Local Non-Malleable Codes in the Bounded Retrieval Model

Dana Dachman-Soled [⋆], Mukul Kulkarni, and Aria Shahverdi

University of Maryland, College Park, USA
{danadach@ece., mukul@terpmail., ariash@}umd.edu

Abstract. In a recent result, Dachman-Soled et al. (TCC '15) proposed a new notion called locally decodable and updatable non-malleable codes, which informally, provides the security guarantees of a non-malleable code while also allowing for efficient random access. They also considered locally decodable and updatable non-malleable codes that are *leakage-resilient*, allowing for adversaries who continually leak information in addition to tampering.

The bounded retrieval model (BRM) (cf. [Alwen et al., CRYPTO '09] and [Alwen et al., EUROCRYPT '10]) has been studied extensively in the setting of leakage resilience for cryptographic primitives. This threat model assumes that an attacker can learn information about the secret key, subject only to the constraint that the overall amount of leaked information is upper bounded by some value. The goal is then to construct cryptosystems whose secret key length grows with the amount of leakage, but whose runtime (assuming random access to the secret key) is *independent* of the leakage amount.

In this work, we combine the above two notions and construct local non-malleable codes in the split-state model, that are secure against *bounded retrieval* adversaries. Specifically, given leakage parameter ℓ, we show how to construct an efficient, 3-split-state, locally decodable and updatable code (with CRS) that is secure against one-time leakage of any polynomial time, 3-split-state leakage function whose output length is at most ℓ, and one-time tampering via any polynomial-time 3-split-state tampering function. The locality we achieve is polylogarithmic in the security parameter.

1 Introduction

Non-malleable codes were introduced by Dziembowski, Pietrzak and Wichs [39] as a relaxation of error-correcting codes, and are useful in settings where privacy—but not necessarily correctness—is desired. Informally, a coding scheme is *non-malleable* against a tampering function if by tampering with the codeword, the

[⋆] This work is supported in part by an NSF CAREER Award #CNS-1453045, by a research partnership award from Cisco and by financial assistance award 70NANB15H328 from the U.S. Department of Commerce, National Institute of Standards and Technology.

function either keeps the underlying message unchanged or changes it to an unrelated message. The main application of non-malleable codes proposed in the literature is achieving security against leakage and tampering attacks on memory (so-called *physical attacks* or *hardware attacks*) [58,57], although non-malleable codes have also found applications in other areas of cryptography [26,25,46] and theoretical computer science [21].

In this work, we go beyond considering non-malleable codes in the context of physical and/or hardware attacks and consider the problem of providing data assurance in a *network* environment. Our main focus is on providing privacy and integrity for large amounts of dynamic data (such as a large medical database with many authorized users), while allowing for efficient, random access to the data. We are interested in settings where *all* persistent data is assumed vulnerable to attack and there is no portion of memory that is assumed to be fully protected. We protect against *bounded-retrieval* adversaries, who may "leak" (i.e. download) large amounts of data, as long as the total amount leaked is bounded a priori.

In the following, we provide context for the contribution of this work by discussing (1) the limitations of standard non-malleable codes, (2) the recent notion of locally decodable and updatable non-malleable codes (LDUNMC) [29] (for settings where large amounts of dynamic data must be protected) and (3) the reason previous constructions of LDUNMC fall short in our setting.

Drawbacks of standard non-malleable codes. Standard non-malleable codes are useful for protecting small amounts of secret data stored on a device (e.g. cryptographic secret key) but unfortunately are not suitable in settings where, say, an entire database must be protected. This is due to the fact that non-malleable codes do not allow for random access: Once the database is encoded via a non-malleable code, in order to access just a single location, the entire database must first be decoded, requiring a linear scan over the database. Similarly, to update a single location, the entire database must be decoded, updated and re-encoded.

Locally decodable and updatable non-malleable codes (LDUNMC). In a recent result, [29] proposed a new notion called LDUNMC, which informally speaking, provides the security guarantees of a non-malleable code while also allowing for efficient random access (i.e. allowing to decode/update a particular position i of the underlying message via $\mathsf{DEC}^C(i)/\mathsf{UPDATE}^C(i)$). In more detail, we consider a database $D = D_1, \ldots, D_n$ consisting of n blocks, and an encoding algorithm $\mathsf{ENC}(D)$ that outputs a codeword $C = C_1, \ldots, C_{\hat{n}}$ consisting of $\hat{n}$ blocks. As introduced by Katz and Trevisan [54], local decodability means that in order to retrieve a single block of the underlying database, one does not need to read through the whole codeword but rather, one can access just a few locations of the codeword. In 2014, Chandran et al. [17] introduced the notion of local updatability, which means that in order to update (or "re-encode") a single block of the underlying database, one only needs to update a few blocks of the codeword.

As observed by [29], achieving these locality properties requires a modification of the definition of non-malleability: Suppose a tampering function f only modifies one block of the codeword, then it is likely that the output of the decoding algorithm, DEC, remains unchanged in most locations. (Recall DEC gets as input an index $i \in [n]$ and will only access a few blocks of the codeword to recover the i-th block of the database, so it may not detect the modification.) In this case, the (overall) decoding of the tampered codeword $f(C)$ (i.e. $(\mathsf{DEC}^{f(C)}(1), \ldots, \mathsf{DEC}^{f(C)}(n)))$ can be highly related to the original message, which intuitively means it is highly malleable.

To handle this, [29] consider a more fine-grained experiment. They require that for any tampering function f (within some class), there exists a simulator that computes a vector of decoded messages D^* and a set of indices $\mathcal{I} \subseteq [n]$. Here $\mathcal{I}$ denotes the coordinates of the underlying messages that have been tampered with. If $\mathcal{I} = [n]$, then the simulator thinks that the decoded messages are D^*, which should be unrelated to the original messages. On the other hand, if $\mathcal{I} \subsetneq [n]$, the simulator thinks that all the indices not in $\mathcal{I}$ remain unchanged, while those in $\mathcal{I}$ become $\perp$. More formally, the output of the experiment is as follows:

1. If $\mathcal{I} = [n]$ then output the simulator's output D^*, else
2. If $\mathcal{I} \neq [n]$ then for all $i \in \mathcal{I}$, set $D'(i) = \perp$ and for $i \notin \mathcal{I}$, set $D'(i) = D(i)$, where $D(i)$ is the i^{th} block of current underlying message D. Output D'.

This means the tampering function can do one of the following:

1. It destroys block(s) of the underlying messages—i.e. causes DEC to output $\perp$ on those blocks—while keeping the other blocks unchanged, OR
2. If it modifies a block of the underlying message to a valid encoding, then it must have modified *all* blocks to encodings of unrelated messages, thus destroying the original message.

It turns out, as shown by [29], that the above is sufficient for achieving tamper-resilience for RAM computations. Specifically, the above (together with an ORAM scheme) yields a compiler for any RAM program with the guarantee that any adversary who gets input/output access to the compiled RAM program Π running on compiled database D and can additionally apply tampering functions $f \in \mathcal{F}$ to the database D adaptively throughout the computation, learns no more than what can be learned given only input/output access to Π running on database D. Dachman-Soled et al. in [29] considered LDUNMC that are also *leakage-resilient*, thus allowing for adversaries who continually leak information about D in addition to tampering.

Drawbacks of LDUNMC. The final construction in [29] achieved a leakage resilient, LDUNMC in the *split-state* and *relative leakage* model. In the split-state model, the codeword C is divided into sections called split-states and it is assumed that adversarial tampering and leakage on each section is *independent*. In the relative leakage model, the amount of information the adversary can leak is at most ℓ bits, and *all parameters of the system* (including complexity of

$\mathsf{DEC}/\mathsf{UPDATE}$) scale with ℓ. Thus, a main drawback of the construction of [29] is that, since their result is in the relative leakage model, the efficiency of the $\mathsf{DEC}/\mathsf{UPDATE}$ procedures scales with the amount of leakage ℓ allowed from one of the two split-states, which gives rise to the following dilemma: If the amount of leakage, ℓ, is allowed to be large, e.g. $\ell := \Omega(n) \cdot \log|\hat{\Sigma}|$ bits, where $\log|\hat{\Sigma}|$ is the number of bits in each block of the codeword, then *locality* is compromised, since $\mathsf{DEC}/\mathsf{UPDATE}$ must now have complexity that scales with $\Omega(n) \cdot \log|\hat{\Sigma}|$ and thus will need to read/write to at least $\Omega(n)$ data blocks. On the other hand, if it is required that $\mathsf{DEC}/\mathsf{UPDATE}$ have locality at most $\mathrm{polylog}(n)$, then it means that leakage of at most ℓ bits, where $\ell := c \cdot \mathrm{polylog}(n) \cdot \log|\hat{\Sigma}|$, for some $c < 1$, can be tolerated. In this work—motivated by a network setting, in which the adversary typically corrupts a server and modifies memory while downloading large amounts of data—we allow the adversary's leakage budget to be much larger than the complexity of $\mathsf{DEC}/\mathsf{UPDATE}$. We do assume that if an adversary surpasses its budget, its behavior will be detected and halted by network security monitors. Thus, an adversary cannot simply download the entire encoded database (in which case security would be impossible to achieve) without being caught.

1.1 Our Contributions and Results

Our first contribution is the conceptual contribution of introducing the notion of locally decodable and updatable non-malleable codes in the BRM, which we believe to be well-motivated, for the reasons discussed above.

We then construct LDUNMC in the split-state model, that are secure against *bounded retrieval* adversaries. The bounded retrieval model (BRM) (cf. [10,9]) has been studied extensively in the setting of leakage resilience for cryptographic primitives (e.g. public key encryption, digital signatures and identification schemes). This threat model assumes that an attacker can repeatedly and adaptively learn information about the secret key, subject only to the constraint that the overall amount of leaked information is upper bounded by some value. Cryptosystems in the BRM have the property that while the secret key length grows with the amount of leakage, the runtime (assuming random access to the secret key) is *independent* of the leakage amount. Thus, the parameters of interest in a bounded retrieval model cryptosystem are the following: (1) The leakage parameter ℓ, which gives the upper bound on the overall amount of leakage; (2) The locality t of the scheme which determines the number of locations of the secret key that must be accessed to perform an operation (e.g. decryption or signing); and (3) The relative leakage $\alpha := \ell/|\mathsf{sk}|$, which gives the ratio of the amount of leakage to secret key length. Since we consider bounded retrieval adversaries in the context of locally decodable and updatable codes, our threat model differs from the standard BRM threat model in the following ways:

- We consider the protection of arbitrary data (not limited to the secret key of a cryptosystem).

- We allow adversarial tampering in addition to bounded leakage and do not assume that any portion of memory is tamper-proof[1].
- We assume that both leakage and tampering are *split-state*, i.e. that the leakage/tampering functions are applied independently to different sections of memory.

In our setting, we retain the same parameters of interest ℓ, t, α as above, with the only differences that each split-state must be able to tolerate at least ℓ bits of leakage and the overall relative leakage, α is taken to be the minimum relative leakage over all split-states, where the relative leakage for each split-state is computed as the maximum amount of allowed leakage for that split-state (which may be greater than ℓ) divided by the size of that split-state.

We additionally restrict ourselves to a one-time tampering and leakage model (we discuss below the difficulties of extending to a fully continuous setting), where the experiment proceeds as follows: The adversary interacts with a challenger in an arbitrary polynomial number of rounds and may adaptively choose two rounds i, j where $i \leq j$, specifying a single leakage function $g \in \mathcal{G}$ in round i and a single tampering function $f \in \mathcal{F}$ in round j. The adversary gets to observe the leakage in round i before specifying tampering function f in round j. At the end of the experiment, the entire decoding of the (corrupted) codeword in each round is released in addition to the leakage obtained in each round. Our security requirement follows the ideal/real paradigm and requires that a simulator can simulate the output of the leakage as well as the decoding of *each position in each round*, without knowing the underlying encoded message. More precisely, as in the definition of [29], in each round the simulator outputs a vector of decoded data D^* along with a set of indices $\mathcal{I} \subseteq [n]$. Here $\mathcal{I}$ denotes the coordinates of the underlying messages that have been tampered with. If $\mathcal{I} = [n]$, then the simulator must output a complete vector of decoded messages D^*. On the other hand, if $\mathcal{I} \subsetneq [n]$, the simulator gets to output "same" for all messages not in $\mathcal{I}$, while those in $\mathcal{I}$ become $\perp$. When the output of the real and ideal experiments are compared, positions designated as "same" are replaced with either the original data in that position or with the most recent value placed in that position by an update instruction. We next state our main result:

Theorem 1 (Informal). *Under standard assumptions we have that for security parameter $\lambda \in \mathbb{N}$ and $\ell := \ell(\lambda)$, there exists an efficient, 3-split-state,* LDUNMC *(with CRS) in the bounded retrieval model that is secure against one-time tampering and leakage for tampering class $\mathcal{F}$ and leakage class $\mathcal{G}$, where*

- *$\mathcal{F}$ consists of all efficient, 3-split-state functions $f = (f_1, f_2, f_3)$.*
- *$\mathcal{G}$ consists of all efficient, 3-split-state functions $g = (g_1, g_2, g_3)$, such that g_1, g_2, g_3 each output at most ℓ bits.*

The scheme has locality $t := t(\lambda) \in \mathrm{polylog}(\lambda)$ and relative leakage $\alpha := \alpha(\lambda) \in \frac{1}{8} - o(1)$.

[1] [37] also allowed for tampering in the BRM setting, but required portions of memory to be completely tamper-proof.

In fact, the number of bits leaked from the third split-state can be much larger than ℓ and, in particular, will depend on the total size of the data being stored. The above theorem guarantees that, regardless of the size of the database, the relative leakage (for all three split-states) will be at least $\frac{1}{8} - o(1)$.

The above theorem can be instantiated assuming the existence of collision-resistant hash functions with subexponential security, NIZK with simulation sound extractability and identity-based hash proof systems, which can be realized from a variety of assumptions including standard assumptions in bilinear groups and lattices.

To obtain our result of a RAM-compiler against 3-split-state adversaries in the BRM, we note that using the same construction and proof of Theorem 4.6 in [29], we obtain a tamper and leakage resilient compiler $\mathsf{TLR\text{-}RAM} = (\mathsf{CompMem}, \mathsf{CompNext})$ that is one-time tamper and leakage resilient w.r.t. function families $\mathcal{F}, \mathcal{G}$ above, given an ORAM compiler that is access-pattern hiding and a one-time non-malleable and leakage resilient LDUNMC w.r.t. function families $\mathcal{F}, \mathcal{G}$ as above. Moreover, the locality of the final compiled program, is $t \cdot t'$, where t is the locality of the underlying LDUNMC and t' is the locality of the underlying ORAM.

