $y = y_\ell \circ y_r$, where $y_\ell \in \{0,1\}^{n_4}$, and $y_r \in \{0,1\}^{n_1 - n_4}$ our extractor is defined as:

$$\mathbf{2NMExt}(x, y) := \mathbf{E}(y_\ell \circ y_r, \mathbf{C}(x, y_\ell)) \ . \tag{7}$$

Let $f : \{0,1\}^{n_3} \to \{0,1\}^{n_3}$ and $g : \{0,1\}^{n_1} \to \{0,1\}^{n_1}$. For any $y \in \{0,1\}^{n_1}$, by $g(y)_\ell$ we denote the $n_4$ bit prefix of $g(y)$. We assume that $f$ does not have any fixed points. The proof for the case when $g$ does not having any fixed points is similar (in fact, simpler) as we explain later.

**Right strongness.** We first prove that our non-malleable extractor is right strong.

**Claim 1.** *Let $\widetilde{Y}$ be a random variable with min-entropy $k_2^* - \log 1/\tau$ and is independent of $X$. Consider the randomized function $T_{f,g}$ that given $a, b, c$, samples $\mathbf{C}(f(X), c)$ conditioned on $\mathbf{C}(X, b) = a$, i.e.,*

$$T_{f,g} : a, b, c \mapsto \mathbf{C}(f(X), c)_{|\mathbf{C}(X,b)=a} \ .$$

*Then:*

$$\Delta\left(\begin{array}{ccc|c} \mathbf{C}(X, \widetilde{Y}_\ell) & ; & U_d & \widetilde{Y}_r \\ \mathbf{E}(\widetilde{Y}_\ell \circ \widetilde{Y}_r, \mathbf{C}(X, \widetilde{Y}_\ell)) & & \mathbf{E}(\widetilde{Y}_\ell \circ \widetilde{Y}_r, U_d) & \widetilde{Y}_\ell \\ \mathbf{E}(g(\widetilde{Y}), \mathbf{C}(f(X), g(\widetilde{Y})_\ell)) & & \mathbf{E}(g(\widetilde{Y}), T_{f,g}(U_d, \widetilde{Y}_\ell, g(\widetilde{Y})_\ell)) & g(\widetilde{Y})_\ell \end{array}\right) \leq \delta_{\mathbf{C}} \ . \tag{8}$$

*Proof.* We have that $H_\infty(X) \geq k_1^* \geq k_3$ and $H_\infty(\widetilde{Y}_\ell) \geq k_2^* - \log 1/\tau - |\widetilde{Y}_r| = k_2^* - \log 1/\tau - (n_1 - n_4) \geq k_4$, and $X, \widetilde{Y}_\ell$ are independently distributed. It follows that $\Delta\left(\mathbf{C}(X, \widetilde{Y}_\ell); U_d \middle| \widetilde{Y}_\ell\right) \leq \delta_{\mathbf{C}}$. Then, Lemma 3 implies that

$$\Delta\left(\mathbf{C}(X, \widetilde{Y}_\ell); U_d \middle| \widetilde{Y}_\ell, \widetilde{Y}_r, g(\widetilde{Y})_\ell\right) \leq \delta_{\mathbf{C}} \ .$$

Observing that since $\widetilde{Y}_r$ is independent of $\mathbf{C}(f(X), g(\widetilde{Y})_\ell), \mathbf{C}(X, \widetilde{Y}_\ell)$ given $\widetilde{Y}_\ell, g(\widetilde{Y})_\ell$, we have that the tuple $\mathbf{C}(X, \widetilde{Y}_\ell), \widetilde{Y}_\ell, \widetilde{Y}_r, T_{f,g}(\mathbf{C}(X, \widetilde{Y}_\ell), \widetilde{Y}_\ell, g(\widetilde{Y})_\ell)$ is identically distributed as $\mathbf{C}(X, \widetilde{Y}_\ell), \widetilde{Y}_\ell, \widetilde{Y}_r, \mathbf{C}(f(X), g(\widetilde{Y})_\ell)$. Again applying Lemma 3, we get the desired statement. □

Now, let $\mathcal{Y}_0$ be the set of $y$ such that $g(y)_\ell = y_\ell$, and $\mathcal{Y}_1$ be the set of all $y$ such that $g(y)_\ell \neq y_\ell$ (in other words, $\mathcal{Y}_0$ contains all the fixed-points of $g$, and $\mathcal{Y}_1$ is the complement set). Also, let $\mathcal{Y}_{0,0}$ be the set of all $y \in \mathcal{Y}_0$ such that $\Pr[C(X, y_\ell) = C(f(X), y_\ell)] \leq \sqrt{\varepsilon_{Collision}}$, and $\mathcal{Y}_{0,1} = \mathcal{Y}_0 \setminus \mathcal{Y}_{0,0}$.

**Claim 2.** *If $\Pr[Y \in \mathcal{Y}_1] \geq \tau$, then*

$$\Delta\left(\begin{array}{ccc|c} \mathbf{E}(\widetilde{Y}_\ell \circ \widetilde{Y}_r, \mathbf{C}(X, \widetilde{Y}_\ell)) & ; & U_m & \widetilde{Y}_\ell \\ \mathbf{E}(g(\widetilde{Y}), \mathbf{C}(f(X), g(\widetilde{Y})_\ell)), & & \mathbf{E}(g(\widetilde{Y}), \mathbf{C}(f(X), g(\widetilde{Y})_\ell)) & \widetilde{Y}_r \end{array}\right) \leq \delta_{\mathbf{C}} + \delta_{\mathbf{E}} \ , \tag{9}$$

*where $\widetilde{Y} = Y|_{Y \in \mathcal{Y}_1}$.*

*Proof.* Notice that conditioned on $Y$ being in $\mathcal{Y}_1$, $g$ does not have a fixed point. Thus, since $U_{n_2}$ is independent of $\widetilde{Y}_r$ given $\widetilde{Y}_\ell, g(\widetilde{Y})_\ell$, and $H_\infty(U_{n_2}) = n_2 \geq k_2$, $H_\infty(\widetilde{Y}_r|\widetilde{Y}_\ell, g(\widetilde{Y}_r)) \geq k_2^* - \log 1/\tau - 2n_4 \geq k_1$, by the definition of a strong non-malleable extractor, we have that

$$\Delta\left(\begin{array}{c}\mathbf{E}(\widetilde{Y}_\ell \circ \widetilde{Y}_r, U_{n_2}) \\ \mathbf{E}(g(\widetilde{Y}), T_{f,g}(U_{n_2}, \widetilde{Y}_\ell, g(\widetilde{Y})_\ell))\end{array} ; \begin{array}{c}U_m \\ \mathbf{E}(g(\widetilde{Y}), T_{f,g}(U_{n_2}, \widetilde{Y}_\ell, g(\widetilde{Y})_\ell))\end{array} \middle| \begin{array}{c}\widetilde{Y}_\ell \\ \widetilde{Y}_r\end{array}\right) \leq \delta_{\mathbf{E}} .$$

Furthermore, from Claim 1 and Lemma 3, we get that

$$\Delta\left(\begin{array}{c}\mathbf{E}(\widetilde{Y}_\ell \circ \widetilde{Y}_r, U_{n_2}) \\ \mathbf{E}(g(\widetilde{Y}), T_{f,g}(U_{n_2}, \widetilde{Y}_\ell, g(\widetilde{Y})_\ell))\end{array} ; \begin{array}{c}\mathbf{E}(\widetilde{Y}_\ell \circ \widetilde{Y}_r, \mathbf{C}(X, \widetilde{Y}_\ell)) \\ \mathbf{E}(g(\widetilde{Y}), \mathbf{C}(f(X), g(\widetilde{Y})_\ell)\end{array} \middle| \begin{array}{c}\widetilde{Y}_\ell \\ \widetilde{Y}_r\end{array}\right) \leq \delta_{\mathbf{C}} .$$

The desired statement follows from triangle inequality. □

Similarly, we prove the following claim.

**Claim 3.** *If* $\Pr[Y \in \mathcal{Y}_{0,0}] \geq \tau$*, then*

$$\Delta\left(\begin{array}{c}\mathbf{E}(\widetilde{Y}_\ell \circ \widetilde{Y}_r, \mathbf{C}(X, \widetilde{Y}_\ell)) \\ \mathbf{E}(g(\widetilde{Y}), \mathbf{C}(f(X), g(\widetilde{Y})_\ell)),\end{array} ; \begin{array}{c}U_m \\ \mathbf{E}(g(\widetilde{Y}), \mathbf{C}(f(X), g(\widetilde{Y})_\ell))\end{array} \middle| \begin{array}{c}\widetilde{Y}_\ell \\ \widetilde{Y}_r\end{array}\right) \leq \delta_{\mathbf{E}} + 2\delta_{\mathbf{C}} + \sqrt{\varepsilon_{Collision}} , \tag{10}$$

*where* $\widetilde{Y} = Y|_{Y \in \mathcal{Y}_{0,0}}$.

*Proof.* Notice that the probability that $\mathbf{C}(X, \widetilde{Y}) = \mathbf{C}(f(X), g(\widetilde{Y})_\ell)$ is at most $\sqrt{\varepsilon_{Collision}}$. Thus, by Claim 1, the probability that $U_{n_2} = T_{f,g}(U_{n_2}, \widetilde{Y}_\ell, g(\widetilde{Y})_\ell)$ is at most $\sqrt{\varepsilon_{Collision}} + \delta_{\mathbf{C}}$. Also, since $U_{n_2}$ is independent of $\widetilde{Y}_r$ given $\widetilde{Y}_\ell, g(\widetilde{Y})_\ell$, and $H_\infty(U_{n_2}) = n_2 \geq k_2$, $H_\infty(\widetilde{Y}_r|\widetilde{Y}_\ell, g(\widetilde{Y}_r)) \geq k^* - \log 1/\tau - 2n_4 \geq k_2$, by the definition of a strong non-malleable extractor, we have that

$$\Delta\left(\begin{array}{c}\mathbf{E}(\widetilde{Y}_\ell \circ \widetilde{Y}_r, U_{n_2}) \\ \mathbf{E}(g(\widetilde{Y}), T_{f,g}(U_{n_2}, \widetilde{Y}_\ell, g(\widetilde{Y})_\ell))\end{array} ; \begin{array}{c}U_m \\ \mathbf{E}(g(\widetilde{Y}), T_{f,g}(U_{n_2}, \widetilde{Y}_\ell, g(\widetilde{Y})_\ell))\end{array} \middle| \begin{array}{c}\widetilde{Y}_\ell \\ \widetilde{Y}_r\end{array}\right) \leq \delta_{\mathbf{E}} + \delta_{\mathbf{C}} + \sqrt{\varepsilon_{Collision}} .$$

Furthermore, from Claim 1 and Lemma 3, we get that

$$\Delta\left(\begin{array}{c}\mathbf{E}(\widetilde{Y}_\ell \circ \widetilde{Y}_r, U_{n_2}) \\ \mathbf{E}(g(\widetilde{Y}), T_{f,g}(U_{n_2}, \widetilde{Y}_\ell, g(\widetilde{Y})_\ell))\end{array} ; \begin{array}{c}\mathbf{E}(\widetilde{Y}_\ell \circ \widetilde{Y}_r, \mathbf{C}(X, \widetilde{Y}_\ell)) \\ \mathbf{E}(g(\widetilde{Y}), \mathbf{C}(f(X), g(\widetilde{Y})_\ell)\end{array} \middle| \begin{array}{c}\widetilde{Y}_\ell \\ \widetilde{Y}_r\end{array}\right) \leq \delta_{\mathbf{C}} .$$

The desired statement follows from triangle inequality. □

We now show that $Y \in \mathcal{Y}_{0,1}$ with small probability.

