Privacy Amplification with Tamperable Memory via Non-malleable Two-source Extractors

Divesh Aggarwal∗  Maciej Obremski†  João Ribeiro‡  Mark Simkin§  Luisa Siniscalchi¶

Abstract

We extend the classical problem of privacy amplification to a setting where the active adversary, Eve, is also allowed to fully corrupt the internal memory (which includes the shared randomness, and local randomness tape) of one of the honest parties, Alice and Bob, before the execution of the protocol. We require that either one of Alice or Bob detects tampering, or they agree on a shared key that is indistinguishable from the uniform distribution to Eve.

We obtain the following results:

(1) We give a privacy amplification protocol via low-error non-malleable two-source extractors with one source having low min-entropy. In particular, this implies the existence of such (non-efficient) protocols;

(2) We show that even slight improvements to the state-of-the-art explicit non-malleable two-source extractors would lead to explicit low-error, low min-entropy two-source extractors, thereby resolving a long-standing open question. This suggests that obtaining (information-theoretically secure) explicit non-malleable two-source extractors for (1) might be hard;

(3) We present explicit constructions of low-error, low min-entropy non-malleable two-source extractors in the CRS model of (Garg, Kalai, Khurana, Eurocrypt 2020), assuming either the quasi-polynomial hardness of DDH or the existence of nearly-optimal collision-resistant hash functions;

(4) We instantiate our privacy amplification protocol with the above mentioned non-malleable two-source extractors in the CRS model, leading to explicit, computationally-secure protocols. This is not immediate from (1) because in the computational setting we need to make sure that, in particular, all randomness sources remain samplable throughout the proof. This requires upgrading the assumption of quasi-polynomial hardness of DDH to sub-exponential hardness of DDH.

We emphasize that each of the first three results can be read independently.

∗National University of Singapore. dcsdiva@nus.edu.sg
†National University of Singapore.obremski.math@gmail.com
‡Imperial College London. j.lourenco-ribeiro17@imperial.ac.uk
§Aarhus University. simkin@cs.au.dk
¶Concordium Blockchain Research Center, Aarhus University. lsiniscalchi@cs.au.dk
1 Introduction

Privacy amplification. The setting of privacy amplification is fundamental in cryptography, and it has deep connections to randomness extractors. Strong seeded extractors yield non-interactive privacy amplification protocols against a passive eavesdropper [BBR88, BBCM95], while strong seeded non-malleable extractors were introduced by Dodis and Wichs [DW09] to obtain 2-round privacy amplification protocols against active adversaries, a setting originally introduced in [MW97]. This has led to a deep line of work constructing explicit seeded non-malleable extractors (and hence such privacy amplification protocols) with significantly improved parameters (see [Li19] and references therein).

Privacy amplification resilient against memory-tampering active adversaries. We introduce a natural extension of privacy amplification against active adversaries where the active adversary also has memory-tampering capabilities. Remarkably, we show that non-malleable two-source extractors (even without efficient preimage sampling) can be used to design privacy amplification protocols in this stronger adversarial setting.

More precisely, we extend the classical problem of Maurer and Wolf [MW97] to a setting where the active adversary, Eve, is also allowed to fully corrupt the internal memory of one of the honest parties, Alice and Bob, before the execution of the protocol. Informally, in an 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 tapes $A$ and $B$, respectively, which may also be weak sources. We say $(W, A)$ (resp. $(W, B)$) is Alice’s memory (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, say, Alice is chosen, then Alice’s memory $(W, A)$ is replaced by $(\tilde{W}, \tilde{A}) = F(W, A)$. Eve does not learn the output of $F$, and Alice and Bob do not know whether (or which) memory was corrupted. Crucially, note that the secret $W$ and the randomness tape are tampered together, which means that the corrupted secret and tape may be arbitrarily correlated. Finally, Alice and Bob run some interactive protocol where Eve is allowed to tamper all messages between the honest parties. The goal of the privacy amplification protocol is twofold:

1. Eve is passive: If Eve does not tamper neither of Alice’s or Bob’s memories nor does she tamper any of the messages between them, then Alice and Bob must agree on a shared key that is (statistically or computationally) indistinguishable from the uniform distribution to Eve.

2. Eve is active: In this case, with high probability either one of Alice or Bob detects tampering, or they agree on a shared key that is indistinguishable from the uniform distribution to Eve.

We show that low-error non-malleable two-source extractors with sufficiently low min-entropy requirement on one of the sources yield 4-round privacy amplification protocols resilient against memory-tampering active adversaries with good parameters.

Non-malleable two-source extractors. A natural strengthening of two-source extractors are non-malleable two-source extractors (also known as seedless non-malleable extractors). Non-malleable two-source extractors were introduced by Cheraghchi and Guruswami [CG17] in the single-tampering setting and by Chattopadhyay, Goyal, and Li [CGL16] in the multi-tampering setting. Roughly speaking, a function $\text{nmExt} : \{0,1\}^n \times \{0,1\}^n \rightarrow \{0,1\}^m$ 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 on several inputs correlated with the original sources. In other words, we require that
\[
nmExt(X, Y), nmExt(f_1(X), g_1(Y)), \ldots, nmExt(f_r(X), g_r(Y)) \\
\approx \varepsilon U_m, nmExt(f_1(X), g_1(Y)), \ldots, nmExt(f_r(X), g_r(Y)),
\]
where \(X\) and \(Y\) are independent sources with enough min-entropy, \(f_i, g_i : \{0, 1\}^n \rightarrow \{0, 1\}^n\) for \(i = 1, \ldots, r\) are arbitrary tampering functions such that \((f_i, g_i)\) has no fixed points, \(U_m\) is uniform over \(\{0, 1\}^m\) and independent of the rest, and \(\approx \varepsilon\) means the two distributions are \(\varepsilon\)-close in statistical distance (for small \(\varepsilon\)).

The state-of-the-art construction of a non-malleable two-source extractor by Li [Li19] requires min-entropy \((1 – poly(1/r))n\) to handle \(r\) tamperings. In particular, if \(r\) is constant, then the existing explicit non-malleable extractors require min-entropy \((1 - \gamma)n\) for a small constant \(\gamma > 0\). On the other hand, the probabilistic method shows that there exist non-malleable two-source extractors for min-entropy \(\delta n\), with \(\delta > 0\) an arbitrarily small constant, handling \(n^{\Omega(1)}\) tamperings with error \(2^{-\Omega(n)}\) and output length \(\Omega(n)\) [CGGL20].

As stated above, any low-error non-malleable two-source extractor with sufficiently low min-entropy requirement yields a privacy amplification protocol in our setting. Moreover, our protocol is efficient if the underlying extractor is efficient. We explain below why explicitly constructing such objects might be challenging.

**Implications of improved non-malleable two-source extractors.** We prove that small improvements to the parameters of [CGL16, Li17, Li19] lead to explicit low-error two-source extractors for min-entropy \(\delta n\) with a small constant \(\delta > 0\).

The problem of constructing explicit low-error two-source extractors for low min-entropy sources was an important focus of research in pseudorandomness over more than 30 years, with fundamental connections to combinatorics and many applications in computer science. The first non-trivial explicit 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 \(\gamma n\), 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 incompressible 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. Recently, an improved analysis by Lewko [Lew19] showed that Bourgain’s extractor can handle sources with min-entropy \(4n/9\). In another groundbreaking work, Chattopadhyay and Zuckerman [CZ19] succeeded in constructing explicit 1-bit two-source extractors for polylogarithmic min-entropy with polynomially small error (this was quickly improved to larger output length [Li16] and near-logarithmic min-entropy [BDT17, Coh17, Li17], with the state-of-the-art currently found in [Li19]). In spite of all this progress, we are still far from resolving the question of finding an explicit construction of a low-error two-source extractor for polylogarithmic min-entropy.

Our result shows that the constructions of [CGL16, Li17, Li19] are almost the best we can hope for without solving the above mentioned long standing open question.
Constructions of non-malleable two-source extractors in the CRS model. We consider the Common Reference String (CRS) model introduced by Garg, Kalai, and Khurana [GKK20]. At a high-level, in this model a CRS is sampled once and for all, and we consider three adversaries with full access to the CRS: The first adversary (the sampler) samples independent randomness sources with enough min-entropy, the second adversary (the tamperer) is allowed to tamper with the source samples, and the third adversary (the distinguisher) attempts to distinguish the output of the extractor from a uniform distribution given also access to the extractor’s outputs on tampered versions.

We present two explicit constructions of non-malleable two-source extractors in the CRS model with significantly improved parameters. Assuming the quasi-polynomial hardness of the DDH assumption,\(^1\) we construct a low-error non-malleable two-source extractor in the CRS model for much lower min-entropy and handling many more tamperings than its best statistical counterparts [CGL16, Li17, Li19], against a computationally bounded distinguisher. This construction achieves essentially the same parameters as the extractor from [GKK20], which only handles one-sided tampering, under the same hardness assumption. While the previous construction requires a bounded distinguisher, we also give a simple low-error non-malleable two-source extractor in the CRS model for very low min-entropy against a computationally unbounded distinguisher, assuming the existence of nearly optimal collision-resistant hash functions.

We can exploit our explicit constructions of non-malleable two-source extractors in the CRS model to obtain explicit 4-round privacy amplification protocols resilient against memory-tampering active adversaries in the CRS model with very good parameters. We remark that this task is not trivial in the CRS model, because the shared secret \(W\) and randomness tapes \(A\) and \(B\) are arbitrarily correlated with the CRS, and Eve also has full knowledge of the CRS at all times. Moreover, care is needed in this computational setting because we need to ensure that sources remain samplable by appropriately sized circuits even after some conditionings.

1.1 Comparison to previous work

Privacy amplification. The setting of fuzzy privacy amplification, which is very loosely related (see discussion below) to our notion of privacy amplification with tamperable memory, has also received significant attention. Here, the secrets of Alice and Bob are not necessarily equal, but may only be close in some metric. Fuzzy extractors [DORS08] yield non-interactive fuzzy privacy amplification protocols, effectively showing that information reconciliation and regular privacy amplification can be accomplished together in a single round. When the adversary is active, robust fuzzy extractors can be used to obtain such fuzzy privacy amplification protocols [BDK+05, CDF+08, DKK+12]. Similar problems have been studied in the computational setting [DHP+18, EJOR20].

Privacy amplification with tamperable memory is harder than regular privacy amplification against a passive or active adversary, and is incomparable to fuzzy privacy amplification. In our setting, there is no guarantee that the secrets held by Alice and Bob are close according to some distance after tampering, and, unlike other privacy amplification settings, the tampered secret may even be correlated with the party’s randomness. On the other hand, in fuzzy privacy amplification one requires that privacy be achieved even when Alice’s and Bob’s secrets are different (but close enough), provided the adversary remains passive during the protocol. In our setting, we must allow the parties to abort if either Alice’s or Bob’s memory is tampered, as the task is impossible otherwise.

\(^1\)By quasi-polynomial hardness of the DDH assumption we mean no algorithm running in time \(n^{\log n}\) solves the Decisional Diffie-Hellman problem with non-negligible (in \(n\)) advantage.
Computational extractors. Early work by Trevisan and Vadhan [TV00] can be interpreted as giving explicit extractors for a single source with logarithmic min-entropy in the CRS model (a similar remark was already made in [DRV12]). Under strong hardness assumptions, they also construct explicit deterministic extractors for high min-entropy sources samplable by bounded-size circuits. However, they prove the strong negative result that, for both settings above, the running time of the extractor must be larger than the time needed to sample the source. In particular, if one wishes to extract randomness from all efficiently samplable sources in the CRS model, then the extractor in question cannot be efficient. Dodis, Ristenpart, and Vadhan [DRV12] implicitly show that this negative result can be avoided if one instead focuses on single-source condensers in the CRS model, assuming the existence of nearly optimal collision-resistant hash functions. Computational seeded extractors were also studied by Dachman-Soled, Gennaro, Krawczyk, and Malkin [DGKM12], who considered the standard approach of composing an information-theoretic extractor with a pseudorandom generator.

In a different setting, Kalai, Li, and Rao [KLR09] studied two-source extractors for information-theoretic sources (without a CRS) against a computationally bounded distinguisher. They succeed in constructing such extractors for linear min-entropy sources, under the assumption that nearly optimal exponentially secure one-way permutations exist. To avoid the reliance on such strong assumptions, Garg, Kalai, and Khurana [GKK20] initiate the study of two-source extractors in the CRS model. They focus solely on the setting with efficiently samplable sources and computationally bounded distinguishers, and assume the subexponential hardness of the DDH assumption (a weaker assumption relative to that required by [KLR09]). Under these conditions, they construct a special type of two-source extractor that lies between seeded and non-malleable two-source extractors, in the sense that neither source is required to be uniform, but only the second source is allowed to be tampered. They give such explicit extractors in the CRS model with balanced sources for min-entropy matching that of the best explicit statistical two-source extractors. Then, they exploit this extractor and results of [BACD+18] to construct an extractor of the same type for unbalanced sources with lower min-entropy. We remark that the assumption in [GKK20] can be weakened to quasi-polynomial hardness of the DDH assumption if one is aiming to match the min-entropy requirements of the best explicit statistical two-source extractors, as is done in the first part of [GKK20]. To go below such min-entropy requirements, a subexponential hardness assumption appears to be necessary.

Our computational non-malleable two-source extractors are constructed in the CRS model of [GKK20]. Consequently, our results are incomparable to those of [TV00, KLR09, DGKM12]. As mentioned before, [GKK20] construct two-source extractors that handle one-sided tampering In contrast, we focus on constructing non-malleable two-source extractors, which handle two-sided tampering. Moreover, there are other key differences with respect to [GKK20]. Our first result shows how to construct non-malleable two-source extractors in the CRS model for low min-entropy (against an unbounded distinguisher) from collision-resistant hash functions and statistical non-malleable two-source extractors for very high min-entropy. In comparison, previous results on low-error computational (even malleable) extractors for low min-entropy in the CRS model require at least subexponential hardness assumptions. For our second construction, we make use of a quasi-polynomial hardness assumption, and similarly to [GKK20] consider a computationally bounded distinguisher. We are able to essentially match the parameters of the one-sided tampering extractor obtained in [GKK20] under the same hardness assumption. Our last construction of a non-malleable two-source extractor in the CRS model against an unbounded distinguisher is

\footnote{By subexponential hardness of the DDH assumption we mean that there exists a constant \(c \in (0, 1)\) such that no algorithm running in time at most \(2^{n^c}\) solves the Decisional Diffie-Hellman problem with non-negligible (in \(n\)) advantage.}
extremely simple, but requires the same strong hardness assumption as [DRV12] (nearly optimal collision-resistant hash functions). A comparison of our constructions with previous work can be found in Table 1.

Other works on cryptography with tamperable memory. Besides the concept of non-malleability, the extension of cryptographic problems to settings with tamperable memory has also been considered in various ways, e.g., [GLM+04, IPSW06, KKS11]. Most relevant to our privacy amplification problem, Austrin, Chung, Mahmoody, Pass, and Seth [ACM+14] study key agreement protocols, which are intimately connected to privacy amplification, in a setting where the adversary is allowed to tamper the randomness of both parties via an online $p$-tampering attack before the protocol starts. This setting and the associated result are incomparable to ours. Indeed, there are two key differences: On the one hand, we consider arbitrary tampering attacks that jointly target the randomness and shared secret of a party, which are much stronger than the online $p$-tampering attacks considered in [ACM+14]. On the other hand, we must restrict tampering to one of the parties, as otherwise privacy amplification is impossible.

1.2 Technical Overview

1.2.1 Privacy amplification resilient against memory-tampering active adversaries

We introduce the setting of privacy amplification resilient against memory-tampering active adversaries, and show that low-error non-malleable two-source extractors with good min-entropy requirements can be used to design privacy amplification protocols in this setting, both in the information-theoretic and computational settings. To be more precise, we consider the 4-round protocol illustrated in Figure 1 instantiated with an appropriate strong non-malleable two-source extractor $\text{nmExt}$.

<table>
<thead>
<tr>
<th>Alice</th>
<th>Bob</th>
</tr>
</thead>
<tbody>
<tr>
<td>Memory: ($W, A$)</td>
<td>Memory: ($W, B$)</td>
</tr>
<tr>
<td>$R_A = \text{nmExt}(W, A</td>
<td></td>
</tr>
<tr>
<td>$A' \xrightarrow{A} B'$</td>
<td>$[R_A]<em>\alpha \xrightarrow{} [R_A]</em>\alpha'$</td>
</tr>
<tr>
<td>$[R_B]<em>{\alpha-2\alpha}' \xleftarrow{} [R_B]</em>{\alpha-2\alpha}$</td>
<td>If $[R_B]<em>\alpha = [R_A]</em>\alpha'$ then $S_B = [R_B]_{2\alpha}$; Otherwise $S_B = \perp$</td>
</tr>
<tr>
<td>If $[R_A]<em>{\alpha-2\alpha} = [R_B]</em>{\alpha-2\alpha}'$ then $S_A = [R_A]_{2\alpha}$; Otherwise $S_A = \perp$</td>
<td></td>
</tr>
</tbody>
</table>

Figure 1: 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 $[x]_{j:} = (x_{j+1}, \ldots, x_n)$.