Applications. Our encoding scheme can be used to protect data privacy and integrity while a RAM program is being computed on it in situations where: (1) the data is stored across at least 3 servers, (2) the attacker can corrupt all servers and launch a fully coordinated attack, (3) the attacker cannot download too much data from any of the servers at once. (3) can be justified either by assuming that the attacker has limited storage capacity or that an attacker who tries to download too much data will be detected by network security monitors. The advantage of using our approach of LDUNMC versus simply using encryption to achieve privacy and a Merkle tree to achieve integrity is that our approach allows tampering and leakage on *all* persistent data, whereas the former approach requires certain parts of memory (e.g. the parts storing the secret keys for encryption/decryption and the root of the Merkle tree) to be leak and tamper-free.

Difficulty of achieving continual tampering and leakage in the BRM setting. In order to achieve continual security in the BRM model an attacker must be prevented from running an attack in which it internally simulates the *decode* algorithm by leaking the required information from the appropriate split-state each time a read request is issued (this would trivially break privacy). The overall leakage of such an attack is bounded—and so it will always qualify as a BRM attack—since the local decodability property guarantees that only a small number of locations will be read. Indeed, our construction is vulnerable to such an attack: We store the first part of the secret key in one split-state, the second part of the secret key in a second split-state and ciphertexts in the third split-state. An attacker can first leak a target ciphertext from the third split-state, learn the locations required for decryption from the first split-state, leak those locations, then learn the locations required for decryption from the second split-state and leak those locations. It is unlikely (over the coins of update) that during this three-round attack any of the relevant locations in the first and second split-states are overwritten by the updater, since the few locations accessed by an update are randomly distributed. Thus, after three rounds of leakage the attacker has sufficient information to decrypt the target ciphertext. We leave open the question of whether such an attack can be generalized to show an impossibility result for continual LDUNMC in the BRM.

1.2 Techniques

Our construction proceeds in three stages:

Leakage Only (2-split-state construction). Here the attacker submits a single split-state leakage function $g := (g_1, g_2)$ and is not allowed to tamper. To achieve security, we encrypt the database block-by-block using a CPA-secure public key encryption (PKE) scheme in the BRM model. The codeword then has two split-states: The first contains the secret key and the second contains the ciphertexts. The locality and relative leakage of the scheme will be the same as that of the underlying encryption scheme. Even though the leakage is on both the secret key and ciphertexts, regular PKE in the BRM is sufficient since the leakage $g := (g_1, g_2)$ on both split-states is submitted simultaneously.

Leakage and Partial Tampering (2-split-state construction). Here the attacker submits a split-state leakage function $g := (g_1, g_2)$ followed by a split-state tampering function $f = (f_1, f_2)$, where f_1 is required to be the *identity function.* In terms of the previous construction, this means that the attacker gets to tamper with the ciphertexts only, but not the secret key. A first attempt to extend the previous construction is to use a CCA-secure PKE scheme in the BRM instead of a CPA-secure scheme. This will allow the simulator to use the CCA oracle to decrypt any encrypted blocks of the database that have been modified via tampering, thus ruling out mauling attacks on any individual block. Unfortunately, it does not prevent mauling attacks across blocks. Namely, some encrypted blocks can be replaced with fresh valid encryptions while others remain the same, leading to a valid, decoded database which is different, but correlated to the original data. To prevent this, we tie together the encrypted blocks in the database using a Merkle tree and store the Merkle tree in the second split-state along with the ciphertexts. During decode and update, we check that the relevant ciphertext block is consistent with the Merkle root. Unfortunately, this still does not work since the tampering function f_2 can be used to update the Merkle tree and root to be consistent with the modified ciphertexts at the leaves. Therefore, we additionally store a secret key for a signature scheme in the BRM model in the first split-state and include a signature on the root of the Merkle tree in the second split-state, which is verified during each decode and update. Note, however, that existentially unforgeable signatures are impossible in the BRM model, since an attacker can always use its leakage query g_1 to learn a signature on a new message. Nevertheless, so-called *entropic* signatures are possible [10,11][2]. Entropic signatures guarantee unforgeability for message distributions that have high entropy, even conditioned on the adversary's view after receiving the output of g_1 but before receiving the output of g_2. Thus, to argue non-malleability we show that either (1) The ciphertexts contained in the second split-state are *all* low entropy, conditioned on the adversary's view after receiving the output of g_1 but before receiving the output of g_2. In this case, it means that $\mathcal{I} = [n]$, i.e. all the ciphertexts have been modified and so the decryption across all blocks will lead to an unrelated database or (2) At least one ciphertext has high entropy, conditioned on the adversary's view after receiving the output of g_1 but before receiving the output of g_2. In this case, we argue that the root of the Merkle tree has high entropy and so an adversary who produces a forged signature violates the entropic security of the BRM signature scheme. We refer reader to the full version of the paper [27] for further details.

Full Leakage and Tampering (3-split-state construction). When trying to extend the above construction to allow tampering on the secret (and public) keys, it becomes clear that the entire secret key cannot be stored in a single split-state due to the following trivial attack: The adversary leaks a single ciphertext from the second split-state using leakage function g_2 and subsequently tampers with the first split-state using a tampering function f_1 such that f_1 does nothing if the leaked ciphertext decrypts to 0, and otherwise erases the entire contents of the first split-state. Such an attack clearly breaks non-malleability, since the entire codeword will decode properly if the leaked block contained a 0, and decode to $\perp$ otherwise. To overcome this attack, we introduce a third split-state: We store the secret keys across the first two split-states and store the public keys and ciphertexts in the third. We also replace the CCA-secure public key encryption scheme in the BRM with a new primitive we introduce called *CCA secure SS-BRM public key encryption*, which may be of independent interest (See Subsection 2.2 for the definition and the full version of the paper [27] for a construction and security proof). Given leakage parameter ℓ, such an encryption scheme stores the secret key in a split-state and guarantees CCA security even under ℓ bits of split-state leakage both before and *after* seeing the challenge ciphertext. The final construction is as follows: The first split-state stores the first part of secret key of the SS-BRM PKE scheme, the secret key of the BRM signature scheme, and a Merkle tree of the former two keys with root R_1. The second split-state stores the second part of the secret key of the SS-BRM PKE scheme, and a Merkle tree of the key with root R_2. The third split-state contains the ciphertexts, Merkle tree and signature on the root as in the previous construction and, in addition, stores a simulation-sound NIZK proof of knowledge

[2] The constructions cited above are in the random oracle model. However, as discussed in the full version of the paper [27], the primitive we require is slightly weaker than regular entropic signatures in the BRM and can be constructed in a straightforward manner in the standard model, without use of random oracles. For conceptual simplicity we present our constructions and state our theorems in terms of the existence of entropic signatures in the BRM.

of the pre-images of R_1 and R_2, with *local* verifiability (this is the reason a CRS is necessary). The property of local verifiability is necessary to ensure locality of decode/update and is achieved by using a probabilistically checkable proof (PCP) on top of a regular NIZK. Note that while computation of the PCP is expensive, this need only be done a single time, during the encode procedure, but the proof remains static during decode/update. Decode/update proceed as in the previous construction and additionally, during each decode/update, the proof is verified using the local verifier. Each time a location is accessed in the first or second split-state during decode/update, the corresponding locations in the Merkle tree of the first and second split-state are checked and compared with the R_1 and R_2 values contained in the proof statement in the third split-state. If they do no match, an error is outputted. In the security proof, we reduce a leakage/tampering adversary A to an adversary A' against the SS-BRM PKE scheme. To achieve this, when A submits its tampering query $f = (f_1, f_2, f_3)$, A' will use its post challenge leakage query to output a bit corresponding to each leaf block in the first and second split-state indicating whether the block is consistent with the corresponding Merkle root, R_1 or R_2. Now in order to decode and update there are two cases, if the hash values R_1 or R_2 change, then the statement of the NIZK changes and a candidate encryption and signature secret key can be extracted from the proof. If the public keys, R_1 and R_2 do not change, then the candidate encryption and signature secret keys are the original keys and the CCA oracle can be used for decryption. In addition, during each decode/update, before the candidate secret keys are used to perform the decryption or signing operation, the post-challenge leakage is used to verify that the corresponding blocks needed to perform the operation are consistent with the R_1 and R_2 values contained in the proof. If yes, the candidate key is used to decrypt or sign. If not, then an error is produced. See Section 3.

On 2 vs 3 split-states. A natural question is whether we can reduce the number of split-states to 2, which would be optimal. Towards answering this question, recall our newly introduced notion *CCA secure SS-BRM public key encryption*, (described in the previous section), which given leakage parameter ℓ, stores the secret key in a split-state and guarantees CCA security even under ℓ bits of split-state leakage before and *after* seeing the challenge ciphertext. This notion gives rise to a 3-split-state construction of LDUNMC in the BRM model, since each split-state of the key and the ciphertext must be stored separately. We note that our construction of CCA secure SS-BRM public key encryption, given in the full version [27] achieves a stronger notion of security, where the secret key $\mathsf{sk} := \mathsf{sk}_1 || \mathsf{sk}_2$ is split into two parts and two phases of leakage are allowed: In the first phase, leakage is allowed on sk_1 and on (sk_2, c), where c is the challenge ciphertext. Then, the challenge ciphertext is given to the adversary and an additional leakage query is allowed on sk_1 and on sk_2. While this notion seems useful for achieving 2-split-state construction of LDUNMC in the BRM model, since sk_1 can be stored in one split-state and (sk_2, c) in the other, this approach does not work for our construction (as we elaborate below). We therefore choose to present the simpler notion of *CCA secure SS-BRM public key encryption* in

Subsection 2.2 and we refer reader to the full version of the paper [27] for the construction/security proof.

The above does not help in reducing our construction from 3 to 2 split-states since our proof requires one of the split-states (which contains the ciphertexts, the Merkle tree, the signature on the root and the simulation-sound NIZK proof of knowledge) to be *entirely public*, and thus must be stored in a separate state, apart from both sk_1 and sk_2. This allows us to fully simulate the entire contents of the split-state after the tampering function has been applied, which enables us to use the NIZK knowledge extractor to extract the encryption and signature secret keys from the (tampered) NIZK proof (as described previously). We cannot rely on the BRM security of the encryption/signature scheme to instead *leak* the extracted witness, since the witness corresponds to the encryption and signature secret keys, which are required to be larger than the allowed leakage bound, ℓ, in order for security of the encryption/signature scheme to be possible.

1.3 Related Work

Non-Malleable Codes. The concept of non-malleability, introduced by Dolev, Dwork and Naor [34] has been applied widely in cryptography, in both the computational and information-theoretic setting. Error-correcting codes and early works on tamper resilience [45,50] gave rise to the study of non-malleable codes. The notion of non-malleable codes was formalized in the seminal work of Dziembowski, Pietrzak and Wichs [39]. Split state classes of tampering functions introduced by Liu and Lysyanskaya [62], have subsequently received much attention with a sequence of improvements achieving reduced number of states, improved rate, or other desirable features [36,3,20,2,7,1,56]. Recently [12,13,6,19,41] gave efficient constructions of non-malleable codes for "non-compartmentalized" tampering function classes. Other works on non-malleable codes and memory tampering attacks include [52,42,23,4,51,16,5,53].

There are also several inefficient, existential or randomized constructions for much more general classes of functions in addition to those above [39,22,44]. Choi et al. [24], in the context of designing UC secure protocols via tamperable hardware tokens, consider a variant of non-malleable codes which has *deterministic* encoding and decoding. In contrast, our work relies on both randomized encoding and decoding, as does the recent work of [12]. Chandran et al. [17] introduced the notion of locally updatable and locally decodable codes. This was extended by Dachman-Soled et al. [29] who introduced the notion of *locally decodable and updatable non-malleable codes* with the application of constructing compilers that transform any RAM machine into a RAM machine secure against leakage and tampering. This application was also studied by Faust et al. [43]. Recently, Chandran et al. [18] studied information-theoretic local non-malleable codes. Dachman-Soled et al. [28] gave tight upper and lower bounds on the construction of LDUNMC.

Memory Leakage Attacks. Recently, the area of *Leakage Resilient Cryptography* has received much attention by the community. Here, the goal is to design cryptographic primitives resistant to arbitrary side-channel attacks, permitting the adversary to learn information about the secret key adaptively, as long as the *total amount* of leaked information is bounded by some leakage parameter ℓ. The majority of the results are in the *Relative Leakage Model*, which allows the systems parameters to depend on ℓ with aim of making ℓ as large as possible relative to the length of the secret key. Akavia et al. [8] started the study of side-channel attacks in the *public-key* setting by showing Regev's encryption scheme [67] is leakage resilient in the relative leakage model. Naor and Segev [63] constructed new public-key schemes based on non-lattice assumptions, which allowed for more leakage and achieved CCA security. Katz and Vaikuntanathan [55] subsequently developed signature schemes in the relative leakage model.

The Bounded Retrieval Model (BRM). Introduced in [30,35], the model assumes a bound ℓ on the overall amount of information learned by the adversary during the lifetime of the system (usually by setting ℓ very large). This model differs from the relative leakage model since it ensures that all the system parameters, except the length of the secret key, are independent of ℓ. Dziembowski [35], constructed a symmetric key authenticated key agreement protocol in Random Oracle model for the BRM setting, which was subsequently extended to standard model [15]. Password authentication and secret sharing in the BRM, was studied in [30], and [38] respectively. *Non-interactive* symmetric key encryption schemes using partially compromised keys were constructed by [66] implicitly and by [31] explicitly. The first public key cryptosystems in the BRM were provided by [10] who built leakage-resilient identification schemes, leakage-resilient signature schemes (in the random oracle model), and provided tools for converting schemes in relative leakage model to the BRM. Recently, Faonio et al. [40] presented a construction of another weaker variant of leakage resilient signature schemes (introduced by [65]); in BRM using random oracles. The first PKE scheme in the BRM was provided by [9] based on assumptions like lattices, quadratic residuosity and bilinear maps. Alwen et al. [11] provide an excellent survey of various leakage resilient primitives in BRM.

2 Preliminaries

in this section we introduce the preliminaries on local non-malleable codes, RAM and bounded retrieval model.

2.1 Preliminaries on Local Non-Malleable Codes

In this section we first review the notion of decodable and updatable codes. We then present one time tampering and leakage experiment.