**Claim 4.**

$$\Pr[Y \in \mathcal{Y}_{0,1}] \leq \tau + \sqrt{\varepsilon_{Collision}} .$$

*Proof.* If $\Pr[Y \in \mathcal{Y}_0] < \tau$, then the statement trivially holds. So, we assume $\Pr[Y \in \mathcal{Y}_0] \geq \tau$. Let $\widetilde{Y} = Y|_{Y \in \mathcal{Y}_0}$ Then $H_\infty(\widetilde{Y}) \geq k_2^* - \log 1/\tau - (n_1 - n_4) \geq k_4$. Since $\mathbf{C}$ is collision-resistant, we have that

$$\begin{aligned}\varepsilon_{Collision} &\geq \Pr[\mathbf{C}(X, \widetilde{Y}_\ell) = \mathbf{C}(f(X), g(\widetilde{Y})_\ell)] \\ &> \Pr[\widetilde{Y} \in \mathcal{Y}_{0,1}] \cdot \sqrt{\varepsilon_{Collision}} \\ &\geq \Pr[Y \in \mathcal{Y}_{0,1}] \cdot \sqrt{\varepsilon_{Collision}} .\end{aligned}$$

□

We now conclude the proof of right strongness of our non-malleable extractor as follows. We shorthand $\mathbf{2NMExt}(X, Y), Y, \mathbf{2NMExt}(f(X), g(Y))$ by $\phi(X, Y)$, and $U_m, Y, \mathbf{2NMExt}(f(X), g(Y))$ by $\psi(X, Y)$.

$$\begin{aligned}\Delta\left(\phi(X,Y); \psi(X,Y)\right) \leq \Pr[Y \in \mathcal{Y}_{0,1}] &+ \Pr[Y \in \mathcal{Y}_1] \cdot \Delta\left(\phi(X,Y)|_{Y \in \mathcal{Y}_1}; \psi(X,Y)|_{Y \in \mathcal{Y}_1}\right) \\ &+ \Pr[Y \in \mathcal{Y}_{0,0}] \cdot \Delta\left(\phi(X,Y)|_{Y \in \mathcal{Y}_{0,0}}; \psi(X,Y)|_{Y \in \mathcal{Y}_{0,0}}\right)\end{aligned}$$

$$\leq (\tau + \delta_{\mathbf{E}} + \delta_{\mathbf{C}}) + (\tau + 2\delta_{\mathbf{E}} + \delta_{\mathbf{C}} + \sqrt{\varepsilon_{Collision}}) + (\tau + \sqrt{\varepsilon_{Collision}})$$
$$= 3\tau + 3\delta_{\mathbf{E}} + 2\delta_{\mathbf{C}} + 2\sqrt{\varepsilon_{Collision}} \ .$$

Note that we assumed that $f$ does not have fixed points. On the other hand, if $g$ does not have fixed points then a simpler proof works that does not need to partition the domain into $\mathcal{Y}_{0,0}, \mathcal{Y}_{0,1}, \mathcal{Y}_1$. Since the first source for the non-malleable extractor $\mathbf{E}$, we can conclude the statement similar to Claim 2 with $Y$ instead of $\widetilde{Y}$.

**Left strongness.** The proof of left strongness is nearly the same (the statistical distance statements include $X$ instead of $Y_r$), but we include it here for completeness.

**Claim 5.** *Let $\widetilde{Y}$ be a random variable with min-entropy $k^* - \log 1/\tau$ and is independent of $X$. Consider the randomized function $S$ that given $a, b$, samples $X$ conditioned on $\mathbf{C}(X, b) = a$, i.e.,*

$$S : a, b \mapsto X|_{\mathbf{C}(X,b)=a} \ .$$

*Then:*

$$\Delta\left( \begin{array}{c} \mathbf{C}(X, \widetilde{Y}_\ell) \\ X \end{array} ; U_d, S(U_{n_2}\widetilde{Y}_\ell) \middle| \begin{array}{c} \widetilde{Y}_\ell \\ \widetilde{Y}_r \end{array} \right) \leq \delta_{\mathbf{C}} \ . \tag{11}$$

*Proof.* We have that $H_\infty(X) \geq k_1^* \geq k_3$ and $H_\infty(\widetilde{Y}_\ell) \geq k_2^* - \log 1/\tau - |\widetilde{Y}_r| = k_2^* - \log 1/\tau - (n_1 - n_4) \geq k_4$, and $X, \widetilde{Y}_\ell$ are independently distributed. It follows that $\Delta\left(\mathbf{C}(X, \widetilde{Y}_\ell); U_d \middle| \widetilde{Y}_\ell\right) \leq \delta_{\mathbf{C}}$. Then, using Lemma 3 and observing that since $\widetilde{Y}_r$ is independent of $X$ given $\widetilde{Y}_\ell$, we have that $\mathbf{C}(X, \widetilde{Y}_\ell), \widetilde{Y}_\ell, \widetilde{Y}_r, S(\mathbf{C}(X, \widetilde{Y}_\ell), \widetilde{Y}_\ell)$ is identically distributed as $\mathbf{C}(X, \widetilde{Y}_\ell), \widetilde{Y}_\ell, \widetilde{Y}_r, X$, we get the desired statement. □

Now, let $\mathcal{Y}_0$ be the set of $y$ such that $g(y)_\ell = y_\ell$, and $\mathcal{Y}_1$ be the set of all $y$ such that $g(y)_\ell \neq y_\ell$. Also, let $\mathcal{Y}_{0,0}$ be the set of all $y \in \mathcal{Y}_0$ such that $\Pr[C(X, y_\ell) = C(f(X), y_\ell)] \leq \sqrt{\varepsilon_{Collision}}$, and $\mathcal{Y}_{0,1} = \mathcal{Y}_0 \setminus \mathcal{Y}_{0,0}$.

**Claim 6.** *If $\Pr[Y \in \mathcal{Y}_1] \geq \tau$, then*

$$\Delta\left( \mathbf{E}(\widetilde{Y}_\ell \circ \widetilde{Y}_r, \mathbf{C}(X, \widetilde{Y}_\ell)) \ ; \ U_m \middle| \begin{array}{c} \widetilde{Y}_\ell \\ g(\widetilde{Y})_\ell \\ X \\ \mathbf{E}(g(\widetilde{Y}), \mathbf{C}(f(X), g(\widetilde{Y})_\ell)) \end{array} \right) \leq 2\delta_{\mathbf{C}} + \delta_{\mathbf{E}} \ , \tag{12}$$

*where $\widetilde{Y} = Y|_{Y \in \mathcal{Y}_1}$.*

*Proof.* Notice that conditioned on $Y$ being in $\mathcal{Y}_1$, $g$ does not have a fixed point. Thus, since $U_{n_2}$ is independent of $\widetilde{Y}_r$ given $\widetilde{Y}_\ell, g(\widetilde{Y})_\ell$, and $H_\infty(U_{n_2}) = n_2 \geq k_2$, $H_\infty(\widetilde{Y}_r | \widetilde{Y}_\ell, g(\widetilde{Y}_r)) \geq k^* - \log 1/\tau - 2n_4 \geq k_1$, by the definition of a strong non-malleable extractor, we have that

$$\Delta\left( \ \mathbf{E}(\widetilde{Y}_\ell \circ \widetilde{Y}_r, U_{n_2}) \ ; \ U_m \ \middle| U_{n_2}, \mathbf{E}(g(\widetilde{Y}), \mathbf{C}(f(S(U_{n_2}, \widetilde{Y}_\ell)), g(\widetilde{Y})_\ell)), \widetilde{Y}_\ell, g(\widetilde{Y})_\ell \right) \leq \delta_{\mathbf{E}} \ ,$$

Furthermore, by applying Claim 1 and Lemma 3 twice, we get that

$$\Delta\left( \begin{array}{c} U_m, S(U_{n_2}, \widetilde{Y}_\ell) \\ \mathbf{E}(g(\widetilde{Y}), \mathbf{C}(f(S(U_{n_2}, \widetilde{Y}_\ell)), g(\widetilde{Y})_\ell)) \end{array} ; \begin{array}{c} U_m, X \\ \mathbf{E}(g(\widetilde{Y}), \mathbf{C}(f(X), g(\widetilde{Y})_\ell)) \end{array} \middle| \begin{array}{c} \widetilde{Y}_\ell \\ g(\widetilde{Y})_\ell \end{array} \right) \leq \delta_{\mathbf{C}} \ .$$

and

$$\Delta\left( \begin{array}{c} \mathbf{E}(\widetilde{Y}_\ell \circ \widetilde{Y}_r, U_{n_2}), S(U_{n_2}, \widetilde{Y}_\ell) \\ \mathbf{E}(g(\widetilde{Y}), \mathbf{C}(f(S(U_{n_2}, \widetilde{Y}_\ell)), g(\widetilde{Y})_\ell)) \end{array} ; \begin{array}{c} \mathbf{E}(\widetilde{Y}_\ell \circ \widetilde{Y}_r, \mathbf{C}(X, \widetilde{Y}_\ell)), X \\ \mathbf{E}(g(\widetilde{Y}), \mathbf{C}(f(X), g(\widetilde{Y})_\ell)) \end{array} \middle| \begin{array}{c} \widetilde{Y}_\ell \\ g(\widetilde{Y})_\ell \end{array} \right) \leq \delta_{\mathbf{C}} \ .$$

The desired statement follows from triangle inequality. □

Similarly, we prove the following claim.

**Claim 7.** *If* $\Pr[Y \in \mathcal{Y}_{0,0}] \geq \tau$, *then*

$$\Delta\left( \mathbf{E}(\widetilde{Y}_\ell \circ \widetilde{Y}_r, \mathbf{C}(X, \widetilde{Y}_\ell)) \ ; \ U_m \ \middle| \widetilde{Y}_\ell, g(\widetilde{Y})_\ell, X, \mathbf{E}(g(\widetilde{Y}), \mathbf{C}(f(X), g(\widetilde{Y})_\ell)) \right) \leq \delta_{\mathbf{E}} + 3\delta_{\mathbf{C}} + \sqrt{\varepsilon_{Collision}}\,, \tag{13}$$

*where* $\widetilde{Y} = Y|_{Y \in \mathcal{Y}_{0,0}}$.

