Electronic Colloquium on Computational Complexity, Report No. 129 (2014)

Leakage-resilient non-malleable codes

Divesh Aggarwal* Stefan Dziembowski† Tomasz Kazana‡ Maciej Obremski§

October 7, 2014

Abstract

A recent trend in cryptography is to construct cryptosystems that are secure against physical attacks. Such attacks are usually divided into two classes: the *leakage* attacks in which the adversary obtains some information about the internal state of the machine, and the *tampering* attacks where the adversary can modify this state. One of the popular tools used to provide tamper-resistance are the *non-malleable codes* introduced by Dziembowski, Pietrzak and Wichs (ICS 2010). These codes can be defined in several variants, but arguably the most natural of them are the information-theoretically secure codes in the *k-split-state model* (the most desired case being $k = 2$).

Such codes were constucted recently by Aggarwal et al. (STOC 2014). Unfortunately, unlike the earlier, computationally-secure constructions (Liu and Lysyanskaya, CRYPTO 2012) these codes are not known to be resilient to leakage. This is unsatisfactory, since in practice one always aims at providing resilience against *both* leakage and tampering (especially considering tampering without leakage is problematic, since the leakage attacks are usually much easier to perform than the tampering attacks).

In this paper we close this gap by showing a non-malleable code in the 2-split state model that is secure against leaking almost a 1/12-th fraction of the bits from the codeword (in the bounded-leakage model). This is achieved via a generic transformation that takes as input any non-malleable code $(\mathsf{Enc}, \mathsf{Dec})$ in the 2-split state model, and constructs out of it another non-malleable code $(\mathsf{Enc}', \mathsf{Dec}')$ in the 2-split state model that is additionally leakage-resilient. The rate of $(\mathsf{Enc}', \mathsf{Dec}')$ is linear in the rate of $(\mathsf{Enc}, \mathsf{Dec})$. Our construction requires that Dec is *symmetric*, i.e., for all x, y, it is the case that $\mathsf{Dec}(x, y) = \mathsf{Dec}(y, x)$, but this property holds for all currently known information-theoretically secure codes in the 2-split state model. In particular, we can apply our transformation to the code of Aggarwal et al., obtaining the first leakage-resilient code secure in the split-state model. Our transformation can be applied to other codes (in particular it can also be applied to a recent code of Aggarwal, Dodis, Kazana and Obremski constructed in the work subsequent to this one).

*Computer Science Dept. NYU. Email: divesha@cs.nyu.edu.
†Institute of Informatics, University of Warsaw. Email: std@mimuw.edu.pl.
‡Institute of Informatics, University of Warsaw. Email: tkazana@mimuw.edu.pl.
§Institute of Informatics, University of Warsaw. Email: obremski@mimuw.edu.pl.

ISSN 1433-8092

1 Introduction

Several attacks on cryptographic devices are based on exploiting physical weaknesses in their implementations. Such "physical attacks" are usually based on the *side-channel information* about the internals of the cryptographic device that the adversary can obtain by measuring its running-time, electromagnetic radiation, power consumption (see e.g. [ECR]), or on active tampering (see e.g. [AK96, ECR]). A recent trend in theoretical cryptography, initiated by [MR04, ISW03, IPSW06], is to design schemes that are provably-secure even if their implementations can be attacked.

One of the tools used in this area are the so-called *non-malleable codes* introduced by Dziembowski, Pietrzak and Wichs in 2010 [DPW10]. Informally, a code $(\mathsf{Enc} : \mathcal{M} \to \mathcal{C}, \mathsf{Dec} : \mathcal{C} \to \mathcal{M})$, where Enc is a randomized encoding function, and Dec is a partial decoding function, is *non-malleable* if an adversary that learns $C = \mathsf{Enc}(M)$ is not able to produce $C' = h(C)$ such that $\mathsf{Dec}(C')$ is not equal to M, but is "related" to it. The precise meaning of "not being related" is a little tricky to define but intuitively, what we require is that C' does not depend on C in any non-trivial way. For example: C' equal to C with the first bit set to zero, or C' equal to C with every bit negated, are obviously "related" to C, but a uniformly random C', or a constant C' are unrelated to C. It is easy to see that in order to construct such codes, one needs to restrict in some way the set of possible "manipulation functions" h that the adversary can use in order to compute C' from C. This is because otherwise the adversary could simply let h compute M from C (using the decoding function Dec), compute M' that is "related to M" (by say, negating all the bits of M), and then output $C' = \mathsf{Enc}(M')$. Therefore the non-malleable codes are always defined with respect to a family $\mathcal{H}$ of manipulation functions h that the adversary is allowed to use to compute C' from C.

The main application for this notion is the protection against tampering attacks. Imagine $C = \mathsf{Enc}(M)$ is stored on some device that the adversary can tamper with, and hence he can substitute C with some $C' \neq C$. Suppose $(\mathsf{Enc}, \mathsf{Dec})$ is non-malleable with respect to the set of manipulation functions that the adversary is able to induce by tampering. Then the only thing that the adversary can achieve is that C' will either decode to the same M, or to some M' that is totally unrelated to M. This is useful, since many practical attacks on cryptographic schemes are based on the so-called "related key attacks" [BK03], where the adversary is able to break a scheme $\mathsf{S}(K)$ (where K is the secret key) by having access to a device $\mathsf{S}(K')$ for some K' that is related to K. Clearly, storing K in an encoded form $\mathsf{Enc}(K)$ provides protection against such attacks. In [DPW10] the authors describe also other applications of non-malleable codes. In particular they show how to use them in combination with the *algorithmic tamper proof security* framework of Gennaro et al. [GLM+04]. Recently, Faust et al. used the non-malleable codes to construct Random Access Machines secure against tampering and leakage attacks [FMNV14b], and Coretti et al. [CMTV14] have shown how to use the non-malleable codes to construct public-key encryption schemes.

Since the invention of the non-malleable codes, there has been a significant effort to construct codes that would be secure against interesting classes of families. In [DPW10] the authors show a construction of efficient codes secure against bit-wise tapering, i.e. when every bit of the codeword is manipulated independently (this is achieved using the algebraic manipulation detection codes of Cramer et al. [CDF+08]). They also provide an existential result that for every sufficiently small family $\mathcal{H}$ of manipulation functions there exists a (not necessarily efficient) non-malleable code secure against it. This immediately gives a construction of non-malleable codes secure in the random oracle model [BR93].

Previous constructions of non-malleable codes in the split-state model. A very attractive and natural family of manipulation functions can be defined using the so-called *split-state model*. Assume that C is represented as a sequence of blocks $C = (C_1, \cdots, C_k)$. Then $\mathcal{H}$ is a family of *k-split state manipulation functions* if every $h \in \mathcal{H}$ manipulates each element $C_1, \ldots, C_k$ independently, i.e., for every h there exist functions $\{h_i\}_{i=1}^k$ such that $h(C_1, \ldots, C_k) = (h_1(C_1), \ldots, h_k(C_k))$. A practical justification for such a model comes from an observation that it may be easy to achieve in real life, by simply placing every C_i on a separate chip. Of course, the fewer parts are needed, the stronger the model is, and in particular the most desirable case is $k = 2$. In the sequel, we will sometimes refer to the 2-split state model simply as the "split model".

The aforementioned existential result of [DPW10] implies that there exist non-malleable codes in the 2-split state model. The problem of showing an efficient construction of such codes was left open in [DPW10]. The first step towards solving it was made by Liu and Lysyanskaya [LL12], who showed a construction of non-malleable codes computationally secure in the 2-split state model. Dziembowski, Kazana and Obremski [DKO13] provided an efficient construction of information-theoretically non-malleable codes that works only for messages of length 1. The problem of constructing information-theoretically secure codes for messages of arbitrary length was finally solved by Aggarval, Dodis and Lovett [ADL14]. Their construction is based on the methods from additive combinatorics, including the so-called *Quasi-polynomial Freiman-Ruzsa Theorem*, and involves a substantial blow-up in the size of the codeword ($|C| = \tilde{O}((|M| + \kappa)^7)$, where κ is the security parameter). Very recently Chattopadhyay and Zuckerman [CZ14] have shown a construction of non-malleable codes in 10-split state model that achieves linear blow-up.

A subsequent construction of non-malleable codes in the split-state model. In a paper subsequent to this one, Aggarwal et al. [ADKO14] show a general transformation of any k-split state model secure non-malleable code into one secure in the 2-split state model, that involves a linear blow-up in the codeword size. This, together with the result of [CZ14] gives a construction of a non-malleable code in the 2-split state model with codeword of length linear in $|M|$. Their construction uses some of the techniques developed in this work. In particular, one of the steps of their construction which can be seen as a generalization of our reduction is a reduction from the 2-split-state tampering family to the so called 2-part t-lookahead tampering family. However, the result of [ADKO14] does not consider leakage-resilience, and considering the number of levels of encoding required by their result, it is unlikely that their construction is resilient to any significant leakage.

Leakage-resilience of non-malleable codes. The ultimate goal of the "physically secure cryptography" is to provide both tampering- and leakage-resilience. The basic definition of the non-malleable codes does not consider any type of leakage information that the adversary can obtain about the codeword through the side channels. This may be considered unrealistic, as in practice it may be often relatively easy for the adversary to obtain such information (probably easier than to perform the tampering attacks). Therefore, it would be desirable to include also such attacks in this definition. The first paper that considered *leakage-resilient* non-malleable codes was [LL12] (in the computational settings). Our definition essentially follows their ideas, except that we consider the information-theoretic settings.

Let us now explain informally the concept of leakage-resilient non-malleable codes in the 2-split state model (the formal definition appears in Section 3). First consider the question what would be the most natural definition of leakage and tampering attacks. To be as general as possible we should give to the adversary right to simultaneously tamper the codeword $C = (L, R)$ and leak

information from it. The leakage will be modeled by allowing the adversary to choose functions $\mathsf{Leak}_i^{\mathsf{L}}$ and $\mathsf{Leak}_i^{\mathsf{R}}$ and learn $\mathsf{Leak}_i^{\mathsf{L}}(L)$ and $\mathsf{Leak}_i^{\mathsf{R}}(R)$ (respectively). The entire process should happen in several rounds, and the adversary should be adaptive (i.e. his behavior in round i should depend on what he learned in the previous rounds). The functions will be arbitrary, except that we will have a bound on the total number of bits leaked from L and R, where the "number of leaked bits" is measured in terms of the total out size of the $\mathsf{Leak}_i^{\mathsf{L}}(L)$ and $\mathsf{Leak}_i^{\mathsf{L}}(R)$ functions. This is essentially the *independent leakage model* first considered in [DP08] (inspired by the "only computation leaks" paradigm of Micali and Reyzin [MR04]) and then in a sequence of papers (see, e.g.: [DDV10, FKPR10, GR12, DF12, BDL14]). It makes particular sense to use it in our context, as it is also motivated by the assumption that L and R are stored on two separate memory parts. Observe also that if we allowed joint leakage from L and R then we would need to have some additional restrictions on the leakage functions, as otherwise the adversary could choose a leakage function that first computes $M = \mathsf{Dec}(L, R)$ and then outputs the first bit $M[1]$ of M. This, in turn, would allow him to choose tampering functions that simply overwrite the original encoding with (L', R') such that $\mathsf{Dec}(L', R')$ is equal to $(M[1], 0, \ldots, 0)$ (such M' is obviously "related" to M and with overwhelming probability it is not equal to M). For similar reasons it is obvious that we always need some sort of restriction on the leakage functions $\mathsf{Leak}_i^{\mathsf{L}}$ and $\mathsf{Leak}_i^{\mathsf{R}}$, since if the adversary learns the entire L (say) then he can then easily choose a leakage function $\mathsf{Leak}_i^{\mathsf{R}}$ that first computes $\mathsf{Dec}(L, R)$ and then outputs $M[1]$.

It is also easy to see that without loss of generality we can restrict the adversary to choose deterministic leakage functions (since we can always convert a random function to a deterministic one by fixing its random input). Another natural observation is that it is enough to consider the case when all the leakage happens before the tampering functions are chosen. This is because the result of any leakage Leak_i from a tampered codeword $f(C)$ can be computed by a function $\mathsf{Leak}'_i = \mathsf{Leak}_i \circ f$ that is applied directly to C. The formal definition of our model appears in Section 3.

1.1 Our contribution

As argued above, leakage-resilence is an important property for may applications of the non-malleable codes. Unfortunatelly, this aspect of these codes has been ignored in many recent papers on this topic. In particular, the authors of [ADL14, CZ14] do not consider leakage at all. Proving that the code of [ADL14] is resilient to significant amounts of leakage seems highly non-trivial (if not impossible), as one would need to adapt their "additive combinatorics" argument to consider leakage. What would probably be easier (but still very far from immediate) would be to prove some leakage-resilience of the 10-split state encoding of [CZ14]. Leakage-resilience was considered in [DKO13], but their construction works only for messages of length 1. To summarize: until now, no construction of leakage-resilient 2-split state non-malleable codes for messages longer than 1 was known. Providing such a construction is the main contribution of this work.

In fact, our contribution is much more general. We show a generic transformation that takes as input any non-malleable code $(\mathsf{Enc}, \mathsf{Dec})$ in the 2-split state model, and constructs out of it another non-malleable code $(\mathsf{Enc}', \mathsf{Dec}')$ in the 2-split state model that additionally is secure against leaking a constant fraction of the bits from the codeword. The rate of $(\mathsf{Enc}', \mathsf{Dec}')$ is linear in the rate of $(\mathsf{Enc}, \mathsf{Dec})$. The only thing that we require is that $(\mathsf{Enc}, \mathsf{Dec})$ is *symmetric*, i.e., $\mathsf{Dec}(L, R) = \mathsf{Dec}(R, L)$. Since the code of [ADL14] has this property, thus, combining this result with ours, we obtain a leakage-resilient 2-split state non-malleable code.

Let us also note that the code from the subsequent work of [ADKO14] (built by applying a reduction from 10-split to 2-split state to the code of [CZ14]) is also symmetric, and therefore we

can instantiate $(\mathsf{Enc}, \mathsf{Dec})$ with this construction, obtaining that $(\mathsf{Enc}', \mathsf{Dec}')$ is a constant rate and can tollerate leakage of a linear size.