Definition 1 (Locally Decodable and Updatable Code). *Let $\Sigma, \hat{\Sigma}$ be sets of strings, and $n, \hat{n}, p, q$ be some parameters. An $(n, \hat{n}, p, q)$ locally decodable and updatable coding scheme consists of three algorithms* (ENC, DEC, UPDATE) *with the following syntax:*

- *The encoding algorithm* ENC (perhaps randomized) *takes input an n-block (in Σ) database and outputs an $\hat{n}$-block (in $\hat{\Sigma}$) codeword.*

- *The (local) decoding algorithm* DEC *takes input an index in* $[n]$*, reads at most* p *blocks of the codeword, and outputs a block of the database in* Σ*. The overall decoding algorithm simply outputs* $(\mathsf{DEC}(1), \mathsf{DEC}(2), \ldots, \mathsf{DEC}(n))$*.*
- *The (local) updating algorithm* UPDATE (perhaps randomized) *takes inputs an index in* $[n]$ *and a string in* $\Sigma \cup \{\epsilon\}$*, and reads/writes at most* q *blocks of the codeword. Here the string* ϵ *denotes the procedure of refreshing without changing anything.*

Let $C \in \hat{\Sigma}^{\hat{n}}$ *be a codeword. For convenience, we denote* $\mathsf{DEC}^C, \mathsf{UPDATE}^C$ *as the processes of reading/writing individual blocks of the codeword, i.e. the codeword oracle returns or modifies an individual block upon a query. Recall that* C *is a random access memory where the algorithms can read/write to the memory* C *at individual different locations.*

Definition 2 (Correctness). *An* $(n, \hat{n}, p, q)$ *locally decodable and updatable coding scheme (with respect to* $\Sigma, \hat{\Sigma}$*) satisfies the following properties. For any database* $D = (D_1, D_2, \ldots, D_n) \in \Sigma^n$*, let* $C = (C_1, C_2, \ldots, C_{\hat{n}}) \leftarrow \mathsf{ENC}(D)$ *be a codeword output by the encoding algorithm. Then we have:*

- *for any index* $i \in [n]$*,* $\Pr[\mathsf{DEC}^C(i) = D_i] = 1$*, where the probability is over the randomness of the encoding algorithm.*
- *for any update procedure with input* $(i, v) \in [n] \times \Sigma \cup \{\epsilon\}$ *and for all* $j \in \mathbb{N}$*, let* $C^{(j+1)}$ *be the resulting codeword by running* $\mathsf{UPDATE}^{C^{(j)}}(i, v)$*. Then we have* $\Pr[\mathsf{DEC}^{C^{(j+1)}}(i) = v] = 1$*, where the probability is over the encoding and update procedures. Moreover, the decodings of the other positions remain unchanged.*

Following [29], our definition includes a third party called the *updater*, who reads the underlying messages and decides how to update the codeword. This notion captures the RAM program computing on the underlying, unencoded data. The adversary learns the location that the updater updated the messages, but not the content of the updated messages.

Our experiment is interactive and consists of rounds: The adversary adaptively chooses two rounds i, j such that $i \leq j$, submits a leakage function in round i, gets its output and then submits a tampering function in round j. We assume WLOG that at the end of each round, the updater runs UPDATE, and the codeword will be somewhat updated and refreshed. The security experiment then considers the decoding of the entire message after each round.

Definition 3 (One Time Tampering and Leakage Experiment). *Let* λ *be the security parameter,* $\mathcal{F}, \mathcal{G}$ *be some families of functions. Let* (ENC, DEC, UPDATE) *be an* $(n, \hat{n}, p, q)$*-locally decodable and updatable coding scheme with respect to* $\Sigma, \hat{\Sigma}$*. Let* $\mathcal{U}$ *be an updater that takes input a database* $D \in \Sigma^n$ *and outputs an index* $i \in [n]$ *and* $v \in \Sigma \cup \{\epsilon\}$*. Flags* Leaked *and* $\mathsf{Tampered}$ *will be set to 0 and let* r *be the total number of rounds. Then for any blocks of databases* $D = (D_1, D_2, \ldots, D_n) \in \Sigma^n$*, and any (non-uniform) adversary* $\mathcal{A}$*, any updater* $\mathcal{U}$ *define the following experiment* $\mathbf{TamperLeak}_{\mathcal{A},\mathcal{U},D}$*:*

- *Let $D^{(0)} = D$. The challenger first computes an initial encoding $C^{(0)} \leftarrow \mathsf{ENC}(D)$.*
- *Then the following procedure repeats, at each round j, recall $C^{(j)}$ be the current codeword and $D^{(j)}$ be the underlying database:*
  - *The updater computes $(i^{(j)}, v) \leftarrow \mathcal{U}(D^{(j)})$ for the challenger. The challenger runs $\mathsf{UPDATE}^{C^{(j)}}(i^{(j)}, v)$.*
  - *$\mathcal{A}$ sends either a tampering function $f \in \mathcal{F}$ and/or a leakage function $g \in \mathcal{G}$ or $\perp$ to the challenger.*
  - *if* Leaked *is 0 and g is sent by $\mathcal{A}$, the challenger sends back a leakage $\ell = g(C^{(j+1)})$ and sets* Leaked *to 1.*
  - *if* Leaked *is 1,* Tampered *is 0 and f is sent by $\mathcal{A}$, the challenger replaces the codeword with $f(C^{(j+1)})$ and sets* Tampered *to 1.*
  - *if* Leaked *is 1,* Tampered *is 1, ignore any function sent by $\mathcal{A}$.*
  - *We define $D^{(j+1)} \overset{\text{def}}{=} \left(\mathsf{DEC}^{C^{(j+1)}}(1), \ldots, \mathsf{DEC}^{C^{(j+1)}}(n)\right)$. Where $C^{(j+1)}$ is the tampered codeword.*
  - *$\mathcal{A}$ may terminate the procedure at any point.*
- *Let r be the total number of rounds. At the end, the experiment outputs $\left(\ell, D^{(0)}, \ldots, D^{(r)}\right)$.*

Definition 4 (One Time Non-malleability and Leakage Resilience against Attacks). *An $(n, \hat{n}, p, q)$-locally decodable and updatable coding scheme with respect to $\Sigma, \hat{\Sigma}$ is non-malleable against $\mathcal{F}$ and leakage resilient against $\mathcal{G}$ if for all* PPT *(non-uniform) adversaries $\mathcal{A}$, and* PPT *updater $\mathcal{U}$, there exists some* PPT *(non-uniform) simulator $\mathcal{S}$ such that for any $D = (D_1, \ldots, D_n) \in \Sigma^n$, $\textbf{TamperLeak}_{\mathcal{A},\mathcal{U},D}$ is (computationally) indistinguishable to the following ideal experiment $\textbf{Ideal}_{\mathcal{S},\mathcal{U},D}$:*

- *The experiment proceeds in rounds. Let $D^{(0)} = D$ be the initial database.*
- *At each round j, the experiment runs the following procedure:*
  - *At the beginning of each round, the updater runs $(i^{(j)}, v) \leftarrow \mathcal{U}(D^{(j)})$ and sends the index $i^{(j)}$ to the simulator. If $v = \epsilon$, set $D^{(j+1)} := D^{(j)}$ otherwise the experiment updates $D^{(j+1)}$ as follows: $D^{(j+1)} := D^{(j)}$ for all coordinates except $i^{(j)}$, and set $D^{(j+1)}[i^{(j)}] := v$.*
  - *$\mathcal{S}$ outputs $(\mathcal{I}^{(j+1)}, \boldsymbol{w}^{(j+1)})$, where $\mathcal{I}^{(j+1)} \subseteq [n]$.*
  - *Define*

$$D^{(j+1)} = \begin{cases} \boldsymbol{w}^{(j+1)} & \text{if } \mathcal{I}^{(j+1)} = [n] \\ D^{(j+1)}|_{\mathcal{I}^{(j+1)}} := \perp, D^{(j+1)}|_{\bar{\mathcal{I}}^{(j+1)}} := D^{(j+1)}|_{\bar{\mathcal{I}}^{(j+1)}} & \text{otherwise} \end{cases}$$

  where $\boldsymbol{x}|_{\mathcal{I}}$ denotes the coordinates $\boldsymbol{x}[v]$ where $v \in \mathcal{I}$, and bar denotes complement.
- *Let r be the total number of rounds. $\mathcal{S}$ outputs ℓ and the experiment outputs $\left(\ell, D^{(0)}, \ldots, D^{(r)}\right)$.*

2.2 Preliminaries on RAM and Primitives in the BRM

We define random access machine, public key encryption in BRM and signature schemes in the BRM and introduce a new construction called Split-State Public Key Encryption in Bounded Retrieval Model ($\mathsf{SS\text{-}BRM\text{-}PKE}$).

Preliminaries on Random Access Machines. We consider RAM programs to be interactive stateful systems $\langle \Pi, \mathsf{state}, D\rangle$, where Π denotes a next instruction function, state denotes the current state stored in registers, and D denotes the content of memory. Upon input state and a value d, the next instruction function outputs the next instruction I and an updated state state'. The initial state of the RAM machine, state, is set to $(\mathsf{start}, *)$. We denote by $\mathsf{A}^D(x)$, the execution of RAM algorithm A with random access to array D and explicit input x. We define operator *Access* which outputs the access patterns of $\mathsf{A}^D(x)$, and denote by $\boldsymbol{I}$ the locations in D accessed by $\mathsf{A}^D(x)$. Thus, we write $\boldsymbol{I} \xleftarrow{Access} \mathsf{A}^D(x)$.

Public Key Encryption in the BRM. A public key encryption scheme ($\mathcal{E}$) in the BRM consists of the algorithms (KeyGen, $\mathsf{Encrypt}$, $\mathsf{Decrypt}$), which are all parameterized by a security parameter λ and a leakage parameter ℓ. The syntax and correctness property of an encryption scheme follow the standard notion of public-key encryption. We define the following CPA game, with leakage ℓ, between an adversary $\mathcal{A}$ and a challenger.

- **Key Generation:** The challenger computes $(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{KeyGen}(1^\lambda, 1^\ell)$ and gives pk to the adversary $\mathcal{A}$.
- **Leakage:** The adversary $\mathcal{A}$ selects a PPT function $g : \{0,1\}^* \to \{0,1\}^\ell$ and gets $g(\mathsf{sk})$ from the challenger.
- **Challenge:** The adversary $\mathcal{A}$ selects two messages m_0, m_1. The challenger chooses $b \leftarrow \{0,1\}$ uniformly at random and gives $c \leftarrow \mathsf{Encrypt}^{\mathsf{pk}}(m_b)$ to the adversary $\mathcal{A}$.
- **Output:** The adversary $\mathcal{A}$ outputs a bit $b' \in \{0,1\}$. We say that $\mathcal{A}$ wins the game if $b' = b$.

For any adversary $\mathcal{A}$, the advantage of $\mathcal{A}$ in the above game is defined as $\mathbf{Adv}^{\mathrm{CPA}}_{\mathcal{E},\mathcal{A}}(\lambda, \ell) \stackrel{\mathrm{def}}{=} |\Pr[\mathcal{A} \text{ wins}] - \frac{1}{2}|$.

Definition 5 (Leakage-Resilient PKE). *[9] A public-key encryption scheme $\mathcal{E}$ is leakage-resilient, if for any polynomial $\ell(\lambda)$ and any PPT adversary $\mathcal{A}$, we have $\mathbf{Adv}^{\mathrm{CPA}}_{\mathcal{E},\mathcal{A}}(\lambda, \ell(\lambda)) = \mathsf{negl}(\lambda)$.*

Definition 6 (PKE in the BRM). *[9] We say that a leakage-resilient PKE scheme is a **PKE in the BRM**, if the public-key size, ciphertext size, encryption-time and decryption-time (and the number of secret-key bits read by decryption) are independent of the leakage-bound ℓ. More formally, **there exist** polynomials $\mathsf{pksize}, \mathsf{ctsize}, \mathsf{encT}, \mathsf{decT}$, such that, **for any** polynomial ℓ and any $(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{KeyGen}(1^\lambda, 1^\ell)$, $m \in \mathcal{M}$, $c \leftarrow \mathsf{Encrypt}^{\mathsf{pk}}(m)$, the scheme satisfies:*

1. *Public-key size is $|\mathsf{pk}| \leq O(\mathsf{pksize}(\lambda))$, ciphertext size is $|c| \leq O(\mathsf{ctsize}(\lambda, |m|))$.*

2. *Run-time of* $\mathsf{Encrypt}^{\mathsf{pk}}(m)$ *is* $\leq O(\mathsf{encT}(\lambda, |m|))$.
3. *Run-time of* $\mathsf{Decrypt}^{\mathsf{sk}}(c)$*, and the number of bits of* sk *accessed is* $\leq O(\mathsf{decT}(\lambda, |m|))$.

The ***relative-leakage*** *of the scheme is* $\alpha \overset{def}{=} \frac{\ell}{|\mathsf{sk}|}$.

Alwen et al. [9] give a generic transformation to construct a CCA-secure PKE scheme in the BRM using Naor-Young "double encryption" paradigm.

Signature Scheme in BRM. Consists of three algorithms: $(\mathsf{Gen}, \mathsf{Sign}, \mathsf{Verify})$. Attacker is separated into two parts, first part, $\mathcal{A}_1$, will interact with leakage oracle and signing oracle and output an arbitrary hint for the second part, $\mathcal{A}_2$. $\mathcal{A}_2$ only accesses signature oracle and tries to forge the signature of a message. The Entropic Unforgeability attack Game EUG_ℓ^λ is as follows:

1. Challenger select $(\mathsf{vk}, help, \mathsf{sk}_\sigma) \leftarrow \mathsf{Gen}(1^\lambda)$ and gives vk to $\mathcal{A}_1$.
2. Adversary $\mathcal{A}_1$ is given access to signing oracle $\mathcal{S}_{\mathsf{sk}_\sigma}(\cdot)$ and leakage oracle $\mathcal{O}_{\mathsf{sk}_\sigma}^{\lambda,\ell}(.)$ and outputs a hint $v \in \{0,1\}^*$.
3. Adversary $\mathcal{A}_2$ is given access to hint v and signing oracle $\mathcal{S}_{\mathsf{sk}_\sigma}(\cdot)$ and outputs message, signature pair (m, σ).

We define the advantage of the attacker $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ to be the probability that $\mathsf{Verify}^{\mathsf{vk}}(m, \sigma) = 1$ and that the signing oracle was never queried with m.

