Inception Makes Non-malleable Codes Stronger

Divesh Aggarwal[1], Tomasz Kazana[2], and Maciej Obremski[2,3]

[1] Ecole Polytechnique Federale de Lausanne
[2] University of Warsaw
[3] Aarhus University

Abstract. Non-malleable codes (NMCs), introduced by Dziembowski, Pietrzak and Wichs [DPW10], provide a useful message integrity guarantee in situations where traditional error-correction (and even error-detection) is impossible; for example, when the attacker can completely overwrite the encoded message. NMCs have emerged as a fundamental object at the intersection of coding theory and cryptography.
A large body of the recent work has focused on various constructions of non-malleable codes in the split-state model. Many variants of NMCs have been introduced in the literature i.e. strong NMCs, super strong NMCs and continuous NMCs. Perhaps the most useful notion among these is that of continuous non-malleable codes, that allows for continuous tampering by the adversary.
In this paper we give the first efficient, information-theoretic secure construction of continuous non-malleable codes in 2-split-state model. Enroute to our main result, we obtain constructions for almost all possible notion of non-malleable codes that have been considered in the split-state model, and for which such a construction is possible. Our result is obtained by a series of black-box reductions starting from the non-malleable codes from [ADL14].
One of the main technical ingredient of our result is a new concept that we call *inception coding*. We believe it may be of independent interest.

1 Introduction

Non-malleable Codes. Non-malleable codes (NMCs), introduced by Dziembowski, Pietrzak and Wichs [DPW10], provide a useful message integrity guarantee in situations where traditional error-correction (and even error-detection) is impossible; for example, when the attacker can completely overwrite the encoded message. NMCs have emerged as a fundamental object at the intersection of coding theory and cryptography.
Informally, given a tampering family $\mathcal{F}$, an NMC $(\mathsf{Enc}, \mathsf{Dec})$ against $\mathcal{F}$ encodes a given message m into a codeword $c \leftarrow \mathsf{Enc}(m)$ in a way that, if the adversary modifies m to $c' = f(c)$ for some $f \in \mathcal{F}$, then the the message $m' = \mathsf{Dec}(c')$ is either the original message m, or a completely "unrelated value". As has been shown by the recent progress [DPW10, LL12, DKO13, ADL14, FMVW14, FMNV14, CG14a, CG14b, CZ14, Agg15, ADKO15b, ADKO15a, CGL15, AGM+15b, AGM+15a, AAnHKM+16] NMCs

aim to handle a much larger class of tampering functions $\mathcal{F}$ than traditional error-correcting or error-detecting codes, at the expense of potentially allowing the attacker to replace a given message x by an unrelated message x'. NMCs are useful in situations where changing x to an unrelated x' is not useful for the attacker (for example, when x is the secret key for a signature scheme.)

Strong Non-malleable Codes. A stronger notion of non-malleability was also considered in [DPW10] in which, whenever the codeword c is modified to $c' = f(c) \neq c$, the decoded message $m' = \mathsf{Dec}(c')$ is independent of m. This is in contrast to the plain notion of non-malleability where some modification of the codeword c could still result in $m' = m$. Indeed, this is the case in some of the previous constructions of non-malleable codes like [ADL14, ADKO15a]. For the purpose of conveniently defining continuous non-malleable codes, an even stronger notion called super-strong non-malleable codes has been considered in the literature [FMNV14, JW15]. Informally speaking, in this notion, if $c' \neq c$ is a valid codeword, then c' must be independent of c.
An intermediate notion can also be considered where if $m' = \mathsf{Dec}(c') \notin \{m, \perp\}$, then c' must be independent of c. To be consistent with other notions of non-malleable codes, we call these super non-malleable codes.

Continuous Non-malleable Codes. It is clearly realistically possible that the attacker repeatedly tampers with the device and observes the outputs. As mentioned in [JW15], non-malleable codes can provide protection against these kind of attacks if the device is allowed to freshly re-encode its state after each invocation to make sure that the tampering is applied to a fresh codeword at each step. after each execution the entire content of the memory is erased. While such perfect erasures may be feasible in some settings, they are rather problematic in the presence of tampering. Due to this reason, Faust et al. [FMNV14] introduced an even stronger notion of non-malleable codes called continuous non-malleable codes where security is achieved against continuous tampering of a single codeword *without* re-encoding. Jafargholi and Wichs [JW15] considered four variants of continuous non-malleable codes depending on

- Whether tampering is *persistent* in the sense that the tampering is always applied to the current version of the tampered codeword, and all previous versions of the codeword are lost. The alternative definition considers non-persistent tampering where the tampering always occurs on the original codeword.
- Whether tampering to an invalid codeword (i.e., when the decoder outputs $\perp$) causes a *"self-destruct"* and the experiment stops and the attacker cannot gain any additional information, or alternatively whether the attacker can always continue to tamper and gain information.

Split-State Model. Although any kind of non-malleable codes codes do not exist if the family of "tampering functions" $\mathcal{F}$ is completely unre-

stricted,[4] they are known to exist for many broad tampering families $\mathcal{F}$. One such natural family is the family of tampering functions in the so called *t-split-state* model. In this model, the codeword is "split" into $t > 1$ states $c = (c_1, \ldots, c_t)$; a tampering function f is viewed as a list of t functions $(f_1, \ldots, f_t)$ where each function f_i tampers with corresponding component c_i of the codeword independently: i.e., the tampered codeword is $c' = (f_1(c_1), \ldots, f_t(c_t))$.

This family is interesting since it seems naturally useful in applications, especially when t is low and the shares $y_1, \ldots, y_t$ are stored in different parts of memory, or by different parties. Not surprisingly, the setting of $t = 2$ appears the most useful (but also the most challenging from the technical point of view), so it received the most attention so far [DPW10, LL12, DKO13, ADL14, FMNV14, CG14a, CG14b, CZ14, ADKO15b, ADKO15a] and is also the focus of our work.

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

There have been a series of recent results culminating in constructions of efficient non-malleable codes in the split-state model [DKO13, ADL14, CZ14, ADKO15a]. However, there is no known efficient construction in the continuous setting. Since the work of [FMNV14] rules out the possibility of such a construction for the case of non-persistent tampering, the best one can hope for is an efficient construction for the case of persistent tampering in the split-state model.

Our Results. The main result of the paper is the following:

Theorem 1. *For any k, there exists an efficient (in k) information-theoretically secure persistent continuous $2^{-k^{\Theta(1)}}$-non-malleable code with self-destruct in the split-state model that encodes k-bit messages to $\mathsf{poly}(k)$-bit codewords.*

The construction is obtained in a series of steps. We first show a simple reduction that any scheme in the split-state model that is a super-strong non-malleable code is also a persistent continuous non-malleable code. We believe that this result is interesting on its own. The statement is proven for the split-state model and a discussion about other model is placed in Remark 4.

Our main technical reduction is one that shows that any coding scheme that is super non-malleable in the split-state model can be converted into

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

a scheme that is super-strong non-malleable in the split-state model. It is worth mentioning that in particular it proves existance of efficient strong non-malleable codes which was stated as a open problem in [DPW10].
To do that we develop a new technique we called *inception coding*. Given the super non-malleable scheme $(\mathsf{Enc}, \mathsf{Dec})$ we modify encoding procedure to sacrifice small suffix of the message (it will not carry any message related information anymore) to replace it with validity checks for each of the states. $\mathsf{Enc}(m', \mathsf{check}_x, \mathsf{check}_y) = (X, Y)$ such that $\mathsf{Verify}(\mathsf{check}_x; X) = \mathsf{Verify}(\mathsf{check}_y; Y) = \mathrm{OK}$. Those checks can carry uniform seeds inside, which makes it easier to come up with various constructions. We settled on the construction combining Reed-Solomon codes with storing random coordinates of the codeword (induced by a random seed). Then we show recursive technique that makes checks arbitrary small (at the cost of security). Modified scheme encodes slightly shorter messages but it is crucial for clean transition from super non-malleable codes to super strong non-malleable codes. We also prove that this modification does not spoil the security of original code.
Finally, to complete the proof, we show that the coding scheme from [ADL14] is super non-malleable. This proof was surprisingly involved, since we need to argue that for any two tampered codewords c'_1, c'_2 of two distinct messages, if they do not decode to $\perp$ or the original messages, respectively, then the two tampered codewords are indistinguishable. This required a careful re-analysis of the cases in [ADL14].