Our key technical argument is contained in Theorem 5.1 that can be of independent interest. Informally, in this theorem we consider a "parallel composition of the inner product encodings", i.e., we consider encoding of a pair of messages $x_1, x_2 \in \mathbb{F}$ as random elements $L_1, R_1, L_2, R_2 \in \mathbb{F}^n$ such that $\langle L_1, R_1 \rangle = x_1$, and $\langle L_2, R_2 \rangle = x_2$. We show that it is partly resilient to tampering in the following sense. If (L_1, L_2) and (R_1, R_2) are independently tampered to obtain (L_1', L_2') and (R_1', R_2'), and then we decode to get $x_1' = \langle L_1', R_1' \rangle$, and $x_2' = \langle L_2', R_2' \rangle$, then x_1', x_2' can only have a limited dependence on x_1, x_2. The proof of this result is done using a careful combinatorial argument that among other techniques, makes extensive use of the two-source extractor property of the inner-product, and Vazirani's XOR Lemma.

1.2 Other related work

The notion of non-malleability was introduced in cryptography by Dwork et al. [DDN98]. Formal treatment of the tampering attacks was initiated in [IPSW06, GLM+04]. The non-malleable codes were also studied by Cheraghchi and Guruswami, who in [CG14b] show improved constructions of the non-malleable codes secure against bit-wise tampering and show a connection between the non-malleable codes and the seedless non-malleable extractors (which is a new notion that they introduce). In [CG14a] the same authors study the problem of the capacity of non-malleable codes secure against different (non-split-state) families. Extensions of non-malleable codes to the case of *continuous* tampering were studied in [FMNV14a]. Non malleable codes secure against tampering functions coming from restricted complexity classes were studied in [FMVW14], and secure against the linear tampering functions were considered in [CCP12].

Simultaneous leakage and tampering attacks were also considered in [LL10] (who consider a more restricted type of leakage, called the "probing attacks"), in [KKS11] who construct tamper- and leakage-resilient encryption and signature schemes, and in [DK12] who show a general way to transform any cryptographic functionality into one that is secure against tampering with individual bits, and leaking a logarithmic amount of information. Probabilistic tampering attacks on boolean circuits (where the adversary can tamper each wire with a certain probability) were also considered in [FPV11].

2 Preliminaries

For a set T, let U_T denote a uniform distribution over T, and, for an integer ℓ, let U_ℓ denote uniform distribution over ℓ bit strings. The *statistical distance* between two random variables A, B is defined by $\Delta(A, B) = \frac{1}{2} \sum_v |\Pr[A = v] - \Pr[B = v]|$. We use $A \approx_\varepsilon B$ as shorthand for $\Delta(A, B) \leq \varepsilon$.

Lemma 2.1. *For any (randomized) function α, if $\Delta(A, B) \leq \varepsilon$, then $\Delta(\alpha(A), \alpha(B)) \leq \varepsilon$.*

The *min-entropy* of a random variable W is $\mathbf{H}_\infty(W) \stackrel{\text{def}}{=} -\log(\max_w \Pr[W = w])$, and the *conditional* min-entropy of W given Z is $\mathbf{H}_\infty(W|Z) \stackrel{\text{def}}{=} -\log\left(\mathbb{E}_{z \leftarrow Z} \max_w \Pr[W = w | Z = z]\right)$.[1]

Definition 2.2. *We say that an efficient function $\mathsf{Ext} : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^m$ is an (n, k, m, ε)*-two-source extractor *[CG88] if for all independent sources $X, Y \in \{0,1\}^n$ such that min-entropy $\mathbf{H}_\infty(X) + \mathbf{H}_\infty(Y) \geq k$, we have $(Y, \mathsf{Ext}(X, Y)) \approx_\varepsilon (Y, U_m)$, and $(X, \mathsf{Ext}(X, Y)) \approx_\varepsilon (X, U_m)$.*

[1] Note that we use the variant of conditional entropy where the logarithm is taken *after* $\max_w$ is determined. This definition was introduced in [DORS08] (it was called an *average min-entropy* there).

For n being an integer multiple of m, and interpreting elements of $\{0,1\}^m$ as elements from $\mathbb{F}_{2^m}$ and those in $\{0,1\}^n$ to be from $(\mathbb{F}_{2^m})^{n/m}$, we have that the inner product function defined as $\langle (a_1,\ldots,a_{n/m}),(b_1,\ldots,b_{n/m})\rangle := a_1b_1+\cdots+a_{n/m}b_{n/m}$ is a good 2-source extractor (cf. eg. [CG88, Rao07]).

Lemma 2.3. *For all positive integers m, n such that n is a multiple of m, and for all $\varepsilon > 0$, there exists an efficient $(n, n+m+2\log\left(\frac{1}{\varepsilon}\right), m, \varepsilon)$ 2-source extractor.*

We will need the following results. The proofs of these results can be found in Appendix A for completeness. The following is a simple result from [ADL14].

Lemma 2.4. *Let $X_1, Y_1 \in \mathcal{A}_1$, and $Y_1, Y_2 \in \mathcal{A}_2$ be random variables such that $\Delta((X_1,X_2)\ ;\ (Y_1,Y_2)) \leq \varepsilon$. Then, for any non-empty set $\mathcal{A}' \subseteq \mathcal{A}_1$, we have*

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

A *leakage oracle* is a machine Ω that takes as input $(L,R) \in \{0,1\}^n \times \{0,1\}^n$ and then answers the *leakage queries* of a type (L, f) and (R, g), where $f, g : \{0,1\}^n \to \{0,1\}^*$. Each query (L, f_i) (resp.: (R, g_i)) is answered with $f_i(L)$ (resp.: $g_i(R)$) or $\perp$. An interactive machine $\mathcal{A}$ that issues the leakage queries is called a *leakage adversary*. Let $\mathsf{Leak}_{\mathsf{L}}^{\mathcal{A}}(L)$ (resp.: $\mathsf{Leak}_{\mathsf{R}}^{\mathcal{A}}(R)$) denote the concatenation of all the non-$\perp$ answers to the (L, f_i) (resp.: (R, g_i)) queries of $\mathcal{A}$. Moreover, let $\mathsf{Leak}^{\mathcal{A}}(L,R) := (\mathsf{Leak}_{\mathsf{L}}^{\mathcal{A}}(L), \mathsf{Leak}_{\mathsf{R}}^{\mathcal{A}}(R))$. The oracle Ω is m-bounded if it gives the non-$\perp$ answers to the (L, f_i) queries as long as $|\mathsf{Leak}_{\mathsf{L}}^{\mathcal{A}}(L)| \leq m$ and the non-$\perp$ answers to (R, f_i) queries as long as $|\mathsf{Leak}_{\mathsf{R}}^{\mathcal{A}}(R)| \leq m$. The following result follows easily Lemma 4 of [DP07] and Lemma 2.2 of [DORS08].

Lemma 2.5. *Let $\tilde{L} \in \{0,1\}^n$ and $\tilde{R} \in \{0,1\}^n$ be two independent random variables, and let $\mathcal{A}$ be an arbitrary leakage adversary interacting with an m-bounded oracle $\Omega(\tilde{L}, \tilde{R})$. Then $\tilde{L}$ and $\tilde{R}$ are independent given $\mathsf{Leak}^{\mathcal{A}}(\tilde{L}, \tilde{R})$. Moreover, for every $\delta > 0$ we have*

$$\Pr\left(\mathbf{H}_\infty(\tilde{L} \mid \mathsf{Leak}^{\mathcal{A}}(\tilde{L},\tilde{R}) = a) \leq \log|\mathcal{L}| - m - \log(1/\delta)\right) \leq \delta$$

(where $a := \mathsf{Leak}^{\mathcal{A}}(\tilde{L},\tilde{R})$), and

$$\Pr\left(\mathbf{H}_\infty(\tilde{R} \mid \mathsf{Leak}^{\mathcal{A}}(\tilde{L},\tilde{R}) = b) \leq \log|\mathcal{L}| - m - \log(1/\delta)\right) \leq \delta,$$

(where $b := \mathsf{Leak}^{\mathcal{A}}(\tilde{L},\tilde{R})$).

We say that $(\mathsf{Enc}_{\mathsf{LR}} : \mathcal{M} \to \mathcal{L} \times \mathcal{R}, \mathsf{Dec}_{\mathsf{LR}} : \mathcal{L} \times \mathcal{R} \to \mathcal{M})$ is an *ε-leakage-resilient encoding in the split-state model* [DDV10] if for every $M_0, M_1 \in \mathcal{M}$ we have that

$$\Delta(\mathsf{Leak}(\mathsf{Enc}_{\mathsf{LR}}(M_0))\ ;\ \mathsf{Leak}(\mathsf{Enc}_{\mathsf{LR}}(M_1)) \leq \varepsilon.$$

Such encodings can be easily constructed from the 2-source extractors [DDV10]. The following is a generalization of the Vazirani's XOR Lemma (it is proven in Appendix A).

Lemma 2.6. *Let $X = (X_1,\ldots,X_t) \in \mathbb{F}^t$ be a random variable, where $\mathbb{F}$ is a finite field of order q. Assume that for all $a_1,\ldots,a_t \in \mathbb{F}^t$ not both zero, $\Delta(\sum_{i=1}^t a_iX_i\ ;\ U) \leq \varepsilon$, where U is uniform in $\mathbb{F}$. Then $\Delta(X_1,\ldots,X_t\ ;\ U_1,\ldots,U_t) \leq \varepsilon q^t$, where $U_1,\ldots,U_t$ are independent and uniform in $\mathbb{F}^t$.*

3 The defintion of the Leakage Resilient Non-Malleable Codes

In this section we present the defintion of the leakage resilient non-malleable codes in the split-state model. We first recall the definition of non-malleable codes in the split-state model from [DPW10, ADL14]. As discussed already informally the introduction in this model we assume that the codeword is split into two parts which are tampered independently.

Definition 3.1. *A* coding scheme in the split-state model *consists of two functions: a randomized encoding function* $\mathsf{Enc} : \mathcal{M} \mapsto \mathcal{L} \times \mathcal{R}$*, and a deterministic decoding function* $\mathsf{Dec} : \mathcal{L} \times \mathcal{R} \mapsto \mathcal{M} \cup \{\perp\}$ *such that, for each* $M \in \mathcal{M}$, $\Pr(\mathsf{Dec}(\mathsf{Enc}(M)) = M) = 1$ *(over the randomness of the encoding algorithm). Suppose* $\mathcal{L} = \mathcal{R}$ *and denote* $\mathcal{C} := \mathcal{L}(= \mathcal{R})$*. A coding scheme* $(\mathsf{Enc}, \mathsf{Dec})$ *is* symmetric *is for every* $(L, R) \in \mathcal{C}$ *we have that* $\mathsf{Dec}(L, R) = \mathsf{Dec}(R, L)$*.*

Definition 3.2. *Let* $(\mathsf{Enc} : \mathcal{M} \to \mathcal{C}^2, \mathsf{Dec} : \mathcal{C}^2 \to \mathcal{M})$ *be a coding scheme in a split state model. For tampering functions* $f, g \in \mathcal{C}^{\mathcal{C}}$*, and* $m \in \mathcal{M}$*, define the tampering-experiment*

$$\mathsf{Tamper}_m := \left\{ \begin{array}{c} (L, R) \leftarrow \mathsf{Enc}(m), \\ (\tilde{L}, \tilde{R}) := (f(L), g(R)) \\ \tilde{m} = \mathsf{Dec}(\tilde{L}, \tilde{R}) \\ \textit{Output: } \tilde{m}, \end{array} \right\}$$

which is a random variable over the randomness of the encoding function Enc*. We say that a coding scheme* $(\mathsf{Enc}, \mathsf{Dec})$ is ε-non-malleable w.r.t. $\mathcal{F}$ *if for each* $f \in \mathcal{F}$*, there exists a distribution (corresponding to the simulator)* D *over* $\mathcal{M} \cup \{\perp, \mathsf{same}\}$*, such that, for all* $m \in \mathcal{M}$*, we have that the statistical distance between* Tamper_m *and*

$$\mathsf{Sim}_m := \left\{ \begin{array}{c} \tilde{m} \leftarrow D \\ \textit{Output: } m \textit{ if } \tilde{m} = \mathsf{same}, \textit{ and } \tilde{m}, \textit{ otherwise} \end{array} \right\}$$

is at most ε*. Additionally,* D *should be efficiently samplable given oracle access to* f *and* g*.*

We now define the notion of non-malleability against the leakage adversaries (which was first formulated by [LL12]). As explained in the introduction it is enough to consider the scenario where the adversary first learns some bounded information about the codeword (via the leakage oracle), and then chooses the tampering functions. Formally we have the following.

Definition 3.3. *Let* $\mathsf{Enc}, \mathsf{Dec}$ *be a coding scheme from* $\{0,1\}^k$ *to* $\{0,1\}^n \times \{0,1\}^n$*, and let* $\gamma \in [0, 1)$ *be a parameter. Let* $\mathcal{A}$ *be any adversary that has oracle access to a* γn*-bounded leakage oracle* $\Omega(L, R)$ *(cf. 2), where* $L, R \in \{0,1\}^n$*, and outputs functions* (f, g) *such that* $f, g : \{0,1\}^m \to \{0,1\}^m$*. Let* $m \in \{0,1\}^k$ *be a message. Consider the following tampering experiment.*

$$\mathsf{Tamper}^{\gamma}_m := \left\{ \begin{array}{c} (L, R) \leftarrow \mathsf{Enc}(m), \\ (f, g) = \mathcal{A}(L, R), \\ (\tilde{L}, \tilde{R}) := (f(L), g(R)), \\ \tilde{m} = \mathsf{Dec}(\tilde{L}, \tilde{R}) \\ \textit{Output: } \tilde{m}, \end{array} \right\}$$

which is a random variable over the randomness of the encoding function Enc*. We say that a coding scheme* $(\mathsf{Enc}, \mathsf{Dec})$ is γ-leakage resilient ε-non-malleable code *if for each* $\mathcal{A}$*, there exists a distribution* D *over* $\{0,1\}^k \cup \{\perp, \mathsf{same}\}$*, such that, for all* $m \in \{0,1\}^k$*, we have that the statistical distance between* $\mathsf{Tamper}^{\gamma}_m$ *and*

$$\mathsf{Sim}_m := \left\{ \begin{array}{c} \tilde{m} \leftarrow D \\ \textit{Output: } m \textit{ if } \tilde{m} = \mathsf{same}, \textit{ and } \tilde{m}, \textit{ otherwise.} \end{array} \right\}$$

is at most ε. Additionally, D should be efficiently samplable given oracle access to $f, g, \mathsf{Leak}_1, \mathsf{Leak}_2$.