Definition 7 (Signature Scheme). *[10] Let* $View_{\mathcal{A}_1}$ *be a random variable denoting the view of* $\mathcal{A}_1$ *which includes its random coin and the responses it gets from signing oracle and leakage oracle. Let* $MSG_{\mathcal{A}_2}$ *be a random variable of the messages output by* $\mathcal{A}_2$ *in* EUG_ℓ^λ*. Adversary* $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ *is entropic if* $\tilde{H}_\infty(MSG_{\mathcal{A}_2} \mid View_{\mathcal{A}_1}) \geq \lambda$ *for security parameter* λ*. We say a signature scheme is entropically unforgeable with leakage* ℓ *if the advantage of adversary* $\mathcal{A}$ *in* EUG_ℓ^λ *is negligible in* λ*.*

Remark 1. Entropic signatures in the BRM can be constructed in the random oracle (RO) model (cf. [10,11]). Combining a signature scheme in the relative leakage model (with additional properties) such as [55] with the leakage amplification techniques of [10], it may be possible to construct entropic signatures in the BRM without RO. However, as discussed in full version of the paper [27], the primitive we require is slightly weaker than regular entropic signatures in the BRM and can be constructed in a straightforward manner in the standard model, without RO. Nevertheless, for conceptual simplicity we present our constructions and state our theorems in terms of the existence of entropic signatures in the BRM.

Split-State Public Key Encryption in the BRM (SS-BRM-PKE) We define a new primitive called as Split-State Public Key Encryption in Bounded Retrieval Model (SS-BRM-PKE) with the following properties:

1. The secret key sk is stored in the split-state $\mathsf{sk}_1||\mathsf{sk}_2$ and the adversary is allowed to obtain leakage on sk_1 and sk_2 independently.

2. The encryption scheme is secure in the bounded retrieval model, as defined in Definition 6 with respect to the split-state leakage.
3. The encryption scheme is chosen plaintext attack (CPA)-secure even in the presence of adversary who can observe the access pattern of the blocks of pk and $\mathsf{sk}_1||\mathsf{sk}_2$ accessed during encryption and decryption procedure.
4. The scheme is CPA-secure against an adversary getting additional split-state leakage (bounded) on the secret key, even *after* receiving the ciphertext.

Formally, a public key encryption scheme ($\mathcal{E}$) in the SS-BRM consists of the algorithms (KeyGen, $\mathsf{Encrypt}$, $\mathsf{Decrypt}$), which are all parameterized by a security parameter λ and a leakage parameter ℓ. The syntax and correctness property of an encryption scheme follow the standard notion of public-key encryption. We define the following semantic-security game ($\mathsf{SS\text{-}BRM\text{-}PKE\text{-}CPA}$) with leakage ℓ between an adversary $\mathcal{A}$ and a challenger.

- **Key Generation:** The challenger computes $(\mathsf{pk}, \mathsf{sk}_1||\mathsf{sk}_2) \leftarrow \mathsf{KeyGen}(1^\lambda, 1^\ell)$ and gives pk to the adversary $\mathcal{A}$.
- **Message Commitment:** The adversary $\mathcal{A}$ selects two messages m_0, m_1.
- **Pre-challenge Leakage:** The adversary $\mathcal{A}$ selects a PPT function $g := (g_1, g_2) : \{0,1\}^* \times \{0,1\}^* \rightarrow \{0,1\}^\ell \times \{0,1\}^\ell$ and gets $L_1 := g_1(\mathsf{sk}_1)$, $L_2 := g_2(\mathsf{sk}_2)$ from the challenger.
- **Challenge:** The challenger chooses $b \leftarrow \{0,1\}$ uniformly at random and gives $c \leftarrow \mathsf{Encrypt}^{\mathsf{pk}}(m_b)$ to the adversary $\mathcal{A}$.
- **Encryption Access Patterns:** The challenger also sends the access pattern $(i^{(1)}, i^{(2)}, \ldots, i^{(t)})$ corresponding to the encryption procedure, to $\mathcal{A}$.
- **Post-challenge Leakage:** The adversary $\mathcal{A}$ selects a PPT function $g' := (g'_1, g'_2) : \{0,1\}^* \times \{0,1\}^* \rightarrow \{0,1\}^\ell \times \{0,1\}^\ell$ and gets $L'_1 := g'_1(L_1, L_2, c, \mathsf{sk}_1)$, $L'_2 := g'_2(L_1, L_2, c, \mathsf{sk}_2)$ from the challenger.
- **Decryption Access Patterns:** The challenger also sends the access pattern $(S^1, S^2) \xleftarrow{Access} \mathsf{Decrypt}^{\mathsf{sk}_1||\mathsf{sk}_2}(c)$, to $\mathcal{A}$. S^i is a set of indices s^i_j of sk_i for $i \in \{1,2\}$ and $j \in [n]$, where $|\mathsf{sk}_1| = |\mathsf{sk}_2| = n$. Also, $|S^i| = t$, where t is the number of locations of sk_1 and sk_2 required to be accessed to decrypt any ciphertext.
- **Output:** The adversary $\mathcal{A}$ outputs a bit $b' \in \{0,1\}$. We say that $\mathcal{A}$ wins the game if $b' = b$.

For any adversary $\mathcal{A}$, the advantage of $\mathcal{A}$ in the above game is defined as $\mathbf{Adv}^{\mathsf{SS\text{-}BRM\text{-}PKE\text{-}CPA}}_{\mathcal{E},\mathcal{A}}(\lambda, \ell) \overset{\text{def}}{=} |\Pr[\mathcal{A}\,\text{wins}] - \frac{1}{2}|$. It should be noted that the decryption access patterns indicating which parts of secret key were accessed during the decryption must be provided to the adversary only *after* the leakage information, otherwise the adversary can simply ask for the leakage on the secret key positions "relevant" to the decryption of the challenge ciphertext.

Chosen Ciphertext Attack (CCA) security for $\mathsf{SS\text{-}BRM\text{-}PKE}$ can be defined as the natural analogue of the above $\mathsf{SS\text{-}BRM\text{-}PKE\text{-}CPA}$ security experiment above. We refer reader to full version of the paper [27] for the formal definition and the construction. Given a $\mathsf{SS\text{-}BRM\text{-}PKE\text{-}CPA}$ scheme, a $\mathsf{SS\text{-}BRM\text{-}PKE\text{-}CCA}$ scheme can be constructed via the double encryption paradigm (cf. [64,60,9]).

2.3 Additional Preliminaries

In this section we present definitions which are being used in the constructions.

Definition 8 (Entropy). *The min-entropy of a random variable X is defined as $H_\infty(X) = -\log(\max_x \Pr[X = x])$. The conditional min-entropy of a random variable X, conditioned on the experiment $\mathcal{E}$ is $\tilde{H}_\infty(X|\mathcal{E}) = -\log(\max_{\mathcal{A}} \Pr[\mathcal{A}^{\mathcal{E}(\cdot)}() = X])$. In the special case that $\mathcal{E}$ is a non-interactive experiment which simply outputs a random variable Z, it is written as $\tilde{H}_\infty(X|Z)$.*

Definition 9 (Seed-Dependent Condenser [33]). *An efficient function $\mathsf{Cond} : \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^m$ is a seed-dependent $([\boldsymbol{H}_\infty \geq k] \to_\varepsilon [\boldsymbol{H}_\infty \geq k'], t)$-condenser if for all probabilistic adversaries $\mathcal{A}$ of size at most t who take a random seed $S \leftarrow \{0,1\}^d$ and output (using more coins) a sample $X \leftarrow \mathcal{A}(S)$ of entropy $\boldsymbol{H}_\infty(X|S) \geq k$, the joint distribution $(S, \mathsf{Cond}(X; S))$ is ε-close to some (S, R), where $\boldsymbol{H}_\infty(R|S) \geq k'$.*

We present the collision resistant hash function and Merkle Tree which are being used to prevent mauling attacks.

Definition 10 (Collision-Resistant Hash Function Family [33]). *A family of hash functions $\mathcal{H} := \{h : \{0,1\}^* \to \{0,1\}^m\}$ is (t, δ)-collision-resistant if for any (non-uniform) attacker $\mathcal{B}$ of size at most t,*

$$\Pr[H(X_1) = H(X_2) \wedge X_1 \neq X_2] \leq \delta \text{ where } H \leftarrow \mathcal{H} \text{ and } (X_1, X_2) \leftarrow \mathcal{B}(H).$$

Theorem 2 (Theorem 4.1 [33]). *Fix any $\beta > 0$. If $\mathcal{H}$ is a $(2t, 2^{\beta-1}/2^m)$-collision-resistant hash function family, then $\mathsf{Cond}(X; H) \overset{def}{=} H(x)$ for $H \leftarrow \mathcal{H}$ is a seed-dependent $(([\mathbf{H}_\infty \geq m-\beta+1] \to [\mathbf{H}_\infty \geq m-\beta+\log\varepsilon]), t)$-condenser.*

Definition 11 (Merkle Tree). *Let $h : \mathcal{X} \times \mathcal{X} \to \mathcal{X}$ be a hash function that maps two blocks of messages to one.[3] A Merkle Tree $\mathsf{Tree}_h(M)$ takes as input a message $M = (m_1, m_2, \ldots, m_n) \in \mathcal{X}^n$. Then it applies the hash on each pair (m_{2i-1}, m_{2i}), resulting in $n/2$ blocks. Then again, it partitions the blocks into pairs and applies the hash on the pairs, which results in $n/4$ blocks. This is repeated $\log n$ times, resulting a binary tree with hash values, until one block remains. We call this value the root of Merkle Tree denoted $\mathsf{Root}_h(M)$, and the internal nodes (including the root) as $\mathsf{Tree}_h(M)$. Here M can be viewed as leaves.*

Theorem 3. *Assuming h is a collision resistant hash function. Then for any message $M = (m_1, m_2, \ldots, m_n) \in \mathcal{X}^n$, any polynomial time adversary $\mathcal{A}$, $\Pr\Big[(m_i', p_i) \leftarrow \mathcal{A}(M, h) : m_i' \neq m_i, p_i \text{ is a consistent path with } \mathsf{Root}_h(M)\Big] \leq \mathsf{negl}(\lambda)$.*

Moreover, given a path p_i passing through the leaf m_i; and a new value m_i', there is an algorithm that computes $\mathsf{Root}_h(M')$ in time $\mathrm{poly}(\log n, \lambda)$, where $M' = (m_1, \ldots, m_{i-1}, m_i', m_{i+1}, \ldots, m_n)$.

[3] Here we assume $|\mathcal{X}|$ is greater than the security parameter.

In the following we present simulation-sound extractable NIZK proof for which an efficient construction can be found in [47].

Definition 12 (NIZK Proof System). *Let R be an efficiently computable binary relation. For pairs $(x, w) \in R$ we call x the statement and w the witness. Let L be the language consisting of statements in R. A proof system for a relation R consists of a crs generation algorithm* (CRSGEN)*, prover* (P) *and verifier* (V)*, which satisfy completeness and soundness properties as follows.*

Definition 13 (Completeness). *For all $x \in L$ and all the witnesses w*

$$\Pr\left[\mathsf{V}(crs, x, \pi \leftarrow \mathsf{P}(crs, x, w)) = 1\right] \geq 1 - negl(\lambda)$$

Definition 14 (Computational Zero-Knowledge). *We call* $(\mathsf{CRSGEN}, \mathsf{P}, \mathsf{V})$ *an NIZK proof for relation R if there exists a polynomial time simulator $\mathcal{S} = (\mathcal{S}_1, \mathcal{S}_2)$ such that for all non-uniform polynomial time adversaries $\mathcal{A}$ we have*

$$\Pr\left[crs \leftarrow \mathsf{CRSGEN}(1^\lambda) : \mathcal{A}^{\mathsf{P}(crs,\cdot,\cdot)}(crs) = 1\right]$$

$$\overset{c}{\approx}$$

$$\Pr\left[(crs, \tau) \leftarrow \mathcal{S}_1(1^\lambda) : \mathcal{A}^{\mathcal{S}(crs,\tau,\cdot,\cdot)}(crs) = 1\right]$$

where $\mathcal{S}(crs, \tau, x, w) = \mathcal{S}_2(crs, \tau, x)$ for $(x, w) \in R$ and both oracles output failure if $(x, w) \notin R$.

Definition 15 (Simulation-Sound Extractability [47]). *Consider an NIZK proof of knowledge* $(\mathsf{CRSGEN}, \mathsf{P}, \mathsf{V}, \mathcal{S}_1, \mathcal{S}_2, E_1, E_2)$*. Let $\mathcal{S}E_1$ be an algorithm that outputs (crs, τ, ξ) such that it is identical to $\mathcal{S}_1$ when restricted to the first two parts (crs, τ). We say the NIZK proof is simulation sound if for all non-uniform polynomial time adversaries we have*

$$\begin{aligned}\Pr[(crs, \tau, \xi) \leftarrow & \mathcal{S}E_1(1^\lambda); (x, \pi) \leftarrow \mathcal{A}^{\mathcal{S}_2(crs,\tau,\cdot)}(crs, \xi); w \leftarrow E_2(crs, \xi, x, \pi) : \\ & (x, \pi) \notin Q \text{ and } (x, w) \notin R \text{ and } \mathsf{V}(crs, x, \pi) = 1] \approx 0\end{aligned} \tag{1}$$

where Q is the list of simulation queries and responses (x_i, π_i).

Definition 16 (Probabilistically Checkable Proofs [14]). *For functions $r, q : \mathbb{N} \rightarrow \mathbb{N}$ we say that a probabilistic oracle machine V is a (r, q)-PCP verifier if, on input a binary string x of length n and given oracle access to a binary string π, V runs in time $2^{O(r(n))}$, tosses $r(n)$ coins, makes $q(n)$ queries to π, and outputs either 1 (accept) or 0 (reject). A language L belongs in the class $PCP_s[r(n), q(n)]$ if there exists a (r, q)-PCP verifier V_L such that the following holds:*

1. *Completeness: If $x \in L$ then there exists π such that $\Pr_R[V_L^\pi(x; R) = 1] = 1$.*
2. *Soundness: If $x \notin L$ then for every π it holds that $\Pr_R[V_L^\pi(x; R) = 1] < 1/2$.*

Theorem 4 (PCP Theorem). *NP = PCP[O(log n), O(1)].*

To achieve negligible soundness, we can run the verifier polylogarithmic number of times in parallel, which results in polylogarithmic number of verifier queries to the proof, π. In [14], they give constructions of PCPs with the above properties, which also allow for knowledge extraction. I.e., assuming $\Pr_R[V_L^\pi(x; R) = 1] \geq 1/2$, there is an efficient extractor which, given π, can extract a witness w for the statement $x \in L$.

3 Achieving Full One-Time Tamper and Leakage Resilience (OT-TLR)

We next present our construction to achieve full resilience against one time leakage and tampering attacks. The relevant definitions can be found in Subsection 2.3. As a preliminary step, we present a construction for achieving resilience against one time leakage and partial tampering attacks and we refer to full version of the paper [27] for the details of the construction.

