Electronic Colloquium on Computational Complexity, Revision 1 of Report No. 78 (2017)

Continuous Non-Malleable Codes in the 8-Split-State Model

Divesh Aggarwal* Nico Döttling† Jesper Buus Nielsen‡ Maciej Obremski‡
Erick Purwanto*

April 6, 2018

Abstract

Non-malleable codes (NMCs), introduced by Dziembowski, Pietrzak and Wichs [DPW10], provide a useful message integrity guarantee in situations where traditional error-correction (and even error-detection) is impossible; for example, when the attacker can completely overwrite the encoded message. NMCs have emerged as a fundamental object at the intersection of coding theory and cryptography. In particular, progress in the study of non-malleable codes and the related notion of non-malleable extractors has led to new insights and progress on even more fundamental problems like the construction of multi-source randomness extractors.

A large body of the recent work has focused on various constructions of non-malleable codes in the split-state model. Many variants of NMCs have been introduced in the literature i.e. strong NMCs, super strong NMCs and continuous NMCs. The most general, and hence also the most useful notion among these is that of continuous non-malleable codes, that allows for continuous tampering by the adversary.

We present the first efficient information-theoretically secure continuously non-malleable code in the constant split-state model, where there is a self-destruct mechanism which ensures that the adversary loses access to tampering after the first failed decoding.

We believe that our main technical result could be of independent interest and some of the ideas could in future be used to make progress on other related questions.

*National University of Singapore
†Friedrich-Alexander-University Erlangen-Nuremberg
‡Aarhus University

ISSN 1433-8092

1 Introduction

1.1 Non-malleable Codes

Non-malleable codes (NMCs), introduced by Dziembowski, Pietrzak and Wichs [DPW10], provide a useful message integrity guarantee in situations where traditional error-correction (and even error-detection) is impossible; for example, when the attacker can completely overwrite the encoded message. NMCs have emerged as a fundamental object at the intersection of coding theory and cryptography.

Informally, given a tampering family $\mathcal{F}$, an NMC $(\mathsf{Enc}, \mathsf{Dec})$ against $\mathcal{F}$ encodes a given message m into a codeword $c \leftarrow \mathsf{Enc}(m)$ in a way that, if the adversary modifies c to $c' = f(c)$ for some $f \in \mathcal{F}$, then the the message $m' = \mathsf{Dec}(c')$ is either the original message m, or a completely "unrelated value". Formally, we require that if $m' \neq m$, then m' can be simulated using just the tampering function f, but without knowing anything about the tampered codeword c'.

As has been shown by the recent progress [DPW10, LL12, DKO13, ADL14, FMVW14, FMNV14, CG14a, CG14b, CZ14, Agg15, ADKO15b, ADKO15a, AB16, CGL16, AGM$^+$15b, AGM$^+$15a, AAnHKM$^+$16, AKO17, Li17] NMCs aim to handle a much larger class of tampering functions $\mathcal{F}$ than traditional error-correcting or error-detecting codes, at the expense of potentially allowing the attacker to replace a given message m by an unrelated message m'. NMCs are useful in situations where changing m to an unrelated m' is not useful for the attacker (for example, when m is the secret key for a signature scheme.)

Continuous Non-malleable Codes. It is clearly realistically possible that the attacker repeatedly tampers with the device and observes the outputs. The definition in [DPW10] allows the adversary to tamper the codeword *only once*. We call this *one-shot* tampering. Faust et al.[FMNV14] consider a stronger model where the adversary can iteratively submit tampering functions f_i and learn $m_i = \mathsf{Dec}(f_i(c))$. We call this the *continuous tampering model*. This stronger security notion is needed in many settings, for instance when using NMCs to make tamper resilient computations on von Neumann architectures [FMNV15]. As mentioned in [JW15], non-malleable codes can provide protection against these kind of attacks if the device is allowed to freshly re-encode its state after each invocation to make sure that the tampering is applied to a fresh codeword at each step. After each execution the entire content of the memory is erased. While such perfect erasures may be feasible in some settings, they are rather problematic in the presence of tampering. Due to this reason, Faust et al. [FMNV14] introduced an even stronger notion of non-malleable codes called continuous non-malleable codes where security is achieved against continuous tampering of a single codeword *without* re-encoding. Some additional restrictions are, however, necessary in the continuous tampering model. If the adversary was given an unlimited budget of tampering queries, then, given that the class of tampering functions is sufficiently expressive (e.g. it allows to overwrite single bits of the codeword), the adversary can efficiently learn the entire message just by observing whether tampering queries leave the codeword unmodified or lead to decoding errors, see e.g. [GLM$^+$04].

To overcome this general issue, [FMNV14] assume a *self-destruct* mechanism which is triggered by decoding errors. In particular, once the decoder outputs a special symbol $\perp$ the device *self-destructs* and the adversary loses access to his tampering oracle. This model still allows an adversary many tamper attempts, as long as his attack remains covert. Jafargholi and Wichs [JW15] considered four variants of continuous non-malleable codes depending on

- Whether tampering is *persistent* in the sense that the tampering is always applied to the current version of the tampered codeword, and all previous versions of the codeword are lost.

The alternative definition considers non-persistent tampering where the device resets after each tampering, and the tampering always occurs on the original codeword.

- Whether tampering to an invalid codeword (i.e., when the decoder outputs $\perp$) causes a *"self-destruct"* and the experiment stops and the attacker cannot gain any additional information, or alternatively whether the attacker can always continue to tamper and gain information.

In this work, we will exclusively focus on continuous NMC in the non-persistent self-destruct model. We shorthand such codes by sdCNMC.

Split-State Model. Although any kind of non-malleable codes do not exist if the family of "tampering functions" $\mathcal{F}$ is completely unrestricted,[1] they are known to exist for many large classes of tampering families $\mathcal{F}$.

In [DPW10] the authors considered one such natural family of tampering functions. They gave a construction of an efficient code which is non-malleable with respect to bit-wise tampering, i.e., tampering functions that modify each bit of the codeword arbitrarily but independently of the value of the other bits of the codeword. Later works [DKO13, ADL14, CZ14, CG14b, Agg15, AB16, Li17] provided efficient constructions in a stronger model called the s-split state model where the codeword is split into s parts called *states*, which can each be tampered arbitrarily but independently of the other states. If the codeword has length n, then the result of [DPW10] can be seen as a result for the n-state model. The physical motivation for this model is that one might place the different states on physically separated memories, for instance on different memory chips, and hope this makes it impossible to tamper with one part in a way which depends on the value of the other part. Clearly, one would like s to be as small as possible. This family is interesting since it seems naturally useful in applications, especially when s is low and the shares $y_1, \ldots, y_s$ are stored in different parts of memory, or by different parties. Not surprisingly, the setting of $t = 2$ appears the most useful (but also the most challenging from the technical point of view), so it received the most attention so far [DPW10, LL12, DKO13, ADL14, FMNV14, CG14a, CG14b, CZ14, ADKO15b, ADKO15a] and is also the focus of our work.

While some of the above-mentioned results achieve security only against computationally bounded adversaries, we focus on security in the information-theoretic setting, i.e., security against unbounded adversaries. The known results in the information-theoretic setting can be summarized as follows. First, [DPW10] showed the existence of (strong) non-malleable codes, and this result was improved by [CG14a] who showed that the optimal rate of these codes is $1/2$. Faust et al. [FMNV14] showed the impossibility of continuous non-malleable codes against non-persistent 2-split-state tampering. Later [JW15] showed that continuous non-malleable codes exist in the split-state model if the tampering is persistent, and [AKO17] gave an efficient construction of such codes.

There have been a series of recent results culminating in constructions of efficient non-malleable codes in the split-state model [DKO13, ADL14, CZ14, ADKO15a, CGL16, Li17].

1.2 Continuous Non-Malleable Codes in the Split-State Model and Our Result

Faust et al. [FMNV14] constructed a sdCNMC in the 2-state model which is secure against computationally bounded adversaries. A recent result [AKO17] gave a construction of non-malleable

[1] In particular, $\mathcal{F}$ should not include "re-encoding functions" $f(c) = \mathsf{Enc}(f'(\mathsf{Dec}(c)))$ for any non-trivial function f', as $m' = \mathsf{Dec}(f(\mathsf{Enc}(m))) = f'(m)$ is obviously related to m.

codes secure against persistent continuous tampering. It was shown in [FMNV14] that it is *impossible* to construct an information theoretic sdCNMC for the much more interesting 2-state model with non-persistent tampering. This leaves the following question open.

Question 1. *Does there exist a code that is non-malleable in the c-split persistent continuous tampering model for some constant c?*

In [CMTV15] a sdCNMC was constructed in the bit-wise tampering model, which can be seen as an n-state model. However, very little progress has been made towards resolving Question 1. The only result that achieves some sort of non-malleable codes secure against persistent continuous tampering is the result by Chattopadhyay, Goyal, and Li [CGL16]. They achieve this by constructing a so-called many-many non-malleable code in the 2-split state model. Their construction achieves non-malleability as long as the number of rounds of tampering is at most n^γ for some constant $\gamma < 1$, where n is the length of the codeword. Their result has a natural barrier and it is unlikely that their ideas can be used to achieve a construction that allows more than $O(n)$ rounds of tampering. This is both because their construction does not allow self-destruct and is for the 2-split state model, and it is known [FMNV14, AKO17] that continuous non-malleable codes with $\omega(n)$ rounds of tampering is impossible both for the two split-state model and for the constant split-state model that does not allow self-destruct.

We construct an information-theoretic sdCNMCs for the 8-state model.

Theorem 1 (Informal). *There exists an efficient, explicit construction of non-persistent self-destruct $2^{O(k)}$-round continuous $2^{-\Omega(k)}$-non-malleable codes which encodes messages of length k bits into 8 states, each of size $O(k \log k)$.*

1.3 Overview of the Construction and Techniques

In this section, we will provide an overview of our construction and the main ideas for its security proof. Our construction combines two Hadamard extractors with a 3-source non-malleable extractor. The construction is given as follows.

1.3.1 Our Construction

Let $\mathbb{K}$ be a finite field of size 2^n, which is an extension field $\mathbb{F}$ of size $2^{n/\ell}$ for an appropriately chosen divisor ℓ of n. Our construction uses the following:

- A three source non-malleable extractor $\mathsf{nmExt} : \mathbb{K}^3 \to \{0,1\}^{3k}$ with $k = \theta(n/\log n)$, where the min-entropy for each source is required to be at least $(1-\delta)n$, for some constant δ,
- A 2-source Hadamard extractor $\langle \cdot, \cdot \rangle : (\mathbb{K}^3) \times (\mathbb{K}^3) \to \mathbb{K}$, and
- A 2-source Hadamard extractor $\langle \cdot, \cdot \rangle : (\mathbb{F}^{3\ell}) \times (\mathbb{F}^{3\ell}) \to \mathbb{F}$.

We define

$$\mathsf{nmExt}' : (\{0,1\}^n)^3 \to \{0,1\}^{3k} \cup \{\perp\}$$

as $\mathsf{nmExt}'(x_1, x_2, x_3) = \mathsf{nmExt}(x_1, x_2, x_3)$ if $\mathsf{nmExt}(x_1, x_2, x_3) \in 0^{2k} \| y$ for some $y \in \{0,1\}^k$, and $\perp$, otherwise.

Encoding: Our encoding procedure takes as input a message $m \in \{0,1\}^k$, and does the following.

- Sample $X = (X_1, X_2, X_3)$ from $(\mathbb{K} \setminus \{0\})^3$ uniformly such that $\mathsf{nmExt}(X) = 0^{2k} \| m$.

- Sample $S = (S_1, S_2, S_3)$ from $(\mathbb{K} \setminus \{0\})^3$ uniformly such that $\mathsf{nmExt}(S) = 0^{2k} \| r$ for some r in $\{0,1\}^k$.
- $V = \langle X, S \rangle_{\mathbb{K}}$.
- $W = \langle X, S \rangle_{\mathbb{F}}$.
- Output the eight parts $(X_1, X_2, X_3, S_1, S_2, S_3, V, W)$.

Decoding: The decoding procedure is canonical, i.e., on input (x, s, v, w), we first check if x and s pass the two inner product checks and are in the correct domains (i.e. all components non-zero), we try to decode x and s and if neither reports an error we return the decoded value of x.

The adversary, in each round, will choose some functions, $f_1, f_2, f_3, g_1, g_2, g_3, h_1 : \mathbb{K} \to \mathbb{K}$, $h_2 : \mathbb{F} \to \mathbb{F}$ and will apply these functions to the eight respective parts. Let $f(X)$ denote $(f_1(X_1), f_2(X_2), f_3(X_3))$ and $g(S)$ denote $(g_1(S_1), g_2(S_2), g_3(S_3))$ In order to prove (continuous) non-malleability of the construction, we need to show that even if we collect all the messages obtained after decoding the tampered codewords in multiple rounds excluding any round where all the chosen functions are identity functions (in this case decoding the tampered codeword yields the original message), this should not reveal any useful information about the original message. To formalize this, we define the tampering experiment to output a special symbol same whenever all functions are identity functions. Then, it is required to prove that for any two messages, the output distributions of the corresponding tampering experiments are statistically close to each other. In fact, in this work, we consider a stronger notion of continuous non-malleable codes called super-strong continuous non-malleable codes in which every time the adversary tampers $(c \to c')$, $c' \neq c$, and c' decodes to a valid message, the adversary will learn the whole tampered codeword c'.[2]

1.3.2 Proof Ideas

Before looking at the ideas behind the security of our construction, it is instructive to revisit the reason behind the impossibility of constructions for 2-state information-theoretic continuous non-malleable codes [FMNV14]. The main idea behind the attack given in [FMNV14] was to find a triple ℓ, r_0, r_1 such that $\mathsf{Dec}(\ell, r_0), \mathsf{Dec}(\ell, r_1) \neq \perp$. Given ℓ, r_0 and r_1, the attack proceeds by overwriting the first state with ℓ, while the second state is overwritten by r_b where b is the first bit of the second state, thereby revealing one bit of information. Repeating this idea for different bits of the codeword, after a linear number of rounds, the adversary will recover the entire codeword.

In our construction, if the adversary decides to preserve a significant amount of entropy of the original codeword when tampering, i.e., the tampering function is close to being bijective, then the non-malleability of nmExt should be sufficient to achieve not just non-malleability but error detection - $\mathsf{nmExt}(f(X))$ is close to being uniform and independent of $\mathsf{nmExt}(X)$ by the non-malleability of nmExt, and hence the tampered codeword decodes to $\perp$ with high probability. However, if the adversary decides to carry only a very small amount of entropy into the tampered codeword, there is nothing preventing him from learning some small amount of information as in the attack by [FMNV14] described above. Generally, it is not possible to always detect such *low entropy tampering*. Nevertheless, our proof ensures that every time the adversary tries to learn some information about the original codeword, he will risk being detected with a probability proportional

[2]The reason we talk about this stronger tampering oracle is because it is much easier and cleaner to prove statements in the super strong tampering model. One could hope that if one considers the weaker notion of continuous non-malleable codes, one might be able to prove this result for a smaller number of parts, but all our effort in this direction indicates that it is likely much harder to prove statements if we don't allow super strong tampering.

to the amount of information he is trying to learn. To ensure that this will be the case, we will carefully analyze how the adversary can learn anything about the codeword.

As mentioned above, the tampering experiment for our code is of the *super-strong* type, i.e., every time the adversary tampers ($C \to C'$), $C' \neq C$, and C' decodes to a valid message, the adversary will learn the whole tampered codeword C'. Notice that given

$$C' = (f_1(X_1), f_2(X_2), f_3(X_3), g_1(S_1), g_2(S_2), g_3(S_3), h_1(V), h_2(W))$$

all the adversary learns is that

- $X_i \in \mathcal{X}_i$ for $i = 1, 2, 3$
- $S \in \mathcal{S}$ for $i = 1, 2, 3$
- $V \in \mathcal{V}$
- $W \in \mathcal{W}$,

where $\mathcal{X} \times \mathcal{Y} \times \mathcal{V} \times \mathcal{W}$ is the preimage of c' for the function $(f_1, f_2, f_3, g_1, g_2, g_3, h_1, h_2)$. In round r of the tampering experiment the adversary will learn that the codeword belongs to some domain $\mathcal{X}^{(r)} \times \mathcal{S}^{(r)} \times \mathcal{V}^{(r)} \times \mathcal{W}^{(r)}$, and will progressively try to make these sets as small as possible. In the [FMNV14] attack described above, the domain size is reduced by a factor of two each time, eventually revealing the entire codeword. As long as we can make sure that the domain doesn't become too small, we will be able to argue that if the adversary wants to learn more information (make the set smaller) there is a significant risk of getting detected. We sketch below the idea for showing this for $r = 1$, i.e. the first round, and the argument for the following rounds follows by a slightly tricky inductive argument.

Depending on the functions $f_1, f_2, f_3, g_1, g_2, g_3$, we partition each of $\mathcal{X}_1, \mathcal{X}_2, \mathcal{X}_3, \mathcal{S}_1, \mathcal{S}_2, \mathcal{S}_3$ which induces a partition on the whole domain. For instance $\mathcal{X}_1$ is partitioned into $\ell + 1$ parts for some parameter $\ell = \omega(1)$, as follows.

- $\mathcal{X}_{1,0}$ is the part where the function f_1 is identity, i.e., $\{x \in \mathcal{X}_1 : f_1(x) = x\}$.
- For $i = 1, \dots, \ell$, $\mathcal{X}_{1,i}$ is defined such that f_1 has between $2^{n(i-1)/\ell}$ and $2^{n \cdot i/\ell}$ preimages.

This implies that for each partition, the entropy of X_1 conditioned on $f_1(X_1)$ is nearly fixed (upto an additive term $n/\ell = o(n)$). The other sets $\mathcal{X}_2, \mathcal{X}_3, \mathcal{S}_1, \mathcal{S}_2, \mathcal{S}_3$ are partitioned similarly. Each partition of the form

$$\mathcal{X}_{1,i_1}, \mathcal{X}_{2,i_2}, \mathcal{X}_{3,i_3}, \mathcal{S}_{1,j_1}, \mathcal{S}_{2,j_1}, \mathcal{S}_{3,j_3}, \mathcal{V}, \mathcal{W} .$$

Type-1 corresponds to $i_1 = i_2 = i_3 = j_1 = j_2 = j_3 = 0$.