We provide an informal argument for why the protocol from Figure 1 works in the information-theoretic setting when the randomness tapes $A$ and $B$ of Alice and Bob, respectively, are sufficiently shorter than the shared secret $W$. If Eve is passive and simply eavesdrops on the communication between Alice and Bob, then the fact that $\text{nmExt}$ is a strong extractor implies that Alice and Bob output strings $S_A \neq \perp$ and $S_B \neq \perp$, respectively, such that $S_A = S_B$ and which are close to uniform with respect to Eve’s view. Assume now that Eve is active and corrupts Alice. This means that
Alice’s memory, \((W, A)\), is replaced by an arbitrary function \((\tilde{W}, \tilde{A}) = F(W, A)\). We show that, with high probability over the fixings \(A = a\) and \(\tilde{A} = \tilde{a}\), with high probability either one of Alice or Bob aborts (i.e., outputs \(\bot\)), or we have \(S_A = S_B \neq \bot\) and \(S_A, S_B\) are close to uniform from Eve’s view. Observe that, after fixing \(A = a\) and \(\tilde{A} = \tilde{a}\), we have that \(\tilde{W}\) is now a tampering of \(W\) only. Moreover, assuming that \(A\) is appropriately shorter than \(W\), with high probability it holds that \(W\) still has enough min-entropy after conditioning on \(A = a\) and \(\tilde{A} = \tilde{a}\). For the sake of exposition, suppose that \(\tilde{W} \neq W\) always. We claim that, in this case, Bob detects tampering and aborts. Indeed, note that \(R_A = \text{nmExt}(\tilde{W}, a\|B)\) can be written as \(R_A = \text{nmExt}(g_1(W), g_2(\tilde{a}\|B))\) for tampering functions \(g_1\) and \(g_2\), where \(g_1\) has no fixed points. Therefore, by the properties of \(\text{nmExt}\), we conclude that, even after revealing \((a, \tilde{a}, B, R_A)\), we have that \(R_B = \text{nmExt}(W, \tilde{a}\|B)\) is close to uniform. As a result, in the third round of the protocol, Eve can only guess a (long enough) prefix of \(R_B\) with very small probability. Therefore, Bob aborts with high probability, as desired. As an example, we can obtain the following informal result.

**Theorem 1** (Informal). If \(\text{nmExt}\) is a low-error strong non-malleable two-source extractor for sources with min-entropy \(0.8n\) and \(0.05n\), respectively, then there exists a 4-round privacy amplification protocol resilient against memory-tampering active adversaries when \(H_\infty(W) \geq 0.95n\) and \(H_\infty(A), H_\infty(B) \geq 0.05n\) whenever \(|A|, |B| \leq 0.1n\).

Since (inefficient) non-malleable two-source extractors are known to exist with much better parameters than those required above [CGGL20], we readily conclude that 4-round privacy amplification protocols resilient against memory-tampering active adversaries exist with very good parameters. However, we do not know any explicit constructions of non-malleable two-source extractors with sufficiently good min-entropy requirements, and in Section 1.2.2 we give evidence that obtaining such extractors appears to be extremely challenging.

Nevertheless, we show that, extending the notion of privacy amplification resilient against memory-tampering active adversaries to the CRS model (that we formalize later), we can exploit our explicit constructions of non-malleable two-source extractors in the CRS model to obtain explicit 4-round privacy amplification protocols resilient against memory-tampering active adversaries in the CRS model with very good parameters. We remark that this task is not trivial in the CRS model, because the shared secret \(W\) and randomness tapes \(A\) and \(B\) are arbitrarily correlated with the CRS, and Eve also has full knowledge of the CRS at all times. Moreover, care is needed in this computational setting because we need to ensure that sources remain samplable by appropriately sized circuits even after some conditionings. We overcome this by using a strong non-malleable two-source extractor that allows the left source to be sampled in subexponential time.

**Theorem 2** (Informal). Assuming the sub-exponential hardness of the DDH assumption, there exists an explicit 4-round privacy amplification protocol resilient against memory-tampering active adversaries in the CRS model for \(W \in \{0,1\}^n\) such that \(H_\infty(W) \geq 0.52n\) and \(A, B\) with sublinear min-entropy.

Formal statements and more details can be found in Section 8.

**Discussion of the extraction property for privacy amplification.** In the standard setting of privacy amplification (which does not allow for tampering of memory or randomness tapes) some authors require an extra property from the protocol. If any one of Alice or Bob (say, Alice) does not abort (but the other party does abort), then the key derived by Alice should still be close to uniform and independent of Eve’s view. This property is called extraction in [DLWZ14, Definition
blocks. (Received as input a source $X$ requires an additional security when one party aborts. We note that this property is impossible to achieve in the setting where Alice’s randomness tape is controlled by Eve. In this case, Alice would need to extract uniform randomness from a weak random source $W$ without access to any additional randomness, which is known to be impossible [CG88]. We note also that if the memory and randomness tapes are not tampered with, then, by the definition of a strong non-malleable two-source extractor, our protocol also fulfills the extraction property.

1.2.2 Slightly better non-malleable extractors imply great two-source extractors

To show that small improvements to the best known low-error non-malleable two-source extractors lead to explicit low-error two-source extractors for low min-entropy sources, we consider an explicit non-malleable two-source extractor $\text{nmExt}$ for high min-entropy sources handling enough tamperings, and two independent $n$-bit sources $X$ and $Y$ with min-entropy $\delta n$, for some small constant $\delta > 0$. In other words, $X$ and $Y$ have min-entropy rate $\delta$.

If we had access to a uniform seed, we could apply seeded condensers to transform $X$ and $Y$ into shorter sources $X'$ and $Y'$ which are (statistically close to) sources with high min-entropy rate. Then, computing $\text{nmExt}(X', Y')$ would lead to nearly uniform randomness without even exploiting the non-malleability of $\text{nmExt}$. Although deterministic condensers do not exist, there does exist a deterministic object with related properties, called a *somewhere-condenser*. Such an object $\text{SCond}$ receives as input a source $X$ with min-entropy rate $\delta$, and outputs $X' = \text{SCond}(X)$ composed of $\ell$ blocks $(X'_1, X'_2, \ldots, X'_\ell)$, with the property that for some random variable $I$ it holds that $X'_i$ is statistically close to a source with min-entropy rate $1 - \gamma$. Importantly, we can write the blocks $X'_i$ for $i \neq I$ as randomized tamperings of the *good* block $X'_I$. Analogously, computing $Y' = \text{SCond}(Y)$ leads to $\ell$ blocks $(Y'_1, Y'_2, \ldots, Y'_\ell)$ and a random index $J$ such that $Y'_j$ is close to a source with high min-entropy rate, and $Y'_j$ for $j \neq J$ can be written as randomized tamperings of $Y'_J$. Combined with the non-malleability properties of $\text{nmExt}$, these observations naturally lead to the candidate two-source extractor $\text{Ext}$ given by

$$\text{Ext}(X, Y) = \bigoplus_{i,j \in [\ell]} \text{nmExt}(X'_i || p_i, Y'_j || p_j),$$

where $p_i$ and $p_j$ are suffixes added to ensure that the tamperings induced by the somewhere-condenser do not have fixed points. In order to prove that $\text{Ext}$ indeed extracts from the low min-entropy sources $X$ and $Y$, it is enough to show that $\text{nmExt}(X'_I || p_I, Y'_J || p_J)$ is close to uniform given the side information $\text{nmExt}(X'_i || p_i, Y'_j || p_j)$ for $(i, j) \neq (I, J)$. This is equivalent to requiring that $\text{nmExt}$ resists $\ell^2 - 1$ tamperings. Explicit constructions of somewhere-condensers with good parameters are known [BKS+10, Raz05, Zuc06, Li11]. In particular, we can take the number of blocks $\ell$ to be a constant depending only on $\delta$ and $\gamma$, and the error to be exponentially small in the length of the output blocks. Therefore, our argument goes through provided we have an explicit non-malleable two-source extractor for min-entropy rate $1 - \gamma$ handling $\ell^2 - 1$ tamperings. Moreover, the resulting extractor $\text{Ext}$ has low error if $\text{nmExt}$ does so.

Overall, our reduction above trades the number of tamperings handled with lowering the original min-entropy requirement of the underlying non-malleable two-source extractor. We leave formal details of our general result for Section 4, and present here one important case.

**Theorem 3** (Informal). For every constant $\gamma > 0$ there exists a constant $C_\delta$ such that if there exists an explicit low-error non-malleable two-source extractor $\text{nmExt}$ for min-entropy rate $1 - \gamma$ handling $C_\delta$ tamperings, then there exists an explicit low-error two-source extractor for min-entropy
rate $\delta$. In particular, if $\text{nmExt}$ handles $r = \omega(1)$ tamperings, then for every constant $\delta > 0$ there exists an explicit low-error two-source extractor for min-entropy rate $\delta$.

Interestingly, by [Li17] (see Proposition 5) we have explicit constructions of low-error non-malleable extractors for constant min-entropy rate $1 - \gamma$ (with $\gamma$ a small constant) and a constant number of tamperings, and $r = \omega(1)$ tamperings for any min-entropy rate $1 - o(1)$. If this result is improved to handle any superconstant number of tamperings with some constant min-entropy rate, then Corollary 3 implies that we have explicit low error two-source extractors for any linear min-entropy rate. Even improving the number of tamperings handled to a large enough constant for some constant min-entropy rate would already yield significantly improved explicit low-error two-source extractors. We remark also that small improvements on the non-malleable two-source extractor from [CGL16] are enough to make our argument go through as well. We discuss this in detail in Section 4. Finally, note that the non-malleable two-source extractors we require for our reduction are far from optimal. Indeed, it is known that, for any constant $\delta > 0$, with high probability a random function is a non-malleable two-source extractor for $n$-bit sources with min-entropy $\delta n$ handling $r = n^\Omega(1)$ tamperings with error $2^{-\Omega(n)}$ [CGGL20].

1.2.3 Side quest: Slightly better non-malleable extractors imply great computational non-malleable extractors under standard assumptions

Given our reduction above, it is natural to wonder whether $\text{Ext}$ defined in (1) can be made non-malleable. Unfortunately, it is not clear how to achieve that in the information-theoretic setting. Indeed, one can tamper $X$ into $\overline{X} \neq X$ such that $S\text{Cond}(X) = S\text{Cond}(\overline{X})$, and this suffices to break the (information-theoretic) non-malleability of $\text{Ext}$. We move this problem to the CRS model [GKK20] (for a discussion of the CRS model, see Section 1.2.4), and ask instead whether $\text{Ext}$ can be made non-malleable in this computational model.

Modifying the extractor. Intuitively, the only way to break non-malleability of $\text{Ext}$ is to proceed as above by finding valid tamperings of $X$ and $Y$ that lead to collisions at the input to the underlying non-malleable two-source extractor $\text{nmExt}$. In the CRS model, we overcome this problem by sampling a collision-resistant hash function $H$ from any family of collision-resistant hash functions secure against polynomial-time adversaries with not too long output (namely, output length $o(n)$, where $n$ is the length of $X$), and including the hashes $H(X)$ and $H(Y)$ as input to $\text{nmExt}$. In other words, we use the intuition above to show that for $\text{CRS} = H$, the modified function

$$
\text{cnmExt}(X, Y, H) = \bigoplus_{i,j \in [\ell]} \text{nmExt}(X'_i \| p_i \| H(X), Y'_j \| p_j \| H(Y)) ,
$$

where we recall that $(X'_1, X'_2, \ldots, X'_\ell) = S\text{Cond}(X)$, is a low-error two-source non-malleable extractor in the CRS model for low min-entropy, provided the underlying $\text{nmExt}$ can handle $\ell^2 - 1$ tamperings. Remarkably, we obtain an exact analogue of Theorem 3 in the CRS model from standard assumptions and with added non-malleability. More details can be found in Section 5.

1.2.4 Non-malleable extractors in the CRS model

Since our previous result is conditional on small improvements on the information-theoretic non-malleable two-source extractors from [CGL16, Li19], we turn to obtaining unconditional explicit constructions of non-malleable two-source extractors in the CRS model. Table 1 compares our constructions with previous results on computational two-source extractors. In the following, we formally describe the CRS model.
The CRS model. In this model, we assume that a CRS (denoted CRS) is first efficiently sampled and set once and for all. Our goal is to extract either computationally or statistically perfect randomness from independent weak sources $X$ and $Y$ which are sampled from CRS by a computationally bounded sampler. As side information, we disclose the output of the extractor on tampered versions of $X$ and $Y$. More precisely, for arbitrary computationally bounded functions $g_1$ and $g_2$, we reveal the output of the extractor on $\overline{X} = g_1(X, \text{CRS})$ and $\overline{Y} = g_2(Y, \text{CRS})$. We say a function $\text{cnmExt}$ is a non-malleable two-source extractor in the CRS model if it holds that

$$\text{cnmExt}(X, Y, \text{CRS}), \text{cnmExt}(\overline{X}, \overline{Y}, \text{CRS}), \text{CRS} \approx U, \text{cnmExt}(\overline{X}, \overline{Y}, \text{CRS}), \text{CRS},$$

where $U$ is uniformly distributed and independent of the remaining random variables, and $\approx$ denotes either computational or statistical indistinguishability. Although we do not discuss it in the following paragraphs, we allow more than one tampering of $X$ and $Y$, and also allow the sampler to leak additional auxiliary information about $X$ to help the distinguisher. Note that the CRS is quite different from an independent uniform seed, since both the sources and the tampering functions are allowed to depend adversarially on the CRS. Formal definitions can be found in Section 2.4.

Finally, we remark that the well-known upper bound of $2n$ tamperings for statistical non-malleable two-source extractors also holds in the CRS model.\(^3\) This is unlike one-sided tampering, in which case an unbounded (polynomial) number of tamperings is allowed in the computational setting.

Non-malleable two-source extractors in the CRS model from quasi-polynomial hardness. Building on techniques developed in [BHK11, GKK20], we construct an explicit non-malleable two-source extractor against a computationally bounded distinguisher assuming the quasipolynomial hardness of DDH with essentially the same parameters as the corresponding extractor from [GKK20], which only handles one-sided tampering.

The basis for our extractor is a family $\mathcal{F}$ of lossy functions, first introduced and constructed by Peikert and Waters [PW11]. Roughly speaking, $\mathcal{F}$ is a family of functions $f : \{0, 1\}^n \rightarrow \{0, 1\}^n$ containing both injective and lossy functions, i.e., functions with small image size. The security of $\mathcal{F}$ ensures that for $f \in \mathcal{F}$ injective with probability $1/2$ and lossy with probability $1/2$ no computationally bounded adversary can guess whether $f$ is injective or lossy with non-negligible advantage. Moreover, we also require families of collision-resistant hash functions $\mathcal{H}_1$ and $\mathcal{H}_2$ with output lengths not too large.

We show that a simple modification of the extractor from [GKK20] for one-sided tampering is enough to obtain a non-malleable two-source extractor $\text{cnmExt}$ in the CRS model for error and min-entropy requirements matching those of the best statistical malleable two-source extractors under the quasi-polynomial hardness of the DDH assumption. This construction is quite flexible, and we shall see that upgrading the hardness assumption to the subexponential hardness of the DDH assumption also allows us to assume that one of the sources can be sampled in subexponential time. This will prove useful for devising explicit privacy amplification protocols resilient against memory-tampering adversaries in the CRS model.