Of course, every ε-non-malleable code is also a 0-leakage resilient ε-non-malleable code. On the other hand, it is easy to find codes that are ε-non-malleable but are not ξ-leakage resilient ε-non-malleable for an arbitrarily small ξ. For example, consider an ε-non-malleable code $(\mathsf{Enc}, \mathsf{Dec})$, and construct another code $(\mathsf{Enc}', \mathsf{Dec}')$ as follows. Let

$$\mathsf{Enc}'(M) = (\underbrace{(L, \cdots, L)}_{\lceil 1/\xi \rceil \text{ times}}, \underbrace{(R, \cdots, R)}_{\lceil 1/\xi \rceil \text{ times}}),$$

where $(L, R) \leftarrow \mathsf{Enc}(M)$. The decoding function for $(L', R') = ((L_1, \ldots, L_{\lceil 1/\xi \rceil}), (R_1, \ldots, R_{\lceil 1/\xi \rceil})$ is defined as: $\mathsf{Dec}'(L', R') = \perp$ if for some i, j we have $L_i \neq L_j$ or $R_i \neq R_j$, and $\mathsf{Dec}'(L', R') = \mathsf{Dec}(L_1, R_1)$ otherwise. It is easy to show that $(\mathsf{Enc}', \mathsf{Dec}')$ is also ε-non-malleable. On the other hand, clearly, it is *not* ξ-leakage resilient ε-non-malleable, since the adversary can simply leak L_1 and R_i (since $|L_i|/|L'| = |R_i|/|R'| = 1/(\lceil 1/\xi \rceil) \leq \xi$) and hence he can compute M before he chooses the tampering functions. Actually, it would even be enough for the adversary to leak L_i from one part (L, say), since in this case he could make the tampering function g fully dependent on M (since $M = \mathsf{Dec}(L_1, R_1)$), and, e.g., tamper with R only if $M = 0$ (which obviously means that the code is malleable).

4 Our construction

This section contains the main construction of our paper. Let $(\mathsf{Enc} : \mathcal{M} \to \mathcal{X} \times \mathcal{X}, \mathsf{Dec} : \mathcal{X} \times \mathcal{X} \to \mathcal{M})$ be a (not leakage resilient) symmetric ε-non-malleable code in the split state model. Let $\gamma \in [0, 1/12)$ be a parameter. We are going to construct a γ-leakage resilient 3ε-non-malleable code $(\mathsf{Enc}', \mathsf{Dec}')$ in the split state mode (the code $(\mathsf{Enc}', \mathsf{Dec}')$ will also be symmetric).

The first obvious idea for constructing such a code could be to define $\mathsf{Enc}'(m)$ as follows: first compute $(x_1, x_2) = \mathsf{Enc}(m)$, and then "encode" both x_1 and x_2 using the leakage-resilient encoding (cf. Section 2). To be more concrete choose an encoding of [DDV10] that is based on the inner product function[2]. Let (ℓ_1, r_1) and (ℓ_2, r_2) be such leakage-resilient encodings of x_1 and x_2, respectively. It is clear that given $(\ell_1, r_1, \ell_2, r_2)$ one can easily compute m as $\mathsf{Dec}(\langle \ell_1, r_1 \rangle, \langle \ell_2, r_2 \rangle)$.

Of course, what remains to be defined is how the variables ℓ_1, r_1, ℓ_2, and r_2 are represented in the final encoding, or, in other words: on which memory part one would store each of these variables. One option, of course, would be to move to the 4-split state model and say that the result of the encoding is $(\ell_1, r_1, \ell_2, r_2)$ (i.e. each of these variables can leak and be tampered independently). This approach can be proven secure, but it is clearly suboptimal since it increases to 4 the number of memory parts needed to implement the scheme.[3]

If we restrict ourselves to the 2-split state model then we could simply think of putting some of the ℓ_1, ℓ_2, r_1, r_2 variables on one part of the encoding and the remaining ones on the other part. It is easy to see that ℓ_1 and r_1 cannot be put together on one memory part (a symmetric argument works for ℓ_2 and r_2). This is because if the leakage function can be applied directly to ℓ_1 and r_1 then the adversary choose a function that it simply internally decodes x_1 from (ℓ_1, r_1) and leaks directly from x_1. Hence, the code would need to be non-malleable even if the adversary can choose

[2] In this encoding in order to encode a message x one chooses random vectors ℓ and r (in some $\mathbb{F}^n$) such that $\langle \ell, r \rangle = x$, and to decode the message one simply computes $\langle \ell, r \rangle$.

[3] One can be tempted to say that in this case we can apply the transformation from the subsequent paper [ADKO14] to reduce the number of parts from 4 to 2, but for this approach to work one would need to show that the construction of [ADKO14] preserves the leakage-resilience which seems highly non-trivial.

the tampering function g (that is applied to x_2) after learning x_1, which is impossible (cf. the discussion at the end of Section 3).

Hence, the only option that has chances to work is to define the encoding of m to be equal to $((\ell_1, \ell_2), (r_1, r_2))$. Observe that the adversary can now obviously "swap" x_1 and x_2 by changing the encoding to $((\ell_2, \ell_1), (r_2, r_1))$. This is ok for us, since we assumed that our encoding is symmetric. He can also "copy" elements, and produce an encoding $((\ell_1, \ell_1), (r_1, r_1))$ (or $((\ell_2, \ell_2), (r_2, r_2))$). In this case the decoded value (x'_1, x'_2) will be equal to (x_1, x_1) (resp.: (x_2, x_2)). It turns out that this is also ok, since every non-malleable code in the 2-split state is essentially also a 2-out-of-2 secret sharing function (we prove this fact in Lemma 6.1), and thus x_1 and x_2 individually do not provide any significant information about the encoded message m (which, of course, implies that $\mathsf{Dec}_{\mathsf{NM}}(x_1, x_1)$ is unrelated to m). Of course these attacks can be combined with tampering attacks applied to each of ℓ_1, ℓ_2, r_1 and r_2 individually. For example the adversary can transform the encoding to $((\ell_1, c \cdot \ell_1), (r_1, r_1))$, which (from the linearity of the inner product) would decode to $(x_1, c \cdot x_1)$. This, however, is not a problem, since such individual tampering is obviously tolerated by every non-malleable code.

Unfortunately, it turns out the the adversary can launch some more sophisticated attacks. Observe that in our encoding the values (ℓ_1, ℓ_2) and (r_1, r_2) can be treated as vectors of length $2n$. Suppose the adversary permutes both of them with the same random permutation σ, and let $(\ell'_1, \ell'_2) = \sigma(\ell_1, \ell_2)$ and $(r'_1, r'_2) = \sigma(r_1, r_2)$. Then the inner product of the $2n$-long vectors remains unchanged (i.e. $\langle (\ell'_1, \ell'_2), (r'_1, r'_2) \rangle = \langle (\ell_1, \ell_2), (r_1, r_2) \rangle$), and therefore $\langle \ell_1, r_1 \rangle + \langle \ell_2, r_2 \rangle = \langle \ell'_1, r'_1 \rangle + \langle \ell'_2, r'_2 \rangle$, which means that $x'_1 + x'_2 = x_1 + x_2$ (where x'_1 and x'_2 are the results of decoding the manipulated encodings). Since $\langle \ell'_1, r'_1 \rangle$ is uniformly random, thus one can think of this attack as $(x'_1, x'_2) := (x_1 + Z, x_2 - Z)$ for some random Z. Fortunately, the non-malleable codes are obliviously secure against attacks that add and subtract constants to the different parts of the encoding. Nevertheless, this example indicates that analyzing all possible strategies of the adversary may be non-trivial.

In Section 5 we characterize all such strategies by dividing them into classes. Very roughly speaking, it turns out that the attacks described above are examples of attacks from each of these classes. Namely: the adversary can either make x'_1 depend only on x_1 and x'_2 on x_2 (this case is denoted $\mathcal{D}_{\mathsf{id}}$), or x'_1 depend on x_2 and x'_2 on x_1 (case $\mathcal{D}_{\mathsf{swap}}$), or make both x'_1 and x'_2 depend *only* on x_1 (case $\mathcal{D}_{\mathsf{forget},2}$) or only on x_2 (case $\mathcal{D}_{\mathsf{forget},1}$). He can also make x'_1 depend in an arbitrary way on x_1, x_2 and x'_2 (case $\mathcal{D}_{\mathsf{unif},2}$).This comes at a cost of making x_1, x_2 and x'_2 uniform and independent (note that the "$(x'_1, x'_2) := (x_1 + Z, x_2 - Z)$" attack falls into this category). Symmetrically, he can make x'_2 depend in an arbitrary way on x_1, x_2 and x'_1 (case $\mathcal{D}_{\mathsf{unif},1}$).

What remains is to prove security of the non-malleable codes when the adversary can perform the attacks from classes $\mathcal{D}_{\mathsf{id}}, \mathcal{D}_{\mathsf{swap}}, \mathcal{D}_{\mathsf{forget},1}, \mathcal{D}_{\mathsf{forget},2}, \mathcal{D}_{\mathsf{unif},1}$, and $\mathcal{D}_{\mathsf{unif},2}$. This is done in Section 6. In order to handle the cases $\mathcal{D}_{\mathsf{unif},1}$, and $\mathcal{D}_{\mathsf{unif},2}$ we need to modify our construction slightly. Namely, we make the leakage-resilient encoding "sparse" in the sense that a decoding of random codeword with overwhelming probability yields $\perp$ (this is slightly reminiscent of the construction of [DKO13] where a similar technique was used to construct the non-malleable codes for 1-bit messages). This is achieved by requiring that the decoded value has to be in some sparse subset of $\mathbb{F}$ of size $q' \ll |\mathbb{F}|$. It will be convenient to define this set as the set of all x's such that $\psi(x) \leq q'$, where $\psi : \mathbb{F} \to [q]$ is an arbitrary bijection. The technical details follow.

Our construction Let n be an integer, and let $\mathbb{F} = \mathbb{F}_q$ be a finite field, and let $q' < q$ be an integer. Let $\prec$ be a total order on $\mathbb{F}$, and let $\psi : \mathbb{F} \to [q]$ be a bijection such that $a \prec b$ if and only $\psi(a) < \psi(b)$, for all $a, b \in \mathbb{F}$. Define the "leakage-resilient" decoding function $\mathsf{Dec}_{\mathsf{LR}} : \mathbb{F}^{2n} \times \mathbb{F}^{2n} \to [q'] \times [q'] \cup \{\perp\}$

as follows:

$$\mathsf{Dec}_{\mathsf{LR}}\left((\ell_1,\ell_2),\ (r_1,r_2)\right) = \begin{cases} \perp & \text{if } \psi(\langle \ell_1, r_1\rangle) > q',\ \text{or } \psi(\langle \ell_2, r_2\rangle) > q' \\ (\psi(\langle \ell_1, r_1\rangle)\ ,\ \psi(\langle \ell_2, r_2\rangle)) & \text{otherwise.} \end{cases}$$

We then define $\mathsf{Enc}_{\mathsf{LR}} : [q'] \times [q'] \to \mathbb{F}^{2n} \times \mathbb{F}^{2n}$ as follows: for any $x \in [q'] \times [q']$, $\mathsf{Enc}_{\mathsf{LR}}(x)$ is a random element y in $\mathbb{F}^{2n} \times \mathbb{F}^{2n}$, such that $\mathsf{Dec}_{\mathsf{LR}}(y) = x$. The following is our main result. The proof is given in Section 6.

Theorem 4.1. *Let $(\mathsf{Enc}_{\mathsf{NM}}, \mathsf{Dec}_{\mathsf{NM}})$ be an ε-non-malleable code from $\{0,1\}^k$ to $[q'] \times [q']$ in the split-state model (for any $\varepsilon \in (0, 1/10)$) where $\mathsf{Dec}_{\mathsf{NM}}$ is a symmetric function. Let $(\mathsf{Enc}_{\mathsf{LR}}, \mathsf{Dec}_{\mathsf{LR}})$ be as above, with $q \geq \frac{q'}{\varepsilon}$. Then for any $\gamma < \frac{1}{12}$ the encoding scheme $(\mathsf{Enc}_{\mathsf{LR}} \circ \mathsf{Enc}_{\mathsf{NM}}, \mathsf{Dec}_{\mathsf{NM}} \circ \mathsf{Dec}_{\mathsf{LR}})$ is an efficient 3ε-non-malleable γ-leakage resilient code in the split-state model from $\{0,1\}^k$ to $\mathbb{F}_q^n \times \mathbb{F}_q^n$, where $n = O\left(\frac{1}{1/12-\gamma}\right)$.*

Thus, using the result of [ADL14, Agg14], we get the following result.

Corollary 4.2. *For any $\gamma < \frac{1}{12}$ and any $\varepsilon \in (0, 3/10)$, there exists an efficient γ-leakage-resilient ε-non-malleable code in the split-state model from k-bit messages to $\Theta\left(\frac{(k+\log(1/\varepsilon))^7}{1/12-\gamma}\right)$-bit codewords.*

Also, we get the following stronger result by combining Theorem 4.1 with an upcoming result [ADKO14], which gives a constant-rate non-malleable code in the split-state model.

Corollary 4.3. *For any $\gamma < \frac{1}{12}$ and any $\varepsilon \in (0, 3/10)$, there exists an efficient γ-leakage-resilient ε-non-malleable code in the split-state model from k-bit messages to $\Theta\left(\frac{k+\log(1/\varepsilon)}{1/12-\gamma}\right)$-bit codewords.*

5 The joint distribution of $\phi_{f,g}(L, R)$

Before we proceed to the proof of Theorem 4.1 we need some auxiliary machinery that will allow us the characterize how a distribution of $\langle f_1(L_1, L_2), g_1(R_1, R_2)\rangle, \langle f_2(L_1, L_2), g_2(R_1, R_2))\rangle$ can depend on the distribution of $\langle L_1, R_1\rangle, \langle L_2, R_2\rangle$ (for arbitrary functions f_1, f_2, g_1, and g_2). Let $\mathbb{F} = \mathbb{F}_q$ be a finite field. Let $(L_1, L_2), (R_1, R_2)$ be independent and distributed uniformly over $\mathcal{L}, \mathcal{R} \subseteq \mathbb{F}^{2n}$, respectively. Let $f_1, g_1, f_2, g_2 : \mathbb{F}^n \times \mathbb{F}^n \to \mathbb{F}^n$ be a pair of functions. We consider the following family of distributions

$$\phi_{f,g}(L, R) := (\langle L_1, R_1\rangle, \langle L_2, R_2\rangle, \langle f_1(L_1, L_2), g_1(R_1, R_2)\rangle, \langle f_2(L_1, L_2), g_2(R_1, R_2))\rangle \in \mathbb{F}^4\ ,$$

In this section, we analyze the possible joint distribution of $\phi_{f,g}(L, R)$ over $\mathbb{F}^4$ for arbitrary functions f_1, g_1, f_2, g_2. First, define the following set of distributions (which were already informally discussed in Section 4).

