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

Information Theoretic Continuously Non-Malleable Codes in the Constant Split-State Model

Nico Döttling[1], Jesper Buus Nielsen[2], and Maciej Obremski[2]

[1] UC Berkeley
[2] Aarhus University

Abstract. We present an 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. Prior to our result only codes with computational security were known for this model, and it has been an open problem to construct such a code with information theoretic security. As a conceptual contribution we also introduce the notion of a one-way non-malleable code, which is the main new ingredient in our construction. In this notion, the tampering adversary's goal is to recover the encoded message rather than to distinguish the encodings of two messages. Our technical contribution is two-fold.

- We show how to construct a full fledged continuously non-malleable code from a one-way continuously non-malleable code while only increasing the number of states by a constant factor.
- We construct a one-way continuously non-malleable code in the constant split state model with information theoretic security.

1 Introduction

Non-malleable codes were introduced by Dziembowski, Pietrzak and Wichs [DPW10] as a relaxation of error correcting codes and error detecting codes. A code takes a message m and encodes it as a possibly longer and possibly randomized codeword $c \leftarrow \mathsf{Enc}(m)$. During storage or transmission the codeword might become modified into a modified codeword $c' = \mathsf{Tamper}(c)$, where Tamper is a function describing this modification. Applying the decoding algorithm yields a message $m' = \mathsf{Dec}(c')$. Various flavors of non-malleable codes provide different guarantees on the relation between m and m'. It is generally impossible to give any meaningful guarantees if the tampering function is unrestricted. Therefore, the tampering function Tamper is assumed to come from some class $\mathbb{T}$ of functions.

As an example, in the well known notion of error correcting codes the messages are vectors over a finite alphabet and it is guaranteed that $m' = m$ as long as the class $\mathbb{T}$ of tampering functions is restricted to erasing or modifying some limited number of symbols. In the relaxed notion of error detecting codes it is guaranteed that $m' \in \{m, \perp\}$ (where $\perp$ signals a decoding error) as long as the tampering is restricted to erasing or modifying some limited number of positions in the vectors.

Non-malleable codes (NMC) come with the guarantee that the decoded message $m' = \mathsf{Dec}(c')$ corresponding to the tampered codeword c' is either identical to the original message m or a message *unrelated* to m. In other words, if there is a decoding error, then the resulting message will be independent of the original message m. Technically, we require that if $m' \neq m$, then m' can be simulated using just the tampering function Tamper, but without knowing anything about the tampered codeword c'.

ISSN 1433-8092

The canonical application domain for this flavor of code is protecting functionalities implemented in hardware for crypto-enabled cards like signature cards. As an example, to securely store a secret key k on a card, first encode k into $c = \mathsf{Enc}(k)$. When in need of k the card will first compute $k = \mathsf{Dec}(c)$ and then e.g. output $\sigma = \mathsf{sig}_k(m)$. In presence of a physical tampering attack on the card, the codeword might get changed into a codeword $c' = \mathsf{Tamper}(c)$. If Tamper is a tampering function from the class $\mathbb{T}$ against which the code is resilient, it is guaranteed that either the output is the correct signature $\sigma = \mathsf{sig}_k(m)$ or $\sigma = \mathsf{sig}_{k'}(m)$ for a key k' that is unrelated to k. Since the tampering adversary could have simulated k' from just Tamper, it might as well have computed $\sigma = \mathsf{sig}_{k'}(m)$ without interacting with the card at all.

In [DPW10] the authors construct 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, Li16] provided stronger results by considering a model where the codeword is split into s parts called *states*, which can each be tampered arbitrarily but independent 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. NMCs have been constructed for $s = 2$ [ADL14] and it is clearly impossible to get a NMC for $s = 1$.

In [DPW10] it was also shown that if the class $\mathbb{T}$ of tampering functions is essentially just a little bit short of being the class of all functions, then there exists an (inefficient) NMC secure against this class of tampering. The proof used the probabilistic method and is non-constructive. Improvements and explicit constructions were later given in [FMVW14, CG14a]. Other works considered tampering via permutations and perturbations [AGM$^+$14], which are not captured in the split-state model. In this work, however, we will focus on split state tampering.

The definition in [DPW10] allows the adversary to be computationally unbounded. We call this an *information theoretic* NMC. Later works considered a notion of *computational* NMC where the adversary and tampering functions are restricted to efficient computations, see for instance [CKM11, LL12, AAnHKM$^+$16]. It is clearly desirable to try to construct NMCs without relying on unproven computational assumptions, and in this work we focus exclusively on information theoretic NMCs.

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 Tamper_i and learn $m_i = \mathsf{Dec}(\mathsf{Tamper}_i(c))$. We call this the *continuous tampering model*. This stronger security notion is needed in many setting, for instance when using NMCs to make tamper resilient computations on von Neumann architectures [FMNV15]. 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$^+$03].

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] provide a general study of when CNMCs can be built assuming a self-destruct mechanism and/or persistency. Persistency means that once the adversary tampers a codeword, the result of this tampering persists, i.e., the tampered codeword is not reset to its original state after each tampering query. In the non-persistent model on the other hand, each tamper query is performed on a fresh copy of the original codeword.

In this work, we will exclusively focus on continuous NMC in the non-persistent self-destruct model. Call such codes sdCNMC for short.

Faust et al. [FMNV14] constructed an sdCNMC in the 2-state model which is secure against computationally bounded adversaries. It was shown in the same work that it is *impossible* to construct an information theoretic sdCNMC for the 2-state model. It was left as an open problem to construct an information-theoretic sdCNMC for an s-state model for an $s > 2$. In [CMTV15] a sdCNMC was constructed in the bit-wise tampering model, which can be seen as an n-state model. However, no progress has been made in constructing information-theoretic sdCNMCs for the setting where the number of split-states s is constant.

1.1 Our Contributions

We construct an information-theoretic sdCNMCs for the 188-state model. This number can likely be significantly improved, most likely to around 34, but we settled on 188 states to keep the proofs somewhat simpler. The following theorem states our main result.

Theorem 1 (Informal). *There exists an efficient, explicit construction of non-persistent self-destruct continuous non-malleable codes which encodes messages of length n bits into $t \leq 188$ states each of size $O(n)$, with security $2^{-\Omega(n)}$.*

As a *conceptual contribution* and a technical building block we introduce the notion of *one-way* NMC (owNMC). This relaxed security notion requires that a (potentially unbounded) continuous tampering adversary should not be able to guess a *high-entropy* message m in the tampering experiment. This primitive is similar in spirit to the computational notion of *one-way functions*. In particular, one-way functions do not hide pre-images of function values entirely (in an indistinguishability sense), but only guarantee that it is hard to compute a pre-image given a random image of the function. The relation between owNMC and NMC parallels the relation between one-wayness and semantic security in computational cryptography.

We show that there is a natural construction of sdCNMCs from owCNMC that uses two encodings of the owCNMC and applies a two-source extractor to the two encoded values. The rationale of this construction is that even an unbounded adversary cannot guess the encoded values even after multiple tampering attempts, hence they must still have high min-entropy, and therefore the output of the extractor is uniformly random. The transformation works for any owCNMC and the Hadamard Extractor.

Theorem 2 (Informal). *There exists a black-box transformation that given any owCNMC in the constant split-state model produces a sdCNMC in the split-state model.*

This new conceptual approach is the main idea which allows our constructions and proofs to circumnavigate the obstacles that have hindered previous attempts to constructing an information theoretic sdCNMC. In particular, small amounts of leakage, as an adversary may obtain them in a continuous tampering experiment do not harm the security of owNMCs, whereas the standard indistinguishability notion is rather brittle with respect to leakage.

2 Technical Introduction to One-way NMC

In this section, we will provide an overview of our construction of a one-way CNMC and the main ideas for its security proof. Our construction combines two Hadamard extractors with a super-strong NMC or NM-extractor. We require the following properties from this super-strong NMC.

Properties of the Underlying Super-Strong NMC (or NM-Extractor). Let t be a constant parameter, and Enc be a t-split state super-strong NMC (or NM-Extractor). The code Enc should have following properties (discussed in more detail in Definition 10):

Leakage resilience: Should be leakage resilient against some constant rate leakage
Detection of close to bijective tampering: For any f close to bijective it holds that $\mathsf{Dec}(f(c)) = \perp$ with overwhelming probability.

In Section 7 we will discuss instantiations with Super-Strong NMC as well as NM-Extractors. In this outline we will only discuss the instantiation from super-strong NMCs.

Construction. Let $\mathbb{K} \supset \mathbb{F}$ be finite fields. Given a message M and a uniformly random value R, the encoding procedure of our owCNMC proceeds as follows.

- Encode M and R with the super-strong NMC: $\mathsf{Enc}(M) = X_1, ..., X_t$; $\mathsf{Enc}(R) = S_1, ..., S_t$, where $X_i, S_i \in \mathbb{K} \setminus \{0\}$.
- Add two checks: $V = \langle X, S \rangle_{\mathbb{K}}$ and $W = \langle X, S \rangle_{\mathbb{F}}$. Note that it holds that $W = \mathrm{tr}_{\mathbb{K} \to \mathbb{F}}(V)$, where $\mathrm{tr}_{\mathbb{K} \to \mathbb{F}}$ is the field trace.
- The codeword is given by $c = (X_1, ..., X_t, S_1, ..., S_t, V, W)$

Learning overview. The tampering experiment for our one-way code is of the *super-strong* type, i.e., every time the adversary tampers ($c \to c'$) and c' decodes to valid message, the adversary will learn the whole tampered codeword c'. Notice that given $c' = (f_1(X_1), ..., f_t(X_t), g_1(S_1)..., g_t(S_t), f_V(V), f_W(W))$, all the adversary learns is that

- $X = (X_1, ..., X_t) \in \mathcal{A}_X$
- $S = (S_1, ..., S_t) \in \mathcal{A}_S$
- $V \in \mathcal{A}_V$
- $W \in \mathcal{A}_W$,

where $\mathcal{A}_X \times \mathcal{A}_Y \times \mathcal{A}_V \times \mathcal{A}_W$ is the preimage of c' for tampering function. In each round of the tampering experiment the adversary will have some knowledge $K = (\mathcal{A}_X, \mathcal{A}_S, \mathcal{A}_V, \mathcal{A}_W)$ about c and will attempt to learn more, i.e., make the sets $\mathcal{A}_X, \mathcal{A}_S, \mathcal{A}_V, \mathcal{A}_W$ smaller. As long as these sets aren't too small, we will be able to argue that the adversary has to pay with the risk of getting detected if he wants to learn more information (make the set smaller).

Tampering and domain partition in each round. In each round we partition the domain of the functions that tamper on $X_1, ..., X_t, S_1, ..., S_t$, including previously obtained knowledge K, as follows (for details see Definition 12):

id: This part of the domain does not change under the current tampering function.
1-1: On this part the tampering function is *close* to being bijective (but not id).
med: On this part only a 'medium' amount of entropy of the original state is preserved by the tampering function.
rest: On this part only a very small amount of the entropy of the original state is preserved is preserved by the tampering function.

Every single one of the $2t$ states is split this way, and all combinations of $(\text{id}, \text{1-1}, \text{med}, \text{rest})^{2t}$ fall in one of the 5 disjoint *cube classes*:

1. Class-1 contains only the $(\text{id})^{2t}$ cube.
2. Class-2 contains all cubes for which the following is true: ($X' \neq X$ or $S' \neq S$) and (X', 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.
3. Class-3 contains all cubes which do not fall into any of above classes (in particular it means that (X', S') lost quite a bit information about the original (X, S)) and (X', S') carries still a substantial/medium amount of the information/entropy about (X, S).
4. Class-4 contains all cubes which do not fall into any of above classes but (X', S') still carries some entropy
5. Class-5 contains only the $(\text{rest})^{2t}$ cube, that is (X', S') is close to constant

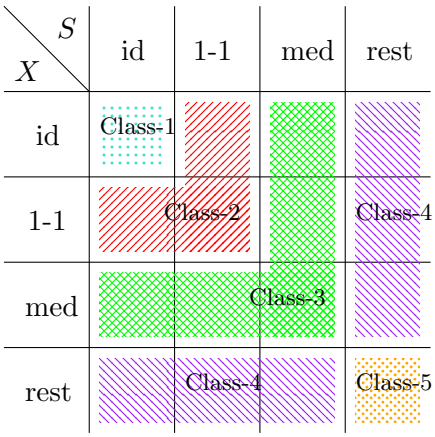

Fig. 1. Pictorial overview over the classes. Both X and S are shown as one-dimensional, but are in fact t-dimensional

Analysis of the tampering in each of the cubes classes. We show that if the codeword falls into either class $2, 3$ or 4, then the tampering will be detected with probability $1 - \varepsilon$ for a negligible ε:

– In Class−2 the underlying super-strong NMC will detect the tampering.
– In Class−3 the check $\langle X', S' \rangle_{\mathbb{F}} = W'$ will fail. The reason is that (X', S') has lost enough information about (X, S) such that $W = \langle X, S \rangle_{\mathbb{F}}$ is independent of (X', S') (via a routine leakage argument). To pass the check the adversary must correctly tamper $W \to W'$, but W' has high entropy and is independent of W.
– In Class−4 the reasoning is quite similar to Class−3, but we use the check on $\langle X', S' \rangle_{\mathbb{K}} = V'$. We argue that (X', S') has lost enough information about X, S (again via a leakage argument) such that V is independent of (X', S'). Since every part is tampered independently, all $X_i, S_i \neq 0$ and either X' or S' still has *some* remaining entropy, the value $V' = \langle X', S' \rangle_{\mathbb{K}}$ will have some remaining entropy. Again, we reach the conclusion that V' is unpredictable and independent of V and the function that tampers V has only negligible chance to guess V' correctly.

The only way the adversary can learn something and survive (not get detected) is if he falls in Class−1 or Class-5. This will let him learn which class he landed in, which will carry information. Moreover, in Class−5 there might be close-to-constant but not constant functions (which if he does not get detected potentially gives additional knowledge to the adversary). We will split the analysis in two phases. The adversary will when he picks his tampering function have some initial knowledge K. He then submits his tampering function. In Phase 1 of the analysis we only let him learn whether he fell into Class−1 or Class−5, without specifying exactly which output was obtained in case of Class−5 (i.e., in Phase 1 the whole Class−5 is treated as a one, perfectly constant function). Then his knowledge K gets updated based on this information and only in phase 2 of the analysis (which happens only if adversary felt into Class−5) will we tell the adversary the exact codeword learned in Class-5 and deal with close-to-constant functions.

Phase 1: Learning between Class−1 and Class−5. For these cases we will show that it is impossible to cover the whole domain with Class−1 and Class−5 tampering functions. Via an $\varepsilon-$independence argument we can show that either the whole domain is covered by Class−1, the whole domain is covered by Class−5, or there exist parts of the domain that fall into other classes and, as we mentioned above, the other classes lead to detection, except with negligible probability. We also refer to these zones as *death zones*.

Let us start with an observation. Assume that A is a Class−1 part of the domain. Let B be the current knowledge of adversary (i.e., the current domain, the adversary knows that the codeword c is a uniformly random point in B). If at this point the adversary learns that the codeword c is in A, the amount of information he obtains is exactly

$$\log(1/\Pr[c \in A | c \in B]) \ .$$

We show that both Class−1 and Class−5 have their *individual death-zones*, i.e., disjoint parts of the domain that fall into Classes $2, 3, 4$, which have the property that if the adversary tries to learn k bits in case of the codeword being in Class−1, the death-zone D_1 assigned to this class will fulfill the following condition:

$$\Pr[c \in \text{Class-1} \mid c \in \text{Class-1} \cup D_1] \leq 2^{-\frac{1}{2}k}$$

or in other words

$$\Pr[c \in \text{Class-1} \mid c \in \text{Class-1} \cup D_1] \leq 2^{-\frac{1}{2}\log \Pr^{-1}[c \in \text{Class-1}]}$$

where all above events are conditioned on the previous knowledge of the adversary. The analogue of the above will hold for D_5, the death-zone of Class-5.

These *individual death-zones* ensure that every time the adversary tries to learn something new (i.e., pin down c to a smaller domain) he has to risk being detected. Moreover, the detection probability is *proportional* to the amount of information the adversary is attempting to learn.

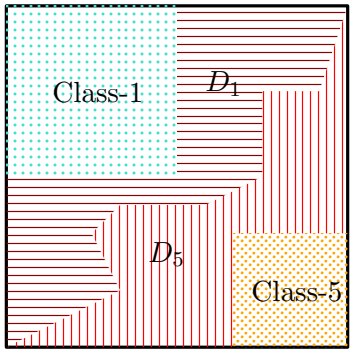

Fig. 2. Pictorial overview over death-zones for Class-1 and Class-5. The domain is already shrunk to the adversarial knowledge K.