For simplicity, we illustrate only the case where $\mathcal{H}_1 = \mathcal{H}_2$. To set the CRS, first we sample hash functions $h \leftarrow \mathcal{H}$ with output length $\ell$. Then, we sample $b \leftarrow \{0, 1\}^{2\ell}$, and sample $f_{ij}$ from $\mathcal{F}$ for $i \in [2\ell]$ and $j \in \{0, 1\}$ such that $f_{ib}$ is injective and $f_{i1-b}$ is lossy for every $i$. Given such CRS, we

\(^3\)Since there exist pairs $(a, b)$ and $(a', b)$ such that $\text{nmExt}(a, b) \neq \text{nmExt}(a', b)$, we can learn one bit of $X$ by applying efficient tampering functions $g_1$ such that $g_1(x) = a$ if $x_i = 0$ and $g_1(x) = a'$ otherwise, and $g_2$ such that $g_2(y) = b$ for all $y$. We can then perform analogous tamperings for $Y$ in place of $X$. 

define our candidate non-malleable two-source extractor in the CRS model as
\[
\text{cnmExt}(X, Y, \text{CRS}) = \text{Ext}(f_h(X)\|h(Y))(X, Y),
\]
where \(\text{Ext}\) is a statistical strong two-source extractor, and
\[
f_{a_1}(x) = f_{2a_1}(f_{2a_2}(\cdots (f_{2a_{2^t}}(x)) \cdots)).
\]

Let \(\overline{X}\) and \(\overline{Y}\) denote tamperings of \(X\) and \(Y\), respectively. First, due to the security properties of the family of lossy functions \(F\) under the quasi-polynomial hardness of the DDH assumption, we show that we can assume that \(h(X)\|h(Y) = b\) and \(h(X)\|h(Y) \neq h(\overline{X})\|h(\overline{Y})\) hold simultaneously. Under these conditions, it follows that \(f_{h(X)\|h(Y)}\) is an injective function and \(f_{h(\overline{X})\|h(\overline{Y})}\) has small image size. Our final goal is to show that \(\text{cnmExt}(X, Y, \text{CRS})\) is computationally close to uniform given \(\text{cnmExt}(\overline{X}, \overline{Y}, \text{CRS})\). Since \(f_{h(\overline{X})\|h(\overline{Y})}\) has small image size and \(h\) has small output length, it follows that \(X\) and \(Y\) are still independent do not lose much min-entropy when we reveal \(f_{h(\overline{X})\|h(\overline{Y})}(\overline{X}), \text{cnmExt}(\overline{X}, \overline{Y}, \text{CRS})\), and all the hashes. This allows us to invoke the statistical properties of \(\text{Ext}\) to obtain the desired result.

As an example, instantiating \(\text{Ext}\) with the best known statistical two-source extractors [Bou05, Raz05, Lew19, CZ19] yields the following informal result. Formal statements and more details can be found in Section 6.

**Theorem 4 (Informal).** Assuming the quasi-polynomial hardness of the DDH assumption, there exist explicit non-malleable two-source extractors in the CRS model with essentially the same parameters as the best explicit information-theoretic two-source (malleable) extractors.

**Simple non-malleable two-source extractors in the CRS model from nearly optimal collision-resistant hash functions, against an unbounded distinguisher.** Since our previous result holds only for a computationally bounded distinguisher, we ask whether we can devise an explicit non-malleable two-source extractor in the CRS model secure against computationally unbounded distinguishers, potentially by strengthening the underlying hardness assumption. We show that this is possible with a simple construction, provided we assume the existence of nearly optimal collision-resistant hash functions (in the sense that a birthday attack is essentially the best possible). In practice, this is not a far-fetched assumption: For most widely deployed hash functions such as SHA-256, SHA-512, and SHA-3 we currently cannot do better than a birthday attack.

Our construction is given by \(\text{cnmExt}(X, Y, H) = \text{nmExt}(H(X), H(Y))\), where \(H\) is sampled from a family of nearly optimal collision-resistant hash functions \(H\), and \(\text{CRS} = H\). Intuitively, the security of this construction follows not only from the collision-resistance of \(H\), but also from the fact that both \(H(X)\) and \(H(Y)\) are statistically close to high min-entropy sources [DRV12]. Formal statements and more details can be found in Section 7.

**Theorem 5 (Informal).** If there exist nearly optimal collision-resistant hash functions \(h : \{0, 1\}^n \rightarrow \{0, 1\}^\ell\) for some \(\ell = \Omega(\text{polylog}(n))\), then there exists an explicit low-error non-malleable two-source extractor for \(n\)-bit sources with min-entropy \(\ell\) in the CRS model.

We can instantiate our privacy amplification protocol with the non-malleable two-source extractors obtained in either Theorem 4 or Theorem 5. However, since the proofs are nearly identical, we instantiate only with Theorem 4, and obtain the result mentioned in Theorem 2. We note here that the issues with efficient samplability require that we allow one of the sources to be sampled in subexponential time. This is not a problem for the extractor from Theorem 5, but in the case of the extractor from Theorem 4 we need to upgrade the quasi-polynomial DDH assumption to subexponential hardness of DDH.
1.3 Organization

We would like to emphasize that all sections of the paper (with the exception of Section 8) can, together with the preliminaries (Section 2), be read independently of each other. In the following, we list the results shown in each section.

- In Section 3, we describe and analyze our information-theoretic privacy amplification protocol.
- In Section 4, we show that a slight improvement in the construction of non-malleable two-source extractors would imply low-error low min-entropy two-source extractors, thereby resolving a long-standing open question.
- In Section 5, we discuss a modification of the above reduction. We show that a small improvement in non-malleable two-source extractors, along with the assumption that collision-resilient hash functions exist, implies low-error, low min-entropy non-malleable two-source extractors in the CRS model.
- Section 6 focuses on non-malleable extractors in the CRS model obtained from the quasi-polynomial hardness of the DDH assumption.
- In Section 7, we give a simple non-malleable extractors in the CRS model obtained from nearly optimal collision-resistant hash functions.
- In Section 8, we instantiate the privacy amplification protocol from Section 3 with the non-malleable extractor from Section 6. Instantiating with the non-malleable extractor from Section 7 is analogous, and thus we omit it.

2 Preliminaries

2.1 Notation

Random variables are usually denoted by uppercase letters such as $X$, $Y$, and $Z$. Sets are usually denoted by uppercase calligraphic letters such as $S$ and $T$. Given two strings $x$ and $y$, we denote their concatenation by $x||y$. Additionally, given an $n$-symbol string $x$, we define $[x]_i = (x_1, x_2, \ldots, x_i)$, $[x]_{i:j} = (x_{i+1}, x_{i+2}, \ldots, x_j)$, and $[x]_i: = (x_{i+1}, x_{i+2}, \ldots, x_n)$. The base-2 logarithm is denoted by $\log$. We say an algorithm is size-$t$ if it can be computed by a (possibly randomized) circuit of size at most $t$. Moreover, we use $\text{poly}(n)$ to denote an arbitrary polynomial in $n$.

2.2 Statistical distance and min-entropy

In this section, we introduce the basic concepts of statistical distance and min-entropy, along with useful lemmas.

**Definition 1** (Statistical distance). Given two distributions $X$ and $Y$ over a set $\mathcal{X}$, the statistical distance between $X$ and $Y$, denoted by $\Delta(X; Y)$, is defined as

$$\Delta(X; Y) = \max_{S\subseteq \mathcal{X}} |\Pr[X \in S] - \Pr[Y \in S]| = \frac{1}{2} \sum_{x \in \mathcal{X}} |\Pr[X = x] - \Pr[Y = x]|.$$ 

We may write $\Delta(X; Y|Z)$ as shorthand for $\Delta(X, Z; Y, Z)$, and say that $X$ and $Y$ are $\eps$-close, also written $X \approx_{\eps} Y$, if $\Delta(X; Y) \leq \eps$. For a random variable $X \in \{0, 1\}$, we informally call $\Delta(X; U_1) = |\Pr[X = 1] - 1/2|$ the bias of $X$.
Definition 2 (Min-entropy). Given a distribution $X$ over $X$, the min-entropy of $X$, denoted by $H_\infty(X)$, is defined as

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

Definition 3 (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

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

Lemma 1 ([DORS08]). Given arbitrary distributions $X$ and $Z$ such that $|\text{supp}(Z)| \leq 2^\lambda$, we have

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

Lemma 2 ([MW97]). For arbitrary distributions $X$ and $Z$, it holds that

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

Lemma 3. Suppose $X$ and $Z$ are random variables such that $\tilde{H}_\infty(X|Z) \geq k$ and $E$ is an event with $\Pr[E] \geq p$. Then, it holds that

$$\tilde{H}_\infty(X|E, Z) := \tilde{H}_\infty((X|E)|Z) \geq k - \log(1/p).$$

Proof. We have

$$\mathbb{E}_{z \leftarrow Z} \left[\max_{x} \Pr[X = x|E, Z = z]\right] = \sum_z \Pr[Z = z|E] \cdot \max_x \frac{\Pr[X = x, E|Z = z]}{\Pr[E|Z = z]}$$

$$\leq \sum_z \Pr[Z = z|E] \cdot \max_x \frac{\Pr[X = x|Z = z]}{\Pr[E|Z = z]}$$

$$= \sum_z \frac{\Pr[Z = z]}{\Pr[E]} \cdot \max_x \Pr[X = x|Z = z]$$

$$\leq \frac{1}{p} \cdot \mathbb{E}_{z \leftarrow Z} \left[\max_{x} \Pr[X = x|Z = z]\right]$$

$$\leq \frac{2^{-k}}{p},$$

where the second inequality follows from $\Pr[E] \geq p$ and the last inequality follows from the fact that $\tilde{H}_\infty(X|Z) \geq k$. \qed

2.3 Extractors and condensers

We present some important objects from pseudorandomness.

Definition 4 ((n,k)-source). A distribution $X \in \{0,1\}^n$ is said to be an $(n,k)$-source if $H_\infty(X) \geq k$. Moreover, $X$ is said to be flat if it is uniformly distributed over a set of size at least $2^k$.

Definition 5 ((k_1,k_2,ε)-extractor). A function $\text{Ext} : \{0,1\}^n \times \{0,1\}^n \rightarrow \{0,1\}^m$ is said to be a (strong, average-case) $(k_1,k_2,ε)$-extractor if for independent random variables $(X,W)$ and $Y$ such that $\tilde{H}_\infty(X|W) \geq k_1$ and $Y$ is an $(n,k_2)$-source we have

$$\text{Ext}(X,Y), Y, W \approx_\epsilon U_m, Y, W.$$ If $k_1 = k_2 = k$, we say $\text{Ext}$ is a (strong, average-case) $(k,ε)$-extractor.
It is easy to see that every non-average-case \((k, \varepsilon)\)-extractor \(\text{Ext}\) is also an average-case \((k + \log(1/\gamma), \varepsilon + \gamma)\)-extractor for any \(\gamma > 0\). We will need the following explicit two-source extractors.

**Proposition 1** ([Bou05, Lew19]). There exists an explicit strong average-case \((k, \varepsilon)\)-extractor \(\text{Ext} : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}\) with \(k = 0.45n\) and \(\varepsilon = 2^{-\Omega(n)}\).

**Proposition 2** ([Raz05]). For any constant \(\gamma > 0\) there exists an explicit strong average-case \((k_1, k_2, \varepsilon)\)-extractor \(\text{Ext} : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^m\) with \(k_1 = (1/2 + \gamma)n\), \(k_2 = O(\log n)\), \(\varepsilon = 2^{-\Omega(n)}\), and \(m = \Omega(n)\).

**Proposition 3** ([CZ19]). There exists an explicit strong average-case \((k, \varepsilon)\)-extractor \(\text{Ext} : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}\) with \(k = \text{polylog}(n)\) and \(\varepsilon = n^{-\Omega(1)}\).

**Definition 6** \(((k_1, k_2, \varepsilon, r)\)-non-malleable extractor). A function \(\text{nmExt} : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^m\) is said to be a \((\text{strong, average-case}) (k_1, k_2, \varepsilon, r)\)-non-malleable extractor if for every pair of independent distributions \((X, W)\) and \(Y\) such that \(H_\infty(X|W) \geq k_1\) and \(Y\) is an \((n, k_2)\)-source, and every family of tampering functions \(g_{i_1}, g_{i_2} : \{0,1\}^n \to \{0,1\}^n\) where one of \(g_{i_1}\) and \(g_{i_2}\) has no fixed points for all \(i = 1, \ldots, r\), we have

\[
\Delta(\text{nmExt}(X, Y); U_m|Y, W, \text{nmExt}(g_{i_1}(X), g_{i_2}(Y)), \ldots, \text{nmExt}(g_{r_1}(X), g_{r_2}(Y)))) \leq \varepsilon.
\]

If \(k_1 = k_2 = k\), we say \(\text{nmExt}\) is a \((\text{strong, average-case}) (k, \varepsilon, r)\)-non-malleable extractor.

**Proposition 4** ([CGL16], [GSZ20, Appendix A]). There exists an explicit strong average-case \((k, \varepsilon, r)\)-non-malleable extractor \(\text{nmExt} : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^m\) where \(k = n - n^\Omega(1), \varepsilon = 2^{-n^\Omega(1)}, r = n^\Omega(1)\), and \(m = n^\Omega(1)\).

**Proposition 5** ([Li17], [GSZ20, Appendix A]). For every constant \(r\) there exists a small enough constant \(\gamma > 0\) such that there exists an explicit strong average-case \((k, \varepsilon, r)\)-non-malleable extractor \(\text{nmExt} : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^m\) where \(k = (1 - \gamma)n\), \(\varepsilon = 2^{-\Omega(n/\log n)}\), and \(m = \Omega(n/\log n)\).

Moreover, if \(k = (1 - o(1))n\), then there is \(r = \omega(1)\) such that there exists an explicit strong \((k, \varepsilon, r)\)-non-malleable extractor with \(\varepsilon = 2^{-n^\Omega(1)}\) and \(m = n^\Omega(1)\).

Although Li [Li17] presents its non-malleable extractor for the case \(r = 1\) only, it is straightforward to check that it can be extended to more than one tampering as above.

The following lemma states that non-malleable extractors are also resilient against tampering functions with independent shared randomness.

**Lemma 4.** Let \(\text{nmExt} : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^m\) be a \((k, \varepsilon, r)\)-non-malleable extractor, and let \(R\) be an arbitrary distribution over some set \(\mathcal{R}\). Then, for any tuple of functions \((g_{i_1}, g_{i_2})\in[r]\) of the form \(g_{i_1}, g_{i_2} : \{0,1\}^n \times R \to \{0,1\}^n\) such that for every fixing \(R = \text{rand}\) and \(i = 1, \ldots, r\) either \(g_{i_1}(:, \text{rand})\) or \(g_{i_2}(:, \text{rand})\) has no fixed points, it holds that

\[
\Delta(\text{nmExt}(X, Y); U_m|\text{nmExt}(g_{i_1}(X, R), g_{i_2}(Y, R)), \ldots, \text{nmExt}(g_{r_1}(X, R), g_{r_2}(Y, R)), R) \leq \varepsilon
\]

whenever \(X\) and \(Y\) are independent \((n, k)\)-sources also independent of \(R\).

Moreover, if \(\text{nmExt}\) is strong, \((g_{i_1}, g_{i_2})\in[r]\) are as above and \(F : \{0,1\}^n \times \mathcal{R} \to \{0,1\}^*\) is an arbitrary function, we have

\[
\Delta(\text{nmExt}(X, Y); U_m|F(Y, R), \text{nmExt}(g_{i_1}(X, R), g_{i_2}(Y, R)), \ldots, \text{nmExt}(g_{r_1}(X, R), g_{r_2}(Y, R)), R) \leq \varepsilon
\]
Proof. The claim follows from the fact that the desired inequality holds for every fixing $R = \text{rand}$ by the definition of non-malleable extractor (in the case of strong non-malleable extractors, also because $F(Y, \text{rand})$ is a function of $Y$ only).

**Definition 7** (Somewhere-$k$ sources). A distribution $Y = (Y_1, \ldots, Y_\ell) \in \{0,1\}^{m-\ell}$ is said to be an elementary somewhere-$k$ source if there is $i \in [\ell]$ such that $H_\infty(Y_i) \geq k$. Then, a distribution $Y \in \{0,1\}^{m-\ell}$ is said to be a somewhere-$k$ source if $Y$ is a convex combination of elementary somewhere-$k$ sources.

**Definition 8** (Somewhere-condenser). A function $S\text{Cond} : \{0,1\}^n \rightarrow \{0,1\}^{m-\ell}$ is said to be a $(\delta \rightarrow \delta', \varepsilon)$-somewhere condenser if for every $(n, \delta n)$-source $X$ there exists a somewhere-$(\delta' m)$ source $Y \in \{0,1\}^{m-\ell}$ such

$$S\text{Cond}(X) \approx_{\varepsilon} Y.$$ 

We will need the following two somewhere condensers due to Zuckerman and Li [Zuc06, Li11]. The first one transforms an input source with potentially low min-entropy rate into a somewhere-$k$ source with constant min-entropy rate. The second somewhere condenser transforms an input source with constant min-entropy rate into a somewhere-$k$ source with potentially large min-entropy rate. We note that other somewhere-condensers have also been constructed in [BKS+10, Raz05].

We begin by stating a somewhere-condenser that condenses sources to min-entropy rate $3/4$, due to Zuckerman [Zuc06].

**Lemma 5.** For $\delta$ and $n$ such that $\delta n = \omega(1)$ there is an explicit $(\delta \rightarrow 3/4, \varepsilon)$-somewhere condenser $S\text{Cond} : \{0,1\}^n \rightarrow \{0,1\}^{m-\ell}$ with $\ell = \text{poly}(1/\delta)$, $m = n/\text{poly}(1/\delta)$, and $\varepsilon = 2^{-\Omega(m)}$.