Construction $\mathit{\Pi} = (\mathsf{ENC}, \mathsf{DEC}, \mathsf{UPDATE})$. Let $\mathcal{E} = (\mathsf{KeyGen}, \mathsf{Encrypt}, \mathsf{Decrypt})$ be a CCA-secure SS-BRM-PKE scheme, $\mathcal{V} = (\mathsf{Gen}, \mathsf{Sign}, \mathsf{Verify})$ be a signature scheme in the BRM and H is a family of collision resistance hash functions and $\mathit{\Pi}_{NIZK}$, $\mathit{\Pi}_{PCP}$ which are NIZK and PCP proof systems, respectively. Then we consider the following coding scheme:

Preprocessing. $crs \leftarrow \mathsf{CRSGEN}(1^\lambda)$ and $h \leftarrow H$ are sampled and $CRS := (crs, h)$ is published. Note that the size of CRS depends on security parameter, but not on the size of the database nor on the leakage parameter ℓ. Note that CRS is implicit input to all algorithms.

$\mathsf{ENC}(D)$: On input database $D = (D_1, D_2, \ldots, D_n) \in \mathit{\Sigma}^n$:

- Choose $(\mathsf{pk}, \mathsf{sk}_\varepsilon^1, \mathsf{sk}_\varepsilon^2) \leftarrow \mathcal{E}.\mathsf{KeyGen}(1^\lambda, 1^\ell)$, where $\mathsf{sk}_\varepsilon^1 \in \hat{\mathit{\Sigma}}^{n'_1}, \mathsf{sk}_\varepsilon^2 \in \hat{\mathit{\Sigma}}^{n'_2}$, and define $\mathsf{sk}_\varepsilon := (\mathsf{sk}_\varepsilon^1 || \mathsf{sk}_\varepsilon^2)$, $(\mathsf{vk}, \mathsf{sk}_\sigma) \leftarrow \mathcal{V}.\mathsf{Gen}(1^\lambda)$.
- Set $\tilde{D}_0 := 0$.
- Compute $\tilde{D}_i \leftarrow \mathcal{E}.\mathsf{Encrypt}^{\mathsf{pk}}(D_i)$ for $i \in [n]$. Let $\tilde{D} := \tilde{D}_0, \ldots, \tilde{D}_n$. Set[4] $T_{\tilde{D}} := \mathsf{Tree}_h(\tilde{D})$, $\sigma := \mathcal{V}.\mathsf{Sign}^{\mathsf{sk}_\sigma}(R_{\tilde{D}})$, where $R_{\tilde{D}} := \mathsf{Root}_h(T_{\tilde{D}})$.
- Construct the hash tree for secret keys $\mathsf{sk}_\varepsilon^1, \mathsf{sk}_\sigma, T_{\mathsf{sk}^1} = \mathsf{Tree}_h(\mathsf{sk}_\varepsilon^1, \mathsf{sk}_\sigma)$ and $R_{\mathsf{sk}^1} := \mathsf{Root}_h(T_{\mathsf{sk}^1})$. Repeat the same procedure for secret key $\mathsf{sk}_\varepsilon^2$ and compute $T_{\mathsf{sk}^2} = \mathsf{Tree}_h(\mathsf{sk}_\varepsilon^2)$ and $R_{\mathsf{sk}^2} := \mathsf{Root}_h(T_{\mathsf{sk}^2})$.
- For the statement $x_{NIZK} = (\mathsf{pk}, \mathsf{vk})||$ "I know pre-images of hashes $R_{\mathsf{sk}^1}, R_{\mathsf{sk}^2}$" and witness $w = (\mathsf{sk}_\varepsilon || \mathsf{sk}_\sigma)$ construct the proof $\pi_{NIZK} \leftarrow \mathit{\Pi}_{NIZK}.\mathsf{P}(crs, x_{NIZK}, w)$.
- For the statement $x_{PCP} =$ "I know an accepting NIZK proof for the statement x_{NIZK}", construct a proof $\pi_{PCP} \leftarrow \mathit{\Pi}_{PCP}.\mathsf{P}(crs, x_{PCP}, \pi_{NIZK})$.

[4] We additionally pad the tree T with dummy leaves consisting of uniform random values to ensure that the relative leakage on the second split state, C_2 is at least $\frac{1}{6}$.

- Output codeword $C := (C_1, C_2, C_3) \in \hat{\Sigma}^{n_1} \times \hat{\Sigma}^{n_2} \times \hat{\Sigma}^{n_3}$, where

$$C_1 := (\mathsf{sk}_\varepsilon^1, \mathsf{sk}_\sigma, T_{\mathsf{sk}^1}, R_{\mathsf{sk}^1}) \quad C_2 := (\mathsf{sk}_\varepsilon^2, T_{\mathsf{sk}^2}, R_{\mathsf{sk}^2})$$

$$C_3 := (\mathsf{pk}, \mathsf{vk}, \tilde{D}, T_{\tilde{D}}, R_{\tilde{D}}, \sigma, \pi_{PCP})$$

$\mathsf{DEC}^C(i)$: On input $i \in [n]$:

- Parse $C := (\mathsf{sk}_\varepsilon^1, \mathsf{sk}_\sigma, T_{\mathsf{sk}^1}, R_{\mathsf{sk}^1}, \mathsf{sk}_\varepsilon^2, T_{\mathsf{sk}^2}, R_{\mathsf{sk}^2}, \mathsf{pk}, \mathsf{vk}, \tilde{D}, T_{\tilde{D}}, R_{\tilde{D}}, \sigma, \pi_{PCP})$.
- Check whether $\tilde{D}_0 := 0$. If not, output $\perp$ and terminate.
- Read path p_i in $T_{\tilde{D}}$, corresponding to leaf i and use p_i to recompute $\hat{R} = \mathsf{Root}_h(p_i)$.
- Check that $\hat{R} := R_{\tilde{D}}$. If not, output $\perp$ and terminate.
- Check that $\mathcal{V}.\mathsf{Verify}^{\mathsf{vk}}(R_{\tilde{D}}, \sigma) = 1$. If not, output $\perp$ and terminate.
- Run $\Pi_{PCP}.\mathsf{V}(crs, x_{PCP}, \pi_{PCP})$ if outputs 0, output $\perp$ and terminate.
- For each accessed location of $\mathsf{sk}_\varepsilon^1$ and $\mathsf{sk}_\varepsilon^2$, read the paths in T_{sk^1} and T_{sk^2}, respectively. Compute $\hat{R}_{\mathsf{sk}^1} = \mathsf{Root}_h(T_{\mathsf{sk}^1})$, $\hat{R}_{\mathsf{sk}^2} = \mathsf{Root}_h(T_{\mathsf{sk}^2})$ and verify that $\hat{R}_{\mathsf{sk}^1} = R_{\mathsf{sk}^1}$ and $\hat{R}_{\mathsf{sk}^2} = R_{\mathsf{sk}^2}$ for each of them. If any of the verification failed, output $\perp$ and terminate.
- Output $D_i := \mathcal{E}.\mathsf{Decrypt}^{\mathsf{sk}_\varepsilon^1 || \mathsf{sk}_\varepsilon^2}(\tilde{D}_i)$.

$\mathsf{UPDATE}^C(i, v)$: On inputs an index $i \in [n]$, and a value $v \in \Sigma$:

- Run $\mathsf{DEC}^C(i)$. If it outputs $\perp$, set $\tilde{D}_0 := 1$, write back to memory and terminate.
- Parse $C := (\mathsf{sk}_\varepsilon^1, \mathsf{sk}_\sigma, T_{\mathsf{sk}^1}, R_{\mathsf{sk}^1}, \mathsf{sk}_\varepsilon^2, T_{\mathsf{sk}^2}, R_{\mathsf{sk}^2}, \mathsf{pk}, \mathsf{vk}, \tilde{D}, T_{\tilde{D}}, R_{\tilde{D}}, \sigma, \pi_{PCP})$.
- Set $\tilde{D}'_i \leftarrow \mathcal{E}.\mathsf{Encrypt}^{\mathsf{pk}}(v)$ Let $\tilde{D}' := \tilde{D}_0, \ldots, \tilde{D}_{i-1}, \tilde{D}'_i, \tilde{D}_{i+1}, \ldots, \tilde{D}_n$.
- Read path p_i in $T_{\tilde{D}}$, corresponding to leaf i and use $(p_i, \tilde{D}'_i)$ to compute a new path p'_i (that replaces $\tilde{D}_i$ by $\tilde{D}'_i$). Set $R'_{\tilde{D}} = \mathsf{Root}_h(p'_i)$. Let $T'_{\tilde{D}}$ denote the updated tree.
- Compute $\sigma' := \mathcal{V}.\mathsf{Sign}^{\mathsf{sk}_\sigma}(R'_{\tilde{D}})$.
- For each accessed location of sk_σ read the paths in T_{sk^1}. Compute $\hat{R}_{\mathsf{sk}^1} = \mathsf{Root}_h(T_{\mathsf{sk}^1})$ and verify that $\hat{R}_{\mathsf{sk}^1} = R_{\mathsf{sk}^1}$ for each of them. If any of the verification failed, output $\perp$ and terminate.
- Write back $(\tilde{D}'_i, T'_{\tilde{D}}, p'_i, R'_{\tilde{D}}, \sigma')$ yielding updated codeword $C' := (C'_1, C'_2, C'_3)$ where

$$C'_1 := (\mathsf{sk}_\varepsilon^1, \mathsf{sk}_\sigma, T_{\mathsf{sk}^1}, R_{\mathsf{sk}^1}) \quad C'_2 := (\mathsf{sk}_\varepsilon^2, T_{\mathsf{sk}^2}, R_{\mathsf{sk}^2})$$

$$C'_3 := (\mathsf{pk}, \mathsf{vk}, \tilde{D}', T'_{\tilde{D}'}, R'_{\tilde{D}'}, \sigma', \pi_{PCP}).$$

Locality of the construction. DEC and UPDATE must read the entire CRS, whose size depends only on security parameter λ and not on the size of the data. In addition, using the SS-BRM-PKE scheme, refer to full version [27] for construction, (along with sub-exponentially hard PRG), and the PCP of [14], DEC and UPDATE must make polylog(λ) number of random accesses to C.

Remark 2. Note that although computing the PCP proof π_{PCP} is expensive, it is only done a single time, during ENC, but remains static during UPDATE.

Theorem 5. *For security parameter $\lambda \in \mathbb{N}$, leakage parameter $\ell := \ell(\lambda)$, alphabet Σ such that $\log|\Sigma| \in \Omega(\lambda)$, and database size $n := n(\lambda)$: Assume $\mathcal{E} = (\mathsf{KeyGen}, \mathsf{Encrypt}, \mathsf{Decrypt})$ is a CCA-secure SS-BRM PKE scheme with leakage parameter $2\ell + \lambda$ and relative leakage $\alpha < 1$, $\mathcal{V} = (\mathsf{Gen}, \mathsf{Sign}, \mathsf{Verify})$ is a signature scheme in the BRM with leakage parameter $2\ell + \lambda$ and relative leakage $\alpha < 1$, H is a family of collision resistant hash functions with sub-exponential security, and Π_{NIZK}, Π_{PCP} are NIZK with simulation-sound extractability and PCP proof systems, respectively. Then Π is a one-time tamper and leakage resilient locally decodable and updatable code taking messages in Σ^n to codewords in $\hat{\Sigma}^{n_1} \times \hat{\Sigma}^{n_2} \times \hat{\Sigma}^{n_3}$, which is secure against tampering class*

$$\bar{\mathcal{F}} \stackrel{\text{def}}{=} \left\{ \begin{matrix} f : \hat{\Sigma}^{n_1} \times \hat{\Sigma}^{n_2} \times \hat{\Sigma}^{n_3} \to \hat{\Sigma}^{n_1} \times \hat{\Sigma}^{n_2} \times \hat{\Sigma}^{n_3} \ \textit{and}\ |f| \le \mathrm{poly}(\lambda),\ \textit{s. t. :} \\ f = (f_1, f_2, f_3),\ f_1 : \hat{\Sigma}^{n_1} \to \hat{\Sigma}^{n_1},\ f_2 : \hat{\Sigma}^{n_2} \to \hat{\Sigma}^{n_2},\ f_3 : \hat{\Sigma}^{n_3} \to \hat{\Sigma}^{n_3}. \end{matrix} \right\},$$

and is leakage resilient against the class

$$\bar{\mathcal{G}} \stackrel{\text{def}}{=} \left\{ \begin{matrix} g : \hat{\Sigma}^{n_1} \times \hat{\Sigma}^{n_2} \times \hat{\Sigma}^{n_3} \to \{0,1\}^{\ell} \times \{0,1\}^{\ell} \times \{0,1\}^{\frac{n_3 \cdot \log|\hat{\Sigma}|}{6}} \\ \textit{and}\ |g| \le \mathrm{poly}(\lambda),\ \textit{s.t. :} \\ g = (g_1, g_2, g_3),\ g_1 : \hat{\Sigma}^{n_1} \to \{0,1\}^{\ell},\quad g_2 : \hat{\Sigma}^{n_2} \to \{0,1\}^{\ell}, \\ g_3 : \hat{\Sigma}^{n_3} \to \{0,1\}^{\frac{n_3 \cdot \log|\hat{\Sigma}|}{6}}. \end{matrix} \right\}.$$

Moreover, Π has relative leakage $\frac{\alpha}{8} - o(1)$.

Proof. To prove the theorem, for any efficient adversary $\mathcal{A}$, we must construct a simulator $\mathcal{S}$, such that for any initial database $D \in \Sigma^n$ and any efficient updater $\mathcal{U}$, the experiment of one time attack $\mathbf{TamperLeak}_{\mathcal{A},\mathcal{U},D}$ is indistinguishable from the ideal experiment $\mathbf{Ideal}_{\mathcal{S},\mathcal{U},D}$.