Background. The notion of non-malleability was introduced by Dolev, Dwork and Naor [DDN00], and has found many applications in cryptography. Traditionally, non-malleability is defined in the computational setting, but recently non-malleability has been successfully defined and applied in the information-theoretic setting (generally resulting in somewhat simpler and cleaner definitions than their computational counterparts). For example, in addition to non-malleable codes studied in this work, the work of Dodis and Wichs [DW09] defined the notion of non-malleable extractors as a tool for building round-efficient privacy amplification protocols.
Finally, the study of non-malleable codes falls into a much larger cryptographic framework of providing counter-measures against various classes of tampering attacks. This work was pioneered by the early works of [ISW03, GLM+03, IPSW06], and has since led to many subsequent models. We do not list all such tampering models, but we refer to [KKS11, LL12] for an excellent discussion of various such models.

Other Related Work. In addition to the works mentioned above, non-malleable codes have been studied in various tampering models in several recent results. For tampering functions of size $2^{\mathsf{poly}(n)}$, rate-1 codes (with efficient encoding and decoding) exist, and can be obtained efficiently with overwhelming probability [FMVW14].
Cheraghchi and Guruswami [CG14b] gave a rate 1 non-malleable code against the class of bitwise-tampering functions, where each bit of the codewords is tampered independently. Recently, Agrawal et al. [AGM+15b, AGM+15a] improved this result by giving a explicit rate-1 code against

a stronger class of tampering functions, which in addition to tampering with each bit of the codeword independently, can also permute the bits of the resulting codeword after tampering, was achieved in [AGM+15b, AGM+15a].

In the "split state" setting, an encoding scheme was proposed in [CKM11]. For the case of only two states, an explicit non-malleable code for encoding one-bit message was proposed by [DKO13]. This was improved by Aggarwal et al [ADL14] to a scheme that encodes larger messages but with rate $1/\mathsf{poly}(k)$ where k is the length of the message. This was further improved to obtain a constant-rate non-malleable code in [CZ14, ADKO15a].

Another related result by Aggarwal et al [ADKO15b] obtained efficient construction of non-malleable codes in a model where the adversary, in addition to performing split-state tampering, is also allowed some limited interaction between the two states.

In the computational setting, there has been a sequence of works constructing non-malleable codes and its variants [LL12, FMNV14]. Chandran et al. [CGM+15] also rely on the computational setting in defining their new notion of *blockwise non-malleable codes*. Blockwise non-malleable codes are a generalization of the split-state model (and the recent lookahead model of [ADKO15a]) where the adversary tampers with one state at a time.

2 Preliminaries

For a set S, we let U_S denote the uniform distribution over S. For an integer $m \in \mathbb{N}$, we let U_m denote the uniform distribution over $\{0,1\}^m$, the bit-strings of length m. For a distribution or random variable X we write $x \leftarrow X$ to denote the operation of sampling a random x according to X. For a set S, we write $s \leftarrow S$ as shorthand for $s \leftarrow U_S$.

The Hamming distance between two strings $(a_1, \ldots, a_m)$, $(b_1, \ldots, b_m) \in \{0,1\}^m$ is the number of $i \in [m]$ such that $a_i \neq b_i$. We denote it as $\mathsf{Ham}((a_1, \ldots, a_m)\ ;\ (b_1, \ldots, b_m))$.

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

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

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

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

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

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

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

Note that $\Delta(W,Z) = \max_D(\Pr[D(W)=1] - \Pr[D(Z)=1])$, where D is a probabilistic function. We say W is ε-close to Z, denoted $W \approx_\varepsilon Z$, if $\Delta(W,Z) \leq \varepsilon$. We write $\Delta(W,Z|Y)$ as shorthand for $\Delta((W,Y),(Z,Y))$, and note that $\Delta(W,Z|Y) = \mathbb{E}_{y \leftarrow Y} \Delta(W|Y=y, Z|Y=y)$.

Reed-Solomon Codes. In Section 4 we will use standard Reed-Solomon error-correcting codes. This is useful and interesting mathematical object with vast literature on. However we will need only the following fact:

Lemma 2. *There exist a function* $RS : \{0,1\}^n \to \{0,1\}^{n+n^B\lceil \log n \rceil}$. *such that:*
– *Hamming distance between any two elements of the image of* RS *is at least* $n^B + 1$,
– *For any* $x \in \{0,1\}^n$ *there exist a unique sequence of bits* $u \in \{0,1\}^{n^B\lceil \log n \rceil}$ *such that* $x||u$ *is an element of the image of* RS*;*
– *For every* $u \in \{0,1\}^{n^B\lceil \log n \rceil}$ *the set of all* $x \in \{0,1\}^n$ *such that* $x||u$ *is an element of the image of* RS *is affine subspace of* $\{0,1\}^n$.

Proof. We can define RS as any Reed-Solomon error-correcting code with alphabet $\Sigma = \{0,1\}^{\lceil \log n \rceil}$, message length $k^* = n/\lceil \log n \rceil$ and codeword length $n^* = n^B + n/\lceil \log n \rceil$. The above properties of RS follow from standard properties of Reed-Solomon code. We omit details. □

The elements of the image of RS are called valid codewords for RS.

3 Various definitions of Non-Malleable Codes

Definition 1. (DPW Non-Malleable Code.) *Let* $(\mathsf{Enc} : \mathcal{M} \to \mathcal{X} \times \mathcal{X}, \mathsf{Dec} : \mathcal{X} \times \mathcal{X} \to \mathcal{M} \cup \{\perp\})$ *be an encoding scheme. For* $f, g : \mathcal{X} \to \mathcal{X}$ *and for any* $m \in \mathcal{M}$ *define the experiment* $\mathsf{DPWTamper}_m^{f,g}$ *as:*

$$\mathsf{DPWTamper}_m^{f,g} = \left\{ \begin{array}{c} (X,Y) \leftarrow \mathsf{Enc}(m), \\ X' := f(X), Y' := g(Y) \\ m' := \mathsf{Dec}(X', Y') \\ \textit{output: } m' \end{array} \right\}$$

We say that an encoding scheme $(\mathsf{Enc}, \mathsf{Dec})$ *is* ε-DPW-non-malleable in split-state model *if for every functions* $f, g : \mathcal{X} \to \mathcal{X}$ *there exists distribution* $D^{f,g}$ *on* $\mathcal{M} \cup \{\mathsf{same}, \perp\}$ *such that for every* $m \in \mathcal{M}$ *we have*

$$\mathsf{DPWTamper}_m^{f,g} \approx_\varepsilon \left\{ \begin{array}{c} d \leftarrow D^{f,g} \\ \textit{if } d = \mathsf{same} \textit{ then output } m \\ \textit{otherwise output } d. \end{array} \right\}$$

We will consider the following alternative definition of non-malleable code, which will be a smoother transition to the subsequent definitions in this section. We show the equivalence of this definition to Definition 1 in Appendix A.

Definition 2. (Non-Malleable Code.) *We say that an encoding scheme* $(\mathsf{Enc} : \mathcal{M} \to \mathcal{X} \times \mathcal{X}, \mathsf{Dec} : \mathcal{X} \times \mathcal{X} \to \mathcal{M} \cup \{\perp\})$ *is* ε-non-malleable in split-state model *if for every functions* $f, g : \mathcal{X} \to \mathcal{X}$ *there exists family of distributions* $\{D^{f,g}_{x,y}\}_{x,y \in \mathcal{X}}$ *each on* $\{0,1\}$ *such that for every* $m_0, m_1 \in \mathcal{M}$

$$\mathsf{Tamper}^{f,g}_{m_0} \approx_\varepsilon \mathsf{Tamper}^{f,g}_{m_1}$$

where

$$\mathsf{Tamper}^{f,g}_{m} = \left\{ \begin{array}{c} (X,Y) \leftarrow \mathsf{Enc}(m), \\ \textit{output } \textbf{same} \textit{ if } \mathsf{Dec}(X,Y) = \mathsf{Dec}(f(X), g(Y)) \wedge D^{f,g}_{X,Y} = 0 \\ \textit{else output: } \mathsf{Dec}(f(X), g(Y)) \end{array} \right\}$$

Some results in the literature like [FMNV14, JW15] have considered a notion of super-strong non-malleable codes. We introduce the following intermediate notion of super non-malleable codes.