*Proof.* Notice that the probability that $\mathbf{C}(X, \widetilde{Y}) = \mathbf{C}(f(X), g(\widetilde{Y})_\ell)$ is at most $\sqrt{\varepsilon_{Collision}}$. Thus, by Claim 1, the probability that $U_{n_2} = \mathbf{C}(S(U_{n_2}, \widetilde{Y}_\ell), g(\widetilde{Y})_\ell)$ is at most $\sqrt{\varepsilon_{Collision}} + \delta_{\mathbf{C}}$. Also, since $U_{n_2}$ is independent of $\widetilde{Y}_r$ given $\widetilde{Y}_\ell, g(\widetilde{Y})_\ell$, and $H_\infty(U_{n_2}) = n_2 \geq k_2$, $H_\infty(\widetilde{Y}_r|\widetilde{Y}_\ell, g(\widetilde{Y}_r)) \geq k^* - \log 1/\tau - 2n_4 \geq k_1$, by the definition of a strong non-malleable extractor, we have that

$$\Delta\left( \mathbf{E}(\widetilde{Y}_\ell \circ \widetilde{Y}_r, U_{n_2}) \ ; \ U_m \ \middle| U_{n_2}, \mathbf{E}(g(\widetilde{Y}), \mathbf{C}(f(S(U_{n_2}, \widetilde{Y}_\ell)), g(\widetilde{Y})_\ell)), \widetilde{Y}_\ell, g(\widetilde{Y})_\ell \right) \leq \delta_{\mathbf{E}} + \delta_{\mathbf{C}} + \sqrt{\varepsilon_{Collision}}\,.$$

Furthermore, by applying Claim 1 and Lemma 3 twice, we get that

$$\Delta\left(U_m, S(U_{n_2}, \widetilde{Y}_\ell), \mathbf{E}(g(\widetilde{Y}), \mathbf{C}(f(S(U_{n_2}, \widetilde{Y}_\ell)), g(\widetilde{Y})_\ell)); U_m, X, \mathbf{E}(g(\widetilde{Y}), \mathbf{C}(f(X), g(\widetilde{Y})_\ell)) \,\middle|\, \widetilde{Y}_\ell, g(\widetilde{Y})_\ell \right) \leq \delta_{\mathbf{C}}\,.$$

and

$$\Delta\left( \begin{array}{c} \mathbf{E}(\widetilde{Y}_\ell \circ \widetilde{Y}_r, U_{n_2}), S(U_{n_2}, \widetilde{Y}_\ell) \\ \mathbf{E}(g(\widetilde{Y}), \mathbf{C}(f(S(U_{n_2}, \widetilde{Y}_\ell)), g(\widetilde{Y})_\ell)) \end{array} ; \begin{array}{c|c} \mathbf{E}(\widetilde{Y}_\ell \circ \widetilde{Y}_r, \mathbf{C}(X, \widetilde{Y}_\ell)), X & \widetilde{Y}_\ell \\ \mathbf{E}(g(\widetilde{Y}), \mathbf{C}(f(X), g(\widetilde{Y})_\ell)) & g(\widetilde{Y})_\ell \end{array} \right) \leq \delta_{\mathbf{C}}\,.$$

The desired statement follows from triangle inequality. □

We then conclude the proof of right strongness of our non-malleable extractor exactly as we obtained left strongness. □

# 5 Collision resistance of Extractors

## 5.1 Generic Collision Resistance for Seeded Extractors

**Lemma 13.** *Let* $\mathtt{ext} : [(n,k),(d,d) \mapsto m \sim \varepsilon]$ *be a strong seeded extractor. Then there exists a strong seeded extractor* $\mathbf{crTre} : [(n,k),(d+z,d+z) \mapsto m - 2\log(1/\varepsilon_{Collision}) \sim \varepsilon + \varepsilon_T + \sqrt{\varepsilon_{Collision}}]$ *with collision probability* $\varepsilon_{Collision}$ *and* $z = O(\log(1/\varepsilon_{Collision}) \log^2(\log(1/\varepsilon_{Collision})) \log(1/\varepsilon_T))$.

*Proof.* We will first mention [RRV99]'s construction of **Tre**. The aforementioned construction uses an error correcting code and a weak design, defined respectively as below:

**Lemma 14** (Error Correcting Code, Lemma 35 of [RRV99])**.** *For every* $n \in \mathbb{N}$, *and* $\delta > 0$, *there exists a code* $\mathtt{EC} : \{0,1\}^n \to \{0,1\}^{\hat{n}}$ *where* $\hat{n} = poly(n, 1/\delta)$ *such that for* $x, x' \in \{0,1\}^n$ *with* $x \neq x'$, *it is the case that* $\mathtt{EC}(x)$ *and* $\mathtt{EC}(x')$ *disagree in at least* $(\frac{1}{2} - \delta)\hat{n}$ *positions.*

**Definition 9** (Weak Design, Definition 6 of [RRV99])**.** *A family of sets* $S_1, \ldots, S_m \subseteq [d]$ *is a weak* $(\ell, \rho)$*-design if:*

1. *For all* $i$, $|S_i| = \ell$;
2. *For all* $i$,
$$\sum_{j<i} 2^{|S_i \cap S_j|} \leq \rho \cdot (m-1).$$

In particular, any family of disjoint sets $S_1, \ldots, S_m \subseteq [d]$ with $|S_i| = \ell$ is trivially a weak design as well.

Extractor **Tre** operates in the following way: $X$ is firstly evaluated on an error correcting code $\mathtt{EC}$ to obtain $\hat{X}$. Then viewing seed bits $Z$ as $Z_1 \circ Z_2 \circ \ldots \circ Z_d$, then the $i^{th}$ bit of $\mathbf{Tre}(X, Z)$ is given as the $(Z_{|S_i})^{th}$ bit of $\hat{X}$ where $Z_{|S_i}$ is understood to specify an $\ell$-bit index $Z_{j_1} \circ Z_{j_2} \circ \ldots \circ Z_{j_\ell}$ for $S_i = \{j_1, j_2, \ldots, j_\ell\}$. In short, the output is given as:

$$\mathbf{Tre}(X, Z) = \hat{X}(Z_{|S_1}) \circ \hat{X}(Z_{|S_2}) \circ \cdots \circ \hat{X}(Z_{|S_m}).$$

The modification is to truncate the output of $\texttt{ext}(X,S)$ by $t = \frac{5}{2}\log(1/\varepsilon_{Collision})$ bits, and then treating $Z$ as $\frac{4t}{5}$ blocks of $\ell = O(\log^2(t)\log(1/\varepsilon_T))$ many bits, we concatenate the output with $\frac{4t}{5}$ bits. In short, the output is given as:

$$\mathbf{crTre}(X, S \circ Z)_i = \begin{cases} \texttt{ext}(X,S)_i & ,\text{if } i \leq m-t \\ \hat{X}(Z_{i-(m-t)}) & ,\text{if } i > m-t \end{cases}$$

where $Z_j$ denotes the $j^{th}$ block of $Z$.

To show that **crTre** is indeed a strong extractor, note that $S$ and $Z$ are independent and furthermore by Lemma 6 $\tilde{H}_\infty(X|\texttt{ext}(X,S),S) \geq k - m + t \geq t$. Instantiating **crTre** with a family of disjoint sets, an error correcting code EC with minimum distance $(\frac{1}{2} - \frac{\varepsilon_T}{4m})\hat{n}$ for inputs of min-entropy $(t, \frac{4t}{5})$ and seed length $O(\log(1/\varepsilon_{Collision})\log^2(t)\log(1/\varepsilon_T))$, Lemma 9 implies that:

$$\Delta\left(\texttt{ext}(X,S)\mathbf{Tre}(X,Z); \texttt{ext}(X,S), U_{\Omega(t)} \,|S,Z\right) \leq \varepsilon_T + 2^{-\frac{t}{5}}$$

which in turn yields us:

$$\Delta\left(\texttt{ext}(X,S) \circ \mathbf{Tre}(X,Z); U_{m-O(t)} \,|S,Z\right) \leq \varepsilon + \varepsilon_T + 2^{-\frac{t}{5}} = \varepsilon + \varepsilon_T + \sqrt{\varepsilon_{Collision}}$$

As for the collision probability, note that for any $x$ and fixed-point-free function $f$:

$$\begin{aligned} \Pr[\mathbf{crTre}(x, S\circ Z) = \mathbf{crTre}(f(x), S\circ Z)] &\leq \Pr\left[\forall i, \texttt{EC}(x)(Z_i) = \texttt{EC}(f(x))(Z_i)\right] \\ &\leq \left(\frac{1}{2} + \frac{\varepsilon_T}{4m}\right)^{2\log(1/\varepsilon_{Collision})} \\ &\leq \varepsilon_{Collision} \end{aligned}$$

Since this bound holds for all possible values $x$, it follows that it holds for any random variable $X$ as well. □

An instantiation that will suit our purpose will be to use Trevisan's extractor **Tre** as ext. Then for any $n, k$, we have $\mathbf{crTre} : [(n,k),(d,d) \mapsto \Omega(k) \sim 3\varepsilon_T]$ with $d = O(\log^2(n)\log(1/\varepsilon_T)) + O(\log(1/\varepsilon_T)\log^2(\log(1/\varepsilon_T))\log(1/\varepsilon_T)) = O(\log^2(n)\log^2(1/\varepsilon_T))$ such that $\varepsilon = \varepsilon_T$ andwith collision probability $\varepsilon_{Collision} = (\varepsilon_T)^2 < 2^{-\Omega(k)}$.

## 5.2 Collision Resistance of the Raz Extractor

**Lemma 15.** *For any $n_1, n_2, k_1, k_2, m$ and any $0 < \delta < \frac{1}{2}$ such that:*

1. $k_1 \geq 12\log(n_2 - k_2) + 15$,
2. $n_2 \geq 6\log n_2 + 2\log n_1 + 4$,
3. $k_2 \geq (\frac{1}{2} + \delta)\cdot n_2 + 3\log n_2 + \log n_1 + 4$,
4. $m = \Omega(\min\{n_2, k_1\})$,

*there exists a strong two-source extractor $\mathbf{Raz} : [(n_1,k_1),(n_2,k_2) \mapsto m \sim \varepsilon]$, such that $\varepsilon = 2^{-\frac{3m}{2}}$ with collision probability $2^{-m+1}$.*

*Proof.* We will show that the two-source extractor by Raz satisfies the collision resistant property. We first recap [Raz05]'s construction. Given independent sources $X \sim (n_1,k_1)$ and $Y \sim (n_2,k_2)$, $\mathbf{Raz}(X,Y)$ uses $Y$ as seed (using Lemma 5) to construct $m \cdot 2^{n_2}$ many 0-1 random variables $Z_{(i,X)}(Y)$ with $i \in [m]$ and $x \in \{0,1\}^{n_1}$, where random variables are $(t',\varepsilon)$-biased for $t' \geq t \cdot m$.