The simulator $\mathcal{S}$ first samples random coins for the updater $\mathcal{U}$, so its output just depends on its input given the random coins. Then $\mathcal{S}$ works as follows:

- Initially $\mathcal{S}$ samples $(\mathsf{pk}, \mathsf{sk}_{\varepsilon}^1, \mathsf{sk}_{\varepsilon}^2) \leftarrow \mathcal{E}.\mathsf{KeyGen}(1^\lambda, 1^\ell)$, $(\mathsf{vk}, \mathsf{sk}_\sigma) \leftarrow \mathcal{V}.\mathsf{Gen}(1^\lambda)$, $crs \leftarrow \mathsf{CRSGEN}(1^\lambda)$ and $h \leftarrow H$, sets $\tilde{D}_0 = 0$ and generates n encryptions of 0, i.e., $\tilde{D}_1, \tilde{D}_2, \ldots, \tilde{D}_n$ where $\tilde{D}_i \leftarrow \mathcal{E}.\mathsf{Encrypt}^{\mathsf{pk}}(0)$ for $i \in [n]$. Let $\tilde{D}^{(1)} := \tilde{D}_0, \tilde{D}_1, \ldots, \tilde{D}_n$. $\mathcal{S}$ computes $T_{\tilde{D}}^{(1)} := \mathsf{Tree}_h(\tilde{D}^{(1)})$. Let $\sigma^{(1)} = \mathcal{V}.\mathsf{Sign}^{\mathsf{sk}_\sigma}(R_{\tilde{D}}^{(1)})$, where $R_{\tilde{D}}^{(1)}$ is the root of the tree $T_{\tilde{D}}^{(1)}$. $\mathcal{S}$ computes $T_{\mathsf{sk}^i} := \mathsf{Tree}_h(\mathsf{sk}^i)$ for $i \in \{1, 2\}$, R_{sk^i} denotes the root of the tree T_{sk^i}. $\mathcal{S}$ keeps global variables $\mathsf{flag}, \mathsf{Leaked}, \mathsf{Tampered} = 0$.
- At each round j, let $C^{(j)} := (C_1^{(j)}, C_2^{(j)}, C_3^{(j)})$, where

  $$C_1^{(j)} := (\mathsf{sk}_{\varepsilon}^1, \mathsf{sk}_\sigma, T_{\mathsf{sk}^1}, R_{\mathsf{sk}^1}) \quad C_2^{(j)} := (\mathsf{sk}_{\varepsilon}^2, T_{\mathsf{sk}^2}, R_{\mathsf{sk}^2})$$

  $$C_3^{(j)} := (\mathsf{pk}, \mathsf{vk}, \tilde{D}^{(j)}, T_{\tilde{D}}^{(j)}, R_{\tilde{D}}^{(j)}, \sigma^{(j)}, \pi_{PCP}),$$

  denote the current simulated codeword stored by $\mathcal{S}$ and let $w^{(j)}$ denote the simulator's output in the previous round. In the first round, $w_i^{(0)} := \mathsf{same}$ for all $i \in [n]$. In each round, $\mathcal{S}$ does the following:

Simulating Update:

- If $\mathsf{flag} = 0$, $\mathcal{S}$ does the following: Receives an index $i^{(j)} \in [n]$ from the updater. Runs $\mathsf{UPDATE}^{C^{(j)}}(i^{(j)}, 0)$. Let $C^{(j+1)}$ be the resulting codeword after the update.
- If $\mathsf{flag} = 1$, $\mathcal{S}$ does the following: Computes $(i^{(j)}, v) \leftarrow \mathcal{U}(\boldsymbol{w}^{(j)})$ on his own, and runs $\mathsf{UPDATE}^{C^{(j)}}(i^{(j)}, v)$. Let $C^{(j+1)}$ be the resulting codeword after the update.

Simulating the Round's Output:

- $\mathcal{S}$ sets $(\tilde{D}_0, \tilde{D}_1, \ldots, \tilde{D}_n) := \tilde{D}^{(j+1)}$.
- $\mathcal{S}$ emulates the adversary $\mathcal{A}$ and receives $g_1, g_2, g_3 \in \bar{\mathcal{G}}$ and $f_1, f_2, f_3 \in \bar{\mathcal{F}}$.
- If Leaked is 0, then $\mathcal{S}$ computes $\ell_1 := g_1(\mathsf{sk}_\varepsilon^1, \mathsf{sk}_\sigma, T_{\mathsf{sk}^1}, R_{\mathsf{sk}^1})$, $\ell_2 := g_2(\mathsf{sk}_\varepsilon^2, T_{\mathsf{sk}^2}, R_{\mathsf{sk}^2})$, $\ell_3 := g_3(\mathsf{pk}, \mathsf{vk}, \tilde{D}^{(j+1)}, T_{\tilde{D}}^{(j+1)}, R_{\tilde{D}}^{(j+1)}, \sigma^{(j+1)}, \pi_{PCP})$ sets $\ell := (\ell_1, \ell_2, \ell_3)$ and sets Leaked to 1.
- If $\mathsf{Leaked} = 1$ and $\mathsf{Tampered} = 0$, $\mathcal{S}$ computes $C' = (C_1', C_2', C_3')$ where

  $$C_1' := (\mathsf{sk}_\varepsilon^{'1}, \mathsf{sk}_\sigma', T_{\mathsf{sk}^1}', R_{\mathsf{sk}^1}') := f_1(C_1) \quad C_2' := (\mathsf{sk}_\varepsilon^{'2}, T_{\mathsf{sk}^2}', R_{\mathsf{sk}^2}') := f_2(C_2)$$

  $$C_3' := (\mathsf{pk}', \mathsf{vk}', \tilde{D}', T_{\tilde{D}'}', R_{\tilde{D}'}', \sigma', \pi_{PCP}') := f_3(C_3).$$

  and sets $\mathsf{Tampered}$ to 1.
- If $\mathsf{flag} = 0$, $\mathcal{S}$ does the following:
  - $\mathcal{S}$ sets $\mathcal{I}^{(j+1)} = \{u : \forall u \in [n]\ s.t.\ \tilde{D}_u' \neq \tilde{D}_u \vee \mathsf{DEC}^{C'}(u) = \perp\}$, i.e. the indices where $\tilde{D}'$ is not equal to $\tilde{D}$ or where decode evaluates to $\perp$. $\mathcal{S}$ sets $\mathcal{I}^{(j+1)} = [n]$ if $x_{NIZK}' \neq x_{NIZK}$. If $\mathcal{I}^{(j+1)} = [n]$, $\mathcal{S}$ sets $\mathsf{flag} := 1$. If $\mathcal{I}^{(j+1)} \neq [n]$, $\mathcal{S}$ outputs $\{\ell, \boldsymbol{w}^{(j+1)}\}$, where $w^{(j+1)}[i] = \perp$ for $i \in \mathcal{I}^{(j+1)}$ and $w^{(j+1)}[i] = \mathit{same}$ for $i \notin \mathcal{I}^{(j+1)}$.
- If $\mathsf{flag} = 1$, $\mathcal{S}$ simulates the real experiment faithfully: For $i \in [n]$, $\mathcal{S}$ sets $\boldsymbol{w}^{(j+1)}[i] := \mathsf{DEC}^{(C')}(i)$, i.e. running the real decoding algorithm. Then $\mathcal{S}$ outputs $\{\ell, \boldsymbol{w}^{(j+1)}\}$.

To show $\mathbf{TamperLeak}_{\mathcal{A},\mathcal{U},D} \approx \mathbf{Ideal}_{\mathcal{S},\mathcal{U},D}$, we consider several hybrids.

Hybrid H_0: This is exactly the experiment $\mathbf{Ideal}_{\mathcal{S},\mathcal{U},D}$.

Hybrid H_1: Change π_{PCP} to a simulated proof, using ZK property of the underlying NIZK.

Claim 3.1. $H_0 \overset{c}{\approx} H_1$.

Event EV_3: $x_{NIZK} \neq x_{NIZK}'$, the verifier accepts, but the extractor fails to extract the witness from π_{PCP}.

The following claim is due to the simulation-sound extractability property of the proof system.

Claim 3.2. *EV_3 occurs with negligible probability in hybrid H_1.*

Hybrid H_2: We use the knowledge extractor of the PCP and NIZK to extract $\mathsf{sk}'_\varepsilon, \mathsf{sk}'_\sigma$. Everything in the decoding algorithm remains the same up to the final bullet in which the decryption is done by using sk'_ε, instead of using the contents of memory. Everything in the update algorithm also remains the same up to second to last bullet, where signing will now be done with sk'_σ, instead of using the contents of memory.

The following claim is due to collision resistance of h.

Claim 3.3. $H_1 \overset{c}{\approx} H_2$.

Hybrid H_3: The simulator does not encrypt all 0's (i.e. $\mathcal{E}.\mathsf{Encrypt}^{\mathsf{pk}}(0)$); instead, it encrypts the real messages.

Claim 3.4. $H_2 \overset{c}{\approx} H_3$.

Proof. Assume there exists an efficient adversary $\mathcal{A}$ distinguishing hybrids H_2 and H_3 with non-negligible advantage. We construct an efficient adversary $\mathcal{A}'$ breaking the SS-BRM-PKE-CCA security of the encryption scheme $\mathcal{E}$. $\mathcal{A}'$ participates externally in the security game for the SS-BRM PKE scheme (See Subsection 2.2 for definition) while internally instantiating $\mathcal{A}$. We next describe $\mathcal{A}'$:

- $\mathcal{A}'$ receives pk from **Key Generation** of its external challenger.
- $\mathcal{A}'$ samples $(\mathsf{vk}, \mathsf{sk}_\sigma) \leftarrow \mathcal{V}.\mathsf{Gen}(1^\lambda)$, $h \leftarrow H$, $(crs', \tau, \xi) \leftarrow SE_1(1^\lambda)$. $\mathcal{A}'$ sets $CRS := (crs', h)$.
- Let $D_1, \ldots, D_n$ denote the initial contents of the database. $\mathcal{A}'$ runs the updater (with fixed coins, as described above) to obtain all the updates $D'_1, \ldots, D'_p$ in advance (where $p := p(\lambda)$ for polynomial $p(\cdot)$ denotes the runtime of the Updater). $\mathcal{A}'$ submits vectors of messages $\boldsymbol{D}_0, \boldsymbol{D}_1$, of dimension $n+p$, as **Message Commitment**. Where $\boldsymbol{D}_0$ is a vector of all 0's and $\boldsymbol{D}_1$ corresponds to the messages as described above.
- $\mathcal{A}'$ instantiates $\mathcal{A}$ on input CRS and waits to receive leakage query (g_1, g_2, g_3) from $\mathcal{A}$.
- Upon receiving leakage query (g_1, g_2, g_3), $\mathcal{A}'$ submits the following **Pre-challenge** split-state leakage query to its challenger:

$$G_1(\mathsf{sk}^1_\varepsilon) := (\mathsf{Root}_h(\mathsf{Tree}_h(\mathsf{sk}^1_\varepsilon, \mathsf{sk}_\sigma)), g_1(\mathsf{sk}^1_\varepsilon, \mathsf{sk}_\sigma, T_{\mathsf{sk}^1}, R_{\mathsf{sk}^1}))$$
$$G_2(\mathsf{sk}^2_\varepsilon) := (\mathsf{Root}_h(\mathsf{Tree}_h(\mathsf{sk}^2_\varepsilon), g_2(\mathsf{sk}^2_\varepsilon, T_{\mathsf{sk}^2}, R_{\mathsf{sk}^2})),$$

  where $R_{\mathsf{sk}^1} := \mathsf{Root}_h(\mathsf{Tree}_h(\mathsf{sk}^1_\varepsilon, \mathsf{sk}_\sigma))$ and $R_{\mathsf{sk}^2} := \mathsf{Root}_h(\mathsf{Tree}_h(\mathsf{sk}^2_\varepsilon))$.
- $\mathcal{A}'$ receives in return the output of its leakage queries $(R_{\mathsf{sk}^1}||\ell_1, R_{\mathsf{sk}^2}||\ell_2)$ as well as challenge ciphertexts $\tilde{D}_i$, $i \in [n]$ and $\tilde{D}'_j$, $j \in [p]$. Let $\tilde{D}^{(1)} := (\tilde{D}_1, \ldots, \tilde{D}_n, \tilde{D}'_1, \ldots, \tilde{D}'_p)$. $\mathcal{A}'$ computes $T^{(1)}_{\tilde{D}} := \mathsf{Tree}_h(\tilde{D}^{(1)})$ and computes $\sigma^{(1)} = \mathcal{V}.\mathsf{Sign}^{\mathsf{sk}_\sigma}(R^{(1)}_{\tilde{D}})$, where $R^{(1)}_{\tilde{D}} := \mathsf{Root}_h(\mathsf{Tree}_h(\tilde{D}^{(1)}))$. $\mathcal{A}'$ keeps global variables $\mathsf{flag}, \mathsf{Leaked}, \mathsf{Tampered} = 0$.

- $\mathcal{A}'$ uses the simulated proof $\pi'_{NIZK} \leftarrow \mathcal{S}_2(crs', \tau, x_{NIZK} = (R_{\mathsf{sk}^1}, R_{\mathsf{sk}^2}))$ to construct the simulated PCP proof π'_{PCP}. Note that $\mathcal{A}'$ now knows the entire contents of the third partition of the codeword, $C_3 := (\mathsf{pk}, \mathsf{vk}, \tilde{D}^{(1)}, T^{(1)}_{\tilde{D}}, R^{(1)}_{\tilde{D}'}, \sigma^{(1)}, \pi'_{PCP}))$. Also note that we assume the proof π'_{PCP} contains the statement x'_{PCP} (and thus also x'_{NIZK}) to be proven, which includes the hash values $R_{\mathsf{sk}^1}, R_{\mathsf{sk}^2}$.
- $\mathcal{A}'$ rewinds $\mathcal{A}$ back to the beginning and instantiates $\mathcal{A}$.
- At each round j, let

$$C_3^{(j)} := (\mathsf{pk}, \mathsf{vk}, \tilde{D}^{(j)}, T^{(j)}_{\tilde{D}}, R^{(j)}_{\tilde{D}}, \sigma^{(j)}, \pi'_{PCP})$$

denote the third partition of the current simulated codeword stored by $\mathcal{A}'$. We maintain the invariant that $\mathcal{A}'$ knows the entire contents of $C_3^{(j)}$, for $j \in [p]$. Let $w^{(j)}$ denote the simulator's output in the previous round. In the first round, $w_i^{(0)} := \mathsf{same}$ for all $i \in [n]$. In each round, $\mathcal{A}'$ does the following:

Simulating Update:

- If $\mathsf{flag} = 0$, $\mathcal{A}'$ does the following: Computes the next index $i^{(j)} \in [n]$ generated by the updater. Runs $\overline{\mathsf{UPDATE}}^{C^{(j)}}(i^{(j)}, \perp, \tilde{D}'_j)$. Let $C^{(j+1)}$ be the resulting codeword after the update.
- If $\mathsf{flag} = 1$, $\mathcal{A}'$ does the following: Computes $(i^{(j)}, v) \leftarrow \mathcal{U}(\boldsymbol{w}^{(j)})$ on his own, and runs $\overline{\mathsf{UPDATE}}^{C^{(j)}}(i^{(j)}, v, \perp)$. Let $C^{(j+1)}$ be the resulting codeword after the update.