Type-2 contains all partitions for which the following is true: ($f(X) \neq X$ or $g(S) \neq S$) and $(f(X), g(S))$ contains almost full information about (X, S), i.e., all tampering functions are close to bijective or id, but at least one tampering function is not the identity.

Type-3 contains all partitions which do not fall into any of above classes (in particular it means that $(f(X), g(S))$ lost quite a bit information about the original (X, S)), but $(f(X), g(S))$ still carries a substantial/medium amount of information/entropy about (X, S).

Type-4 contains all partitions which do not fall into any of above classes but $(f(X), g(S))$ still carries some entropy

Type-5 contains the partition where $(f(X), g(S))$ is close to constant, i.e., $i_1 = i_2 = i_3 = j_1 = j_2 = j_3 = \ell$.

Analysis of the tampering for each type of partition. In this section, we often implicitly assume that X is independent of S in order to simplify the informal argument, even though there is some limited dependence introduced by the fact that $\langle X, S\rangle_{\mathbb{K}} \in \mathcal{V}$, etc. For details about why this dependence does not hurt us, we would suggest the reader to read the full proofs.

We show that if for a given tampering function the codeword c falls into either class $2, 3$ or 4, then the tampering will be detected with probability $1 - \varepsilon$ for a negligible ε:

In Type-2: On this part of the domain the adversary will attempt to apply close to bijective tampering functions. Either this part of the domain will have negligible size, or the adversary will be detected by the check for nmExt'.

In Type-3: We will argue that the check $\langle f(X), g(S)\rangle_{\mathbb{F}} = h_2(W)$ will fail. To see this, notice that the adversary applied non-bijective tampering, and the vectors $f(X), g(S)$ have a substantial amount of entropy. The argument below follows from the strong extraction properties of the inner-product extractor: The vectors $f(X)$ and $g(S)$ do not carry enough information about X, S, i.e., one of $\widetilde{\mathbf{H}}_\infty(X|f(X))$ or $\widetilde{\mathbf{H}}_\infty(S|g(S))$ is not too small. Thus $\langle X, S\rangle_{\mathbb{F}}$ and $\langle f(X), g(S)\rangle_{\mathbb{F}}$ are almost independent. However $f(X), g(S)$ have enough entropy to keep $\langle f(X), g(S)\rangle_{\mathbb{F}}$ uniform. The adversary will not be able to guess $\langle f(X), g(S)\rangle_{\mathbb{F}}$ even given $\langle X, S\rangle_{\mathbb{F}}$. Thus he will fail at the check $h_2(\langle X, S\rangle_{\mathbb{F}}) = \langle f(X), g(S)\rangle_{\mathbb{F}}$ and this tampering will be detected.

In Type-4: The reasoning is quite similar to Type-3, but we use the check on $\langle f(X), g(S)\rangle_{\mathbb{K}} = h_1(V)$. The adversary applied far-from-bijective tampering, and the vectors $f(X), g(S)$ still have some small amount of entropy. The argument below follows from the strong extraction properties of the inner product extractor: The vectors $f(X)$ and $g(S)$ only carry a very small amount of information about X, S. Thus $\langle X, S\rangle_{\mathbb{K}}$ and $\langle f(X), g(S)\rangle_{\mathbb{K}}$ are almost independent. However $f(X), g(S)$ still have enough entropy to keep $\langle f(X), g(S)\rangle_{\mathbb{K}}$ unpredictable (not uniform, but with substantial min-entropy). The adversary will not be able to guess $\langle f(X), g(S)\rangle_{\mathbb{K}}$ even given $\langle X, S\rangle_{\mathbb{K}}$, thus he will fail at the check $h_1(\langle X, S\rangle_{\mathbb{K}}) = \langle f(X), g(S)\rangle_{\mathbb{K}}$ and this tampering will be detected.

This leads to the conclusion that the only way that the adversary can learn something and survive (i.e. not get detected) is if the original codeword falls into Type-1 or Type-5. If the codeword was in Type-1, the tampering experiment will output `same` (unless one of the inner product checks fails and the tampered codeword decodes to $\perp$). If the codeword was in Type-5, then the output will be some codeword c', and the adversary will learn whether the codeword is Type 1 or Type 5 with respect to the choice of functions f and g. Moreover, on Type-5 there might be close-to-constant but non-constant functions (which, if he does not get detected, potentially provide additional knowledge to the adversary).

Even if the adversary is in a Type 1 or Type 5 partition and succeeds to go to the next round without causing self-destruct, this is not a reason to worry as long as the size of the domain remains large enough. On the other hand, if the adversary can manage to land himself in a small enough domain, this means that the adversary already obtained a lot of information about the codeword, and might be able to recover the message. However, if such small domains are few and scarce, then the probability that the adversary lands in such a domain is quite small. The main cause of concern is if there are many such small domains that cover a significant fraction of the ambient space. In the following, we show that this is not possible.

Type 1 or Type 5: Notice that the adversary is in a Type 1 or a Type 5 partition if either each of $i_1, i_2, i_3, j_1, j_2, j_3$ is 0, or each is equal to ℓ. Since the indices $i_1, i_2, i_3, j_1, j_2, j_3$ are independently distributed random variables, a simple application of the Cauchy Schwarz inequality shows that

$$\sqrt{p_1} + \sqrt{p_5} \leq 1 ,$$

where p_1 is the probability of being in a Type 1 partition, and p_5 is the probability of being a Type 5 partition.

Type 5: Just like in the case of Type 4 partitions, we have that the vectors $f(X)$ and $g(S)$ only carry a very small amount of information about X, S. Thus $\langle X, S\rangle_{\mathbb{K}}$ and $\langle f(X), g(S)\rangle_{\mathbb{K}}$ are nearly independent. The Type 5 partition corresponds to the domain where each of $f_1, f_2, f_3, g_1, g_2, g_3$ is close to a constant and can be further subdivided such that for each of these subpartitions, each of $f_1, f_2, f_3, g_1, g_2, g_3$ output a fixed value. Intuitively speaking, if say, each of these functions takes two different values then there are potentially 64 different values of $\langle f(X), g(S)\rangle_{\mathbb{K}}$ (although some of these 64 values could be the same), and so the function h_1 cannot guess this value with sufficiently large probability, unless all the inner products magically become equal. Formally, we show in this case that

$$p_{5,1}^{7/8} + \cdots + p_{5,d}^{7/8} \leq p_5^{7/8} ,$$

where $p_{5,1}, \ldots, p_{5,d}$ are the respective probabilities of being in various subpartitions of Type 5 such that $h_1(\langle X, S\rangle_{\mathbb{K}}) = \langle f(X), g(S)\rangle_{\mathbb{K}}$ holds within these subpartitions.

Together, these results imply that

$$q_1^{7/8} + q_2^{7/8} + \cdots + q_{d+1}^{7/8} \leq 1 , \tag{1}$$

where $q_1, \ldots, q_{d+1}$ is a renaming of $p_1, p_{5,1}, \ldots, p_{5,d}$. A simple application of Hölder's inequality implies that for any $\varepsilon \geq 0$,

$$\sum_{q_i \leq \varepsilon} q_i = \sum_{q_i \leq \varepsilon} q_i^{7/8} \cdot q_i^{1/8} \leq \sum_{q_i \leq \varepsilon} q_i^{7/8} \cdot \varepsilon^{1/8} \leq \varepsilon^{1/8} .$$

For an appropriately chosen ε, this implies that it is not possible that there are many small domains on which the decoder does not self-destruct, and their union is large. This concludes the intuitive overview of our proof.

We would like to again emphasize that for ease of exposition, we ignored many intricacies of the formal proof, and made many simplifying assumptions, one of these being that here we assumed that $X_1, X_2, X_3, S_1, S_2, S_3$ are independent, even though they have some limited dependence (which in particular introduces small errors in the statements above) because of the fact that $\langle X, S\rangle_{\mathbb{K}} \in \mathcal{V}$, $\langle X, S\rangle_{\mathbb{F}} \in \mathcal{W}$, $\mathsf{nmExt}'(X) \neq \perp$, and $\mathsf{nmExt}'(S) \neq \perp$. For the formal proofs, we refer the reader to Section 3.

1.4 Conclusions and Open Questions

We give a construction of a $2^{-\Omega(k)}$-non-malleable code from k bit messages to $O(k \log k)$ bit codewords in the 8-split state model secure against continuous tampering. The main building block of our construction is a non-malleable 3-source extractor construction from [Li17], and the Hadamard 2-source extractor.

Prior results achieved continuous non-malleability only for a sublinear number of rounds. The main reason for difficulty in achieving non-malleable codes against continuous tampering is that the adversary can potentially obtain useful information in each round, and even if one bit of information about the codeword is obtained in each round, this is already catastrophic and does not allow non-malleability beyond a linear number of rounds.

Our idea of proving that our construction achieves non-malleability for a large number of rounds is that we ensure that whenever the adversary tampers to gain useful information about the codeword, there is a risk of a decoding error resulting in self-destruct. Central to our proof strategy is what we believe a very novel technique where we obtained and used an inequality of the form 1 to bound the statistical distance between two random experiments. In particular, our main technical result in Theorem 5 where we bound the statistical distance between two random variables by $(\frac{\rho}{q})^c+\varepsilon$, where q is proportional to the size of the domain, c is a constant, and ρ, ε are appropriately chosen parameters, might seem very unusual, but appears naturally in our proof.

The following are natural questions left open by our work.

1. Improve the rate of our code.
2. Improve the number of split states to a number smaller than 8.

The first of these questions can be resolved immediately by a non-malleable extractor with parameters (output length) better than the one given in [Li17]. As for the second question, our construction has a natural barrier and the number of states can likely not be improved by any simple modification. However, we hope that our techniques can lead to new insights that might help resolve this question.

Lastly, in the recent years, progress related to non-malleable codes has led to useful ideas for solving even more fundamental problems like constructing better two-source or multi-source extractors. We hope that our construction and/or techniques can find other similar applications.

2 Preliminaries

All logarithms are to the base 2. For any function $h : \mathcal{X} \to \mathcal{Y}$, we define $h^{-1}(y) := \{x \in \mathcal{X} : h(x) = y\}$.

For a set S, we let U_S denote the uniform distribution over S. For an integer $m \in \mathbb{N}$, we let U_m denote the uniform distribution over $\{0,1\}^m$, the bit-strings of length m. We denote two independent bitstrings of length m by U_m, U'_m. For a distribution or random variable X we write $x \leftarrow X$ to denote the operation of sampling a random x according to X. For a set S, we write $s \leftarrow S$ as shorthand for $s \leftarrow U_S$. For a random variable Z, $f(Z)|_{Z\in\mathcal{C}}$ denotes the distribution $f(Z)$ conditioned on the event that $Z \in \mathcal{C}$.

2.1 Entropy and Statistical Distance

The *min-entropy* of a random variable X is defined as $\mathbf{H}_\infty(X) \stackrel{\text{def}}{=} -\log(\max_x \Pr[X = x])$. We say that X is an (n, k)*-source* if $X \in \{0,1\}^n$ and $\mathbf{H}_\infty(X) \geq k$. For $X \in \{0,1\}^n$, we define the *entropy rate* of X to be $\mathbf{H}_\infty(X)/n$. We also define *average (aka conditional) min-entropy* of a random variable X conditioned on another random variable Z as

$$\widetilde{\mathbf{H}}_\infty(X|Z) \stackrel{\text{def}}{=} -\log\left(\mathbb{E}_{z\leftarrow Z}\left[\max_x \Pr[X = x|Z = z]\right]\right) = -\log\left(\mathbb{E}_{z\leftarrow Z}\left[2^{-\mathbf{H}_\infty(X|Z=z)}\right]\right)$$

where $\mathbb{E}_{z\leftarrow Z}$ denotes the expected value over $z \leftarrow Z$. We have the following lemma.

Lemma 1 ([DORS08]). *Let (X, W) be some joint distribution. Then,*

- *For any* $s > 0$, $\Pr_{w \leftarrow W}[\mathbf{H}_\infty(X|W = w) \geq \widetilde{\mathbf{H}}_\infty(X|W) - s] \geq 1 - 2^{-s}$.
- *If* Z *has at most* 2^ℓ *possible values, then* $\widetilde{\mathbf{H}}_\infty(X|(W, Z)) \geq \widetilde{\mathbf{H}}_\infty(X|W) - \ell$.

The *statistical distance* between two random variables W and Z distributed over some set S is

$$\Delta(W; Z) := \max_{T \subseteq S}(|W(T) - Z(T)|) = \frac{1}{2}\sum_{s \in S}|W(s) - Z(s)|.$$

Note that $\Delta(W; Z) = \max_D(\Pr[D(W) = 1] - \Pr[D(Z) = 1])$, where D is a probabilistic function. We say W is ε-close to Z, denoted $W \approx_\varepsilon Z$, if $\Delta(W; Z) \leq \varepsilon$. We write $\Delta(W; Z|Y)$ as shorthand for $\Delta((W, Y); (Z, Y))$. The following is folklore, and is easy to see.

Lemma 2. *For any two random variables* X, Y*, and any randomized function* f*, we have that*

$$\Delta(f(X); f(Y)) \leq \Delta(X; Y) .$$

2.2 Extractors

An extractor [NZ96] can be used to extract uniform randomness out of a weakly-random value which is only assumed to have sufficient min-entropy. Our definition follows that of [DORS08], which is defined in terms of conditional min-entropy.

Definition 1 (Extractors). *An efficient function* $\mathsf{Ext} : \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^m$ *is an (average-case, strong)* (k, ε)-extractor*, if for all* X, Z *such that* X *is distributed over* $\{0,1\}^n$ *and* $\widetilde{\mathbf{H}}_\infty(X|Z) \geq k$*, we get*

$$\Delta(\ (Z, Y, \mathsf{Ext}(X; Y))\ ;\ (Z, Y, U_m)\ ) \leq \varepsilon$$

where $Y \equiv U_d$ *denotes the coins of* Ext *(called the* seed*). The value* $L = k - m$ *is called the* entropy loss *of* Ext*, and the value* d *is called the* seed length *of* Ext.

Definition 2 (Two-Source Extractors). *A function* $\mathsf{Ext} : \mathcal{X}_1 \times \mathcal{X}_2 \to \mathcal{Z}$ *is called a* (k, ε)*-two-source extractor, if it holds for all tuples* $((X_1, Y_1), (X_2, Y_2))$ *for which* (X_1, Y_1) *is independent of* (X_2, Y_2) *and* $\widetilde{\mathbf{H}}_\infty(X_1|Y_1) + \widetilde{\mathbf{H}}_\infty(X_2|Y_2) \geq k$ *that*

$$\Delta(\mathsf{Ext}(X_1, X_2)\ ;\ U_{\mathcal{Z}} \mid Y_1, Y_2) \geq \varepsilon\ .$$

A well-known flexible two-source extractor is the Hadamard extractor or inner-product extractor.

Lemma 3 ([CG88, ADL14]). *For any finite field* $\mathbb{F}_q$ *of cardinality* q *and any positive integer* n*, the function* $\mathsf{Ext} : \mathbb{F}_q^n \times \mathbb{F}_q^n \to \mathbb{F}_q$ *given by*

$$\mathsf{Ext}(X_1, X_2) := \langle X_1, X_2 \rangle = X_{1,1} \cdot X_{2,1} + \cdots + X_{1,n} \cdot X_{2,n}$$

is a (k, ε)*-two-source extractor for any* $k \geq (n+1)\log q + 2\log\left(\frac{1}{\varepsilon}\right)$.

We denote the above inner product by $\langle X_1, X_2 \rangle_{\mathbb{F}_q}$. We will drop the subscript if the field is clear from the context.
We will also use non-malleable t-source extractor.

Definition 3 (Non-Malleable t-Source Extractor). *A function* $\mathsf{nmExt} : (\mathcal{X})^t \to \mathcal{Z}$ *is called a* t*-source* (k, ε)*-non-malleable extractor if the following property holds. For all independently distributed tuples* $((X_1, Y_1), (X_2, Y_2), \ldots, (X_t, Y_t))$ *such that* $\widetilde{\mathbf{H}}_\infty(X_i|Y_i) \geq k$*, and for any split-state* *tampering function $f = (f_1, \dots, f_t)$, $f_i : \mathcal{X} \to \mathcal{X}$ such that there exists f_i without fixed points, it holds that*

$$\Delta\big(\mathsf{nmExt}(X)\ ;\ U_{\mathcal{Z}} \mid \mathsf{nmExt}(f(X)),\ Y_1, \dots, Y_t\big) \ \leq\ \varepsilon\ ,$$

where $X = (X_1, \dots, X_t)$, and $f(X) = (f_1(X_1), \dots, f_t(X_t))$.

The following result gives the best known 2-source non-malleable extractor.

Theorem 2 ([Li17]). *For any finite field $\mathbb{K}$ of cardinality 2^n, there exists a constant $\delta^\star \in (0, 1/3)$, and a function $\mathsf{nmExt}_2 : \mathbb{K}^2 \to \{0,1\}^{3k}$ such that the function nmExt is a 2-source $((1-\delta^\star)n, 2^{-1000k})$ non-malleable extractor with $k = \Theta(n/\log n)$. Moreover, it is efficiently pre-image sampleable.*

For this paper, we need a 3-source non-malleable extractor. The construction from the above result can be easily modified to obtain a 3-source non-malleable extractor.