- $\mathcal{D}_{\mathsf{id}} := \{(U_1, U_2, h_1(U_1, Z), h_2(U_2, Z))\}$, where h_1, h_2 are functions from $\mathbb{F} \times \mathcal{Z}$ to $\mathbb{F}$, U_1, U_2 are independent and uniform in $\mathbb{F}$, and $Z \in \mathcal{Z}$ is some random variable independent of U_1, U_2.
- $\mathcal{D}_{\mathsf{swap}} := \{(U_1, U_2, h_1(U_2, Z), h_2(U_1, Z))\}$, where h_1, h_2 are functions from $\mathbb{F} \times \mathcal{Z}$ to $\mathbb{F}$, U_1, U_2 are independent and uniform in $\mathbb{F}$, and $Z \in \mathcal{Z}$ is some random variable independent of U_1, U_2.
- $\mathcal{D}_{\mathsf{unif},1} := \{(U_1, U_2, U_3, W)\}$, where U_1, U_2, U_3 are independent and uniform in $\mathbb{F}$, and W is a random variable over $\mathbb{F}$ arbitrarily correlated to U_1, U_2, U_3.

- $\mathcal{D}_{\mathsf{unif},2} := \{(U_1, U_2, W, U_3)\}$, where U_1, U_2, U_3 are independent and uniform in $\mathbb{F}$, and W is a random variable over $\mathbb{F}$ arbitrarily correlated to U_1, U_2, U_3.
- $\mathcal{D}_{\mathsf{forget},1} := \{(U_1, U_2, h_1(U_2, Z), h_2(U_2, Z))\}$, where h_1, h_2 are functions from $\mathbb{F} \times \mathcal{Z}$ to $\mathbb{F}$, U_1, U_2 are independent and uniform in $\mathbb{F}$, and $Z \in \mathcal{Z}$ is some random variable independent of U_1, U_2.
- $\mathcal{D}_{\mathsf{forget},2} := \{(U_1, U_2, h_1(U_1, Z), h_2(U_1, Z))\}$, where h_1, h_2 are functions from $\mathbb{F} \times \mathcal{Z}$ to $\mathbb{F}$, U_1, U_2 are independent and uniform in $\mathbb{F}$, and $Z \in \mathcal{Z}$ is some random variable independent of U_1, U_2.

Define $\mathcal{D}$ to be the family of convex combinations of

$$\mathcal{D}_{\mathsf{id}} \cup \mathcal{D}_{\mathsf{swap}} \cup \mathcal{D}_{\mathsf{unif},1} \cup \mathcal{D}_{\mathsf{unif},2} \cup \mathcal{D}_{\mathsf{forget},1} \cup \mathcal{D}_{\mathsf{forget},2} \ .$$

We show that for any f, g, the value of $\phi_{f,g}(L, R)$ is statistically close to some distribution in $\mathcal{D}$ if $\mathcal{L}, \mathcal{R}$ have size at least $q^{2n(1-\gamma)}$.

Theorem 5.1. *Let $\mathbb{F} = \mathbb{F}_q$ be a finite field with $q \geq 4$, $n \geq 48$ be an integer, and $\gamma \in [0, 1/12)$. Let $L = (L_1, L_2)$, and $R = (R_1, R_2)$ be distributed uniformly at random in sets $\mathcal{L}, \mathcal{R}$ of size at least $q^{2n(1-\gamma)}$. For any $f_1, f_2, g_1, g_2 : \mathbb{F}^{2n} \to \mathbb{F}^n$, there exists a distribution $D \in \mathcal{D}$ such that*

$$\Delta(\phi_{f,g}(L, R) \ ; \ D) \leq 7^2 \cdot 2^{-s}.$$

for any $s \leq ((\frac{1}{12} - \gamma)n - \frac{5}{4}) \log q - \frac{5}{6}$.

We give a proof of this theorem in Section 8.

6 Concluding Theorem 4.1 from Theorem 5.1

Before we present our proof, we state a result showing that non-malleable codes in 2−split state model also have the secret sharing property, i.e., that given any one part of the encoding of m, it is impossible to guess the message m. The proof of this can be found in Appendix B.

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 code 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 $(X_1^1, X_2^2) \leftarrow \mathsf{Enc}(m_1)$. Then $\Delta(X_0 \, ; \, X_1) \leq 2\varepsilon$.*

Proof of Theorem 4.1. Let $n = \left\lceil \frac{6}{1/12-\gamma} \right\rceil$. Fix the message $m \in \mathcal{M}$, and let $\mathsf{Enc}_{\mathsf{NM}}(m) = (X_1, X_2)$, and $\mathsf{Enc}_{\mathsf{LR}}(X_1, X_2) = (L, R)$. Furthermore, fix manipulation functions $f, g : \mathbb{F}^n \times \mathbb{F}^n \to \mathbb{F}^n \times \mathbb{F}^n$ and the parameter $\gamma \in [0, \frac{1}{12})$. We need to analyze the distribution Tamper_m^γ as in Definition 3.3. Before this, consider the following. Choose $\gamma' = \frac{1/12+\gamma}{2}$, so that $(1/12 - \gamma')n = (\gamma' - \gamma)n \geq 3$. Let $\tilde{L}, \tilde{R}$ be uniform in $\mathbb{F}^n$. From Lemma 2.5 we know that the min-entropies of $\tilde{L}$ and $\tilde{R}$ conditioned on the knowledge of $\mathsf{Leak}^{\mathcal{A}}(\tilde{L}, \tilde{R})$ are at least $2n \log q(1 - \gamma')$ with probability at least $1 - 2 \cdot q^{2n(\gamma-\gamma')}$. So, at the cost of at most $2 \cdot q^{2n(\gamma-\gamma')}$ in the adversary's success probability, we can restrict ourselves to the case where $\tilde{L}$ and $\tilde{R}$ are distributed over uniformly over a set of size at least $q^{2n(1-\gamma')}$. Consider the joint distribution

$$\langle \tilde{L}_1, \tilde{R}_1 \rangle, \langle \tilde{L}_2, \tilde{R}_2 \rangle, \langle f_1(\tilde{L}_1, \tilde{L}_2), g_1(\tilde{R}_1, \tilde{R}_2) \rangle, \langle f_2(\tilde{L}_1, \tilde{L}_2), g_2(\tilde{R}_1, \tilde{R}_2) \rangle \ ,$$

conditioned on the knowledge of $\mathsf{Leak}^{\mathcal{A}}(\tilde{L}, \tilde{R})$. By Theorem 5.1, this has statistical distance at most

$$49 \cdot 2^{5/6} \cdot q^{5/4-(1/12-\gamma')n} + 2 \cdot q^{2n(\gamma-\gamma')} \leq 100 q^{-7/4} \leq 100 \left(\frac{\varepsilon^2}{2^k} \right)^{7/4} \leq \frac{\varepsilon}{2^{k+1}}$$

from some distribution D in $\mathcal{D}$. Here we used that $\varepsilon < 1/10$, and $q' \geq \frac{2^k}{\varepsilon}$. This holds for any non-malleable code in the 2-split-state model. Note that for any known non-malleable code in this model (in particular, those used in Corollary 4.2, and Corollary 4.3), we have that $q' \gg \frac{2^k}{\varepsilon}$. Since D is a convex combination (depending on f, g, and $\mathcal{A}$) of distributions in $\mathcal{D}_{\mathsf{forget},1}$, $\mathcal{D}_{\mathsf{forget},2}$, $\mathcal{D}_{\mathsf{unif},1}$, $\mathcal{D}_{\mathsf{unif},2}$, $\mathcal{D}_{\mathsf{id}}$, and $\mathcal{D}_{\mathsf{swap}}$, without loss of generality we will analyze the distribution $\mathsf{Tamper}^{\gamma}_{m}$ under the assumption that D belongs to one of these sets. Hence, we consider the following cases.

$D \in \mathcal{D}_{\mathsf{forget},1}$**:** In this case, D is of the form $U_1, U_2, h_1(U_2, Z), h_2(U_2, Z)$, where U_1, U_2 are independent and uniform in $\mathbb{F}$, and Z is independent of U_1, U_2. Of course, in our case L_1, R_1, L_2 and R_2 are not entirely uniform and independent, as they are a random encoding of a fixed message m. To take it into account we use Lemma 2.4, that states that in this case the statistical distance gets mutiplied by 2 divided by the probability that a random message M is equal to m (which is equal to 2^{-k}). Hence, we get that $\mathsf{Tamper}^{\gamma}_{m}$ has statistical distance at most

$$2^{k+1} \cdot \frac{\varepsilon}{2^{k+1}} = \varepsilon$$

from

$$V_1 = \mathsf{Dec}_{\mathsf{NM}}\left(\psi\left(h_1\left(\psi^{-1}\left(X_2\right), Z\right)\right), \psi\left(h_2\left(\psi^{-1}\left(X_2\right), Z\right)\right)\right) \ ,$$

where $\mathsf{Enc}_{\mathsf{NM}}(m) = (X_1, X_2)$, and Z is independent of X_1, X_2. Since V_1 is independent of X_1, using Lemma 6.1 we get the desired result (as X_2 cannot carry enough information to make V_1 dependent on m.

$D \in \mathcal{D}_{\mathsf{forget},2}$**:** This case is similar to the previous one.

$D \in \mathcal{D}_{\mathsf{unif},1}$**:** In this case, D is of the form U_1, U_2, U_3, W, where U_1, U_2, U_3 are independent and uniform in $\mathbb{F}$, and $W \in \mathbb{F}$ is arbitrarily correlated to U_1, U_2, U_3. Again, by Lemma 2.4, this implies that $\mathsf{Tamper}^{\gamma}_{m}$ has statistical distance at most

$$2^{k+1} \cdot \frac{\varepsilon}{2^{k+1}} = \varepsilon$$

from

$$V_2 = \mathsf{Dec}_{\mathsf{NM}}\left(\psi\left(U_3\right), W'\right) \ ,$$

where $\mathsf{Enc}_{\mathsf{NM}}(m) = (X_1, X_2)$, U_3 is uniform and independent in $\mathbb{F}$, W' is arbitrarily correlated to X_1, X_2, U_3. Note that $\psi(U_3) = \perp$ with probability $1 - q'/q$. Thus, $\mathsf{Tamper}^{\gamma}_{m}$ has statistical distance at most $\varepsilon + q'/q \leq 2\varepsilon$ from $\perp$.

$D \in \mathcal{D}_{\mathsf{unif},2}$**:** This case is similar to the previous one.

$D \in \mathcal{D}_{\mathsf{id}}$**:** In this case, D is of the form $U_1, U_2, h_1(U_1, Z), h_2(U_2, Z)$, where U_1, U_2 are independent and uniform in $\mathbb{F}$, and Z is independent of U_1, U_2. By Lemma 2.4, this implies that $\mathsf{Tamper}^{\gamma}_{m}$ has statistical distance at most

$$2^{k+1} \cdot \frac{\varepsilon}{2^{k+1}} = \varepsilon$$

from

$$V_3 = \mathsf{Dec}_{\mathsf{NM}}\left(\psi\left(h_1\left(\psi^{-1}\left(X_1\right), Z\right)\right), \psi\left(h_2\left(\psi^{-1}\left(X_2\right), Z\right)\right)\right) \ ,$$

where $\mathsf{Enc}_{\mathsf{NM}}(m) = (X_1, X_2)$, and Z is independent of X_1, X_2. It is easy to see that V_3 is ε-close to Sim_m by the ε-non-malleability of $(\mathsf{Enc}_{\mathsf{NM}}, \mathsf{Dec}_{\mathsf{NM}})$.

$D \in \mathcal{D}_{\mathsf{swap}}$**:** Using the fact that the decoding function is symmetric, this case is similar to the previous one.

□

7 Existential Result using [CG14b]

Cheraghchi and Guruswami [CG14b] introduced the notion of seedless non-malleable extractors as a step towards constructing non-malleable codes defined as follows.

Definition 7.1. *A function* $\mathsf{NMExt} : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^k$ *is a two-source non-malleable* (m, ε)*-extractor if, for every pair of independent random variables* X, Y *over* $\{0,1\}^n$ *such that* $\mathbf{H}_\infty(X) \geq m$*, and for any functions* $f, g : \{0,1\}^n \to \{0,1\}^n$*, there exists a distribution* D *over* $\{0,1\}^k \cup \{\mathsf{same}\}$*, such that*

$$\Delta(\mathsf{NMExt}(X,Y), \mathsf{NMExt}(f(X), g(Y)\ ;\ U_k, \mathsf{copy}(D, U_k)) \leq \varepsilon\ ,$$

where U_k *is uniformly random in* $\{0,1\}^k$*, and* $\mathsf{copy}(D, U_k) = U_k$ *if* $D = \mathsf{same}$*, and* D*, otherwise.*

It was shown in [CG14b] that assuming the existence of non-malleable extractors with $m = n$ immediately gives non-malleable codes with good rate. We observe that their proof easily extends to show that non-malleable extractors with small m implies non-malleable codes with good rate that also tolerate large amount of leakage.

Theorem 7.2. *Let* $\mathsf{NMExt} : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^k$ *be a two-source non-malleable* (m, ε)*-extractor. Define a coding scheme* $(\mathsf{Enc}, \mathsf{Dec})$ *with message length* k *and block length* $2n$ *as follows. The decoder* Dec *is defined as* $\mathsf{Dec}(x, y) := \mathsf{NMExt}(x, y)$*.*

The encoder, given a message s*, outputs a uniformly random element* (X, Y) *in* $\{0,1\}^n \times \{0,1\}^n$ *such that* $\mathsf{Dec}(X, Y) = s$*. Then the pair* $(\mathsf{Enc}, \mathsf{Dec})$ *is* $(\varepsilon \cdot (2^k + 1)$*-non-malleable,* $1 - \frac{m}{n})$*-leakage-resilient code against split-state tampering.*

We now mention the result from [CG14b] showing the existence of non-malleable codes.

Theorem 7.3. *Let* $\mathsf{NMExt} : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^k$ *be a random function. For any* $\varepsilon, \delta > 0$*, and* $m \leq n$*, with probability at least* $1 - \delta$*, the function* NMExt *is a two-source non-malleable extractor provided that*

$$m \geq \max(k + \frac{3}{2} \cdot \log 1/\varepsilon + \frac{1}{2} \log\log(1/\delta)\ ,\ \log n + \log\log(1/\delta) + O(1))\ .$$

Combining Theorem 7.2 and Theorem 7.3 gives us the following corollary.