Learning within Class-5. In this case we discuss the scenario where the adversary attempts to further partition Class-5 into parts of the domain where he applies different constant functions. We show that in this case he *loses control* over the $\langle X, S\rangle_{\mathbb{K}} = V$ check, and therefore again each truly-constant zone in which he succeeds to fulfill the check can be assigned an *individual death-zone* D_i which fulfills:

$$\Pr[c \in A_i | c \in A_i \cup D_i] \leq 2^{-\frac{1}{2t+2}\log \Pr^{-1}[c \in A_i]} \ .$$

Again, all events are conditioned on previous knowledge of the adversary. As before, this ensures that if the the adversary tries to learn k new bit of information, he will risk a probability of detection of at least $1 - 2^{-\frac{1}{2t+2}k}$.

Wrapping everything up and the K-game. To tie the analyses of the different classes together, we will look at an experiment we call the *K-game*. The K-game has the following rules:

- Setup: The game picks a codeword c uniformly at random.
- In each round the adversary chooses a list of non-intersecting sets $(B_i)_i$. If it holds $c \in B_i$, then the adversary learns the index i and the domain in the next round is set to B_i.
- For each set B_i the adversary has to choose a set D_i (again all sets D_i are non-intersecting and does not intersect with the sets B_i) such that

$$\Pr(c \in B_i \mid c \in B_i \cup D_i) < 2^{-1/(2t)k}$$

where k is the amount of information that adversary would learn from the event $c \in B_i$, i.e., $k = -\log(|B_i|/|\text{current domain}|)$.
- The adversary wins if at some point the size of the current domain is below a certain threshold.
- If at any point the event $c \in D_i$ occurs for some index i, the adversary loses and the game is over.

Remark 1. The above sketch covers the overall structure of the proof. In the full proof there are many corner cases to be covered, and we mention but two of these here. The size of the set that leads to a win depends on the underlying code. All learning lemmata discussed for Class$-2, 3, 4$ guarantee detection only if the domain in this round was not too small, in particular in our instantiations the threshold will be roughly $2^{n-C\cdot n}$, where 2^n is the size of whole domain and $C < 1$ is some constant. Moreover, if the Class$-2, 3, 4$ events themselves are too small, we cannot guarantee that detection will occur. However in this case the probability that the codewords falls into one of these cases is negligible via a standard domain partition argument.

3 Preliminaries and Technical Lemmas

If $\mathcal{Z}$ is a set then $Z \leftarrow \mathcal{Z}$ will denote a random variable sampled uniformly from $\mathcal{Z}$. We start with some standard definitions and lemmas about the statistical distance. Recall that if X and X' are random variables over the same set $\mathcal{X}$ then the *statistical distance between X and X'* is denoted by $\Delta(X; X')$, and defined as $\Delta(X; X') = \frac{1}{2}\sum_{x\in\mathcal{X}} |\Pr X = x - \Pr X' = x|$. If the variables X and X' are such that $\Delta(X; X') \leq \varepsilon$ then we say that X is ε-close to X', and write $X \approx_\varepsilon X'$. If $\mathcal{E}, \mathcal{E}'$ are some events then by $\Delta(X|\mathcal{E}\ ;\ X'|\mathcal{E}')$ we will denote the distance between variables $\widetilde{X}$ and $\widetilde{X}'$, distributed according to the conditional distributions $P_{X|\mathcal{E}}$ and $P_{X'|\mathcal{E}'}$.

If $U_\mathcal{X}$ is the uniform distribution over $\mathcal{X}$ then $d(X|\mathcal{E}) := \Delta(X|\mathcal{E}; U_\mathcal{X})$ is called *statistical distance of X from uniform given the event $\mathcal{E}$*. Moreover, if Y is independent from X then $d(X|Y) := \Delta((X, Y); (U_\mathcal{X}, Y))$ is called *statistical distance of X from uniform given the variable Y*. More generally, if $\mathcal{E}$ is an event then $d(X|Y, \mathcal{E}) := \Delta((X, Y)|\mathcal{E}; (U_\mathcal{X}, Y)|\mathcal{E})$. It is easy to see that $d(X|Y)$ is equal to the average $\sum_y \Pr(Y = y) \cdot d(X|Y = y) = \mathbb{E}_y(d(X|Y = y))$.

Definition 1 ((Average-) Min-Entropy). *Let X have finite support $\mathcal{X}$. The min-entropy $\mathbf{H}_\infty(X)$ of X is defined by*

$$\mathbf{H}_\infty(X) = -\log \max_{x\in\mathcal{X}} \Pr(X = x).$$

For an event $\mathcal{E}$, the conditional min-entropy $\mathbf{H}_\infty(X|\mathcal{E})$ of X given $\mathcal{E}$ is defined by

$$\mathbf{H}_\infty(X|\mathcal{E}) = -\log \max_{x\in\mathcal{X}} \Pr(X = x|\mathcal{E}).$$

For an event $\mathcal{E}$ and a random variable Y with finite support $\mathcal{Y}$, the average min-entropy $\widetilde{\mathbf{H}}_\infty(X|Y, \mathcal{E})$ of X given Y and $\mathcal{E}$ is defined by

$$\widetilde{\mathbf{H}}_\infty(X|Y, \mathcal{E}) = -\log \mathbb{E}_y \max_{x\in\mathcal{X}} \Pr(X = x|Y = y, \mathcal{E}).$$

Randomness extractors will be the workhorses of our non-malleable code constructions.

Definition 2 (Flexible Two-Source Extractors). *A function* $\mathsf{Ext} : \mathcal{X}_1 \times \mathcal{X}_2 \to \mathcal{Z}$ *is called a flexible* (ε, δ)*-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* $\widetilde{\mathbf{H}}_\infty(X_1|Y_1) + \widetilde{\mathbf{H}}_\infty(X_2|Y_2) \geq \log(|\mathcal{X}|) + \log(|\mathcal{Y}|) - \delta$ *that*

$$d(\mathsf{Ext}(X_1, X_2)|Y_1, Y_2) \geq \varepsilon.$$

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

Lemma 1 (Hadamard Extractor [ADL14]). *The function* $\mathsf{Ext} : \mathbb{F}_q^n \times \mathbb{F}_q^n \to \mathbb{F}_q$ *given by* $\mathsf{Ext}(x, y) = \langle x, y \rangle$ *is a flexible* (ε, δ) *extractor for* $\delta \leq (n-1)\log(q) - 2\log(1/\varepsilon)$.

Definition 3 (Non-malleable t-Source Extractors). *A function* $\mathsf{Ext} : (\mathcal{X})^t \to \mathcal{Y}$ *is called a* t*-source* (ε, δ)*-non-malleable extractor if the following property holds. For every random variable* $X = (X_1, \ldots, X_t) \in \mathcal{X}^t$ *for which* $X_1, \ldots, X_t$ *are independent and* $\mathbf{H}_\infty(X) \geq t \cdot \log|\mathcal{X}| - \delta$*, for any split-state tampering function* $f = (f_1, \ldots, f_t)$ *such that there exists* f_i *without fixed points it holds that*

$$\Delta\left((\mathsf{Ext}(X), \mathsf{Ext}(f(X))); (U, \mathsf{Ext}(f(X))\right) \leq \varepsilon,$$

where U *is distributed uniformly on* $\mathcal{Y}$.

Recently, a 9-source non-malleable extractor was constructed by Chattopadhyay and Zuckerman [CZ14].

Theorem 3 ([CZ14]). *For some* $\delta > 0$ *there exists a polynomial time construction of a* (k, ε) *non-malleable 10-source extractor* $\mathsf{nmExt} : (\mathbb{F}_q^n)^{10} \to \mathbb{F}_q^m$ *with* $k = (1-\delta)n$, $\varepsilon = 2^{-\Omega(n)}$ *and* $m = \Omega(k)$. *Moreover,* nmExt *is efficiently preimage samplable.*

We will now assemble a few basic technical lemmata that we will need for our proofs.

Lemma 2 (Bayes' rule for statistical distance [DKO13]). *Let* $(X, Y) \in \mathcal{X} \times \mathcal{Y}$ *be a random variable such that* $d(X|Y) \leq \varepsilon$. *Then for every* $x \in \mathcal{X}$ *we have*

$$\Delta(Y|X = x \ ; \ Y) \leq 2|\mathcal{X}|\varepsilon.$$

Lemma 3. *Let* X, T *be any arbitrarily correlated random variables and let* $\mathcal{E}$ *be random event then*

$$\widetilde{\mathbf{H}}_\infty(X|T, \mathcal{E}) \geq \widetilde{\mathbf{H}}_\infty(X|T) - \log\frac{1}{\Pr(\mathcal{E})}.$$

Proof.

$$\begin{aligned}
\widetilde{\mathbf{H}}_\infty(X|T, \mathcal{E}) - \log\Pr(\mathcal{E}) &= -\log \mathbb{E}_t \max_x \Pr(X = x|T = t, \mathcal{E}) - \log\Pr(\mathcal{E}) \\
&= -\log \sum_t \max_x \Pr(X = x|T = t, \mathcal{E}) \cdot \Pr(T = t|\mathcal{A}) \cdot \Pr(\mathcal{E}) \\
&= -\log \sum_t \max_x \Pr(X = x, T = t, \mathcal{E}) \\
&\geq -\log \sum_t \max_x \Pr(X = x, T = t) \\
&= \widetilde{\mathbf{H}}_\infty(X|T)
\end{aligned}$$

Lemma 4 (Entropy-preservation of inner-product for uncorrelated distributions). *Let $X, S \in \mathbb{F}^t$ be random variables such that variables $X_1, \ldots, X_t, S_1, \ldots, S_t$ are independent and all non-zero, then*

$$\mathbf{H}_\infty(\langle X; S\rangle_{\mathbb{F}}) \geq \frac{\max(\mathbf{H}_\infty(S); \mathbf{H}_\infty(X))}{t}$$

Proof. Assume w.l.o.g that $\mathbf{H}_\infty(S) \geq \mathbf{H}_\infty(X)$. As the components of S are independent, a simple averaging argument yields that there exists an index $i \in \{1, \ldots, t\}$ such that $\mathbf{H}_\infty(S_i) \geq \mathbf{H}_\infty(S)/t$. As X_i and S_i are independent and $X_i \neq 0$, it holds that $\mathbf{H}_\infty(X_i \cdot S_i) \geq \mathbf{H}_\infty(S_i) \geq \mathbf{H}_\infty(S)/t$. By independence of the components of X and S it follows that $\mathbf{H}_\infty(\langle X; S\rangle_{\mathbb{F}}) \geq \mathbf{H}_\infty(S)/t$. □

Lemma 5 (Entropy-preservation of inner-product for correlated distributions). *Let X be random variable over $\mathcal{X}^l$, let C be random variable such that for every c we have $\mathbf{H}_\infty(X|C = c) \geq l \cdot \log|\mathcal{X}| - d$, where $d < \log|\mathcal{X}|$. Then for any non-zero $v \in \mathcal{X}^l$*

$$\mathbf{H}_\infty(\langle X, v\rangle_{\mathcal{X}} \mid C = c) \geq \log|\mathcal{X}| - d$$

for every c in $\mathsf{supp}(C)$.

Proof. Let $X' = X|(C = c)$. Random variable X' has min-entropy $l \cdot \log|\mathcal{X}| - d$. Without loss of generality we can assume X' is a flat distribution. Then $|\mathsf{supp}(X')| = \frac{|\mathcal{X}|^l}{2^d}$ while $|\{x \mid \langle x, v\rangle = a\}| = \frac{|\mathcal{X}|^l}{|\mathcal{X}|}$ for every a. Thus via a quantitive argument $\mathbf{H}_\infty(\langle X', v\rangle_{\mathcal{X}}) \geq -\log\frac{|\mathcal{X}|^{l-1}}{|\mathcal{X}|^l \cdot 2^{-d}} = \log|\mathcal{X}| - d$. □

Lemma 6 (Death-zones generation lemma). *Let $\mathbb{F}$ 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:*

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

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

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

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 will define two convolutions:

$$(A_i *_\times B_i)(z) = \sum_{x,y : xy = z} A_i(x) B_i(y),$$

$$(A_i *_+ B_i)(z) = \sum_{x,y : x+y = z} A_i(x) B_i(y).$$

1. 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 $1/2 \leq \alpha \leq 1$.

2. Now, notice, again via Young's inequality for the "additive" convolution:

$$1 \geq \prod_{i=1}^{t} ||A_i^\alpha(.) *_\times B_i^\alpha(.)||_{\frac{1}{2\alpha-1}} \geq$$
$$\geq |||[A_1^\alpha(.) *_\times B_1^\alpha(.)] *_+ \ldots *_+ [A_t^\alpha(.) *_\times B_t^\alpha(.)]||_{\frac{1}{2n\alpha-(2n-1)}}$$

for $\frac{2t-1}{2t} \leq \alpha \leq 1$.

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

$$1 \geq |||[A_1^\alpha(.) *_\times B_1^\alpha(.)] *_+ \ldots *_+ [A_t^\alpha(.) *_\times B_t^\alpha(.)]||_\infty$$

□

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* $\mathsf{Tamper}_C^{\mathsf{state}}(f)$*, 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*

$\mathsf{Tamper}_C^{\mathsf{state}}(f)$:
If $\mathsf{state} = \mathtt{dead}$ *output* $\perp$
$C' \leftarrow f(C)$
If $C' = C$ *output* `same`
$M' \leftarrow \mathsf{Dec}(C')$
If $M' = \perp$ *set* $\mathsf{state} \leftarrow \mathtt{dead}$ *and output* $\perp$
Otherwise output C'

Fix a tampering adversary $\mathcal{A}$ *and a codeword* $C \in \mathcal{C}$*. We define the continuous tampering experiment* $\mathsf{CT}_{\mathcal{A},M}$ *by*

$\mathsf{CT}_C(\mathcal{A})$:
$\mathsf{state} \leftarrow \mathtt{alive}$
$v \leftarrow \mathcal{A}^{\mathsf{Tamper}_C^{\mathsf{state}}(\cdot)}$
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 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*

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

where $C_0 \leftarrow \mathsf{Enc}(M_0)$ *and* $C_1 \leftarrow \mathsf{Enc}(M_1)$*.*

Remark 2. [AKO16] 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.

Definition 7 ((Continuously-) One-Way NMC). *We say that an coding scheme* $(\mathsf{Enc}, \mathsf{Dec})$ *with* $\mathsf{Enc} : \mathcal{M} \to \mathcal{C}$ *and* $\mathsf{Dec} : \mathcal{C} \to \mathcal{M} \cup \{\perp\}$ *is* $\delta-$*One-Way-Continuous if for a random* M *uniformly distributed over* $\mathcal{M}$ *it holds that*

$$\Pr_{t \leftarrow \mathsf{CT}_{\mathcal{A},M}} [\mathbf{H}_\infty(C) - \mathbf{H}_\infty(C|\mathsf{CT}_{\mathcal{A},M} = t) \leq \delta] \geq 1 - \varepsilon.$$

where $C = \mathsf{Enc}(M)$ *is the codeword generated by the tampering experiment.*

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

Definition 8 (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* $C_i \to C_i$*.*

5 From Continuous One-Way NMC to Continuous NMC

In this section, we show how a continuously non-malleable code $(\mathsf{Enc}, \mathsf{Dec})$ can be constructed from a continuously one-way non-malleable code $(\mathsf{Enc}_0, \mathsf{Dec}_0)$. The underlying idea is very basic: Share a 0^k-padded encoding of the message M into two random shares M_1 and M_2 by inverting the Hadamard extractor. Now these shares are each encoded by Enc_0. To decode, first decode the two shares M_1 and M_2 using Dec_0 and then compute $\langle M_1, M_2 \rangle$. If this is correctly encoded, i.e., of the form $0^k||M$, output M, otherwise output $\perp$.

The intuition behind this construction is the following. By the continuous one-way property of $(\mathsf{Enc}_0, \mathsf{Dec}_0)$, a tampering adversary will not be able learn more than δ bits about each of M_1 and M_2. Moreover, independence of M_1 and M_2 is preserved during the tampering experiment.

The only critical tampering queries by the adversary are such queries where one side is preserved, but the other side is changed (say overwritten)—we call these *mixed queries*. In this case, we cannot simulate tampering queries with a one-way non-malleable code, as in a reduction to the owCNMC one of the oracles would return `same` making it impossible for us to compute the correct inner product. However, we will show that such queries lead to an immediate decoding error via the 0^k check.

Construction 1 *Let ℓ be a sufficiently large constant, let $\mathcal{M}$ be a finite message space and let $\mathbb{F}_q$ be the finite field of size q. Let $(\mathsf{Enc}_0, \mathsf{Dec}_0)$ be a t-split state scheme with message space $\mathcal{M}$. The $2t$-split state scheme $(\mathsf{Enc}, \mathsf{Dec})$ is given as follows.*

$\mathsf{Enc}(M)$:	$\mathsf{Dec}(C_1, C_2)$:
Pick $X, Y \leftarrow (\mathbb{F}_q \backslash \{0\})^\ell$ *uniformly such that* $\langle X, Y \rangle = 0^k \| M$	$X \leftarrow \mathsf{Dec}_0(C_1)$
$C_1 \leftarrow \mathsf{Enc}_0(X)$	$Y \leftarrow \mathsf{Dec}_0(C_2)$
$C_2 \leftarrow \mathsf{Enc}_0(Y)$	*Check if* $X \neq \bot, Y \neq \bot$ *and* $X, Y \in (\mathbb{F}_q \backslash \{0\})^\ell$ *If not output* $\bot$
Output (C_1, C_2)	*Parse* $0^k \| M \leftarrow \langle X, Y \rangle$ *If parsing fails output* $\bot$
	Output $M \in \mathcal{M}$

We will now show that $(\mathsf{Enc}, \mathsf{Dec})$ is a continuously non-malleable code.