Theorem 3. *For any finite field $\mathbb{K}$ of cardinality 2^n, there exists a constant $\delta \in (0, 1/3)$, and a function $\mathsf{nmExt} : \mathbb{K}^3 \to \{0,1\}^{3k}$ such that the function nmExt is a 3-source $((1-\delta)n, 2^{-1000k})$ non-malleable extractor with $k = \Theta(n/\log n)$. Moreover, it is efficiently pre-image sampleable.*

Proof. Let $(X_1, Y_1), (X_2, Y_2), (X_3, Y_3)$ be as in Definition 3. Consider the following construction.

$$\mathsf{nmExt}(X_1, X_2, X_3) := \mathsf{nmExt}_2(X_1, X_2) \oplus \mathsf{nmExt}_2(X_2, X_3) \oplus \mathsf{nmExt}_2(X_3, X_1)\ ,$$

where by $\oplus$, we mean the bitwise XOR function. Let the functions applied to the three parts be f_1, f_2, f_3, one of which has no fixed points. Without loss of generality, let f_1 be the function with no fixed points. We have that

$$\widetilde{\mathbf{H}}_\infty(X_1 \mid Y_1,\ \mathsf{nmExt}_2(X_3, X_1),\ \mathsf{nmExt}_2(f_3(X_3), f_1(X_1))) \geq n - n \cdot \delta - 6k \geq n(1 - \delta^\star)\ ,$$

and

$$\widetilde{\mathbf{H}}_\infty(X_2 \mid Y_2,\ \mathsf{nmExt}_2(X_2, X_3),\ \mathsf{nmExt}_2(f_2(X_2), f_3(X_3))) \geq n - n \cdot \delta - 6k \geq n(1 - \delta^\star)\ ,$$

where we assumed that $\delta = \delta^\star/2$, and $\delta n \geq 12k$. Thus, the statistical distance between $\mathsf{nmExt}_2(X_1, X_2)$ and U_{3k} conditioned on $\mathsf{nmExt}_2(f_1(X_1), f_2(X_2))$, Y_1, $\mathsf{nmExt}_2(X_3, X_1)$, $\mathsf{nmExt}_2(f_3(X_3), f_1(X_1))$, Y_2, $\mathsf{nmExt}_2(X_2, X_3)$, and $\mathsf{nmExt}_2(f_2(X_2), f_3(X_3))$ is at most 2^{-1000k}, which implies using Lemma 2 that

$$\Delta\left(\mathsf{nmExt}(X_1, X_2, X_3)\ ;\ U_{3k} \mid \mathsf{nmExt}(f_1(X_1), f_2(X_2), f_3(X_3))\, Y_1,\ Y_2,\ Y_3\right) \leq 2^{-1000k}\ ,$$

□

2.3 Trace function

For a finite field $A = \mathbb{F}_{2^m}$, and for its extension field $B = \mathbb{F}_{2^n}$, we define the trace function $\mathrm{tr}_{B\to A} : B \to A$ as (see for instance [SW15])

$$\mathrm{tr}_{B\to A} = \sum_{i=0}^{\frac{n}{m}-1} x^{2^{m\cdot i}}\ .$$

We will need the following properties of the trace function.

- Let $A = \mathbb{F}_{2^m}$ be a finite field, $B = \mathbb{F}_{2^n}$ be an extension field of A, and $C = \mathbb{F}_{2^r}$ be an extension field of B. Then,

$$\forall x \in C,\ \ \mathrm{tr}_{C\to A}(x) = \mathrm{tr}_{B\to A}(\mathrm{tr}_{C\to B}(x))\ .$$

- It is convenient to choose the group isomorphism $\phi : A^{n/m} \to B$ such that for any $x, y \in A^{n/m}$

$$\langle x, y \rangle = \mathrm{tr}_{B\to A}(\phi(x) \cdot \phi(y)) \ .$$

These two together imply that for any finite field $A = \mathbb{F}_{2^m}$, and for its extension field $B = \mathbb{F}_{2^n}$, and any integer ℓ, and any $x, y \in B^\ell$, there is a group isomorphism from $\psi : B^\ell \to A^{n\ell/m}$ such that

$$\langle \psi(x), \psi(y) \rangle_A = \mathrm{tr}_{B\to A}(\langle x, y \rangle_B) \ .$$

We will need this result on many occasions. Using a slight abuse of notation, we will denote $\langle \psi(x), \psi(y) \rangle_A$ by $\langle x, y \rangle_A$.

2.4 Definitions related to Non-Malleable Codes

Definition 4 (Coding Schemes). *A coding scheme is a pair* $(\mathsf{Enc}, \mathsf{Dec})$*, where* $\mathsf{Enc} : \mathcal{M} \to \mathcal{C}$ *is a randomized function and* $\mathsf{Dec} : \mathcal{C} \to \mathcal{M} \cup \{\perp\}$ *is a deterministic function, such that it holds for all* $M \in \mathcal{M}$ *that* $\mathsf{Dec}(\mathsf{Enc}(M)) = M$*.*

We will now define the continuous super strong tampering experiment. In this experiment the adversary is provided with the tampered codeword C' (instead of the output of the decoder) whenever $C' \neq C$ and the decoder does not output $\perp$.

Definition 5 ((Continuous-) Super Strong Tampering Experiment). *We will define continuous non-persistent self-destruct non-malleable codes analogously to [JW15]. Fix a coding scheme* $(\mathsf{Enc}, \mathsf{Dec})$ *with message space* $\mathcal{M}$ *and codeword space* $\mathcal{C}$*. Also fix a family of functions* $\mathcal{F} : \mathcal{C} \to \mathcal{C}$*. We will first define the tampering oracle* $\mathsf{Tamp}_C^{\mathsf{state}}(f)$*, for which initially* $\mathsf{state} = \mathtt{alive}$*. For a tampering function* $f \in \mathcal{F}$ *and a codeword* $c \in \mathcal{C}$ *define the tampering oracle by*

$\mathsf{Tamp}_c^{\mathsf{state}}(f)$:
  If $\mathsf{state} = \mathtt{dead}$ *output* $\perp$
  $c' \leftarrow f(c)$
  If $c' = c$ *output* $\mathtt{same}$
  $m' \leftarrow \mathsf{Dec}(c')$
  If $m' = \perp$ *set* $\mathsf{state} \leftarrow \mathtt{dead}$ *and output* $\perp$
  Otherwise output c'

Fix a codeword $c \in \mathcal{C}$*. We define the continuous tampering experiment* CT_C^r *by*

CT_C^r :
  $\mathsf{state} \leftarrow \mathtt{alive}$
  For $i = 1$ *to* r
    Choose functions f
    $v \leftarrow \mathsf{Tamp}_c^{\mathsf{state}}(f)$
    Output v

Definition 6. *Let* $(\mathsf{Enc}, \mathsf{Dec})$ *be a coding scheme and* CT *be its corresponding continuous tampering experiment for a class* $\mathcal{F}$ *of tampering functions. We say that* $(\mathsf{Enc}, \mathsf{Dec})$ *is an* ε*-secure* r*-round continuously non-malleable code against* $\mathcal{F}$*, if it holds for all tampering adversaries* $\mathcal{A}$ *and all pairs of messages* $m_0, m_1 \in \mathcal{M}$ *that*

$$\mathsf{CT}_{C_0}^r(\mathcal{A}) \approx_\varepsilon \mathsf{CT}_{C_1}^r(\mathcal{A}),$$

where $C_0 \leftarrow \mathsf{Enc}(m_0)$ *and* $C_1 \leftarrow \mathsf{Enc}(m_1)$*.*

Remark 1. *[AKO17] In any model allowing bitwise tampering, in particular in the $t-$split state model, the* self-destruct *mechanism is necessary when the size of the messages is at least* 3*.*

The only family of tampering functions we are concerned with in this work are split state tampering functions.

Definition 7 (Split State Tampering). *Let $C = C_1 \times \cdots \times C_s$. The class of spit state tampering functions $\mathcal{F}_s$ consists of all functions f of the form $f = (f_1, \ldots, f_s)$ where $f(c_1, \ldots, c_s) = (f_1(c_1), \ldots, f_s(c_s))$ for all $(c_1, \ldots, c_s) \in C_1 \times \cdots \times C_s$. Here the f_i are arbitrary functions $C_i \to C_i$.*

2.5 Some Useful Results

Lemma 4 (Deathzone Generation Lemma). *Let $\mathbb{F}_q$ be a finite field. Let $A_1, \ldots, A_t, B_1, \ldots, B_t$ be independent, non-zero random variables. Denote $A = (A_1, \ldots, A_t)$ and $B = (B_1, \ldots, B_t)$. Then*

$$\max_{c \in \mathbb{F}} \sum_{a,b \in \mathbb{F}^t : \langle a,b \rangle_{\mathbb{F}} = c} \left(\Pr\left[(A,B) = (a,b)\right]\right)^{\frac{2t-1}{2t}} \ \leq \ 1 \, .$$

Proof. Let us begin with Young's inequality for convolution:

$$||f_1 * f_2 * \cdots * f_t||_r \ \leq \ \prod_{i=1}^{t} ||f_i||_{p_i}$$

whenever $\sum_{i=1}^{t} \frac{1}{p_i} = \frac{1}{r} + n - 1$ and $+\infty \geq p_1, \ldots, p_t, r \geq 1$.
We will identify random variable A_i with its distribution $A_i(.)$ where $A_i(x) = \Pr[A_i = x]$. We define two convolutions:

$$\begin{aligned} (A_i *_\times B_i)(z) &= \sum_{x,y \,:\, xy = z} A_i(x)\, B_i(y) \, , \\ (A_i *_+ B_i)(z) &= \sum_{x,y \,:\, x+y = z} A_i(x)\, B_i(y) \, . \end{aligned}$$

Notice that for every i, via Young's inequality, we get

$$1 \ = \ ||A_i^\alpha(.)||_{\frac{1}{\alpha}} \cdot ||B_i^\alpha(.)||_{\frac{1}{\alpha}} \ \geq \ ||A_i^\alpha(.) *_\times B_i^\alpha(.)||_{\frac{1}{2\alpha-1}}$$

for $1/2 \leq \alpha \leq 1$.
Notice again via Young's inequality for the "additive" convolution, we get

$$\begin{aligned} 1 \ &\geq \ \prod_{i=1}^{t} ||A_i^\alpha(.) *_\times B_i^\alpha(.)||_{\frac{1}{2\alpha-1}} \\ &\geq \ ||[A_i^\alpha(.) *_\times B_i^\alpha(.)] *_+ \cdots *_+ [A_t^\alpha(.) *_\times B_t^\alpha(.)]||_{\frac{1}{2n\alpha-(2n-1)}} \ , \end{aligned}$$

for $\frac{2t-1}{2t} \leq \alpha \leq 1$.
Now we take $\alpha = \frac{2t-1}{2t}$ and we get

$$1 \geq ||[A_i^\alpha(.) *_\times B_i^\alpha(.)] *_+ \cdots *_+ [A_t^\alpha(.) *_\times B_t^\alpha(.)]||_\infty \, .$$

□

Lemma 5. *Suppose* $2\,\Delta(P;Q)=\sum_{i=1}^{n}|p_i-q_i|=\varepsilon$*, where* $p_i=\Pr[P=x_i]$ *and* $q_i=\Pr[Q=x_i]$*; and*

$$\sum_{i=1}^{m} p_i^r \;\le\; \alpha\;,$$

for $r<1$*. Then*

$$\sum_{i=1}^{m} q_i^r \;\le\; \alpha\,+\,\varepsilon^r\cdot m^{1-r}\;.$$

Proof.

$$\begin{aligned}
\sum_{i=1}^{m} q_i^r &= \sum_{i=1}^{m}\left(p_i+|p_i-q_i|\right)^r \\
&\le \sum_{i=1}^{m}\left(p_i^r+|p_i-q_i|^r\right) \\
&= \sum_{i=1}^{m} p_i^r \,+\, \sum_{i=1}^{m}|p_i-q_i|^r \\
&\le \alpha\,+\,\sum_{i=1}^{m}|p_i-q_i|^r \\
&\le \alpha\,+\,\left(\sum_{i=1}^{m}|p_i-q_i|\right)^r\cdot\left(\sum_{i=1}^{m}1\right)^{1-r} \qquad (2)\\
&= \alpha\,+\,\varepsilon^r\cdot m^{1-r}\;,
\end{aligned}$$

where inequality 2 follows from Hölder's inequality.

□

Lemma 6 ([CG14b]). *Let* $\mathcal{D}$ *and* $\mathcal{D}'$ *be distributions over the same finite space* Ω*, and suppose they are* ε*-close to each other. Let* $E\subseteq\Omega$ *be any event such that* $\mathcal{D}(E)=p$*. Then, the conditional distributions* $\mathcal{D}|E$ *and* $\mathcal{D}'|E$ *are* (ε/p)*-close.*

3 From One-time to Continuous Tampering

3.1 Our construction

By Theorem 3, we have that there exists a constant c, such that for all n, and $k\le\frac{c\cdot n}{\log n}$, there is a function

$$\mathsf{nmExt}:(\mathbb{K})^3\to\{0,1\}^{3k}$$

that is a $(1-\delta,2^{-1000k})$ non-malleable 3-source extractor. We choose the largest such $k=\Theta(n/\log n)$ such that $\ell=\frac{n}{50k}=O(\log n)$ is an integer. Also, define

$$\mathsf{nmExt}':(\{0,1\}^n)^3\to\{0,1\}^{3k}\cup\{\perp\}$$

as $\mathsf{nmExt}'(x_1,x_2,x_3)=\mathsf{nmExt}(x_1,x_2,x_3)$ if $\mathsf{nmExt}(x_1,x_2,x_3)\in 0^{2k}\|y$ for some $y\in\{0,1\}^k$, and $\perp$, otherwise.

Let $\mathbb{K}$ be a finite field of size 2^n, and let $\mathbb{F}$ be a finite field of size 2^{50k}. Notice that there is a natural bijection between $\mathbb{K}$ and $\mathbb{F}^\ell$. We further assume that $k\le\min\left(\frac{\delta n}{1000},\frac{n}{5000}\right)$.

Encoding: Our encoding procedure Enc takes as input a message $m \in \{0,1\}^k$, and does the following.

- Sample X from $(\mathbb{K} \setminus \{0\})^3$ uniformly such that $\mathsf{nmExt}(X) = 0^{2k} \| m$.
- Sample S from $(\mathbb{K} \setminus \{0\})^3$ uniformly such that $\mathsf{nmExt}(S) = 0^{2k} \| r$ for some r in $\{0,1\}^k$.
- $V = \langle X, S \rangle_{\mathbb{K}}$.
- $W = \langle X, S \rangle_{\mathbb{F}}$.
- Output (X, S, V, W).

Decoding: Our decoding procedure Dec takes as input some x, s, v, w and does the following.

- If $(x, s, v, w) \notin (\mathbb{K} \setminus \{0\})^6 \times \mathbb{K} \times \mathbb{F}$, then output $\perp$.
- If $\mathsf{nmExt}'(x) = \perp$, output $\perp$.
- If $\mathsf{nmExt}'(s) = \perp$, output $\perp$.
- If $v \neq \langle x, s \rangle_{\mathbb{K}}$, output $\perp$.
- If $w \neq \langle x, s \rangle_{\mathbb{F}}$, output $\perp$.
- Otherwise, output m^*, where $\mathsf{nmExt}(x) = 0^{2k} \| m^*$.

3.2 The statement of the Main Result

Let $f_1, f_2, f_3, g_1, g_2, g_3, h_1 : \mathbb{K} \to \mathbb{K}$, $h_2 : \mathbb{F} \to \mathbb{F}$ be arbitrary functions, and let $f = (f_1, f_2, f_3)$ and $g = (g_1, g_2, g_3)$.

Definition 8 (Continuous Tampering Experiment). *We will first define the tampering oracle* $\mathsf{Tamp}_c^{\mathsf{state}}(f, g, h_1, h_2)$*, for* $\mathsf{state} \in \{\mathsf{alive}, \mathsf{dead}\}$ *and for*

$$c = (x_1, x_2, x_3, s_1, s_2, s_3, \langle x, s \rangle_{\mathbb{K}}, \langle x, s \rangle_{\mathbb{F}}) \; .$$

For a tampering function (f, g, h_1, h_2) *define the tampering oracle by*

$\mathsf{Tamp}_c^{\mathsf{state}}(f, g, h_1, h_2)$ *:*
    If $\mathsf{state} = \mathsf{dead}$ *output* $\perp$
    If $(x, s, \langle x, s \rangle_{\mathbb{K}}, \langle x, s \rangle_{\mathbb{F}}) = (f(x), g(s), h_1(\langle x, s \rangle_{\mathbb{K}}), h_2(\langle x, s \rangle_{\mathbb{F}})$ *output* same
    If $(\mathsf{nmExt}'(f(x)) = \perp)$
        or $(\mathsf{nmExt}'(g(s)) = \perp)$
        or $(\langle f(x), g(s) \rangle_{\mathbb{K}} \neq h_1(\langle x, s \rangle_{\mathbb{K}}))$
        or $(\langle f(x), g(s) \rangle_{\mathbb{F}} \neq h_2(\langle x, s \rangle_{\mathbb{F}}))$
        set $\mathsf{state} \leftarrow \mathsf{dead}$ *and output* $\perp$
    Otherwise output $(f(x), g(s), h_1(\langle x, s \rangle_{\mathbb{K}}), h_2(\langle x, s \rangle_{\mathbb{F}})$

Fix some $c = (x, s, v, w)$*, with* $x, s \in \mathbb{K}^3$*,* $v \in \mathbb{K}$*, and* $w \in \mathbb{F}$*. We define the continuous tampering experiment* CT_c^r *by*
CT_c^r *:*
    $\mathsf{state} \leftarrow \mathsf{alive}$
    For $i = 1$ *to* r
        Choose functions $f_1, f_2, f_3, g_1, g_2, g_3, h_1, h_2$*.*
        $\psi \leftarrow \mathsf{Tamp}_c^{\mathsf{state}}(f, g, h_1, h_2)$*.*
        Output ψ

The following result which shows that continuously tampering a codeword for polynomially many rounds does not reveal any useful information about the codeword.

Theorem 4. *Let X, S be uniform in $(\mathbb{K} \setminus \{0\})^3$ conditioned on the event that $\mathsf{nmExt}'(X) \neq \perp$ and $\mathsf{nmExt}'(S) \neq \perp$. Let C be the random variable*

$$(X, S, \langle X, S\rangle_{\mathbb{K}}, \langle X, S\rangle_{\mathbb{F}}) \ .$$

For any integer $r \geq 0$, we have that

$$\Delta\big((\mathsf{CT}_C^r, \mathsf{nmExt}(X))\,;\,(\mathsf{CT}_C^r, 0^{2k}\|U_k)\big) \ \leq\ 2^{-2k}\cdot 10\cdot r\ ,$$

where U_k is a uniform k-bit string independent from X, S.

The main result of the paper is obtained as an easy corollary of Theorem 4, as stated below.