Corollary 7.4. *Let* $n = \mathsf{poly}(k)$*, and let* $\mathsf{NMExt} : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^k$ *be a random function. With probability at least* $1 - \frac{1}{2^{2^k}}$*, the scheme* $(\mathsf{NMExt}^{-1}, \mathsf{NMExt})$ *is* 2^{-k}*-non-malleable,* $1 - \frac{5k}{n}$*-leakage-resilient.*

This implies that with probability very close to 1, a random function is an excellent leakage-resilient non-malleable code, and we can arbitrarily increase the amount of leakage (upto the total length of each part) at the cost of increasing the length of the codeword.

8 Proof of Theorem 5.1

8.1 The general strategy

Our strategy is to divide $\mathcal{L} \times \mathcal{R}$ into several disjoint parts, and prove that $\phi_{f,g}(L, R)$ is close to some distribution in $\mathcal{D}$ for each of these parts separately. Let $L = (L_1, L_2)$, and $R = (R_1, R_2)$. Also, let $|\mathbb{F}| = q$, and $\tau = 1 - \gamma$. The following simple lemma shows that it suffices to bound the statistical distance between $\phi_{f,g}(L, R)$ and some distribution in $\mathcal{D}$ for (L, R) restricted to partitions of $\mathcal{L} \times \mathcal{R}$. This was shown in [ADL14].

Lemma 8.1. *Let $\mathcal{S} \subseteq \mathcal{L} \times \mathcal{R}$. Let $\mathcal{S}_1, \ldots, \mathcal{S}_k$ be a partition of $\mathcal{S}$. Also, let $D_1, \ldots, D_k$ be some distribution in $\mathcal{D}$. Assume that for all $1 \leq i \leq k$,*

$$\Delta\left(\phi_{f,g}(L,R)|_{(L,R)\in\mathcal{S}_i} \;;\; D_i\right) \leq \varepsilon_i \;.$$

Then there exists a distribution $D \in \mathcal{D}$ such that

$$\Delta\left(\phi_{f,g}(L,R)|_{(L,R)\in\mathcal{S}} \;;\; D\right) \leq \sum \varepsilon_i \frac{|\mathcal{S}_i|}{|\mathcal{S}|} \;.$$

We construct a partition of $\mathcal{L} \times \mathcal{R}$ in Section 8.2. Then in Sections 8.3.1—8.3.4 we analyze the behavior of $\phi_{f,g}(L,R)$ on the constructed parts. Finally, in Section 8.4 we show how to combine the facts proven in previous sections in order to obtain the statement of the theorem.

8.2 Partitioning the set $\mathcal{L} \times \mathcal{R}$.

We next define a partitioning of $\mathcal{L} \times \mathcal{R}$ based on f and g to which we will apply Lemma 8.1. This is done independently for $\mathcal{L}$ and $\mathcal{R}$ and hence we will focus only on $\mathcal{L}$ (the partitioning of $\mathcal{R}$ is done analogously). On a high level, our partitioning is constructed as follows: first we partition $\mathcal{L}$ into sets $\mathcal{L}_{\mathsf{ffb},1}, \mathcal{L}_{\mathsf{ffb},2}$, and $\mathcal{L}_1$. Then we partition $\mathcal{L}_1$ into $\mathcal{L}_{\mathsf{mix},1}, \mathcal{L}_{\mathsf{mix},2}$, and $\mathcal{L}_2$. Finally, we partition $\mathcal{L}_2$ into $\mathcal{L}_{\mathsf{id}}, \mathcal{L}_{\mathsf{swap}}$, and $\mathcal{L}_{\mathsf{rem}}$ (the meaning of the acronyms in the subscripts should become clear when the sets are defined). Altogether, we partition $\mathcal{L}$ into 7 sets $\mathcal{L}_{\mathsf{ffb},1}, \mathcal{L}_{\mathsf{ffb},2}, \mathcal{L}_{\mathsf{mix},1}, \mathcal{L}_{\mathsf{mix},2}, \mathcal{L}_{\mathsf{id}}, \mathcal{L}_{\mathsf{swap}}$, and $\mathcal{L}_{\mathsf{rem}}$.

Let $\beta_1 = \frac{1}{3}n\log q - 4(\tau - \frac{11}{12})n\log q + 4\log q + 4s + 4$, and let $\beta_2 = \frac{1}{3}n\log q - 4(\tau - \frac{11}{12})n\log q + 6\log q + 3s + 2$. We first partition $\mathcal{L}$ into $\mathcal{L}_{\mathsf{ffb},1}, \mathcal{L}_{\mathsf{ffb},2}$, and $\mathcal{L}_1$. Recall that the elements of $\mathcal{L}$ are pairs $(\ell_1, \ell_2) \in \mathbb{F}^n \times \mathbb{F}^n$. Intutively $\mathcal{L}_{\mathsf{ffb},i}$ (for $i \in \{1,2\}$) will consist of the elements of $\mathcal{L}$ on which the function f is "far from a bijection", by which we mean that it "glues" at least $2^{\beta_1/2}$ elements on the ith component (cf. Steps 2 and 3 below). The set $\mathcal{L}_1$ will consists of the remaining elements (i.e. those that are "close to the bijection"). Since we want $\mathcal{L}_{\mathsf{ffb},1}, \mathcal{L}_{\mathsf{ffb},2}$, and $\mathcal{L}_1$ to be a partition, thus $\mathcal{L}_{\mathsf{ffb},1}$ and $\mathcal{L}_{\mathsf{ffb},2}$ have to be disjoint. Hence we first construct $\mathcal{L}_{\mathsf{ffb},1}$, and then, using the same method we construct $\mathcal{L}_{\mathsf{ffb},2}$, but in this construction we consider only ℓ's that belong to $\mathcal{L}^* := \mathcal{L} \setminus \mathcal{L}_{\mathsf{ffb},1}$. The set $\mathcal{L}_1$ consits of the elements of $\mathcal{L}$ that were not included in $\mathcal{L}_{\mathsf{ffb},1}$ or $\mathcal{L}_{\mathsf{ffb},2}$. To avoid repetition, we present the procedures for constructing $\mathcal{L}_{\mathsf{ffb},1}$ and $\mathcal{L}_{\mathsf{ffb},2}$ as one algorithm, whose behaviour depends on i. This algorithm, presented below, is executed first for $i = 1$ and then for $i = 2$.

1. Initialize $\mathcal{L}_{\mathsf{ffb},i}$ to be empty, and let $\mathcal{L}^* := \mathcal{L}$ if $i = 1$, and $\mathcal{L}^* := \mathcal{L} \setminus \mathcal{L}_{\mathsf{ffb},1}$, otherwise.
2. Let $\mathcal{W}$ be a largest subset of $\mathcal{L}^*$ such that for any two $\ell, \ell' \in \mathcal{W}$ it holds that $\ell_i \neq \ell'_i$, and $f(\ell) = f(\ell')$.
3. If $|\mathcal{W}| \geq 2^{\beta_1/2}$, then set $\mathcal{L}^* = \mathcal{L}^* \setminus \mathcal{W}$, set $\mathcal{L}_{\mathsf{ffb},i} = \mathcal{L}_{\mathsf{ffb},i} \cup \mathcal{W}$, and go to Step 2.
4. Return $\mathcal{L}_{\mathsf{ffb},i}$.

The set $\mathcal{L}_1$ is defined to be

$$\mathcal{L}_1 = \mathcal{L} \setminus (\mathcal{L}_{\mathsf{ffb},1} \cup \mathcal{L}_{\mathsf{ffb},2}) \;.$$

The justification for this choice is that for $\tilde{L}$ chosen uniformly at random from $\mathcal{L}_{\mathsf{ffb},i}$, we have

$$\mathbf{H}_\infty(\tilde{L}_i | f(\tilde{L}) = y) \geq \frac{\beta_1}{2} \;,$$

where $y := f(\tilde{L})$ (this is because the number of pre-images of y under f, projected on the ith component, is at least $2^{\beta_1/2}$). Also, we have that for any $y \in \mathbb{F}^n$, the total number of elements $\ell \in \mathcal{L}_1$ such that $f(\ell) = y$ is at most $\left(2^{\frac{\beta_1}{2}}\right)^2 = 2^{\beta_1}$.

Recall that every $f : \mathbb{F}^n \times \mathbb{F}^n \to \mathbb{F}^n \times \mathbb{F}^n$ can be represened as a pair of functions $f_1, f_2 : \mathbb{F}^n \times \mathbb{F}^n \to \mathbb{F}^n$ defined as $(f_1(\ell), f_2(\ell)) := f(\ell)$. We further partition the set $\mathcal{L}_1$ depending on how $f_1(\ell), f_2(\ell)$ depend on ℓ_1, ℓ_2 for $\ell \in \mathcal{L}_1$. We will now define partitioning of $\mathcal{L}_1$. Before we do it, let us state the following auxiliary definition (note that it is defined for $\mathcal{L}$, not for $\mathcal{L}_1$).

Definition 8.2. *Define $T^{i\to j} \subset \mathcal{L}$ for $i, j \in \{1, 2\}$, as the set of all elements $\ell \in \mathcal{L}$ such that*

$$\left|\left\{\ell^* \in \mathcal{L} \;\middle|\; \ell_i = \ell_i^* \text{ and } f_j(\ell) = f_j(\ell^*)\right\}\right| \geq \frac{q^n}{2^{\beta_2}} .$$

Let us now prove the following simple result justifying the definition of $T^{i\to j}$. Intuitively, this result shows that for every $\ell \in T^{i\to j}$, the value of $f_j(\ell)$ can be computed given ℓ_i and a little more information.

Lemma 8.3. *Let $\ell \in T^{i\to j}$ for some $i, j \in [t]$. Then there exists some functions $a_{i,j} : T^{i\to j} \mapsto \{0,1\}^{\beta_2}$ and $\psi_{i,j} : \mathbb{F}^n \times \{0,1\}^{\beta_2} \mapsto \mathbb{F}^n$ such that for all $\ell \in T^{i\to j}$,*

$$f_j(\ell) = \psi_{i,j}(\ell_i, a_{i,j}(\ell)) .$$

Proof. Given $\ell \in T^{i\to j}$, let $T' = \{\ell^* \in T^{i\to j} \mid \ell_i^* = \ell_i\}$. Then, clearly $|T'| \leq |\mathbb{F}^n| = q^n$. Consider a partition of T' into sets $T'_1, \ldots, T'_m$ according to the value of function f_j. More formally, for any $u, v \in [m]$, and any $\ell' \in T'_u$, $\ell'' \in T'_v$, we have that $f_j(\ell') = f_j(\ell'')$ if and only if $u = v$. By definition of $T^{i\to j}$, we have that $|T'_u| \geq \frac{q^n}{2^{\beta_2}}$ for all $u \in [m]$. Thus

$$m \leq \frac{|T'| \cdot 2^{\beta_2}}{q^n} \leq 2^{\beta_2} .$$

We define $a_{i,j}(\ell)$ as the binary representation of k such that $\ell \in T'_k$. Now, it is easy to see that we can determine $f_j(\ell)$ given ℓ_i and $a_{i,j}(\ell)$. □

We now define disjoint subsets $\mathcal{L}_{\mathsf{mix},1}, \mathcal{L}_{\mathsf{mix},2} \subseteq \mathcal{L}_1$ as follows.

$$\mathcal{L}_{\mathsf{mix},1} := \left\{\ell \in \mathcal{L}_1 \;\middle|\; \ell \notin T^{1\to 1} \cup T^{2\to 1}\right\} ,$$

$$\mathcal{L}_{\mathsf{mix},2} := \left\{\ell \in \mathcal{L}_1 \setminus \mathcal{L}_{\mathsf{mix},1} \;\middle|\; \ell \notin T^{1\to 2} \cup T^{2\to 2}\right\} .$$

Informally speaking, $\ell \in \mathcal{L}_{\mathsf{mix},j}$ implies that $f_j(\ell)$ depends on both ℓ_1 and ℓ_2. Now, let

$$\mathcal{L}_2 := \mathcal{L}_1 \setminus (\mathcal{L}_{\mathsf{mix},1} \cup \mathcal{L}_{\mathsf{mix},2}) .$$

We denote $\mathcal{T}(\ell, i)$ to be the set of $j \in \{1, 2\}$ such that $\ell \in T^{i\to j}$. Note that by the definition of $\mathcal{L}_{\mathsf{mix},j}$, for any $\ell \in \mathcal{L}_2$ we have that $\mathcal{T}(\ell, 1) \cup \mathcal{T}(\ell, 2) = \{1, 2\}$. We further partition $\mathcal{L}_2$ into $\mathcal{L}_{\mathsf{id}}$, $\mathcal{L}_{\mathsf{swap}}$, and $\mathcal{L}_{\mathsf{rem}}$ as follows.

$$\mathcal{L}_{\mathsf{id}} := \left\{\ell \in \mathcal{L}_2 \;\middle|\; \mathcal{T}(\ell, 1) = \{1\},\ \mathcal{T}(\ell, 2) = \{2\}\right\} ,$$

$$\mathcal{L}_{\mathsf{swap}} := \left\{\ell \in \mathcal{L}_2 \setminus \mathcal{L}_{\mathsf{id}} \;\middle|\; \mathcal{T}(\ell, 1) = \{2\},\ \mathcal{T}(\ell, 2) = \{1\}\right\} ,$$

and

$$\mathcal{L}_{\mathsf{rem}} := \mathcal{L}_2 \setminus (\mathcal{L}_{\mathsf{id}} \cup \mathcal{L}_{\mathsf{swap}}) .$$

The partitioning of $\mathcal{R}$ is defined similarly. We will later consider the partitions of $\mathcal{L} \times \mathcal{R}$ to be the product of individual partitions of $\mathcal{L}$ and $\mathcal{R}$ (hence, at the end $\mathcal{L} \times \mathcal{R}$ is partitioned into 7^2 parts).

8.3 Analyzing the parts

We will argue that for any part, either its probability is small, or $\phi_{f,g}(L,R)$ conditioned on (L,R) belonging to it, is close to some distribution in $\mathcal{D}$. We then apply Lemma 8.1 to obtain a proof of Theorem 5.1.