The idea is to generate a sequence random variables are $\varepsilon$-biased for tests of size $2tm$, and then the probability of collision can be bounded in a similar manner as the proof that function is a two-source extractor. Define $\gamma_i(X,Y) = (-1)^{Z_{i,X}(Y)}$ and let $f$ be any fixed-point-free function. Furthermore let $t' \geq 2\cdot mt$ for some value of $t$ such that the set of random variables $Z_{(i,x)}(Y)$ are $(t',\varepsilon)$-biased. The idea will be to show that we can leverage the $(t,\varepsilon)$-biasedness to show that with high probability over the choice of $X$, for each $i \in [m]$, the probability of the extractor colliding on the $i^{th}$ bit is close to $1/2$. Then we use the Lemma 2 to argue that overall the probability of colliding on all bits is small.

More formally, define $\gamma_i(X,Y) = \mathbb{E}\left[(-1)^{Z_{i,X}(Y)}\right]$, and let $f$ be any fixed-point free function. We will first bound $|\gamma_i(X,Y)|$.

**Claim 8** (Claim 3.2 in [Raz05])**.** *For any $i \in [m]$, any $r \in [t']$ and any set of distinct values $x_1, \ldots, x_r \in \{0,1\}^{n_1}$:*

$$\sum_{y \in \{0,1\}^{n_2}} \prod_{j=1}^{r} (-1)^{Z_{i,x_j}(y)} \leq 2^{n_2} \cdot \varepsilon$$

*Proof.* Since $Z_{i,x}$ are $(t', \varepsilon)$-biased:

$$\begin{aligned}\sum_{y \in \{0,1\}^{n_2}} (-1)^{Z_{i,x_j}(y)} &= \sum_{y \in \{0,1\}^{n_2}} (-1)^{\bigoplus_j Z_{i,x_j}(y)} = 2^{n_2} \sum_{y \in \{0,1\}^{n_2}} \Pr[U_{n_2} = y](-1)^{\bigoplus_j Z_{i,x_j}(y)} \\ &= 2^{n_2}(-1)^{\bigoplus_j Z_{i,x_j}(U_{n_2})} \leq 2^{n_2} \cdot \varepsilon\end{aligned}$$

□

**Claim 9.** *Letting $Z_{(i,x)}(Y)$ be $(2t, \varepsilon)$-biased, $\Pr[Z_{(i,x)}(Y) = Z_{(i,f(x))}(Y)] = \Pr[Z_{(i,x)}(Y) \oplus Z_{(i,f(x))}(Y) = 0] \leq \frac{1}{2} + \varepsilon'$ where:*

$$\varepsilon' = 2^{(n_2 - k_2)/t} \cdot \left(\varepsilon^{1/t} + (2t) \cdot 2^{-\frac{k_1}{3}}\right)$$

*Proof.* Let $t$ be some even positive integer, then consider $(\gamma(X,Y)\gamma(f(X),Y))^t$. By Jensen's inequality we can bound the term as:

$$\begin{aligned}(\gamma(X,Y)\gamma(f(X),Y))^t &= \left(\frac{1}{2^{k_1+k_2}} \sum_{(x,y) \in \mathbf{supp}(X,Y)} (-1)^{Z_{(i,x)}(y) \oplus Z_{(i,f(x))}(y)}\right)^t \\ &\leq \left(\frac{1}{2^{k_2}}\right) \sum_{y \in \mathbf{supp}(Y)} \left(\frac{1}{2^{k_1}} \sum_{x \in \mathbf{supp}(X)} (-1)^{Z_{(i,x)}(y) \oplus Z_{(i,f(x))}(y)}\right)^t \\ &\leq \left(\frac{1}{2^{k_2}}\right) \sum_{y \in \{0,1\}^{n_2}} \left(\frac{1}{2^{k_1}} \sum_{x \in \mathbf{supp}(X)} (-1)^{Z_{(i,x)}(y) \oplus Z_{(i,f(x))}(y)}\right)^t \\ &= \left(\frac{1}{2^{k_2 + k_1 \cdot t}}\right) \sum_{x_1, \ldots, x_t \in \mathbf{supp}(X)} \sum_{y \in \{0,1\}^{n_2}} \prod_{j=1}^{t} (-1)^{Z_{(i,x_j)}(y) \oplus Z_{(i,f(x_j))}(y)}\end{aligned}$$

Then we partition the summands (based on $x_1, \ldots, x_t$) into two categories: (1) When the values $x_1, \ldots, x_t, f(x_1), \ldots, f(x_t)$ has at least one unique value $x$ that does not otherwise occur in $x_1, \ldots, x_t$ and $f(x_1), \ldots, f(x_t)$ or else (2) when the every value in $x_1, \ldots, x_t, f(x_1), \ldots, f(x_t)$ occurs at least twice.

(1) In the first case, Claim 8 implies the respective summands can be bounded by $2^{n_1} \cdot \varepsilon$ and there are at most $2^{k_1 \cdot t}$ many of these summands. (2) In the latter case, we will bound the sum using the following claim:

**Claim 10.** *If $x_1, \ldots, x_t, f(x_1), \ldots, f(x_t)$ are such that every value occurs at least twice and $f(x_i) \neq x_i$ for all $i \in [t]$, then there exists a subset of indices $S \subseteq [t]$ such that $|S| \leq \frac{2}{3}t$ and $\{x_1, \ldots, x_t\} \subseteq \{x : s \in S\} \cup \{f(x) : s \in S\}$.*

*Proof.* Define $A$ to contain the of values of $x_1, \ldots, x_t$ that occur at least twice within $x_1, \ldots, x_t$. Define $S_A$ be the set of indices of the first occurrence of each value in $A$, and furthermore define $B$ to be $\{x_1, \ldots, x_t\} \backslash \{x_j, f(x_j) : j \in S_A\}$. Then if $|A| = \ell$, $|B| = r \leq t - 2\ell$. Let $B = \{b_1, \ldots, b_r\}$.

Since each $x_1, \ldots, x_t, f(x_1), \ldots, f(x_t)$ has that every value occurs twice, and $b_i$ for any $i \in [r]$ does not occur in $\{x, f(x) : x \in S_A\}$, it implies that $b_1, \ldots, b_r \in B$ must be a fixed-point-free permutation of $f(B_1), \ldots, f(B_r)$. Thus, the permutation $f$ defines a disjoint union of cycles over the set $B$. Define $S_B$ to be the set that for each such cycle includes every alternate element. More precisely, for each such cycle, say $(b_{i_1}, \ldots, b_{i_q})$ with

$$f(b_{i_1}) = b_{i_2}, f(b_{i_2}) = b_{i_3}, \ldots, f(b_{i_{q-1}}) = b_{i_q}, f(b_{i_q}) = b_{i_1} \ ,$$

we include $b_{i_1}, b_{i_3}, \ldots, b_{i_{1+2\lfloor (q-1)/2 \rfloor}}$ in the set $S_B$. Then $S = S_A \cup S_B$ satisfy the desired condition. Also,

$$|S_B| \leq r \max_{q \in \mathbb{N} \setminus \{1\}} \frac{\lceil q/2 \rceil}{q} \leq \frac{2r}{3} \ ,$$

since $\frac{\lceil q/2 \rceil}{q}$ is $1/2$ when $q$ is even, and $(q+1)/2q$ when $n$ is odd, and hence is maximized for $q = 3$. Thus,

$$|S| \leq \ell + \frac{2r}{3} \leq \ell + \frac{2(t-2\ell)}{3} = \frac{2t}{3} - \frac{\ell}{3} \leq \frac{2t}{3} ,$$

as needed. □

To obtain the bound on the number of summands in the case (2), note that there are $\binom{2^{k_1}}{\frac{2}{3}t}$ possible sets $S$, and for each set, there are $\left(\frac{4t}{3}\right)^t$ possible sequences that satisfy Case 2. In each such case, we bound the summand by $2^{n_2}$. Combining the two cases, we get that:

$$\begin{aligned}
(\gamma(X,Y)\gamma(f(X),Y))^t &\leq \left(\frac{1}{2^{k_2+k_1\cdot t}}\right) \sum_{x_1,\ldots,x_t \in \mathbf{supp}(X)} \sum_{y\in\{0,1\}^{n_2}} \prod_{j=1}^{t} (-1)^{Z_{(i,x_j)}(y) \oplus Z_{(i,f(x_j))}(y)} \\
&\leq \left(\frac{1}{2^{k_2+k_1\cdot t}}\right) \left(2^{k_1\cdot t} 2^{n_2}\cdot\varepsilon + 2^{n_2}\binom{2^{k_1}}{\frac{2}{3}t}\left(\frac{4t}{3}\right)^t\right) \\
&\leq \left(\frac{1}{2^{k_2+k_1\cdot t}}\right) \left(2^{k_1\cdot t} 2^{n_2}\cdot\varepsilon + 2^{n_2}(2t)^t\cdot 2^{-\frac{k_1}{3}t}\right) \\
|\gamma(X,Y)\gamma(f(X),Y)| &\leq 2^{(n_2-k_2)/t}\cdot\left(\varepsilon^{1/t} + (2t)\cdot 2^{-\frac{k_1}{3}} .\right)
\end{aligned}$$

□

Now that we have shown that for any coordinate $i \in [m]$, the probability the extractor collides on the $i^{th}$ bit is at most $\frac{1}{2} + \varepsilon'$, we wish to invoke the Lemma 2 to argue that the probability the extractor collides on all the coordinates is small.

Define $\tau \subseteq [m]$, and consider the set of random variables $\left\{\bigoplus_{i\in\tau} Z_{i,x}(Y) \oplus \bigoplus_{i\in\tau} Z_{i,f(x)}(Y) : x \in \{0,1\}^{n_1}\right\}$. Since $|\tau| \leq m$, the set of random variables is $\varepsilon$-biased for linear tests of size up to $\frac{2t'}{m}$, and hence $\bigoplus_{i\in\tau} Z_{i,x}(Y) \oplus \bigoplus_{i\in\tau} Z_{i,f(x)}(Y)$ is $\varepsilon'$-biased by Claim 9. Then by the Lemma 2, since this holds for any $\tau \subseteq [m]$, the sequence $(Z_{1,X}(Y)\oplus Z_{1,f(X)}(Y), \ldots, Z_{m,X}(Y)\oplus Z_{m,f(X)}(Y))$ is $\varepsilon'\cdot 2^{\frac{m}{2}}$-close to $U_m$. It follows that, the probability of collision is at most:

$$2^{-m} + \varepsilon'\cdot 2^{\frac{m}{2}} = 2^{-m} + 2^{\frac{m}{2}}\cdot 2^{(n_2-k_2)/t}\cdot\left(\varepsilon^{1/t} + (2t)\cdot 2^{-\frac{k_1}{3}}\right) .$$

We now bound the probability of collision based on our choice of parameters. Recall that Lemma 5 asserts that we can construct $m\cdot 2^{n_2}$ many variables $Z_{(i,x)}$ that are $(t',\varepsilon)$-biased using $2\lceil \log(1/\varepsilon) + \log\log(m2^{n_2}) + \log(t')\rceil = 2\lceil \log(1/\varepsilon) + \log\log(m2^{n_2}) + \log(2mt)\rceil$ random bits. Set $\varepsilon = 2^{-r}$ where $r = \frac{1}{2}n_2 + 3\log n_2 + \log n_1$, $n_2 \geq 16$ and $k_1 \geq 64$. We then bound the probability separately depending on $k_1$'s value relative to $4(n_2-k_2)$.