Corollary 1. *Let $m_0, m_1 \in \{0,1\}^k$, and let $C^{(0)} \leftarrow \mathsf{Enc}(m_0)$, and let $C^{(1)} \leftarrow \mathsf{Enc}(m_1)$. For any integer $r \geq 0$, we have that*

$$\Delta\big((\mathsf{CT}_{C^{(0)}}^r\,;\,(\mathsf{CT}_{C^{(1)}}^r\big) \ \leq\ 2^{-k}\cdot 20\cdot r\ .$$

Proof. By Theorem 4, for any $r \geq 0$, and the random variable

$$C = (X, S, \langle X, S\rangle_{\mathbb{K}}, \langle X, S\rangle_{\mathbb{F}})$$

we have that

$$\Delta\big((\mathsf{CT}_C^r, \mathsf{nmExt}(X))\,;\,(\mathsf{CT}_C^r, 0^{2k}\|U_k)\big) \ \leq\ 2^{-2k}\cdot 10\cdot r\ ,$$

where X, S are distributed as in Theorem 4. Thus conditioning on the event that $\mathsf{Dec}(C) = m_i$ for $i = 0, 1$, which is the same as the event that $\mathsf{nmExt}(X) = 0^{2k}\|m_i$ and using Lemma 6, we get that

$$\begin{aligned}\Delta\big((\mathsf{CT}_C^r, \mathsf{nmExt}(X))|_{\mathsf{nmExt}(X)=0^{2k}\|m_0}\,;\,(\mathsf{CT}_C^r, 0^{2k}\|U_k)|_{U_k=m_0}\big) &= \Delta\big((\mathsf{CT}_{C^{(0)}}^r\,;\,(\mathsf{CT}_C^r\big)\\ &\leq 2^{-k}\cdot 10\cdot r\ ,\end{aligned}$$

and

$$\begin{aligned}\Delta\big((\mathsf{CT}_C^r, \mathsf{nmExt}(X))|_{\mathsf{nmExt}(X)=0^{2k}\|m_1}\,;\,(\mathsf{CT}_C^r, 0^{2k}\|U_k)|_{U_k=m_1}\big) &= \Delta\big((\mathsf{CT}_C^r 0\,;\,(\mathsf{CT}_C^r\big)\\ &\leq 2^{-k}\cdot 10\cdot r\ ,\end{aligned}$$

The result then follows by triangle inequality. □

To prove Theorem 4, we will show the more general statement, i.e., Theorem 5 which immediately implies Theorem 4. We introduce the following parameters: $\rho = 2^{-40k}$. Also, for any sets $\mathcal{X}, \mathcal{S} \subseteq \mathbb{K}^3$, $\mathcal{V} \subseteq \mathbb{K}$ and $\mathcal{W} \subseteq \mathbb{F}$, we shorthand

$$p[\mathcal{X}, \mathcal{S}, \mathcal{V}, \mathcal{W}] := \Pr[(\widetilde{X}, \widetilde{S}, \langle \widetilde{X}, \widetilde{S}\rangle_{\mathbb{K}}, \langle \widetilde{X}, \widetilde{S}\rangle_{\mathbb{F}}) \in \mathcal{X}\times\mathcal{S}\times\mathcal{V}\times\mathcal{W}]$$

and

$$q[\mathcal{X}, \mathcal{S}, \mathcal{V}, \mathcal{W}] := \Pr[(\widetilde{X}, \widetilde{S}, \langle \widetilde{X}, \widetilde{S}\rangle_{\mathbb{K}}, \langle \widetilde{X}, \widetilde{S}\rangle_{\mathbb{F}}) \in \mathcal{X}\times\mathcal{S}\times\mathcal{V}\times\mathcal{W} \mid \mathsf{nmExt}'(\widetilde{X}) \neq \perp,\ \mathsf{nmExt}'(\widetilde{S}) \neq \perp]$$

where $\widetilde{X}, \widetilde{S}$ are uniform in $\mathbb{K}^3$.

Remark 2. *Our proof will proceed by partitioning the space in a way that the eight parts of our codeword remain independent. We introduced above the definition of the probability of landing in a particular partition. The reason we needed two different definitions depending on whether the codeword is a valid codeword or not is because we want to prove a statement for valid codewords but the proof technique crucially requires us to prove statements assuming that the eight parts of the codeword are independent. The following result shows that as long as* $q[\mathcal{X}, \mathcal{S}, \mathcal{V}, \mathcal{W}]$ *is not too small,* $p[\mathcal{X}, \mathcal{S}, \mathcal{V}, \mathcal{W}]$ *and* $q[\mathcal{X}, \mathcal{S}, \mathcal{V}, \mathcal{W}]$ *are nearly equal. This statement is required only to overcome the above mentioned technical annoyance and the reader can safely skip the proof.*

Lemma 7. *Let* $\mathcal{X}_1, \mathcal{X}_2, \mathcal{X}_3, \mathcal{S}_1, \mathcal{S}_2, \mathcal{S}_3, \mathcal{V} \subseteq \mathbb{K}$*, and let* $\mathcal{W} \subseteq \mathbb{F}$*. We denote* $\mathcal{X} = (\mathcal{X}_1, \mathcal{X}_2, \mathcal{X}_3)$ *and* $\mathcal{S} = (\mathcal{S}_1, \mathcal{S}_2, \mathcal{S}_3)$*. If* $q[\mathcal{X}, \mathcal{S}, \mathcal{V}, \mathcal{W}] \geq 2^{-800k}$*, then*

$$\frac{p[\mathcal{X}, \mathcal{S}, \mathcal{V}, \mathcal{W}]}{q[\mathcal{X}, \mathcal{S}, \mathcal{V}, \mathcal{W}]} = 1 \pm 2^{-180k} \ ,$$

and

$$\frac{\Pr[\widetilde{X} \in \mathcal{X},\ \widetilde{S} \in \mathcal{S},\ U_n \in \mathcal{V},\ \mathrm{tr}_{\mathbb{K}\to\mathbb{F}}(U_n) \in \mathcal{W}]}{q[\mathcal{X}, \mathcal{S}, \mathcal{V}, \mathcal{W}]} = 1 \pm 2^{-180k} \ ,$$

where $\widetilde{X}, \widetilde{S}$ *are uniform in* $\mathbb{K}^3$*, and* U_n *is uniform in* $\mathbb{K}$*.*

Theorem 5. *Let* $\mathcal{X}_1, \mathcal{X}_2, \mathcal{X}_3, \mathcal{S}_1, \mathcal{S}_2, \mathcal{S}_3 \subseteq \mathbb{K} \setminus \{0\}$*,* $\mathcal{V} \subseteq \mathbb{K}$*, and let* $\mathcal{W} \subseteq \mathbb{F}$*. We denote* $\mathcal{X} = (\mathcal{X}_1, \mathcal{X}_2, \mathcal{X}_3)$ *and* $\mathcal{S} = (\mathcal{S}_1, \mathcal{S}_2, \mathcal{S}_3)$*. Let* (X, S) *be random variables uniform in* $\{0,1\}^{6n}$ *conditioned on the event that* $X_i \in \mathcal{X}_i$*,* $S_i \in \mathcal{S}_i$ *for* $i = 1, 2, 3$*,* $\mathsf{nmExt}'(X) \neq \bot$*,* $\mathsf{nmExt}'(S) \neq \bot$*,* $\langle X, S\rangle_{\mathbb{K}} \in \mathcal{V}$*, and* $\langle X, S\rangle_{\mathbb{F}} \in \mathcal{W}$*. Let* C *be the random variable*

$$(X, S, \langle X, S\rangle_{\mathbb{K}}, \langle X, S\rangle_{\mathbb{F}}) \ .$$

For any integer $r \geq 0$*, we have that*

$$\Delta\left((\mathsf{CT}^r_C, \mathsf{nmExt}(X))\,;\,(\mathsf{CT}^r_C, 0^{2k}\|U_k)\right) \ \leq\ \left(\frac{\rho}{q[\mathcal{X}, \mathcal{S}, \mathcal{V}, \mathcal{W}]}\right)^{\frac{1}{8}} + 9 \cdot r \cdot 2^{-2k} \ , \qquad (3)$$

where U_k *is a uniform* k*-bit string independent from* X, S*.*

We will prove Theorem 5 by partitioning the ambient space into appropriate subsets such that Equation 3 holds for each of these partitions. Theorem 5 can then be shown by the following lemma.

Lemma 8. *Let* $\mathcal{X}_1, \mathcal{X}_2, \mathcal{X}_3, \mathcal{S}_1, \mathcal{S}_2, \mathcal{S}_3, \mathcal{V} \subseteq \mathbb{K}$*, and let* $\mathcal{W} \subseteq \mathbb{F}$*. We denote* $\mathcal{X} = (\mathcal{X}_1, \mathcal{X}_2, \mathcal{X}_3)$ *and* $\mathcal{S} = \mathcal{S}_1, \mathcal{S}_2, \mathcal{S}_3$*. Let* X, S *be random variables uniform in* $\{0,1\}^{6n}$ *conditioned on the event that* $X_i \in \mathcal{X}_i$*,* $S_i \in \mathcal{S}_i$ *for* $i = 1, 2, 3$*,* $\mathsf{nmExt}'(X) \neq \bot$*,* $\mathsf{nmExt}'(S) \neq \bot$*,* $\langle X, S\rangle_{\mathbb{K}} \in \mathcal{V}$*, and* $\langle X, S\rangle_{\mathbb{F}} \in \mathcal{W}$*. Let* C *be the random variable*

$$(X, S, \langle X, S\rangle_{\mathbb{K}}, \langle X, S\rangle_{\mathbb{F}}) \ .$$

Let $\mathcal{P}_1, \mathcal{P}_2, \ldots, \mathcal{P}_t$ *be a partitioning of* $\mathcal{X} \times \mathcal{S} \times \mathcal{V} \times \mathcal{W}$*. Then we have that for any integer* $r \geq 0$*, if*

$$\Delta\left((\mathsf{CT}^r_C, \mathsf{nmExt}(X))|_{C\in\mathcal{P}_j}\,;\,(\mathsf{CT}^r_C, 0^{2k}\|U_k)|_{C\in\mathcal{P}_j}\right) \leq \varepsilon_j$$

then

$$\Delta\left((\mathsf{CT}^r_C, \mathsf{nmExt}(X))\,;\,(\mathsf{CT}^r_C, 0^{2k}\|U_k)\right) \ \leq\ \sum_{j=1}^{t} \frac{q[\mathcal{P}_j]}{q[\mathcal{X} \times \mathcal{S} \times \mathcal{V} \times \mathcal{W}]} \cdot \varepsilon_j \ ,$$

where U_k *is a uniform* k*-bit string independent from* X, S*.*

Proof. Let $\mathcal{A}$ be the sample space of $(\mathsf{CT}_C^r, \mathsf{nmExt}(X))$. Then, by definition,

$$\Delta = \Delta\left((\mathsf{CT}_C^r, \mathsf{nmExt}(X))\,;\,(\mathsf{CT}_C^r, 0^{2k}\|U_k)\right)$$

is given by

$$\begin{aligned}
\Delta &= \frac{1}{2}\cdot\sum_{a\in\mathcal{A}}\left|\Pr[(\mathsf{CT}_C^r, \mathsf{nmExt}(X)) = a] - \Pr[(\mathsf{CT}_C^r, 0^{2k}\|U_k) = a]\right| \\
&= \frac{1}{2}\cdot\sum_{a\in\mathcal{A}}\left|\sum_{j=1}^{t}\Pr[(\mathsf{CT}_C^r, \mathsf{nmExt}(X)) = a,\ C\in\mathcal{P}_j] - \Pr[(\mathsf{CT}_C^r, 0^{2k}\|U_k) = a,\ C\in\mathcal{P}_j]\right| \\
&\le \frac{1}{2}\cdot\sum_{a\in\mathcal{A}}\sum_{j=1}^{t}\Pr[C\in\mathcal{P}_j]\cdot\left|\Pr[(\mathsf{CT}_C^r, \mathsf{nmExt}(X)) = a \mid C\in\mathcal{P}_j] - \Pr[(\mathsf{CT}_C^r, 0^{2k}\|U_k) = a \mid C\in\mathcal{P}_j]\right| \\
&= \frac{1}{2}\cdot\sum_{j=1}^{t}\Pr[C\in\mathcal{P}_j]\cdot\sum_{a\in\mathcal{A}}\left|\Pr[(\mathsf{CT}_C^r, \mathsf{nmExt}(X)) = a \mid C\in\mathcal{P}_j] - \Pr[(\mathsf{CT}_C^r, 0^{2k}\|U_k) = a \mid C\in\mathcal{P}_j]\right| \\
&= \sum_{j=1}^{t}\frac{q[\mathcal{P}_j]}{q[\mathcal{X}\times\mathcal{S}\times\mathcal{V}\times\mathcal{W}]}\cdot\varepsilon_j\ .
\end{aligned}$$

□

We will now partition each of $\mathcal{X}_1, \mathcal{X}_2, \mathcal{X}_3, \mathcal{S}_1, \mathcal{S}_2, \mathcal{S}_3$ which will induce a partitioning of the whole space. The partitions are chosen in a way that if, say, X_i (respectively, S_i) for $i\in\{1,2,3\}$ is uniformly distributed over a particular partition of $\mathcal{X}_i$ (respectively, $\mathcal{S}_i$), then this gives a precise estimate of $\widetilde{\mathbf{H}}_\infty(X_i|f_i(X_i))$ (respectively, $\widetilde{\mathbf{H}}_\infty(S_i|g_i(S_i))$.

Definition 9 (Partition). *We partition the set $\mathcal{X}_1\subseteq\{0,1\}^n$ based on the function f_1 as follows.*

1. $\mathcal{X}_{1,0} = \{x\in\mathcal{X}_1\ :\ f_1(x) = x\}$.
2. $\mathcal{X}_1 = \mathcal{X}_1\setminus\mathcal{X}_{1,0}$.
3. *For* $i = 1,\ldots,\ell-1,\ \ \mathcal{X}_{1,i} = \{x\in\mathcal{X}_1\ :\ |f_1^{-1}(f_1(x))\cap\mathcal{X}_1|\in[2^{100k\cdot(i-1)}, 2^{100k\cdot i})\}$.
4. $\mathcal{X}_{1,\ell} = \{x\in\mathcal{X}_1\ :\ |f_1^{-1}(f_1(x))\cap\mathcal{X}_1|\ge 2^{100k\cdot(\ell-1)}\}$

$\mathcal{X}_2, \mathcal{X}_3, \mathcal{S}_1, \mathcal{S}_2, \mathcal{S}_3$ *are partitioned similarly as above.*

We classify the partitions obtained according to the following types.

Definition 10 (Classification of Partitions). *Let $i_1, i_2, i_3, j_1, j_2, j_3$ be one of $\{0,1,\ldots,\ell\}$. We then classify the partition*

$$\mathcal{P} := \mathcal{X}_{1,i_1}\times\mathcal{X}_{2,i_2}\times\mathcal{X}_{3,i_3}\times\mathcal{S}_{1,j_1}\times\mathcal{S}_{2,j_2}\times\mathcal{S}_{3,j_3}\times\mathcal{V}\times\mathcal{W}$$

of $\mathcal{X}\times\mathcal{S}\times\mathcal{V}\times\mathcal{W}$ as follows.

Type 1: *We say that $\mathcal{P}$ is a Type 1 partition if $i_1 = i_2 = i_3 = j_1 = j_2 = j_3 = 0$.*

Type 2: *We say that $\mathcal{P}$ is a Type 2 partition if*

1. *$\mathcal{P}$ is not a Type 1 partition, i.e., at least one of $i_1, i_2, i_3, j_1, j_2, j_3 > 0$.*

2. *Each of* $i_1, i_2, i_3, j_1, j_2, j_3$ *is at most* $\frac{\delta n}{100k} - 1$.

Type 3: *We say that* $\mathcal{P}$ *is a Type 3 partition if the following hold*

1. $\mathcal{P}$ *is not a Type 1 or Type 2 partition, i.e., at least one of* $i_1, i_2, i_3, j_1, j_2, j_3 > \frac{\delta n}{100k} - 1$.
2. $i_1 + i_2 + i_3 + j_1 + j_2 + j_3 \leq \frac{n}{40k}$.

Type 4: *We say that* $\mathcal{P}$ *is a Type 4 partition if*

1. $\mathcal{P}$ *is not a Type 1, 2, or 3 partition, , i.e.,* $i_1 + i_2 + i_3 + j_1 + j_2 + j_3 > \frac{n}{40k}$.
2. *At least one of* $i_1, i_2, i_3, j_1, j_2, j_3$ *is not* ℓ.

Type 5: *We say that* $\mathcal{P}$ *is a Type 5 partition if* $i_1 = i_2 = i_3 = j_1 = j_2 = j_3 = \ell$.

In the following we classify partitions of Type 1 and Type 5 further into subpartitions, but before this, we introduce the following definition.

Definition 11. *We define the following subsets of* $\mathcal{V}$.

- $\mathcal{V}_{\mathsf{same}} = \{v \in \mathcal{V} \ : \ h_1(v) = v\}$.
- $\overline{\mathcal{V}_{\mathsf{same}}} = \mathcal{V} \setminus \mathcal{V}_{\mathsf{same}}$.
- *For all* $y \in \{0,1\}^n$, $\mathcal{V}_y = \{v \in \mathcal{V} \ : \ h_1(v) = y\}$.
- *For all* $y \in \{0,1\}^n$, $\overline{\mathcal{V}_y} = \mathcal{V} \setminus \mathcal{V}_y$.

We similarly define $\mathcal{W}_{\mathsf{same}}, \overline{\mathcal{W}_{\mathsf{same}}}, \mathcal{W}_z, \overline{\mathcal{W}_z}$ *for all* $z \in \mathbb{F}$ *via the function* h_2.

Using this classification, we now further partition Type 1 and Type 5 partitions.

Definition 12. *Let* $\mathcal{X}_{\mathsf{same}} = \mathcal{X}_{1,0} \times \mathcal{X}_{2,0} \times \mathcal{X}_{3,0}$ *and let* $\mathcal{S}_{\mathsf{same}} = \mathcal{S}_{1,0} \times \mathcal{S}_{2,0} \times \mathcal{S}_{3,0}$

Type 1a: *We say that* $\mathcal{X}_{\mathsf{same}} \times \mathcal{S}_{\mathsf{same}} \times \mathcal{V}_{\mathsf{same}} \times \mathcal{W}_{\mathsf{same}}$ *is a Type 1a partition.*

Type 1b: *We say that the following are Type 1b partitions:*

- $\mathcal{X}_{\mathsf{same}} \times \mathcal{S}_{\mathsf{same}} \times \mathcal{V} \times \overline{\mathcal{W}_{\mathsf{same}}}$.
- $\mathcal{X}_{\mathsf{same}} \times \mathcal{S}_{\mathsf{same}} \times \overline{\mathcal{V}_{\mathsf{same}}} \times \mathcal{W}_{\mathsf{same}}$.