Definition 3. (Super Non-Malleable Code.) *We say that an encoding scheme* $(\mathsf{Enc} : \mathcal{M} \to \mathcal{X} \times \mathcal{X}, \mathsf{Dec} : \mathcal{X} \times \mathcal{X} \to \mathcal{M} \cup \{\perp\})$ *is* ε-super non-malleable in split-state model *if for every functions* $f, g : \mathcal{X} \to \mathcal{X}$ *there exists family of distributions* $\{D^{f,g}_{x,y}\}_{x,y \in \mathcal{X}}$ *each on* $\{0,1\}$ *such that for every* $m_0, m_1 \in \mathcal{M}$

$$\mathsf{SuperTamper}^{f,g}_{m_0} \approx_\varepsilon \mathsf{SuperTamper}^{f,g}_{m_1}$$

where $\mathsf{SuperTamper}^{f,g}_{m} =$

$$\left\{ \begin{array}{c} (X,Y) \leftarrow \mathsf{Enc}(m), \\ \textit{output } \textbf{same} \textit{ if } \mathsf{Dec}(X,Y) = \mathsf{Dec}(f(X), g(Y)) \wedge D^{f,g}_{X,Y} = 0 \\ \textit{else if } \mathsf{Dec}(f(X), g(Y)) = \perp \textit{ output } \perp \\ \textit{else output: } (f(X), g(Y)) \end{array} \right\}$$

Definition 4. (Super Strong Non-Malleable Code.) *We say that an encoding scheme* $(\mathsf{Enc} : \mathcal{M} \to \mathcal{X} \times \mathcal{X}, \mathsf{Dec} : \mathcal{X} \times \mathcal{X} \to \mathcal{M} \cup \{\perp\})$ *is* ε-super strong non-malleable in split-state model *if for every functions* $f, g : \mathcal{X} \to \mathcal{X}$ *and for every* $m_0, m_1 \in \mathcal{M}$

$$\mathsf{SuperStrongTamper}^{f,g}_{m_0} \approx_\varepsilon \mathsf{SuperStrongTamper}^{f,g}_{m_1}$$

where

$$\mathsf{SuperStrongTamper}^{f,g}_{m} = \left\{ \begin{array}{c} (X,Y) \leftarrow \mathsf{Enc}(m), \\ \textit{output } \textbf{same} \textit{ if } (X,Y) = (f(X), g(Y)) \\ \textit{else if } \mathsf{Dec}(f(X), g(Y)) = \perp \textit{ output } \perp \\ \textit{else output: } (f(X), g(Y)) \end{array} \right\}$$

Definition 5. (Continuous Non-Malleable Code.) *[JW15] define four types of continuous non-malleable codes based on two flags:* $\mathsf{sd} \in \{0,1\}$ (self-destruct) *and* $\mathsf{prs} \in \{0,1\}$ (persistent). *We say that an encoding scheme* $(\mathsf{Enc} : \mathcal{M} \to \mathcal{X} \times \mathcal{X}, \mathsf{Dec} : \mathcal{X} \times \mathcal{X} \to \mathcal{M} \cup \{\perp\})$ *is* $(\mathsf{T}, \varepsilon)$-continuous $[\mathsf{sd}, \mathsf{prs}]$ non-malleable in split-state model *if for every Adversary* $\mathcal{A}$ *and for every* $m_0, m_1 \in \mathcal{M}$

$$\mathsf{ConTamper}_{\mathcal{A},\mathsf{T},m_0} \approx_\varepsilon \mathsf{ConTamper}_{\mathcal{A},\mathsf{T},m_1}$$

where $\mathsf{ConTamper}_{\mathcal{A},\mathsf{T},m} =$

$$\left\{\begin{array}{l} (X,Y) \leftarrow \mathsf{Enc}(m), \\ f_0, g_0 \equiv \mathsf{id}, \\ \textbf{Repeat} \quad i = 1,2,...,\mathsf{T} \\ \quad \mathcal{A} \textit{ chooses functions } f_i', g_i' \\ \quad \textbf{if } \mathsf{prs} = 1 \textbf{ then } f_i = f_i' \circ f_{i-1},\ g_i = g_i' \circ g_{i-1} \\ \quad\quad \textbf{else } f_i = f_i',\ g_i = g_i' \\ \quad \textbf{if } (f_i(X), g_i(Y)) = (X,Y) \textbf{ then output same} \\ \quad\quad \textbf{else} \\ \quad\quad \textbf{if } \mathsf{Dec}(f_i(X), g_i(Y)) = \perp \textbf{ then output } \perp \textbf{ if } \mathsf{sd} = 1 \textbf{ then experiment stops} \\ \quad\quad\quad \textbf{else output } (f_i(X), g_i(Y)) \textbf{ if } \mathsf{prs} = 1 \textbf{ then experiment stops} \end{array}\right\}$$

Remark 1. [FMNV14] show that non-persistent continuous non-malleable codes are impossible to construct in 2-split state model.

Remark 2. In any model allowing bitwise tampering, in particular in 2−split state model, *non-self-destruct* property is impossible to archive if space of messages has at least 3 elements.

Proof. Let $c = (c_1, c_2, c_3, ...)$ be codeword, we apply function $c \to (0, c_2, c_3, ...)$
- if tampering experiment returned $\perp$ then we learned that $c_1 = 1$
- if tampering experiment returned **same** then we learned that $c_1 = 0$
- if tampering experiment returned something else we can repeat the experiment for $(1, c_2, c_3, ...)$ and limit space of possible messages that were encoded to 2 thus breaking the security immediately.

we can repeat the process with other coordinates and in the end learn either whole codeword or limit space to 2 possibilities.

4 Inception Coding Technique

4.1 Check Functions

Definition 6. *A function* $C : \{0,1\}^s \times \{0,1\}^n \to \{0,1\}^m$ *is called an* ε-check *if for any* $f : \{0,1\}^n \to \{0,1\}^n$ *and any* x *such that* $x \neq f(x)$,

$$\Pr_{S \leftarrow \{0,1\}^s}(C(S,x) = C(S, f(x))) \leq \varepsilon$$

In this section we will define several check functions. However, first we start with definition of auxiliary functions Check_1 and $\mathsf{Check}_{2,\varepsilon}$.

Definition 7. *Let* $0 < B < 1$ *and let function* $\mathsf{Check}_1 : \{0,1\}^n \to \{0,1\}^{n^B \lceil \log n \rceil}$ *be such that* $X||\mathsf{Check}_1(X)$ *is a valid codeword for RS (Correctness of this definition follows from Lemma 2).*

Definition 8. *Let* $t = 2n^{1-B}\lceil \log(1/\varepsilon) \rceil$*, and let* $\mathsf{Check}_2 : \{0,1\}^{t\lceil \log(n) \rceil} \times \{0,1\}^n \to \{0,1\}^t$ *be a simple sampler function defined as follows. Let* $s = s_1 \| s_2 \| \cdots \| s_t$ *be such that each* s_j *is a bit-string of length* $\lceil \log(n) \rceil$*. Then* $\mathsf{Check}_2(s, x) := x_{s_1} \dots x_{s_t}$*, where* x_{s_j} *is the bit of* x *at position* s_j*, when written in binary form.*

Lemma 3. *Let* $t = 2n^{1-B}\lceil \log(1/\varepsilon) \rceil$ *and let*

$$\mathsf{Check} : \{0,1\}^{t\lceil \log(n) \rceil} \times \{0,1\}^n \to \{0,1\}^{n^B \log n + t}$$

be defined as $\mathsf{Check}(s, x) = \mathsf{Check}_1(x)||\mathsf{Check}_2(s, x)$*. Then* Check *is a* 2ε*-check.*

Proof. If $\mathsf{Ham}(x; f(x)) < n^B$ then by Lemma 2, $\mathsf{Check}_1(x) \neq \mathsf{Check}_1(f(x))$. So, without loss of generality, we assume that $\mathsf{Ham}(x; f(x)) \geq n^B$. For $t = 2n^{1-B}\lceil \log(1/\varepsilon) \rceil$ and a uniformly random $S = S_1 \| \cdots \| S_t$, $\mathsf{Check}_2(S, x) \neq \mathsf{Check}_2(S, f(x))$ if and only if $x_{S_j} = f(x)_{S_j}$ for all $j \in [t]$. Thus,

$$\begin{aligned}\Pr_{S \leftarrow \{0,1\}^s}(\mathsf{Check}_2(S, x) = \mathsf{Check}_2(S, f(x))) &\leq \left(1 - \frac{n^B}{2^{\lceil \log n \rceil}}\right)^{2n^{1-B}\lceil \log(1/\varepsilon) \rceil} \\ &\leq \left(1 - \frac{1}{2n^{1-B}}\right)^{n^{1-B}\lceil \log(1/\varepsilon) \rceil} \leq \left(\frac{1}{2}\right)^{\lceil \log(1/\varepsilon) \rceil} \leq \varepsilon.\end{aligned}$$

□

For our construction, we would require a check of length n^c for a small constant $c > 0$. In the following, we show how to compose check functions to decrease their size.