**If $k_1 \leq 4(n_2-k_2)$:** Choose $t$ to be the smallest even integer such that $t \geq \frac{8(n_2-k_2)}{k_1}$. Then $t \leq n_2 - k_2$, or else that would imply that $k_1 \leq 8$. Then it follows that:

$$\frac{8(n_2-k_2)}{k_1} \leq t \leq \frac{16(n_2-k_2)}{k_1} \leq \frac{8n_2}{k_1}$$

Using the inequality above:

$$\begin{aligned}
2^{(n_2-k_2)/t}\cdot\left(\varepsilon^{1/t} + (2t)\cdot 2^{-\frac{k_1}{3}}\right) &\leq 2^{(n_2-k_2-r)/t} + \frac{32(n_2-k_2)}{k_1}2^{-\frac{k_1}{3}} \leq 2^{-\delta n_2/t} + \frac{32(n_2-k_2)}{k_1}2^{-\frac{k_1}{3}} \\
&\leq 2^{-\delta n_2/t} + 2^{-\frac{k_1}{3}+\frac{k_1}{12}} \leq 2^{-\delta\frac{k_1}{8}} + 2^{-\frac{k_1}{4}} \leq 2^{-\delta\frac{k_1}{8}+1}
\end{aligned}$$

**Otherwise, if $k_1 > 4(n_2-k_2)$:** Set $t = 2$. Then:

$$\begin{aligned}
2^{(n_2-k_2)/2}\cdot\left(\varepsilon^{1/2} + 4\cdot 2^{-\frac{k_1}{3}}\right) &= 2^{(n_2-k_2-r)/2} + 2^{(n_2-k_2)/2}\cdot 4\cdot 2^{-\frac{k_1}{3}} \\
&\leq 2^{-\delta n_2/2} + 2^{(n_2-k_2)/2}\cdot 4\cdot 2^{-\frac{k_1}{3}} \\
&\leq 2^{-\delta n_2/2} + 2^{-\frac{k_1}{8}}
\end{aligned}$$

Choosing $m \leq \delta\min\{\frac{n_2}{4}, \frac{k_1}{16}\} - 1$, we get that the collision probability is at most $2^{-m} + 2^{\frac{m}{2}-2m-1} \leq 2^{-m+1}$. □

# 6 A Fully Non-malleable Seeded Extractor

In this section, we will use **crTre** as **C** and **Li** as **E** with the following instantiations:

1. **crTre** is an extractor given by $[(n_x, k_x), (s, s) \mapsto d \sim \varepsilon_T]$ for $s = O(\log^2(n_x)\log^2(1/\varepsilon_T)$, and $d = \Omega(k_x)$, with collision probability $\left(\frac{\varepsilon_T}{3}\right)^2$.
2. **Li** is an extractor given by $[(d, (1-\gamma)d), (d, (1-\gamma)d) \mapsto m \sim \varepsilon_L]$ for some constant $\gamma$, $m = \Omega(d)$, and $\varepsilon_L = 2^{-d\left(\frac{\log\log d}{\log d}\right)}$.

with $\varepsilon_{Collision} = 2^{-(k_x)^c}$ for some $c < \frac{1}{2}$. It follows that $s = o(d)$.

**Theorem 2.** *For any $n_x, k_x$, there exists a fully non-malleable seeded extractor* $\mathbf{FNMExt} : [(n_x, k_x), (s+d, s+d) \mapsto m \sim \varepsilon_{fnm}]$ *with $m = \Omega(k_x)$, $d < k_x$, $s = O(\log^2(n_x)\log^2(\varepsilon_T))$, $\varepsilon_{fnm} < 10\varepsilon_T$ with $\varepsilon_T = 2^{-(\frac{k_x}{2})^c}$ for some $c < \frac{1}{2}$.*

*Proof.* It suffices to show that for our choice of parameters, the entropy requirements of **crTre** and **Li** are met.

Setting input parameters $n_3 = n_x$, $k_1^* = k_x$, $n_4 = k_4 = s$, $k_2^* = s + d$, and extractor parameters $n_1 = n_2 = d$, $k_1 = k_2 = (1-\gamma)d$, $k_3 = k_x$, note that indeed $k_1^* \geq k_3$. Furthermore,

$$k_2^* = s + d = s + k_4 + n_1 - n_4$$
$$k_2^* = d + s \geq \left(\frac{\gamma}{2}\right)d + (1-\gamma)d + 2s$$

And thus by our choice of $s$, $\varepsilon_{fnm} \leq 3 \cdot 2^{-(\frac{k_x}{2})^{2c}} + 7\varepsilon_T < 10\varepsilon_T$ with $\varepsilon_T = 2^{-(\frac{k_x}{2})^c}$ for some $c < \frac{1}{2}$. □

It will also be useful in the subsequent subsection that we relax the entropy requirement of this extractor.

**Theorem 3.** *For any $n_x, k_x$, there exists a fully non-malleable seeded extractor* $\mathbf{FNMExt} : [(n_x, k_x), (s+d, s+d-1) \mapsto m \sim \varepsilon_{fnm}]$ *with $m = \Omega(k_x)$, $d < k_x$, $s = O(\log^2(n_x)\log^2(\varepsilon_T))$, $\varepsilon_{fnm} < 12\varepsilon_T$ with $\varepsilon_T = 2^{-(\frac{k_x}{2})^c}$ for some $c < \frac{1}{2}$.*

*Proof.* By Lemma 19 and Lemma 20, **crTre** can also be viewed as $\mathbf{crTre} : [(n_x, k_x), (s, s-1) \mapsto \Omega(k_x) \sim 2\varepsilon_T]$ with collision probability $2\varepsilon_{Collision} = 2\left(\frac{\varepsilon_T}{3}\right)^2 \leq \varepsilon_T^2$.

For a similar choice of parameters: $n_3 = n_x$, $k_1^* = k_x$, $n_4 = s$, $k_4 = s - 1$ $k_2^* = s + d$, and extractor parameters $n_1 = n_2 = d$, $k_1 = k_2 = (1-\gamma)d$, $k_3 = k_x$, note that indeed $k_1^* \geq k_3$. Furthermore,

$$k_2^* = s + d - 1 = s + s - 1 + d - s = s + k_4 + n_1 - n_4$$
$$k_2^* = s + d - 1 \geq \left(\frac{\gamma}{2}\right)d + (1-\gamma)d + 2s - 1$$

And thus by our choice of $s$, $\varepsilon_{fnm} \leq 3 \cdot 2^{-(\frac{k_x}{2})^{2c}} + 9\varepsilon_T < 12\varepsilon_T$ with $\varepsilon_T = 2^{-(\frac{k_x}{2})^c}$ for some $c < \frac{1}{2}$. □

# 7 A Two-Source Non-malleable Extractor

In this section, we will use **Raz** as **C** and **FNMExt** as **E** from Theorem 3 with the following instantiations:

1. $\mathbf{Raz} : [(n_x, k_x), (n_\ell, k_\ell) \mapsto d \sim 2^{-(1.5)d}]$ with $d = \Omega(\min\{k_x, k_\ell\})$ and collision probability $2^{-d+1}$.
2. $\mathbf{FNMExt} : [(n_y, \tau \cdot d), (d, d-1) \mapsto m \sim \varepsilon_{fnm}]$ is a two-source non-malleable extractor for some $0 < \tau < 1$, $m = \Omega(d)$, and $\varepsilon_{fnm} < 12 \cdot \varepsilon_T$ with $\varepsilon_T < 2^{-\Omega((m)^c)}$ for some $c < \frac{1}{2}$.

**Theorem 4.** *There exists a two source non-malleable seeded extractor* $\mathbf{2NMExt} : [(n_x, k_x), (n_y, k_y) \mapsto m \sim \varepsilon_{tnm}]$, *and $m = \Omega(\min\{n_y, k_x\})$, such that:*

1. $k_x \geq 12\log(n_y - k_y) + 15$,
2. $n_y \geq 30\log(n_y) + 10\log(n_x) + 20$,
3. $k_y \geq (\frac{4}{5} + \gamma)n_y + 3\log(n_y) + \log(n_x) + 4$,

*4.* $\varepsilon_{tnm} \leq 3 \cdot 2^{-\frac{9\gamma}{10} n_y} + 40 \cdot \varepsilon_T$ *where* $\varepsilon_T = 2^{-\Omega(d^c)}$ *with* $c < \frac{1}{2}$.

*Proof.* For any given $Y \sim (n_y, k_y)$, we treat it as $Y = Y_\ell \circ Y_r$ where $|Y_\ell| = n_\ell$ and $|Y_r| = n_r$.

The extractor $\mathbf{Raz} : [(n_x, k_x), (n_\ell, k_\ell) \mapsto d \sim 2^{-(1.5)d}]$ from Lemma 15 requires the following conditions:

1. $k_x \geq 12 \log(n_\ell - k_\ell) + 15$
2. $n_\ell \geq 6 \log n_\ell + 2 \log n_x + 4$,
3. $k_\ell \geq (\frac{1}{2} + \gamma) \cdot n_\ell + 3 \log n_\ell + \log n_x + 4$,
4. $d \leq \gamma \min\{\frac{n_\ell}{4}, \frac{k_x}{16}\} - 1$

for some $0 < \gamma < \frac{1}{2}$.