Simulating the Round's Output:

- $\mathcal{A}'$ sets $(\tilde{D}_0, \tilde{D}_1, \ldots, \tilde{D}_n) := \tilde{D}^{(j+1)}$, $T_{\tilde{D}} := T^{(j+1)}_{\tilde{D}}$, and $R_{\tilde{D}} := R^{(j+1)}_{\tilde{D}}$ and $\sigma = \sigma^{(j+1)}$.
- $\mathcal{A}'$ emulates the adversary $\mathcal{A}$ and receives $g_1, g_2, g_3 \in \bar{\mathcal{G}}$, $f_1, f_2, f_3 \in \bar{\mathcal{F}}$.
- If Leaked is 0, then $\mathcal{A}'$ computes $\ell_3 := g_3(C_3^{(j+1)})$ (recall ℓ_1, ℓ_2 were received previously), returns $\ell := (\ell_1, \ell_2, \ell_3)$ to $\mathcal{A}$ and sets Leaked to 1.
- If Leaked is 1 and $\mathsf{Tampered}$ is 0, then $\mathcal{A}'$ computes $C'_3 := f_3(C_3^{(j+1)})$, and sets $\mathsf{Tampered}$ to 1. $\mathcal{A}'$ submits the following **Post-challenge** split-state leakage query to its challenger: $F_1(\mathsf{sk}^1_\varepsilon) := f'_1(\mathsf{sk}^1_\varepsilon, \mathsf{sk}_\sigma, R^{(j+1)}_{\mathsf{sk}^1})$ and $F_2(\mathsf{sk}^2_\varepsilon) := f'_2(\mathsf{sk}^2_\varepsilon, R^{(j+1)}_{\mathsf{sk}^2})$, where f'_1 computes $C'_1 := f_1(C_1^{(j+1)})$ and then outputs a vector $\boldsymbol{\eta_1} \in \{0,1\}^{n'_1}$ such that for all $i \in [n'_1]$, $\boldsymbol{\eta_1}[i] = 1$ if the path p_i in the Merkle tree in C'_1 is consistent with the root contained in π'_{PCP} and 0 otherwise. Similarly, f'_2 computes $C'_2 := f_2(C_2^{(j+1)})$ and then outputs a vector $\boldsymbol{\eta_2} \in \{0,1\}^{n'_2}$ such that for all $i \in [n'_2]$, $\boldsymbol{\eta_2}[i] = 1$ if the path p_i in in the Merkle tree in C'_2 is consistent with the root contained in π'_{PCP} and 0 otherwise.
- $\mathcal{A}'$ additionally receives the **Decryption Access Patterns** for the challenge ciphertexts, i.e. , $(S_i^1, S_i^2) \xleftarrow{Access} \mathcal{E}.\mathsf{Decrypt}^{\mathsf{sk}^1_\varepsilon || \mathsf{sk}^2_\varepsilon}(\tilde{D}_i)$, $i \in [n]$ and $(S_j^1, S_j^2) \xleftarrow{Access} \mathcal{E}.\mathsf{Decrypt}^{\mathsf{sk}^1_\varepsilon || \mathsf{sk}^2_\varepsilon}(\tilde{D}'_j)$, $j \in [p]$.

- If $\mathsf{flag} = 0$, $\mathcal{A}'$ does the following:
  - $\mathcal{A}'$ sets $\mathcal{I}^{(j+1)} = \{u : \forall u \in [n] \ s.t. \ \tilde{D}'_u \neq \tilde{D}_u \vee \overline{\mathsf{DEC}}^{C'}(u) = \perp\}$, i.e. the indices where $\tilde{D}'$ is not equal to $\tilde{D}$ or where decode evaluates to $\perp$. $\mathcal{A}'$ checks π'_{PCP} and sets $\mathcal{I}^{(j+1)} = [n]$ if $x'_{NIZK} \neq x_{NIZK}$. If $\mathcal{I}^{(j+1)} = [n]$, $\mathcal{A}'$ sets $\mathsf{flag} := 1$. If $\mathcal{I}^{(j+1)} \neq [n]$, $\mathcal{S}$ outputs $\{\ell, \boldsymbol{w}^{(j+1)}\}$, where $w^{(j+1)}[i] = \perp$ for $i \in \mathcal{I}^{(j+1)}$ and $w^{(j)}[i] = \mathit{same}$ for $i \notin \mathcal{I}^{(j+1)}$.
- If $\mathsf{flag} = 1$, $\mathcal{A}'$ sets $\boldsymbol{w}^{(j+1)}[i] := \overline{\mathsf{DEC}}^{(C')}(i)$, for $i \in [n]$, and outputs $\{\ell, \boldsymbol{w}^{(j+1)}\}$.

– Once p rounds have completed, $\mathcal{A}'$ outputs whatever $\mathcal{A}$ does and terminates.

$\overline{\mathsf{DEC}}$, $\overline{\mathsf{UPDATE}}$ are defined as follows.

– $\overline{\mathsf{DEC}}^{C}(i)$: On input $i \in [n]$ in round $j \in [p]$:

- Parse $C_3 := (\mathsf{pk}', \mathsf{vk}', \tilde{D}, T_{\tilde{D}}, R_{\tilde{D}}, \sigma, \pi'_{PCP})$.
- Check whether $\tilde{D}_0 := 0$. If not, output $\perp$ and terminate.
- Read path p_i in $T_{\tilde{D}}$, corresponding to leaf i and use p_i to recompute $\hat{R} = \mathsf{Root}_h(p_i)$.
- Check that $\hat{R} := R_{\tilde{D}}$. If not, output $\perp$ and terminate.
- Check that $\mathcal{V}.\mathsf{Verify}^{\mathsf{vk}'}(R_{\tilde{D}}, \sigma) = 1$. If not, output $\perp$ and terminate.
- Run $V_{PCP}(crs', \pi'_{PCP})$ if outputs 0, output $\perp$ and terminate.
- Let $(\mathcal{S}^1_j, \mathcal{S}^2_j)$ be decryption access patterns; $\forall s^1 \in S^1_j$ and $\forall s^2 \in S^2_j$, if $\boldsymbol{\eta_1}[s^1] = 1$ and $\boldsymbol{\eta_2}[s^2] = 1$ then continue. Else, output $\perp$ and terminate.
- If $x'_{NIZK} \neq x_{NIZK}$ output $D_i := \mathcal{E}.\mathsf{Decrypt}^{\mathsf{sk}'_\varepsilon}(\tilde{D}_i)$, where $\mathsf{sk}'_\varepsilon \leftarrow \mathit{\Pi}_{NIZK}.E_2(crs', \xi, \pi_{NIZK})$ is the secret key extracted from the proof π'_{PCP}. E_2 is the witness extractor similar to Definition 15. Else, compute $D_i := \mathcal{E}.\mathsf{Decrypt}^{\mathsf{sk}_\varepsilon}(\tilde{D}_i)$, by querying the decryption oracle for the CCA secure $\mathsf{SS\text{-}BRM\text{-}PKE}$ with the original secret key.

– $\overline{\mathsf{UPDATE}}^{C}(i, v, \tilde{D}'_j)$: On inputs an index $i \in [n]$, a value $v \in \Sigma$ and a ciphertext $\tilde{D}'_j \in \widehat{\Sigma}$ in round $j \in [p]$:

- Run $\overline{\mathsf{DEC}}^{C}(i)$. If it outputs $\perp$, set $\tilde{D}_0 := 1$, write back to memory and terminate.
- Parse $C_3 := (\mathsf{pk}', \mathsf{vk}', \tilde{D}, T_{\tilde{D}}, R_{\tilde{D}}, \sigma, \pi'_{PCP})$.
- If $v = \perp$, Let $\tilde{D}' := \tilde{D}_0, \ldots, \tilde{D}_{i-1}, \tilde{D}'_j, \tilde{D}_{i+1}, \ldots, \tilde{D}_n$. Read path p_i in $T_{\tilde{D}}$, corresponding to leaf i and use $(p_i, \tilde{D}'_j)$ to compute a new path p'_i (that replaces $\tilde{D}_i$ by $\tilde{D}'_j$). Set $R_{\tilde{D}'} = \mathsf{Root}_h(p'_i)$. Let $T_{\tilde{D}'}$ denote the updated tree.
- If $v \neq \perp$, set $\tilde{D}''_i \leftarrow \mathcal{E}.\mathsf{Encrypt}^{\mathsf{pk}'}(v)$. Otherwise, set $\tilde{D}''_i := \tilde{D}'_j$. Let $\tilde{D}' := \tilde{D}_0, \ldots, \tilde{D}_{i-1}, \tilde{D}''_i, \tilde{D}_{i+1}, \ldots, \tilde{D}_n$. Read path p_i in $T_{\tilde{D}}$, corresponding to leaf i and use $(p_i, \tilde{D}''_i))$ to compute a new path p'_i (that replaces $\tilde{D}_i$ by $\tilde{D}''_i$). Set $R_{\tilde{D}'} = \mathsf{Root}_h(p'_i)$. Let $T_{\tilde{D}'}$ denote the updated tree.
- Let $S^\sigma_j \xleftarrow{Access} \mathcal{V}.\mathsf{Sign}^{\mathsf{sk}_\sigma}(R_{\tilde{D}'})$; $\forall s \in S^\sigma_j$, if $\boldsymbol{\eta_1}[s] = 1$ then continue. Else, output $\perp$ and terminate.

- If $x'_{NIZK} \neq x_{NIZK}$ Compute $\sigma' := \mathcal{V}.\mathsf{Sign}^{\mathsf{sk}'_\sigma}(R'_{\tilde{D}})$, where $\mathsf{sk}'_\sigma \leftarrow E_2(crs, \xi, \pi_{NIZK})$ is the secret key extracted from the proof π'_{PCP}. E_2 is the witness extractor similar to Definition 15. Otherwise, compute $\sigma' := \mathcal{V}.\mathsf{Sign}^{\mathsf{sk}_\sigma}(R'_{\tilde{D}})$, where where sk_σ is the original secret key.
- Write back $(\tilde{D}'_i, p'_i, R_{\tilde{D}'}, \sigma')$ yielding updated codeword

$$C'_3 := (\mathsf{pk}', \mathsf{vk}', h, \tilde{D}', T_{\tilde{D}'}, R_{\tilde{D}'}, \sigma', \pi'_{PCP}).$$

If $\tilde{D}_i$, $i \in [n]$ and $\tilde{D}'_j$, $j \in [p]$ are encryptions of all 0's then the view of $\mathcal{A}$ is identical to its view in Hybrid H_2. Alternatively, if $\tilde{D}_i$, $i \in [n]$ and $\tilde{D}'_j$, $j \in [p]$ are encryptions of the honest data values, then the view of $\mathcal{A}$ is identical to its view in Hybrid H_3. Thus, if $\mathcal{A}$ distinguishes with non-negligible advantage, then $\mathcal{A}'$ distinguishes encryptions of all 0's from encryptions of correct data with non-negligible advantage, breaking the CCA security of the encryption scheme and resulting in contradiction.

Hybrid H_4: In the case that pk, vk are changed and $flag = 1$, go back to using $\mathsf{sk}^1_\varepsilon$ and $\mathsf{sk}^2_\varepsilon$ for decryption .

The following claim is due to collision resistance of h.

Claim 3.5. $H_3 \overset{c}{\approx} H_4$.

Hybrid H_5: Go back to using the real crs and real proof π_{PCP}.

The following claim is due to the zero knowledge property of the proof system.

Claim 3.6. $H_4 \overset{c}{\approx} H_5$.

Hybrid H_6: This is exactly the experiment $\mathbf{TamperLeak}_{\mathcal{A},\mathcal{U},D}$.

Claim 3.7. $H_5 \overset{c}{\approx} H_6$.

Proof. The only difference between H_5 and real experiment is the case where

$$\mathsf{flag} = 0, \tilde{\mathsf{D}}'_\mathsf{u} \neq \tilde{\mathsf{D}}_\mathsf{u} \text{ and } \mathsf{DEC}^{\mathsf{C}'}(\mathsf{u}) \neq \bot,$$

($\mathcal{S}$ would output $\bot$ at position u whereas real experiment would output $\mathsf{DEC}^{C'}(u) \neq \bot$) which can only happen if events EV_1 or EV_2 occur (see Figure 1 for their definition).

We next claim that both events occur with negligible probability, thus showing that Hybrids H_5 and H_6 differ with negligible probability.

Claim 3.8. EV_1 and EV_2 occur with negligible probability in H_5.

We omit the proof of the above claim since it is nearly identical to the corresponding claims in the proof of the construction for partial one-time tamper and leakage resilience and we refer reader to the full version of the paper [27] for that proof.

This completes the proof of Theorem 5.

Event EV_1:

- $\mathsf{pk}'||\mathsf{vk}' = \mathsf{pk}||\mathsf{vk}$. (otherwise $\mathsf{flag} = 1$)
- $\mathcal{I}^{(j+1)} \neq [n]$. (otherwise $\mathsf{flag} = 1$)
- $R' \neq R^{(j+1)}$.
- $\mathsf{Verify}(\mathsf{vk}, R', \sigma') = 1$.

Event EV_2:

- $\mathsf{pk}'||\mathsf{vk}' = \mathsf{pk}||\mathsf{vk}$. (otherwise $\mathsf{flag} = 1$)
- $\mathcal{I}^{(j+1)} \neq [n]$. (otherwise $\mathsf{flag} = 1$)
- $R' = R^{(j+1)}$.
- For some $i \in \mathcal{I}^{(j+1)}$, we have that for $\tilde{D}'_i$ and corresponding path p'_i, $R'_{\tilde{D}} = \mathsf{Root}_h(p'_i)$.

Fig. 1: Events EV_1 and EV_2.