Theorem 4. *Assume that $(\mathsf{Enc}_0, \mathsf{Dec}_0)$ is an (ε, δ)-secure continuously one-way non-malleable code where $\varepsilon = 2^{-\Omega(\log(q))}$. Let CT be the continuous tampering experiment for the coding scheme $(\mathsf{Enc}, \mathsf{Dec})$ given in Construction 1. Then it holds for all continuous tampering adversaries $\mathcal{A}$ and for all messages $M_0, M_0 \in \mathcal{M}$ that*

$$\Delta\left(\mathsf{CT}_{C_0}(\mathcal{A}); \mathsf{CT}_{C_1}(\mathcal{A})\right) \leq 2^{-\Omega(\log q)},$$

where $C_0 \leftarrow \mathsf{Enc}(M_0)$ and $C_1 \leftarrow \mathsf{Enc}(M_1)$. In other words, $(\mathsf{Enc}, \mathsf{Dec})$ is a $2^{-\Omega(\log q)}$-secure continuously non-malleable code.

Proof. We will prove the theorem with a hybrid argument. Let $\mathcal{A}$ be a continuous tampering adversary against the tampering experiment $\mathsf{CT}_{C_b}(\mathcal{A})$, where $b \in \{0, 1\}$, $M_0, M_1 \in \mathcal{M}$, $C_0 \leftarrow \mathsf{Enc}(M_0)$ and $C_1 \leftarrow \mathsf{Enc}(M_1)$. In the following, assume that $\mathcal{A}$ makes at most $r = \mathsf{poly}(n)$ queries to the tampering oracle.

Consider the following hybrids.

- Hybrid $\mathcal{H}_0$: This is the real experiment $\mathsf{CT}_{C_b}(\mathcal{A})$.
- Hybrid $\mathcal{H}_i$ (for $i = 1, \ldots, r$): The same as $\mathcal{H}_{i-1}$, except that if for $j \leq i$ the j-th tamper query (f_j, g_j) of $\mathcal{A}$ is such that either $\mathsf{Tamper}_{C_1}(f_j) = \mathtt{same}$ and $\mathsf{Tamper}_{C_2}(g_j) \notin \{\mathtt{same}, \bot\}$ or $\mathsf{Tamper}_{C_1}(f_j) \notin \{\mathtt{same}, \bot\}$ and $\mathsf{Tamper}_{C_2}(g_j) = \mathtt{same}$, then output $\bot$ and abort.
- Hybrid $\mathcal{H}_{r+1}$: The same as $\mathcal{H}_1$, except that X and Y are chosen uniformly at random

Clearly, in $\mathcal{H}_{r+1}$ the output of the tampering experiment is independent of the message M_b, as X and Y were chosen uniformly at random. Thus the adversary's advantage of guessing b correctly is 0 in this experiment.

We will first show that for $i = 1, \ldots, r$ the hybrids $\mathcal{H}_{i-1}$ and $\mathcal{H}_i$ are statistically close.

Define the event E_i as either $\mathsf{Tamper}_{C_1}(f_i) = \mathtt{same}$ and $\mathsf{Tamper}_{C_2}(g_i) \notin \{\mathtt{same}, \bot\}$ or $\mathsf{Tamper}_{C_1}(f_i) \notin \{\mathtt{same}, \bot\}$ and $\mathsf{Tamper}_{C_2}(g_i) = \mathtt{same}$ happens and there exists an $\hat{M}$ such that

$\langle \mathsf{Dec}(f_i(C_1)), \mathsf{Dec}(g_i(C_2))\rangle = 0^k \| \hat{M}$. In other words, E_i is the event that $f_i(C_1), g_i(C_2)$ is a valid codeword of the code $(\mathsf{Enc}, \mathsf{Dec})$ and it holds that either $f_i(C_1) = C_1$ or $g_i(C_2) = C_2$.

First observe that conditioned to $\neg E_i$, the hybrids $\mathcal{H}_{i-1}$ and $\mathcal{H}_i$ are identically distributed from the view of $\mathcal{A}$. Thus, $\Pr[E_i]$ gives us an upper bound on the statistical distance between $\mathcal{H}_{i-1}$ and $\mathcal{H}_i$.

Consider an alternative experiment $\tilde{\mathcal{H}}_{i-1}$, which is identical to $\mathcal{H}_{i-1}$, except that the experiment stops after the i-th query. Clearly, the probability that E_i happens in $\mathcal{H}_{i-1}$ is identical to the probability that E_i happens in $\tilde{\mathcal{H}}_{i-1}$. Now consider the following modification $\hat{\mathcal{H}}_{i-1}$ of $\tilde{\mathcal{H}}_{i-1}$: In this experiment both X and Y are chosen uniformly at random without the restriction that $\langle X, Y\rangle = 0^k \| M$.

Our strategy is to first show that $\hat{\mathcal{H}}_{i-1}$ of $\tilde{\mathcal{H}}_{i-1}$ are statistically close, then we will show that the event E_i has at most negligible probability in $\hat{\mathcal{H}}_{i-1}$. This readily implies that event E_i also has negligible probability in $\mathcal{H}_{i-1}$.

The view of $\mathcal{A}$ in $\tilde{\mathcal{H}}_{i-1}$ after round i consists of the information learned in prior rounds, and, if no abort happened after the i-th query, $f_i(C_1)$ and $g_i(C_2)$. If $\mathsf{Dec}(f_i(C_1)) \neq X$ and $\mathsf{Dec}(g_i(C_2)) \neq Y$, then it follows immediately from the security of the underlying one-way non-malleable code that both X and Y have high min-entropy given the view of the adversary, and therefore $\langle X, Y\rangle$ is statistically close to uniform. Thus assume now that wlog that $\mathsf{Dec}(f_i(C_1)) = X$ and $\mathsf{Dec}(g_i(C_2)) \neq Y$, i.e. (f_i, g_i) is a mixed query.

Now, observe that the leakage on X and Y that $\mathcal{A}$ got until round i is independent. To see this note that by the definition of $\mathcal{H}_{i-1}$ all mixed queries for rounds $j < i$ lead to an abort. Furthermore, since we reached round i no decoding resulted in $\perp$. Since we consider a super strong tampering game this means that in each round the adversary received $(f_j(C_1), g_j(C_2))$, which clearly is independent leakage on the two codewords. Let $K_1(X)$ be the leakage of X and $K_2(Y)$ be the leakage of Y. Since the game reached round i it means the decoding still did not abort. This in particular implies that in all previous rounds neither $f_j(C_1)$ nor $g_j(C_2)$ decoded to an error. By the security of the owCNMC $(\mathsf{Enc}_0, \mathsf{Dec}_0)$, it therefore holds that $\mathbf{H}_\infty(X | K_1(X) = k_1) \geq \ell q - \delta$ and $\mathbf{H}_\infty(Y | K_2(Y) = k_2) \geq \ell q - \delta$, except with probability 2ε.

Now observe that by the flexible extraction property of the Hadamard extractor (Lemma 1) it holds that

$$\Delta((\langle X, Y\rangle, X, g_i(C_2)) | K_1(X) = k_1, K_2(Y) = k_2), (U, X, g_i(C_2) | K_1(X) = k_1, K_2(Y) = k_2)) \leq 1/q^2,$$

where $U \in \mathbb{F}_q$ is uniformly random an independent of X and Y. Using Lemma 2 we conclude that

$$\begin{aligned}\Delta((X, g_i(C_2)) | \langle X, Y\rangle = 0^k \| M, K_1(X) = k_1, K_2(Y) = k_2, (X, g_i(C_2) | K_1(X) = k_1, K_2(Y) = k_2)) \\ \leq 2q \cdot 1/q^2 = 2/q.\end{aligned}$$

As $(X, g_i(C_2)) | \langle X, Y\rangle = 0^k \| M, K_1(X) = k_1, K_2(Y) = k_2$ is the view of $\mathcal{A}$ in $\tilde{\mathcal{H}}_{i-1}$ and $(X, g_i(C_2) | K_1(X) = k_1, K_2(Y) = k_2)$ its view in $\hat{\mathcal{H}}_{i-1}$, it follows immediately that $\Delta(\tilde{\mathcal{H}}_{i-1}, \hat{\mathcal{H}}_{i-1}) \leq 2/q + 2\varepsilon = 2^{-\Omega(\log(q))}$.

Now, in $\hat{\mathcal{H}}_{i-1}$ it holds that X and Y are independent. Thus observe that in this experiment

$$\begin{aligned}\Pr[E_i] &= \Pr[\exists M' \in \{0,1\}^{\log(q)-k} \text{ s.t. } \langle X, g_i(C_2)\rangle = 0^k \| M'] \\ &\leq \sum_{M' \in \{0,1\}^{\log(q)-k}} \Pr[\langle X, g_i(C_2)\rangle = 0^k \| M'] \\ &\leq \sum_{M' \in \{0,1\}^{\log(q)-k}} 2^{-(\log(q)-\delta)} \\ &\leq 2^{\log(q)-k} \cdot 2^{-\log(q)+\delta} \\ &= 2^{\delta-k},\end{aligned}$$

where the second inequality follows by Lemma 5. We conclude that event E_i happens with probability at most $2^{\delta-k} + 2^{-\Omega(\log(q))} = 2^{-\Omega(\log(q))}$ in $\mathcal{H}_{i-1}$. Thus, we can conclude that the statistical distance between $\mathcal{H}_{i-1}$ and $\mathcal{H}_i$ is at most $2^{-\Omega(\log(q))}$.

Finally, observe that $\mathcal{H}_{r+1}$ is identically distributed to $\hat{\mathcal{H}}_r$. As we have seen that the statistical distance between $\hat{\mathcal{H}}_r$ and $\mathcal{H}_r$ is at most $2^{-\Omega(\log(q))}$, we can conclude that the statistical distance between $\mathcal{H}_0$ and $\mathcal{H}_{r+1}$ is at most $(r+1)2^{-\Omega(\log(q))} = 2^{-\Omega(\log(q))}$ in $\mathcal{H}_{i-1}$. This concludes the proof. □

6 Constructing Continuously One-Way Non-Malleable Codes

We now present our construction of a owCNMC and its analysis.

6.1 Construction

Our code $(\mathsf{Enc}, \mathsf{Dec})$ is derived from an underlying code $(\mathcal{E}, \mathcal{D})$. We start by giving our construction generically. We specify the requirements on the components and parameters below.

Definition 9 $(\mathsf{Enc}, \mathsf{Dec})$**.** *Let $\mathbb{K}$ be a finite field and assume we have an encoding algorithm $\mathcal{E} : \mathcal{M} \to \mathbb{K}^t$ and corresponding decoding function $\mathcal{D} : \mathbb{K}^t \to \mathcal{M} \cup \{\perp\}$, for a constant $t > 0$. Let $\mathbb{F} \subset \mathbb{K}$ be a subfield.*

$\mathsf{Enc}(M)$:
- $R \leftarrow \mathbb{K}$
- $X \leftarrow \mathcal{E}(M)$
- *Reject and resample until* $X \in (\mathbb{K}\backslash\{0\})^t$
- $S \leftarrow \mathcal{E}(R)$
- *Reject and resample until:*
- $S \in (\mathbb{K}\backslash\{0\})^t$ *and* $\langle X, S\rangle_{\mathbb{K}} \neq 0$
- $V = \langle X, S\rangle_{\mathbb{K}}$
- $W = \langle X, S\rangle_{\mathbb{F}}$
- *Output* (X, S, V, W) $\in (\mathbb{K})^t \times (\mathbb{K})^t \times \mathbb{K} \times \mathbb{F}$

$\mathsf{Dec}(X, S, V, W)$:
- *Check whether:*
  - $X \in (\mathbb{K}\backslash\{0\})^t$
  - $S \in (\mathbb{K}\backslash\{0\})^t$
  - $\mathcal{D}(X) \neq \perp$,
  - $\mathcal{D}(S) \neq \perp$,
  - $\langle X, S\rangle_{\mathbb{K}} = V$,
  - $\langle X, S\rangle_{\mathbb{F}} = W$.
- *If any check fails output* $\perp$
- *Otherwise, output* $\mathcal{D}(X) \in \mathcal{M}$

Definition 10. *We call an underlying encoding scheme* $(\mathcal{E}, \mathcal{D})$ $(\delta_{\mathrm{D}}, \varepsilon_{\mathrm{D}}, \delta_{\mathrm{L}}, k, \varepsilon_{\mathrm{L}})$-admissible *if it fulfils the following requirements. Throughout this section we use* n *to denote* $\log|\mathbb{K}|$.

Canonical $\mathcal{E}$ procedure: $\mathcal{E}(m)$ *is uniform in* $\{c : \mathcal{D}(c) = m\}$.

Detection of close to bijective tampering: $\delta_{\mathrm{D}} > 0$ *and if* $X_1, \ldots, X_t \in \mathbb{K}$ *are independent random variables such that for* X *being the conditional distribution* $((X_1, \ldots, X_t)|D(X_1, \ldots, X_t) \neq \perp)$ *it holds that*

$$\mathbf{H}_\infty(X) \geq t \cdot n - \delta_{\mathrm{D}}$$

and deterministic function $f = (f_1, \ldots, f_t),\ f_i : \mathbb{K} \to \mathbb{K}$ *is such that*

$$\mathbf{H}_\infty(f(X)) \geq t \cdot n - \delta_{\mathrm{D}}$$

and $f(X) \neq X$ *then*

$$\Delta\left[(\mathcal{D}(X), \mathcal{D}(f(X)))\,; (U, \perp)\right] \leq \varepsilon_{\mathrm{D}}\ .$$

High density of valid codewords: $k < \delta$ *and*

$$\mathbf{H}_\infty(\mathcal{E}(U)) = n \cdot t - k\ .$$

Leakage resilient storage: $\delta_{\mathrm{L}} > 0$ *and* $\varepsilon_{\mathrm{L}} > 0$ *and the following holds. If* $X \in (\mathbb{K})^t$ *is such that*

$$\mathbf{H}_\infty(X) \geq t \cdot n - \delta_{\mathrm{L}}$$

and $X_1, \ldots, X_t$ *are independent random variables and* $f = (f_1, \ldots, f_t), f_i : \mathbb{K} \to \mathbb{K}$ *is such that*

$$\mathbf{H}_\infty(U|f_i(U) = u) \geq \frac{1}{3} \cdot n$$

then

$$\Delta\left[(f_1(X_1), \ldots, f_t(X_t) \mid \mathcal{D}(X) \neq \perp)\,; (f_1(X_1), \ldots, f_t(X_t))\right] \leq \varepsilon_{\mathrm{L}}\ .$$

Parameter restrictions:

$$\begin{aligned} |\mathbb{F}| &= 2^{\delta_{\mathrm{D}}/7t} \\ t &\geq 49 \\ n &\geq 2\delta_{\mathrm{D}} \\ k &\leq \frac{1}{28t}\delta_{\mathrm{D}} \\ \delta_{\mathrm{L}} &\geq \frac{1}{14t}\delta_{\mathrm{D}} \end{aligned}$$

It is instructive to think of the parameters as having the following asymptotic behaviours: $\delta_{\mathrm{L}}, k = \Theta(n)$ and $\varepsilon_{\mathrm{L}}, \varepsilon_{\mathrm{D}} = O(2^{-n})$, but this is not needed for the formal statements below.

6.2 Analysis

Theorem 5. *If* $(\mathcal{E}, \mathcal{D})$ *is* $(\delta_{\mathrm{D}}, \varepsilon_{\mathrm{D}}, \delta_{\mathrm{L}}, k, \varepsilon_{\mathrm{L}})$-admissible*, then* $(\mathsf{Enc}, \mathsf{Dec})$ *is a* (δ, ε)*-one-way continuous NMC. If the adversary is restricted to tampering* r *times, then*

$$\delta \leq \rho,$$

$$\varepsilon \leq \rho^{\tau} + O(r \cdot \psi),$$

where

$$n = \log(|\mathbb{K}|) \ ,$$

$$\psi = \gamma\rho^{-1} + \varepsilon_{\mathrm{L}} + \varepsilon_{\mathrm{D}} + 2^{-\Omega(n)} + 2^{-\Omega(\delta_{\mathrm{D}})} \ ,$$

$$\tau = \frac{1}{2t+2} \ ,$$

$$\gamma = 2^{-\frac{1}{28t}\delta_{\mathrm{D}}} \ ,$$

$$\rho = 2^{-\frac{1}{60t}\delta_{\mathrm{D}}} \ .$$

In the rest of the section we will analyze an adversary $\mathcal{A}$ attacking $(\mathsf{Enc}, \mathsf{Dec})$ in the continuous super one-way NMC game. During the attack $\mathcal{A}$ will learn information on the codeword (X, S, V, W). We define a class of benign knowledge for which the code is still secure.