Setting $n_\ell = (\frac{2}{5} - \gamma) n_y$ (and consequently $n_r = (\frac{3}{5} + \gamma) n_y$), we first show that indeed the input requirements for **Raz** are met. Note that

$$(n_y - k_y) - (n_\ell - k_\ell) = n_y - k_y - (n_\ell - (k_y - n_r)) = 0$$

which implies that:

$$k_x \geq 12 \log(n_y - k_y) + 15 = 12 \log(n_\ell - k_\ell) + 15$$

Next:

$$n_\ell \geq \frac{1}{5} n_y \geq 6 \log(n_y) + 2 \log(n_x) + 4 \geq 6 \log(n_\ell) + 2 \log(n_x) + 4$$

And lastly:

$$\begin{aligned} k_\ell \geq k_y - n_r &= (\frac{4}{5} + \gamma) n_y + 3 \log(n_\ell) + \log(n_x) + 4 - (\frac{3}{5} + \gamma) n_y \\ &= (\frac{1}{5}) n_y + 3 \log(n_\ell) + \log(n_x) + 4 \\ &= (\frac{1}{5})(\frac{1}{0.4 - \gamma}) n_\ell + 3 \log(n_\ell) + \log(n_x) + 4 \\ &\geq (\frac{1}{2} + \frac{5\gamma}{4}) n_\ell + 3 \log(n_\ell) + \log(n_x) + 4 \end{aligned}$$

Setting input parameters $n_3 = n_x$, $k_1^* = k_x$, $n_1 = n_y$, $k_2^* = (\frac{4}{5} + \gamma) n_y$, and extractor parameters $n_4 = n_\ell$, $k_4 = k_\ell$, $n_1 = n_y$, $k_1 = \tau \cdot d$, $n_2 = d$, $k_2 = d - 1$ for some $0 < \tau < 1$, we get that $k_1^* \geq k_3$. Furthermore:

$$\begin{aligned} k_2^* - k_4 - n_1 + n_4 &= k_y - k_\ell - n_y + n_\ell \\ &= k_y - k_\ell - (\frac{3}{4} + \gamma) n_y \\ &\geq \left(\frac{1}{5} + \gamma\right) n_y - \left(\frac{1}{2} + \gamma\right)\left(\frac{2}{5} - \gamma\right) n_y \\ &= \left(\frac{11}{10}\gamma + \gamma^2\right) n_y \end{aligned}$$

and:

$$k_2^* - k_1 - 2n_4 = k_2^* - \tau \cdot d - 2n_\ell \geq \gamma n_y - \tau\gamma \frac{n_\ell}{4} \geq \frac{9\gamma}{10} n_y$$

Thus, by Theorem 1 it follows that $\mathbf{2NMExt} : [(n_3, k_1^*), (n_1, k_2^*) \mapsto m \sim \varepsilon_{tnm}]$ is a strong non-malleable extractor with error:

$$\begin{aligned} \varepsilon_{tnm} &\leq 3 \cdot 2^{-\frac{9\gamma}{10} n_y} + 36 \cdot \varepsilon_T + 2 \cdot 2^{-\frac{3}{2} d} + 2\sqrt{2^{-d+1}} \\ &\leq 3 \cdot 2^{-\frac{9\gamma}{10} n_y} + 40 \cdot \varepsilon_T \end{aligned}$$

where $\varepsilon_T = 2^{-\Omega(d^c)}$ with $c < \frac{1}{2}$. □

# 8 A Two-Source Non-malleable Extractor With Rate $\frac{1}{2}$

In this section we make use of **2NMExt** from the previous section to obtain a strong two-source unbalanced non-malleable extractor with rate $\frac{1}{2}$.

**Lemma 16** (Theorem 5 of [AKO+21])**.** *If* $\mathbf{2NMExt} : [(n_1, k_1), (n_2, k_2) \mapsto d \sim \varepsilon_1]$ *is a strong two-source unbalanced non-malleable extractor, with* $n_2 = o(n_1)$ *and* $\mathtt{ext} : [(n_1, k_1), (d, d) \mapsto \ell \sim \varepsilon_2]$ *is a strong seeded extractor, then there exists a two source non-malleable extractor* $\mathbf{2NMExt}^* : [(n_1, k_1), (n_2, k_2) \mapsto \ell \sim \varepsilon_1 + \varepsilon_2]$*. Furthermore, if* $k_1, \ell < \frac{n_1}{2}$*, then* $\mathbf{2NMExt}^*$ *has a rate of* $\frac{1}{2}$*.*

**Theorem 5.** *There exists an extractor* $\mathbf{2NMExt}^* : [(n_1, k_1), (n_2, k_2) \mapsto \ell \sim \varepsilon_1 + \varepsilon_2]$ *such that:*

1. $k_1 \geq \max\{12\log(n_2 - k_2) + 15, \log^3(n_1)\log(1/\varepsilon_2)\}$
2. $n_2 \geq \max\{30\log(n_2) + 10\log(n_1) + 20, \log^3(n_1)\log(1/\varepsilon_2)\}$
3. $k_2 \geq (\frac{4}{5} + \gamma)n_2 + 3\log(n_2) + \log(n_1) + 4$
4. $\varepsilon_1 \leq 3 \cdot 2^{-\frac{9\gamma}{10}n_2} + 40 \cdot \varepsilon_T$ *where* $\varepsilon_T = 2^{-\Omega(d^c)}$ *with* $c < \frac{1}{2}$
5. $\ell < \frac{k_1}{2}$

*Furthermore, if* $n_2 = o(n_1)$*,* $k_1, \ell < \frac{n_1}{2}$*, then* $\mathbf{2NMExt}^*$ *has a rate of* $\frac{1}{2}$*.*

*Proof.* By Theorem 4 there exists an extractor $\mathbf{2NMExt} : [(n_1, k_1), (n_2, k_2) \mapsto m \sim \varepsilon_1]$ such that:

1. $k_1 \geq 12\log(n_2 - k_2) + 15$
2. $n_2 \geq 30\log(n_2) + 10\log(n_1) + 20$
3. $k_2 \geq (\frac{4}{5} + \gamma)n_2 + 3\log(n_2) + \log(n_1) + 4$
4. $\varepsilon_1 \leq 3 \cdot 2^{-\frac{9\gamma}{10}n_2} + 40 \cdot \varepsilon_T$ where $\varepsilon_T = 2^{-\Omega(d^c)}$ with $c < \frac{1}{2}$
5. $m = \Omega(\min\{n_2, k_1\})$

Using Lemma 11, $\mathbf{Tre} : [(n_1, k_1), (m, m) \mapsto \Omega(k_1) \sim \varepsilon_2]$ is a strong seeded extractor with $m = O(\log^2(n_1)\log(1/\varepsilon_2))$. Thus by Lemma 16 there exists a two source non-malleable extractor $\mathbf{2NMExt}^* : [(n_1, k_1), (n_2, k_2) \mapsto \Omega(k_1) \sim \varepsilon_1 + \varepsilon_2]$.

Furthermore, with $n_2 = o(n_1)$ and $k_1, \ell < \frac{n_1}{2}$, we get that $\mathbf{2NMExt}^*$ has a rate of at most $\frac{n_1}{2(n_1+n_2)} < \frac{1}{2}$. □

# References


[ADKO15] Divesh Aggarwal, Yevgeniy Dodis, Tomasz Kazana, and Maciej Obremski. Non-malleable reductions and applications. In *Proceedings of the Forty-Seventh Annual ACM Symposium on Theory of Computing*, STOC '15, page 459–468, New York, NY, USA, 2015. Association for Computing Machinery.

[ADL18] Divesh Aggarwal, Yevgeniy Dodis, and Shachar Lovett. Non-malleable codes from additive combinatorics. *SIAM Journal on Computing*, 47(2):524–546, 2018.

[ADN+19] Divesh Aggarwal, Ivan Damgård, Jesper Buus Nielsen, Maciej Obremski, Erick Purwanto, Joao Ribeiro, and Mark Simkin. Stronger leakage-resilient and non-malleable secret sharing schemes for general access structures. In *Annual International Cryptology Conference*, pages 510–539. Springer, 2019.

[AGHP90] N. Alon, O. Goldreich, J. Hastad, and R. Peralta. Simple construction of almost k-wise independent random variables. In *Proceedings [1990] 31st Annual Symposium on Foundations of Computer Science*, pages 544–553 vol.2, 1990.

[AHL16] Divesh Aggarwal, Kaave Hosseini, and Shachar Lovett. Affine-malleable extractors, spectrum doubling, and application to privacy amplification. In *2016 IEEE International Symposium on Information Theory (ISIT)*, pages 2913–2917. Ieee, 2016.

[AKO+21] Divesh Aggarwal, Bhavana Kanukurthi, Sai Lakshmi Bhavana Obbattu, Maciej Obremski, and Sruthi Sekar. Rate one-third non-malleable codes. Cryptology ePrint Archive, Report 2021/1042, 2021.

[AO20] Divesh Aggarwal and Maciej Obremski. A constant rate non-malleable code in the split-state model. In *2020 IEEE 61st Annual Symposium on Foundations of Computer Science (FOCS)*, pages 1285–1294. IEEE, 2020.

[AOR+20] Divesh Aggarwal, Maciej Obremski, João Ribeiro, Mark Simkin, and Luisa Siniscalchi. Privacy amplification with tamperable memory via non-malleable two-source extractors. Cryptology ePrint Archive, Report 2020/1371, 2020.

[BCD+18] Avraham Ben-Aroya, Eshan Chattopadhyay, Dean Doron, Xin Li, and Amnon Ta-Shma. A new approach for constructing low-error, two-source extractors. In *Proceedings of the 33rd Computational Complexity Conference*, CCC '18, pages 3:1–3:19, Germany, 2018. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik.

[BDT17] 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 *Proceedings of the 49th Annual ACM SIGACT Symposium on Theory of Computing*, STOC 2017, page 1185–1194, New York, NY, USA, 2017. Association for Computing Machinery.

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

[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.

[CG17] Mahdi Cheraghchi and Venkatesan Guruswami. Non-malleable coding against bit-wise and split-state tampering. *Journal of Cryptology*, 30(1):191–241, Jan 2017.

[CGL16] Eshan Chattopadhyay, Vipul Goyal, and Xin Li. Non-malleable extractors and codes, with their many tampered extensions. In *Proceedings of the forty-eighth annual ACM symposium on Theory of Computing*, pages 285–298. ACM, 2016.

[Coh17] Gil Cohen. Towards optimal two-source extractors and Ramsey graphs. In *Proceedings of the 49th Annual ACM SIGACT Symposium on Theory of Computing*, STOC 2017, pages 1157–1170, New York, NY, USA, 2017. ACM.

[CZ19] Eshan Chattopadhyay and David Zuckerman. Explicit two-source extractors and resilient functions. *Annals of Mathematics*, 189(3):653–705, 2019.

[DDV10] Francesco Davì, Stefan Dziembowski, and Daniele Venturi. Leakage-resilient storage. In Juan A. Garay and Roberto De Prisco, editors, *Security and Cryptography for Networks*, pages 121–137, Berlin, Heidelberg, 2010. Springer Berlin Heidelberg.

[DKK+12] Yevgeniy Dodis, Bhavana Kanukurthi, Jonathan Katz, Leonid Reyzin, and Adam Smith. Robust fuzzy extractors and authenticated key agreement from close secrets. *IEEE Transactions on Information Theory*, 2012.

[DKO13] Stefan Dziembowski, Tomasz Kazana, and Maciej Obremski. Non-malleable codes from two-source extractors. In *Annual Cryptology Conference*, pages 239–257. Springer, 2013.

[DORS08] Yevgeniy Dodis, Rafail Ostrovsky, Leonid Reyzin, and Adam Smith. Fuzzy extractors: How to generate strong keys from biometrics and other noisy data. *SIAM Journal on Computing*, 38(1):97–139, 2008.