Improving upon the analysis of [Zuc06], Li [Li11] obtained the following somewhere-condenser that condenses sources to potentially very high min-entropy rate. A version of this somewhere-condenser also appears in [BDT16].

**Lemma 6.** For every $T = T(n) < n$ there exists a $(3/4 \rightarrow 1 - 1/T, \varepsilon)$-somewhere-condenser $S\text{Cond} : \{0,1\}^n \rightarrow \{0,1\}^{m-\ell}$ with $\ell = T^{5/2}$, $m = n/T^{\frac{5\log(3/2)}{2}}$, and $\varepsilon = 2^{-n/T^c}$ for some $c > 1$, provided $n$ is large enough.

Combining Lemmas 5 and 6 immediately leads to the following corollary.

**Corollary 1.** For every constant $\delta > 0$ and every $T = T(n) < n$ there exists a $(\delta \rightarrow 1 - 1/T, \varepsilon)$-somewhere-condenser $S\text{Cond} : \{0,1\}^n \rightarrow \{0,1\}^{m-\ell}$ with $\ell = O_\delta(T^{5/2})$, $m = \Omega_\delta(n/T^{\frac{5\log(3/2)}{2}})$, and $\varepsilon = 2^{-\Omega_\delta(n/T^c)}$ for some absolute constant $c > 1$, provided $n$ is large enough.

### 2.4 Computational extractors in the CRS model

In this section, we present the relevant definitions of computational pseudorandom objects in the CRS model. As usual, all parameters are functions of a single security parameter $\lambda$. For the sake of clarity, we do not write this dependence explicitly in the rest of the paper.

**Definition 9** (Samplable sources in the CRS model). A tuple

$$(X, Y, \text{AUX}) \in \{0,1\}^n \times \{0,1\}^n \times \{0,1\}^\lambda$$

is said to be a tuple of $(t_1, t_2, k_1, k_2)$-samplable sources in the CRS model if there exists CRS $\in \{0,1\}^c$ such that the following hold:

---

4The work [BDT16] has been retracted. However, the somewhere-condenser presented there is a restatement of the one of Li [Li11], and is correct.
• There exist a size-$t_1$ circuit $G_1$ and a size-$t_2$ circuit $G_2$ such that $X \leftarrow G_1(CRS)$ and $(Y, AUX) \leftarrow G_2(CRS)$.

• $X$ and $(Y, AUX)$ are conditionally independent given CRS.

• $H_\infty(X|CRS = \text{crs}) \geq k_1$ and $H_\infty(Y|CRS = \text{crs}) \geq k_2$ for every fixing CRS = crs.

When AUX is the empty string, we say $(X, Y)$ are $(t_1, t_2, k_1, k_2)$-samplable sources without auxiliary information.

For simplicity, when $t_1 = t_2 = t$ we say that $(X, Y, AUX)$ are $(t, k_1, k_2)$-samplable, when $k_1 = k_2 = k$ we say that $(X, Y, AUX)$ are $(t, t, k)$-samplable, and when both hold we say that $(X, Y, AUX)$ are $(t, k)$-samplable.

**Definition 10** (Non-malleable extractor in the CRS model). A function $\text{cnmExt} : \{0,1\}^n \times \{0,1\}^n \times \{0,1\}^c \rightarrow \{0,1\}^m$ is said to be a $(t_1, t_2, t'_1, t'_2, t'', k_1, k_2, \varepsilon, r)$-non-malleable extractor in the CRS model if there is CRS $\in \{0,1\}^c$ such that the following holds:

For every tuple $(X, Y, AUX)$ of $(t_1, t_2, k_1, k_2)$-samplable sources from CRS, every tuple of deterministic size-$t'_1$ circuits $g_{11}, \ldots, g_{1r} : \{0,1\}^n \times \{0,1\}^c \rightarrow \{0,1\}^n$ and size-$t''_2$ $g_{21}, \ldots, g_{2r} : \{0,1\}^n \times \{0,1\}^a \times \{0,1\}^c \rightarrow \{0,1\}^n$ such that for every $i \in [r]$ and every fixing CRS = crs either $g_{1i}(\cdot, \text{crs})$ has no fixed points or $g_{2i}(\cdot, \text{aux}, \text{crs})$ has no fixed points for every fixing $AUX = \text{aux}$, and every size-$t''$ adversary $A$ we have

\[
| \Pr[A(\text{cnmExt}(X, Y, CRS), L_1, \ldots, L_r, AUX, CRS) = 1] - \Pr[A(U_m, L_1, \ldots, L_r, AUX, CRS) = 1] | \leq \varepsilon,
\]

where $L_i = \text{cnmExt}(g_{1i}(X, CRS), g_{2i}(Y, AUX, CRS), CRS)$. We set $t'' = \infty$ to denote that $A$ is allowed to be computationally unbounded.

We say $\text{cnmExt}$ is a $(t_1, t_2, t'_1, t'_2, t'', k, \varepsilon, r)$-non-malleable extractor without auxiliary information if the above holds for all $(t_1, t_2, k_1, k_2)$-samplable sources $(X, Y)$ without auxiliary information.

For simplicity, when $t_1 = t_2 = t$, $t'_1 = t'_2 = t'$, and $k_1 = k_2 = k$, we say that $\text{cnmExt}$ is a $(t, t', t'', k, \varepsilon, r)$-non-malleable extractor in the CRS model.

Observe that every non-malleable extractor resilient to auxiliary information is, in particular, strong.

### 2.5 Other relevant computational objects

In this section, we present other computational objects that will prove useful throughout the paper.

**Definition 11** ($(t, \delta)$-collision-resistant hash function family). A family of functions $\mathcal{H}$ is said to be $(t, \delta)$-collision-resistant if for every size-$t$ adversary $A$ it holds that

\[
\Pr[X_1 \neq X_2, H(X_1) = H(X_2)] \leq \delta,
\]

where $H \leftarrow \mathcal{H}$ and $(X_1, X_2) \leftarrow A(H)$.

**Definition 12** (Seed-dependent condenser). A function $\text{Cond} : \{0,1\}^n \times \{0,1\}^d \rightarrow \{0,1\}^m$ is said to be a $(k \rightarrow_\varepsilon k', t)$-seed-dependent condenser if for every $X \leftarrow \mathcal{G}(S)$, where $S \leftarrow \{0,1\}^d$, $\mathcal{G}$ is a size-$t$ circuit, and $H_\infty(X|S) \geq k$, it holds that

\[
\text{Cond}(X, S), S \approx_\varepsilon Z, S,
\]

where $H_\infty(Z|S) \geq k'$.
Dodis, Ristenpart, and Vadhan [DRV12] showed that collision-resistant hash functions with strong security are good seed-dependent condensers.

**Lemma 7** ([DRV12]). Suppose $\mathcal{H}$ is a family of $(t, 2^{\beta - 1 - m})$-collision-resistant hash functions $h : \{0,1\}^n \rightarrow \{0,1\}^m$ for some $\beta > 0$. Then, the function $\text{Cond}(X,H) = H(X)$ where $H \leftarrow \mathcal{H}$ is an $(m - \beta + 1 \rightarrow \varepsilon, m - \beta - \log(1/\varepsilon), t)$-seed-dependent condenser.

We will also require the following notion of a family of lossy functions, first introduced and constructed by Peikert and Waters [PW11].

**Definition 13** ($(t,n,\omega)$-lossy function family). A function family $\mathcal{F} = \{F\}_{\lambda \in \mathbb{N}}$ is a $(t,n,\omega)$-lossy function family if the following conditions hold:

- There are two PPT seed generation algorithms $G_{\text{inj}}$ and $G_{\text{loss}}$ such that for any size-$\text{poly}(t)$ adversary $A$ it holds that
  $$|\Pr_{s \leftarrow G_{\text{inj}}(1^\lambda)}[A(s) = 1] - \Pr_{s \leftarrow G_{\text{loss}}(1^\lambda)}[A(s) = 1]| = \text{negl}(t);$$
- For every $\lambda \in \mathbb{N}$ and every $f \in \mathcal{F}_{\lambda}$, $f : \{0,1\}^n \rightarrow \{0,1\}^n$.
- For every $\lambda \in \mathbb{N}$ and every $s \in G_{\text{inj}}$, $f_s \in \mathcal{F}_{\lambda}$ is injective.
- For every $\lambda \in \mathbb{N}$ and every $s \in G_{\text{loss}}$, $f_s \in \mathcal{F}_{\lambda}$ is lossy, i.e., its image size is at most $2^{n-\omega}$.
- There exists a PPT algorithm $\text{Eval}$ such that $\text{Eval}(s,x) = f_s(x)$ for every $\lambda \in \mathbb{N}$, every $s$ in the support of $G_{\text{inj}}(1^\lambda) \cup G_{\text{loss}}(1^\lambda)$, and every $x \in \{0,1\}^n$.

**Lemma 8** ([PW11, BHK11]). For any constant $\gamma \in (0,1)$ and for every $\Omega(\lambda) \leq n \leq \text{poly}(\lambda)$ there exists a $(t,n,\omega)$-lossy function family with $t = \lambda \log \lambda$ and $\omega = n - n^{1/2}$, assuming the quasi-polynomial hardness of the DDH assumption.

### 3 Privacy amplification resilient against memory-tampering active adversaries in the information-theoretic setting

In the following section, we formalize the notion of privacy amplification resilient against memory-tampering active adversaries, and show that non-malleable two-source extractors are natural tools for designing such privacy amplification protocols in the information-theoretic setting. We extend the result to the computational setting in Section 8.

We begin by formally defining with we mean by a privacy amplification protocol against memory-tampering active adversaries.

**Definition 14** (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 $F : \{0,1\}^{\ell_1} \times \{0,1\}^{\ell_2} \rightarrow \{0,1\}^{\ell_1} \times \{0,1\}^{\ell_2}$ 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 \((C'_2, C'_4, \ldots, C'_r)\), and Bob outputs \(S_B \in \{0, 1\}^m \cup \{\perp\}\) as a deterministic function of \((W, B)\) and \((C'_1, C'_3, \ldots, C'_r)\).

**Definition 15** (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

  \[
  S_A, C \approx_U U_m, C, \tag{3}
  \]

  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 (3).

We refer the reader to Section 1.2.1 for the discussion of other variants of privacy amplification. We are now ready to state our main result in the information-theoretic setting, which states that every strong non-malleable two-source extractor with appropriate parameters yields a 4-round privacy amplification protocol resilient against memory-tampering active adversaries via the protocol illustrated in Figure 1.

**Theorem 6.** Let \(\text{nmExt} : \{0, 1\}^{\ell_1} \times \{0, 1\}^{2\ell_2} \rightarrow \{0, 1\}^{m+2\alpha}\) be a strong \((k_1 - \ell_2 - 2\gamma - 1, k_2 - \gamma - 1, \varepsilon)\)-non-malleable two-source extractor. Then, there exists an \((r = 4, \ell_1, k_1, \ell_2, k_2, m, \varepsilon, \delta = \varepsilon + 2^{-\alpha} + 2 \cdot 2^{-\gamma})\)-privacy amplification protocol against memory-tampering active adversaries. Moreover, the protocol is explicit if \(\text{nmExt}\) is explicit.

**Proof.** We consider the 4-round protocol from Figure 1. Without loss of generality, we may assume that Eve is deterministic. We proceed by cases:

1. **Eve is passive:** Then, we have \(R_A = R_B\) (and hence \(S_A = S_B \neq \perp\)), and the desired result follows by noting that

   \[
   R_A = \text{nmExt}(W, A \parallel B), A \parallel B \approx_U U_{m+2\alpha}, A \parallel B, \quad \text{since} \quad W \text{ is independent of } A \parallel B, \quad H\infty(W) \geq k_1, \quad H\infty(A \parallel B) \geq 2k_2, \quad \text{and} \quad \text{nmExt} \text{ is a strong extractor. This implies that } S_A, C \approx_U U_m, C, \quad \text{where } C = (A, B, [R_A]_{2\alpha}) \text{ denotes Eve’s view.}
   \]

2. **Eve is active and Alice is corrupted:** Denote \((\tilde{W}, \tilde{A}) = F(W, A)\), and consider arbitrary fixings \(A = a\) and \(\tilde{A} = \tilde{a}\). Note that \(\tilde{W}\) is now a deterministic tampering of \(W\), and that, by Lemmas 1 and 2 and the fact that \(|\tilde{A}| = \ell_2\), it holds that

   \[
   H\infty(W|A = a, \tilde{A} = \tilde{a}) \geq H\infty(W|A, \tilde{A}) - \gamma
   \]
with probability at least $1 - 2^{-\gamma}$ over the fixings. We assume that the fixings above satisfy (4), and simply add a $2^{-\gamma}$ term to $\delta$ via a union bound. We now have

$$R_A = \text{nmExt}(\tilde{W}, \tilde{a} \parallel |B|)$$

and

$$R_B = \text{nmExt}(W, \tilde{a}' \parallel |B|),$$

where $\tilde{a}'$ is a deterministic function of $\tilde{a}$ (hence it is fixed), and $|B|$ is a deterministic function of $B$ since $A$ and $\tilde{A}$ are fixed. As a result, $W$ and $\tilde{a}' \parallel |B|$ are independent, and we can write $\tilde{W} = f(W)$ and $\tilde{a}' \parallel |B| = g(\tilde{a}' \parallel |B|)$ for deterministic tampering functions $f$ and $g$. Let $\mathcal{L} = \{w : f(w) = w\}$ and $\mathcal{R} = \{b : g(\tilde{a}' \parallel b) = \tilde{a}' \parallel b\}$. We now argue differently depending on whether $W \in \mathcal{L}$ and $B \in \mathcal{R}$ hold or not. We begin by noting that if either $\Pr[W \in \mathcal{L} \land B \in \mathcal{R}] < 2^{-\gamma}$ or $\Pr[W \notin \mathcal{L} \lor B \notin \mathcal{R}] < 2^{-\gamma}$, then we can add a $2^{-\gamma}$ term to $\delta$ via a union bound and assume that the opposite event holds. We are thus reduced to the two cases below:

(a) If $\Pr[W \in \mathcal{L} \land B \in \mathcal{R}] = \Pr[W \in \mathcal{L}] \cdot \Pr[B \in \mathcal{R}] \geq 2^{-\gamma}$, by Lemma 3 it holds that

$$H_\infty(W|A = a, \tilde{A} = \tilde{a}, W \in \mathcal{L}) \geq k_1 - \ell_2 - 2\gamma$$

(5)

and

$$H_\infty(B|A = a, \tilde{A} = \tilde{a}, B \in \mathcal{R}) \geq k_2 - \gamma.$$  

(6)

Therefore, since under this conditioning we still have that $W$ and $\tilde{a}' \parallel |B|$ are independent and they both have enough min-entropy by (5) and (6), it is the case that $R_A = R_B$ and

$$R_A = \text{nmExt}(W, \tilde{a} \parallel |B|), \tilde{a}' \parallel |B| \approx \epsilon U_{m+2\alpha}, \tilde{a}' \parallel |B|.$$  

If $[R_A]'_\alpha = [R_A]_\alpha$ and $[R_B]'_{\alpha,2\alpha} = [R_B]_{\alpha,2\alpha}$, then $S_A = S_B \neq \perp$ and $S_A, C \approx \epsilon U_m, C$, where $C = (\tilde{a}, \tilde{a}', B, B', [R_A]_{2\alpha}, [R_A]'_{2\alpha})$ denotes Eve’s view. Otherwise, we have either $S_A = \perp$ or $S_B = \perp$ with probability 1.

(b) On the other hand, if $\Pr[W \notin \mathcal{L} \lor B \notin \mathcal{R}] \geq 2^{-\gamma}$, by Lemma 3 it either holds that

$$H_\infty(W|A = a, \tilde{A} = \tilde{a}, W \notin \mathcal{L}) \geq k_1 - \ell_2 - 2\gamma - 1$$

(7)

or

$$H_\infty(B|A = a, \tilde{A} = \tilde{a}, B \notin \mathcal{R}) \geq k_2 - \gamma - 1.$$  

(8)

Assume that (7) holds and condition on $W \notin \mathcal{L}$. The proof when (8) holds and we condition on $B \notin \mathcal{R}$ is analogous. Then, we have that $f$ has no fixed points over the support of $W$ under this conditioning, and so, by the fact that $\text{nmExt}$ is a strong $(k_1 - \ell_2 - 2\gamma - 1, k_2 - \gamma - 1, \epsilon)$-non-malleable extractor, $W$ and $\tilde{a}' \parallel |B|$ are independent, (7) and that $H_\infty(\tilde{a}' \parallel |B|) \geq k_2$, it holds that

$$\Delta(R_B = \text{nmExt}(W, \tilde{a}' \parallel |B|); U_{m+2\alpha}|R_A = \text{nmExt}(f(W), g(\tilde{a}' \parallel |B|)), \tilde{a}' \parallel |B|) \leq \epsilon.$$  

This implies that the probability that $[R_A]'_\alpha = [R_B]_\alpha$, and hence $S_B \neq \perp$, is at most $\epsilon + 2^{-\alpha}$, which we add to $\delta$ via a union bound.
3. **Eve is active and Bob is corrupted**: The reasoning follows analogously to the previous case, but we set \((\tilde{W}, \tilde{B}) = F(W, B)\) and fix \(B\) and \(\tilde{B}\) instead.