Definition 11 (benign knowledge). *Consider an adversary* $\mathcal{A}$ *with information on a codeword* (X, S, V, W)*. Formally, let* $\mathcal{A}$ *be the random variable denoting the knowledge of the adversary on the codeword. We say* $\mathcal{A}$ *is benign if there exist set* $\mathcal{A}_X, \mathcal{A}_S \subseteq \mathbb{K}^t$*,* $A_V \subseteq \mathbb{K}$*, and* $A_W \subseteq \mathbb{F}$ *such that* (X, S, V, W) *conditioned on* $\mathcal{A}$ *is distributed as a random codeword sampled as* $(X, S, V, W) \leftarrow \mathsf{Enc}(x)$ *for a uniformly random* x *conditioned on* $(X, S, V, W) \in \mathcal{A}_X \times \mathcal{A}_S \times A_V \times A_W$*. Furthermore,* $\mathcal{A}_X$ *should be a cube, i.e., there exist* $\mathcal{A}_{X,1}, \ldots, \mathcal{A}_{X,t}$ *such that* $\mathcal{A}_X = \mathcal{A}_{X,1} \times \cdots \times \mathcal{A}_{X,t}$*. Similarly* $\mathcal{A}_S$ *should be a cube. We call such a knowledge benign. When* $\mathcal{A}$ *is benign we use* $K = (\mathcal{A}_X, \mathcal{A}_S, \mathcal{A}_V, \mathcal{A}_W)$ *to specify the knowledge learned. We use* $\Pr[K]$ *to denote* $\Pr[(X', S', V', W') \in K]$ *when* $(X', S', V', W') \leftarrow \mathsf{Enc}(U)$*.*

The K-game We start by defining and analysing an abstract game called the K-game.

- The game is played on some benign K.
- The game has a parameter $0 \leq \varepsilon < 1$, called the *death zone slack*,
  a parameter $0 \leq \sigma < 1$, called the *survival probability bound*,
  a parameter $0 < \tau \leq 1$ called the *death rate*,
  and a parameter $0 \leq \rho < 1$ called the *target probability*.
- We use $\mathsf{Enc}(K)$ to denote the distribution of (X, S, V, W) given by sampling $\mathsf{Enc}(U)$ conditioned on $\mathsf{Enc}(U) \in K$.

In the game the move of the player is to give a strategy σ. After that there is a move by the game which is to sample $(X, S, V, W) \leftarrow \mathsf{Enc}(K)$.

- A *strategy* σ consists of $(\{(B_i, D_i)\}_{i=1}^{\ell}, Z)$, where B_i, D_i and Z are events defined on (X, S, V, W).

– The events B_i are called *survival events*.
– The events D_i are called *death events*.
– All the events $B_1, \ldots, B_\ell, D_1, \ldots, D_\ell$ should be disjoint. Let $B = \cup_i B_i$ and $D = \cup_i D_i$. It should hold that $\Pr[S \cup D | K] = 1$.
– It should hold that[3] $\Pr[Z \mid K] \leq \sigma$.
– For each B_i let K_i be the distribution of $(X, S, V, W) \leftarrow \mathsf{Enc}(K)$ conditioned on B_i.
– It should hold that each K_i is benign.
– Finally it should hold for all B_i that

$$\Pr[B_i \mid B_i \cup D_i] \leq \Pr[B_i \mid K]^\tau + \varepsilon \ . \tag{2}$$

Let $\mathcal{A}$ be an unbounded adversary playing the K-game. We denote the outcome of the game by $G_{\mathcal{A}}(K, \varepsilon, \sigma, \tau, \rho)$. The game proceeds as follows.

1. If $\Pr[K] \leq \rho$, then $G_{\mathcal{A}}(K, \varepsilon, \sigma, \tau, \rho) = 1$.
2. Otherwise, input K to $\mathcal{A}$ and receive from $\mathcal{A}$ a strategy σ.
3. Then sample $(X, S, V, W) \leftarrow \mathsf{Enc}(K)$.
4. If Z, then $G_{\mathcal{A}}(K, \varepsilon, \sigma, \tau, \rho) = 1$.
5. Otherwise, if D, then $G_{\mathcal{A}}(K, \varepsilon, \sigma, \tau, \rho) = 0$.
6. Otherwise, there exist i such that B_i, and then $G_{\mathcal{A}}(K, \varepsilon, \sigma, \tau, \rho) = G_{\mathcal{A}}(K_i, \varepsilon, \sigma, \tau, \rho)$.
7. We say that $\mathcal{A}$ wins the game iff $G_{\mathcal{A}}(K, \varepsilon, \sigma, \tau, \rho) = 1$. Clearly $\Pr[G_{\mathcal{A}}(K, \varepsilon, \sigma, \tau, \rho) = 1] = \mathbb{E}[G_{\mathcal{A}}(K, \varepsilon, \sigma, \tau, \rho)]$.

Notice that if the adversary survives a move in the game and recursively has to play K_i, then it learned that $(X, S, V, W) \in K_i$. Specifically, it learned $\kappa_i = -\log \Pr[B_i \mid K]$ bits of knowledge. To balance this learning, we required that the adversary specified a death event D_i, which is the "price" we charge it for learning κ_i. Let $\alpha_i = -\log \Pr[B_i \mid B_i \cup D_i]$. Then the probability of being alive after learning B_i given that you are in B_i or its death event is $2^{-\alpha_i}$. The requirement on the size of the death event can then be phrased as $\alpha_i \geq \tau \kappa_i$. In other words, if you learn κ_i bits, then you survive with probability at most $2^{-\tau\kappa_i}$. Hence τ is the rate at which learning knowledge translates into death.

Lemma 7 (Knowledge). *For all $\mathcal{A}$ it holds that $\mathbb{E}[G_{\mathcal{A}}(K, \varepsilon, \sigma, \tau, \rho)] \leq (\rho / \Pr[K])^\tau + r \cdot (\varepsilon + \sigma)$, where r denotes the number of rounds the game was played.*

[3] The reason behind introduction of the event Z is that for technical reasons when we later use the K-game to analyse our code there will some corner case which happen with negligible probability that break the overall clean structure of the proof. We sweep these up by putting them all into the event Z. As it happens, it gives a more elegant analysis to not require the set Z to be disjoined from the sets B_i and D_i.

Proof. For an event E we use $G(K|E)$ to denote $\mathbb{E}[G_{\mathcal{A}}(K,\varepsilon,\sigma,\tau,\rho)|E]$. If $\Pr[K] \leq \rho$, then $G(K) = 1$ and $(\rho/\Pr[K])^\tau + \varepsilon \geq 1$. Assume then that $\Pr[K] > \rho$. Let $E_i = B_i \cup D_i$.

$$
\begin{aligned}
G(K) &= \sum_i \Pr[E_i] G(K|E_i) \\
&\overset{4}{\leq} \sum_i \Pr[E_i] \Pr[B_i|E_i] G(K_i) + \Pr[Z] \\
&\overset{5}{\leq} \sum_i \Pr[E_i] \Pr[B_i|E_i] \left((\rho/\Pr[K_i])^\tau + (r-1)(\varepsilon+\sigma)\right) + \sigma \\
&\leq \sum_i \Pr[E_i] \Pr[B_i|E_i] (\rho/\Pr[K_i])^\tau + (r-1)(\varepsilon+\sigma) + \sigma \\
&\leq \sum_i \Pr[E_i] (\Pr[B_i|E_i] - \varepsilon)(\rho/\Pr[K_i])^\tau + \varepsilon + (r-1)(\varepsilon+\sigma) + \sigma \\
&\leq \sum_i \Pr[E_i] (\Pr[B_i|K])^\tau)(\rho/\Pr[K_i])^\tau + r(\varepsilon+\sigma) \\
&\leq \sum_i \Pr[E_i] (\Pr[B_i|K])^\tau ((\rho/(\Pr[K]\Pr[S_i|K]))^\tau) + r(\varepsilon+\sigma) \\
&\leq \sum_i \Pr[E_i] (\rho/\Pr[K])^\tau + r(\varepsilon+\sigma) \\
&\leq (\rho/\Pr[K])^\tau + r(\varepsilon+\sigma) \ .
\end{aligned}
$$

□

Let $K_0 = \mathbb{K}^{2t+1} \times \mathbb{F}$ denote the situation where the adversary has no knowledge on the codeword. Then $\Pr[K_0] = 1$ and $\mathbb{E}[G_{\mathcal{A}}(K_0,\varepsilon,\sigma,\tau,\rho) \leq \rho^\tau + r \cdot (\varepsilon+\sigma)$.

We use the above lemma to analyse the success probability of an adversary $\mathcal{A}$ against our code as follows. Along the analysis we will define some negligible events. If these happen the knowledge is no longer benign, so when they happen we simply assume that $\mathcal{A}$ wins by default. These events will correspond to Z in the K-game. We then keep the invariant that if the tampering adversary did not already win the game by default or made the tampering oracle output $\perp$, then the knowledge K of the adversary is benign. We then show that any tampering request corresponds to picking a legal strategy in the K-game, and that if Z does not happen and D happens, then the tampering query makes the tampering oracle output $\perp$. Furthermore, if any B_i happens the knowledge learned by the tampering query is exactly K_i. We then use the Knowledge Lemma to conclude that at the point where the tampering oracle outputs $\perp$, the adversary still has high entropy on the codeword, which implies security of our code.

Technical Lemmas We will now prove some technical lemmas. Along the way we make some definitions which vaguely link these lemmas to the K-game. After proving the lemmas we will then put the pieces together.

[4] Follows from fact that Z doesn't have to be disjoined.
[5] Follows from inequality (2).

In the following lemmas we consider an adversary who already has knowledge K and which then does one more tampering attack. In each of the lemmas we assume that K is benign and that $\Pr[K] \geq \rho$. We assume $\mathcal{A}$ tampers X with $f = (f_1, \ldots, f_t)$, tampers S with $g = (g_1, \ldots, g_t)$, tampers V with f_V and tampers W with f_W.

Definition 12. *Let $f_i : \mathbb{K} \to \mathbb{K}$ be a tampering function. We define the following partition of $\mathbb{K}$ for U uniformly distributed over $\mathbb{K}$.*

$$\begin{aligned}
\mathbb{C}^{f_i}_{id} &= \{x \in \mathbb{K} \,|\, f_i(x) = x\},\\
\mathbb{C}^{f,i}_{[a;b]} &= \{x \in \mathbb{K} \setminus \mathbb{C}^{f}_{id} \mid \mathbf{H}_\infty(U|f(U) = f_i(x)) \in [a,b]\}\\
\mathbb{C}^{f_i}_{1-1} &= \mathbb{C}^{f_i}_{[0;\frac{6}{7t}\delta_{\mathrm{D}}]}\\
\mathbb{C}^{f_i}_{med} &= \mathbb{C}^{f_i}_{[\frac{6}{7t}\delta_{\mathrm{D}};\ \frac{1}{3}\cdot n+\frac{2}{7t}\delta_{\mathrm{D}}]}\\
\mathbb{C}^{f_i}_{rest} &= \mathbb{C}^{f_i}_{[\frac{1}{3}\cdot n+\frac{2}{7t}\delta_{\mathrm{D}};\ n]}.
\end{aligned}$$

Definition 13. *We will consider cubes of the form*

$$\prod_{i=1}^{t} A_i \times \prod_{i=1}^{t} B_i,$$

where each $A_i, B_i \subseteq \mathbb{K}$. For valid tampering functions $f, g : \mathbb{K}^t \to \mathbb{K}^t$, we define the following Cube Classes *that will partition $\mathbb{K}^{2t}$:*

1. *There is only* 1 *cube in Class-*1*:*

$$\forall_i\ A_i = C^{f_i}_{id},\ B_i = C^{g_i}_{id}.$$

2. *Class-*2 *are the cubes of the form:*

$$A_i \in \{C^{f_i}_{id}, C^{f_i}_{1-1}\} \text{ and } B_i \in \{C^{g_i}_{id}, C^{g_i}_{1-1}\},$$

   and there exists i such that $A_i \neq C^{f_i}_{id}$ or $B_i \neq C^{g_i}_{id}$.

3. *Class-*3 *cubes are of the form:*

$$A_i \in \{C^{f_i}_{id}, C^{f_i}_{1-1}, C^{f_i}_{med}, C^{f_i}_{rest}\} \text{ and } B_i \in \{C^{g_i}_{id}, C^{g_i}_{1-1}, C^{g_i}_{med}, C^{g_i}_{rest}\},$$

   and there exists i such that $A_i \in \{C^{f_i}_{med}, C^{f_i}_{rest}\}$ or $B_i \in \{C^{g_i}_{med}, C^{g_i}_{rest}\}$,
   and in each half of the vector describing this cube there is at most 12 *coordinates that are equal to $C^{\cdot i}_{rest}$.*
4. *Class-*4 *includes all cubes that weren't included above except $\prod_{i=1}^{t} C^{f_i}_{rest} \times \prod_{i=1}^{t} C^{g_i}_{rest}$*
5. *Class-*5 *includes only one cube that is*

$$\prod_{i=1}^{t} C^{f_i}_{rest} \times \prod_{i=1}^{t} C^{g_i}_{rest}$$

Let C be a cube of any class. We use the following notation:

- by $X \in C$ we mean that $X \in C_X$, where C_X is the projection of cube C on the first t coordinates.
- by $S \in C$ we mean that $S \in C_S$, where C_S is the projection of cube C on the last t coordinates.

6.3 Handling Class-2 Events

Lemma 8 (Case 2). *If C is a* Class-2 *cube and*

$$\Pr\left((X,S) \in C \mid K\right) \geq \gamma \frac{1}{\rho},$$

then the probability that $\mathcal{D}(f(X)) = \perp$ given K, C is at least $1 - O(\varepsilon_{\mathrm{D}}) - O(2^{-n})$.

Intuition: 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.

Proof. W.l.o.g. let us assume that one coordinate not equal to $\mathbb{C}^i_{id}$ is in the first half of the vector describing the cube C. Let X' be the conditional distribution $X|X \in (C \cap \mathcal{A}_X)$. From the whole random event K via inner product properties only $X \in \mathcal{A}_X$ has non-negligible "influence" on X. Thus we will ignore the remaining events for now (we include an extra epsilon later on). First notice that

$$\Pr\left((X,S) \in \mathbb{C}^f_{1-1} \times (\mathbb{C}^g_{id} \cup \mathbb{C}^g_{1-1}) \mid K\right) \geq \gamma \frac{1}{\rho} \Rightarrow \Pr\left(X \in \mathbb{C}^f_{1-1} \cap \mathcal{A}_X\right) \geq \gamma.$$

Via the property *high density of codewords* in Definition 10 we know that

$$\mathbf{H}_\infty(X) \geq t \cdot n - k$$

thus

$$\mathbf{H}_\infty(X') \geq t \cdot n - \log \frac{1}{\gamma} - k \geq t \cdot n - \delta_{\mathrm{D}}.$$

We know that $X' \in C$ and that C is a *Class*-2 cube, so

$$\mathbf{H}_\infty(f(X')) \geq \left(t \cdot n - \log \frac{1}{\gamma} - k\right) - t \cdot (\frac{6}{7t}\delta_{\mathrm{D}}) \geq t \cdot n - \delta_{\mathrm{D}}.$$

Using the property *detection of almost bijective tampering* in Definition 10 we obtain:

$$\Delta\left[\left(\mathcal{D}(X'), \mathcal{D}(f(X'))\right); \left(\mathcal{D}(X'), \perp'\right)\right] \leq \varepsilon_{\mathrm{D}}.$$

Thus, the probability that $\mathcal{D}(f(X')) \neq \perp$ is less or equal ε_{D}. On top of $X \in \mathcal{A}_X$, the adversary also knows $S \in \mathcal{A}_S, \langle X,S\rangle_{\mathbb{K}} \in A_V, \langle X,S\rangle_{\mathbb{F}} \in A_W$, where $\langle X,S\rangle_{\mathbb{F}} \in A_W$ is redundant since $\langle X,S\rangle_{\mathbb{F}} = \mathrm{tr}(\langle X,S\rangle_{\mathbb{K}})$, where tr is a trace function. Since $\Pr(K) \geq \rho \gg 2^{-n}$, using the strong extraction properties of the Hadamard extractor we obtain:

$$\Delta\left([X|K];\ [X|X \in \mathcal{A}_X]\right) \ll O(2^{-n})\ .$$

From this we obtain the bound $O(\varepsilon_{\mathrm{D}}) + O(2^{-n})$. □

Definition 14 (Class-2 Events). *For each Class-2 cube we define a win event Z_2. If $|C \cap K| \leq \gamma/\rho$, then $Z_2 = C \cap K$. Otherwise Z_2 is the set of $(X, S, V, W) \in K \cap C$ for which $\mathcal{D}(f(X)) \neq \perp$ and $\mathcal{D}(g(X)) \neq \perp$. In the first case*

$$\Pr[Z_2|K] \leq \gamma \frac{1}{\rho} \ .$$

In the second case

$$\Pr[Z_2|K, C] \leq O(\varepsilon_{\text{D}}) + O(2^{-n}) \ .$$

6.4 Handling Class-3 Events

Lemma 9 (Case 3). *If C is a* Class-3 *cube and*

$$\Pr\left((X, S) \in C \mid K\right) \geq \gamma \frac{1}{\rho},$$

then

$$\Pr(f_W(\langle X; Y\rangle_{\mathbb{F}}) = \langle f(X); g(Y)\rangle_{\mathbb{F}} \mid K, (X, S) \in C) \leq 2^{-\Omega(\delta_{\text{D}})} \ .$$

Intuition: The adversary will not be able to guess $\langle f(X); g(Y)\rangle_{\mathbb{F}}$ even given $\langle X; Y\rangle_{\mathbb{F}}$. He lost too much entropy and $\langle X; Y\rangle_{\mathbb{F}}, \langle f(X); g(Y)\rangle_{\mathbb{F}}$ are now independent, and vectors $f(X), g(S)$ have enough entropy to keep $\langle f(X); g(Y)\rangle_{\mathbb{F}}$ uniform.