[DPW18] Stefan Dziembowski, Krzysztof Pietrzak, and Daniel Wichs. Non-malleable codes. *J. ACM*, 65(4), April 2018.

[DW09] Yevgeniy Dodis and Daniel Wichs. Non-malleable extractors and symmetric key cryptography from weak secrets. In *Proceedings of the Forty-first Annual ACM Symposium on Theory of Computing*, STOC '09, pages 601–610, New York, NY, USA, 2009. ACM.

[GK18] Vipul Goyal and Ashutosh Kumar. Non-malleable secret sharing. In *Proceedings of the 50th Annual ACM SIGACT Symposium on Theory of Computing*, STOC 2018, page 685–698, New York, NY, USA, 2018. Association for Computing Machinery.

[GSZ21] Vipul Goyal, Akshayaram Srinivasan, and Chenzhi Zhu. Multi-source non-malleable extractors and applications. In *Eurocrypt*, 2021.

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

[JKS93] Thomas Johansson, Gregory Kabatianskii, and Ben J. M. Smeets. On the relation between a-codes and codes correcting independent errors. In *Advances in Cryptology - EUROCRYPT '93, Workshop on the Theory and Application of of Cryptographic Techniques, Lofthus, Norway, May 23-27, 1993, Proceedings*, pages 1–11, 1993.

[Lew19] Mark Lewko. An explicit two-source extractor with min-entropy rate near 4/9. *Mathematika*, 65(4):950–957, 2019.

[Li12] Xin Li. Non-malleable extractors, two-source extractors and privacy amplification. In *2012 IEEE 53rd Annual Symposium on Foundations of Computer Science*, pages 688–697. IEEE, 2012.

[Li16] Xin Li. Improved two-source extractors, and affine extractors for polylogarithmic entropy. In *2016 IEEE 57th Annual Symposium on Foundations of Computer Science (FOCS)*, pages 168–177, Oct 2016.

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

[Li19a] Xin Li. Non-malleable extractors and non-malleable codes: Partially optimal constructions. In *34th Computational Complexity Conference (CCC 2019)*. Schloss Dagstuhl-Leibniz-Zentrum fuer Informatik, 2019.

[Li19b] Xin Li. Non-malleable extractors and non-malleable codes: Partially optimal constructions. In *Proceedings of the 34th Computational Complexity Conference*, CCC '19, Dagstuhl, DEU, 2019. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik.

[MW97] Ueli Maurer and Stefan Wolf. Privacy amplification secure against active adversaries. In Burton S. Kaliski, editor, *Advances in Cryptology — CRYPTO '97*, pages 307–321, Berlin, Heidelberg, 1997. Springer Berlin Heidelberg.

[OS18] Maciej Obremski and Maciej Skórski. Inverted leftover hash lemma. ISIT, 2018.

[Raz05] Ran Raz. Extractors with weak random seeds. In *Proceedings of the Thirty-seventh Annual ACM Symposium on Theory of Computing*, STOC '05, pages 11–20, New York, NY, USA, 2005. ACM.

[RRV99] Ran Raz, Omer Reingold, and Salil Vadhan. Extracting all the randomness and reducing the error in trevisan's extractors. In *Proceedings of the Thirty-First Annual ACM Symposium on Theory of Computing*, STOC '99, page 149–158, New York, NY, USA, 1999. Association for Computing Machinery.

# A Privacy Amplification against Memory Tampering Active Adversaries.

Below two definitions are taken verbatim from [AOR+20].

**Definition 10** (Protocol against memory-tampering active adversaries)**.** *An* $(r, \ell_1, k_1, \ell_2, k_2, m)$-protocol against memory-tampering active adversaries *is a protocol between Alice and Bob, with a man-in-the-middle Eve, that proceeds in* $r$ *rounds. Initially, we assume that Alice and Bob have access to random variables* $(W, A)$ *and* $(W, B)$*, respectively, where* $W$ *is an* $(\ell_1, k_1)$*-source (the* secret*), and* $A$*,* $B$ *are* $(\ell_2, k_2)$*-sources (the* randomness tapes*) independent of each other and of* $W$*. The protocol proceeds as follows:*

*In the first stage, Eve submits an arbitrary function $F : \{0,1\}^{\ell_1} \times \{0,1\}^{\ell_2} \to \{0,1\}^{\ell_1} \times \{0,1\}^{\ell_2}$ and chooses one of Alice and Bob to be corrupted, so that either $(W, A)$ is replaced by $F(W, A)$ (if Alice is chosen), or $(W, B)$ is replaced by $F(W, B)$ (if Bob is chosen).*

*In the second stage, Alice and Bob exchange messages $(C_1, C_2, \ldots, C_r)$ over a non-authenticated channel, with Alice sending the odd-numbered messages and Bob the even-numbered messages, and Eve is allowed to replace each message $C_i$ by $C'_i$ based on $(C_1, C'_1, \ldots, C_{i-1}, C'_{i-1}, C_i)$ and independent random coins, so that the recipient of the $i$-th message observes $C'_i$. Messages $C_i$ sent by Alice are deterministic functions of $(W, A)$ and $(C'_2, C'_4, \ldots, C'_{i-1})$, and messages $C_i$ sent by Bob are deterministic functions of $(W, B)$ and $(C'_1, C'_3, \ldots, C'_{i-1})$.*

*In the third stage, Alice outputs $S_A \in \{0,1\}^m \cup \{\perp\}$ as a deterministic function of $(W, A)$ and $(C'_2, C'_4, \ldots)$, and Bob outputs $S_B \in \{0,1\}^m \cup \{\perp\}$ as a deterministic function of $(W, B)$ and $(C'_2, C'_4, \ldots)$.*

**Definition 11** (Privacy amplification protocol against memory-tampering active adversaries)**.** *An $(r, \ell_1, k_1, \ell_2, k_2, m, \varepsilon, \delta)$-privacy amplification protocol against memory-tampering active adversaries is an $(r, \ell_1, k_1, \ell_2, k_2, m)$-protocol against memory-tampering active adversaries with the following additional properties:*

- **If Eve is passive:** *In this case, $F$ is the identity function and Eve only wiretaps. Then, $S_A = S_B \neq \perp$ with $S_A$ satisfying*
$$S_A, C \approx_\varepsilon U_m, C, \tag{14}$$
*where $C = (C_1, C'_1, C_2, C'_2, \ldots, C_r, C'_r)$ denotes Eve's view.*
- **If Eve is active:** *Then, with probability at least $1 - \delta$ either $S_A = \perp$ or $S_B = \perp$ (i.e., one of Alice and Bob detects tampering), or $S_A = S_B \neq \perp$ with $S_A$ satisfying (14).*

One building block of our extension is MAC:

**Definition 12.** *A family of functions $\mathtt{MAC} : \{0,1\}^\gamma \times \{0,1\}^\tau \to \{0,1\}^\delta, \mathtt{Verify} : \{0,1\}^\gamma \times \{0,1\}^\delta \times \{0,1\}^\tau \to \{0,1\}$ is said to be a $\mu-$secure one time message authentication code if*

1. *For $k_a \in_R \{0,1\}^\tau$, $\forall\, m \in \{0,1\}^\gamma$, $\Pr[\mathtt{Verify}(m, \mathtt{MAC}_{k_a}(m), k_a) = 1] = 1$,*
*where for any $(m, t)$, $\mathtt{Verify}(m, t, k_a) := \begin{cases} 1 \text{ if } \mathtt{MAC}(m, k_a) = t \\ 0 \text{ otherwise} \end{cases}$*
2. *For any $m \neq m', t, t'$, $\Pr_{k_a}[\mathtt{MAC}(m, k_a) = t | \mathtt{MAC}(m', k_a) = t'] \leq \mu$, where $k_a \in_R \{0,1\}^\tau$.*

**Lemma 17.** *[JKS93, DKK+12] For any $\gamma, \varepsilon > 0$ there is an efficient $\varepsilon-$secure one time $\mathtt{MAC}$ with $\delta \leq (\log(\gamma) + \log(\frac{1}{\varepsilon}))$, $\tau \leq 2\delta$, where $\tau, \gamma, \delta$ are key, message, tag length respectively.*

Let us analyse the protocol described in Figure 2 (we copy the figure below). Let **2NMExt** be a $[(\ell_1, k_1 - 2\ell_2 - 2\gamma - 1), (2 \cdot \ell_2, \ell_2 - \gamma - 1) \mapsto 4\alpha \sim \epsilon]$ strong non-malleable extractor for some parameter $\gamma > 0$. Let shared secret $W \in \{0,1\}^{\ell_1}$ have min-entropy $k_1$, let $A_1, A_2, B_1, B2 \in \{0,1\}^{\ell_2}$ be uniform random variables. If Eve is passive the security is straight forward thus we will only consider the case of active Eve. We will follow the original proof [AOR+20] very closely. Let us focus on the case where Alice is the one with corrupted memory $F(W, (A_1, A_2)) = \tilde{W}, (\tilde{A}_1, \tilde{A}_2)$. Since randomness $(\tilde{A}_1, \tilde{A}_2)$ is controlled by the adversary we can simply reveal $(\tilde{a}_1, \tilde{a}_2) = (\tilde{A}_1, \tilde{A}_2)$ it along with original randomness $(a_1, a_2) = (A_1, A_2)$, this makes $\tilde{W}$ only a function of $W$, let's denote it as $\tilde{W} = f(W)$, moreover let us denote $B'_1 = g(B_1)$. As in the original paper we define $\mathcal{L} = \{w : f(w) = w\}$ and $\mathcal{R} = \{b_1 : g(b) = b\}$.

In the proof of Theorem 6 in [AOR+20] in point (2.b) authors prove that if $\Pr(W \notin \mathcal{L} \vee B_1 \notin \mathcal{R} \vee a_1 = \tilde{a}_1) > 2^{-\gamma}$ then $\Pr(S_B \neq \perp \mid W \notin \mathcal{L} \vee B_1 \notin \mathcal{R}) < \epsilon + 2^{-\alpha}$, thus Bob will abort.