Lemma 4. *If* $ch^1 : \{0,1\}^{s_1} \times \{0,1\}^n \mapsto \{0,1\}^{m_1}$ *is an* ε_1*-check and* $ch^2 : \{0,1\}^{s_2} \times \{0,1\}^{m_1} \mapsto \{0,1\}^{m_2}$ *is an* ε_2*-check then* $ch : \{0,1\}^{s_1+s_2} \times \{0,1\}^n \mapsto \{0,1\}^{m_2}$ *given by*

$$ch(x, s_1 \| s_2) := ch^2(ch^1(x, s_1), s_2)$$

is an $(\varepsilon_1 + \varepsilon_2)$*-check function.*

Proof. Let $S_1 \| S_2 \leftarrow U_{s_1+s_2}$, and let $E_1 = E_1(x, S_1)$ be the event that $ch^1(x, S_1) = ch^1(f(x), S_1)$ and $E_2 = E_2(x, S_1, S_2)$ be the event that $ch^2(ch^1(x, S_1), S_2) = ch^2(ch^1(f(x), S_1), S_2)$. Then

$$\begin{aligned}\Pr(E_2) &\leq \Pr(E_1) + \Pr(E_2 \mid \overline{E_1}) \\ &\leq \varepsilon_1 + \varepsilon_2 \ .\end{aligned}$$

□

Lemma 5. *Let E be such that $\lceil \log(1/\varepsilon) \rceil = n^{E/2}$. Then there exist a $\frac{2\log E}{\log(1-E/2)}\varepsilon$-check $\mathsf{Check}^\star : \{0,1\}^s \times \{0,1\}^n \mapsto \{0,1\}^m$ such that:*

$$m \leq n^E,$$
$$s \leq \frac{\log E}{\log(1-E/2)} n^{3E/2} \lceil \log n \rceil .$$

Proof. We will apply Lemma 4 several times to our Check in Lemma 3 to construct a different check function with parameters more convenient for our application. In Lemma 3 we already defined an 2ε-check for n-bit strings

$$\text{Seed length} = n^{1-B}\lceil \log n \rceil \lceil \log(1/\varepsilon) \rceil,$$
$$\text{Length of check} = n^B \lceil \log n \rceil + n^{1-B} \lceil \log(1/\varepsilon) \rceil,$$

where $1/2 < B < 1$. For our final choice of parameters, B will be a constant close to 1.
Now, we use $(t-1)$ times lemma 4 to compose Check with itself (of course each time n is smaller; however we keep 2ε and B the same each time).and get the following $2t\varepsilon$-check $\mathsf{Check}^\star$:

$$\text{Length of check} \leq n^{(B+\delta)^t},$$
$$\text{Seed length} \leq t n^{1-B} \lceil \log n \rceil \lceil \log(1/\varepsilon) \rceil .$$

where δ is such that $(n')^B \lceil \log n' \rceil + (n')^{1-B} \lceil \log(1/\varepsilon) \rceil \leq (n')^{B+\delta}$ for $n' = n^{(B+\delta)^t}$.
Now, let us put $B = 1-E$, $\delta = E/2$ and $t = \frac{\log E}{\log(1-E/2)}$ to the above and we get (this just re-notation not a different function) a $\frac{2\log E}{\log(1-E/2)}\varepsilon$-check $\mathsf{Check}^\star$ with the following properties:

$$\text{Length of check} \leq n^E,$$
$$\text{Seed length} \leq \frac{\log E}{\log(1-E/2)} n^E \lceil \log n \rceil \lceil \log(1/\varepsilon) \rceil .$$

if $\lceil \log(1/\varepsilon) \rceil < n^{E-3E^2/2}$.
This final statement is obtained by putting $\lceil \log(1/\varepsilon) \rceil = n^{E/2} < n^{E-3E^2/2}$. □

Definition 9. *For clarity let us define functions $\mathsf{s}, \mathsf{c}, \varepsilon$ as follows:*

$$\mathsf{s}(n,E) = \frac{\log E}{\log(1-E/2)} n^{3E/2} \lceil \log n \rceil$$
$$\mathsf{c}(n,E) = n^E$$
$$\varepsilon(n,E) = \frac{2\log E}{\log(1-E/2)} 2^{-n^{E/2}}$$

Remark 3. It is important to notice that for any $s \in \{0,1\}^{\mathsf{s}(n,E)}$ and any $r \in \{0,1\}^{\mathsf{c}(n,E)}$ set $A_{s,r} = \{X \in \{0,1\}^n \mid \mathsf{Check}^\star(s,X) = r\}$ is an affine subspace of $\{0,1\}^n$. This follows from Lemma 2 and definition of $\mathsf{Check}_{2,\varepsilon}$.

4.2 Inception Coding

Let $\mathsf{Enc} : \{0,1\}^k \to \{0,1\}^n \times \{0,1\}^n, \mathsf{Dec} : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^k \cap \{\perp\}$ be ε'-super non-malleable scheme in 2-split state model, and for any message m and any affine subspaces $A_{s_x,r_x}, A_{s_y,r_y} \subset \{0,1\}^n$ of large dimensions[5] it is possible to efficiently sample from set $\{(X,Y) \in (A_{s_x,r_x} \times A_{s_y,r_y}) \,|\, \mathsf{Dec}(X,Y) = m\}$.
We will give a coding scheme that is super-strong non-malleable.

Definition 10. *The* Inception *version of above-mentioned scheme* $(\mathsf{Enc}, \mathsf{Dec})$ *is defined as follows. We first define the decoding function* $\mathcal{I}\mathsf{Dec} : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^{k-2(\mathsf{s}(n,E)+\mathsf{c}(n,E))} \cup \{\perp\})$. *For any* $x, y \in \{0,1\}^n$,

- $\mathsf{Dec}(x,y) = (m, s_x, r_x, s_y, r_y)$, *where* $s_x, s_y \in \{0,1\}^{\mathsf{s}(n,E)}$ *and* $r_x, r_y \in \{0,1\}^{\mathsf{c}(n,E)}$
- *If* $\mathsf{Check}^\star(s_x, x) = r_x$ *and* $\mathsf{Check}^\star(s_y, y) = r_y$ *then* $\mathcal{I}\mathsf{Dec}(x,y) = m$ *else* $\mathcal{I}\mathsf{Dec}(x,y) = \perp$.

The encoding function $\mathcal{I}\mathsf{Enc} : \{0,1\}^{m-2(\mathsf{s}(n,E)+\mathsf{c}(n,E))} \to \{0,1\}^n \times \{0,1\}^n$ *is defined as follows. For any* $m \in \{0,1\}^{k-2\mathsf{s}(n,E)-2\mathsf{c}(n,E)}$,

- *Choose uniformly at random* s_x, s_y *from* $\{0,1\}^{\mathsf{s}(n,E)}$, *and* r_x, r_y *from* $\{0,1\}^{\mathsf{c}(n,E)}$.
- *Sample* (X,Y) *from set* $\{(x,y) \in (A_{s_x,r_x} \times A_{s_y,r_y}) \,|\, \mathcal{I}\mathsf{Dec}(x,y) = m\}$,
- $\mathcal{I}\mathsf{Enc}(m) = (X,Y)$.

We will need the following lemma.

Lemma 6 ([ADKO15b, Lemma 6.1]). *Let* $\mathsf{Dec} : \mathcal{X} \times \mathcal{X} \to \mathcal{M}$, *and* $\mathsf{Enc} : \mathcal{M} \to \mathcal{X} \times \mathcal{X}$ *be* $\varepsilon-$*non-malleable scheme in* $2-$*split state model for some* $\varepsilon < \frac{1}{2}$. *For any pair of messages* $m_0, m_1 \in \mathcal{M}$, *let* $(X_1^0, X_2^0) \leftarrow \mathsf{Enc}(m_0)$, *and let* $(X_1^1, X_2^1) \leftarrow \mathsf{Enc}(m_1)$. *Then* $\Delta(X_1^0\,;\, X_1^1) \le 2\varepsilon$.