We present a corollary of Theorem 6 to showcase that strong non-malleable two-source extractors with good parameters yield privacy amplification protocols against memory-tampering active adversaries with likewise good parameters.

**Corollary 2.** Suppose that for some constant \(\delta > 0\) there exists a strong \((k = \delta n, \varepsilon, r = 1)\)-non-malleable extractor \(\text{nmExt} : \{0, 1\}^n \rightarrow \{0, 1\}^n \rightarrow \{0, 1\}^{m'}\) with \(m' = \Omega(n)\). Then, there exists an \((r = 4, \ell_1 = n, k_1 = 3\delta n, \ell_2 = 1.5\delta n, k_2 = 1.1\delta n, m = \Omega(n), \varepsilon, \delta = \varepsilon + 2^{-\Omega(n)}\)-privacy amplification protocol against memory-tampering active adversaries. Moreover, the protocol is explicit if \(\text{nmExt}\) is explicit.

We currently do not know explicit constructions of non-malleable two-source extractors with parameters matching those required for Corollary 2, although it is known that there exist such (inefficient) extractors with significantly better parameters [CGGL20]. Thus, we leave this connection between non-malleable two-source extractors and privacy amplification with a very strong adversary as an interesting motivation for further study of such extractors with lower min-entropy requirement in the information-theoretic setting. In Section 8, we show that we can construct explicit privacy amplification protocols against memory-tampering active adversaries in the computational setting from computational strong non-malleable two-source extractors.

### 4 From slightly better non-malleable extractors to great two-source extractors

In this section, we show that slight improvements on the state-of-the-art explicit constructions of non-malleable two-source extractors [CGL16, Li17] are enough to obtain low error two-source extractors for low linear min-entropy. More precisely, we have the following result.

**Theorem 7.** For every constant \(\delta > 0\) there exists a constant \(C_\delta > 0\) such that the following holds:

If for \(m\) large enough and some \(\gamma = \gamma(m) \geq 1/m\) there exists an explicit \((m(1-\gamma) 3 log m, \varepsilon, C_\delta \cdot (1/\gamma)^6)\)-non-malleable extractor \(\text{nmExt} : \{0, 1\}^m \times \{0, 1\}^m \rightarrow \{0, 1\}\), then there exists an explicit \((\delta n, \varepsilon')\)-extractor \(\text{Ext} : \{0, 1\}^n \times \{0, 1\}^n \rightarrow \{0, 1\}\) with \(\varepsilon' = \varepsilon + 2^{-\Omega(\gamma n)}\) and \(n = \Theta(m \cdot (1/\gamma)^c)\), where \(c\) is an absolute constant.

**Proof.** Let \(\text{nmExt} : \{0, 1\}^m \times \{0, 1\}^m \rightarrow \{0, 1\}\) be the non-malleable extractor with the parameters as in the theorem statement, and let \(\text{SCond} : \{0, 1\}^n \rightarrow \{0, 1\}^{m' \cdot \ell}\) be the \((\delta \rightarrow 1 - \gamma, \varepsilon)\)-somewhere condenser from Corollary 1, and \(m = m' + \lceil \log \ell \rceil\).

Consider the function \(F : \{0, 1\}^n \times \{0, 1\}^n \rightarrow \{0, 1\}\) defined as

\[
F(X, Y) = \bigoplus_{i,j \in [\ell]} \text{nmExt}(\text{SCond}(X)_i \parallel p_i, \text{SCond}(Y)_j \parallel p_j),
\]

where \(p_i\) denotes the \(\lceil \log \ell \rceil\)-bit binary representation of \(i \in [\ell]\). We prove that \(F\) is an extractor with the desired parameters.

By the properties of \(\text{SCond}\), there exist \(V, W \in \{0, 1\}^{m' \ell}\) independent somewhere-\(k'\) sources with \(k' = (1 - \gamma)m'\) such that \(\text{SCond}(X) \approx_{\varepsilon_1} V\) and \(\text{SCond}(Y) \approx_{\varepsilon_1} W\) for \(\varepsilon_1 = 2^{-\Omega(\gamma n)}\). Therefore, it suffices to show that

\[
\bigoplus_{i,j \in [\ell]} \text{nmExt}(V_i \parallel p_i, W_j \parallel p_j) \approx_{\varepsilon} U_1,
\]

(9)
and the desired result follows by combining the previous observations with the triangle inequality. By the properties of $V$ and $W$, there exist independent random variables $I, J \in [\ell]$ such that
\[ H_\infty(V_i | I = i), H_\infty(W_j | J = j) \geq (1 - \gamma)m'. \]
Consider arbitrary fixings $I = i$ and $J = j$. We show that (9) holds for all fixings, and hence it holds in general as well. Under such a fixing, it is enough to show that
\[ \Delta(\text{nmExt}(V_i || p_i, W_j || p_j); U_1(\text{nmExt}(V_{i'} || p_{i'}, W_{j'} || p_{j'}))_{(i', j') \neq (i, j)}) \leq \varepsilon. \]  
(10)
We will now use the properties of $\text{nmExt}$ to prove (10). Note that we can jointly simulate all pairs $(V_{i'} || p_{i'}, W_{j'} || p_{j'})$ for $(i', j') \neq (i, j)$ as randomized split-memory-tamperings of $(V_i || p_i, W_j || p_j)$. In other words, there exist randomized functions $g_{1'}, g_{2j'} : \{0,1\}^m \times \mathcal{R} \rightarrow \{0,1\}^m$, all sharing the same independent randomness $R \in \mathcal{R}$, such that
\[ (V_i || p_i, W_j || p_j), (g_{1'}, (V_i || p_i, R), g_{2j'}(W_j || p_j, R))_{(i', j') \neq (i, j)} \sim (V_i || p_i, W_j || p_j), (V_{i'} || p_{i'}, W_{j'} || p_{j'})_{(i', j') \neq (i, j)}. \]
Indeed, on input $(v_i || p_i, w_j || p_j)$, this can be done by sampling $V' = (V | I = i, V = v_i)$ and $W' = (W | J = j, W = w_j)$ using the extra independent randomness $R$, and setting $g_{1'}(v_i || p_i, R) = V' || p_{i'}$ and $g_{2j'}(w_j || p_j, R) = W' || p_{j'}$ for all $(i', j') \neq (i, j)$. Moreover, since $p_a \neq p_b$ for $a \neq b$, all tampering functions $g_{1'}$ and $g_{2j'}$ above have no fixed points for every fixing of the randomness. Finally, since $\ell = O((1/\gamma)^{5/2})$ and $\gamma \geq 1/m$, it follows that
\[ H_\infty(V_i || p_i), H_\infty(W_j || p_j) \geq (1 - \gamma)m' \geq (1 - \gamma)m - 3\log m \]
and that $\text{nmExt}$ handles at least $\ell^2 \leq C_\delta(1/\gamma)^5$ tamperings for a suitable constant $C_\delta > 0$ depending only on $\delta$. Taking into account these observations and noting that $V_i || p_i$ and $W_j || p_j$ are independent, we can invoke Lemma 4 to conclude (10) holds, which completes the proof.

We now present two remarkable corollaries of Theorem 7, one of which was already informally presented in Section 1.2.

**Corollary 3.** Suppose that for some $r = r(m) = \omega(1)$, $\varepsilon = \varepsilon(m)$, and some constant $c > 0$ there is an explicit $(m(1 - \gamma), \varepsilon, r)$-non-malleable extractor for large enough $m$. Then, for any constant $\delta > 0$ and large enough $n$ there exists an explicit $(\delta n, \varepsilon')$-extractor with $\varepsilon' = \varepsilon(\Omega(n)) + 2^{-\Omega(n)}$.

**Corollary 4.** There exists an absolute constant $\alpha > 0$ such that if for some constant $\beta < \alpha$ there exists an explicit $(m - m^{1-\beta}, \varepsilon, m^{\beta})$-non-malleable extractor $\text{nmExt} : \{0,1\}^m \times \{0,1\}^m \rightarrow \{0,1\}$, then for any constant $\delta > 0$ and large enough $n$ there exists an explicit $(\delta n, \varepsilon')$-extractor with $\varepsilon' = \varepsilon(\Omega(1)) + 2^{-n^{\Omega(1)}}$.

According to Corollary 4, improving the min-entropy requirement of the CGL extractor in Proposition 4 to $m - m^{\alpha_0}$ for a sufficiently small constant $\alpha_0 > 0$ would immediately yield explicit low error two-source extractors for any linear min-entropy rate.

5 Side quest: From slightly better non-malleable extractors to great computational non-malleable extractors under standard assumptions

In this section, we show how the construction used to prove Theorem 7 can also be used to obtain computational non-malleable extractors for low min-entropy efficiently samplable sources, efficient
tampering, and a \textit{computationally unbounded} distinguisher from slight improvements on the state-of-the-art constructions of non-malleable extractors for high min-entropy sources. This can be achieved under the weak hardness assumption that families of collision-resistant hash functions with decent parameters exist.

\textbf{Theorem 8.} For every constant $\delta > 0$ there exists a constant $C_\delta > 0$ such that the following holds:

If for $m$ large enough and some $\gamma = \gamma(m) \geq 1/m$ there exists an explicit $(m(1 - \gamma) - 3 \log m - m_h, \epsilon = \text{negl}(m), C_\delta \cdot (1/\gamma)^5)$-non-malleable extractor $\text{nmExt} : \{0, 1\}^m \times \{0, 1\}^m \rightarrow \{0, 1\}$, then there exists an explicit $(\text{poly}(n), \text{poly}(n), \infty, k = \delta n, \epsilon = \text{negl}(m), r = 1)$-non-malleable extractor $\text{cnmExt} : \{0, 1\}^n \times \{0, 1\}^n \rightarrow \{0, 1\}$ in the CRS model without auxiliary information with $n = \Theta(m \cdot (1/\gamma)^5)$, where $c$ is an absolute constant, provided that there exists a family $\mathcal{H}$ of $(\text{poly}(n), \text{negl}(n))$-collision-resistant hash functions $h : \{0, 1\}^n \rightarrow \{0, 1\}^{m_h}$ with $m_h = o(n)$.

\textbf{Proof.} Towards proving the desired statement, we modify the construction used to prove Theorem 7 by including the hashes of the sources in the input to $\text{nmExt}$. More precisely, we set $\text{CRS} = H$ for $H \leftarrow \mathcal{H}$, and consider the function $\text{cnmExt} : \{0, 1\}^n \times \{0, 1\}^n \times \mathcal{H} \rightarrow \{0, 1\}$ defined as

$$\text{cnmExt}(X, Y, H) = \bigoplus_{i,j \in [\ell]} \text{nmExt}(\text{SCond}(X)_i \| p_i \| H(X), \text{SCond}(Y)_j \| p_j \| H(Y)),$$

where $\text{nmExt}$ is as in the theorem statement, $\text{SCond} : \{0, 1\}^n \rightarrow \{0, 1\}^{m' \cdot \ell}$ is the $(\delta/2 \rightarrow 1 - \gamma, \epsilon_1)$-somewhere condenser from Corollary 1, $p_i$ denotes the $[\log \ell]$-bit binary representation of $i$, and $m = m' + [\log \ell] + m_h$.

Fix $(t, \delta n)$-samplable sources $X$ and $Y$ and size-$\text{poly}(t)$ deterministic tampering functions $g_1, g_2 : \{0, 1\}^n \times \mathcal{H} \rightarrow \{0, 1\}^n$ such that for each $h \in \mathcal{H}$, one of $g_1(\cdot, h)$ and $g_2(\cdot, h)$ has no fixed points. Our goal is to show that

$$\text{cnmExt}(X, Y, H), \text{cnmExt}(X', Y', H), H \approx_1 U_1, \text{cnmExt}(X', Y', H), H,$$

\hspace{1cm} (11)

where $X' = g_1(X, H)$ and $Y' = g_2(Y, H)$, and $\epsilon = \text{negl}(n)$. We begin by claiming that the collision-resistance of $\mathcal{H}$ ensures that

$$\Pr_H[X \neq X', H(X) = H(X')] = \text{negl}(n),$$

$$\Pr_H[Y \neq Y', H(Y) = H(Y')] = \text{negl}(n).$$

Indeed, if this does not hold, then we can break the collision-resistance of $\mathcal{H}$ by considering the size-$\text{poly}(t)$ adversary that on input $H \leftarrow \mathcal{H}$ first samples $(X, Y)$, and then outputs either $(X, X')$ or $(Y, Y')$ with probability $1/2$. Since one of $g_1(\cdot, h)$ and $g_2(\cdot, h)$ has no fixed points for each fixing $H = h$, this adversary succeeds with non-negligible probability. With this in mind, with probability $1 - \text{negl}(n)$ over the fixing $H = h$, we have $\Pr[X \neq X', h(X) = h(X')] = \text{negl}(n)$ and $\Pr[Y \neq Y', h(Y) = h(Y')] = \text{negl}(n)$. Throughout the remainder of the proof we can fix such $h \in \mathcal{H}$ and assume that $g_1(\cdot, h)$ has no fixed points without loss of generality. Moreover, we will also condition $X$ on the events $h(X) \neq h(X')$ and $h(X) = z_1$ and $Y$ on the event $h(Y) = z_2$ from now on. Since $h(X) \neq h(X')$ holds with probability $1 - \text{negl}(n)$, by Lemmas 1 and 2 we have

$$H_\infty(X|h(X) \neq h(X'), h(X) = z_1) \geq \delta n - 1 - m_h - \text{negl}(n) \geq \delta n/2$$

with probability $1 - \text{negl}(n)$ over the choice of $z_1$. Likewise, we have $H_\infty(Y|h(Y) = z_2) \geq \delta n/2$ with probability $1 - \text{negl}(n)$ over the choice of $z_2$. From here onwards, fix such $z_1$ and $z_2$. 