Proof. W.l.o.g. let us assume that the coordinate that is equal to $\mathbb{C}^{\cdot i}_{med}$ or $\mathbb{C}^{\cdot i}_{rest}$ is in the first half of the vector describing the cube C. Let X' and S' be the conditional distributions $X|X \in (C \cap \mathcal{A}_X)$ and $S|S \in (C \cap \mathcal{A}_S)$. From the assumptions we know that

$$\begin{aligned}
&\widetilde{\mathbf{H}}_\infty(X'|f(X')) \geq \frac{6}{7t}\delta_{\text{D}} - \log\frac{1}{\gamma} - k \\
&\mathbf{H}_\infty(S') \geq t \cdot n - \log(\frac{1}{\gamma}) - k \\
&\mathbf{H}_\infty(f(X')) \geq (t-12)(\frac{2}{3} \cdot n - \frac{2}{7t}\delta_{\text{D}}) - \log\frac{1}{\gamma} - k \\
&\mathbf{H}_\infty(g(S')) \geq (t-12)(\frac{2}{3} \cdot n - \frac{2}{7t}\delta_{\text{D}}) - \log\frac{1}{\gamma} - k \geq (t-12)\frac{2}{3} \cdot n - \frac{3}{7}\delta_{\text{D}}.
\end{aligned}$$

Via the strong extraction property of the Hadamard-extractor (Lemma 1) and Bayes' rule for the statistical distance (Lemma 2) we know that

$$\begin{aligned}
d(\langle X', S'\rangle_{\mathbb{F}}|f(X'), S') &\leq 2^{-\frac{\widetilde{\mathbf{H}}_\infty(X'|f(X') + \mathbf{H}_\infty(S') - (t\cdot n) - \log|\mathbb{F}|}{2}} = \\
&= 2^{-\frac{(\frac{6}{7t}\delta_{\text{D}} - \log\frac{1}{\gamma} - k) + (t\cdot n - \log\frac{1}{\gamma} - k) - (t\cdot n) - (\frac{1}{7t}\delta_{\text{D}})}{2}} \leq 2^{-\frac{2}{7t}\delta_{\text{D}}} \ .
\end{aligned}$$

Thus it holds for any m that

$$\begin{aligned}
&\Delta((f(X'), S')|\langle X', S'\rangle_{\mathbb{F}} = m;\ (f(X'), S')) \leq 2 \cdot 2^{\frac{1}{7t}\delta_{\text{D}}} \cdot 2^{-\frac{2}{7t}\delta_{\text{D}}} = 2 \cdot 2^{-\frac{1}{7t}\delta_{\text{D}}}, \\
&\Delta\left(\langle f(X'), g(S')\rangle_{\mathbb{F}}|\langle X', S'\rangle_{\mathbb{F}} = m;\ \langle f(X'), g(S')\rangle_{\mathbb{F}}\right) \leq 2 \cdot 2^{-\frac{1}{7t}\delta_{\text{D}}} \ .
\end{aligned}$$

We further know that

$$\begin{aligned} d(\langle f(X'), g(S')\rangle_{\mathbb{F}}) &\leq 2^{-\frac{2\cdot\left((t-12)\frac{2}{3}\cdot n-\frac{3}{7}\delta_{\mathrm{D}}\right)-(t\cdot n)-(\frac{1}{7}\delta_{\mathrm{D}})}{2}} \\ &= 2^{-\frac{\frac{1}{3}t\cdot n-16\cdot n-\frac{6}{7}\delta_{\mathrm{D}}-\frac{1}{7t}\delta_{\mathrm{D}}}{2}} \\ &\leq 2^{-\frac{1}{2}n}. \end{aligned}$$

Thus we can conclude that

$$d(\langle f(X'), g(S')\rangle_{\mathbb{F}} \mid \langle X', S'\rangle_{\mathbb{F}} = m) \leq 2 \cdot 2^{-\frac{1}{7t}\delta_{\mathrm{D}}} + 2^{-\frac{1}{2}n} \leq 4 \cdot 2^{-\frac{1}{7t}\delta_{\mathrm{D}}}.$$

From this we get that

$$\forall_{m,\tilde{m}}\ \Pr(\langle f(X'), g(S')\rangle_{\mathbb{F}} = \tilde{m} \mid \langle X', S'\rangle_{\mathbb{F}} = m) \leq \frac{1}{|\mathbb{F}|} + 4 \cdot 2^{-\frac{1}{7t}\delta_{\mathrm{D}}}\ .$$

Now notice that for all $\tilde{m}$ and all $m \in \mathrm{tr}(A_V)$, where tr is a trace function:

$$\begin{aligned} &\frac{1}{|\mathbb{F}|} + 4 \cdot 2^{-\frac{1}{7t}\delta_{\mathrm{D}}} \geq \Pr(\langle f(X'), g(S')\rangle_{\mathbb{F}} = \tilde{m} \mid \langle X', S'\rangle_{\mathbb{F}} = m) = \\ &= \Pr(\langle f(X'), g(S')\rangle_{\mathbb{F}} = \tilde{m} \mid \langle X', S'\rangle_{\mathbb{F}} = m, \langle X', S'\rangle_{\mathbb{K}} \in \mathcal{A}_V) \cdot \Pr(\langle X', S'\rangle_{\mathbb{K}} \in \mathcal{A}_V \mid \langle X', S'\rangle_{\mathbb{F}} = m) + \\ &+ \Pr(\langle f(X'), g(S')\rangle_{\mathbb{F}} = \tilde{m} \mid \langle X', S'\rangle_{\mathbb{F}} = m, \langle X', S'\rangle_{\mathbb{K}} \notin \mathcal{A}_V) \cdot \Pr(\langle X', S'\rangle_{\mathbb{K}} \notin \mathcal{A}_V \mid \langle X', S'\rangle_{\mathbb{F}} = m) \geq \\ &\geq \Pr(\langle f(X'), g(S')\rangle_{\mathbb{F}} = \tilde{m} \mid \langle X', S'\rangle_{\mathbb{F}} = m, \langle X', S'\rangle_{\mathbb{K}} \in \mathcal{A}_V) \cdot \Pr(\langle X', S'\rangle_{\mathbb{K}} \in \mathcal{A}_V \mid \langle X', S'\rangle_{\mathbb{F}} = m) \\ &= \Pr(\langle f(X), g(S)\rangle_{\mathbb{F}} = \tilde{m} \mid K, (X, S) \in C, \langle X', S'\rangle_{\mathbb{F}} = m) \cdot \Pr(\langle X', S'\rangle_{\mathbb{K}} \in \mathcal{A}_V \mid \langle X', S'\rangle_{\mathbb{F}} = m). \end{aligned} \tag{3}$$

Now we will show that for $m \in \mathrm{tr}(\mathcal{A}_V)$:

$$\Pr_m\left(\Pr(\langle X', S'\rangle_{\mathbb{K}} \in \mathcal{A}_V \mid \langle X', S'\rangle_{\mathbb{F}} = m) \geq \rho^2\right) \geq 1 - \rho \geq 1 - 2^{-\Omega(\delta_{\mathrm{D}})}, \tag{4}$$

where m is sampled according to distribution $\langle X', S'\rangle_{\mathbb{F}} | \langle X', S'\rangle \in A_V$. We sample m this way since the adversary a priori knows that X, S are consistent with knowledge K and that they fall into cube C, then he produces function f_W which only then "sees" element m and attempts to tamper it.

The proof is by contradiction. Let us denote

$$\mathsf{bad} = \left\{a \in \mathbb{F} \mid \Pr(\langle X', S'\rangle_{\mathbb{K}} \in \mathcal{A}_V \mid \langle X', S'\rangle_{\mathbb{F}} = a) < \rho^2\right\}$$

From assumptions on knowledge K we know that $\Pr(\langle X', S'\rangle_{\mathbb{K}} \in \mathcal{A}_V) \geq \rho$. For all $a \in \mathsf{bad}$ we have:

$$\Pr(\langle X', S'\rangle_{\mathbb{K}} \in \mathcal{A}_V \mid \langle X', S'\rangle_{\mathbb{F}} = a) < \rho^2$$

$$\frac{\Pr(\langle X', S'\rangle_{\mathbb{F}} = a \mid \langle X', S'\rangle_{\mathbb{K}} \in \mathcal{A}_V) \cdot \Pr(\langle X', S'\rangle_{\mathbb{K}} \in \mathcal{A}_V)}{\Pr(\langle X', S'\rangle_{\mathbb{F}} = a)} < \rho^2$$

$$\Pr(\langle X', S'\rangle_{\mathbb{F}} = a \mid \langle X', S'\rangle_{\mathbb{K}} \in \mathcal{A}_V) < \frac{\Pr(\langle X', S'\rangle_{\mathbb{F}} = a)}{\Pr(\langle X', S'\rangle_{\mathbb{K}} \in \mathcal{A}_V)} \cdot \rho^2 \leq \Pr(\langle X', S'\rangle_{\mathbb{F}} = a) \cdot \rho$$

$$\sum_{a \in \mathsf{bad}} \Pr(\langle X', S'\rangle_{\mathbb{F}} = a \mid \langle X', S'\rangle_{\mathbb{K}} \in \mathcal{A}_V) \leq \sum_{a \in \mathsf{bad}} \Pr(\langle X', S'\rangle_{\mathbb{F}} = a) \cdot \rho \leq \rho.$$

Given that m is sampled accordingly to distribution $\langle X', S'\rangle_{\mathbb{F}} | \langle X', S'\rangle \in A_V$ this gives us (4). Now with (3) and (4) we obtain:

$$\Pr(\langle f(X), g(S)\rangle_{\mathbb{F}} = \tilde{m} \mid K, (X, S) \in C, \langle X', S'\rangle_{\mathbb{F}} = m) \leq \frac{1}{\rho^2}\left(\frac{1}{|\mathbb{F}|} + 4 \cdot 2^{-\frac{1}{7t}\delta_{\mathrm{D}}}\right) \leq 2^{-\Omega(\delta_{\mathrm{D}})},$$

with probability at least $1 - 2^{-\Omega(\delta_{\mathrm{D}})}$ over the choice of m. Which means that the value of $\langle f(X'), g(S')\rangle_{\mathbb{F}}$ is unpredictable from the view of the function f_W. □

Definition 15 (Class-3 Events). *For each Class-3 cube we define a win event Z_3. If $|C \cap K| \leq \gamma/\rho$, then $Z_3 = C \cap K$. Otherwise Z_3 is the set of $(X, S, V, W) \in K \cap C$ for which $f_W(\langle X; S\rangle_{\mathbb{F}}) = \langle f(X); g(S)\rangle_{\mathbb{F}}$. In the first case*

$$\Pr[Z_3|K] \leq \gamma\frac{1}{\rho}\ .$$

In the second case

$$\Pr[Z_3|K, C] \leq 2^{-\Omega(\delta_{\mathrm{D}})}\ .$$

6.5 Handling Class-4 Events

Lemma 10 (Case 4). *Let C be* Class-4 *cube and*

$$\Pr\left((X, S) \in C) \mid K\right) \geq \gamma\frac{1}{\rho},$$

then

$$\Pr(f_V(\langle X; S\rangle_{\mathbb{K}}) = \langle f(X); g(S)\rangle_{\mathbb{K}} \mid K, (X, S) \in C) \leq 2^{-\Omega(n)}\ .$$

Intuition: The adversary will not be able to guess $\langle f(X); g(Y)\rangle_{\mathbb{K}}$ even given $\langle X; Y\rangle_{\mathbb{K}}$. He lost too much entropy and $\langle X; Y\rangle_{\mathbb{K}}, \langle f(X); g(Y)\rangle_{\mathbb{K}}$ are now independent. Vectors $f(X), g(S)$ have enough entropy to keep $\langle f(X); g(Y)\rangle_{\mathbb{F}}$ unpredictable (not uniform, but with substantial min-entropy).

Proof. W.l.o.g. let us assume that in the first half of the vector describing C there is more than 12 coordinates equal to $\mathbb{C}^{\cdot i}_{rest}$. Let X' be a conditional distribution $X|X \in (C \cap \mathcal{A}_X)$ and let S' be the conditional distribution $S|S \in (C \cap \mathcal{A}_S)$. From the assumptions we know that

$$\begin{aligned}
&\mathbf{H}_\infty(X') \geq t \cdot n - \log \frac{1}{\gamma} - k \\
&\widetilde{\mathbf{H}}_\infty(X'|f(X')) \geq 12 \cdot (\frac{1}{3}n + \frac{2}{7t}\delta_{\mathrm{D}}) - \log \frac{1}{\gamma} - k, \\
&\mathbf{H}_\infty(S') \geq t \cdot n - \log(\frac{1}{\gamma}) - k.
\end{aligned}$$

Via strong extraction property of the Hadamard-extractor (Lemma 1) and the Bayes' rule for the statistical distance (Lemma 2) we know that

$$\begin{aligned}
d(\langle X', S'\rangle_{\mathbb{K}}|f(X'), S') &\leq 2^{-\frac{\widetilde{\mathbf{H}}_\infty(X'|f(X')+\mathbf{H}_\infty(S')-(t\cdot n)-n}{2}} \\
&= 2^{-\frac{(12\cdot(\frac{1}{3}n+\frac{2}{7t}\delta_{\mathrm{D}})-\log\frac{1}{\gamma}-k)+(t\cdot n-\log(\frac{1}{\gamma})-k)-(t\cdot n)-(n)}{2}} \\
&\leq 2^{-\left(\frac{3}{2}n\right)}.
\end{aligned}$$

Thus it holds for any for any $m \in \mathbb{K}$ that

$$\begin{aligned}
&\Delta((f(X'), S')|\langle X', S'\rangle_{\mathbb{K}} = m;\ (f(X'), S')) \leq 2 \cdot 2^n \cdot 2^{-\left(\frac{3}{2}n\right)} = 2 \cdot 2^{-\frac{1}{2}n}, \\
&\Delta\left(\langle f(X'), g(S')\rangle_{\mathbb{K}}|\langle X', S'\rangle_{\mathbb{K}} = m;\ \langle f(X'), g(S')\rangle_{\mathbb{K}}\right) \leq 2 \cdot 2^{-\frac{1}{2}n} = 2^{-\Omega(n)}. \qquad (5)
\end{aligned}$$

Notice that now the whole K is included in the conditioning above, $X \in \mathcal{A}_X, S \in A_S$ got included in the definition of X', S' and the $\langle X, S\rangle_{\mathbb{K}} \in \mathcal{A}_V$ is covered the in conditioning above, the last part of K is $\langle X, S\rangle_{\mathbb{F}} \in \mathcal{A}_W$ but that follows easily from the fact that if $\mathrm{tr}_{\mathbb{K}\to\mathbb{F}}$ denotes trace function from extension field $\mathbb{K}$ into $\mathbb{F}$ then $\langle X, S\rangle_{\mathbb{F}} = \mathrm{tr}_{\mathbb{K}\to\mathbb{F}}(\langle X, S\rangle_{\mathbb{K}})$. This makes the conditioning on inner product over the smaller field obsolete.