Lemma 7. *Let* $k \ge 3$, *and let* $\varepsilon < 1/20$. *If* $(\mathsf{Enc}, \mathsf{Dec})$ *is* ε*-non-malleable scheme then for every sets* $A, B \subset \{0,1\}^n$ *and every messages* $m_0, m_1 \in \{0,1\}^k$

$$|\Pr(\mathsf{Enc}(m_0) \in A \times B) - \Pr(\mathsf{Enc}(m_1) \in A \times B)| \le \varepsilon$$

Proof. We claim that there exist $x, y, z, w \in \{0,1\}^n$ such that $m_0, m_1, \mathsf{Dec}(x,w)$, $\mathsf{Dec}(z,w)$, and $\mathsf{Dec}(z,y)$ are all different from $\mathsf{Dec}(x,y)$. Before proving this claim, we show why this implies the given result. Consider the tampering functions f, g such that $f(c) = x$ if $c \in A$, and $f(c) = z$, otherwise, and $g(c) = y$ if $c \in B$, and $g(c) = w$, otherwise. Thus, for $b = 0, 1$, $\mathsf{Tamper}_{m_b}^{f,g} = \mathsf{Dec}(x,y)$ if and only if $\mathsf{Enc}(m_b) \in A \times B$. The result then follows from the ε-non-malleability of $(\mathsf{Enc}, \mathsf{Dec})$.
Now, to prove the claim, we will use the probabilistic method. Let U be uniform in $\{0,1\}^k$, and let $X, Y \leftarrow \mathsf{Enc}(U)$. Furthermore, let $W, Z \in \{0,1\}^n$ be uniform and independent of X, Y, U. We claim that X, Y, Z, W satisfy the required property with non-zero probability.
It is easy to see that the probability that $\mathsf{Dec}(X,Y) = U$ is either of m_0 or m_1 is at most $2/2^k$. Also, by Lemma 6, we have that except with probability 2ε, X is independent of U. Also, W is independent of U. Thus,

[5] $\dim(A_{s_x,r_x}) = \dim(A_{s_y,r_y}) = n - (\mathsf{c}(n,E) + \mathsf{s}(n,E))$

the probability that $\mathsf{Dec}(X, W) = U$ is at most $2\varepsilon + 1/2^k$. Similarly, the probability that $\mathsf{Dec}(Z, Y) = U$ is at most $2\varepsilon + 1/2^k$. Finally, W, Z are independent of U, and so the probability that $\mathsf{Dec}(Z, W) = U$ is at most $\frac{1}{2^k}$.
Thus, by union bound, the probability that X, Y, Z, W do not satisfy the condition of the claim is at most $\frac{5}{2^k} + 4\varepsilon \leq \frac{5}{8} + 4\varepsilon < 1$. □

Lemma 8. *Let* $(\mathsf{Enc}, \mathsf{Dec})$ *be an* ε*-non-malleable code. For any* $m \in \{0,1\}^{k-2(\mathsf{c}(n,E)+\mathsf{s}(n,E))}$ *and* $s_x, s_y \leftarrow \{0,1\}^{\mathsf{s}(n,E)}, r_x, r_y \leftarrow \{0,1\}^{\mathsf{c}(n,E)}$,

$$\Pr(\mathsf{Enc}(m, s_x, r_x, s_y, r_y) \in A_{s_x,r_x} \times A_{s_y,r_y}) > 2^{-2\mathsf{c}(n,E)} - \varepsilon$$

Proof. By Lemma 7, we have that

$$|\Pr(\mathsf{Enc}(0^k) \in A_{s_x,r_x} \times A_{s_y,r_y}) - \Pr(\mathsf{Enc}(m, s_x, r_x, s_y, r_y) \in A_{s_x,r_x} \times A_{s_y,r_y})|$$

is at most ε. So, we will bound the probability that $\Pr(\mathsf{Enc}(0^k) \in A_{s_x,r_x} \times A_{s_y,r_y})$. Fix $\mathsf{Enc}(0^k) = (X, Y)$, and s_x, s_y. Now, $(X, Y) \in A_{s_x,r_x} \times A_{s_y,r_y}$ if and only if $r_x = \mathsf{Check}^\star(s_x, X)$, and $r_y = \mathsf{Check}^\star(s_y, Y)$ which happens with probability $2^{-2\mathsf{c}(n,E)}$. □

In order to prove the super non-malleability property, we introduce the following intermediate notion.

Definition 11. (Inception Super Non-Malleable Code.) *Let* $(\mathsf{Enc} : \{0,1\}^k \to \{0,1\}^n \times \{0,1\}^n, \mathsf{Dec} : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^k \cup \{\perp\})$ *be a coding scheme. We say that* $(\mathsf{Enc}, \mathsf{Dec})$ *is* ε*-inception super non-malleable in split-state model if for every functions* $f, g : \mathcal{X} \to \mathcal{X}$ *there exists family of distributions* $\{D^{f,g}_{x,y}\}_{x,y \in \{0,1\}^n}$ *each on* $\{0,1\}$ *such that for every* $m_0, m_1 \in \{0,1\}^{k-(\mathsf{c}(n,E)+\mathsf{s}(n,E))}$

$$\mathsf{IncSuperTamper}^{f,g}_{m_0} \approx_\varepsilon \mathsf{IncSuperTamper}^{f,g}_{m_1}$$

where $\mathsf{IncSuperTamper}^{f,g}_m =$

$$\left\{ \begin{array}{c} s_x, s_y \leftarrow \{0,1\}^{\mathsf{s}(n,E)}\ ,\ r_x, r_y \leftarrow \{0,1\}^{\mathsf{c}(n,E)} \\ \mathsf{Enc}(m, s_x, r_x, s_y, r_y) \to (X, Y),\ \textit{s.t. } \mathsf{Check}^\star(s_x, X) = r_x \textit{ and } \mathsf{Check}^\star(s_y, Y) = r_y \\ \textit{if } \mathsf{Dec}(f(X), g(Y)) = \perp \textit{ output } \perp \\ \textit{output } \textbf{same} \textit{ if } \mathsf{Dec}(X, Y) = \mathsf{Dec}(f(X), g(Y)) \wedge D^{f,g}_{X,Y} = 0 \\ \textit{else output: } (f(X), g(Y)) \end{array} \right\}$$

Lemma 9. *If* $(\mathsf{Enc}, \mathsf{Dec})$ *is* ε*-super non-malleable scheme then* $(\mathsf{Enc}, \mathsf{Dec})$ *is* ε'*-inception super non-malleable scheme, where* $\varepsilon' = \frac{6\varepsilon + 2^{-2\mathsf{s}(n,E)-2\mathsf{c}(n,E)}}{2^{-2\mathsf{c}(n,E)} - \varepsilon}$.

Proof. Let $f : \{0,1\}^n \mapsto \{0,1\}^n$, $g : \{0,1\}^n \mapsto \{0,1\}^n$ be arbitrary functions. We choose s_x, s_y uniformly at random from $\{0,1\}^{\mathsf{s}(n,E)}$, and r_x, r_y uniformly at random from $\{0,1\}^{\mathsf{c}(n,E)}$. Define

$$f'(x) = \begin{cases} f(x) \text{ if } x \in A_{s_x,r_x} \\ 0^n, \text{ otherwise.} \end{cases}$$

$$g'(y) = \begin{cases} g(y) \text{ if } y \in A_{s_y,r_y} \\ 0^n \text{ otherwise.} \end{cases}$$

Let $m \in \{0,1\}^{k-2\mathsf{s}(n,E)-2\mathsf{c}(n,E)}$ be any message. Let $(X_b, Y_b) \leftarrow \mathsf{Enc}(m_b, s_x, r_x, s_y, r_y)$ for $b = \{0,1\}$. For $b = \{0,1\}$, we shorthand $\mathsf{SuperTamper}^{f',g'}_{(m_b,s_x,r_x,s_y,r_y)}$ by T_b and the range of T_b be $\mathcal{R} = \{0,1\}^n \times \{0,1\}^n \cup \perp, \mathsf{same}$. Also, let $\mathcal{A} = A_{s_x,r_x} \times A_{s_y,r_y}$, and let $\Pr((X_b, Y_b) \in \mathcal{A}) = p_b$. By Lemma 7, we have that $|p_0 - p_1| \leq \varepsilon$, and by Lemma 8, we have that $p_0 \geq 2^{-2\mathsf{c}(n,E)} - \varepsilon$. Also, note that conditioned on the event that $X_b, Y_b \notin \mathcal{A}$, then $(f(X_b), g(Y_b))$ depends on at most one of X_b, Y_b, and hence by Lemma 6, it is independent of m_b, s_x, r_x, s_y, r_y, except with probability at most 2ε. Thus, for T_b to output same, the functions f, g must be such that they should be able to guess s_x, s_y, r_x, r_y, which happens with probability at most $2^{-2\mathsf{s}(n,E)-2\mathsf{c}(n,E)}$. Therefore, the statistical distance between T_0 and T_1 conditioned on the event that $X_b, Y_b \notin \mathcal{A}$ is at most $2\varepsilon + 2^{-2\mathsf{s}(n,E)-2\mathsf{c}(n,E)}$. T_b is independent of m_b except with probability at most 2ε. Also, by the super non-malleability assumption, we have that $\Delta(T_0; T_1) \leq \varepsilon$. Thus, we have that