8.3.1 Case: "f or g is far from bijection"

Lemma 8.4. *For $i = 1, 2$, and $\mathcal{R}^* \subset \mathcal{R}$, if $|\mathcal{L}_{\mathsf{ffb},i} \times \mathcal{R}^*| \geq q^{4\tau n} \cdot 2^{-s}$ then there exists a distribution D that is a convex combination of distributions in $\mathcal{D}_{\mathsf{forget},i}$ such that*

$$\Delta(\phi_{f,g}(L,R)|_{(L,R)\in\mathcal{L}_{\mathsf{ffb},i}\times\mathcal{R}^*}\ ; D) \leq 2^{-s}\ .$$

Proof. Without loss of generality, let $i = 1$, and let $|\mathcal{L}_{\mathsf{ffb},1} \times \mathcal{R}| \geq q^{4\tau n} \cdot 2^{-s}$. Let $\tilde{L}, \tilde{R}$ be distributed uniformly over $\mathcal{L}_{\mathsf{ffb},1}$ and $\mathcal{R}^*$ respectively. Note that by the assumption we have that $|\mathcal{L}_{\mathsf{ffb},1}| \geq q^{2\tau n} \cdot 2^{-s}$ and $|\mathcal{R}^*| \geq q^{2\tau n} \cdot 2^{-s}$. Thus,

$$\mathbf{H}_\infty(\tilde{L}_1) \geq (2\tau - 1)n \log q - s \quad \text{and} \quad \mathbf{H}_\infty(\tilde{L}_2|\tilde{L}_1) \geq (2\tau - 1)n \log q - s\ , \tag{8.5}$$

and

$$\mathbf{H}_\infty(\tilde{R}_1) \geq (2\tau - 1)n \log q - s \quad \text{and} \quad \mathbf{H}_\infty(\tilde{R}_2|\tilde{R}_1) \geq (2\tau - 1)n \log q - s\ . \tag{8.6}$$

Denote $\langle \tilde{L}_k, \tilde{R}_k \rangle$ by X_k, and $\langle f_k(\tilde{L}), g_k(\tilde{R}) \rangle$ by X'_k for $k = 1, 2$. We have that

$$\mathbf{H}_\infty(\tilde{L}_1|X_2, f(\tilde{L})) \geq \frac{\beta_1}{2} - \log q\ .$$

Also, using Lemma 2.5, we get that $\tilde{L}$ and $\tilde{R}$ (and hence $\tilde{L}_1$ and $\tilde{R}_1$) are independent given $f(\tilde{L})$, $\tilde{R}_2$, and X_2. Thus, using the fact that Ext is a strong two-source extractor, we have that

$$X_1, \tilde{R}_1, X_2, f(\tilde{L}), \tilde{R}_2 \approx_{2^{-(s+1)}} U_1, \tilde{R}_1, X_2, f(\tilde{L}), \tilde{R}_2\ ,$$

where U_1 is uniformly random in $\mathbb{F}$. This implies that

$$X_1, X_2, X'_1, X'_2 \approx_{2^{-(s+1)}} U_1, X_2, X'_1, X'_2\ . \tag{8.7}$$

Now, X'_1, X'_2 are independent of U_1, and can be seen as a randomized function of X_2. Let

$$U_1, X_2, X'_1, X'_2 \equiv U_1, X_2, h_1(X_2, Z), h_2(X_2, Z)\ ,$$

for Z independent of U_1, X_2. Using Equation 8.5 and 8.6, and that Ext is a two-source randomness extractor, we have that X_2 is $2^{-(s+1)}$-close to uniform. Thus, using equation triangle inequality, we get that

$$X_1, X_2, X'_1, X'_2 \approx_{2^{-s}} U_1, U_2, h_1(U_2, Z), h_2(U_2, Z)\ ,$$

which implies the result. □

In a symetric way we can prove the following.

Lemma 8.8. *For $i = 1, 2$, and $\mathcal{L}^* \subset \mathcal{L}$, if $|\mathcal{L}^* \times \mathcal{R}_{\mathsf{ffb},i}| \geq q^{4\tau n} \cdot 2^{-s}$ then there exists a distribution D that is a convex combination of distributions in $\mathcal{D}_{\mathsf{forget},i}$ such that*

$$\Delta(\phi_{f,g}(L,R)|_{(L,R)\in\mathcal{L}^*\times\mathcal{R}_{\mathsf{ffb},i}}\ ; D) \leq 2^{-s}\ .$$

8.3.2 Case: "output of f or g is mixed"

Lemma 8.9. *For $j = 1, 2$, and $\mathcal{R}^* \subset \mathcal{R}$, if $|\mathcal{L}_{\mathsf{mix},j} \times \mathcal{R}^*| \geq q^{4\tau n} \cdot 2^{-s}$ then there exists a distribution D that is a convex combination of distributions in $\mathcal{D}_{\mathsf{unif},j}$, such that*

$$\Delta(\phi_{f,g}(L,R)|_{(L,R)\in\mathcal{L}_{\mathsf{mix},j}\times\mathcal{R}^*} \ ; D) \leq 2^{-s} \ .$$

Proof. Let us assume that $|\mathcal{L}_{\mathsf{mix},1} \times \mathcal{R}^*| \geq q^{4\tau n} \cdot 2^{-s}$. (Case $j = 2$ is analogous.) From the assumptions we have that $|\mathcal{L}_{\mathsf{mix},1}| \geq q^{2\tau n} \cdot 2^{-s}$ and $|\mathcal{R}^*| \geq q^{2\tau n} \cdot 2^{-s}$. Let $\tilde{L}, \tilde{R}$ be distributed uniformly over $\mathcal{L}_{\mathsf{mix},1}$ and $\mathcal{R}^*$ respectively. Denote $\mathsf{Ext}(\tilde{L}_k, \tilde{R}_k)$ by X_k, and $\langle f_k(\tilde{L}), g_k(\tilde{R})\rangle$ by X'_k for $k = 1, 2$. Reasoning similarly as in Lemma 8.4, we have that X_1 is $q^{-3} \cdot 2^{-(s+1)}$-close to uniform, and also X_2 is $q^{-3} \cdot 2^{-(s+1)}$-close to uniform given $\tilde{L}_1, \tilde{R}_1$, and hence using the hybrid argument, we have that

$$X_1, X_2 \approx_{2^{-s}q^{-3}} U_1, U_2 \ , \tag{8.10}$$

where U_1, U_2, are independent and uniformly distributed in $\mathbb{F}$. We now give a lower bound for $\mathbf{H}_\infty(\tilde{L}_i|f_1(\tilde{L}))$ for $i = 1, 2$ using the definition of $\mathcal{L}_{\mathsf{mix},1}$.

$$\begin{aligned}
\mathbf{H}_\infty(\tilde{L}_i|f_j(\tilde{L})) &= -\log\left(\sum_{y\in\mathbb{F}^n} \max_{\ell_i\in\mathbb{F}^n} \Pr(\tilde{L}_i = \ell_i \ \wedge f_j(\tilde{L}) = y)\right) \\
&\geq -\log\left(\sum_{y\in\mathbb{F}^n} \frac{q^n 2^{-\beta_2}}{|\mathcal{L}_{\mathsf{mix},1}|}\right) \\
&\geq -\log\left(\frac{q^{2n}2^{-\beta_2}}{q^{2\tau n}2^{-s}}\right) \geq \beta_2 - 2(1-\tau)n\log q - s \ .
\end{aligned}$$

Thus, we have that for $i = 1, 2$, X_i is $2^{-s-1}q^{-3}$-close to uniform given $f_1(\tilde{L}), \tilde{R}$, and hence,

$$\Delta\left(X_i, \mathsf{Ext}(f_1(\tilde{L}), g_1(\tilde{R})) \ ; \ U_i, \mathsf{Ext}(f_1(\tilde{L}), g_1(\tilde{R}))\right) \leq q^{-3}2^{-s-1} \ .$$

Also, since $\mathcal{L}_{\mathsf{mix},1}$ and $\mathcal{R}^*$ are in the complement of $\mathcal{L}_{\mathsf{ffb}}$, and $\mathcal{R}_{\mathsf{ffb}}$, respectively, we have that

$$\mathbf{H}_\infty(f_j(\tilde{L})) \geq \mathbf{H}_\infty(f(\tilde{L})) - n\log q \geq (2\tau - 1)n\log q - \beta_1 - s \ ,$$

and

$$\mathbf{H}_\infty(g_j(\tilde{R})) \geq (2\tau - 1)n\log q - \beta_1 - s \ .$$

This implies that

$$\Delta\left(X_i, X'_1 \ ; \ U_i, U'_1\right) \leq q^{-3} \cdot 2^{-s} \ , \tag{8.11}$$

where U'_1 is uniform in $\mathbb{F}$.
Now, we claim that

$$\Delta(X_1, X_2, X'_1 \ ; \ U_1, U_2, U'_1) \leq 2^{-s} \ . \tag{8.12}$$

If not, then by the XOR Lemma, there exist a_1, a_2, a_3, not all zero such that $a_1X_1 + a_2X_2 + a_3X'_1$ is *not* $2^{-s} \cdot q^{-3}$ close to uniform. By Equation 8.10, we have that $a_3 \neq 0$, and by equation 8.11, we have that $a_1, a_2 \neq 0$. Consider two sources in $\mathbb{F}^3$ as $(a_1\tilde{L}_1, a_2\tilde{L}_2, a_3f_1(\tilde{L}))$ and $(\tilde{R}_1, \tilde{R}_2, g_1(\tilde{R}))$. Applying Ext to these two sources gives $a_1X_1 + a_2X_2 + a_3X'_1$. The two sources have min-entropy at least $2\tau n\log q - s$, and hence $\sum_{i=1}^t a_iX_i + a_{t+1}\mathsf{Ext}(f_j(\tilde{L}), g_j(\tilde{R}))$ is $2^{-s}q^{-3}$-close to uniform, which is a contradiction. □

Symmetrically, we get that

Lemma 8.13. *For $j = 1, 2$, and $\mathcal{L}^* \subset \mathcal{L}$, if $|\mathcal{L}^* \times \mathcal{R}_{\mathsf{mix},j}| \geq q^{4\tau n} \cdot 2^{-s}$ then*

$$\Delta(\phi_{f,g}(L,R)|_{(L,R)\in\mathcal{L}^*\times\mathcal{R}_{\mathsf{mix},j}}\ ; D) \leq 2^{-s}\ ,$$

for some D that is a convex combination of distributions in $\mathcal{D}_{\mathsf{unif},j}$.

8.3.3 Case "$\tilde{L} \in \mathcal{L}_{\mathsf{id}} \cup \mathcal{L}_{\mathsf{swap}}$ and $\tilde{R} \in \mathcal{R}_{\mathsf{id}} \cup \mathcal{R}_{\mathsf{swap}}$"

Lemma 8.14. *If $|\mathcal{L}_{\mathsf{id}} \times \mathcal{R}_{\mathsf{swap}}| \geq q^{4\tau n} \cdot 2^{-s}$ then there exists a distribution D that is a convex combination of distributions in $\mathcal{D}_{\mathsf{forget},1}$ such that*

$$\Delta(\phi_{f,g}(L,R)|_{(L,R)\in\mathcal{L}_{\mathsf{id}}\times\mathcal{R}_{\mathsf{swap}}}\ ; D) \leq 2^{-s}\ .$$

Proof. This proof is almost identical to that of Lemma 8.4, except that it makes crucial use of Lemma 8.3. Let $|\mathcal{L}_{\mathsf{id}} \times \mathcal{R}_{\mathsf{swap}}| \geq q^{4\tau n} \cdot 2^{-s}$. Let $\tilde{L}, \tilde{R}$ be distributed uniformly over $\mathcal{L}_{\mathsf{id}}$ and $\mathcal{R}_{\mathsf{swap}}$ respectively. Note that by the assumption we have that $|\mathcal{L}_{\mathsf{id}}| \geq q^{2\tau n} \cdot 2^{-s}$ and $|\mathcal{R}_{\mathsf{swap}}| \geq q^{2\tau n} \cdot 2^{-s}$. Thus, for $k = 1, 2$,

$$\mathbf{H}_\infty(\tilde{L}_k|\tilde{L}_{k-1}) \geq (2\tau - 1)n \log q - s\ , \tag{8.15}$$

and

$$\mathbf{H}_\infty(\tilde{R}_k|\tilde{R}_{k-1}) \geq (2\tau - 1)n \log q - s\ , \tag{8.16}$$

where $\tilde{L}_0 = \tilde{R}_0 \equiv 0$. Denote $\langle \tilde{L}_k, \tilde{R}_k \rangle$ by X_k, and $\langle f_k(\tilde{L}), g_k(\tilde{R}) \rangle$ by X'_k for $k = 1, 2$. By Lemma 8.3, there exists maps $a_{1,1}$, $a_{2,2}$ from $\mathcal{L}_{\mathsf{id}}$ to $\{0,1\}^{\beta_2}$, and $b_{1,2}$, $b_{2,1}$ from $\mathcal{R}_{\mathsf{swap}}$ to $\{0,1\}^{\beta_2}$, such that $f_1(\tilde{L})$, $f_2(\tilde{L})$, $g_1(\tilde{R})$, $g_2(\tilde{R})$ are determined uniquely given $(\tilde{L}_1, a_{1,1}(\tilde{L}))$, $(\tilde{L}_2, a_{2,2}(\tilde{L}))$, $(\tilde{R}_2, b_{2,1}(\tilde{R}))$, $(\tilde{R}_1, b_{1,2}(\tilde{R}))$, respectively.

Also, using Lemma 2.5, we get that $\tilde{L}$ and $\tilde{R}$ (and hence $\tilde{L}_1$ and $\tilde{R}_1$) are independent given $X_2 = \langle \tilde{L}_2, \tilde{R}_2 \rangle$, X'_1, and X'_2. Thus, using the fact that Ext is a strong two-source extractor, we have that

$$X_1, \tilde{R}_1, X_2, f(\tilde{L}), \tilde{R}_2 \approx_{2^{-(s+1)}} U_1, \tilde{R}_1, X_2, f(\tilde{L}), \tilde{R}_2\ ,$$

where U_1 is uniformly random in $\mathbb{F}$. This implies that

$$X_1, X_2, X'_1, X'_2 \approx_{2^{-(s+1)}} U_1, X_2, X'_1, X'_2\ .$$

Now, X'_1, X'_2 are independent of U_1, and can be seen as a randomized function of X_2. Let

$$U_1, X_2, X'_1, X'_2 \equiv U_1, X_2, h_1(X_2, Z), h_2(X_2, Z)\ ,$$

for Z independent of U_1, X_2. Using Equation 8.15 and 8.16, and that Ext is a two-source randomness extractor, we have that X_2 is $2^{-(s+1)}$-close to uniform. Thus, using equation triangle inequality, we get that

$$X_1, X_2, X'_1, X'_2 \approx_{2^{-s}} U_1, U_2, h_1(U_2, Z), h_2(U_2, Z)\ ,$$

which implies the result. □

Symmetrically, we get the following:

Lemma 8.17. *If $|\mathcal{L}_{\mathsf{swap}} \times \mathcal{R}_{\mathsf{id}}| \geq q^{4\tau n} \cdot 2^{-s}$ then there exists a distribution D that is a convex combination of distributions in $\mathcal{D}_{\mathsf{forget},1}$ such that*

$$\Delta(\phi_{f,g}(L,R)|_{(L,R)\in\mathcal{L}_{\mathsf{swap}}\times\mathcal{R}_{\mathsf{id}}}\ ; D) \leq 2^{-s}\ .$$

We now look at the case when L, R are restricted to $\mathcal{L}_{\mathsf{id}}$, and $\mathcal{R}_{\mathsf{id}}$, respectively.