22
Given the fixings in the previous paragraph, by the properties of $\text{SCond}$ there exist independent somewhere-$k'$ sources $V, W \in \{0, 1\}^{m \ell}$ with $k' = (1 - \gamma)m'$ and independent random variables $I, J \in [\ell]$ such that $\text{SCond}(X) \approx \varepsilon_1$, $V$ and $\text{SCond}(Y) \approx \varepsilon_1$, $W$, and

\[
H_\infty(V_i | I = i) \geq (1 - \gamma)m' \geq (1 - \gamma)m - 3\log m - m_0, \quad (12)
\]
\[
H_\infty(W_j | J = j) \geq (1 - \gamma)m' \geq (1 - \gamma)m - 3\log m - m_0. \quad (13)
\]

for all valid fixings $I = i$ and $J = j$. We now wish to proceed by replacing $\text{SCond}(X)$ and $\text{SCond}(Y)$ by $V$ and $W$, respectively, in our analysis. Observe that we can write $A(\text{SCond}(X)) = \langle \text{SCond}(X'), i || h(X') \rangle_{i \in [\ell]}$ for a randomized function $A$ that on input $v$ samples $x$ from $(X | \text{SCond}(X) = v)$ and sets $A(v) = \langle \text{SCond}(g_1(x, h)), i || h(g_1(x, h)) \rangle_{i \in [\ell]}$ (if the sampling of $x$ fails, simply output a fixed bitstring whose suffix differs from $z_1$). By our conditioning, we may assume that $A(v) \neq v || i || z_1$ for all $i \in [\ell]$. Analogously to the proof of Theorem 7, we can write $B(\text{SCond}(Y)) = \langle \text{SCond}(Y'), j || h(Y') \rangle_{j \in [\ell]}$ for a randomized function $B$. Therefore, it now suffices to show that

\[
\bigoplus_{i,j \in [\ell]} \text{nmExt}(\text{SCond}(X)_i || i || z_1, \text{SCond}(Y)_j || j || z_2), \bigoplus_{i,j \in [\ell]} \text{nmExt}(A(\text{SCond}(X))_i, B(\text{SCond}(Y))_j)
\]

\[
\approx \varepsilon_1 U_1, \bigoplus_{i,j \in [\ell]} \text{nmExt}(A(\text{SCond}(X))_i, B(\text{SCond}(Y))_j). \quad (14)
\]

Using the fact that $\text{SCond}(X), \text{SCond}(Y) \approx \varepsilon_1$, $V, W$, the condition in (14) follows if we show that

\[
\bigoplus_{i,j \in [\ell]} \text{nmExt}(V_i || i || z_1, W_j || j || z_2), \bigoplus_{i,j \in [\ell]} \text{nmExt}(A(V)_i, B(W)_j)
\]

\[
\approx \varepsilon_1 U_1, \bigoplus_{i,j \in [\ell]} \text{nmExt}(A(V)_i, B(W)_j). \quad (15)
\]

Consider arbitrary fixings $I = i^*$ and $J = j^*$. We show that then we have

\[
\Delta(\text{nmExt}(V_{i^*} || i || z_1, W_{j^*} || j || z_2)); U_1
\]

\[
\left(\text{nmExt}(V_{i^*} || i || z_1, W_{j^*} || j || z_2)_{(i,j) \neq (i^*, j^*)}, \text{nmExt}(A(V)_i, B(W)_j)_{i,j \in [\ell]} \right) \leq \varepsilon, \quad (16)
\]

which implies (15) and concludes the proof. Analogously to the proof of Theorem 7, we can write $g_{11}^1(V_{i^*} || i || z_1, R) = V_i || i || z_1$ and $g_{12}^2(W_{j^*} || j || z_2, R) = W_j || j || z_2$ for randomized tampering functions $g_{11}^1, g_{12}^2 : \{0, 1\}^m \times R \rightarrow \{0, 1\}^m$ for $i \neq i^*$ and $j \neq j^*$. Observe that the $g_{11}^1$’s and $g_{12}^2$’s have no fixed points, since $p_i \neq p_i^*$ and $p_j \neq p_j^*$. Moreover, we can also write $g_{21}^2(V_{i^*} || i || z_1, R) = A(V)_i$ and $g_{22}^2(W_{j^*} || j || z_2, R) = B(W)_j$ for randomized tampering functions $g_{21}^2, g_{22}^2 : \{0, 1\}^m \times R \rightarrow \{0, 1\}^m$ for $i \neq i^*$. By our previous conditioning, we know that $g_{11}^1$ has no fixed points, i.e., $g_{11}^1(V_{i^*} || i || z_1, r) \neq V_{i^*} || i || z_1$ for all $r$. Finally, since there are at most $2\ell^2 \leq C_\delta(1/\gamma)^5$ tamperings for a suitably large constant $C_\delta$ depending only on $\delta$, and since $V_{i^*} || p_{i^*} || z_1$ and $W_{j^*} || p_{j^*} || z_2$ are independent and $H_\infty(V_{i^*} || p_{i^*} || z_2), H_\infty(W_{j^*} || p_{j^*} || z_2) \geq (1 - \gamma)m - 3\log m - m_0$ by (12) and (13), we can invoke Lemma 4 to conclude (16) holds, which completes the proof.

Similarly to the previous section, we present two corollaries that are especially meaningful given the current state-of-the-art constructions of non-malleable two-source extractors [CGL16, Li17], one of which was already informally presented in Section 1.2.
Corollary 5. Suppose that for some \( r = r(m) = \omega(1) \), \( \varepsilon = \text{negl}(m) \), and some constant \( c > 0 \) there is an explicit \((m(1 - \gamma), \varepsilon, r)\)-non-malleable extractor for large enough \( m \). Then, for any constant \( \delta > 0 \) and large enough \( n \) there exists an explicit \((\text{poly}(n), \text{poly}(n), \infty, k = \delta n, \varepsilon = \text{negl}(n), r = 1)\)-non-malleable extractor in the CRS model without auxiliary information, provided that there exists a family \( H \) of \((\text{poly}(n), \text{negl}(n))\)-collision resistant hash functions \( h : \{0,1\}^n \rightarrow \{0,1\}^{m_h} \) with \( m_h = o(n) \).

Corollary 6. There exists an absolute constant \( \alpha > 0 \) such that if for some constant \( \beta < \alpha \) there exists an explicit \((m - m^{1-\beta}, \varepsilon = \text{negl}(m), m^{6\beta})\)-non-malleable extractor \( \text{nmExt} : \{0,1\}^m \times \{0,1\}^m \rightarrow \{0,1\} \), then for any constant \( \delta > 0 \) and large enough \( n \) there exists an explicit \((\text{poly}(n), \text{poly}(n), \infty, k = \delta n, \varepsilon = \text{negl}(n), r = 1)\)-non-malleable extractor in the CRS model without auxiliary information, provided that there exists a family \( H \) of \((\text{poly}(n), \text{negl}(n))\)-collision resistant hash functions \( h : \{0,1\}^n \rightarrow \{0,1\}^{m_h} \) with \( m_h \leq n^\rho \) for a small enough constant \( \rho > 0 \).

6 Computational non-malleable extractors from quasi-polynomial hardness assumptions

In this section, we construct computational non-malleable two-source extractors in the CRS model assuming the quasi-polynomial hardness of the DDH assumption. We begin by constructing such a non-malleable extractor for relatively high min-entropy that handles many tamperings. Then, we use this construction as a stepping stone to obtain a non-malleable extractor in the CRS model for low min-entropy.

Theorem 9. Suppose the following objects exist:

- A family \( \mathcal{H}_1 \) of \((\text{poly}(t_{11}), \text{negl}(t_{11}))\)-collision-resistant hash functions \( h : \{0,1\}^n \rightarrow \{0,1\}^\ell_1 \);
- A family \( \mathcal{H}_2 \) of \((\text{poly}(t_{12}), \text{negl}(t_{12}))\)-collision-resistant hash functions \( h : \{0,1\}^n \rightarrow \{0,1\}^\ell_2 \);
- A family of \((\text{poly}(t_2), n, \omega)\)-lossy functions \( F \), where \( t_2 \geq 2^{\ell_1 + \ell_2} \), with \( 2^{\ell_1} = t_{11}^{\omega(1)} \), \( 2^{\ell_2} = t_{12}^{\omega(1)} \), and \( \omega = n - n^\gamma \) for some constant \( \gamma \in (0,1) \);
- A strong \((k_1, k_2, \varepsilon)\)-extractor \( \text{Ext} : \{0,1\}^n \times \{0,1\}^n \rightarrow \{0,1\}^m \), where \( \Omega(t_1) \leq n \leq \text{poly}(t_1) \) for \( t_1 = \min(t_{11}, t_{12}) \).

Then, there exists an explicit \((\text{poly}(t_{11}), \text{poly}(t_{12}), \text{poly}(t_1), \text{poly}(t_2), k'_1 = k_1 + r(2\ell_1 + 2n^\gamma), k'_2 = k_2 + r(2\ell_2 + m + \log^2 n), \varepsilon + \text{negl}(n), r)\)-non-malleable extractor \( \text{nmExt} : \{0,1\}^n \times \{0,1\}^n \rightarrow \{0,1\}^m \) in the CRS model.

We instantiate Theorem 9 with the best known explicit statistical two-source extractors in Section 6.2.

6.1 Proof of Theorem 9

Our candidate construction is as follows: First, to define CRS, begin by sampling \( b \leftarrow \{0,1\}^{\ell} \), where \( \ell = \ell_1 + \ell_2 \), and then sample functions \( f_{ij} \) from \( F \) for \( i \in [\ell] \) and \( j \in \{0,1\} \) such that \( f_{ib_i} \) is injective and \( f_{i1-b_i} \) is lossy for each \( i \). Finally, sample \( h_1 \leftarrow \mathcal{H}_1 \) and \( h_2 \leftarrow \mathcal{H}_2 \), and set

\[
\text{CRS} = (h_1, h_2, (f_{ij})_{i \in [\ell], j \in \{0,1\}}) \in \{0,1\}^c.
\]
Our function $\text{cnmExt} : \{0,1\}^n \times \{0,1\}^n \times \{0,1\}^c \rightarrow \{0,1\}$ is defined as

$$\text{cnmExt}(x, y, \text{CRS}) = \text{Ext}(f_{h_1(x)}[h_2(y)](x), y),$$

where for $a \in \{0,1\}$ we denote $f_a(x) = f_{1a_1}(f_{2a_2}(\cdots(f_{la_l}(x))\cdots)).$

For the sake of exposition, we present the proof for the case $r = 1$ only. The extension to $r > 1$ tamperings is straightforward. In order to show Theorem 9, we must argue that, for arbitrary $(\text{poly}(t_{11}), \text{poly}(t_{12}), k'_1, k'_2)$-samplable sources $(X, Y, \text{AUX})$, valid size-$\text{poly}(t_1)$ tampering functions $g_1 : \{0,1\}^n \times \{0,1\}^c \rightarrow \{0,1\}^n$ and $g_2 : \{0,1\}^n \times \{0,1\}^n \times \{0,1\}^c \rightarrow \{0,1\}^n$, and every size-$\text{poly}(t_2)$ distinguisher $\mathcal{A}$ it holds that

$$|\Pr[\mathcal{A}(\text{cnmExt}(X, Y, \text{CRS}), \text{cnmExt}(\overline{X}, \overline{Y}, \text{CRS}), \text{AUX}, \text{CRS}) = 1] - \Pr[\mathcal{A}(U_1, \text{cnmExt}(\overline{X}, \overline{Y}, \text{CRS}), \text{AUX}, \text{CRS}) = 1]| \leq \varepsilon + \text{negl}(t_1), \quad (17)$$

where $\overline{X} = g_1(X, \text{CRS})$ and $\overline{Y} = g_2(Y, \text{AUX}, \text{CRS})$. As a first step, we prove that it suffices to consider cases where $h(X) || h(Y) \neq h(\overline{X}) || h(\overline{Y})$ and $h(X) || h(Y) = b$, where $b$ denotes the indices of the injective functions $(f_{h_b}), h \in [\ell]$.

**Lemma 9.** Let $\mathcal{E}$ denote the event that $h_1(X) || h_2(Y) \neq h_1(\overline{X}) || h_2(\overline{Y})$ and $h_1(X) || h_2(Y) = b$ hold simultaneously. Then, if

$$|\Pr[\mathcal{A}(\text{cnmExt}(X, Y, \text{CRS}), \text{cnmExt}(\overline{X}, \overline{Y}, \text{CRS}), \text{AUX}, \text{CRS}) = 1|E]\Pr[\mathcal{A}(U_1, \text{cnmExt}(\overline{X}, \overline{Y}, \text{CRS}), \text{AUX}, \text{CRS}) = 1|E]| \leq \varepsilon + \text{negl}(t_1), \quad (18)$$

it follows that (17) holds.

**Proof.** We proceed similarly to the proof of the analogous claim in [GKK20]. Suppose that (18) holds for every tuple of $(\text{poly}(t_{11}), \text{poly}(t_{12}), k'_1, k'_2)$-samplable sources $(X, Y, \text{AUX})$, tampering functions $g_1$ and $g_2$, and size-$\text{poly}(t_2)$ adversary $\mathcal{A}$, but

$$|\Pr[\mathcal{A}(\text{cnmExt}(X, Y, \text{CRS}), \text{cnmExt}(\overline{X}, \overline{Y}, \text{CRS}), \text{AUX}, \text{CRS}) = 1] - \Pr[\mathcal{A}(U_1, \text{cnmExt}(\overline{X}, \overline{Y}, \text{CRS}), \text{AUX}, \text{CRS}) = 1]| > \varepsilon + 1/p(t_1), \quad (19)$$

where $\overline{X} = g_1(X, \text{CRS})$ and $\overline{Y} = g_2(Y, \text{AUX}, \text{CRS})$, for some pair of $(\text{poly}(t_{11}), \text{poly}(t_{12}), k'_1, k'_2)$-samplable sources $(X, Y, \text{AUX})$, some tampering functions $g_1$ and $g_2$, some size-$\text{poly}(t_2)$ adversary $\mathcal{A}$, and some polynomial $p$. We show that this breaks the $t_2$-security of the family of lossy functions $\mathcal{F}$. By the $t_2$-security of $\mathcal{F}$, we know that for every size-$\text{poly}(t_2)$ adversary $\mathcal{B}$ we have

$$2^{-t} - \text{negl}(t_2) \leq \Pr[\mathcal{B}(\text{CRS}) = b] \leq 2^{-t} + \text{negl}(t_2). \quad (20)$$

Consider the size-$\text{poly}(t_2)$ adversary $\mathcal{B}$ that on input $\text{CRS}$ samples $(X, Y, \text{AUX})$, and first checks whether $h_1(X) || h_2(Y) \neq h_1(\overline{X}) || h_2(\overline{Y})$. If that is the case, then $\mathcal{B}$ outputs $b' \leftarrow h_1(X) || h_2(Y)$ as a guess for $b$, else it outputs $b' \leftarrow \{0,1\}^\ell$. Since $\Pr[h_1(X) || h_2(Y) = h_1(\overline{X}) || h_2(\overline{Y})] = \text{negl}(t_1)$ by the collision-resistance of $\mathcal{H}$ and the fact that $\overline{X} \neq X$ or $\overline{Y} \neq Y$ by hypothesis, using (20) we have that

$$(1 - \text{negl}(t_1))2^{-t} - \text{negl}(t_2) \leq \Pr[h_1(X) || h_2(Y) = b, h(X) || h(Y) \neq h(\overline{X}) || h(\overline{Y})] \leq (1 + \text{negl}(t_1))2^{-t} + \text{negl}(t_2). \quad (21)$$

We now proceed to construct a size-$\text{poly}(t_2)$ adversary $\mathcal{B}'$ such that

$$\Pr[\mathcal{B}'(\text{CRS}) = b] \geq 1.5 \cdot 2^{-t}.$$

This contradicts (20), which concludes the proof. On input $\text{CRS}$ and for $N = p(t_{11} + t_{12})^3$, $\mathcal{B}'$ proceeds as follows:
1. Sample \((X, Y, AUX)\) from \(CRS\). If \(h_1(X)\|h_2(Y) = h_1(\overline{X})\|h_2(\overline{Y})\), then re-sample. Otherwise, set \(z = h_1(X)\|h_2(Y)\). Note that this takes time \(\text{poly}(t_{11} + t_{12})\).

2. For \(i \in [N]\): Sample \((X_i, Y_i, AUX_i)\) from \(CRS\) conditioned on \(h_1(X_i)\|h_2(Y_i) = z\) and \(h_1(X_i)\|h_2(Y_i) \neq h(\overline{X}_i)\|h(\overline{Y}_i)\). By (21) and the fact that \(2^t = \text{poly}(t_2)\), this takes time \(\text{poly}(t_2)\). Set

\[
\delta_i = |A(\text{cnmExt}(X_i, Y_i, CRS), \text{cnmExt}(\overline{X}_i, \overline{Y}_i, CRS), AUX_i, CRS) - A(U_m, \text{cnmExt}(\overline{X}_i, \overline{Y}_i, CRS), AUX_i, CRS)|,
\]

where \(\overline{X}_i = g_1(X_i, CRS)\) and \(\overline{Y}_i = g_2(Y_i, AUX_i, CRS)\). Note that \(A\) has size \(\text{poly}(t_2)\).

3. Compute \(\delta = \frac{1}{N} \sum_{i=1}^{N} \delta_i\). If \(\delta < \epsilon + \frac{1}{4p(t_{11} + t_{12})}\), then output \(b' = z\). Else, output \(b' \triangleq \{0, 1\}^{2^\ell}\).

We now show that \(\Pr[b' = b] \geq 1.5 \cdot 2^{-\ell}\). It holds that \(\mathbb{E}[\delta | z = b] \leq \epsilon + \text{negl}(t_1) < \epsilon + \frac{1}{2p(t_1)}\). On the other hand, by (19) and (21) we have \(\mathbb{E}[\delta | z \neq b] \geq \epsilon + \frac{1}{2p(t_1)}\). By the Chernoff bound and the choice of \(N = p(t_{11} + t_{12})^3\), we then have

\[
\Pr[b' = b | z = b] = \Pr\left[\delta < \epsilon + \frac{1}{4p(t_1)} \bigg| z = b\right] \geq 1 - \exp(-\Omega(p(t_1))) = 1 - \text{negl}(t_1),
\]

and

\[
\Pr\left[\delta \geq \epsilon + \frac{1}{4p(t_1)} \bigg| z \neq b\right] \geq 1 - \exp(-\Omega(p(t_1))) = 1 - \text{negl}(t_1).
\]

The latter inequality then implies that \(\Pr[b' = b | z \neq b] \geq (1 - \text{negl}(t_1))2^{-\ell}\). Combining these observations with (21) yields

\[
\Pr[b' = b] \geq (2 - \text{negl}(t_1))2^{-\ell} \geq 1.5 \cdot 2^{-\ell},
\]

which contradicts (20), as desired. 