$$
\begin{aligned}
2\varepsilon &\geq \sum_{z \in \mathcal{R}} |\Pr(T_0 = z) - \Pr(T_1 = z)| \\
&\geq \sum_{z \in \mathcal{R}} \Big| \Pr(T_0 = z | (X_0, Y_0) \in \mathcal{A}) \cdot p_0 + \Pr(T_0 = z | (X_0, Y_0) \notin \mathcal{A}) \cdot (1 - p_0) \\
&\quad - \Pr(T_1 = z | (X_1, Y_1) \in \mathcal{A}) \cdot p_1 - \Pr(T_1 = z | (X_1, Y_1) \notin \mathcal{A}) \cdot (1 - p_1) \Big| \\
&\geq p_0 \cdot \sum_{z \in \mathcal{R}} |\Pr(T_0 = z | (X_0, Y_0) \in \mathcal{A}) - \Pr(T_1 = z | (X_1, Y_1) \in \mathcal{A})| - \\
&\quad \sum_{z \in \mathcal{R}} |\Pr(T_0 = z | (X_0, Y_0) \notin \mathcal{A}) - \Pr(T_1 = z | (X_1, Y_1) \notin \mathcal{A})| - 2|p_0 - p_1| \\
&\geq p_0 \cdot \sum_{z \in \mathcal{R}} |\Pr(T_0 = z | (X_0, Y_0) \in \mathcal{A}) - \Pr(T_1 = z | (X_1, Y_1) \in \mathcal{A})| \\
&\quad - 2\varepsilon - 2^{-2\mathsf{s}(n,E)-2\mathsf{c}(n,E)} - 2\varepsilon \,.
\end{aligned}
$$

This implies that

$$
\sum_{z \in \mathcal{R}} |\Pr(T_0 = z | (X_0, Y_0) \in \mathcal{A}) - \Pr(T_1 = z | (X_1, Y_1) \in \mathcal{A})|
$$

is at most $\frac{6\varepsilon + 2^{-2\mathsf{s}(n,E)-2\mathsf{c}(n,E)}}{2^{-2\mathsf{c}(n,E)} - \varepsilon}$. Looking at the definition of inception super non-malleable scheme, we get that this implies the desired result. □

Theorem 2. *If* $(\mathsf{Enc}, \mathsf{Dec})$ *is* ε*−super non-malleable scheme then* $(\mathcal{I}\mathsf{Enc}, \mathcal{I}\mathsf{Dec})$ *is* $O(\varepsilon(n,E) + \varepsilon' + \varepsilon)$*-super strong non-malleable code, where*

$$
\varepsilon' = \frac{6\varepsilon + 2^{-2\mathsf{s}(n,E)-2\mathsf{c}(n,E)}}{2^{-2\mathsf{c}(n,E)} - \varepsilon} \,.
$$

Proof. Consider any tampering functions f, g, and any message m. In order to show the desired result, we compare $\mathsf{IncSuperTamper}^{f,g}_m$ and $\mathsf{SuperStrongTamper}^{f,g}_m$ experiments.
If $\mathsf{IncSuperTamper}^{f,g}_m = \perp$, then clearly $\mathsf{SuperStrongTamper}^{f,g}_m = \perp$.

If $\mathsf{IncSuperTamper}_m^{f,g} = \mathsf{same}$, then we claim that except with probability at most $\varepsilon(n, E)$, $\mathsf{SuperStrongTamper}_m^{f,g}$ is either $\perp$ or same. To see this, note that if $\mathsf{IncSuperTamper}_m^{f,g} = \mathsf{same}$ and $\mathsf{SuperStrongTamper}_m^{f,g} \neq \mathsf{same}$ then $\mathsf{Dec}(f(X), g(Y)) = \mathsf{Dec}(X, Y) = (m, s_x, r_x, s_y, r_y)$, and $f(X) \neq X$ or $g(Y) \neq Y$. By Lemma 5, this happens with probability at most $\varepsilon(n, E)$.
If $\mathsf{IncSuperTamper}_m^{f,g}$ is neither $\perp$, nor same, then it is the entire tampered codeword, $f(X), g(Y)$, and so conditioned on this event, $\mathsf{SuperStrongTamper}_m^{f,g}$ is either same, or a deterministic function of $\mathsf{IncSuperTamper}_m^{f,g}$. However, the event that $\mathsf{SuperStrongTamper}_m^{f,g} = \mathsf{same}$ and $\mathsf{IncSuperTamper}_m^{f,g} \neq \mathsf{same}$ implies that $f(X) = X, g(Y) = Y$ and $D_{X,Y}^{f,g} = 1$. This event implies that $\mathsf{IncSuperTamper}_m^{f,g} = (X, Y)$, which can happen with probability at most ε' by Lemma 9.
So, it is sufficient to show that $|\Pr(\mathsf{SuperStrongTamper}_{m_0}^{f,g} = \mathsf{same}) - \Pr(\mathsf{SuperStrongTamper}_{m_1}^{f,g} = \mathsf{same})| \leq \varepsilon$. This follows by Lemma 7 by setting $A = \{x \in \{0,1\}^n : f(x) = x\}$, and $B = \{y \in \{0,1\}^n : g(y) = y\}$. □

5 Super Strong NMC implies Continuous NMC

In this section we will prove the following statement:

Theorem 3. *If* $(\mathsf{Enc}, \mathsf{Dec})$ *is* ε*-Super Strong Non-Malleable Scheme then* $(\mathsf{Enc}, \mathsf{Dec})$ *is a* $(T, (T+1)\varepsilon)-$*Continuous* $[1, 1]$ *Non-Malleable Code.*

Before the actual proof let us fix some notation. Let $\mathcal{A}^*$ be any adversary described in definition 5. Let $(I)_m$ denote the index of a round when ***same*** is not output in the experiment $\mathsf{ConTamper}_{\mathcal{A}^*,\mathsf{T},m}$ and (f_i, g_i) (for $i = 1, \ldots, T$) denote pairs of functions chosen by $\mathcal{A}^*$ (of course we can assume that they are always the same because the choice for the next round does not depend on (X, Y)).
For the main proof, we will need the following lemma:

Lemma 10. $(I)_{m_0} \approx_{T\varepsilon} (I)_{m_1}$.

Proof. Let $0 \leq i \leq T$ be any integer and let:

$$A_1^i = \{X \subset \{0,1\}^n | f_j(X) = X, \text{ for } j < i \text{ and } f_i(X) \neq X\},$$
$$B_1^i = \{Y \subset \{0,1\}^n | g_j(Y) = Y, \text{ for } j < i\},$$
$$A_2^i = \{X \subset \{0,1\}^n | f_j(X) = X, \text{ for } j \leq i\},$$
$$B_2^i = \{Y \subset \{0,1\}^n | g_j(Y) = Y, \text{ for } j < i \text{ and } g_i(Y) \neq Y\}.$$

From the definition of the stop condition for the considered experiment we obviously have that:

$$(I)_m = i \iff \mathsf{Enc}(m) \subset A_1^i \times B_1^i \text{ or } \mathsf{Enc}(m) \subset A_2^i \times B_2^i.$$

It also holds $A_1^i \times B_1^i \cap A_2^i \times B_2^i = \emptyset$, so — from Lemma 7 (used twice: for $A_1^i \times B_1^i$ and for $A_2^i \times B_2^i$) — we have

$$|\Pr(I = i)_{m_0} - \Pr(I = i)_{m_1}| \leq 2\varepsilon,$$

which gives us $(I)_{m_0} \approx_{T\varepsilon} (I)_{m_1}$ as needed. □

Now, since $(\mathsf{Enc}, \mathsf{Dec})$ is ε-Super Strong Non-Malleable Scheme then $(f_i, g_i)_{m_0} \approx_\varepsilon (f_i, g_i)_{m_1}$ for all $i = 1, \ldots, T$. From lemma 10 we also have that $(I)_{m_0} \approx_{T\varepsilon} (I)_{m_1}$, so:

$$(I, f_I(X), g_I(Y))_{m_0} \approx_{T\varepsilon+\varepsilon} (I, f_I(X), g_I(Y))_{m_1},$$

which implies that $(\mathsf{Enc}, \mathsf{Dec})$ is a $(T, (T+1)\varepsilon)$-persistent Continuous Non-Malleable Code with self-destruct.