Definition 13. *For* $\mathbf{a} = (a_1, a_2, a_3) \in \{0,1\}^{3n}$, *let*

$$\mathcal{X}_{\mathbf{a}} = \{(x_1, x_2, x_3) \in \mathcal{X}_{1,\ell} \times \mathcal{X}_{2,\ell} \times \mathcal{X}_{3,\ell} \ : \ f_1(x_1) = a_1, f_2(x_2) = a_2, f_3(x_3) = a_3\} \ .$$

Similarly, define $\mathcal{S}_{\mathbf{b}}$ *for* $\mathbf{b} = (b_1, b_2, b_3) \in \{0,1\}^{3n}$.

Type 5a: *We say that* $\mathcal{X}_{\mathbf{a}} \times \mathcal{S}_{\mathbf{b}} \times \mathcal{V}_{\langle \mathbf{a},\mathbf{b} \rangle_{\mathbb{K}}} \times \mathcal{W}_{\langle \mathbf{a},\mathbf{b} \rangle_{\mathbb{F}}}$ *is a Type 5a partition.*

Type 5b: *We say that the following are Type 5b partitions:*

- $\mathcal{X}_{\mathbf{a}} \times \mathcal{S}_{\mathbf{b}} \times \mathcal{V} \times \overline{\mathcal{W}_{\langle \mathbf{a},\mathbf{b} \rangle_{\mathbb{F}}}}$
- $\mathcal{X}_{\mathbf{a}} \times \mathcal{S}_{\mathbf{b}} \times \overline{\mathcal{V}_{\langle \mathbf{a},\mathbf{b} \rangle_{\mathbb{K}}}} \times \mathcal{W}_{\langle \mathbf{a},\mathbf{b} \rangle_{\mathbb{F}}}$.

If a partition $\mathcal{P}$ is of Type T, then we denote it as $Type(\mathcal{P}) = T$, where $T \in \{1a, 1b, 2, 3, 4, 5a, 5b\}$.

Before bounding the required statistical distance for each partition, we will prove a few general results.

Lemma 9. *Let $\mathcal{X}_1, \mathcal{X}_2, \mathcal{X}_3, \mathcal{S}_1, \mathcal{S}_2, \mathcal{S}_3, \mathcal{V} \subseteq \mathbb{K}$, and let $\mathcal{W} \subseteq \mathbb{F}$. We denote $\mathcal{X} = (\mathcal{X}_1, \mathcal{X}_2, \mathcal{X}_3)$ and $\mathcal{S} = (\mathcal{S}_1, \mathcal{S}_2, \mathcal{S}_3)$. Let $|\mathcal{X}_i| \geq 2^{n-100k}$, $|\mathcal{S}_i| \geq 2^{n-100k}$ for $i = 1,2,3$, and let $q[\mathcal{X}, \mathcal{S}, \mathcal{V}, \mathcal{W}] \geq 2^{-800k}$. Let (X, S) be random variables uniform in $\mathbb{K}^3$ conditioned on the event that $X_i \in \mathcal{X}_i$, $S_i \in \mathcal{S}_i$ for $i = 1,2,3$, $\mathsf{nmExt}'(X) \neq \perp$, $\mathsf{nmExt}'(S) \neq \perp$, $\langle X, S\rangle_{\mathbb{K}} \in \mathcal{V}$, and $\langle X, S\rangle_{\mathbb{F}} \in \mathcal{W}$. Then*

$$\Delta\left(\mathsf{nmExt}(X)\,;\, 0^{2k}\|U_k\right) \leq 2^{-990k}\ ,$$

where U_k is a uniform k-bit string independent from X, S.

Proof. Notice that if X and S were independent and uniform then this would follow trivially from the fact that nmExt is a 3-source extractor (Notice that we don't need the non-malleability property of nmExt for this part of the proof). Thus, in order to show this, it is sufficient to establish that X and S are nearly independent given partial knowledge about $\langle X, S\rangle_{\mathbb{K}}$, and $\langle X, S\rangle_{\mathbb{F}}$. We show this as follows.

Let X', S' be distributed independently and uniform in $\mathcal{X}, \mathcal{S}$, respectively. Notice that $\mathbf{H}_\infty(X') \geq 3n - 300k$, and $\mathbf{H}_\infty(S') \geq 3n - 300k$, and hence $\widetilde{\mathbf{H}}_\infty(X' | \mathsf{nmExt}(X')) \geq 3n - 303k$. By Lemma 3, we get that

$$(\langle X', S'\rangle_{\mathbb{K}},\, \mathsf{nmExt}(X'),\, \mathsf{nmExt}(S')) \;\approx_{2^{-(1000k)}}\; (U_n,\, \mathsf{nmExt}(X'),\, \mathsf{nmExt}(S'))\,,$$

where we assumed that $n \geq 5000k$. Since $\langle X', S'\rangle_{\mathbb{F}} = \mathrm{tr}_{\mathbb{K}\to\mathbb{F}}(\langle X', S'\rangle_{\mathbb{K}})$, where $\mathrm{tr}_{\mathbb{K}\to\mathbb{F}}$ is the field trace function, we have that

$$(\langle X', S'\rangle_{\mathbb{K}},\, \langle X', S'\rangle_{\mathbb{F}},\, \mathsf{nmExt}(X'),\, \mathsf{nmExt}(S')) \;\approx_{2^{-1000k}}\; (U_n,\, \mathrm{tr}_{\mathbb{K}\to\mathbb{F}}(U_n), \mathsf{nmExt}(X'),\, \mathsf{nmExt}(S'))\,.$$

Let $(\widetilde{X}, \widetilde{S})$ be jointly distributed as (X', S') conditioned on $\langle X', S'\rangle_{\mathbb{K}} \in \mathcal{V}$, $\langle X', S'\rangle_{\mathbb{F}} \in \mathcal{W}$. Thus, by Lemma 6, we get that

$$(\mathsf{nmExt}(\widetilde{X}),\, \mathsf{nmExt}(\widetilde{S})) \;\approx_{2^{-1000k}}\; (\mathsf{nmExt}(X'),\, \mathsf{nmExt}(S'))\,.$$

Also, since $\mathbf{H}_\infty(X'_i) \geq n - 100k \geq n(1-\delta)$, $\mathbf{H}_\infty(S'_i) \geq n - 100k \geq n(1-\delta)$ for $n = 1,2,3$. Thus, by Theorem 3, we have that

$$(\mathsf{nmExt}(X'),\, \mathsf{nmExt}(S')) \;\approx_{2\cdot 2^{-1000k}}\; (U_k,\, U'_k)\,.$$

By triangle inequality, we get that

$$(\mathsf{nmExt}(\widetilde{X}), \mathsf{nmExt}(\widetilde{S})) \approx_{3\cdot 2^{-1000k}} (U_k, U'_k)\ .$$

Conditioning on $\mathsf{nmExt}'(\widetilde{X}) \neq \perp$, and $\mathsf{nmExt}'(\widetilde{S}) \neq \perp$ and applying Lemma 6, we obtain the desired result. □

We now show that for any given partition, if the tampering oracle outputs $\perp$ with high probability, then the desired statistical distance for that particular partition is small.

Lemma 10. *Let $\mathcal{X}_1, \mathcal{X}_2, \mathcal{X}_3, \mathcal{S}_1, \mathcal{S}_2, \mathcal{S}_3, \mathcal{V} \subseteq \mathbb{K}$, and let $\mathcal{W} \subseteq \mathbb{F}$. We denote $\mathcal{X} = (\mathcal{X}_1, \mathcal{X}_2, \mathcal{X}_3)$ and $\mathcal{S} = (\mathcal{S}_1, \mathcal{S}_2, \mathcal{S}_3)$. Let (X, S) be random variables uniform in $\{0,1\}^{6n}$ conditioned on the event that $X_i \in \mathcal{X}_i$, $S_i \in \mathcal{S}_i$ for $i = 1,2,3$, $\mathsf{nmExt}'(X) \neq \perp$, $\mathsf{nmExt}'(S) \neq \perp$, $\langle X, S\rangle_{\mathbb{K}} \in \mathcal{V}$, and $\langle X, S\rangle_{\mathbb{F}} \in \mathcal{W}$. Let C be the random variable*

$$(X, S, \langle X, S\rangle_{\mathbb{K}}, \langle X, S\rangle_{\mathbb{F}})\ .$$

If

$$\Pr_C[\mathsf{Tamp}_C^{\mathsf{state}}(f,g,h_1,h_2)=\perp]\geq 1-\varepsilon$$

then for any integer $r\geq 0$

$$\Delta\left((\mathsf{CT}_C^r,\mathsf{nmExt}(X))\,;\,(\mathsf{CT}_C^r,0^{2k}\|U_k)\right)\leq\Delta\left(\mathsf{nmExt}(X)\,;\,0^{2k}\|U_k\right)+2\varepsilon\ ,$$

where U_k is a uniform k-bit string independent from X,S.

Proof. Let T_C denote $\mathsf{Tamp}_C^{\mathsf{state}}(f,g,h_1,h_2)$. Notice that for any $m\in\{0,1\}^{3k}$, we have that

$$\Pr[T_C=\perp,\mathsf{nmExt}(X)=m]\leq\Pr[\mathsf{nmExt}(X)=m]\ .$$

Since we know that the statistical distance between two random variables A and B is

$$\sum_{a:\Pr[A=a]>\Pr[B=a]}(\Pr[A=a]-\Pr[B=a])\ ,$$

we have that

$$\Delta\left((T_C,\mathsf{nmExt}(X))\,;\,(\perp,\mathsf{nmExt}(X))\right)=\Pr[T_C\neq\perp]\leq\varepsilon\ .$$

This implies that

$$\Delta\left((\mathsf{CT}_C^r,\mathsf{nmExt}(X))\,;\,(\perp^r,\mathsf{nmExt}(X))\right)\leq\varepsilon\ , \tag{4}$$

where by $\perp^r$ we mean the tampering oracle outputs $\perp$ in the first and hence in each of the subsequent rounds. By equation 4 and Lemma 2, we have that

$$\Delta\left((\mathsf{CT}_C^r,0^{2k}\|U_k)\,;\,(\perp^r,0^{2k}\|U_k)\right)=\Delta\left(\mathsf{CT}_C^r\,;\,\perp^r\right)\leq\varepsilon\ , \tag{5}$$

By equation 4 and equation 5, and the triangle inequality, we get the desired result. □

It is easy to see that when X,S are restricted to "belong" to a partition of Type 1b and 5b, the tampering oracle outputs $\perp$ with probability 1 and hence for partitions of this type, the corresponding statistical distance can be bounded using Lemma 10 and Lemma 9. We will now see that a similar result holds for Type 2, 3, and 4.

Lemma 11. *[Type 2 partition] Let $\mathcal{X}_{1,i_1},\mathcal{X}_{2,i_2},\mathcal{X}_{3,i_3},\mathcal{S}_{1,j_1},\mathcal{S}_{2,j_3},\mathcal{S}_{3,j_3},\mathcal{V}\subseteq\mathbb{K}$, and let $\mathcal{W}\subseteq\{0,1\}^{2k}$. We denote $\mathcal{X}^\star=(\mathcal{X}_{1,i_1},\mathcal{X}_{2,i_2},\mathcal{X}_{3,i_3})$ and $\mathcal{S}^\star=\mathcal{S}_{1,j_1},\mathcal{S}_{2,j_2},\mathcal{S}_{3,j_3}$. Let $(\mathcal{X}^\star,\mathcal{S}^\star,\mathcal{V},\mathcal{W})$ be a partition of Type 2, and let $q[\mathcal{X}^\star,\mathcal{S}^\star,\mathcal{V},\mathcal{W}]\geq 2^{-45k}$. Let X,S be random variables uniform in $\{0,1\}^{6n}$ conditioned on the event that $X_t\in\mathcal{X}_{t,i_t}$, $S_t\in\mathcal{S}_{t,j_t}$ for $t=1,2,3$, $\mathsf{nmExt}'(X)\neq\perp$, $\mathsf{nmExt}'(S)\neq\perp$, $\langle X,S\rangle_{\mathbb{K}}\in\mathcal{V}$, and $\langle X,S\rangle_{\mathbb{F}}\in\mathcal{W}$. Let C be the random variable*

$$(X,S,\langle X,S\rangle_{\mathbb{K}},\langle X,S\rangle_{\mathbb{F}})\ .$$

Then,

$$\Pr_C[\mathsf{Tamp}_C^{\mathsf{state}}(f,g,h_1,h_2)=\perp]\geq 1-2\cdot 2^{-2k}\ .$$

Proof. In this lemma, the given partition is of Type 2, which means that at least one of $i_1,i_2,i_3,j_1,j_2,j_3\neq 0$, and so without loss of generality, let $i_1>0$. If X_1,X_2,X_3 were independent random variables then, by the non-malleability property of the non-malleable extractor, and the fact that f,g are nearly bijective functions, $\mathsf{nmExt}(X)$ and $\mathsf{nmExt}(f(X))$ are close to being uniform and independent.

However the constraint that $\langle X,S\rangle_{\mathbb{K}} \in \mathcal{V}$ and $\langle X,S\rangle_{\mathbb{F}} \in \mathcal{W}$ might introduce dependence between X_1, X_2, X_3.

To overcome this hurdle, it is sufficient to establish that $X_1, X_2, X_3, S_1, S_2, S_3$ are nearly independent given partial knowledge about $\langle X,S\rangle_{\mathbb{K}}$, and $\langle X,S\rangle_{\mathbb{F}}$. The proof of this is almost identical to that of Lemma 9. The details follow.

Firstly, by Lemma 7, we have that

$$p[\mathcal{X},\mathcal{S},\mathcal{V},\mathcal{W}] \geq 2^{-45k-1} ,$$

and

$$\Pr[\widetilde{X} \in \mathcal{X},\ \widetilde{S} \in \mathcal{S},\ U_n \in \mathcal{V},\ \mathrm{tr}_{\mathbb{K}\to\mathbb{F}}(U_n) \in \mathcal{W}] \geq 2^{-45k-1} ,$$

where $\widetilde{X}, \widetilde{S}$ are independent and uniform in $\mathbb{K}^3$. Let X', S' be distributed independently and uniform in $\mathcal{X}^\star, \mathcal{S}^\star$, respectively. Notice that $\mathbf{H}_\infty(X') \geq 3n - 45k - 1$, and $\mathbf{H}_\infty(S') \geq 3n - 45k - 1$, and hence $\widetilde{\mathbf{H}}_\infty\left(X' | \mathsf{nmExt}(X'), \mathsf{nmExt}(f(X'))\right) \geq 3n - 51k - 2$. By Lemma 3, we get that

$$\Delta\left(\langle X',S'\rangle_{\mathbb{K}}\ ;\ U_n | \mathsf{nmExt}(X'),\ \mathsf{nmExt}(f(X'))\right) \leq 2^{-1000k} ,$$

where we use the fact that $n \geq 5000k$. Since $\langle X',S'\rangle_{\mathbb{F}} = \mathrm{tr}_{\mathbb{K}\to\mathbb{F}}(\langle X',S'\rangle_{\mathbb{K}})$, where $\mathrm{tr}_{\mathbb{K}\to\mathbb{F}}$ is the field trace function, we have that

$$\Delta\left(\langle X',S'\rangle_{\mathbb{K}},\ \langle X',S'\rangle_{\mathbb{F}}\ ;\ U_n,\ \mathrm{tr}_{\mathbb{K}\to\mathbb{F}}(U_n) | \mathsf{nmExt}(X'),\ \mathsf{nmExt}(f(X'))\right) \leq 2^{-1000k} ,$$

Let $(\widetilde{X}, \widetilde{S})$ be jointly distributed as (X', S') conditioned on $\langle X',S'\rangle_{\mathbb{K}} \in \mathcal{V}$, $\langle X',S'\rangle_{\mathbb{F}} \in \mathcal{W}$. Thus, by Lemma 6, we get that

$$\Delta(\Big(\mathsf{nmExt}(\widetilde{X}),\ \mathsf{nmExt}(f(\widetilde{X}))\ ;\ \Big(\mathsf{nmExt}(X'),\ \mathsf{nmExt}(f(X'))\Big) \leq 2^{-955k} .$$

Since $\mathbf{H}_\infty(X'_i) \geq n - 45k \geq n(1-\delta)$, for $i = 1,2,3$, by Theorem 3, we have that

$$\Delta\left(\mathsf{nmExt}(X')\ ;\ U_{3k}\ |\ \mathsf{nmExt}(f(X'))\right) \leq 2^{-1000k} .$$

Also, since the partition is of Type 2 and hence i_1, i_2, i_3 are at most $\frac{\delta n}{100k} - 1$, $\mathbf{H}_\infty(f_i(X'_i)) \geq n(1-\delta)$ for $i = 1,2,3$. Thus, using Theorem 3 we have that

$$\Delta\left(\mathsf{nmExt}(f(X'))\ ;\ U'_{3k}\right) \leq 2^{-1000k} .$$

By triangle inequality, we get that

$$(\mathsf{nmExt}(\widetilde{X}), \mathsf{nmExt}(f(\widetilde{X})) \approx_{3\cdot 2^{-1000k}} (U_{3k}, U'_{3k}) .$$

Conditioning on $\mathsf{nmExt}'(\widetilde{X}) \neq \perp$, by Lemma 6, we get that

$$(\mathsf{nmExt}(X), \mathsf{nmExt}(f(X)) \approx_{2^{-98k}} (0^{2k} \| U_k, U'_{3k}) .$$

Thus, the probability that $\mathsf{nmExt}'(f(X)) = \perp$, and hence $\mathsf{Tamp}^{\mathsf{state}}_C(f,g,h_1,h_2) = \perp$ is at least $1 - 2^{-2k} - 2^{-98k}$. □

Lemma 12. *[Type 3 partition] Let $\mathcal{X}_{1,i_1}, \mathcal{X}_{2,i_2}, \mathcal{X}_{3,i_3}, \mathcal{S}_{1,j_1}, \mathcal{S}_{2,j_3}, \mathcal{S}_{3,j_3}, \mathcal{V} \subseteq \mathbb{K}$, and let $\mathcal{W} \subseteq \{0,1\}^{2k}$. We denote $\mathcal{X}^\star = (\mathcal{X}_{1,i_1}, \mathcal{X}_{2,i_2}, \mathcal{X}_{3,i_3})$ and $\mathcal{S}^\star = (\mathcal{S}_{1,j_1}, \mathcal{S}_{2,j_2}, \mathcal{S}_{3,j_3})$. Let $(\mathcal{X}^\star, \mathcal{S}^\star, \mathcal{V}, \mathcal{W})$ be a partition of Type 3, and let $q[\mathcal{X}^\star, \mathcal{S}^\star, \mathcal{V}, \mathcal{W}] \geq 2^{-45k}$. Let (X,S) be random variables uniform in $\{0,1\}^{6n}$ conditioned on the event that $X_t \in \mathcal{X}_{t,i_t}$, $S_t \in \mathcal{S}_{t,j_t}$ for $t = 1,2,3$, $\mathsf{nmExt}'(X) \neq \perp$, $\mathsf{nmExt}'(S) \neq \perp$, $\langle X,S\rangle_{\mathbb{K}} \in \mathcal{V}$, and $\langle X,S\rangle_{\mathbb{F}} \in \mathcal{W}$. Let C be the random variable*

$$(X, S, \langle X,S\rangle_{\mathbb{K}}, \langle X,S\rangle_{\mathbb{F}}) .$$

Then,

$$\Pr_C[\mathsf{Tamp}^{\mathsf{state}}_C(f,g,h_1,h_2) = \perp] \geq 1 - 2^{-4k} .$$

Proof. Since the partition is of Type 3, at least one of $i_1, i_2, i_3, j_1, j_2, j_3 > \frac{\delta n}{100k} - 1$ and

$$i_1 + i_2 + i_3 + j_1 + j_2 + j_3 \leq \frac{n}{40k} .$$

Without loss of generality, let $i_1 > \frac{\delta n}{100k} - 1$.