Since the cube C is a *Class*-4 cube we know there exists at least one coordinate which is $\mathbb{C}^{\cdot i}_{med}$ or $\mathbb{C}^{\cdot i}_{1-1}$ or $\mathbb{C}^{\cdot i}_{id}$. W.l.o.g. let us assume that coordinate is in the first half of the cube vector. Let $\tilde{X}$ be uniformly distributed over $(C_X \cap \mathcal{A}_X)$ where C_X is the projection of the cube vector to the first half of the coordinates. Also since $\Pr(X \in (C \cap \mathcal{A}_S)) \geq \gamma$ and $\mathbf{H}_\infty(X) \geq t \cdot n - k$ and $\mathcal{E}$ is the canonical procedure we know that for uniform random U it holds that $P(\mathcal{D}(U) \neq \perp) \geq 2^{-k}$ and thus $\Pr(U \in (C_X \cap \mathcal{A}_X)) \geq \gamma \cdot 2^{-k}$. By that we obtain the following:

$$\begin{aligned}
&\mathbf{H}_\infty(\tilde{X}) \geq t \cdot n - \log(\frac{1}{\gamma}) - k \\
&\mathbf{H}_\infty(f(\tilde{X})) \geq \frac{1}{3} \cdot n + \frac{2}{7t}\delta_{\mathrm{D}} - \log \frac{1}{\gamma} - k \geq \frac{1}{3} \cdot n\ . \qquad (6)
\end{aligned}$$

Since we know that $f_i(\tilde{X}_i)$ are all independent random variables we get via the entropy preservation property of the inner product (Lemma 4) that

$$\mathbf{H}_\infty(\langle f(\tilde{X}), g(S')\rangle_{\mathbb{K}}) \geq \frac{\frac{1}{3} \cdot n}{t}$$

Thus we get

$$\max_z \Pr(\langle f(\tilde{X}), g(S')\rangle_{\mathbb{K}} = z) \leq 2^{-\frac{\frac{1}{3}\cdot n}{t}}.$$

Since

$$\Pr(\mathcal{D}(U) \neq \perp \mid U \in (C_X \cap \mathcal{A}_X)) = \Pr(U \in (C_X \cap \mathcal{A}_X) \mid \mathcal{D}(U) \neq \perp) \cdot \frac{\Pr(\mathcal{D}(U) \neq \perp)}{\Pr(U \in (C_X \cap \mathcal{A}_X))} \geq \gamma \cdot 2^{-k} .$$

Hence

$$\max_z \Pr(\langle f(X'), g(S')\rangle_{\mathbb{K}} = z) = \max_z \Pr(\langle f(\tilde{X}), g(S')\rangle_{\mathbb{K}} = z \mid \mathcal{D}(\tilde{X}) \neq \perp) \leq 2^{-(\frac{n}{3t} - \log\frac{1}{\gamma} - k)} \leq 2^{-\frac{n}{4t}}$$

Via the above and (5) we get that for any $m \in \mathbb{K}$ the following holds:

$$\max_z \Pr(\langle f(X'), g(S')\rangle_{\mathbb{K}} = z | \langle X', S'\rangle_{\mathbb{K}} = m, K) \leq 2^{-\frac{n}{4t}} + 2 \cdot 2^{-\frac{1}{2}n} \leq 2^{-\Omega(n)},$$

which means that $\langle f(X'), g(S')\rangle_{\mathbb{K}}$ is unpredictable from the view of f_V even given K. □

Definition 16 (Class-4 Events). *For each Class-4 cube we define a win event Z_4. If $|C \cap K| \leq \gamma/\rho$, then $Z_4 = C \cap K$. Otherwise Z_4 is the set of $(X, S, V, W) \in K \cap C$ for which $f_V(\langle X; S\rangle_{\mathbb{K}}) = \langle f(X); g(S)\rangle_{\mathbb{K}}$. In the first case*

$$\Pr[Z_4|K] \leq \gamma\frac{1}{\rho} .$$

In the second case

$$\Pr[Z_4|K, C] \leq 2^{-\Omega(\delta_{\mathrm{D}})} .$$

6.6 Handling Class-1 and Class-5 Events

Lemma 11 (1-or-5 strategy). *Let C_1 be the Class-1 cube and define a survival event $B_1 = C_1 \cap K$. Let C_5 be the Class-5 cube and define a survival event $B_5 = C_5 \cap K$. The corresponding K_1 and K_5 are benign. There exist D_1, D_5 and event Z' such that $(\{(B_1, D_1), (B_5, D_5)\}, Z_2 \vee Z_3 \vee Z_4 \vee Z')$ is a legal strategy in $G(K, \varepsilon, \tau = \frac{1}{2t+2}, \sigma, \rho)$ for $\varepsilon = 2^{-n}$ and $\sigma = O(\frac{1}{\rho}) + O(\varepsilon_{\mathrm{L}}) + O(\varepsilon_{\mathrm{D}}) + 2^{-\Omega(n)} + 2^{-\Omega(\delta_{\mathrm{D}})}$. Furthermore, if D_1 or D_5 occurs, then the tampering oracle outputs $\perp$.*

The lemma follows directly from the following lemma.

Definition 17. *Let $I : \mathbb{K}^t \to \mathcal{Z}_p$ be defined as follows*

$$I(X) = \begin{cases} -1, & \text{if } X \in \mathbb{C}_{rest}^{f,1} \times \ldots \times \mathbb{C}_{rest}^{f,t} \\ 1, & \text{if } X \in \mathbb{C}_{id}^{f,1} \times \ldots \times \mathbb{C}_{id}^{f,t} \\ 2, & \text{if otherwise} \end{cases} \tag{7}$$

We define $I(S)$ in the exactly same way.

Lemma 12. *If $X, S \in \mathbb{K}^t$ are valid and distributed uniformly such that $X \in \mathcal{A}_X, S \in \mathcal{A}_S, \langle X, S\rangle_{\mathbb{K}} \in \mathcal{A}_{\mathbb{K}}$ then there exist sets D_{id} and D_{rest} such that*

1. $\Pr[(I(X), I(S)) = (1,1) \mid (X,S) \in I^{-1}(1) \times I^{-1}(1) \cup D_{id}] \leq 2^{-\frac{1}{2}\log \Pr^{-1}[(I(X),I(S))=(1,1)]} + 2^{-n}$
2. $\Pr[(I(X), I(S)) = (-1,-1) \mid (X,S) \in I^{-1}(1) \times I^{-1}(1) \cup D_{rest}] \leq 2^{-\frac{1}{2}\log \Pr^{-1}[(I(X),I(S))=(-1,-1)]} + 2^{-n}$
3. $D_{id} \cap D_{rest} = \emptyset$, *and* $D_{id} \cap \left((I^{-1}(1) \times I^{-1}(1) \cap (I^{-1}(-1) \times I^{-1}(-1)\right) = \emptyset$, *and* $D_{rest} \cap \left((I^{-1}(1) \times I^{-1}(1) \cap (I^{-1}(-1) \times I^{-1}(-1)\right) = \emptyset$.

Intuition: From the above equations we will calculate the required size of sets D_{id} and D_{rest}, then we will show that there are at least $|D_{id}| + |D_{rest}|$ points of the domain that do not fall into either the identity-cube or rest-cube. That will conclude the existence proof for sets D_{id} (or D_1) and D_{rest} (or D_5).

Proof. Let X' be uniformly distributed over $\mathcal{A}_X$, such that $\mathcal{D}(X) \neq \perp$ and let S' be uniformly distributed on $\mathcal{A}_S$, such that $\mathcal{D}(S) \neq \perp$. First we will show that there exist sets $D_{id}, D_{rest} \subseteq X^{2t}$ such that

1. $\Pr[(I(X'), I(S')) = (1,1) \mid (X',S') \in I^{-1}(1) \times I^{-1}(1) \cup D_{id}] \leq 2^{-\frac{1}{2}\log \Pr^{-1}[(I(X'),I(S'))=(1,1)]}$
2. $\Pr[(I(X'), I(S')) = (-1,-1) \mid (X',S') \in I^{-1}(1) \times I^{-1}(1) \cup D_{rest}] \leq 2^{-\frac{1}{2}\log \Pr^{-1}[(I(X'),I(S'))=(-1,-1)]}$
3. $D_{id} \cap D_{rest} = \emptyset$, and $D_{id} \cap \left((I^{-1}(1) \times I^{-1}(1) \cap (I^{-1}(-1) \times I^{-1}(-1)\right) = \emptyset$, and $D_{rest} \cap \left((I^{-1}(1) \times I^{-1}(1) \cap (I^{-1}(-1) \times I^{-1}(-1)\right) = \emptyset$.

From the first two conditions we can calculate the required size of sets D_{id}, D_{rest}:

$$\frac{\Pr[(I(X'), I(S')) = (1,1)]}{\Pr[(I(X'), I(S')) = (1,1)] + \Pr[(X',S') \in D_{id}]} \leq \Pr[(I(X'), I(S')) = (1,1)]^{1/2}$$

$$\Pr[(I(X'), I(S')) = (1,1)]^{1/2} - \Pr[(I(X'), I(S')) = (1,1)] \leq \Pr[(X',S') \in D_{id}]$$

From Lemma 6 we obtain:

$$\sum_{\substack{a,b \in \mathcal{Z}_p \\ a \cdot b = 1}} \Pr[(I(X'), I(S')) = a, b]^{\frac{1}{2}} \leq 1$$

$$\sum_{\substack{a,b \in \mathcal{Z}_p \\ a \cdot b = 1}} \left(\Pr[(I(X'), I(S')) = a, b]^{\frac{1}{2}} - \Pr[(I(X'), I(S')) = a, b]\right) \leq 1 - \sum_{\substack{a,b: \\ a \cdot b \neq 1}} \Pr[(I(X'), I(S')) = a, b]$$

$$\Pr[(I(X'), I(S')) \in D_{id}] + \Pr[(I(X'), I(S')) \in D_{rest}] \leq 1 - \sum_{\substack{a,b: \\ a \cdot b \neq 1}} \Pr[(I(X'), I(S')) = a, b] \ ,$$

which concludes existential proof for such sets. We will show that these sets fulfil the conditions listed in the lemma statement. We know that

$$\mathbf{H}_\infty(X') \geq t \cdot n - \log \frac{1}{\rho} - k,$$
$$\mathbf{H}_\infty(S') \geq t \cdot n - \log \frac{1}{\rho} - k,$$
$$\widetilde{\mathbf{H}}_\infty(X' | I(X')) \geq t \cdot n - \log \frac{1}{\rho} - k - 2 \ .$$

Via the strong extraction property of the Hadamard-extractor (Lemma 1) and Bayes' rule for the statistical distance (Lemma 2) we know that

$$\begin{aligned} d(\langle X', S'\rangle_{\mathbb{K}} | I(X'), S') &\leq 2^{-\frac{\widetilde{\mathbf{H}}_\infty(X'|I(X')+\mathbf{H}_\infty(S')-(t\cdot n)-n}{2}} \\ &= 2^{-\frac{(t\cdot n-\log\frac{1}{\rho}-k-2)+(t\cdot n-\log\frac{1}{\rho}-k)-(t\cdot n)-(n)}{2}} \\ &\leq 2^{-3n}. \end{aligned}$$

Thus it holds for any $m \in \mathbb{K}$ that

$$\begin{aligned} &\Delta((I(X'), S') | \langle X', S'\rangle_{\mathbb{K}} = m;\ (I(X'), S')) \leq 2 \cdot 2^n \cdot 2^{-3n} = 2 \cdot 2^{-2n}, \\ &\Delta\left(I(X'), I(S') | \langle X', S'\rangle_{\mathbb{K}} = m;\ I(X'), I(S')\right) \leq 2^{-n} \\ &\Delta\left(I(X), I(S);\ I(X'), I(S')\right) \leq 2^{-n}. \end{aligned}$$

which shows it is indeed possible to find required sets. □

Proof (Lemma 11). We let $D_1 = D_{id}$ and we let $D_5 = D_{rest}$. Let $S = S_1 \cup S_5$. Note the $S = I^{-1}(1) \cup I^{-1}(1)$. We have from the proof of the above lemma that the sets have the correct sizes for $\varepsilon = 2^{-n}$. Furthermore, if S_1 happens, then K_1 is again benign as the Class-1 cube is a cube, and if S_5 happens, then K_5 is again benign as the Class-5 cube is a cube.

Lemma 13 (Case 1). *Let C be a* Class-1 *cube. When X, S are unchanged then $f_W(\langle X, S\rangle_{\mathbb{F}}) = \langle X, S\rangle_{\mathbb{F}}$ and $f_V(\langle X, S\rangle_{\mathbb{K}}) = \langle X, S\rangle_{\mathbb{K}}$, else* Dec *will return $\perp$. Let $\mathcal{C}_W, \mathcal{C}_V$ be the sets of fixed points of f_W, f_V respectively. Let $\mathcal{C}'_W = \mathcal{C}_W \cap \mathcal{A}_W$ and $\mathcal{C}'_V = \mathcal{C}_V \cap \mathcal{A}_V$, moreover let $K' = K \wedge (\langle X, S\rangle_{\mathbb{F}} \in \mathcal{C}'_W) \wedge (\langle X, S\rangle_{\mathbb{K}} \in \mathcal{C}'_V)$. Then*

$$\begin{aligned} \Pr(\langle X, S\rangle_{\mathbb{F}} \in \mathcal{C}'_W \wedge \langle X, S\rangle_{\mathbb{K}} \in \mathcal{C}'_V \mid (X, S) \in C, K) \leq \\ 2^{-(\log(\Pr(K\wedge(X,S)\in C)) - \log(\Pr(K'\wedge(X,S)\in C)))} \end{aligned}$$

Proof. Obvious via conditional probability. □

Definition 18 (Class-1 Event). *For the Class-1 cube C we define the winning event $Z_1 = \emptyset$ and survival event B_1 to be the set of $(X, S, V, W) \in K \cap C$ for which $\langle X, S\rangle_{\mathbb{F}} \in \mathcal{C}'_W$ and $\langle X, S\rangle_{\mathbb{K}} \in \mathcal{C}'_V$. Let $D_1 = K \cap C \setminus B_1$.*

Lemma 14 (1-strategy). *The strategy $(\{(B_1, D_1)\}, Z)$ is legal for $G(K \cap C, 0, 0, \tau = \frac{1}{2t+2}, \rho)$. Furthermore, the knowledge K_1 corresponding to B_1 happening is benign, and if D_1 happens the tampering oracle outputs $\perp$.*

Proof. We have from the above lemma that $\Pr[B_1 \mid B_1 \cup D_1] \leq \Pr[B_1 \mid K]^{\frac{1}{1}}$, which implies that $\Pr[B_1 \mid B_1 \cup D_1] \leq \Pr[B_1 \mid K]^{\tau}$, as desired.

Lemma 15 (Case 5). *Let C be a* Class-5 *cube. If it holds that*

$$\Pr\left((X, S) \in C \mid K\right) \geq \gamma \frac{1}{\rho}$$

then for all $x, s \in \mathbb{K}^t$ there exist sets $D_{x,s} \subseteq \mathbb{K}^t \times \mathbb{K}^t$ such that:

1. *for all* $a, b \in D_{x,s} : \langle f(a), g(b)\rangle \neq f_V(\langle a, b\rangle$
2. *for any* $(x', s') \neq (x, s) : \quad D_{x',s'} \cap D_{x,s} = \emptyset$
3. $\Pr[(f(\tilde{X}), g(\tilde{S}), f_W(\langle \tilde{X}, \tilde{S}\rangle_{\mathbb{F}}), f_V(\langle \tilde{X}, \tilde{S}\rangle)) = (x, s, \mathrm{tr}(\langle x, s\rangle), \langle x, s\rangle)$
   $\mid (f(\tilde{X}), g(\tilde{S}), f_V(\langle \tilde{X}, \tilde{S}\rangle)) = (x, s, \langle x, s\rangle) \vee (\tilde{X}, \tilde{S}) \in D_{x,s}] \leq$

   $\leq 2^{-\frac{1}{2t+2}\log \Pr^{-1}\left[\left(f(\tilde{X}), g(\tilde{S}), f_W(\langle \tilde{X}, \tilde{S}\rangle_{\mathbb{F}}), f_V(\langle \tilde{X}, \tilde{S}\rangle)\right) = (x, s, \mathrm{tr}(\langle x, s\rangle), \langle x, s\rangle)\right]} + \varepsilon$

where $(\tilde{X}, \tilde{S})$ *is the conditional distributions* $(X, S)|((X, S) \in C, K)$*, and* $\varepsilon = 2(\varepsilon_{\mathrm{L}} + 2^{-n})$ *where* ε_{L} *comes from Definition 10.*

Intuition: In this case $\langle f(X), g(S)\rangle_{\mathbb{K}}$ is independent of $\langle X, S\rangle_{\mathbb{K}}$ and the more the adversary is trying to learn (i.e., pre-images of f, g are smaller) the less control over $\langle f(X), g(S)\rangle_{\mathbb{K}}$ he has.