Lemma 8.18. *If $|\mathcal{L}_{\mathsf{id}} \times \mathcal{R}_{\mathsf{id}}| \geq q^{4\tau n} \cdot 2^{-s}$ then there exists a distribution D that is a convex combination of distributions in $\mathcal{D}_{\mathsf{id}}$ such that*

$$\Delta(\phi_{f,g}(L,R)|_{(L,R)\in\mathcal{L}_{\mathsf{id}}\times\mathcal{R}_{\mathsf{id}}}\ ; D) \leq 2^{-s}\ .$$

Proof. Let $|\mathcal{L}_{\mathsf{id}} \times \mathcal{R}_{\mathsf{id}}| \geq q^{4\tau n} \cdot 2^{-s}$. Let $\tilde{L}, \tilde{R}$ be distributed uniformly over $\mathcal{L}_{\mathsf{id}}$ and $\mathcal{R}_{\mathsf{id}}$ respectively. Note that by the assumption we have that $|\mathcal{L}_{\mathsf{id}}| \geq q^{2\tau n} \cdot 2^{-s}$ and $|\mathcal{R}_{\mathsf{swap}}| \geq q^{2\tau n} \cdot 2^{-s}$. Denote $\langle \tilde{L}_k, \tilde{R}_k \rangle$ by X_k, and $\langle f_k(\tilde{L}), g_k(\tilde{R}) \rangle$ by X'_k for $k = 1, 2$.

By Lemma 8.3, there exists maps $a_{1,1}$, $a_{2,2}$ from $\mathcal{L}_{\mathsf{id}}$ to $\{0,1\}^{\beta_2}$, and $b_{1,1}$, $b_{2,2}$ from $\mathcal{R}_{\mathsf{id}}$ to $\{0,1\}^{\beta_2}$, such that $f_1(\tilde{L})$, $f_2(\tilde{L})$, $g_1(\tilde{R})$, $g_2(\tilde{R})$ are determined uniquely given $(\tilde{L}_1, a_{1,1}(\tilde{L}))$, $(\tilde{L}_2, a_{2,2}(\tilde{L}))$, $(\tilde{R}_1, b_{1,1}(\tilde{R}))$, $(\tilde{R}_2, b_{2,2}(\tilde{R}))$, respectively. We define the random variable Y as

$$Y := \tilde{L}_1,\ \ \tilde{R}_2,\ \ a_{1,1}(\tilde{L}),\ \ a_{2,2}(\tilde{L}),\ \ b_{1,1}(\tilde{R}),\ \ b_{2,2}(\tilde{R})\ .$$

Note that X'_1 is a deterministic function of Y and $\tilde{R}_1$. Similarly, X'_2 is a deterministic function of Y and $\tilde{L}_2$. Let W_1 be independent randomness used to sample $\tilde{R}_1$ given Y and X_1, and let W_2 be independent randomness used to sample $\tilde{L}_2$ given Y and X_2. Note that W_1, W_2 are independent from each other and from X_1, X_2, Y. Therefore, we have that

$$X_1, X_2, X'_1, X'_2 \equiv X_1, X_2, h_1(X_1, Y, W_1), h_2(X_2, Y, W_2)\ , \tag{8.19}$$

for some functions h_1, h_2. Also, using Lemma 2.3, we have that

$$\begin{aligned} X_1, X_2, Y, W_1, W_2 &\approx_{2^{-(s+1)}} U_1, X_2, Y, W_1, W_2 \\ &\approx_{2^{-(s+1)}} U_1, U_2, Y, W_1, W_2\ . \end{aligned}$$

This implies the desired result using equation 8.19, and Lemma 2.1. □

Symmetrically, we get the following:

Lemma 8.20. *If $|\mathcal{L}_{\mathsf{swap}} \times \mathcal{R}_{\mathsf{swap}}| \geq q^{4\tau n} \cdot 2^{-s}$ then there exists a distribution D that is a convex combination of distributions in $\mathcal{D}_{\mathsf{swap}}$ such that*

$$\Delta(\phi_{f,g}(L,R)|_{(L,R)\in\mathcal{L}_{\mathsf{swap}}\times\mathcal{R}_{\mathsf{swap}}}\ ; D) \leq 2^{-s}\ .$$

8.3.4 Remaining cases

Lemma 8.21. *$|\mathcal{L}_{\mathsf{rem}}| \leq q^{2\tau n} 2^{-s}$, and $|\mathcal{R}_{\mathsf{rem}}| \leq q^{2\tau n} 2^{-s}$*

Proof. Consider any $\ell \in \mathcal{L}_{\mathsf{rem}}$. Since $\ell \notin \mathcal{L}_{\mathsf{mix},j}$, we have that $\mathcal{T}(\ell, 1) \cup \mathcal{T}(\ell, 2) = \{1, 2\}$. Also, since $\ell \notin \mathcal{L}_{\mathsf{id}} \cup \mathcal{L}_{\mathsf{swap}}$, there exists some $k \in \{1, 2\}$, such that $\mathcal{T}(\ell, k) = \{1, 2\}$. Thus, using Lemma 8.3, we have that $f(\ell)$ can be determined given ℓ_k, $a_{k,1}, a_{k,2}$. This implies that $f(\ell)$ can be determined given at most $\tau n \log q + 2\beta_2$ bits. Therefore

$$|\mathcal{L}_{\mathsf{rem}}| \leq q^{\tau n} 2^{2\beta_2} \leq q^{2\tau n} 2^{-s}\ .$$

Symmetrically, $|\mathcal{R}_{\mathsf{rem}}| \leq q^{2\tau n} 2^{-s}$.

□

8.4 Finishing the proof

We partitioned $\mathcal{L} \times \mathcal{R}$ into following cases.

- $\mathcal{L}_{\mathsf{ffb},i} \times \mathcal{R}^*$ (see Lemma 8.4)
- $\mathcal{L}^* \times \mathcal{R}_{\mathsf{ffb},i}$ (see Lemma 8.8)
- $\mathcal{L}_{\mathsf{mix},j} \times \mathcal{R}^*$ (see Lemma 8.9)
- $\mathcal{L}^* \times \mathcal{R}_{\mathsf{mix},j}$ (see Lemma 8.13)
- $\mathcal{L}_{\mathsf{id}} \times \mathcal{R}_{\mathsf{swap}}$ (see Lemma 8.14)
- $\mathcal{L}_{\mathsf{swap}} \times \mathcal{R}_{\mathsf{id}}$ (see Lemma 8.17)
- $\mathcal{L}_{\mathsf{id}} \times \mathcal{R}_{\mathsf{id}}$ (see Lemma 8.18)
- $\mathcal{L}_{\mathsf{swap}} \times \mathcal{R}_{\mathsf{swap}}$ (see Lemma 8.20)
- $\mathcal{L}_{\mathsf{rem}} \times \mathcal{R}^*$ and $\mathcal{L}^* \times \mathcal{R}_{\mathsf{rem}}$ (see Lemma 8.21)

We showed that in every case for partition $\mathcal{L}^* \times \mathcal{R}^*$ we get either $\frac{|\mathcal{L}^* \times \mathcal{R}^*|}{|\mathcal{L} \times \mathcal{R}|} \leq 2^{-s}$ or there exists D' from $\mathcal{D}$ such that

$$\Delta(\phi_{f,g}(L,R)|_{L,R \in \mathcal{L}^* \times \mathcal{R}^*} \ ; \ D') \leq 2^{-s},$$

where $\mathcal{D}$ is a convex combination of distributions $\mathcal{D}_{\mathsf{id}} \cup \mathcal{D}_{\mathsf{swap}} \cup \mathcal{D}_{\mathsf{unif},1} \cup \mathcal{D}_{\mathsf{unif},2} \cup \mathcal{D}_{\mathsf{forget},1} \cup \mathcal{D}_{\mathsf{forget},2}$. We partitioned both $\mathcal{L}$ and $\mathcal{R}$ each into 7 subsets, thus by Lemma 8.1 we obtain that there exists a distribution D in $\mathcal{D}$ such that

$$\Delta(\phi_{f,g}(L,R) \ ; \ D) \leq 7^2 \cdot 2^{-s}.$$

This finishes the proof. □

9 Conclusions and Open Problems

Our main result is a generic transformation from non-malleable codes in the 2-split-state model to non-malleable codes in the 2-split-state model that is resilient to leakage of length upto 1/12-th of the length of the codeword. Combining with the best known non-malleable codes in the 2-split state model achieved by a subsequent work [ADKO14], we get constant-rate 1/12-leakage resilient non-malleable codes.

We also observe in Section 7 that the result of [CG14b] implies that we can achieve non-malleable codes resilient to a fraction of leakage arbitrarily close to 1.

Thus, our work can be viewed as initiating the study and achieving a constant factor leakage resilience for information-theoretically secure non-malleable codes. In view of the existential result, the main open question is whether we can give an efficient construction of non-malleable codes that can achieve leakage-resilience larger than a 1/12-th fraction, and thereby make non-malleable codes practically more useful.

References

[ADKO14] Divesh Aggarwal, Yevgeniy Dodis, Tomasz Kazana, and Maciej Obremski. Non-malleable reductions and applications, 2014. Unpublished manuscript.

[ADL14] Divesh Aggarwal, Yevgeniy Dodis, and Shachar Lovett. Non-malleable codes from additive combinatorics. In David B. Shmoys, editor, *46th ACM STOC*, pages 774–783, New York, NY, USA, May 31 – June 3, 2014. ACM Press.

[Agg14] Divesh Aggarwal. Affine-evasive sets modulo a prime. Cryptology ePrint Archive, Report 2014/328, 2014. `http://eprint.iacr.org/`.

[AK96] Ross Anderson and Markus Kuhn. Tamper resistance — a cautionary note. In *The Second USENIX Workshop on Electronic Commerce*, pages 1–11, November 1996.

[BDL14] Nir Bitansky, Dana Dachman-Soled, and Huijia Lin. Leakage-tolerant computation with input-independent preprocessing. In Juan A. Garay and Rosario Gennaro, editors, *CRYPTO 2014, Part II*, volume 8617 of *LNCS*, pages 146–163, Santa Barbara, CA, USA, August 17–21, 2014. Springer, Berlin, Germany.

[BK03] Mihir Bellare and Tadayoshi Kohno. A theoretical treatment of related-key attacks: RKA-PRPs, RKA-PRFs, and applications. In Eli Biham, editor, *Advances in Cryptology—EUROCRYPT 2003*, volume 2656 of *LNCS*. Springer-Verlag, 2003. Full version available at `http://www-cse.ucsd.edu/users/tkohno/papers/RKA/`.

[BR93] Mihir Bellare and Phillip Rogaway. Random oracles are practical: A paradigm for designing efficient protocols. In V. Ashby, editor, *ACM CCS 93*, pages 62–73, Fairfax, Virginia, USA, November 3–5, 1993. ACM Press.

[CCP12] H. Chabanne, G. Cohen, and A Patey. Secure network coding and non-malleable codes: Protection against linear tampering. In *Information Theory Proceedings (ISIT), 2012 IEEE International Symposium on*, pages 2546–2550, July 2012.

[CDF+08] Ronald Cramer, Yevgeniy Dodis, Serge Fehr, Carles Padró, and Daniel Wichs. Detection of algebraic manipulation with applications to robust secret sharing and fuzzy extractors. In Nigel P. Smart, editor, *EUROCRYPT 2008*, volume 4965 of *LNCS*, pages 471–488, Istanbul, Turkey, April 13–17, 2008. Springer, Berlin, Germany.

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

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

[CG14b] Mahdi Cheraghchi and Venkatesan Guruswami. Non-malleable coding against bit-wise and split-state tampering. In *Theory of Cryptography - 11th Theory of Cryptography Conference, TCC 2014, San Diego, CA, USA, February 24-26, 2014. Proceedings*, pages 440–464, 2014.

[CMTV14] Sandro Coretti, Ueli Maurer, Björn Tackmann, and Daniele Venturi. From single-bit to multi-bit public-key encryption via non-malleable codes. Cryptology ePrint Archive, Report 2014/324, 2014. `http://eprint.iacr.org/`.

[CZ14] Eshan Chattopadhyay and David Zuckerman. Non-malleable codes against constant split-state tampering. In *FOCS*, 2014.

[DDN98] Danny Dolev, Cynthia Dwork, and Moni Naor. Non-malleable cryptography, 1998. Manuscript.

[DDV10] Francesco Davì, Stefan Dziembowski, and Daniele Venturi. Leakage-resilient storage. In Juan A. Garay and Roberto De Prisco, editors, *SCN*, volume 6280 of *Lecture Notes in Computer Science*, pages 121–137. Springer, 2010.

[DF12] Stefan Dziembowski and Sebastian Faust. Leakage-resilient circuits without computational assumptions. In Ronald Cramer, editor, *TCC 2012*, volume 7194 of *LNCS*, pages 230–247, Taormina, Sicily, Italy, March 19–21, 2012. Springer, Berlin, Germany.

[DK12] Dana Dachman-Soled and Yael Tauman Kalai. Securing circuits against constant-rate tampering. In Reihaneh Safavi-Naini and Ran Canetti, editors, *CRYPTO 2012*, volume 7417 of *LNCS*, pages 533–551, Santa Barbara, CA, USA, August 19–23, 2012. Springer, Berlin, Germany.

[DKO13] Stefan Dziembowski, Tomasz Kazana, and Maciej Obremski. Non-malleable codes from two-source extractors. In Ran Canetti and Juan A. Garay, editors, *CRYPTO 2013, Part II*, volume 8043 of *LNCS*, pages 239–257, Santa Barbara, CA, USA, August 18–22, 2013. Springer, Berlin, Germany.

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

[DP07] Stefan Dziembowski and Krzysztof Pietrzak. Intrusion-resilient secret sharing. In *FOCS*, pages 227–237. IEEE Computer Society, 2007.

[DP08] Stefan Dziembowski and Krzysztof Pietrzak. Leakage-resilient cryptography. In *49th Symposium on Foundations of Computer Science*, pages 293–302, Philadelphia, PA, USA, October 25–28 2008. IEEE Computer Society.