The intuition behind the proof is that since i_1 is not too small, X has enough entropy given $f(X)$ to ensure that $\langle X, S\rangle_{\mathbb{F}}$ is close to uniform given $f(X), S$ by using the strong extractor property of the inner product. Hence $\langle X, S\rangle_{\mathbb{F}}$ and $\langle f(X), g(S)\rangle_{\mathbb{F}}$ are close to being independent and so the adversary, in order to not decode to $\perp$, should be able to guess $\langle f(X), g(S)\rangle_{\mathbb{F}}$ in the eighth state without having any useful information. Also, since $i_1 + i_2 + i_3 + j_1 + j_2 + j_3$ is not too small, $f(X), g(S)$ together should have enough entropy to ensure that $\langle f(X), g(S)\rangle_{\mathbb{F}}$ is close to being uniform again because the inner product is a strong two-source extractor. This implies that the probability that the decoder does not decode to $\perp$ after tampering is close to 0. Of course, for this argument, we implicitly assumed that X and S are independent and formally we need to take into account the condition that $\langle X, S\rangle_{\mathbb{K}} \in \mathcal{V}$, and $\langle X, S\rangle_{\mathbb{F}} \in \mathcal{W}$ which introduces a limited dependence between X and S. The formal argument is given below.

By Lemma 7, we have that

$$p[\mathcal{X}, \mathcal{S}, \mathcal{V}, \mathcal{W}] \geq 2^{-45k-1} ,$$

and

$$\Pr[\widetilde{X} \in \mathcal{X},\ \widetilde{S} \in \mathcal{S},\ U_n \in \mathcal{V},\ \mathrm{tr}_{\mathbb{K}\to\mathbb{F}}(U_n) \in \mathcal{W}] \geq 2^{-45k-1} .$$

Let X', S' be distributed independently and uniform in $\mathcal{X}^\star, \mathcal{S}^\star$, respectively. We have that $\widetilde{\mathbf{H}}_\infty(X'|f(X')) \geq 100k(i_1 - 1) \geq \delta n - 200k$, and thus $\widetilde{\mathbf{H}}_\infty(X'|f(X'), \mathsf{nmExt}(X')) \geq \delta n - 203k$. Also, $\mathbf{H}_\infty(S') \geq 3n - 45k - 1$. Thus, by Lemma 3,

$$\Delta\left(\langle X', S'\rangle_{\mathbb{F}}\,;\, U_{50k} \mid f(X'), S', \mathsf{nmExt}(X')\right) \leq 2^{-200k} ,$$

where we have used that $\delta n \geq 1000k$. This implies using Lemma 2 that

$$\Delta\left(\langle X', S'\rangle_{\mathbb{F}}\,;\, U_{50k} \mid \langle f(X'), g(S')\rangle_{\mathbb{F}}, \mathsf{nmExt}(X'), \mathsf{nmExt}(S')\right) \leq 2^{-200k} .$$

Also, $\mathbf{H}_\infty(f(X')) \geq 3n - 45k - 100k(i_1 + i_2 + i_3)$, and $\mathbf{H}_\infty(g(S')) \geq 3n - 45k - 100k(j_1 + j_2 + j_3)$. Hence, $\mathbf{H}_\infty(f(X') \mid \mathsf{nmExt}(X')) \geq 3n - 48k - 100k(i_1 + i_2 + i_3)$. Using Lemma 3, we obtain that,

$$\Delta\left(\langle f(X'), g(S')\rangle_{\mathbb{F}}\,;\, U_{50k} \mid \mathsf{nmExt}(X'), \mathsf{nmExt}(S')\right) \leq 2^{-200k} ,$$

where we use the fact that $n \geq 5000k$, and hence

$$3n - 45k + 3n - 48k - 100k(i_1 + i_2 + i_3 + j_1 + j_2 + j_3) - 3n - 50k \geq \frac{n}{2} - 143k \geq 400k .$$

Thus, the triangle inequality implies that

$$\Delta\left(\langle X', S'\rangle_{\mathbb{F}}, \langle f(X'), g(S')\rangle_{\mathbb{F}}\,;\, U_{50k}, U'_{50k} \mid \mathsf{nmExt}(X'), \mathsf{nmExt}(S')\right) \leq 2 \cdot 2^{-200k} .$$

Let $\widetilde{X}, \widetilde{S}$ be distributed as X' conditioned on $\mathsf{nmExt}'(X') \neq \perp$, and S' conditioned on $\mathsf{nmExt}'(S') \neq \perp$, respectively. Then, by conditioned on the event that $\mathsf{nmExt}'(X') \neq \perp$ and $\mathsf{nmExt}'(S') \neq \perp$, and using Lemma 6, we get that

$$\Delta\left(\langle \widetilde{X}, \widetilde{S}\rangle_{\mathbb{F}}, \langle f(\widetilde{X}), g(\widetilde{S})\rangle_{\mathbb{F}}\,;\, U_{50k}, U'_{50k}\right) \leq 2^{-100k} .$$

This implies that

$$\Pr[h_2(\langle \widetilde{X}, \widetilde{S}\rangle_{\mathbb{F}}) = \langle f(\widetilde{X}), g(\widetilde{S})\rangle_{\mathbb{F}}] \leq 2^{-100k} + 2^{-50k} .$$

Thus,

$$\begin{aligned}
\Pr[h_2(\langle \widetilde{X}, \widetilde{S}\rangle_{\mathbb{F}}) = \langle f(\widetilde{X}), g(\widetilde{S})\rangle_{\mathbb{F}} \mid \langle \widetilde{X}, \widetilde{S}\rangle_{\mathbb{K}} \in \mathcal{V},\ \langle \widetilde{X}, \widetilde{S}\rangle_{\mathbb{F}} \in \mathcal{W}] &\leq \frac{\Pr[h_2(\langle \widetilde{X}, \widetilde{S}\rangle_{\mathbb{F}}) = \langle f(\widetilde{X}), g(\widetilde{S})\rangle_{\mathbb{F}}]}{\Pr[\langle \widetilde{X}, \widetilde{S}\rangle_{\mathbb{K}} \in \mathcal{V},\ \langle \widetilde{X}, \widetilde{S}\rangle_{\mathbb{F}} \in \mathcal{W}]} \\
&\leq \frac{2^{-100k} + 2^{-50k}}{2^{-45k}} \\
&\leq 2^{-4k} ,
\end{aligned}$$

which implies the result. □

Lemma 13. *[Type 4 partition] Let $\mathcal{X}_{1,i_1}, \mathcal{X}_{2,i_2}, \mathcal{X}_{3,i_3}, \mathcal{S}_{1,j_1}, \mathcal{S}_{2,j_3}, \mathcal{S}_{3,j_3} \subseteq \mathbb{K} \setminus \{0\}$, $\mathcal{V} \subseteq \mathbb{K}$ and let $\mathcal{W} \subseteq \{0,1\}^{2k}$. We denote $\mathcal{X}^\star = (\mathcal{X}_{1,i_1}, \mathcal{X}_{2,i_2}, \mathcal{X}_{3,i_3})$ and $\mathcal{S}^\star = \mathcal{S}_{1,j_1}, \mathcal{S}_{2,j_2}, \mathcal{S}_{3,j_3}$. Let $(\mathcal{X}^\star, \mathcal{S}^\star, \mathcal{V}, \mathcal{W})$ be a partition of Type 4, and let $q[\mathcal{X}^\star, \mathcal{S}^\star, \mathcal{V}, \mathcal{W}] \geq 2^{-45k}$. Let (X, S) be random variables uniform in $\{0,1\}^{6n}$ conditioned on the event that $X_t \in \mathcal{X}_{t,i_t}$, $S_t \in \mathcal{S}_{t,j_t}$ for $t = 1, 2, 3$, $\mathsf{nmExt}'(X) \neq \perp$, $\mathsf{nmExt}'(S) \neq \perp$, $\langle X, S\rangle_{\mathbb{K}} \in \mathcal{V}$, and $\langle X, S\rangle_{\mathbb{F}} \in \mathcal{W}$. Let C be the random variable*

$$(X, S, \langle X, S\rangle_{\mathbb{K}}, \langle X, S\rangle_{\mathbb{F}}) .$$

Then,

$$\Pr_C[\mathsf{Tamp}_C^{\mathsf{state}}(f, g, h_1, h_2) = \perp] \geq 1 - 2^{-4k} .$$

Proof. Since the partition is of Type 4, at least one of $i_1, i_2, i_3, j_1, j_2, j_3 \neq \ell$ and

$$i_1 + i_2 + i_3 + j_1 + j_2 + j_3 > \frac{n}{40k} .$$

Without loss of generality, let $i_1 \leq \ell - 1$. Also, without loss of generality, let $i_1 + i_2 + i_3 > \frac{n}{80k}$.

The intuition behind the proof is that $i_1 + i_2 + i_3$ is large enough to ensure that X has enough entropy given $f(X)$ to ensure that $\langle X, S\rangle_{\mathbb{K}}$ is close to uniform given $f(X), S$ by using the strong extractor property of the inner product. Hence $\langle X, S\rangle_{\mathbb{K}}$ and $\langle f(X), g(S)\rangle_{\mathbb{K}}$ are close to being independent and so the adversary, in order to decode to a valid message, should be able to guess $\langle f(X), g(S)\rangle_{\mathbb{K}}$ in the seventh state without having any useful information. Also, since $i_1 \leq \ell - 1$ is not too small, $f_1(X_1)$ has a large amount of entropy which in turn implies that $\langle f(X), g(S)\rangle_{\mathbb{K}}$ has a large amount of entropy since $g_1(S_1) \neq 0$. This implies that the probability that the decoder does not decode to $\perp$ after tampering is close to 0. Of course, for this argument to go through, we implicitly assumed that X and S are independent and formally we need to take into account the condition that $\langle X, S\rangle_{\mathbb{K}} \in \mathcal{V}$, and $\langle X, S\rangle_{\mathbb{F}} \in \mathcal{W}$ which introduces a limited dependence between X and S. The formal argument is given below.

By Lemma 7, we have that

$$p[\mathcal{X}, \mathcal{S}, \mathcal{V}, \mathcal{W}] \geq 2^{-45k-1} ,$$

and

$$\Pr[\widetilde{X} \in \mathcal{X},\ \widetilde{S} \in \mathcal{S},\ U_n \in \mathcal{V},\ \mathrm{tr}_{\mathbb{K}\to\mathbb{F}}(U_n) \in \mathcal{W}] \geq 2^{-45k-1} .$$

Let X', S' be distributed independently and uniform in $\mathcal{X}^\star, \mathcal{S}^\star$, respectively. We have that $\widetilde{\mathbf{H}}_\infty(X'|f(X')) \geq 100k(i_1 - 1 + i_2 - 1 + i_3 - 1) \geq \frac{5n}{4} - 300k$, and $\mathbf{H}_\infty(S') \geq 3n - 45k$. Thus, by Lemma 3,

$$\Delta\left(\langle X', S'\rangle_{\mathbb{K}}\,;\, U_n \mid f(X'), S'\right) \leq 2^{-450k} ,$$

where we have used that $n \geq 5000k$. This implies using Lemma 2 that

$$\Delta\left(\langle X', S'\rangle_{\mathbb{K}}\,;\, U_n \mid \langle f(X'), g(S')\rangle_{\mathbb{K}}\right) \leq 2^{-450k} .$$

This implies that

$$\begin{aligned}
\Pr[h_1(\langle X', S'\rangle_{\mathbb{K}}) = \langle f(X'), g(S')\rangle_{\mathbb{K}}] &\leq 2^{-450k} + \Pr[h_1(U_n) = \langle f(X'), g(S')\rangle_{\mathbb{K}}] \\
&\leq 2^{-450k} + 2^{-\mathbf{H}_\infty(\langle f(X'), g(S')\rangle_{\mathbb{K}})} \\
&\leq 2^{-450k} + 2^{-\mathbf{H}_\infty(f_1(X_1'))} \\
&\leq 2^{-450k} + 2^{-55k} \\
&\leq 2^{-54k} , \qquad (6)
\end{aligned}$$

where the second to last inequality uses the fact that $i_1 \leq \ell - 1$, and hence $\mathbf{H}_\infty(f_i(X_i')) \geq 55k$.

Also, since $\widetilde{\mathbf{H}}_\infty(X' | \mathsf{nmExt}(X')) \geq 3n - 45k - 3k$, using a similar argument as above, we have that

$$\Delta\left(\langle X', S'\rangle_{\mathbb{K}}\,;\, U_n \mid \mathsf{nmExt}(X'), \mathsf{nmExt}(S')\right) \leq 2^{-450k} .$$

Additionally, since $\mathbf{H}_\infty(X_i') \geq n - 45k \geq n(1-\delta)$ and $\mathbf{H}_\infty(S_i') \geq n - 45k \geq n(1-\delta)$, for $i = 1, 2, 3$, we have that

$$\Delta\left(\mathsf{nmExt}(X'),\, \mathsf{nmExt}(S')\ ;\ U_{3k},\, U_{3k}'\right) \leq 2 \cdot 2^{-1000k} .$$

Thus, the triangle inequality implies that

$$\Delta\left(\langle X', S'\rangle_{\mathbb{K}},\, \mathsf{nmExt}(X'),\, \mathsf{nmExt}(S')\ ;\ U_n,\, U_{3k},\, U_{3k}'\right) \leq 3 \cdot 2^{-1000k} .$$

This implies that

$$\Pr[E] \geq 2^{-45k} \cdot 2^{-4k} - 3 \cdot 2^{-1000k} \geq 2^{-50k} , \qquad (7)$$

where E is shorthand for the event that $\mathsf{nmExt}(X') \neq \perp$, $\mathsf{nmExt}(S') \neq \perp$, $\langle X', S'\rangle_{\mathbb{K}} \in \mathcal{V}$, and $\mathrm{tr}_{\mathbb{K}\to\mathbb{F}}(\langle X', S'\rangle_{\mathbb{K}}) \in \mathcal{W}$. Combining inequalities 6 and 7, we get that

$$\begin{aligned}
\Pr[h_1(\langle X, S\rangle_{\mathbb{K}}) = \langle f(X), g(S)\rangle_{\mathbb{K}}] &= \Pr[h_1(\langle X', S'\rangle_{\mathbb{K}}) = \langle f(X'), g(S')\rangle_{\mathbb{K}} \mid E] \\
&\leq \frac{\Pr[h_1(\langle X', S'\rangle_{\mathbb{K}}) = \langle f(X'), g(S')\rangle_{\mathbb{K}}}{\Pr[E]} \\
&\leq \frac{2^{-54k}}{2^{-50k}} \\
&\leq 2^{-4k} .
\end{aligned}$$

□

In the above results, we established that the tampering oracle will output $\perp$ with probability very close to 1 for all partitions of Type 2, 3, 4 that are not too small. If the size of the partition is extremely small then Lemma 8 guarantees that such a partition does not contribute much to the statistical distance. Also, for a partition of Type 1b and 5b, the tampering oracle always outputs $\perp$. The following corollary states the bound on the statistical distance conditioned on X, S in a partition of Type 1b, 2, 3, 4, 5b.