The only case left to analyse is the point (2.a) where $W \in \mathcal{L} \wedge B_1 \in \mathcal{R} \wedge a_1 = \tilde{a}_1$. We assume that $\Pr(W \in \mathcal{L} \wedge B_1 \in \mathcal{R} \wedge a_1 = \tilde{a}_1) > 2^{-\gamma}$ (else this case happens with negligible probability). Authors argue that $W$ has enough entropy and thus $R_A$ is $\epsilon$ close to uniform. If $[R_A]'_\alpha = [R_A]_\alpha$ and $[R_B]'_{\alpha:2\alpha} = [R_B]_{\alpha:2\alpha}$, then $S^1_A \circ S^2_A = S^1_B \circ S^2_B \neq \perp$ and $S^1_A \circ S^2_A$ is $\epsilon$ close to uniform given Eve's view. Now we know that $S^1_A \circ S^2_A = S^1_B \circ S^2_B \neq \perp$ and $\tilde{W} = W$ so we can follow with the analysis of the extension: First of all the $\tilde{H}_\infty(W | A_1, A_2, \tilde{A}_1, \tilde{A}_2, W \in \mathcal{L}) > k_1 - 2\ell_2 - \gamma$ (where $|A_i| = \ell$, and $\gamma$ penalty comes from probability of the event $W \in \mathcal{L}$). Now notice that by the security of MAC either $\Pr((A_2 \neq A'_2 \vee B_2 \neq B'_2) \wedge$ neither Alice or Bob Aborts$) < 2 \cdot 2^{-\Omega(\alpha)}$.

| Alice | | Bob |
|---|---|---|
| Memory: $(W, A_1, A_2)$ | | Memory: $(W, B_1, B_2)$ |
| | $A_1 \longrightarrow A'_1$ | |
| | $B'_1 \longleftarrow B_1$ | |
| $R_A = \mathbf{2NMExt}(A_1 \circ B'_1, W)$ | | $R_B = \mathbf{2NMExt}(A'_1 \circ B_1, W)$ |
| | $[R_A]_\alpha \longrightarrow [R_A]'_\alpha$ | |
| | $[R_B]'_{\alpha\cdot 2\alpha} \longleftarrow [R_B]_{\alpha:2\alpha}$ | |
| If $[R_A]_{\alpha\cdot 2\alpha} = [R_B]'_{\alpha:2\alpha}$ then $S^1_A = [R_A]_{2\alpha:3\alpha}$ and $S^2_A = [R_A]_{3\alpha:4\alpha}$ | | If $[R_B]_\alpha = [R_A]'_\alpha$ then $S^1_B = [R_B]_{2\alpha:3\alpha}$ and $S^2_B = [R_B]_{3\alpha:4\alpha}$ |
| Otherwise Abort | | Otherwise Abort |
| | If the parties did not Abort we know that $S^1_A = S^1_B$ and $S^2_A = S^2_B$, and we know that $W$ has not been tampered with | |
| $\sigma_A = \mathtt{MAC}(A_2, S^1_A)$ | $A_2, \sigma_A \longrightarrow A'_2, \sigma'_A$ | $\mathtt{Verify}(A'_2, \sigma'_A, S^1_B)$ |
| $\mathtt{Verify}(B'_2, \sigma'_B, S^2_A)$ | $B'_2, \sigma'_B \longleftarrow B_2, \sigma_B$ | $\sigma_B = \mathtt{MAC}(B_2, S^2_B)$ |
| If verify successful | | If verify successful |
| Output: | | Output: |
| $\mathtt{SExt}(W, A_2 + B'_2)$ | | $\mathtt{SExt}(W, A'_2 + B_2)$ |
| Else Abort | | Else Abort |

Further observe that even if Eve controls $A_2$, and $A_2$ has no entropy and it might depend on $W$, still $B_2$ is uniform and independent of $(A_2)$. Thus $A_2 + B_2$ is uniform[12] and independent of $W$. Now we have uniform independent seed, all we have to do is extract:

Let $\mathtt{SExt} : \{0,1\}^{\ell_1} \times \{0,1\}^{\ell_2} \to \{0,1\}^{0.999\cdot(k_1 - 2\ell_2 - \gamma)}$ is a strong seeded extractor[13] with the error $2^{-\Omega(\ell_2)}$. Since $W$ has enough entropy $\mathtt{SExt}(W, A_2 + B_2)$ is $2^{-\Omega(\ell_2)}$ close to uniform given the view of Eve. The analysis for Eve corrupting Bob is symmetrical. Thus we obtain the following:

**Theorem 6.** *Let* **2NMExt** *be a* $[(\ell_1, k_1 - 2\ell_2 - 2\gamma - 1), (2\cdot\ell_2, \ell_2 - \gamma - 1) \mapsto 4\alpha \sim \epsilon]$ *strong non-malleable extractor. Then, there exists an* $(r = 6, \ell_1, k_1, 2\cdot\ell_2, 2\cdot\ell_2, 0.999\cdot(k_1 - 2\ell - \gamma), 2^{-\Omega(\ell_2)}, \delta = \varepsilon + 2^{-\alpha} + 2\cdot 2^{-\gamma} + 2^{-\Omega(\alpha)})$*-privacy amplification protocol against memory-tampering active adversaries.*

And thus when we plug in our extractor and some example parameters we get:

**Corollary 1.** *For shared secret* $W$ *with* $|W| = n$ *and* $H_\infty(W) > 0.803\cdot n$ *and* $|A_i| = |B_i| = 0.001n$ *we get privacy amplification protocol that outputs* $0.8\cdot n$ *uniform bits, and has a security* $2^{-\Omega(\sqrt{n})}$.

# B Rejection Sampling for Extractors

In this section we present two lemmas that use rejection sampling to lower the entropy requirement for strong two-source extractors and their collision probabilities.

We first define a sampling algorithm $\mathtt{samp}$ that given $Y \sim (n, k - \delta)$, tries to approximate some distribution $Y' \sim (n, k)$. Letting $d = \max_y \left\{ \frac{\Pr[Y'=y]}{\Pr[Y=y]} \right\}$:

$$\mathtt{samp}(y) = \begin{cases} y, & w.p.\ \frac{\Pr[Y'=y]}{d\Pr[Y=y]} \\ \perp, & else \end{cases}$$

**Lemma 18.** *The probability* $\mathtt{samp}(Y') = y$ *is* $\frac{\Pr[Y'=y]}{d}$ *and furthermore, the probability that* $\mathtt{samp}(Y') \neq \perp$ *is* $\frac{1}{d}$. *Consequently, the distribution* $\mathtt{samp}(Y')$ *conditioned on the event that* $\mathtt{samp}(Y') \neq \perp$ *is identical to* $Y$.

[12] Technically speaking Eve can abort protocol by tampering with $A_2$ or $B_2$, Alice and Bob will simply abort. However $A_2$ and $B_2$ are no longer fully uniform conditioned on the event that Eve let them through. This is not a problem, by Lemma 19, this only doubles extraction epsilons.

[13] Constant 0.999 is just a placeholder for any constant less then 1. By [GUV09] we know that such explicit extractor exists.

*Proof.* Letting $\texttt{samp}$ and $d$ be defined as above, then:

$$\Pr[\texttt{samp}(Y) = y] = \frac{1}{d}\frac{\Pr[Y' = y]}{\Pr[Y = y]} \cdot \Pr[Y = y] = \frac{\Pr[Y' = y]}{d}$$

Then it follows that:

$$\Pr[\texttt{samp}(Y) \neq \perp] = \sum_y \Pr[\texttt{samp}(Y') = y] = \sum_y \frac{\Pr[Y' = y]}{d} = \frac{1}{d}$$

Thus, conditioned on the event that $\texttt{samp}(Y) \neq \perp$, $\texttt{samp}(Y)$ is the distribution $Y'$.

$$\Pr[\texttt{samp}(Y) = y | \texttt{samp}(Y) \neq \perp] = \frac{\Pr[\texttt{samp}(Y) \neq \perp | \texttt{samp}(Y) = y]\Pr[\texttt{samp}(Y) = y]}{\Pr[\texttt{samp}(Y) \neq \perp]} = \Pr[Y' = y]$$

□

## B.1 Lowering the Entropy Requirement for Strong Two-Source Extractors

**Lemma 19.** *Let* $\texttt{ext} : [(n_1, k_1), (n_2, k_2) \mapsto m \sim \varepsilon]$ *be a strong two-source extractor using input distributions* $X$ *and* $Y'$*. Then letting* $Y \sim (n_2, k_2 - \delta)$*:*

$$\Delta\left(\texttt{ext}(X, Y); U_m \,|Y\right) \leq 2^\delta \varepsilon$$

*Proof.* Assume by contradiction that $\Delta\left(\texttt{ext}(X, Y); U_m \,|Y\right) > 2^\delta \varepsilon$. Then there exists a distinguisher $A : \{0,1\}^m \to \{0,1\}$ such that $|\Pr[A(\texttt{ext}(X, Y), Y) = 1] - \Pr[A(U_m, Y) = 1]| > 2^\delta \varepsilon$.

The idea is to use $A$ along with Lemma 18 to build a distinguisher $D$ that distinguishes between $\texttt{ext}(X, Y')$ and $U_m$ with probability greater than $\varepsilon$ when given $Y'$. Define $D$ as follows:

$$D(Z, Y') = \begin{cases} A(Z, Y') & , \text{ if } \texttt{samp}(Y') \neq \perp \\ 1 & w.p.\ \frac{1}{2}, \text{ if } \texttt{samp}(Y') = \perp \\ 0 & else \end{cases}$$

Note that by Lemma 18, $\Pr[\texttt{samp}(Y') \neq \perp] \geq \frac{1}{2^\delta}$ and $\texttt{samp}(Y')$ is identical to $Y$ conditioned on the event that $\texttt{samp}(Y') = \perp$. Then the advantage that $D$ distinguishes between $\texttt{ext}(X, Y')$ and $U_m$ given $Y'$ is given as:

$$\begin{aligned} |\Pr[D(\texttt{ext}(X, Y'), Y') = 1] - \Pr[D(U_m, Y') = 1]| &= \Pr[\texttt{samp}(Y) \neq \perp] |\Pr[A(\texttt{ext}(X, Y), Y) = 1] - \Pr[A(U_m, Y) = 1]| \\ &> \frac{1}{2^\delta} 2^\delta \varepsilon = \varepsilon \end{aligned}$$

Which in turn implies that $\Delta\left(\texttt{ext}(X, Y'); U_m \,|Y'\right) > \varepsilon$, which implies the desired contradiction. □

## B.2 Lowering the Entropy Requirement for Collision Resistance in Extractors

**Lemma 20.** *Let* $\texttt{ext} : [(n_1, k_1), (n_2, k_2) \mapsto m \sim \varepsilon]$ *be a strong two-source extractor using input distributions* $X$ *and* $Y$ *that has collision probability* $\varepsilon_{Collision}$*. Then letting* $Y' \sim (n_2, k_2 - \delta)$ *and* $f$ *be any fixed-point-free function:*

$$\Pr[\texttt{ext}(X, Y') = \texttt{ext}(f(X), Y')] \leq 2^\delta \varepsilon_{Collision}$$

*Proof.* By the collision resilience property of $\texttt{ext}$, it follows that:

$$\begin{aligned} \varepsilon_{Collision} &\geq \Pr[\texttt{ext}(X, Y) = \texttt{ext}(f(X), Y)] \\ &\geq \Pr[\texttt{ext}(X, Y) = \texttt{ext}(f(X), Y) | \texttt{samp}(Y) \neq \perp] \Pr[\texttt{samp}(Y) \neq \perp] \\ &= \Pr[\texttt{ext}(X, Y') = \texttt{ext}(f(X), Y')] 2^{-\delta} \end{aligned}$$

□

ECCC ISSN 1433-8092
https://eccc.weizmann.ac.il