[DPW10] Stefan Dziembowski, Krzysztof Pietrzak, and Daniel Wichs. Non-malleable codes. In Andrew Chi-Chih Yao, editor, *ICS 2010*, pages 434–452, Tsinghua University, Beijing, China, January 5–7, 2010. Tsinghua University Press.

[ECR] ECRYPT. Side channel cryptanalysis lounge. last accessed: August 26, 2009. `http://www.crypto.ruhr-uni-bochum.de/en_sclounge.html`.

[FKPR10] Sebastian Faust, Eike Kiltz, Krzysztof Pietrzak, and Guy N. Rothblum. Leakage-resilient signatures. In Daniele Micciancio, editor, *TCC 2010*, volume 5978 of *LNCS*, pages 343–360, Zurich, Switzerland, February 9–11, 2010. Springer, Berlin, Germany.

[FMNV14a] S. Faust, P. Mukherjee, J. Nielsen, and D. Venturi. Continuous non-malleable codes. In *Theory of Cryptography Conference - TCC*. Springer, 2014.

[FMNV14b] Sebastian Faust, Pratyay Mukherjee, Jesper Buus Nielsen, and Daniele Venturi. A tamper and leakage resilient random access machine. Cryptology ePrint Archive, Report 2014/338, 2014. `http://eprint.iacr.org/2014/338`.

[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, *EUROCRYPT 2014*, volume 8441 of *LNCS*, pages 111–128, Copenhagen, Denmark, May 11–15, 2014. Springer, Berlin, Germany.

[FPV11] Sebastian Faust, Krzysztof Pietrzak, and Daniele Venturi. Tamper-proof circuits: How to trade leakage for tamper-resilience. In Luca Aceto, Monika Henzinger, and Ji Sgall, editors, *Automata, Languages and Programming*, volume 6755 of *Lecture Notes in Computer Science*, pages 391–402. Springer Berlin Heidelberg, 2011.

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

[GR12] Shafi Goldwasser and Guy N. Rothblum. How to compute in the presence of leakage. In *53rd FOCS*, pages 31–40, New Brunswick, NJ, USA, October 20–23, 2012. IEEE Computer Society Press.

[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.

[KKS11] Yael Tauman Kalai, Bhavana Kanukurthi, and Amit Sahai. Cryptography with tamperable and leaky memory. In Phillip Rogaway, editor, *CRYPTO 2011*, volume 6841 of *LNCS*, pages 373–390, Santa Barbara, CA, USA, August 14–18, 2011. Springer, Berlin, Germany.

[LL10] Feng-Hao Liu and Anna Lysyanskaya. Algorithmic tamper-proof security under probing attacks. In Juan A. Garay and Roberto De Prisco, editors, *SCN 10*, volume 6280 of *LNCS*, pages 106–120, Amalfi, Italy, September 13–15, 2010. Springer, Berlin, Germany.

[LL12] Feng-Hao Liu and Anna Lysyanskaya. Tamper and leakage resilience in the split-state model. In Reihaneh Safavi-Naini and Ran Canetti, editors, *CRYPTO 2012*, volume 7417 of *LNCS*, pages 517–532, Santa Barbara, CA, USA, August 19–23, 2012. Springer, Berlin, Germany.

[MR04] Silvio Micali and Leonid Reyzin. Physically observable cryptography (extended abstract). In Moni Naor, editor, *First Theory of Cryptography Conference — TCC 2004*, volume 2951 of *LNCS*, pages 278–296. Springer-Verlag, February 19–21 2004.

[Rao07] Anup Rao. An exposition of bourgain 2-source extractor. In *Electronic Colloquium on Computational Complexity (ECCC)*, volume 14, page 034, 2007.

A Proofs of Lemmata from Section 2

Lemma 2.4 *Let $X_1, Y_1 \in \mathcal{A}_1$, and $Y_1, Y_2 \in \mathcal{A}_2$ be random variables such that $\Delta((X_1, X_2)\ ;\ (Y_1, Y_2)) \leq \varepsilon$. Then, for any non-empty set $\mathcal{A}' \subseteq \mathcal{A}_1$, we have*

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

Proof.

$$\begin{aligned}
\Delta(X_2 \mid X_1 \in \mathcal{A}' \,;\, Y_2 \mid Y_1 \in \mathcal{A}') &= \frac{1}{2}\sum_{x\in\mathcal{A}_2}\Big|\Pr(X_2 = x \mid X_1 \in \mathcal{A}') - \Pr(Y_2 = x \mid Y_1 \in \mathcal{A}')\Big| \\
&\le \frac{1}{2}\sum_{x\in\mathcal{A}_2}\Big(\Big|\frac{\Pr(X_2 = x \ \wedge\ X_1 \in \mathcal{A}')}{\Pr(X_1 \in \mathcal{A}')} - \frac{\Pr(Y_2 = x \ \wedge\ Y_1 \in \mathcal{A}')}{\Pr(X_1 \in \mathcal{A}')}\Big| \\
&\qquad + \Pr(Y_2 = x \ \wedge\ Y_1 \in \mathcal{A}')\Big|\frac{1}{\Pr(Y_1 \in \mathcal{A}')} - \frac{1}{\Pr(X_1 \in \mathcal{A}')}\Big|\Big) \\
&\le \frac{\varepsilon}{\Pr(X_1 \in \mathcal{A}')} + \frac{\varepsilon \cdot \sum_{x\in\mathcal{A}_2}\Pr(Y_1 \in \mathcal{A}' \ \wedge\ Y_2 = x)}{\Pr(Y_1 \in \mathcal{A}') \cdot \Pr(X_1 \in \mathcal{A}')} \\
&= \frac{2\varepsilon}{\Pr(X_1 \in \mathcal{A}')}\,.
\end{aligned}$$

□

Lemma 2.6 *Let $X = (X_1, \ldots, X_t) \in \mathbb{F}^t$ be a random variable, where $\mathbb{F}$ is a finite field of order q. Assume that for all $a_1, \ldots, a_t \in \mathbb{F}^t$ not all zero, $\Delta(\sum_{i=1}^t a_i X_i \,;\, U) \le \varepsilon$, where U is uniform in $\mathbb{F}$. Then $\Delta(X_1, \ldots, X_t \,;\, U_1, \ldots, U_t) \le \varepsilon q^{(t+2)/2}$, where $U_1, \ldots, U_t$ are independent and uniform in $\mathbb{F}^t$.*

Proof. The proof uses basic Fourier analysis. Assume $\mathbb{F}$ has characteristic p. Let $\omega = e^{2\pi i/p}$ be a primitive p-th root of unity. Let $\mathrm{Tr} : \mathbb{F} \to \mathbb{F}_p$ denote the trace operator from $\mathbb{F}$ to $\mathbb{F}_p$. The additive characters of $\mathbb{F}$ are given by $\{\chi_a(x) : \mathbb{F} \to \mathbb{C} : a \in \mathbb{F}\}$ defined as

$$\chi_a(x) = \omega^{\mathrm{Tr}(ax)}.$$

The additive characters of $\mathbb{F}^t$ are given by $\chi_{a_1,\ldots,a_t}(x_1, \ldots, x_t) = \Pi_{i=1}^t \chi_{a_i}(x_i)$ for $a_1, \ldots, a_t \in \mathbb{F}$. First, we bound the Fourier coefficients of the distribution of $X = (X_1, \ldots, X_t)$. The $(a_1, \ldots, a_t)$ Fourier coefficient, for all non-zero $(a_1, \ldots, a_t)$, is given by

$$\begin{aligned}
\mathbb{E}[\chi_{a_1,\ldots,a_t}(X_1, \ldots, X_t)] &= \mathbb{E}[\omega^{\mathrm{Tr}(\sum_{i=1}^t a_i X_i)}] = \sum_{b\in\mathbb{F}} \omega^{\mathrm{Tr}(b)} \Pr[\sum_{i=1}^t a_i X_i = b] \\
&= \sum_{b\in\mathbb{F}} \omega^{\mathrm{Tr}(b)} \left(\Pr_X[\sum_{i=1}^t a_i X_i = b] - \frac{1}{|\mathbb{F}|}\right),
\end{aligned}$$

where we used the fact that $\sum_{b\in\mathbb{F}} \omega^{\mathrm{Tr}(b)} = 0$. Hence for all non-zero $(a_1, \ldots, a_t)$,

$$\big|\mathbb{E}[\chi_{a_1,\ldots,a_t}(X_1, \ldots, X_t)]\big| \le \sum_{b\in\mathbb{F}} \left|\Pr[\sum_{i=1}^t a_i X_i = b] - \frac{1}{|\mathbb{F}|}\right| \le 2\varepsilon \cdot |\mathbb{F}|\,.$$

Let $p_{a_1,\ldots,a_t} = \Pr[(X_1, \ldots, X_t) = (a_1, \ldots, a_t)]$. By Parseval's identity,

$$\sum_{a_1,\ldots,a_t\in\mathbb{F}} \left(p_{a_1,\ldots,a_t} - \frac{1}{|\mathbb{F}|}\right)^2 = \sum_{(a_1,\ldots,a_t)\neq 0} \mathbb{E}[\chi_{a_1,\ldots,a_t}(X_1, \ldots, X_t)]^2 \le 4\varepsilon^2 |\mathbb{F}|^{t+2}\,,$$

□

B Proof of Lemma 6.1

We will need the following fact.

Fact B.1. *Let* $\mathsf{Dec} : \mathcal{X} \times \mathcal{X} \to \mathcal{M} \cup \{\perp\}$*, and* $\mathsf{Enc} : \mathcal{M} \to \mathcal{X} \times \mathcal{X}$ *be* ε*-non-malleable scheme in* $2-$*split state model for some* $\varepsilon < \frac{1}{2}$*. For any two messages* $m_0, m_1 \in \mathcal{M}$*, there exist* $x_1^0, x_1^1, x_2 \in \mathcal{X}$ *such that*

- $\mathsf{Dec}(x_1^0, x_2) = m_0$
- $\mathsf{Dec}(x_1^1, x_2) = m_1$

Proof. By contradiction, let us assume there exists $m_0, m_1 \in \mathcal{M}$ such that $\forall_{x_2 \in \mathcal{X}} |\mathsf{Dec}(\mathcal{X}, x_2) \cap \{m_0, m_1\}| = 1$. Let us define sets $\mathcal{X}_2^0, \mathcal{X}_2^1$ as follows

$$\mathcal{X}_2^0 = \{x_2 \in \mathcal{X} \ : \ \mathsf{Dec}(\mathcal{X}, x_2) \cap \{m_0, m_1\} = \{m_0\}\}$$
$$\mathcal{X}_2^1 = \{x_2 \in \mathcal{X} \ : \ \mathsf{Dec}(\mathcal{X}, x_2) \cap \{m_0, m_1\} = \{m_1\}\}$$

Fix arbitrary $x_2^0 \in \mathcal{X}_2^0$, $x_2^1 \in \mathcal{X}_2^1$, and let

$$\mathcal{X}_1^0 = \{x \in \mathcal{X} \ : \ \mathsf{Dec}(x, x_2^0) = m_0\}$$
$$\mathcal{X}_1^1 = \{x \in \mathcal{X} \ : \ \mathsf{Dec}(x, x_2^1) = m_1\}$$

Consider tampering functions $h_1 : \mathcal{X} \to \mathcal{X}$, and $h_2 : \mathcal{X} \to \mathcal{X}$ as follows. Let $h_2(\mathcal{X}_2^0) := x_2^1$ and $h_2(\mathcal{X}_2^1) := x_2^0$, and h_2 is defined arbitrarily in $\mathcal{X} \setminus (\mathcal{X}_2^0 \cup \mathcal{X}_2^1)$. Also, if $\mathcal{X}_1^0 \cap \mathcal{X}_1^1$ is non-empty, then fix some $x \in \mathcal{X}_1^0 \cap \mathcal{X}_1^1$, and let $h_1(c) = x$ for all $c \in \mathcal{X}$. Otherwise choose arbitrary $x_1^0 \in \mathcal{X}_1^0$, $x_1^1 \in \mathcal{X}_1^1$, and let $h_1(\mathcal{X}_1^0) := x_1^1$ and $h_1(\mathcal{X}_1^1) := x_1^0$, and h_1 is defined arbitrarily in $\mathcal{X} \setminus (\mathcal{X}_1^0 \cup \mathcal{X}_1^1)$.

Then, we have that $\mathsf{Tamper}_{m_0} = m_1$, and $\mathsf{Tamper}_{m_1} = m_0$ with probability 1, where Tamper_{m_0} and Tamper_{m_1} are as in Definition 3.2. This implies that there exists a distribution D over $\mathcal{M} \cup \{\perp\}$ such that $\Pr(D = m_0) \geq 1 - \varepsilon$, and $\Pr(D = m_1) \geq 1 - \varepsilon$, which is a contradiction. □

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* $\Delta(X_1^0\,;\, X_1^1) \leq 2\varepsilon$*.*

Proof. By contradiction assume that $\Delta(X_1^0\,;\, X_1^1) > 2\varepsilon$. Then there exists distinguisher $\mathcal{A} : \mathcal{X} \to \{0, 1\}$ such that

$$\Pr(\mathcal{A}(X_1^0) = 1) - \Pr(\mathcal{A}(X_1^1) = 1) > 2\varepsilon \ . \tag{B.2}$$

By Fact B.1 we have $x_1^0, x_1^1, x_2 \in \mathcal{X}$ such that $\mathsf{Dec}(x_1^0, x_2) = m_0$ and $\mathsf{Dec}(x_1^1, x_2) = m_1$. Now let us choose following tampering functions:

$$h_2(r) = x_2, \ \text{ and } \ h_1(\ell) = x_{\mathcal{A}(\ell)}.$$

Consider Tamper_{m_0} and Tamper_{m_1} as in Definiton 3.2. By Equation B.2, we have that

$$\Pr[\mathsf{Tamper}_{m_0} = m_1] - \Pr[\mathsf{Tamper}_{m_1} = m_1] > 2\varepsilon \ . \tag{B.3}$$

From Definition 3.2, we have that there exists a distribution D such that

$$|\Pr[\mathsf{Tamper}_{m_0} = m_1] - \Pr(D = m_1)| \leq \varepsilon, \quad \text{and} \quad |\Pr[\mathsf{Tamper}_{m_1} = m_1] - \Pr(D = m_1) - \Pr(D = \mathsf{same})| \leq \varepsilon \ .$$

By triangle inequality, this implies,

$$\Pr[\mathsf{Tamper}_{m_0} = m_1] - \Pr[\mathsf{Tamper}_{m_1} = m_1] + \Pr(D = \mathsf{same}) \leq 2\varepsilon \ ,$$

which contradicts Equation B.3. □

ECCC ISSN 1433-8092
http://eccc.hpi-web.de