Based on Lemma 9, we can now work under the assumption that the event \(E\) holds and show (18). According to the definition of \(\text{cnmExt}\), in order to prove that (18) holds it is now enough to show that for every size-\(\text{poly}(t_2)\) distinguisher \(\mathcal{A}'\) we have

\[
| \Pr[\mathcal{A}'(\text{Ext}(f_b(X), Y), \text{SideInfo}, AUX, CRS) = 1 | E] - \Pr[\mathcal{A}'(U_m, \text{SideInfo}, AUX, CRS) = 1 | E]| \leq \epsilon + \text{negl}(t_1), \tag{22}
\]

where

\[
\text{SideInfo} = (h_1(X), h_1(\overline{X}), h_2(Y), h_2(\overline{Y}), f_{h_1(X)||h_2(Y)}(\overline{X}), \text{cnmExt}(\overline{X}, \overline{Y}, CRS)).
\]

With this in mind, consider an arbitrary fixing of the side information \(\text{CRS} = \text{crs}\), \(h_1(X)\|h_2(Y) = b = b_1\|b_2, h_1(\overline{X})\|h_2(\overline{Y}) = b' = b'_1\|b'_2\) with \(b' \neq b, f_{b'_1}(\overline{X}) = z', \) and \(\text{cnmExt}(\overline{X}, \overline{Y}, \text{crs}) = y'\). Observe that, under such a fixing, the event \(E\) holds and \(X\) and \(Y\) are independent. This is because, after fixing \(\text{CRS}, h_1(\overline{X})\|h_2(\overline{Y}),\) and \(f_{b'_1}(\overline{X}),\) we have that \(\text{cnmExt}(\overline{X}, \overline{Y}) = \text{Ext}(f_{b'_1}(\overline{X}), \overline{Y})\) is a deterministic function of \(\overline{Y}\). Therefore, it is now enough to show that

\[
| \Pr[\mathcal{A}'(\text{Ext}(f_b(X), Y), b, b', z', y', AUX, crs) = 1] - \Pr[\mathcal{A}'(U_m, b, b', z', y', AUX, crs) = 1]| \leq \epsilon \tag{23}
\]

for arbitrary \(\mathcal{A}'\) with probability \(1 - \text{negl}(t_1)\) over the choice of fixings above.
Note that, by Lemmas 1 and 2, with probability at least \(1 - \text{negl}(t_1)\) over the fixings we have
\[
H_\infty(f_b(X)|\text{CRS}) = \text{crs}, h_1(X) = b_1, h_1(\overline{X}) = b_1', f_{b'}(\overline{X}) = z' \geq k_1' - 2\ell_1 - n^\gamma - \log^2 n
\]
\[
\geq k_1,
\]
since \(f_b\) is injective, \(|h_1(X)| = |h_1(\overline{X})| = \ell_1, \) \(n = \Omega(t_1),\) and \(f_{b'}(\overline{X})\) takes on at most \(2^{n^\gamma}\) values because \(b' \neq b\) (and so at least one index in \(f_{b'}\) corresponds to a lossy function). Moreover, we also have
\[
H_\infty(Y|\text{CRS}) = \text{crs}, h_2(Y) = b_2, h_2(\overline{Y}) = b_2', \text{Ext}(z', \overline{Y}) = y' \geq k_2' - 2\ell_2 - m - \log^2 n
\]
\[
\geq k_2,
\]
since \(|h(Y)| = |h(\overline{Y})| = \ell_2, \) \(|\text{Ext}(z', \overline{Y})| = m,\) and \(n = \Omega(t_1).\) The desired inequality in (23) now follows immediately by noting that \(\text{Ext}\) is a strong \((k_1, k_2, \varepsilon)\)-extractor and that, after fixing \(\text{CRS}, \) \(\text{AUX}\) is a (possibly randomized) function of \(Y\) only.

### 6.2 Instantiations of Theorem 9

In this section, we instantiate Theorem 9 with the explicit statistical two-source extractors presented in Section 2. Throughout this section, we set the following parameters
\[
\Omega(\lambda) \leq n \leq \text{poly}(\lambda), t_1 = \lambda, t_2 = \lambda^{\log \lambda},
\]
where \(\lambda\) is the security parameter. Then, the quasi-polynomial hardness of the DDH assumption allows us to assume the existence of the following objects:

- A family \(\mathcal{H}\) of \((\text{poly}(t_1), \text{negl}(t_1))\)-collision-resistant hash functions \(h : \{0, 1\}^n \rightarrow \{0, 1\}^\ell,\) where \(\ell = \log \lambda \cdot \log \log \lambda.\) Then, we set \(\mathcal{H}_1 = \mathcal{H}_2 = \mathcal{H}\) and \(t_{11} = t_{12} = t_1\) in Theorem 9.

- A family of \((t_2, n, \omega)\)-lossy functions \(\mathcal{F},\) where \(t_2 \geq 2^{2\ell} = t_1^{\omega(1)}\) and \(\omega = n - n^\gamma\) for some constant \(\gamma \in (0, 1).\)

Using Bourgain’s extractor (Proposition 1), we immediately obtain the following corollary.

**Corollary 7.** Assuming quasi-polynomial hardness of the DDH assumption and for any \(n, t_1, \) and \(t_2\) satisfying
\[
\Omega(\lambda) \leq n \leq \text{poly}(\lambda), t_1 = \lambda, t_2 = \lambda^{\log \lambda},
\]
there exists an explicit \((\text{poly}(t_1), \text{poly}(t_1), \text{poly}(t_2), k' = 0.46n, \varepsilon = \text{negl}(t_1), r = \Omega(n^{1-\gamma}))\)-non-malleable extractor \(\text{cnmExt} : \{0, 1\}^n \times \{0, 1\}^n \rightarrow \{0, 1\}\) in the CRS model.

Using Raz’s extractor (Proposition 2), we obtain the following corollary.

**Corollary 8.** Assuming quasi-polynomial hardness of the DDH assumption and for any \(n, t_1, \) and \(t_2\) satisfying
\[
\Omega(\lambda) \leq n \leq \text{poly}(\lambda), t_1 = \lambda, t_2 = \lambda^{\log \lambda},
\]
for all constants \(\delta, r > 0\) there exists an explicit \((\text{poly}(t_1), \text{poly}(t_1), \text{poly}(t_2), k'_1 = (1/2 + \delta)n, k'_2 = \log^3 n, \varepsilon = \text{negl}(t_1), r)\)-non-malleable extractor \(\text{cnmExt} : \{0, 1\}^n \times \{0, 1\}^n \rightarrow \{0, 1\}\) in the CRS model.

Finally, using the Chattopadhyay-Zuckerman extractor (Proposition 3), we obtain the following corollary.
Corollary 9. Assuming quasi-polynomial hardness of the DDH assumption and for any \( n, t_1, \) and \( t_2 \) satisfying
\[
\Omega(\lambda) \leq n \leq \text{poly}(\lambda), t_1 = \lambda, t_2 = \lambda^\log \lambda,
\]
for every constant \( 1 > c > \gamma \) there exists an explicit \((\text{poly}(t_1), \text{poly}(t_1), \text{poly}(t_2), k' = O(n^c), \varepsilon = t_1^{-\Omega(1)}, r = \Omega(n^{c-\gamma})\))-non-malleable extractor \( \text{cnmExt} : \{0,1\}^n \times \{0,1\}^n \rightarrow \{0,1\} \) in the CRS model.

7 A simple non-malleable extractor in the CRS model from nearly optimal collision-resistant hash functions

In this section, we present a simple construction of a non-malleable extractor in the CRS model against computationally bounded samplers and tamperings and against a computationally unbounded distinguisher that can be instantiated from families of nearly optimal collision-resistant hash functions and high min-entropy information-theoretic non-malleable extractors. To be precise, we have the following result.

**Theorem 10.** Suppose \( \mathcal{H} \) is a family of \((3t, 2^{\beta - 1 - m} = \text{negl}(n))\)-collision-resistant hash functions \( h : \{0,1\}^n \rightarrow \{0,1\}^m \), and suppose \( \text{nmExt} : \{0,1\}^m \times \{0,1\}^m \rightarrow \{0,1\} \) is an explicit strong \((m - \beta - 2\log n, \varepsilon = \text{negl}(n), r = 1)\)-non-malleable extractor. Then, there exists an explicit \((t, t, \infty, k = m - \beta + 1, \varepsilon = \text{negl}(n), r = 1)\)-non-malleable extractor \( \text{cnmExt} : \{0,1\}^n \times \{0,1\}^n \rightarrow \{0,1\} \) in the CRS model.

Moreover, if \( \text{nmExt} \) is not strong, then \( \text{cnmExt} \) is a \((t, t, \infty, m, \beta + 1, \varepsilon = \text{negl}(n), r = 1)\)-non-malleable extractor in the CRS model without auxiliary information.

**Remark 1.** Note that, in Theorem 10, the underlying \( \text{nmExt} \) for \( m \)-bit sources and the resulting \( \text{cnmExt} \) for \( n \)-bit sources have similar min-entropy requirements. When \( n \gg m \), this means that we start with an extractor \( \text{nmExt} \) for \( m \)-bit sources with high min-entropy rate, and construct a new extractor \( \text{cnmExt} \) for \( n \)-bit sources with very low min-entropy rate.

**Theorem 10.** We set \( \text{CRS} = H \) for \( H \leftarrow \mathcal{H} \) and consider the function
\[
\text{cnmExt}(x, y, H) = \text{nmExt}(H(x), H(y)).
\]

For the sake of clarity, we present the proof for the case \( r = 1 \) only. The generalization to \( r > 1 \) tamperings is straightforward. Fix \((k = m - \beta + 1, t)\)-samplable sources \((X, Y, \text{AUX})\) and size-\( \text{poly}(t) \) deterministic tampering functions \( g_1, g_2 : \{0,1\}^n \times \mathcal{H} \rightarrow \{0,1\}^n \). Our goal is to show that
\[
\Delta(\text{nmExt}(H(X), H(Y)); U_1|H, \text{nmExt}(H(g_1(X, H)), H(g_2(Y, \text{AUX}, H)))) = \text{negl}(n). \tag{24}
\]

Consider an arbitrary fixing \( H = h \). Making use of the collision-resistance properties of \( \mathcal{H} \), with probability \( 1 - \text{negl}(n) \) over the fixing \( H = h \) it either holds that
\[
\Pr[h(X) = h(g_1(X, h))] = \text{negl}(n) \tag{25}
\]
or
\[
\Pr[h(Y) = h(g_2(Y, \text{AUX}, h))] = \text{negl}(n),
\]

since either \( g_1(\cdot, h) \) has no fixed points for any \( \text{aux} \) or \( g_2(\cdot, \text{aux}, h) \) has no fixed points. We now assume that \( g_1(\cdot, h) \) has no fixed points, in which case (25) holds. The proof for the case where \( g_2(\cdot, \text{aux}, h) \) has no fixed points for any \( \text{aux} \) is analogous. Additionally, by Lemma 7 coupled with Lemma 2, with probability \( 1 - \text{negl}(n) \) over the fixing \( H = h \) we also have
where $V, W \in \{0,1\}^m$ are independent random variables satisfying
\[
H_\infty(V), H_\infty(W) \geq m - \beta - \log^2 n.
\]

After such a fixing, it now suffices to show that
\[
\Delta(nmExt(h(X), h(Y)); U_1|nmExt(h(X'), h(Y')), AUX) = \text{negl}(n),
\]
where $X' = g_1(X, h) \neq X$ and $Y' = g_2(Y, AUX, h)$. We can see $h(X')$ and $(h(Y'), AUX)$ as randomized functions of $h(X)$ and $h(Y)$, respectively. In other words, there exist randomized functions $A$, $B$, and $C$ with shared randomness such that
\[
\text{nmExt}(h(X), h(Y)), \text{nmExt}(h(X'), h(Y')), AUX
\sim \text{nmExt}(h(X), h(Y)), \text{nmExt}(A(h(X)), B(h(Y))), C(h(Y)),
\]
where $\Pr[A(h(X)) = h(X)] = \text{negl}(n)$. Therefore, using (26), in order to prove (27) it is enough to show that
\[
\Delta(nmExt(V, W); U_1|nmExt(A(V), B(W)), C(W)) = \text{negl}(n).
\]
By (26) and the properties of $A$, it also holds that $\Pr[A(V) = V] = \text{negl}(n)$. Therefore, we can condition on the event $A(V) \neq V$ and invoke Lemma 4 with $\text{nmExt}$, $V$, and $W$ (which stay independent and have enough min-entropy after this conditioning) to conclude that (28) holds. The last statement of Theorem 10 follows by an analogous proof with a non-strong $\text{nmExt}$. □

Using the non-malleable extractor from Proposition 5 in the statement of Theorem 10, we immediately obtain the following corollary.

**Corollary 10.** Suppose $H$ is a family of $(3t, 2^{\beta-1-m})$-collision-resistant hash functions $h : \{0,1\}^n \rightarrow \{0,1\}^{m}$ for $\beta = c \cdot m$, where $c > 0$ is a small enough constant. Then, there exists an explicit $(t, t, \infty, k = m - \beta + 1, \varepsilon = \text{negl}(n), r = 1)$-non-malleable extractor $\text{cnmExt} : \{0,1\}^n \times \{0,1\}^n \rightarrow \{0,1\}$ in the CRS model.

Note that the hash output length $m$ in Corollary 10 controls the min-entropy requirement of $\text{cnmExt}$. In particular, if $m = \text{polylog}(n)$, then we obtain a low-error non-malleable two-source extractor for $\text{polylog}(n)$ min-entropy.

The birthday bound tells us that the best possible security for a hash function with $m$-bit outputs we can hope for is $(t, t^2/2^m)$-collision-resistant. In practice, there are several candidates for which brute-force is the best possible attack. Among them are the widely deployed hash functions SHA-256, SHA-512, SHA-3, and discrete logarithm (over elliptic curves) based constructions. Using any of these hash functions in Theorem 10 allows us to obtain a practical low-error non-malleable two-source extractor for sources with polylogarithmic min-entropy.

## 8 Privacy amplification against memory-tampering active adversaries in the CRS model

In this section, we focus on designing efficient privacy amplification protocols resilient against memory-tampering active adversaries in the CRS model. Informally, we consider an analogous setting to Section 3, but assuming that there is a public common reference string $\text{CRS}$, the sources $W$, $A$, and $B$ are efficiently sampleable given the $\text{CRS}$, and that the memory-tampering active adversary Eve is computationally bounded. A formal definition follows below.
Definition 16 (Protocol against memory-tampering active adversaries in the CRS model). An \((r, \lambda, \ell, k_1, \ell_2, k_2, m)\)-protocol against memory-tampering active adversaries in the CRS model 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 \(W \in \{0, 1\}^{\ell_1}\), \(A, B \in \{0, 1\}^{\ell_2}\) are independent, and \(W\) is \((\text{poly}(\lambda), k_1)\)-samplable from CRS, and \(A\) and \(B\) are both \((\text{poly}(\lambda), k_2)\)-samplable from CRS. The protocol proceeds as follows:

In the first stage, Eve submits a size-\(\text{poly}(\lambda)\) circuit \(F: \{0, 1\}^{\ell_1} \times \{0, 1\}^{\ell_2} \times \{0, 1\}^c \rightarrow \{0, 1\}^{\ell_1} \times \{0, 1\}^{\ell_2}\) and chooses one of Alice and Bob to be corrupted, so that either \((W, A)\) is replaced by \(F(W, A, \text{CRS})\) (if Alice is chosen), or \((W, B)\) is replaced by \(F(W, B, \text{CRS})\) (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 \(C_i' \leftarrow A(C_1, C_1', \ldots, C_{i-1}, C_{i-1}', C_i, \text{CRS})\), where \(A\) is a size-\(\text{poly}(\lambda)\) circuit, so that the recipient of the \(i\)-th message observes \(C_i'\). Messages \(C_i\) sent by Alice are deterministic functions of \((W, A)\), CRS, and \((C_1', C_2', \ldots, C_{i-1}')\), and messages \(C_i\) sent by Bob are deterministic functions of \((W, B)\), CRS, 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 \((W, A)\), CRS, and \((C_2', C_4', \ldots)\), and Bob outputs \(S_B \in \{0, 1\}^m \cup \{\perp\}\) as a deterministic function of \((W, B)\), CRS, and \((C_2', C_4', \ldots)\).