Proof. We do not need an efficient construction of the sets $D_{x,s}$, they are here only to prove that whenever the adversary attempts to learn something he will be detected (condition 1) with a probability corresponding to the amount of information he wants to obtain. Let us first prove that there exists sets $D_{x,s}$ fulfilling the following inequality:

$$\begin{aligned}\Pr[(f(\tilde{X}), g(\tilde{S}), f_V(\langle \tilde{X}, \tilde{S}\rangle))& \\ = (x, s, \langle x, s\rangle) \mid (f(\tilde{X}), g(\tilde{S}), f_V(\langle \tilde{X}, \tilde{S}\rangle))(x, s, \langle x, s\rangle) \vee (\tilde{X}, \tilde{S}) \in D_{x,s}] \leq & \quad (8)\\ \leq 2^{-\frac{1}{2t+2}\log \Pr^{-1}\left[\left(f(\tilde{X}), g(\tilde{S}), f_V(\langle \tilde{X}, \tilde{S}\rangle)\right) = (x, s, \langle x, s\rangle)\right]} + \varepsilon &\end{aligned}$$

From (8) we can calculate the required sizes of sets $D_{x,s}$.

$$\begin{aligned}\Pr[(f(\tilde{X}), g(\tilde{S}), f_V(\langle \tilde{X}, \tilde{S}\rangle)) = (x, s, \langle x, s\rangle) \mid (f(\tilde{X}), g(\tilde{S}), f_V(\langle \tilde{X}, \tilde{S}\rangle))& \\ = (x, s, \langle x, s\rangle) \vee (\tilde{X}, \tilde{S}) \in D_{x,s}]& \\ \leq (\Pr[(f(\tilde{X}), g(\tilde{S}), f_V(\langle \tilde{X}, \tilde{S}\rangle)) = (x, s, \langle x, s\rangle)])^{\frac{1}{2t+2}}&\end{aligned}$$

$$\begin{aligned}&\frac{\Pr[(f(\tilde{X}), g(\tilde{S}), f_V(\langle \tilde{X}, \tilde{S}\rangle)) = (x, s, \langle x, s\rangle)]}{\Pr[(f(\tilde{X}), g(\tilde{S}) f_V(\langle \tilde{X}, \tilde{S}\rangle)) = (x, s, \langle x, s\rangle)] + \Pr[(\tilde{X}, \tilde{S}) \in D_{x,s}]}\\ &\leq \Pr[(f(\tilde{X}), g(\tilde{S}), f_V(\langle \tilde{X}, \tilde{S}\rangle)) = (x, s, \langle x, s\rangle)]^{\frac{1}{2t+2}}\end{aligned}$$

$$\begin{aligned}\Pr[(f(\tilde{X}), g(\tilde{S}) f_V(\langle \tilde{X}, \tilde{S}\rangle)) = (x, s, \langle x, s\rangle)]^{\frac{2t+1}{2t+2}} - \Pr[(f(\tilde{X}), g(\tilde{S}), f_V(\langle \tilde{X}, \tilde{S}\rangle)) = (x, s, \langle x, s\rangle)]& \\ \leq \Pr[(\tilde{X}, \tilde{S}) \in D_{x,s}]. & \quad (9)\end{aligned}$$

To show existence of sets $D_{x,s}$ all we need to prove is that:

$$\sum_{(x,s)} \Pr[(f(\tilde{X}), g(\tilde{S}), f_V(\langle \tilde{X}, \tilde{S}\rangle)) \in D_{x,s}] \leq 1 - \sum_{(x,s)} \Pr[(f(\tilde{X}), g(\tilde{S}), f_V(\langle \tilde{X}, \tilde{S}\rangle)) = (x, s, \langle x, s\rangle)]$$

Thus via (9)

$$\sum_{(x,s)} \Pr[(f(\tilde{X}), g(\tilde{S}), f_V(\langle \tilde{X}, \tilde{S}\rangle)) = (x, s, \langle x, s\rangle)]^{\frac{2t+1}{2t+2}} \leq 1. \quad (10)$$

At this point we would like to use Lemma 6, to do that we need to prove independence of $f_i(\tilde{X}_i)$ and $g_i(\tilde{S}_i)$. Let X' be a conditional distribution $X|X \in (C \cap \mathcal{A}_X)$ and let S' be conditional distribution $S|S \in (C \cap \mathcal{A}_S)$. We know that:

$$\begin{aligned}
&\mathbf{H}_\infty(X') \geq t \cdot n - \log \frac{1}{\gamma} - k \geq t \cdot n - \delta_{\mathrm{L}} \\
&\mathbf{H}_\infty(S') \geq t \cdot n - \log(\frac{1}{\gamma}) - k \geq t \cdot n - \delta_{\mathrm{L}} \\
&\widetilde{\mathbf{H}}_\infty(X'|f(X')) \geq t \cdot (\frac{1}{3}n + \frac{2}{7t}\delta_{\mathrm{D}}) - \log \frac{1}{\gamma} - k \geq \frac{1}{3}t \cdot n + \frac{1}{7}\delta_{\mathrm{D}}
\end{aligned}$$

Via the strong extraction property of the Hadamard-extractor (Lemma 1) and Bayes' rule for the statistical distance (Lemma 2) we know that

$$\begin{aligned}
d(\langle X', S'\rangle_{\mathbb{K}}|f(X'), S') &\leq 2^{-\frac{\tilde{\mathbf{H}}_\infty(X'|f(X')+\mathbf{H}_\infty(S')-(t\cdot n)-n}{2}} \\
&= 2^{-\frac{(\frac{1}{3}t\cdot n+\frac{1}{7}\delta_{\mathrm{D}})+(t\cdot n-\log(\frac{1}{\gamma})-k)-(t\cdot n)-(n)}{2}} \\
&\leq 2^{-2n}.
\end{aligned}$$

Thus for U_K uniformly distributed over $\mathcal{A}_F$ and independent of all other random variables:

$$\Delta((f(X'), S')|\langle X', S'\rangle_{\mathbb{K}} = m;\ (f(X'), S')) \leq 2 \cdot 2^n \cdot 2^{-2n} = 2 \cdot 2^{-n}, \tag{11}$$

$$\Delta\left(\left[f(\tilde{X}), g(\tilde{S}), f_V(\langle \tilde{X}, \tilde{S}\rangle)\right]\ ;\ \left[f(X'), g(S'), f_V(U_K)\right]\right) \leq 2 \cdot 2^n \cdot 2^{-2n} = 2 \cdot 2^{-n} \tag{12}$$

We know that $\mathcal{A}_X$ and C are cubes, thus their intersection is a cube. Via Condition 4 in Definition 10 we obtain that $f_1(X'_1), \ldots, f_t(X'_t), g_1(S'_t), \ldots, g_t(S'_t)$ are $2\varepsilon_{\mathrm{L}}$-close to $f_1(U_1), \ldots, g_t(U_{2t})$, where $[U_1, \ldots, U_{2t}]$ is uniformly distributed over the intersection of cubes $\mathcal{A}_X$ and C thus all random variables $f_1(U_1), \ldots, g_t(U_{2t}), f_V(U_K)$ are independent and through (12) we get that:

$$\Delta\left(\left[f(\tilde{X}), g(\tilde{S}), f_V(\langle \tilde{X}, \tilde{S}\rangle)\right]\ ;\ [f_1(U_1), \ldots, g_t(U_{2t}), f_V(U_K)]\right) \leq 2^{-\Omega(n)} \tag{13}$$

Via Lemma 6 applied to vectors $[f_1(U_1), \ldots, f_t(U_t), -1]$ and $[g_1(U_{t+1}), \ldots, g_t(U_{2t}), f_V(U_K)]$ we obtain:

$$\sum_{\substack{(x_1,\ldots,x_t,s_1,\ldots,s_t,c):\\ \langle[x_1,\ldots,x_t,-1];[s_1,\ldots,s_t,c]\rangle=0}} \Pr[(f_1(U_1), \ldots, g_t(U_{2t}), f_V(U_K)) = (x, s, c)]^{\frac{2t+1}{2t+2}} \leq 1$$

Thus we obtain (10) as desired:

$$\sum_{x,s} \Pr[(f(\tilde{X}), g(\tilde{S}), f_V(\langle \tilde{X}, \tilde{S}\rangle)) = (x, s, \langle x, s\rangle)]^{\frac{2t+1}{2t+2}} \leq 1 + 2\varepsilon_{\mathrm{L}} + 2 \cdot 2^{-n} \tag{14}$$

which, via (9) gives us existence of sets $D_{x,s}$ such that :

$$\begin{aligned}
&\Pr[(f(\tilde{X}), g(\tilde{S}), f_V(\langle \tilde{X}, \tilde{S}\rangle)) = (x, s, \langle x, s\rangle) \\
&\mid (f(\tilde{X}), g(\tilde{S}), f_V(\langle \tilde{X}, \tilde{S}\rangle)) = (x, s, \langle x, s\rangle) \vee (\tilde{X}, \tilde{S}) \in D_{x,s}] \leq \\
&\leq 2^{-\frac{1}{2t+2}\log \Pr^{-1}\left[\left(f(\tilde{X}), g(\tilde{S}), f_V(\langle \tilde{X}, \tilde{S}\rangle)\right)=(x,s,\langle x,s\rangle)\right]} + \varepsilon
\end{aligned}$$

Now if we multiply the left hand side by

$$\Pr\left(f_W(\langle\tilde{X},\tilde{S}\rangle) = \mathrm{tr}(\langle x,s\rangle) \mid (f(\tilde{X}), g(\tilde{S}), f_V(\langle\tilde{X},\tilde{S}\rangle)) = (x,s,\langle x,s\rangle)\right)$$

and the right hand side by something larger:

$$\Pr\left(f_W(\langle\tilde{X},\tilde{S}\rangle) = \mathrm{tr}(\langle x,s\rangle) \mid (f(\tilde{X}), g(\tilde{S}), f_V(\langle\tilde{X},\tilde{S}\rangle)) = (x,s,\langle x,s\rangle)\right)^{\frac{1}{2t+2}}$$

we obtain the result. □

Definition 19 (Class-5 Events). *For the Class-5 cube C we define a win event $Z_5 = \emptyset$. For each (x,s) we define a survival event $B_{x,s}$ to be the set of $(X,S,V,W) \in K$ for which*

$$(f(X), g(S), f_W(\langle X,S\rangle_{\mathbb{F}}), f_V(\langle X,S\rangle)) = (x,s,\langle x,s\rangle_{\mathbb{F}}, \langle x,s\rangle_{\mathbb{F}}) \ .$$

We use the death events $D_{x,s}$ from the above lemma.

Lemma 16 (5-strategy). *Let C be the class-5 cube. The strategy $(\{(B_{x,s}, D_{x,s})\}, Z)$ is legal for $G(K \cap C, \varepsilon = 2(\varepsilon_{\mathrm{L}} + 2^{-n}), \sigma = 0, \tau = \frac{1}{2t+2}, \rho)$. Furthermore, each $K_{x,s}$ corresponding to $B_{x,s}$ is benign and if any $D_{x,s}$ occurs, the tampering oracle outputs $\perp$.*

Proof. By the above lemma the death events have the right size when $\varepsilon = 2(\varepsilon_{\mathrm{L}} + 2^{-n})$. Clearly, when $B_{x,s}$ happens the knowledge $K_{x,s}$ is again benign, and by design D triggers $\perp$.

6.7 Putting the Pieces Together

We now link the tampering game to the K-game as follows. Let K_0 denote that $\mathcal{A}$ has no knowledge on the codeword. The game starts at $K = K_0$. We will argue that the probability that the tampering adversary $\mathcal{A}$ makes it happen that $\Pr[K] \leq \rho$ is upper bounded by the probability of some $\mathcal{B}$ winning $G_{\mathcal{B}}(K_0, \varepsilon, \sigma, \tau, \rho)$ for $\varepsilon = O(\varepsilon_{\mathrm{L}}) + O(\varepsilon_{\mathrm{D}}) + 2^{-\Omega(n)} + 2^{-\Omega(\delta_{\mathrm{D}})}$, $\sigma = \gamma\frac{1}{\rho}$, $\tau = \frac{1}{2t+2}$. Note that K_0 is benign. Whenever $\mathcal{A}$ tampers, let K be the knowledge of $\mathcal{A}$ and assume by induction that K is benign. Assume that the random codeword sampled in the game is the same as the one in the tampering game. We first play the 1-or-5-strategy to learn whether the codeword is in the Class-1 or Class-5 cube or some other cube. By design, we lose the K-game only if the tampering oracle outputs $\perp$. Otherwise we win the K-game or we have to recursively play it for $K \cap C_1$ or $K \cap C_5$, where C_1 is the Class-1 cube and C_5 is the Class-5 cube. In the first place we play the 1-strategy. In the second case we play the 5-strategy. Again, by design, we lose the K-game only if the tampering oracle outputs $\perp$. Otherwise we win the game or end up in a survival zone. If we end up in a survival zone, the new K' we have to play is exactly the knowledge of the tampering adversary $\mathcal{A}$. Note that for each tampering query we make two moves in the K-game.

Let r denote the number of tampering queries done by the adversary. It follows by the above analysis and the Knowledge Lemma that when the tampering oracle outputs $\perp$, then $\Pr[\Pr[K] \leq \rho] \leq \rho^{\tau} + 2r \cdot (O(\varepsilon_{\mathrm{L}}) + O(\varepsilon_{\mathrm{D}}) + 2^{-\Omega(n)} + 2^{-\Omega(\delta_{\mathrm{D}})} + \gamma\frac{1}{\rho})$. This concludes the proof of Theorem 5.

7 Instantiation of Definition 10

In this section we discuss various instantiation options. We give a generic method of instantiating with any multi-source non-malleable extractor. This method requires small changes to the proof which are discussed below. The proof modifications are required only for nmExtractors that do not have good *leakage resilient storage* parameters. They lead to slightly worse parameters of ow-CNMC thus they were separated from the main proof into this section.

7.1 Using Super-Strong NMCs

The most straight forward instantiation would be using the super-strong NMC from [AKO16] (with the improved affine evasive function from [Agg15]). Let us briefly recall the construction:

For any $m \in \mathcal{M}$, $\mathsf{Enc}(m) = \mathsf{Enc}_1 \circ \mathsf{Enc}_2(m)$, where for any $m \in \mathcal{M}$, $\mathsf{Enc}_2(m) \leftarrow \{X \in \mathbb{F} \mid h(X) = a||b||m\}$, where h is affine-evasive function, and a, b were chosen uniformly at random. For any $x \in \mathbb{F}$, $\mathsf{Enc}_1(x) = (L, R)$, where $L, R \in \mathbb{F}^N$ are uniform such that $\langle L, R\rangle = x$, $\phi(L, a) =$ valid and $\phi(R, b) =$ valid where ϕ is a check function based on Reed-Salomon codes, such that for every a we get $\Pr_x(\phi(x, a) = \text{valid}) = \frac{1}{|a|}$. The construction is secure for any $N \geq C \cdot \log^4 |\mathbb{F}|$, where C is some constant, which makes the whole codeword length equal to $C \cdot \log^5(|\mathbb{F}|)$.
Let us go through conditions from Definition 10:

Canonical encoder Fulfilled trivially.
Density of codewords Through the inspection of the construction we get that

$$\mathbf{H}_\infty(\mathsf{Enc}(U)) \geq 2 \cdot \log^5(|\mathbb{F}|) - O(\log |\mathbb{F}|)$$

the entropy loss $O(\log |\mathbb{F}|)$ is independent of the choice of N.
Detection of close to bijective tampering Through inspection of Theorem 5 from [AKO16] and Theorem 3 from [ADL14] we obtain that detection is possible for

$$\delta_{\mathrm{D}} = C' \cdot (N)^{1/4}$$

$$\varepsilon_{\mathrm{D}} = \frac{1}{|\mathbb{F}|^{\Omega(1)}}$$

where $C' > 0$ is some constant. To fulfil the parameter requirements, namely $k = \frac{1}{28t}\delta_{\mathrm{D}}$, all we have to do is choose N large enough (above we said that k does not depend on N).
Leakage resilient storage Since the construction is based on the inner-product it is clear that this condition is fulfilled with $\delta_{\mathrm{L}} = \Theta(\log^5 |\mathbb{F}|)$ and $\varepsilon_{\mathrm{L}} = 2^{-\Omega(\log^5 |\mathbb{F}|)}$.

Since all parameters are fulfilled we can instantiate:

Theorem 6. *There exists explicit $(\delta, \varepsilon)-$owCNMC in the $94-$split state model that encodes m bits of message into n bits of codeword, with the following parameters:*

- $\delta \leq \Theta(n^{1/5})$,

– $\varepsilon \leq r \cdot \left(2^{-\Omega(\delta)} + O\left(\frac{1}{n^{\Omega(1)}}\right)\right)$, *where* r *is the number of tampering queries made by the adversary.*
– *for adversary attempting poly*(δ) *queries*

$$\varepsilon \leq \mathsf{negligible}(\delta)$$

– *The length of the codeword is* $n = O(m^5)$.

7.2 Using multi-source non-malleable Extractors.

We start with a definition

Definition 20 (Non-malleable T-Source Extractors). *A function* $\mathsf{Ext} : (\mathcal{B})^T \to \mathcal{Y}$ *is called a* T*-source* (ε, δ)*-non-malleable extractor if the following property holds. For every random variable* $B = (B_1, \ldots, B_T) \in \mathcal{B}^T$ *for which* $B_1, ..., B_T$ *are independent and* $\mathbf{H}_\infty(B_i) \geq t \cdot \log|\mathcal{B}| - \delta$*, for any split-state tampering function* $f = (f_1, ..., f_T)$ *such that there exists* f_i *without fixed points it holds that*

$$\Delta\left((\mathsf{Ext}(B), \mathsf{Ext}(f(B))); (U, \mathsf{Ext}(f(B))\right) \leq \varepsilon,$$

where U *is distributed uniformly on* $\mathcal{Y}$.

We describe below how to modify any T source extractor to fit our requirements.