Corollary 2. *Let $\mathcal{X}_1, \mathcal{X}_2, \mathcal{X}_3, \mathcal{S}_1, \mathcal{S}_2, \mathcal{S}_3, \mathcal{V} \subseteq \mathbb{K}$, and let $\mathcal{W} \subseteq \mathbb{F}$. We denote $\mathcal{X} = (\mathcal{X}_1, \mathcal{X}_2, \mathcal{X}_3)$ and $\mathcal{S} = \mathcal{S}_1, \mathcal{S}_2, \mathcal{S}_3$. Let $q[\mathcal{X}, \mathcal{S}, \mathcal{V}, \mathcal{W}] \geq 2^{-40k}$. Let X, S be random variables uniform in $\{0,1\}^{6n}$*

conditioned on the event that $X_i \in \mathcal{X}_i$*,* $S_i \in \mathcal{S}_i$ *for* $i = 1, 2, 3$*,* $\mathsf{nmExt}'(X) \neq \perp$*,* $\mathsf{nmExt}'(S) \neq \perp$*,* $\langle X, S\rangle_{\mathbb{K}} \in \mathcal{V}$*, and* $\langle X, S\rangle_{\mathbb{F}} \in \mathcal{W}$*. Let* C *be the random variable*

$$(X, S, \langle X, S\rangle_{\mathbb{K}}, \langle X, S\rangle_{\mathbb{F}}) \ .$$

Then for any integer $r \geq 0$*, if*

$$\sum_{\mathcal{P}:\, Type(\mathcal{P}) \in \{1b,\, 2,\, ,3,\, 4,5b\}} \frac{q[\mathcal{P}]}{q[\mathcal{X}, \mathcal{S}, \mathcal{V}, \mathcal{W}]} \cdot \Delta\left((\mathsf{CT}^r_C, \mathsf{nmExt}(X))|_{C\in\mathcal{P}}\,;\, (\mathsf{CT}^r_C, 0^{2k}\|U_k)|_{C\in\mathcal{P}}\right) \leq 5 \cdot 2^{-2k} \ ,$$

where U_k *is a uniform* k*-bit string independent from* X, S*.*

Proof. It follows from the definition that if $\mathcal{P}$ is a Type 1b or Type 5b partition, then either

$$\Pr[\langle f(X), g(S)\rangle_{\mathbb{K}} \neq h_1(\langle X, S\rangle_{\mathbb{K}}) \mid C \in \mathcal{P}] = 1 \ ,$$

or

$$\Pr[\langle f(X), g(S)\rangle_{\mathbb{F}} \neq h_1(\langle X, S\rangle_{\mathbb{F}}) \mid C \in \mathcal{P}] = 1 \ ,$$

and hence

$$\Pr_C[\mathsf{Tamp}^{\mathsf{state}}_C(f, g, h_1, h_2) = \perp \mid C \in \mathcal{P}] = 1 \ .$$

By Lemmata 11, 12, and 13, we have that if $\mathcal{P}$ is a Type 2, 3, or 4 partition then

$$\Pr_C[\mathsf{Tamp}^{\mathsf{state}}_C(f, g, h_1, h_2) = \perp \mid C \in \mathcal{P}] \geq 1 - 2 \cdot 2^{-2k} \ .$$

By Lemma 10, this implies that for any partition $\mathcal{P}$ of Type 1b, 2, 3, 4, 5b, we have that

$$\Delta\left((\mathsf{CT}^r_C, \mathsf{nmExt}(X))|_{C\in\mathcal{P}}\,;\, (\mathsf{CT}^r_C, 0^{2k}\|U_k)|_{C\in\mathcal{P}}\right) \leq \Delta\left(\mathsf{nmExt}(X)|_{C\in\mathcal{P}}\,;\, 0^{2k}\|U_k\right) + 4 \cdot 2^{-2k} \ .$$

So, we need to bound $\Delta\left(\mathsf{nmExt}(X)|_{C\in\mathcal{P}}\,;\, 0^{2k}\|U_k\right)$ for each partition. By Lemma 9, we get that if $q[\mathcal{P}] \geq 2^{-800k}$ then

$$\Delta\left(\mathsf{nmExt}(X)|_{C\in\mathcal{P}}\,;\, 0^{2k}\|U_k\right) \leq 2^{-90k} \ .$$

Thus, $\sum_{\mathcal{P}} \frac{q[\mathcal{P}]}{q[\mathcal{X},\mathcal{S},\mathcal{V},\mathcal{W}]} \cdot \Delta\left((\mathsf{CT}^r_C, \mathsf{nmExt}(X))|_{C\in\mathcal{P}}\,;\, (\mathsf{CT}^r_C, 0^{2k}\|U_k)|_{C\in\mathcal{P}}\right)$, where the sum is over all partitions $\mathcal{P}$ of Type 1b, 2, 3, 4, and 5b is at most

$$\begin{aligned} &\sum_{\mathcal{P}: q[\mathcal{P}] \geq 2^{-800k}} \frac{q[\mathcal{P}]}{q[\mathcal{X}, \mathcal{S}, \mathcal{V}, \mathcal{W}]} \cdot (2^{-90k} + 4 \cdot 2^{-2k}) + \sum_{\mathcal{P}: q[\mathcal{P}] < 2^{-800k}} \frac{q[\mathcal{P}]}{q[\mathcal{X}, \mathcal{S}, \mathcal{V}, \mathcal{W}]} \cdot 1 \\ \leq\ & 2^{-90k} + 4 \cdot 2^{-2k} + \frac{2^{-800k}}{2^{-40k}} \cdot (2^{600k} \cdot 2 + 2 + \ell^6) \\ \leq\ & 5 \cdot 2^{-2k} \ , \end{aligned}$$

where we used that there are 2 partitions of Type 1b, at most ℓ^6 partitions of Type 2, 3, and 4, and each partition of Type 5b contains at least $2^{6n-600k}$ elements from $\mathcal{X}, \mathcal{S}$ that are all distinct, which implies that the number of partitions of Type 5b is at most $2 \cdot 2^{600k}$. □

Lemma 14. *[Type 5 partition] Let* $\mathcal{X}_{1,\ell}, \mathcal{X}_{2,\ell}, \mathcal{X}_{3,\ell}, \mathcal{S}_{1,\ell}, \mathcal{S}_{2,\ell}, \mathcal{S}_{3,\ell} \subseteq \mathbb{K} \setminus \{0\}$*,* $\mathcal{V} \subseteq \mathbb{K}$*, and let* $\mathcal{W} \subseteq \{0,1\}^{2k}$*. We denote* $\mathcal{X}^\star = (\mathcal{X}_{1,\ell}, \mathcal{X}_{2,\ell}, \mathcal{X}_{3,\ell})$ *and* $\mathcal{S}^\star = \mathcal{S}_{1,\ell}, \mathcal{S}_{2,\ell}, \mathcal{S}_{3,\ell}$*. Let* $(\mathcal{X}^\star, \mathcal{S}^\star, \mathcal{V}, \mathcal{W})$ *be a partition of Type 5, and let* $q[\mathcal{X}^\star, \mathcal{S}^\star, \mathcal{V}, \mathcal{W}] \geq 2^{-45k}$*. Let* (X, S) *be random variables uniform in* $\{0,1\}^{6n}$

conditioned on the event that $X_i \in \mathcal{X}_{1,\ell}$*,* $S_i \in \mathcal{S}_{i,\ell}$ *for* $i = 1,2,3$*,* $\mathsf{nmExt}'(X) \neq \perp$*,* $\mathsf{nmExt}'(S) \neq \perp$*,* $\langle X, S\rangle_{\mathbb{K}} \in \mathcal{V}$*, and* $\langle X, S\rangle_{\mathbb{F}} \in \mathcal{W}$*. Then,*

$$\sum_{\mathbf{a},\mathbf{b}} \left(\frac{q[\mathcal{X}_{\mathbf{a}}, \mathcal{S}_{\mathbf{b}}, \mathcal{V}_{\langle \mathbf{a},\mathbf{b}\rangle_{\mathbb{K}}}, \mathcal{W}_{\langle \mathbf{a},\mathbf{b}\rangle_{\mathbb{F}}}]}{q[\mathcal{X}_{1,\ell}, \mathcal{S}_{1,\ell}, \mathcal{V}, \mathcal{W}]}\right)^{7/8} \leq \sum_{\mathbf{a},\mathbf{b}} \Pr[h_1(\langle X, S\rangle_{\mathbb{K}}) = \langle \mathbf{a},\mathbf{b}\rangle_{\mathbb{K}},\ f(X) = \mathbf{a},\ g(S) = \mathbf{b}]^{\frac{7}{8}} \leq 1{+}2^{-50k} .$$

Proof. Since the partition is of Type 5, we have

$$i_1 = i_2 = i_3 = j_1 = j_2 = j_3 = \ell .$$

By Lemma 7, we have that

$$p[\mathcal{X}, \mathcal{S}, \mathcal{V}, \mathcal{W}] \geq 2^{-45k-1} ,$$

and

$$\Pr[\widetilde{X} \in \mathcal{X},\ \widetilde{S} \in \mathcal{S},\ U_n \in \mathcal{V},\ \mathrm{tr}_{\mathbb{K}\to\mathbb{F}}(U_n) \in \mathcal{W}] \geq 2^{-45k-1} .$$

Let X', S' be distributed independently and uniform in $\mathcal{X}^\star, \mathcal{S}^\star$, respectively. We have that

$$\widetilde{\mathbf{H}}_\infty(X'|f(X'), \mathsf{nmExt}(X')) \geq 100k(3\ell-3) - 3k = 3n - 303k , \quad \text{and} \quad \mathbf{H}_\infty(S') \geq 3n - 45k .$$

Thus, by Lemma 3,

$$\Delta\left(\langle X', S'\rangle_{\mathbb{K}}\,;\, U_n \mid f(X'), \mathsf{nmExt}(X'), S'\right) \leq 2^{-1000k} ,$$

where we have used that $n \geq 5000k$. This implies using Lemma 2 that

$$\Delta\left(\langle X', S'\rangle_{\mathbb{K}}\,;\, U_n \mid \langle f(X'), g(S')\rangle_{\mathbb{K}}, \mathsf{nmExt}(X'), \mathsf{nmExt}(S')\right) \leq 2^{-1000k} .$$

Also, $\widetilde{\mathbf{H}}_\infty(X'_i|f_i(X'_i)) \geq 100k(\ell-1) \geq n(1-\delta)$, and $\widetilde{\mathbf{H}}_\infty(S'_i|g_i(S'_i)) \geq 100k(\ell-1) \geq n(1-\delta)$ for $i = 1,2,3$. Thus, by Lemma 3,

$$\Delta\left(\mathsf{nmExt}(X'),\, \mathsf{nmExt}(S')\,;\, U_{3k},\, U'_{3k} \mid \langle f(X'), g(S')\rangle_{\mathbb{K}}\right) \leq 2 \cdot 2^{-200k} .$$

Using triangle inequality, we get that

$$\Delta\left(\langle X', S'\rangle_{\mathbb{K}},\, \mathsf{nmExt}(X'),\, \mathsf{nmExt}(S')\,;\, U_n,\, U_{3k},\, U'_{3k} \mid \langle f(X'), g(S')\rangle_{\mathbb{K}}\right) \leq 3 \cdot 2^{-200k} .$$

Conditioning on $\mathsf{nmExt}'(X') \neq \perp$, $\mathsf{nmExt}'(S') \neq \perp$, $\langle X', S'\rangle_{\mathbb{K}} \in \mathcal{V}$, and $\mathrm{tr}_{\mathbb{K}\to\mathbb{F}}(\langle X', S'\rangle_{\mathbb{K}}) \in \mathcal{W}$ we get that

$$\Delta\left(\langle f(X), g(S)\rangle_{\mathbb{K}},\, \langle X, S\rangle_{\mathbb{K}}\,;\, \langle f(X'), g(S')\rangle_{\mathbb{K}},\, V\right) \leq 2^{-150k} , \tag{8}$$

where V is distributed as U_n conditioned on $U_n \in \mathcal{V}$, and $\mathrm{tr}_{\mathbb{K}\to\mathbb{F}}(U_n) \in \mathcal{W}$. Now using lemma 4 on vector pair $(f_1(X'_1), f_2(X'_2), f_3(X'_3), -1)$ and $(g_1(S'_1), g_2(S'_2), g_3(S'_3), h_1(V))$, and $t = 4$, we obtain

$$\sum_{\substack{(a_1,a_2,a_3,b_1,b_2,b_3,c)\ \mid \\ \langle (a_1,a_2,a_3,-1)\,,\,(b_1,b_2,b_3,c)\rangle_{\mathbb{K}}=0}} \Pr[(f(X'), g(S'), h_1(V)) = (\mathbf{a}, \mathbf{b}, c)]^{\frac{7}{8}} \ \leq\ 1 .$$

Notice that the number of different possible values of the tuple $(a_1, a_2, a_3, b_1, b_2, b_3, c)$ such that $\Pr[(f(X'), g(S'), h_1(V)) = (\mathbf{a}, \mathbf{b}, c)] \neq 0$ is at most 2^{600k}. Thus, using Lemma 5 and the inequality 8, we get that

$$\sum_{\mathbf{a},\mathbf{b}} \Pr[h_1(\langle X, S\rangle_{\mathbb{K}}) = \langle \mathbf{a},\mathbf{b}\rangle_{\mathbb{K}},\ f(X) = \mathbf{a},\ g(S) = \mathbf{b}]^{\frac{7}{8}} \leq 1 + 2^{600k/8} \cdot 2^{-150k\cdot 7/8} \leq 1 + 2^{-50k} .$$

□

Lemma 15. *[Type 1 or Type 5 partition] Let* $\mathcal{X}_1, \mathcal{X}_2, \mathcal{X}_3, \mathcal{S}_1, \mathcal{S}_2, \mathcal{S}_3, \mathcal{V} \subseteq \mathbb{K}$*, and let* $\mathcal{W} \subseteq \{0,1\}^{2k}$*. We denote* $\mathcal{X} = (\mathcal{X}_1, \mathcal{X}_2, \mathcal{X}_3)$ *and* $\mathcal{S} = \mathcal{S}_1, \mathcal{S}_2, \mathcal{S}_3$*. Let* $q[\mathcal{X}, \mathcal{S}, \mathcal{V}, \mathcal{W}] \geq \rho$*. Let* (X, S) *be random variables uniform in* $\{0,1\}^{6n}$ *conditioned on the event that* $X_t \in \mathcal{X}_t$*,* $S_t \in \mathcal{S}_t$ *for* $t = 1,2,3$*,* $\mathsf{nmExt}'(X) \neq \perp$*,* $\mathsf{nmExt}'(S) \neq \perp$*,* $\langle X, S\rangle_{\mathbb{K}} \in \mathcal{V}$*, and* $\langle X, S\rangle_{\mathbb{F}} \in \mathcal{W}$*. Then,*

$$\Pr[X_t \in \mathcal{X}_{t,0},\ S_t \in \mathcal{S}_{t,0} \text{ for } t = 1,2,3]^{1/2} + \Pr[X_t \in \mathcal{X}_{t,\ell},\ S_t \in \mathcal{S}_{t,\ell} \text{ for } t = 1,2,3]^{1/2} \leq 1 + 2^{-90k} ,$$

and hence,

$$\Pr[X_t \in \mathcal{X}_{t,0},\ S_t \in \mathcal{S}_{t,0} \text{ for } t = 1,2,3]^{7/8} + \Pr[X_t \in \mathcal{X}_{t,\ell},\ S_t \in \mathcal{S}_{t,\ell} \text{ for } t = 1,2,3]^{7/8} \leq 1 + 2^{-90k} ,$$

Proof. Let X', S' be distributed independently and uniform in $\mathcal{X}, \mathcal{S}$, respectively. Let $i_1, i_2, i_3, j_1, j_2, j_3 : \mathbb{K} \to \{0, 1, \ldots, \ell\}$ be as defined in the partitioning procedure, i.e., i_1 is a function of X'_1 that indicates the partition in which X'_1 belongs depending on the function f_1, etc.

Since $\widetilde{\mathbf{H}}_\infty(X' | \mathsf{nmExt}(X'), i_1, i_2, i_3) \geq 3n - 40k - 3\log(\ell+1) \geq 3n - 41k$, using Lemma 3, we have that

$$\Delta\left(\langle X', S'\rangle_{\mathbb{K}} \,;\, U_n \mid \mathsf{nmExt}(X'), \mathsf{nmExt}(S'), i_1, i_2, i_3, j_1, j_2, j_3\right) \leq 2^{-450k} .$$

Additionally, since $\widetilde{\mathbf{H}}_\infty(X'_t | i_t) \geq n - 40k - \log(\ell+1) \geq n(1-\delta)$ and $\mathbf{H}_\infty(S'_i) \geq n - 40k - \log(\ell+1) \geq n(1-\delta)$, for $t = 1,2,3$, we have that

$$\Delta\left(\mathsf{nmExt}(X'),\ \mathsf{nmExt}(S') \ ;\ U_{3k},\ U'_{3k} \mid i_1, i_2, i_3, j_1, j_2, j_3\right) \leq 2 \cdot 2^{-200k} .$$

Thus, the triangle inequality implies that

$$\Delta\left(\langle X', S'\rangle_{\mathbb{K}}\, \mathsf{nmExt}(X'),\ \mathsf{nmExt}(S') \ ;\ U_n,\ U_{3k},\ U'_{3k} \mid i_1, i_2, i_3, j_1, j_2, j_3\right) \leq 3 \cdot 2^{-200k} .$$

Conditioning on $\mathsf{nmExt}(X') \neq \perp$, $\mathsf{nmExt}(S') \neq \perp$, $\langle X, S\rangle_{\mathbb{K}} \in \mathcal{V}$, and $\mathrm{tr}_{\mathbb{K}\to\mathbb{F}}(\langle X, S\rangle_{\mathbb{K}}) \in \mathcal{W}$ and using Lemma 6, we get that

$$\Delta\left(i_1(X'_1), i_2(X'_2), i_3(X'_3), j_1(S'_1), j_2(S'_2), j_3(S'_3) \ ;\ i_1(X_1), i_2(X_2), i_3(X_3), j_1(S_1), j_2(S_2), j_3(S_3)\right) \leq 3{\cdot}2^{-200k} . \tag{9}$$

We introduce the following notation. For $r = 0, \ell$, let

$$p_r := \Pr[X'_t \in \mathcal{X}_{t,r} \text{ for } t = 1,2,3] = \Pr[i_1(X'_1) = i_2(X'_2) = i_3(X'_3) = r] ,$$

and

$$q_r := \Pr[S'_t \in \mathcal{S}_{t,r} \text{ for } t = 1,2,3] = \Pr[i_1(S'_1) = i_2(S'_2) = i_3(S'_3) = r] .$$

Then clearly, $p_0 + p_\ell \leq 1$, and $q_0 + q_\ell \leq 1$. This implies

$$\begin{aligned}\Pr[X'_t \in \mathcal{X}_{t,0},\ S'_t \in \mathcal{S}_{t,0} \text{ for } t = 1,2,3]^{1/2} + {} & \Pr[X'_t \in \mathcal{X}_{t,\ell},\ S'_t \in \mathcal{S}_{t,\ell} \text{ for } t = 1,2,3]^{1/2} \\ & = \sqrt{p_0 \cdot q_0} + \sqrt{p_\ell \cdot q_\ell} \\ & \leq \sqrt{p_0 \cdot q_0} + \sqrt{(1-p_0)\cdot(1-q_0)} \\ & \leq 1 ,\end{aligned}$$

using the Cauchy-Schwarz inequality. Thus, using Lemma 5 and the inequality 9, we get that

$$\begin{aligned}\Pr[X_t \in \mathcal{X}_{t,0},\ S_t \in \mathcal{S}_{t,0} \text{ for } t = 1,2,3]^{1/2} + {} & \Pr[X_t \in \mathcal{X}_{t,\ell},\ S_t \in \mathcal{S}_{t,\ell} \text{ for } t = 1,2,3]^{1/2} \\ & \leq 1 + 6 \cdot 2^{-200k \cdot 1/2} \leq 1 + 2^{-90k} .\end{aligned}$$

□

3.3 Proof of Theorem 5

Proof. Now, we prove Theorem 5 by induction on the number of rounds r. For $r = 0$, i.e., when there is no tampering, we need to show that $\mathsf{nmExt}(X)$ is statistically close to $0^{2k} \| U_k$, which follows by Lemma 9. Using Corollary 2, we have that

$$\sum_{\mathcal{P}:\mathrm{Type}(\mathcal{P})\in\{1b,2,,3,4,5b\}} \frac{q[\mathcal{P}]}{q[\mathcal{X},\mathcal{S},\mathcal{V},\mathcal{W}]} \cdot \Delta\left((\mathsf{CT}_C^r, \mathsf{nmExt}(X))|_{C\in\mathcal{P}}\,;\, (\mathsf{CT}_C^r, 0^{2k}\|U_k)|_{C\in\mathcal{P}} \right) \leq 5\cdot 2^{-2k} .$$

Let $\mathcal{Q}_1$ be a partition of Type 1a (note that there is only one such partition), and let $\mathcal{Q}_2, \ldots, \mathcal{Q}_m$ be partitions of Type 5a. Let $\mathcal{X}^\star = (\mathcal{X}_{1,\ell}, \mathcal{X}_{2,\ell}, \mathcal{X}_{3,\ell})$, and $\mathcal{S}^\star = (\mathcal{S}_{1,\ell}, \mathcal{S}_{2,\ell}, \mathcal{S}_{3,\ell})$. We consider two cases.