Remark 4. The above reduction is in the split-state model. It may be interesting to note that the only place that we use a particular property of this model is Lemma 10. It is also obvious that if this lemma does not hold for some model then the reduction will not hold. That means that Lemma 10 describes in some sense a necessary and sufficient property of a tampering model in which the main reduction of this section is true.

6 Instantiating a Super NMC using known results

In [ADL14], Aggarwal et al. gave a construction of non-malleable codes in the split-state model. Here, we argue that the construction of [ADL14] is also super-non-malleable.
Note that for any message m with $\mathsf{Enc}(m) = (X, Y)$, and any functions f, g, the output of the tampering experiment in Definition 2 is the same as that in Definition 3 if $\mathsf{Dec}(f(X), g(Y)) = m$ or $\mathsf{Dec}(f(X), g(Y)) = \perp$. This leads to the following simple observation.

Observation 6.1 *Let $\varepsilon, \varepsilon' > 0$. Let $(\mathsf{Enc} : \mathcal{M} \to \mathcal{X} \times \mathcal{X}, \mathsf{Dec} : \mathcal{X} \times \mathcal{X} \to \mathcal{M} \cup \{\perp\})$ be an ε-non-malleable code in the split-state model. Given $f, g : \mathcal{X} \mapsto \mathcal{X}$, assume there exists a partitioning $(\mathcal{S}_1, \cdots, \mathcal{S}_{s+t}, \mathcal{S}^\star)$ of $\mathcal{X} \times \mathcal{X}$ such that the following hold:*

1. *For all $m \in \mathcal{M}$, $1 \leq i \leq s$, $\Pr_{(X,Y) \leftarrow \mathsf{Enc}(m)}(\mathsf{Dec}(f(X), g(Y)) \in \{m, \perp\} | (X, Y) \in \mathcal{S}_i) \geq 1 - \varepsilon'$.*
2. *For all $m_1, m_2 \in \mathcal{M}$, $s+1 \leq i \leq t$, let (X_1, Y_1), (X_2, Y_2) be the encoding of m_1, m_2 respectively, conditioned on the fact that $(X_1, Y_1), (X_2, Y_2) \in \mathcal{S}_i$. Then $\Delta((f(X_1), g(Y_1)), (f(X_2), g(Y_2)) \leq \varepsilon'$.*
3. *For any $m \in \mathcal{M}$, $\Pr(\mathsf{Enc}(m) \in \mathcal{S}^\star) \leq \varepsilon'$.*

Then, the scheme $(\mathsf{Enc}, \mathsf{Dec})$ is $(\varepsilon + O(\varepsilon'))$-super-non-malleable.

In the above observation, we set $D^{f,g}_{(X,Y)}$ to be 1 if $(X, Y) \in \mathcal{S}_1, \ldots, \mathcal{S}_s$, and 0, otherwise.
Before describing the encoding scheme from [ADL14], we will need the following definition of an affine-evasive function.

Definition 12. *Let $\mathbb{F} = \mathbb{F}_p$ be a finite field. A surjective function $h : \mathbb{F} \mapsto \mathcal{M} \cup \{\perp\}$ is called* (γ, δ)-affine-evasive *if or any $a, b \in \mathbb{F}$ such that $a \neq 0$, and $(a, b) \neq (1, 0)$, and for any $m \in \mathcal{M}$,*

1. *$\Pr_{U \leftarrow \mathbb{F}}(h(aU + b) \neq \perp) \leq \gamma$*

2. $\Pr_{U \leftarrow \mathbb{F}}(h(aU+b) \neq \perp \mid h(U) = m) \leq \delta$
3. *A uniformly random X such that $h(X) = m$ is efficiently samplable.*

Aggarwal [Agg15] showed the following.

Lemma 11. *There exists an efficiently computable $(p^{-3/4}, \Theta(|\mathcal{M}| \log p \cdot p^{-1/4}))$-affine-evasive function $h : \mathbb{F} \mapsto \mathcal{M} \cup \{\perp\}$.*

We now describe the coding scheme from [ADL14] combined with the affine-evasive function promised by Lemma 11. Let $\mathcal{M} = \{1, \ldots, K\}$ and $\mathcal{X} = \mathbb{F}^n$, where $\mathbb{F}$ is a finite field of prime order p such that $p \geq (K/\varepsilon)^{16}$, and n chosen as $C \log^6 p$, where C is some universal constant.
Then for any $m \in \mathcal{M}$, $\mathsf{Enc}(m) = \mathsf{Enc}_1 \circ \mathsf{Enc}_2(m)$, where for any $m \in \mathcal{M}$, $\mathsf{Enc}_2(m)$ is X where X is uniformly random such that $h(X) = m$, where h is affine-evasive function defined earlier, and for any $x \in \mathbb{F}$, $\mathsf{Enc}_1(x) = (L, R)$, where $L, R \in \mathbb{F}^n$ are uniform such that $\langle L, R \rangle = x$.
The decoding algorithm is as follows. For $\ell, r \in \mathbb{F}^n \times \mathbb{F}^n$, $\mathsf{Dec}(\ell, r) = \mathsf{Dec}_2 \circ \mathsf{Dec}_1(\ell, r)$, where for any $\ell, r \in \mathbb{F}^n$, $\mathsf{Dec}_1(\ell, r) = \langle \ell, r \rangle$, and for any $x \in \mathbb{F}$, $\mathsf{Dec}_2(x) = h(x)$.
The following is implicit in [ADL14].

Theorem 4. *Let $f, g : \mathbb{F}^n \mapsto \mathbb{F}^n$ be arbitrary functions. Let $s = \lfloor n/20 \rfloor$, and let $t = \lfloor \frac{s^{1/6}}{c \log p} \rfloor$, for some universal constant c. Then, there exists a set $\mathcal{S} \subset \mathbb{F}^n \times \mathbb{F}^n$ of size at most p^{2n-s} such that $\mathbb{F}^n \times \mathbb{F}^n \setminus \mathcal{S}$ can be partitioned into sets of the form*

1. *$\mathcal{L} \times \mathcal{R}$ such that $(\langle L', R' \rangle, \langle f(L'), g(R') \rangle)$ is p^{-t}-close to uniform for L', R' uniform in $\mathcal{L}, \mathcal{R}$ respectively.*
2. *$\mathcal{L} \times \mathcal{R}$, such that $|\mathcal{L} \times \mathcal{R}| \geq p^{2n-7s}$, and there exists $A \in \mathbb{F}^{n \times n}$, $a, b \in \mathbb{F}$ such that $f(\ell) = A\ell$ for all $\ell \in \mathcal{L}$, and $A^T g(r) = ar + b$ for all $r \in \mathcal{R}$.*
3. *$\mathbb{F}^n \times \mathcal{R}$, such that $|\mathcal{R}| \geq p^{n-t}$, and there exists $y \in \mathbb{F}^n$, such that $g(r) = y$ for all $y \in \mathcal{R}$.*

To argue that the construction given above is also super-non-malleable, we will need the following:

Lemma 12. *Let L and R be independent random variables over $\mathbb{F}^n$. If*

$$\mathbf{H}_\infty(L) + \mathbf{H}_\infty(R) \geq (n+1) \log p + 2 \log\left(\frac{1}{\varepsilon}\right) ,$$

then

$$\Delta((L, \langle L, R \rangle) \; ; \; (L, U_{\mathbb{F}})) \leq \varepsilon \text{ and } \Delta((R, \langle L, R \rangle) \; ; \; (R, U_{\mathbb{F}})) \leq \varepsilon.$$

Lemma 13. *Let $X_1, Y_1 \in \mathcal{A}$, and $X_2, Y_2 \in \mathcal{B}$ be random variables such that $\Delta((X_1, X_2) \; ; \; (Y_1, Y_2)) \leq \varepsilon$. Then, for any non-empty set $\mathcal{A}_1 \subseteq \mathcal{A}$, we have*

$$\Delta(X_2 \mid X_1 \in \mathcal{A}_1 \; ; \; Y_2 \mid Y_1 \in \mathcal{A}_1) \leq \frac{2\varepsilon}{\Pr(X_1 \in \mathcal{A}_1)} .$$

Theorem 5. *The scheme $(\mathsf{Enc}, \mathsf{Dec})$ is a $O(\varepsilon)$-super-non-malleable code.*

Proof. We will argue that each partition promised by Theorem 4 is one of $\mathcal{S}_1, \ldots, \mathcal{S}_{s+t}, \mathcal{S}^\star$ as in Observation 6.1 with $\varepsilon' = \varepsilon$. Clearly, for any $m \in \mathcal{M}$, $\Pr(\mathsf{Enc}(m) \in \mathcal{S}) \leq p^{-s+1} \leq \varepsilon$, and hence we can set $\mathcal{S}^\star = \mathcal{S}$. So, we consider the partitioning of $\mathbb{F}^n \times \mathbb{F}^n \setminus \mathcal{S}$.