References

1. Aggarwal, D., Agrawal, S., Gupta, D., Maji, H.K., Pandey, O., Prabhakaran, M.: Optimal computational split-state non-malleable codes. In: Kushilevitz and Malkin [59], pp. 393–417
2. Aggarwal, D., Dodis, Y., Kazana, T., Obremski, M.: Non-malleable reductions and applications. In: Servedio, R.A., Rubinfeld, R. (eds.) 47th ACM STOC. pp. 459–468. ACM Press (Jun 2015)
3. Aggarwal, D., Dodis, Y., Lovett, S.: Non-malleable codes from additive combinatorics. In: Shmoys, D.B. (ed.) 46th ACM STOC. pp. 774–783. ACM Press (May / Jun 2014)
4. Aggarwal, D., Dziembowski, S., Kazana, T., Obremski, M.: Leakage-resilient non-malleable codes. In: Dodis and Nielsen [32], pp. 398–426
5. Aggarwal, D., Kazana, T., Obremski, M.: Inception makes non-malleable codes stronger. Cryptology ePrint Archive, Report 2015/1013 (2015), http://eprint.iacr.org/2015/1013
6. Agrawal, S., Gupta, D., Maji, H.K., Pandey, O., Prabhakaran, M.: Explicit non-malleable codes against bit-wise tampering and permutations. In: Gennaro, R., Robshaw, M.J.B. (eds.) CRYPTO 2015, Part I. LNCS, vol. 9215, pp. 538–557. Springer, Heidelberg (Aug 2015)
7. Agrawal, S., Gupta, D., Maji, H.K., Pandey, O., Prabhakaran, M.: A rate-optimizing compiler for non-malleable codes against bit-wise tampering and permutations. In: Dodis and Nielsen [32], pp. 375–397
8. Akavia, A., Goldwasser, S., Vaikuntanathan, V.: Simultaneous hardcore bits and cryptography against memory attacks. In: Reingold, O. (ed.) TCC 2009. LNCS, vol. 5444, pp. 474–495. Springer, Heidelberg (Mar 2009)
9. Alwen, J., Dodis, Y., Naor, M., Segev, G., Walfish, S., Wichs, D.: Public-key encryption in the bounded-retrieval model. In: Gilbert, H. (ed.) EUROCRYPT 2010. LNCS, vol. 6110, pp. 113–134. Springer, Heidelberg (May 2010)
10. Alwen, J., Dodis, Y., Wichs, D.: Leakage-resilient public-key cryptography in the bounded-retrieval model. In: Halevi [48], pp. 36–54
11. Alwen, J., Dodis, Y., Wichs, D.: Survey: Leakage resilience and the bounded retrieval model. In: Kurosawa, K. (ed.) ICITS 09. LNCS, vol. 5973, pp. 1–18. Springer, Heidelberg (Dec 2010)
12. Ball, M., Dachman-Soled, D., Kulkarni, M., Malkin, T.: Non-malleable codes for bounded depth, bounded fan-in circuits. In: Fischlin, M., Coron, J.S. (eds.) EUROCRYPT 2016, Part II. LNCS, vol. 9666, pp. 881–908. Springer, Heidelberg (May 2016)

13. Ball, M., Dachman-Soled, D., Kulkarni, M., Malkin, T.: Non-malleable codes from average-case hardness: AC0, decision trees, and streaming space-bounded tampering. Cryptology ePrint Archive, Report 2017/1061 (2017), http://eprint.iacr.org/2017/1061
14. Ben-Sasson, E., Chiesa, A., Genkin, D., Tromer, E.: On the concrete efficiency of probabilistically-checkable proofs. In: Boneh, D., Roughgarden, T., Feigenbaum, J. (eds.) 45th ACM STOC. pp. 585–594. ACM Press (Jun 2013)
15. Cash, D., Ding, Y.Z., Dodis, Y., Lee, W., Lipton, R.J., Walfish, S.: Intrusion-resilient key exchange in the bounded retrieval model. In: Vadhan, S.P. (ed.) TCC 2007. LNCS, vol. 4392, pp. 479–498. Springer, Heidelberg (Feb 2007)
16. Chandran, N., Goyal, V., Mukherjee, P., Pandey, O., Upadhyay, J.: Block-wise non-malleable codes. Cryptology ePrint Archive, Report 2015/129 (2015), http://eprint.iacr.org/2015/129
17. Chandran, N., Kanukurthi, B., Ostrovsky, R.: Locally updatable and locally decodable codes. In: Lindell [61], pp. 489–514
18. Chandran, N., Kanukurthi, B., Raghuraman, S.: Information-theoretic local non-malleable codes and their applications. In: Kushilevitz and Malkin [59], pp. 367–392
19. Chattopadhyay, E., Li, X.: Non-malleable codes and extractors for small-depth circuits, and affine functions. In: Hatami, H., McKenzie, P., King, V. (eds.) 49th ACM STOC. pp. 1171–1184. ACM Press (Jun 2017)
20. Chattopadhyay, E., Zuckerman, D.: Non-malleable codes against constant split-state tampering. In: 55th FOCS. pp. 306–315. IEEE Computer Society Press (Oct 2014)
21. Chattopadhyay, E., Zuckerman, D.: Explicit two-source extractors and resilient functions. In: Wichs and Mansour [69], pp. 670–683
22. Cheraghchi, M., Guruswami, V.: Capacity of non-malleable codes. In: Naor, M. (ed.) ITCS 2014. pp. 155–168. ACM (Jan 2014)
23. Cheraghchi, M., Guruswami, V.: Non-malleable coding against bit-wise and split-state tampering. In: Lindell [61], pp. 440–464
24. Choi, S.G., Kiayias, A., Malkin, T.: BiTR: Built-in tamper resilience. In: Lee, D.H., Wang, X. (eds.) ASIACRYPT 2011. LNCS, vol. 7073, pp. 740–758. Springer, Heidelberg (Dec 2011)
25. Coretti, S., Dodis, Y., Tackmann, B., Venturi, D.: Non-malleable encryption: Simpler, shorter, stronger. In: Kushilevitz, E., Malkin, T. (eds.) TCC 2016-A, Part I. LNCS, vol. 9562, pp. 306–335. Springer, Heidelberg (Jan 2016)
26. Coretti, S., Maurer, U., Tackmann, B., Venturi, D.: From single-bit to multi-bit public-key encryption via non-malleable codes. In: Dodis and Nielsen [32], pp. 532–560
27. Dachman-Soled, D., Kulkarni, M., Shahverdi, A.: Locally decodable and updatable non-malleable codes in the bounded retrieval model. Cryptology ePrint Archive, Report 2017/303 (2017), https://eprint.iacr.org/2017/303
28. Dachman-Soled, D., Kulkarni, M., Shahverdi, A.: Tight upper and lower bounds for leakage-resilient, locally decodable and updatable non-malleable codes. In: Fehr, S. (ed.) PKC 2017, Part I. LNCS, vol. 10174, pp. 310–332. Springer, Heidelberg (Mar 2017)
29. Dachman-Soled, D., Liu, F.H., Shi, E., Zhou, H.S.: Locally decodable and updatable non-malleable codes and their applications. In: Dodis and Nielsen [32], pp. 427–450
30. Di Crescenzo, G., Lipton, R.J., Walfish, S.: Perfectly secure password protocols in the bounded retrieval model. In: Halevi and Rabin [49], pp. 225–244

31. Dodis, Y., Kalai, Y.T., Lovett, S.: On cryptography with auxiliary input. In: Mitzenmacher, M. (ed.) 41st ACM STOC. pp. 621–630. ACM Press (May / Jun 2009)
32. Dodis, Y., Nielsen, J.B. (eds.): TCC 2015, Part I, LNCS, vol. 9014. Springer, Heidelberg (Mar 2015)
33. Dodis, Y., Ristenpart, T., Vadhan, S.P.: Randomness condensers for efficiently samplable, seed-dependent sources. In: Cramer, R. (ed.) TCC 2012. LNCS, vol. 7194, pp. 618–635. Springer, Heidelberg (Mar 2012)
34. Dolev, D., Dwork, C., Naor, M.: Nonmalleable cryptography. SIAM Journal on Computing 30(2), 391–437 (2000)
35. Dziembowski, S.: Intrusion-resilience via the bounded-storage model. In: Halevi and Rabin [49], pp. 207–224
36. Dziembowski, S., Kazana, T., Obremski, M.: Non-malleable codes from two-source extractors. In: Canetti, R., Garay, J.A. (eds.) CRYPTO 2013, Part II. LNCS, vol. 8043, pp. 239–257. Springer, Heidelberg (Aug 2013)
37. Dziembowski, S., Kazana, T., Wichs, D.: Key-evolution schemes resilient to space-bounded leakage. In: Rogaway [68], pp. 335–353
38. Dziembowski, S., Pietrzak, K.: Intrusion-resilient secret sharing. In: 48th FOCS. pp. 227–237. IEEE Computer Society Press (Oct 2007)
39. Dziembowski, S., Pietrzak, K., Wichs, D.: Non-malleable codes. In: Yao, A.C.C. (ed.) ICS 2010. pp. 434–452. Tsinghua University Press (Jan 2010)
40. Faonio, A., Nielsen, J.B., Venturi, D.: Fully leakage-resilient signatures revisited. Theor. Comput. Sci. 660(C), 23–56 (Jan 2017), https://doi.org/10.1016/j.tcs.2016.11.016
41. Faust, S., Hostáková, K., Mukherjee, P., Venturi, D.: Non-malleable codes for space-bounded tampering. In: Katz, J., Shacham, H. (eds.) CRYPTO 2017, Part II. LNCS, vol. 10402, pp. 95–126. Springer, Heidelberg (Aug 2017)
42. Faust, S., Mukherjee, P., Nielsen, J.B., Venturi, D.: Continuous non-malleable codes. In: Lindell [61], pp. 465–488
43. Faust, S., Mukherjee, P., Nielsen, J.B., Venturi, D.: A tamper and leakage resilient von neumann architecture. In: Katz, J. (ed.) PKC 2015. LNCS, vol. 9020, pp. 579–603. Springer, Heidelberg (Mar / Apr 2015)
44. Faust, S., Mukherjee, P., Venturi, D., Wichs, D.: Efficient non-malleable codes and key-derivation for poly-size tampering circuits. In: Nguyen, P.Q., Oswald, E. (eds.) EUROCRYPT 2014. LNCS, vol. 8441, pp. 111–128. Springer, Heidelberg (May 2014)
45. Gennaro, R., Lysyanskaya, A., Malkin, T., Micali, S., Rabin, T.: Algorithmic tamper-proof (ATP) security: Theoretical foundations for security against hardware tampering. In: Naor, M. (ed.) TCC 2004. LNCS, vol. 2951, pp. 258–277. Springer, Heidelberg (Feb 2004)
46. Goyal, V., Pandey, O., Richelson, S.: Textbook non-malleable commitments. In: Wichs and Mansour [69], pp. 1128–1141
47. Groth, J.: Simulation-sound NIZK proofs for a practical language and constant size group signatures. In: Lai, X., Chen, K. (eds.) ASIACRYPT 2006. LNCS, vol. 4284, pp. 444–459. Springer, Heidelberg (Dec 2006)
48. Halevi, S. (ed.): CRYPTO 2009, LNCS, vol. 5677. Springer, Heidelberg (Aug 2009)
49. Halevi, S., Rabin, T. (eds.): TCC 2006, LNCS, vol. 3876. Springer, Heidelberg (Mar 2006)
50. Ishai, Y., Prabhakaran, M., Sahai, A., Wagner, D.: Private circuits II: Keeping secrets in tamperable circuits. In: Vaudenay, S. (ed.) EUROCRYPT 2006. LNCS, vol. 4004, pp. 308–327. Springer, Heidelberg (May / Jun 2006)

51. Jafargholi, Z., Wichs, D.: Tamper detection and continuous non-malleable codes. In: Dodis and Nielsen [32], pp. 451–480
52. Kalai, Y.T., Kanukurthi, B., Sahai, A.: Cryptography with tamperable and leaky memory. In: Rogaway [68], pp. 373–390
53. Kanukurthi, B., Obbattu, S.L.B., Sekar, S.: Four-state non-malleable codes with explicit constant rate. In: Kalai, Y., Reyzin, L. (eds.) TCC 2017, Part II. LNCS, vol. 10678, pp. 344–375. Springer, Heidelberg (Nov 2017)
54. Katz, J., Trevisan, L.: On the efficiency of local decoding procedures for error-correcting codes. In: 32nd ACM STOC. pp. 80–86. ACM Press (May 2000)
55. Katz, J., Vaikuntanathan, V.: Signature schemes with bounded leakage resilience. In: Matsui, M. (ed.) ASIACRYPT 2009. LNCS, vol. 5912, pp. 703–720. Springer, Heidelberg (Dec 2009)
56. Kiayias, A., Liu, F.H., Tselekounis, Y.: Practical non-malleable codes from l-more extractable hash functions. In: Weippl, E.R., Katzenbeisser, S., Kruegel, C., Myers, A.C., Halevi, S. (eds.) ACM CCS 16. pp. 1317–1328. ACM Press (Oct 2016)
57. Kocher, P.C.: Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems. In: Koblitz, N. (ed.) CRYPTO'96. LNCS, vol. 1109, pp. 104–113. Springer, Heidelberg (Aug 1996)
58. Kocher, P.C., Jaffe, J., Jun, B.: Differential power analysis. In: Wiener, M.J. (ed.) CRYPTO'99. LNCS, vol. 1666, pp. 388–397. Springer, Heidelberg (Aug 1999)
59. Kushilevitz, E., Malkin, T. (eds.): TCC 2016-A, Part II, LNCS, vol. 9563. Springer, Heidelberg (Jan 2016)
60. Lindell, Y.: A simpler construction of cca2-secure public-key encryption under general assumptions. In: Biham, E. (ed.) EUROCRYPT 2003. LNCS, vol. 2656, pp. 241–254. Springer, Heidelberg (May 2003)
61. Lindell, Y. (ed.): TCC 2014, LNCS, vol. 8349. Springer, Heidelberg (Feb 2014)
62. Liu, F.H., Lysyanskaya, A.: Tamper and leakage resilience in the split-state model. In: Safavi-Naini, R., Canetti, R. (eds.) CRYPTO 2012. LNCS, vol. 7417, pp. 517–532. Springer, Heidelberg (Aug 2012)
63. Naor, M., Segev, G.: Public-key cryptosystems resilient to key leakage. In: Halevi [48], pp. 18–35
64. Naor, M., Yung, M.: Public-key cryptosystems provably secure against chosen ciphertext attacks. In: 22nd ACM STOC. pp. 427–437. ACM Press (May 1990)
65. Nielsen, J.B., Venturi, D., Zottarel, A.: Leakage-resilient signatures with graceful degradation. In: Krawczyk, H. (ed.) PKC 2014. LNCS, vol. 8383, pp. 362–379. Springer, Heidelberg (Mar 2014)
66. Pietrzak, K.: A leakage-resilient mode of operation. In: Joux, A. (ed.) EUROCRYPT 2009. LNCS, vol. 5479, pp. 462–482. Springer, Heidelberg (Apr 2009)
67. Regev, O.: On lattices, learning with errors, random linear codes, and cryptography. In: Gabow, H.N., Fagin, R. (eds.) 37th ACM STOC. pp. 84–93. ACM Press (May 2005)
68. Rogaway, P. (ed.): CRYPTO 2011, LNCS, vol. 6841. Springer, Heidelberg (Aug 2011)
69. Wichs, D., Mansour, Y. (eds.): 48th ACM STOC. ACM Press (Jun 2016)