CASE 1: $q[\mathcal{X}^\star, \mathcal{S}^\star, \mathcal{V}, \mathcal{W}] < 2^{-45k}$.

In this case, the total probability of falling in a partition of Type 5 is small, and so intuitively the only useful information that can be learnt is by landing in a partition of Type 1a. In this case, by Lemma 8 and the induction hypothesis we have that the statistical distance $\Delta\left((\mathsf{CT}_C^r, \mathsf{nmExt}(X))\,;\,(\mathsf{CT}_C^r, 0^{2k}\|U_k)\right)$ is upper bounded by

$$\begin{aligned}
&\leq 5\cdot 2^{-2k} + \frac{q[\mathcal{X}^\star,\mathcal{S}^\star,\mathcal{V},\mathcal{W}]}{q[\mathcal{X},\mathcal{S},\mathcal{V},\mathcal{W}]}\cdot 1 + \frac{q[\mathcal{Q}_1]}{q[\mathcal{X},\mathcal{S},\mathcal{V},\mathcal{W}]}\cdot\left(\left(\frac{\rho}{q[\mathcal{Q}_1]}\right)^{\frac{1}{8}} + 9\cdot(r-1)\cdot 2^{-2k}\right)\\
&\leq 5\cdot 2^{-2k} + 2^{-5k} + \left(\frac{q[\mathcal{Q}_1]}{q[\mathcal{X},\mathcal{S},\mathcal{V},\mathcal{W}]}\right)^{\frac{7}{8}}\cdot\left(\frac{\rho}{q[\mathcal{X},\mathcal{S},\mathcal{V},\mathcal{W}]}\right)^{\frac{1}{8}} + 9\cdot(r-1)\cdot 2^{-2k}\\
&\leq \left(\frac{\rho}{q[\mathcal{X},\mathcal{S},\mathcal{V},\mathcal{W}]}\right)^{\frac{1}{8}} + 9\cdot r\cdot 2^{-2k} .
\end{aligned}$$

CASE 2: $q[\mathcal{X}^\star, \mathcal{S}^\star, \mathcal{V}, \mathcal{W}] \geq 2^{-45k}$. In this case, by Lemma 8, and the induction hypothesis we have that the statistical distance $\Delta\left((\mathsf{CT}_C^r, \mathsf{nmExt}(X))\,;\,(\mathsf{CT}_C^r, 0^{2k}\|U_k)\right)$ is upper bounded by

$$\begin{aligned}
&\leq 5\cdot 2^{-2k} + \sum_{i=1}^{m}\frac{q[\mathcal{Q}_i]}{q[\mathcal{X},\mathcal{S},\mathcal{V},\mathcal{W}]}\cdot\left(\left(\frac{\rho}{q[\mathcal{Q}_i]}\right)^{\frac{1}{8}} + 9\cdot(r-1)\cdot 2^{-2k}\right)\\
&\leq 5\cdot 2^{-2k} + 2^{-5k} + \sum_{i=1}^{m}\left(\frac{q[\mathcal{Q}_i]}{q[\mathcal{X},\mathcal{S},\mathcal{V},\mathcal{W}]}\right)^{\frac{7}{8}}\cdot\left(\frac{\rho}{q[\mathcal{X},\mathcal{S},\mathcal{V},\mathcal{W}]}\right)^{\frac{1}{8}} + 9\cdot(r-1)\cdot 2^{-2k}\\
&\leq \left(\frac{\rho}{q[\mathcal{X},\mathcal{S},\mathcal{V},\mathcal{W}]}\right)^{\frac{1}{8}}(1+2^{-2k}) + 9(r-1)\cdot 2^{-2k} + 6\cdot 2^{-2k}\\
&\leq \left(\frac{\rho}{q[\mathcal{X},\mathcal{S},\mathcal{V},\mathcal{W}]}\right)^{\frac{1}{8}} + 9\cdot r\cdot 2^{-2k} ,
\end{aligned}$$

where the second to last inequality uses Lemma 14 and Lemma 15.

□

References

[AAnHKM+16] Divesh Aggarwal, Shashank Agrawal, Divya Gupta nad Hemanta K. Maji, Omkant Pandey, and Manoj Prabhakaran. Optimal computational split state non-malleable codes. *To appear in TCC 16-A*, 2016.

[AB16] Divesh Aggarwal and Jop Briët. Revisiting the sanders-bogolyubov-ruzsa theorem in f p n and its application to non-malleable codes. In *Information Theory (ISIT), 2016 IEEE International Symposium on*, pages 1322–1326. Ieee, 2016.

[ADKO15a] Divesh Aggarwal, Yevgeniy Dodis, Tomasz Kazana, and Maciej Obremski. Leakage-resilient non-malleable codes. In *The 47th ACM Symposium on Theory of Computing (STOC)*, 2015.

[ADKO15b] Divesh Aggarwal, Stefan Dziembowski, Tomasz Kazana, and Maciej Obremski. Leakage-resilient non-malleable codes. In *Theory of Cryptography*, volume 9014 of *Lecture Notes in Computer Science*, pages 398–426. Springer Berlin Heidelberg, 2015.

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

[Agg15] Divesh Aggarwal. Affine-evasive sets modulo a prime. *Information Processing Letters*, 115(2):382–385, 2015.

[AGM$^+$15a] Shashank Agrawal, Divya Gupta, Hemanta K. Maji, Omkant Pandey, and Manoj Prabhakaran. Explicit non-malleable codes resistant to permutations. *Advances in Cryptology - CRYPTO*, 2015.

[AGM$^+$15b] Shashank Agrawal, Divya Gupta, HemantaK. Maji, Omkant Pandey, and Manoj Prabhakaran. A rate-optimizing compiler for non-malleable codes against bit-wise tampering and permutations. In *Theory of Cryptography*, volume 9014 of *Lecture Notes in Computer Science*, pages 375–397. Springer Berlin Heidelberg, 2015.

[AKO17] Divesh Aggarwal, Tomasz Kazana, and Maciej Obremski. Inception makes non-malleable codes stronger. In *Theory of Cryptography Conference*, pages 319–343. Springer, 2017.

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

[CG14a] Mahdi Cheraghchi and Venkatesan Guruswami. Capacity of non-malleable codes. In *ITCS*, 2014.

[CG14b] Mahdi Cheraghchi and Venkatesan Guruswami. Non-malleable coding against bit-wise and split-state tampering. In *TCC*, 2014.

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

[CMTV15] Sandro Coretti, Ueli Maurer, Björn Tackmann, and Daniele Venturi. From single-bit to multi-bit public-key encryption via non-malleable codes. In Dodis and Nielsen [DN15], pages 532–560.

[CZ14] Eshan Chattopadhyay and David Zuckerman. Non-malleable codes in the constant split-state model. *FOCS*, 2014.

[DKO13] Stefan Dziembowski, Tomasz Kazana, and Maciej Obremski. Non-malleable codes from two-source extractors. In *Advances in Cryptology-CRYPTO 2013*. Springer, 2013.

[DN15] Yevgeniy Dodis and Jesper Buus Nielsen, editors. *Theory of Cryptography - 12th Theory of Cryptography Conference, TCC 2015, Warsaw, Poland, March 23-25, 2015, Proceedings, Part I*, volume 9014 of *Lecture Notes in Computer Science*. Springer, 2015.

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

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

[FMNV14] S. Faust, P. Mukherjee, J. Nielsen, and D. Venturi. Continuous non-malleable codes. In *Theory of Cryptography Conference - TCC*. Springer, 2014.

[FMNV15] Sebastian Faust, Pratyay Mukherjee, Jesper Buus Nielsen, and Daniele Venturi. A tamper and leakage resilient von neumann architecture. In Jonathan Katz, editor, *Public-Key Cryptography - PKC 2015 - 18th IACR International Conference on Practice and Theory in Public-Key Cryptography, Gaithersburg, MD, USA, March 30 - April 1, 2015, Proceedings*, volume 9020 of *Lecture Notes in Computer Science*, pages 579–603. Springer, 2015.

[FMVW14] S. Faust, P. Mukherjee, D. Venturi, and D. Wichs. Efficient non-malleable codes and key-derivation for poly-size tampering circuits. In *Eurocrypt*. Springer, 2014.

[GLM+04] Rosario Gennaro, Anna Lysyanskaya, Tal Malkin, Silvio Micali, and Tal Rabin. Algorithmic tamper-proof (ATP) security: Theoretical foundations for security against hardware tampering. In Moni Naor, editor, *Theory of Cryptography, First Theory of Cryptography Conference, TCC 2004, Cambridge, MA, USA, February 19-21, 2004, Proceedings*, volume 2951 of *Lecture Notes in Computer Science*, pages 258–277. Springer, 2004.

[JW15] Zahra Jafargholi and Daniel Wichs. Tamper detection and continuous non-malleable codes. In Dodis and Nielsen [DN15], pages 451–480.

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

[LL12] Feng-Hao Liu and Anna Lysyanskaya. Tamper and leakage resilience in the split-state model. In *Advances in Cryptology–CRYPTO 2012*, pages 517–532. Springer, 2012.

[NZ96] Noam Nisan and David Zuckerman. Randomness is linear in space. *Journal of Computer and System Sciences*, 52(1):43–53, 1996.

[SW15] Guanghong Sun and Chuankun Wu. Higher order nonlinearity of niho functions. *Fundamenta Informaticae*, 137(3):403–412, 2015.

Appendix

A Proof of Lemma 7

Proof. Let $\widetilde{X}, \widetilde{S}$ be independent and uniform in $\mathbb{K} \setminus \{0\}$. Since, $q[\mathcal{X}, \mathcal{S}, \mathcal{V}, \mathcal{W}] \geq 2^{-800k}$ we have that

$$\frac{\Pr[\widetilde{X} \in \mathcal{X}]}{\Pr[\mathsf{nmExt}'(\widetilde{X}) \neq \bot]} \cdot \frac{\Pr[\widetilde{S} \in \mathcal{S}]}{\Pr[\mathsf{nmExt}'(\widetilde{S}) \neq \bot]} \geq q[\mathcal{X}, \mathcal{S}, \mathcal{V}, \mathcal{W}] \geq 2^{-800k} .$$

We have by Theorem 3 that $\Pr[\mathsf{nmExt}'(\widetilde{X}) \neq \bot] \geq \frac{1}{2^{2k}} - 2^{-1000k}$, and $\Pr[\mathsf{nmExt}'(\widetilde{S}) \neq \bot] \geq \frac{1}{2^{2k}} - 2^{-1000k}$ which implies that $|\mathcal{X}| \times |\mathcal{S}| \geq 2^{6n-806k}$. Since $806k < \delta n$, again by Theorem 3, we have that

$$\left| \Pr[\mathsf{nmExt}'(\widetilde{X}) \neq \bot,\ \mathsf{nmExt}'(\widetilde{S}) \neq \bot \mid \widetilde{X} \in \mathcal{X},\ \widetilde{S} \in \mathcal{S}] - 2^{-4k} \right| \leq 2 \cdot 2^{-1000k} , \tag{10}$$

and

$$\left| \Pr[\mathsf{nmExt}'(\widetilde{X}) \neq \bot,\ \mathsf{nmExt}'(\widetilde{S}) \neq \bot] - 2^{-4k} \right| \leq 2 \cdot 2^{-1000k} . \tag{11}$$

Let X', S' be distributed independently and uniform in $\mathcal{X}, \mathcal{S}$, respectively. By Lemma 1, $\widetilde{\mathbf{H}}_\infty(X' | \mathsf{nmExt}(X')) + \mathbf{H}_\infty(S') \geq 6n - 810k$. We obtain using Lemma 3 that

$$(\langle X', S' \rangle_{\mathbb{K}},\ \mathsf{nmExt}(X'),\ \mathsf{nmExt}(S')) \ \approx_{2^{-1000k}} \ (U_n,\ \mathsf{nmExt}(X'),\ \mathsf{nmExt}(S')) ,$$

where we assumed that $n \geq 5000k$. Since $\langle X', S' \rangle_{\mathbb{F}} = \mathrm{tr}_{\mathbb{K} \to \mathbb{F}}(\langle X', S' \rangle_{\mathbb{K}})$, where $\mathrm{tr}_{\mathbb{K} \to \mathbb{F}}$ is the field trace function, we have that

$$(\langle X', S' \rangle_{\mathbb{K}},\ \langle X', S' \rangle_{\mathbb{F}},\ \mathsf{nmExt}(X'),\ \mathsf{nmExt}(S')) \ \approx_{2^{-1000k}} \ (U_n,\ \mathrm{tr}_{\mathbb{K} \to \mathbb{F}}(U_n), \mathsf{nmExt}(X'),\ \mathsf{nmExt}(S')) .$$

This implies

$$\left| \Pr[\langle \widetilde{X}, \widetilde{S} \rangle_{\mathbb{K}} \in \mathcal{V},\ \langle \widetilde{X}, \widetilde{S} \rangle_{\mathbb{F}} \in \mathcal{W} \mid \widetilde{X} \in \mathcal{X},\ \widetilde{S} \in \mathcal{S}] - \Pr[U_n \in \mathcal{V},\ \mathrm{tr}_{\mathbb{K} \to \mathbb{F}}(U_n) \in \mathcal{W}] \right| \leq 2^{-1000k} ,$$

and hence

$$\left| p[\mathcal{X}, \mathcal{S}, \mathcal{V}, \mathcal{W}] - \Pr[\widetilde{X} \in \mathcal{X},\ \widetilde{S} \in \mathcal{S},\ U_n \in \mathcal{V},\ \mathrm{tr}_{\mathbb{K} \to \mathbb{F}}(U_n) \in \mathcal{W}] \right| \leq 2^{-1000k} .$$

Furthermore, we have by Theorem 3 that $\Pr[\mathsf{nmExt}'(X') \neq \bot] \geq 2^{-2k} - 2^{-1000k}$ and $\Pr[\mathsf{nmExt}'(X') \neq \bot] \geq 2^{-2k} - 2^{-1000k}$. Thus, conditioning the inequality 10 on the event that $\mathsf{nmExt}'(X') \neq \bot$, and $\mathsf{nmExt}'(S') \neq \bot$, and using Lemma 6, we get that

$$\Pr[\langle \widetilde{X}, \widetilde{S} \rangle_{\mathbb{K}} \in \mathcal{V},\ \langle \widetilde{X}, \widetilde{S} \rangle_{\mathbb{F}} \in \mathcal{W} \mid \widetilde{X} \in \mathcal{X},\ \widetilde{S} \in \mathcal{S},\ \mathsf{nmExt}'(\widetilde{X}) \neq \bot,\ \mathsf{nmExt}'(\widetilde{S}) \neq \bot]$$

is equal to $\Pr[U_n \in \mathcal{V},\ \mathrm{tr}_{\mathbb{K} \to \mathbb{F}}(U_n) \in \mathcal{W}] \pm 2^{-995k}$. This implies, using inequality 10 and 11 that

$$\begin{aligned} q[\mathcal{X}, \mathcal{S}, \mathcal{V}, \mathcal{W}] &= \frac{\Pr[(\widetilde{X}, \widetilde{S}, \langle \widetilde{X}, \widetilde{S} \rangle_{\mathbb{K}}, \langle \widetilde{X}, \widetilde{S} \rangle_{\mathbb{F}}) \in \mathcal{X} \times \mathcal{S} \times \mathcal{V} \times \mathcal{W},\ \mathsf{nmExt}'(\widetilde{X}) \neq \bot,\ \mathsf{nmExt}'(\widetilde{S}) \neq \bot]}{\Pr[\mathsf{nmExt}'(\widetilde{X}) \neq \bot,\ \mathsf{nmExt}'(\widetilde{S}) \neq \bot]} \\ &= \frac{\Pr[\widetilde{X} \in \mathcal{S},\ \widetilde{S} \in \mathcal{S}] \cdot (2^{-4k} \pm 2^{-1000k}) \cdot (\Pr[U_n \in \mathcal{V},\ \mathrm{tr}_{\mathbb{K} \to \mathbb{F}}(U_n) \in \mathcal{W}] \pm 2^{-995k})}{2^{-4k} \pm 2^{-1000k}} \\ &= \Pr[\widetilde{X} \in \mathcal{X},\ \widetilde{S} \in \mathcal{S},\ U_n \in \mathcal{V},\ \mathrm{tr}_{\mathbb{K} \to \mathbb{F}}(U_n) \in \mathcal{W}] \pm 2^{-990k} , \end{aligned}$$

and hence

$$|p[\mathcal{X}, \mathcal{S}, \mathcal{V}, \mathcal{W}] - q[\mathcal{X}, \mathcal{S}, \mathcal{V}, \mathcal{W}]| \leq 2^{-990k} + 2^{-1000k} \leq 2^{-989k} .$$

Using that $q[\mathcal{X}, \mathcal{S}, \mathcal{V}, \mathcal{W}] \geq 2^{-800k}$, we obtain the desired result. □

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