Definition 21. *Let* $k \in N$ *be any constant*

$\mathcal{E}(M)$:	$\mathcal{D}(X_1, \ldots, X_t)$:
$B_1, ..., B_T \leftarrow \{b_1, \ldots, b_T \mid \mathsf{Ext}(b_1, \ldots, b_T) = 0^k \| M\}$	$B_1 = (X_1, ..., X_{\frac{t}{T}})$
$(X_1, ..., X_{\frac{t}{T}}) = B_1$	$\ldots$
$\ldots$	$B_T = (X_{t-\frac{t}{T}+1}, ..., X_t)$
$(X_{t-\frac{t}{T}+1}, ..., X_t) = B_T$	*Check whether:*
Output $(X_1, \ldots, X_t)$	$\mathsf{Dec}(B_1, \ldots, B_T) = 0^k \| M$,
	If the check fails output $\perp$
	Otherwise, output $M \in \mathcal{M}$

Lemma 17. *Scheme* $(\mathcal{E}, \mathcal{D})$ *defined above fulfills:*

Canonical $\mathcal{E}$ procedure: $\mathcal{E}(m)$ *is uniform in* $\{c : \mathcal{D}(c) = m\}$.
Detection of close to bijective tampering: $\delta_{\mathrm{D}} = \frac{1}{2}\delta$ *(where* δ *comes from definition 20) and* $n = \log|\mathbb{K}|$ *and if* $X_1, \ldots, X_t \in \mathbb{K}$ *are independent random variables such that for* X *being the conditional distribution* $((X_1, \ldots, X_t)|D(X_1, ..., X_t) \neq \perp)$ *with*

$$\mathbf{H}_\infty(X) \geq t \cdot n - \delta_{\mathrm{D}}$$

and deterministic function $f = (f_1, \ldots, f_t)$, $f_i : \mathbb{K} \to \mathbb{K}$ *is such that*

$$\mathbf{H}_\infty(f(X)) \geq t \cdot n - \delta_{\mathrm{D}}$$

and $f(X) \neq X$*, then*

$$\Delta\left[(\mathcal{D}(X), \mathcal{D}(f(X)))\,; (U, \perp)\right] \leq 2\varepsilon + 2^{-k}.$$

Proof. From definition 20 we get

$$\Delta\left((\mathsf{Ext}(X_1,\ldots,X_t),\mathsf{Ext}(f_1(X_1),\ldots,f_t(X_t));(U,\mathsf{Ext}(f_1(X_1),\ldots,f_t(X_t))\right)\leq\varepsilon,$$

and we also know that $f(X_1,\ldots,X_t)$ has a lot of entropy so $\mathsf{Ext}(f_1(X_1),\ldots,f_t(X_t))$ is $\varepsilon-$close to uniform, thus $\Pr(cD(X_1,\ldots,X_t)\neq\perp)\leq 2^{-k}$.

High density of valid codewords: *for any k we get:*

$$\mathbf{H}_\infty(\mathcal{E}(U))=n\cdot t-k\ .$$

Thus it is possible to choose k fulfilling the parameters requirements.

Leakage resilient storage: *Take $\delta_{\text{L}}=\frac{T}{2t}\delta$ and the following holds. If $X\in(\mathbb{K})^t$ is such that*

$$\mathbf{H}_\infty(X)\geq t\cdot n-\delta_{\text{L}}$$

and $X_1,\ldots,X_t$ are independent random variables and $f=(f_1,\ldots,f_t)$, $f_i:\mathbb{K}\to\mathbb{K}$ is such that

$$\mathbf{H}_\infty(U|f_i(U)=u)\geq n-\delta_{\text{L}}$$

then

$$\Delta\left[(f_1(X_1),\ldots,f_t(X_t)\mid\mathcal{D}(X)\neq\perp);(f_1(X_1),\ldots,f_t(X_t))\right]\leq 2\varepsilon\ .$$

Proof. This follows straight forward from extractor properties. $\mathbf{H}_\infty(X_i|f_i(X_i))\geq n-2\delta_{\text{L}}$ and thus $\mathbf{H}_\infty(B_i|f_{\frac{i\cdot t}{T}+1}(X_{\frac{i\cdot t}{T}+1}),\ldots,f_{\frac{i\cdot t}{T}+T}(X_{\frac{i\cdot t}{T}+T}))\geq\frac{t}{T}\cdot n-\delta$ thus

$$d(\mathsf{Ext}(B_1,...,B_T)\mid(f_1(X_1),...,f_t(X_T)))\leq\varepsilon.$$

Thus

$$\Delta\left((\mathsf{Ext}(X_1,\ldots,X_t),\mathsf{Ext}(f_1(X_1),\ldots,f_t(X_t));(U,\mathsf{Ext}(f_1(X_1),\ldots,f_t(X_t)))\right)\leq\varepsilon\cdot\frac{1}{(1-2^{-k})}.$$

We can see above that the generic nmExtractor fulfils the *Leakage resilient storage* condition with significantly worse parameters than required. This can be fixed via a small change to the partition of the domain.

In the partition definition we will add one more set:

Definition 22. *Let $f_i:\mathbb{K}\to\mathbb{K}$ be a tampering function. We define the following partition of $\mathbb{K}$ for U uniformly distributed over $\mathbb{K}$.*

$$\begin{aligned}
\mathbb{C}^{f_i}_{id}&=\{x\in\mathbb{K}\,|\,f_i(x)=x\},\\
\mathbb{C}^{f_i}_{[a;b]}&=\{x\in\mathbb{K}\setminus\mathbb{C}^{f}_{id}\mid\mathbf{H}_\infty(U|f(U)=f_i(x))\in[a,b]\}\\
\mathbb{C}^{f_i}_{1\text{-}1}&=\mathbb{C}^{f_i}_{[0;\frac{6}{7t}\delta_{\text{D}}]}\\
\mathbb{C}^{f_i}_{med}&=\mathbb{C}^{f_i}_{[\frac{6}{7t}\delta_{\text{D}};\ \frac{1}{3}\cdot n+\frac{2}{7t}\delta_{\text{D}}]}\\
\mathbb{C}^{f_i}_{rest}&=\mathbb{C}^{f_i}_{[\frac{1}{3}\cdot n+\frac{2}{7t}\delta_{\text{D}};\ n-(\delta_{\text{L}}-\log\frac{1}{\gamma}-k)]}\\
\mathbb{C}^{f_i}_{const}&=\mathbb{C}^{f_i}_{[n-(\delta_{\text{L}}-\log\frac{1}{\gamma}-k);\ n]}.
\end{aligned}$$

Which leads to small modification of *Cubes Classes*:

Definition 23. *1. There is only* 1 *cube in Class-*1*:*

$$\forall_i\ A_i = C_{id}^{f_i},\ B_i = C_{id}^{g_i}.$$

*2. Class-*2 *are the cubes of form:*

$$A_i \in \{C_{id}^{f_i}, C_{1-1}^{f_i}\} \text{ and } B_i \in \{C_{id}^{g_i}, C_{1-1}^{g_i}\},$$

and there exists i *such that* $A_i \neq C_{id}^{f_i}$ *or* $B_i \neq C_{id}^{g_i}$*.*

*3. Class-*3 *cubes are of the form:*

$$A_i \in \{C_{id}^{f_i}, C_{1-1}^{f_i}, C_{med}^{f_i}, C_{rest}^{f_i}, C_{const}^{f_i}\} \text{ and } B_i \in \{C_{id}^{g_i}, C_{1-1}^{g_i}, C_{med}^{g_i}, C_{rest}^{g_i}, C_{const}^{g_i}\},$$

and there exists i *such that* $A_i \in \{C_{med}^{f_i}, C_{rest}^{f_i}, C_{const}^{f_i}\}$ *or* $B_i \in \{C_{med}^{g_i}, C_{rest}^{g_i}, C_{const}^{g_i}\}$*, and in each half of the vector describing this cube there is at most* 12 *coordinates that are equal to* $C_{rest}^{\cdot i}$ *or* $C_{const}^{\cdot i}$*.*

*4. Class-*4 *includes all cubes that weren't included above except* $\prod_{i=1}^{t} C_{const}^{f_i} \times \prod_{i=1}^{t} C_{const}^{g_i}$

*5. Class-*5 *includes only one cube that is*

$$\prod_{i=1}^{t} C_{const}^{f_i} \times \prod_{i=1}^{t} C_{const}^{g_i}$$

This change does not influence the case analysis much.

Case 1, 2, 3 stay exactly the same

Case 4 In inequality (6) we get $\mathbf{H}_\infty(f(\tilde{X})) \geq (\delta_{\mathrm{L}} - \log\frac{1}{\gamma} - k) - \log\frac{1}{\gamma} - k$, thus later on we obtain $\max_z \Pr(\langle f(\tilde{X}), g(S')\rangle_{\mathbb{K}} = z) \leq 2^{-((\delta_{\mathrm{L}} - \log\frac{1}{\gamma} - k) - \log\frac{1}{\gamma} - k)}$ and then

$$\begin{aligned}\max_z \Pr(\langle f(X'), g(S')\rangle_{\mathbb{K}} = z) = \max_z \Pr(\langle f(\tilde{X}), g(S')\rangle_{\mathbb{K}} = z \mid \mathcal{D}(\tilde{X}) \neq \perp) \\ \leq 2^{-\frac{((\delta_{\mathrm{L}} - \log\frac{1}{\gamma} - k) - \log\frac{1}{\gamma} - k) - \log\frac{1}{\gamma} - k}{t}}\end{aligned}$$

Thus via the above and (5) we get that for any $m \in \mathbb{K}$ the following holds:

$$\begin{aligned}\max_z \Pr(\langle f(X'), g(S')\rangle_{\mathbb{K}} = z | \langle X', S'\rangle_{\mathbb{K}} = m, K) &\leq 2^{-\frac{\delta_{\mathrm{L}} - 3\log\frac{1}{\gamma} - 3k}{t}} + 2 \cdot 2^{-\frac{1}{2}n} \\ &\leq 2^{-\Omega(\delta_{\mathrm{L}})},\end{aligned}$$

when $\delta_{\mathrm{L}} - 3\log\frac{1}{\gamma} - 3k = \Omega(\delta_{\mathrm{L}})$ (this will be trivially fulfilled by the choice of γ and k as in Theorem 5 and Definition 10).

This gives us the following parameters for Case 4. Let C be a *Class-*4 cube and

$$\Pr\left((X, S) \in C\right) \mid K) \geq \gamma\frac{1}{\rho},$$

then

$$\Pr(f_V(\langle X; S\rangle_{\mathbb{K}}) = \langle f(X); g(S)\rangle_{\mathbb{K}} \mid K, (X, S) \in C) \leq 2^{-\Omega(\delta_{\mathrm{L}})}$$

Case 5 The parameters are unchanged. The only point where the modified partition comes into play is at equation (13). Since

$$\mathbf{H}_\infty(X_i'|f_i(X_i')) \geq n - (\delta_{\text{L}} - \log\frac{1}{\gamma} - k) - \log\frac{1}{\gamma} - k \geq n - \delta_{\text{L}}$$

we can use Lemma 17 to obtain equation (13).

Corollary 1. *Since the above is true for any k it is possible to set $k = \frac{1}{28t}\delta_{\text{D}}$ and all parameter requirements will be fulfilled. Thus via Theorem 5 we obtain that for any $T-$source (ε, δ)-non-malleable extractor there exists an explicit $(\delta_{ow}, \varepsilon_{ow})$-owCNMC with the following properties:*

- $\delta_{ow} \leq \frac{1}{120t}\delta$,
- $\varepsilon_{ow} \leq r(2^{-\Omega(\delta_{ow})} + O(\varepsilon))$, *where r is the number of tampering queries made by the adversary,*
- *Notice that if r is polynomial in δ_{ow} and ε are negligible in δ_{ow} then*

$$\varepsilon_{ow} \leq \mathsf{negligible}(\delta_{ow})$$

  for an adversary making at most $\mathsf{poly}(\delta_{ow})$ queries.
- *The rate of this owCNMC is equal to $C \cdot \mathsf{nmextrate}$ where C is some constant and $\mathsf{nmextrate}$ is the rate of underlying nmExtractor.*

Proof. To put things together we repeat the same argument as in Section 6.7. We obtain that for an adversary tampering r times:

$$\Pr[\Pr[K] \leq \rho] \leq \rho^\tau + 2r \cdot \left(O(\rho) + O(\varepsilon_{\text{L}}) + O(\varepsilon_{\text{D}}) + 2^{-\Omega(n)} + 2^{-\Omega(\delta_{\text{L}})} + 2^{-\Omega(\delta_{\text{D}})} + \gamma\frac{1}{\rho}\right)$$

Via Lemma 17 we get that $\varepsilon_{\text{D}} = 2\varepsilon + 2^{-k}$ and $\varepsilon_{\text{L}} = 2\varepsilon$. This in particular gives us that

$$\Pr[\Pr[K] \leq 2^{-\frac{1}{60t}(\frac{1}{2}\delta)}] \leq 2^{-\frac{1}{60t}(\frac{1}{2}\delta)\cdot\frac{1}{2t+2}} + 2r \cdot (O(2^{-\frac{1}{60t}(\frac{1}{2}\delta)}) + O(\varepsilon) + O(2^{-k}) + 2^{-\Omega(n)} + 2^{-\Omega(\delta)} + 2^{-\frac{1}{55t}(\frac{1}{2}\delta)})$$

which substituting the remaining parameters leads to

$$\Pr[\Pr[K] \leq 2^{-\frac{1}{60t}(\frac{1}{2}\delta)}] \leq r \cdot (2^{-\Omega(\delta)} + O(\varepsilon)) \ .$$

□

Recently, a 9-source non-malleable extractor was constructed by Chattopadhyay and Zuckerman [CZ14].

Theorem 7 ([CZ14]). *For some $\phi > 0$ there exists a polynomial time construction of a (k, ε) non-malleable 10-source extractor $\mathsf{nmExt} : (\mathbb{F}_q^n)^{10} \to \mathbb{F}_q^m$ with $k = (1-\phi)n$, $\varepsilon = 2^{-\Omega(n)}$ and $m = \Omega(k)$. Moreover, nmExt is efficiently preimage samplable.*

Using Corollary 1 we get:

Theorem 8. *There exists an explicit $(\delta, \varepsilon)-$owCNMC in the 94-split state model that encodes m bits of message into n bits of codeword, with the following parameters:*

- $\delta \leq \Theta(n)$,
- $\varepsilon \leq r \cdot (2^{-\Omega(\delta)} + O(2^{-\Omega(n)}))$, *where r is the number of tampering queries made by the adversary.*
- *For an adversary making poly(δ) queries*

$$\varepsilon \leq \mathit{negligible}(\delta)$$

- *Has constant code rate, i.e., the length of codeword is $n = O(m)$.*

Acknowledgements

The authors would like to thank Ilya Bogdanov who on Mathoverflow provided us with the elegant proof of the Death-Zones Generation Lemma.

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.

[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+14] Shashank Agrawal, Divya Gupta, Hemanta K. Maji, Omkant Pandey, and Manoj Prabhakaran. Explicit non-malleable codes resistant to permutations and perturbations. *IACR Cryptology ePrint Archive*, 2014:841, 2014.

[AKO16] Divesh Aggarwal, Tomasz Kazana, and Maciej Obremski. Inception makes non-malleable codes stronger. Cryptology ePrint Archive, Report Report 2015/1013, 2016. http://eprint.iacr.org/.

[CG14a] Mahdi Cheraghchi and Venkatesan Guruswami. Capacity of non-malleable codes. In Moni Naor, editor, *Innovations in Theoretical Computer Science, ITCS'14, Princeton, NJ, USA, January 12-14, 2014*, pages 155–168. ACM, 2014.

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

[CKM11] Seung Geol Choi, Aggelos Kiayias, and Tal Malkin. Bitr: built-in tamper resilience. In *Advances in Cryptology–ASIACRYPT 2011*, pages 740–758. Springer, 2011.

[CMTV15] Sandro Coretti, Ueli Maurer, Björn Tackmann, and Daniele Venturi. From single-bit to multi-bit public-key encryption via non-malleable codes. In 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*, pages 532–560. Springer, 2015.

[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.

[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] Sebastian Faust, Pratyay Mukherjee, Daniele Venturi, and Daniel Wichs. Efficient non-malleable codes and key-derivation for poly-size tampering circuits. In Phong Q. Nguyen and Elisabeth Oswald, editors, *Advances in Cryptology - EUROCRYPT 2014 - 33rd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Copenhagen, Denmark, May 11-15, 2014. Proceedings*, volume 8441 of *Lecture Notes in Computer Science*, pages 111–128. Springer, 2014.

[GLM+03] 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, *First Theory of Cryptography Conference — TCC 2004*, volume 2951 of *LNCS*, pages 258–277. Springer-Verlag, February 19–21 2003.

[JW15] Zahra Jafargholi and Daniel Wichs. Tamper detection and continuous non-malleable codes. In *Theory of Cryptography*, volume 9014 of *Lecture Notes in Computer Science*, pages 451–480. Springer Berlin Heidelberg, 2015.

[Li16] Xin Li. Improved non-malleable extractors, non-malleable codes and independent source extractors. arXiv Archive, arXiv:1608.00127, 2016. https://arxiv.org.

[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.

ECCC ISSN 1433-8092

https://eccc.weizmann.ac.il