1. $\mathcal{L} \times \mathcal{R}$ such that $(\langle L', R' \rangle, \langle f(L'), g(R') \rangle)$ is p^{-t}-close to uniform for L', R' uniform in $\mathcal{L}, \mathcal{R}$ respectively. In this case, for any message m, if $(L, R) \leftarrow \mathsf{Enc}(m)$, then $\mathsf{Dec}(f(L), g(R))$ conditioned on $(L, R) \in \mathcal{L} \times \mathcal{R}$ is $h(\langle f(L'), g(R') \rangle)$ conditioned on $h(\langle L', R' \rangle) = m$. By Lemma 13, we have that this is $2 \cdot p^{-t+1}$-close to uniform, and hence, by Lemma 11, we have that $h(\langle f(L'), g(R') \rangle) = \perp$ with probability at least $1 - p^{-3/4} - p^{-t+1} \geq 1 - \varepsilon$.
2. $\mathcal{L} \times \mathcal{R}$, such that $|\mathcal{L} \times \mathcal{R}| \geq p^{2n-7s}$, and there exists $A \in \mathbb{F}^{n \times n}$, $a, b \in \mathbb{F}$ such that $f(\ell) = A\ell$ for all $\ell \in \mathcal{L}$, and $A^T g(r) = ar + b$ for all $r \in \mathcal{R}$. In this case, if $a \neq 0$, then using the same argument as in the previous item, we have that $\mathsf{Dec}(f(L), g(R))$ conditioned on $(L, R) \in \mathcal{L} \times \mathcal{R}$ is $\perp$ with probability at least $1 - p^{-1/4} \log p - p^{-t+1} \geq 1 - \varepsilon$.
   So, we can assume without loss of generality that $a = 0$. This means that $\langle f(\ell), g(r) \rangle = b$ for all $\ell \in \mathcal{L}, r \in \mathcal{R}$. Thus, for L', R' uniform in $\mathcal{L}, \mathcal{R}$, respectively, one of $f(L'), g(R')$ is contained in a subspace of $\mathbb{F}^n$ of size $p^{n/2}$. Without loss of generality, let $f(L')$ be contained in a subspace of size $p^{n/2}$. Then, $\mathbf{H}_\infty(L' | f(L')) + \mathbf{H}_\infty(R') \geq (3n/2 - 7s) \log p$. Hence, using Lemma 12, we have that $\langle L', R' \rangle$ is p^{-s}-close to uniform given $f(L')$, and R', and so, using Lemma 13, this partition satisfies item 2 from Observation 6.1.
3. $\mathbb{F}^n \times \mathcal{R}$, such that $|\mathcal{R}| \geq p^{n-t}$, and there exists $y \in \mathbb{F}^n$, such that $g(r) = y$ for all $y \in \mathcal{R}$. Let L', R' uniform in $\mathbb{F}^n, \mathcal{R}$, respectively. Then, using Lemma 12, we have that $\langle L', R' \rangle$ is $p^{-(n-t-1)/2}$-close to uniform given $f(L')$, and $g(R') = y$, and so, using Lemma 13, this partition satisfies item 2 from Observation 6.1.

The result then follows from Observation 6.1. □

By combining Theorem 5, Theorem 2, and Theorem 3, we obtain Theorem 1.

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.

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

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

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

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

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

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

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

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

CGL15. Eshan Chattopadhyay, Vipul Goyal, and Xin Li. Non-malleable extractors and codes, with their many tampered extensions. *CoRR*, abs/1505.00107, 2015.

CGM+15. Nishanth Chandran, Vipul Goyal, Pratyay Mukherjee, Omkant Pandey, and Jalaj Upadhyay. Block-wise non-malleable codes. *IACR Cryptology ePrint Archive*, 2015:129, 2015.

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.

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

DDN00. D. Dolev, C. Dwork, and M. Naor. Nonmalleable cryptography. *SIAM*, 30:391–437, 2000.

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

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

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

DW09. Yevgeniy Dodis and Daniel Wichs. Non-malleable extractors and symmetric key cryptography from weak secrets. In Michael Mitzenmacher, editor, *Proceedings of the 41st Annual ACM Symposium on Theory of Computing*, pages 601–610, Bethesda, MD, USA, 2009. ACM.

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

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

GLM+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.

IPSW06. Yuval Ishai, Manoj Prabhakaran, Amit Sahai, and David Wagner. Private circuits II: Keeping secrets in tamperable circuits. In Serge Vaudenay, editor, *Advances in Cryptology—EUROCRYPT 2006*, volume 4004 of *LNCS*, pages 308–327. Springer-Verlag, 2006.

ISW03. Yuval Ishai, Amit Sahai, and David Wagner. Private circuits: Securing hardware against probing attacks. In Dan Boneh, editor, *Advances in Cryptology—CRYPTO 2003*, volume 2729 of *LNCS*. Springer-Verlag, 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.

KKS11. Yael Tauman Kalai, Bhavana Kanukurthi, and Amit Sahai. Cryptography with tamperable and leaky memory. In *Advances in Cryptology–CRYPTO 2011*, pages 373–390. Springer, 2011.

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.

A Equivalence of Our Non-malleable Codes Definition with that of [DPW10]

Theorem 6. *If* $(\mathsf{Enc}, \mathsf{Dec})$ *is* $\varepsilon-$*non-malleable code then it is* $\varepsilon-$*DPW-non-malleable code.*

Proof. Let us define transform $T_m : \mathcal{M} \cup \{\perp, \mathsf{same}\} \to \mathcal{M} \cup \{\perp\}$ as follows: for any $m' \in \mathcal{M}$ let $T_m(m') = m'$, $T_m(\perp) = \perp$, $T_m(\mathsf{same}) = m$. Notice that $T_m(\mathsf{Tamper}_m^{f,g}) = \mathsf{DPWTamper}_m^{f,g}$. Fix any message m_0, and take $D^{f,g} = \mathsf{Tamper}_{m_0}^{f,g}$. We know that $\mathsf{Tamper}_m^{f,g} \approx_\varepsilon \mathsf{Tamper}_{m_0}^{f,g}$ for any functions f, g and and any message m. Thus

$$T_m(\mathsf{Tamper}_m^{f,g}) \approx_\varepsilon T_m(\mathsf{Tamper}_{m_0}^{f,g}),$$

$$\mathsf{DPWTamper}_m^{f,g} \approx_\varepsilon T_m(D^{f,g}).$$

□

Theorem 7. *If* $(\mathsf{Enc}, \mathsf{Dec})$ *is* $\varepsilon-$*DPW-non-malleable code then it is* $4\varepsilon-$*non-malleable code.*

Proof. Using the notation from Theorem 6, we know that, independent of the choice of $D^{f,g}_{x,y}$ distributions, the following is true:

$$T_m(\mathsf{Tamper}^{f,g}_m) = \mathsf{DPWTamper}^{f,g}_m.$$

Now let $D^{f,g}_{x,y}$ as follows:

$$\Pr(D^{f,g}_{x,y} = 0) = \min\left\{\frac{\Pr(D^{f,g} = \mathsf{same})}{\Pr(\mathsf{DPWTamper}^{f,g}_{\mathsf{Dec}(x,y)} = \mathsf{Dec}(x,y))}, 1\right\}$$

if $\Pr(\mathsf{DPWTamper}^{f,g}_{\mathsf{Dec}(x,y)} = \mathsf{Dec}(x,y)) \neq 0$. Otherwise let $\Pr(D^{f,g}_{x,y} = 0) = 0$.
Notice that now

$$\Pr(\mathsf{Tamper}^{f,g}_m = \mathsf{same}) \approx_\varepsilon \Pr(D^{f,g} = \mathsf{same}).$$

By DPW-non-malleable codes definition we get

$$T_m(\mathsf{Tamper}^{f,g}_m) \approx_\varepsilon T_m(D^{f,g})$$

thus

$$\mathsf{Tamper}^{f,g}_m \approx_{2\varepsilon} D^{f,g},$$

and thus that for any m_0, m_1 we get

$$\mathsf{Tamper}^{f,g}_{m_0} \approx_{4\varepsilon} \mathsf{Tamper}^{f,g}_{m_1}.$$

□