Definition 17 (Privacy amplification protocol against memory-tampering active adversaries in the CRS model). An \((r, \lambda, \ell_1, k_1, \ell_2, k_2, m)\)-privacy amplification protocol against memory-tampering active adversaries in the CRS model is an \((r, \lambda, \ell_1, k_1, \ell_2, k_2, m)\)-protocol against memory-tampering active adversaries in the CRS model with the following additional properties:

- **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
  \[
  S_A, C, \text{CRS} \approx^c_{\lambda} U_m, C, \text{CRS}, \tag{29}
  \]
  where \(C = (C_1, C_1', C_2, C_2', \ldots, C_r, C_r')\) denotes Eve’s view, \(U_m\) is independent of \(C\) and CRS, and \(\approx^c_{\lambda}\) denotes computational indistinguishability for all distinguishers running in time \(\text{poly}(\lambda)\).

- **Eve is active:** Then, with probability at least \(1 - \text{negl}(\lambda)\) 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 (29).

We construct an efficient privacy amplification protocol against memory-tampering active adversaries in the CRS model under a subexponential hardness assumption by combining the protocol illustrated in Figure 1 with a careful instantiation of the non-malleable two-source extractor in the CRS model from Section 6. Combining Theorem 9 with Raz’s extractor (Proposition 2), we have the following explicit non-malleable two-source extractor in the CRS model, which allows the left source to be sampled in subexponential time.

Corollary 11. Assuming the subexponential hardness of the DDH assumption, there exist constants \(0 < \gamma, \eta, c < 1\) such that for any \(0 < \nu < \eta < 1\) and \(n\) large enough there exists an explicit \((\text{poly}(2^n), \text{poly}(n), \text{poly}(n), \text{poly}(2^{\nu n}), k_1 = 0.51 n, k_2 = m + \log^3 n, \varepsilon = \text{negl}(n), r = 1)\)-non-malleable extractor in the CRS model \(\text{cmnExt}: \{0, 1\}^n \times \{0, 1\}^\ell \times \{0, 1\}^c \rightarrow \{0, 1\}^m\) for any \(m \leq cn\) and \(\ell \leq n\).
Proof. We set the parameters
\[ t_{11} = 2^{n^\nu}, t_{12} = n, t_2 = 2^{n^\eta}, \]
where \( 0 < \nu < \eta < 1 \). Therefore, we also have \( t_1 = \min(t_{11}, t_{12}) = n \). The subexponential hardness of the DDH assumption ensures that there exist constants \( 0 < \eta, \gamma < 1 \) such that for all \( 0 < \nu < \eta \), the following primitives exist:

- A family \( \mathcal{H}_1 \) of \( \text{poly}(t_{11}), \negl(t_{11}) \)-collision-resistant hash functions \( h : \{0,1\}^n \rightarrow \{0,1\}^{\ell_1} \), where \( \ell_1 = \lambda^\nu \cdot \log \lambda \);
- A family \( \mathcal{H}_2 \) of \( \text{poly}(t_{12}), \negl(t_{12}) \)-collision-resistant hash functions \( h : \{0,1\}^n \rightarrow \{0,1\}^{\ell_2} \), where \( \ell_1 = \log \lambda \cdot \log \log \lambda \);
- A family of \( (t_2, n, \omega) \)-lossy functions \( \mathcal{F} \) with \( \omega = n-n^\gamma \). Note that \( t_2 \geq 2^{\ell_1+\ell_2} \) and \( 2^{\ell_1} = t_{11}^{\omega(1)} \) and \( 2^{\ell_2} = t_{12}^{\omega(1)} \) by the choice of parameters above.

- The explicit strong \( (k_1 = 0.501n, k_2 = O(\log n), \varepsilon = 2^{-\Omega(n)}) \)-extractor \( \text{Ext} : \{0,1\}^n \times \{0,1\}^n \rightarrow \{0,1\}^m \) for any \( m \leq cn \) from Proposition 2, for some constant \( c > 0 \).

Invoking Theorem 9 with the primitives above, we conclude that there exists an explicit \( \text{poly}(2^{n^\nu}), \text{poly}(n), \text{poly}(n), \text{poly}(2^{n^\eta}), k_1', k_2', \negl(n), r = 1 \)-non-malleable extractor \( \text{cnmExt} : \{0,1\}^n \times \{0,1\}^n \times \{0,1\}^c \rightarrow \{0,1\}^m \), where \( k_1' = k_1 + 2\ell_1 + 2n^\gamma \leq 0.51n \) and \( k_2' = k_2 + 2\ell_2 + m + \log^2 n \leq m + \log^3 n \), provided \( n \) is large enough. The desired statement now follows by considering, for \( \ell \leq n \), the extractor \( \text{cnmExt} : \{0,1\}^n \times \{0,1\}^\ell \times \{0,1\}^c \rightarrow \{0,1\}^m \) defined as

\[ \text{cnmExt}(X, Y, \text{CRS}) = \text{cnmExt}'(X, Y||0^{n-\ell}, \text{CRS}), \]

and observing that \( Y||0^{n-\ell} \) is samplable by a size-\( \text{poly}(n) \) circuit if \( Y \) is too. \( \square \)

We can use the extractor from Corollary 11 to design an explicit 4-round privacy amplification protocol resilient against efficient memory-tampering active adversaries in the CRS model.

Theorem 11. Assuming the subexponential hardness of the DDH assumption, for a small enough constant \( \nu > 0 \) and every \( \log^2 \lambda \leq m \leq \lambda^\nu \), \( m + 2\log^2 \lambda + 2\log^3 \lambda + 1 \leq k_2 \leq \ell_2 \leq \lambda^\nu \) there exists an explicit \( (r = 4, \lambda, \ell_1 = \lambda, k_1 = 0.52\lambda, \ell_2, k_2, m, \varepsilon = \negl(\lambda), \delta = \negl(\lambda)) \)-privacy amplification protocol against memory-tampering active adversaries in the CRS model.

Remark 2. In fact, we may even assume that the distinguisher for the privacy amplification of Theorem 11 is allowed to run in time \( 2^{\lambda^\nu} \).

Proof of Theorem 11. We consider the 4-round protocol from Figure 1 with the explicit non-malleable two-source extractor in the CRS model \( \text{cnmExt} : \{0,1\}^\lambda \times \{0,1\}^{2\ell_2} \times \{0,1\}^c \rightarrow \{0,1\}^{m+2\alpha} \) from Corollary 11 with \( \alpha = \log^2 \lambda \). The proof is similar to the proof of Theorem 6, but we present it for completeness. Without loss of generality, we may assume that Eve is deterministic. We proceed by cases:

1. Eve is passive: Then, we have \( R_A = R_B \) (and hence \( S_A = S_B \neq \perp \)), and the desired result follows by noting that

\[ R_A = \text{cnmExt}(W, A||B, \text{CRS}), A||B, \text{CRS} \approx_{\alpha} U_{m+2\alpha}, A||B, \text{CRS}, \]

since, for every fixing \( \text{CRS} = \text{crs} \ W \) is independent of \( A||B \), \( W \) is \( \text{poly}(\lambda), k_1 \)-samplable from \( \text{CRS} \), and \( (A||B, \text{AUX} = A||B) \) is \( \text{poly}(\lambda), 2k_2 \)-samplable from \( \text{CRS} \). This implies that \( S_A, C \approx_{\alpha} U_m, C, \) where \( C = (A, B, [R_A]_{2\alpha}) \) denotes Eve’s view.
2. **Eve is active and Alice is corrupted:** Denote \((\hat{W}, \hat{A}) = F(W, A)\), and consider arbitrary fixings \(A = a\) and \(\hat{A} = \tilde{a}\). Note that \(\hat{W}\) is now obtained from \(W\) by a deterministic size-poly(\(\lambda\)) circuit, \((W|A = a, \hat{A} = \tilde{a})\) is samplable from CRS to within statistical error \(\text{negl}(\lambda)\) by a circuit of size \(\text{poly}(\lambda, 2^{\ell_2}) = \text{poly}(2^{\lambda r})\) with probability at least \(1 - \text{negl}(\lambda)\) over the fixings, and that, by Lemmas 1 and 2 and the fact that \(\lambda\) is a deterministic function of \(A\) (hence it is fixed), and \(B\) is a deterministic function of \(B\) since \(A\) and \(\hat{A}\) are fixed. As a result, \(W\) and \(\tilde{a}'\|B\) are independent, and we can write \(\hat{W} = f(W)\) and \(\tilde{a}'\|B = g(\tilde{a}'\|B)\) for size-poly(\(\lambda\)) deterministic circuits \(f\) and \(g\). Let \(\mathcal{L} = \{w : f(w) = w\}\) and \(\mathcal{R} = \{b : g(\tilde{a}'\|b) = \tilde{a}'\|b\}\). We now argue differently depending on whether \(W \in L\) and \(B \in R\) hold or not. We begin by noting that if either \(\Pr[W \in L \land B \in R] = \text{negl}(\lambda)\) or \(\Pr[W \notin L \lor B \notin R] = \text{negl}(\lambda)\), then we can add a \(\text{negl}(\lambda)\) term to the final error \(\delta\) via a union bound. We now have

\[
R_A = \text{cnmExt}(\hat{W}, \tilde{a}'\|B', \text{CRS})
\]

and

\[
R_B = \text{cnmExt}(W, \tilde{a}'\|B, \text{CRS}),
\]

where \(\tilde{a}'\) is a deterministic function of \(\tilde{a}\) (hence it is fixed), and \(B'\) is a deterministic function of \(B\) since \(A\) and \(\hat{A}\) are fixed. As a result, \(W\) and \(\tilde{a}'\|B\) are independent, and we can write \(\hat{W} = f(W)\) and \(\tilde{a}'\|B = g(\tilde{a}'\|B)\) for size-poly(\(\lambda\)) deterministic circuits \(f\) and \(g\). Let \(\mathcal{L} = \{w : f(w) = w\}\) and \(\mathcal{R} = \{b : g(\tilde{a}'\|b) = \tilde{a}'\|b\}\). We now argue differently depending on whether \(W \in L\) and \(B \in R\) hold or not. We begin by noting that if either \(\Pr[W \in L \land B \in R] = \text{negl}(\lambda)\) or \(\Pr[W \notin L \lor B \notin R] = \text{negl}(\lambda)\), then we can add a \(\text{negl}(\lambda)\) term to the final error \(\delta\) via a union bound and assume that the opposite event holds. We are thus reduced to the two cases below:

(a) If \(\Pr[W \in L \land B \in R] = \Pr[W \in L] \cdot \Pr[B \in R] \geq \frac{1}{\text{poly}(\lambda)}\), by Lemma 3 it holds that

\[
H_\infty(W|A = a, \hat{A} = \tilde{a}, W \in L, \text{CRS} = \text{crs}) \geq k_1 - \ell_2 - \log^2 \lambda \geq 0.51 \lambda
\]

and

\[
H_\infty(B|A = a, \hat{A} = \tilde{a}, B \in R, \text{CRS} = \text{crs}) \geq k_2 - \log^2 \lambda \geq m + \log^2 \lambda.
\]

Moreover, by the hypothesis above we have that \((W|A = a, \hat{A} = \tilde{a}, W \in L)\) is samplable to within statistical error \(\text{negl}(\lambda)\) by a size-poly(\(2^{\lambda r}\)) circuit from crs, and that \((B|A = a, \hat{A} = \tilde{a}, B \in R)\) is samplable to within statistical error \(\text{negl}(\lambda)\) by a size-poly(\(\lambda\)) circuit from crs. Therefore, since under this conditioning we still have that \(W\) and \(\tilde{a}'\|B\) are independent and they both have enough min-entropy by (31) and (32), it is the case that \(R_A = R_B\) and

\[
R_A = \text{cnmExt}(W, \tilde{a}\|B, \text{crs}), \tilde{a}\|B \approx_\lambda U_{m+2\alpha}, \tilde{a}\|B.
\]

If \([R_A]_\alpha = [R_A]_\alpha\) and \([R_B]_\alpha\|2\alpha = [R_B]_\alpha\|2\alpha\), then \(S_A = S_B \neq \bot\) and \(S_A, C, \text{CRS} \approx_\lambda U_m, C, \text{CRS}, \) where \(C = (\tilde{a}, \tilde{a}', B, B', [R_A]_\alpha, [R_B]_\alpha)\) denotes Eve’s view. Otherwise, we have either \(S_A = \bot\) or \(S_B = \bot\) with probability 1.

(b) On the other hand, if \(\Pr[W \notin L \lor B \notin R] \geq \frac{1}{\text{poly}(\lambda)}\), it either holds that \(\Pr[W \notin L] \geq \frac{1}{\text{poly}(\lambda)}\) or \(\Pr[B \notin R] \geq \frac{1}{\text{poly}(\lambda)}\). Therefore, by Lemma 3 it either holds that

\[
H_\infty(W|A = a, \hat{A} = \tilde{a}, W \notin L, \text{CRS} = \text{crs}) \geq k_1 - 2\ell_2 - \log^2 \lambda - 1 \geq 0.51 \lambda
\]
or

\[ H_\infty(B|A = a, \tilde{A} = \tilde{a}, B \notin \mathcal{R}, \text{CRS} = \text{crs}) \geq k_2 - \log^2 \lambda - 1 \geq m + \log^3 \lambda. \tag{34} \]

Assume that \( \Pr[W \notin \mathcal{L}] \geq \frac{1}{\text{poly}(\lambda)} \) and condition on \( W \notin \mathcal{L} \). The proof when \( \Pr[B \notin \mathcal{R}] \geq \frac{1}{\text{poly}(\lambda)} \) and we condition on \( B \notin \mathcal{R} \) is analogous. Then, we have that \( f \) has no fixed points over the support of \( W \) under this conditioning and that, by the hypothesis above, \((W|A = a, \tilde{A} = \tilde{a}, W \notin \mathcal{L})\) is samplable by a size-poly\((2^\lambda)\) circuit from \( \text{crs} \). Moreover, \((B|A = a, \tilde{A} = \tilde{a})\) is still samplable by a size-poly\((\lambda)\) circuit from \( \text{crs} \) and \( B \) still has min-entropy at least \( m + \log^3 \lambda \) after these fixings. Therefore, we conclude that

\[ R_B = \text{cnmExt}(W, \tilde{a}||B, \text{crs}), R_A = \text{cnmExt}(f(W), g(\tilde{a}||B), \text{crs}), \tilde{a}'||B \approx_c U_{m+2a}, R_A = \text{cnmExt}(f(W), g(\tilde{a}'||B), \text{crs}), \tilde{a}'||B \]

By the choice of \( \alpha = \log^2 \lambda \), this implies that the probability that \( [R_A]_\alpha = [R_B]_\alpha \), and hence \( S_B \neq \bot \), is at most \( \text{negl}(\lambda) \), which we add to \( \delta \) via a union bound.

3. **Eve is active and Bob is corrupted:** The reasoning follows analogously to the previous case, but we set \((\tilde{W}, \tilde{B}) = F(W, B)\) and fix \( B \) and \( \tilde{B} \) instead. 

\[ \square \]

References


<table>
<thead>
<tr>
<th>Work</th>
<th>Min-Entropy Requirements</th>
<th>Sources</th>
<th>Non-Malleability</th>
<th>Error</th>
<th>Distinguisher</th>
<th>Assumptions</th>
</tr>
</thead>
<tbody>
<tr>
<td>[KLR09]</td>
<td>$k \geq \delta n$ for any constant $\delta &gt; 0$</td>
<td>General (without assumptions on sampling efficiency)</td>
<td>No</td>
<td>Negligible</td>
<td>Computationally bounded</td>
<td>Nearly optimal exponentially secure one-way permutations</td>
</tr>
<tr>
<td>[GKK20]</td>
<td>$k_1 = \Omega(n^c)$ and $k_2 = \text{poly}(\log n)$</td>
<td>Efficiently samplable</td>
<td>Polynomial number of tamperings, but only of one source</td>
<td>Negligible</td>
<td>Computationally bounded</td>
<td>Quasi-polynomial hardness of DDH, and CRS.</td>
</tr>
<tr>
<td>This work</td>
<td>$k \geq 0.46n$. Or, $k_1 \geq (1/2 + \delta)n$ and $k_2 = \text{poly}(\log n)$</td>
<td>Efficiently samplable</td>
<td>Multiple tamperings</td>
<td>Negligible</td>
<td>Computationally bounded</td>
<td>Quasi-polynomial hardness of DDH, and CRS.</td>
</tr>
<tr>
<td>This work</td>
<td>$k = \Omega(n^c)$</td>
<td>Efficiently samplable</td>
<td>Multiple tamperings</td>
<td>$n^{-\alpha}$</td>
<td>Computationally bounded</td>
<td>Quasi-polynomial hardness of DDH, and CRS.</td>
</tr>
<tr>
<td>This work</td>
<td>$k = \text{poly}(\log n)$</td>
<td>Efficiently samplable</td>
<td>Multiple tamperings</td>
<td>Negligible</td>
<td>Unbounded</td>
<td>Nearly optimal collision-resistant hash functions</td>
</tr>
</tbody>
</table>

Table 1: Comparison with previous work.